OCCASION

This publication has been made available to the public on the occasion of the 50th anniversary of the United Nations Industrial Development Organisation.

DISCLAIMER

FAIR USE POLICY

CONTACT

Please contact publications@unido.org for further information concerning UNIDO publications.

For more information about UNIDO, please visit us at www.unido.org

UNITED NATIONS INDUSTRIAL DEVELOPMENT ORGANIZATION
Vienna International Centre, P.O. Box 300, 1400 Vienna, Austria
Tel: (+43-1) 26026-0 · www.unido.org · unido@unido.org

23179

UNIDO

Restricted Distr.
CONTRACT NO. 2004/210
June 2005

UNITED NATIONS INDUSTRIAL
DEVELOPMENT ORGANIZATION

ORGINAL: ENGLISH

CENTRE OF TECHNOLOGY TRANSFER
WARSAW UNIVERSITY OF TECHNOLOGY
(Project No.: XP/RER/04/009)

Report of the Training on Quality Improvement

Prof. Jan Bagiński
Representative of Warsaw University of Technology

M. Sc. Eng. Łukasz Babuśka
Representative of Warsaw University of Technology

Table of Contents

<u>Annex A</u>

Training materials

I. Background

Warsaw University of Technology is the biggest technical university in Poland. The WUT pays special attention to international cooperation in the areas of scientific research, technology, publications and culture. In 1999 the University had 162 bilateral agreements of cooperation with many universities and scientific institutions from all over the world.

In 1998 the University sent 2120 of its personnel, postgraduate PhD students and undergraduates to universities in 54 countries. At the same time, the University received 1055 people from 48 countries.

In the year 1998 there were 68 University employees who took part in the works of international organizations such as SEFI, ELLI, EAIE, IACEE, EUROPACE 2000, The Alliance of Universities for Democracy and many others. Many people work for publishers of international periodicals.

The WUT is proud of its participation in the following international programmes: TEMPUS II, TEMPUS II B, INCO-COPERNICUS, COST, the European Union's IV Framework Programme, Action Jean Monnet, PHARE, SOCRATES, LEONARDO, EUREKA.

Centre of Technology Transfer Warsaw University of Technology (CTT WUT) was founded in 1999 August 1st by Rector of Warsaw University of Technology. CTT WUT was created first of al for use great potential of WUT for Small and Medium Enterprises, also for big enterprises, and services. In not many years of activity CTT WUT have many successes, provide cooperation with many small, and medium enterprises, finished international research project with Fraunhofer Institute, and many others. CTT WUT provides many form of collaboration with industry, main form of activity is educational activities: training, seminar, instructions, workshops, individual advices for staff, specially for staff of SME's. Second equally important form of activity is transfer new technology, and new products from university to industry - specially to SME's. This joins with promotional, and educational activity provided by CTT. Centre of Technology Transfer have experienced high staff, and

many young ambitious collaborators, which provide wide activity. Moreover Centre have good collaboration with all faculty of Warsaw University of Technology, with many medium, and small enterprises, and with many government and private institutions.

Scope of the CTT Activities

The main business of the CTT is to help in implementing advanced methods, technologies and systems as well as to inform, to train and to consult. CTT cooperates with every Department of the Warsaw University of Technology, high-priority programmes, Branch Promotion Centres as well as with a couple of different industrial companies, in the following areas:

- modern technologies in the mechanical industries,
- new, advanced materials processes,
- chemical processes,
- electronic devices,
- information systems,
- Quality Assurance Systems, Integrated Management Systems, TQM,
- Environmental System,
- Industrial Safety System.

Mission of the CTT

Develop innovative forms of technology transfer from university to industry and to initiate new forms of education directed towards the companies that introduce new products with new, advanced technologies.

Goals of the CTT

- gathering information about industry's needs and relating it to the scientific potential of the Warsaw University of Technology, conducting research, development and implementation projects,
- R&D units integration, organizing teams of specialists from different areas, for managing research and developing projects,

- forging personal links between the University staff and that of the industry,
- stimulating and organizing scientific research and internal research,
- supplying solutions that meet our clients' requirements.

CTT offers cooperation in the following areas

- implementing new products, inventions, new technological processes and new organizational systems,
- helping create models and prototypes, testing new technological processes as well as elaborate new technologies (supported by 50% grants from the STATE COMMITEE FOR SCENTIFIC RESEARCH),
- organizing, conducting measurements and analyses for small and medium businesses,
- training and consulting.

CTT organizes training courses in the following areas

- Quality Assurance Systems ISO 9000:2000,
- Environmental Systems ISO 14000,
- Integrated Management Systems,
- Industrial Safety Systems (PN-N-18000),
- Total Quality Management (TQM),
- Information Systems.

The Centre of Technology Transfer is the most authoritative training body in Poland for conducting of trainings on:

1. **Security of IT information according to BS 7799-2:2002. Internal auditor training,**
2. **Quality management systems according to ISO 9001:2000 - Internal auditors training,**
3. **Software quality testing.**
4. **Environmental issues: EMAS (Environmental Management Audit Scheme), BAT (Best Available Techniques), BREF (Best available techniques Reference document).**

II. Justification

The general concept of trainings on quality and productivity improvement has become one of the key issues of modern enterprises therefore Centre of Technology Transfer has decided about conducting these trainings.

We have decided to perform these activities, in majority, for small and medium-sized enterprises from automotive parts manufacturers sub-sector because in this sub-sector of polish economy exists a great requirement of quality and productivity improvement. Naturally we have not forgot about different sub-sector of polish economy and small and medium-sized enterprises from other manufacturing sectors could also participate, but as the second priority.

Many developing countries, especially the least developed countries and countries with economies in transition need a help in fundraising so Centre of Technology Transfer have decided to ask a United Nations Industrial Development Organization (UNIDO) about support in conducting trainings.

United Nations Industrial Development Organization (UNIDO), through its programs on developing of industry promotes a quality and productivity improvement. On the basis of the above considerations, trainings on: Security of IT information according to BS 7799-2:2002, Quality management systems according to ISO 9001:2000, Software quality testing, Environmental issues: EMAS (Environmental Management Audit Scheme), BAT (Best Available Techniques), BREF (Best available techniques Reference document), was organized to bring polish companies better look at the issues of quality and productivity improvement. The trainings was held in Warsaw, Poland:

1. Security of IT information according to BS 7799-2:2002 – from 26 to 28 November 2004,
2. Quality management systems according to ISO 9001:2000 – from 3 to 5 December 2004,
3. Software quality testing – from 18 to 20 February 2005,

4. Environmental issues: EMAS (Environmental Management Audit Scheme), BAT (Best Available Techniques), BREF (Best available techniques Reference document) – from 4 to 6 March 2005.

III. Objectives

The hard aims of the trainings were:

- Security of IT information according to BS 7799-2:2002. Internal Auditor Training – Participants receive certificate which is granted by Det Norske Veritas on the basis of positive test results.
- Quality management systems according to ISO 9001:2000. Internal Auditor Training – Participants receive certificate which is granted by ZETOM Katowice on the basis of positive test results.
- Software quality testing – Participants receive certificate which is granted by Software KONFERENCJE on the basis of presence.
- Environmental issues: EMAS (Environmental Management Audit Scheme), BAT (Best Available Techniques), BREF (Best available techniques Reference document) – Participants receive certificate which is granted by RWTUV on the basis of presence.

The soft aims of the trainings were:

- *Security of IT information according to* BS 7799-2:2002. Internal Auditor Training.
  - To present a brief introduction and overview the structure of BS 7799-2:2002,
  - To overview the risk analysis,
  - To discuss about implementing of BS 7799-2:2002 in participant's companies.
- Quality management systems according to ISO 9001:2000. Internal Auditor Training.
  - To present a brief introduction and overview the structure of ISO 9001:2000,
  - To overview the PDCA,
  - To discuss about implementing of ISO 9001:2000 in participant's companies.
- Software quality testing.
  - To present a testing terminology.

- To present a black an white boxes techniques.
- To discuss about implementing different kinds of software tools.

- Environmental issues: EMAS (Environmental Management Audit Scheme), BAT (Best Available Techniques), BREF (Best available techniques Reference document).
  - To present a brief introduction and overview the structure of ISO 14001,
  - To present an Environmental Management Audit Scheme, Best Available Techniques, Best available techniques Reference document,
  - To discuss about benefits resulting from implementing of EMAS (Environmental Management Audit Scheme).

Training program: „Security of IT information according to BS 7799-2:2002 – Internal Auditor Training"

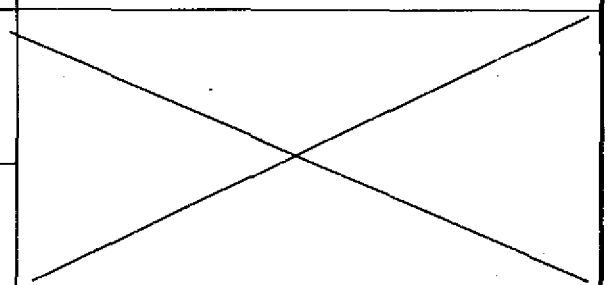
Duration: 3 days – 26 hours.

Time	τ min.	I Day	II Day	III Day
9.00 ⇓ 10.30	90'	Introduction. Interpretation of requirements according to BS 7799-2:2002 and overview guidelines from ISO 17799:2003.	Exercise 2.	Activities post audit. - report, - activities correcting/preventing
10.40 ⇓ 12.10	90'	Benefits from implementing a ISMS. Structure of management system documentation.	Presentation and analysis of the Exercise 2.	Exercise 4. Analysis of the Exercise 4.
12.20 ⇓ 13.40	80'	Interpretation of requirements according to BS 7799-2:2002. Exercise 1. Analysis of the Exercise 1.	Options of the risk management.	Certification process.
14.30 ⇓ 15.50	80'	What is audit ?. - audit of security information system, - auditor, attribute of auditors, - types of auditors.	Overview and identification of risks.	Exam and Summary.
16.00 ⇓ 17.10	70'	Preparation to the audit. - planning of audits, - audit reporting, - program of audit, - check lists.	Conducting of audit - techniques of auditing, - disagreement/observation.	
17.25 ⇓ 18.10	45'		Exercise 3. Analysis of the Exercise 3.	
Lecturer: Marcin Majdecki DNV				

Program of the Quality management systems according to ISO 9001:2000 – Internal Auditor Training.

Training program: „Quality management systems according to ISO 9001:2000 – Internal Auditor Training"

Duration: 3 days – 26 hours.

Time	τ min.	I Day	II Day	III Day
9.00 ⇓ 10.30	90'	Introduction. Series of ISO 9000:2000. Interpretation of requirements ISO 9001:2000	Exercise 3: „Formulating of disagreements" (work in groups)	Introduction to the exercise 6. Exercise 6: „Documenting and presenting conclusion from audit – protocols of *disagreement and closing meeting*".
10.40 ⇓ 12.10	90'	Disagreements. Reference. Classification. Exercise 1: „Reference and classification of disagreements". Analysis of the exercise 1.	Test part I. (20') Presentation and analysis of exercise 3.	Presentation and analysis of the exercise 6. Test part II. (60')
12.20 ⇓ 13.40	80'	Formulating of disagreements. Example. Exercise 2: „Formulating of disagreements" (work in groups)	Planning of the audit – program of audit and plan of audits. Check list. Example.	Audit report. Exercise 7: „Preparation of audit report"
14.30 ⇓ 15.50	80'	Analysis of the exercise 2. Quality audit. Process of quality audit.	Exercise 4: „Preparation of the audit plan and check list" (work in groups)	Analysis of the exercise 7. Summary.
16.00 ⇓ 17.10	70'	Process of quality audit. Auditor.	Analysis of the exercise 4. Introduction to the exercise 5. Exercise 5: „Audit conducting – simulation of the audit"	
17.25 ⇓ 18.10	45'		Exercise 5: „Audit conducting – simulation of the audit". Presentation and analysis if the exercise 5.	
Lecturer: ZETOM.				

Program of the Software quality testing training.

Training program: „ Software quality testing"

Duration: 3 days – 26 hours.

Time	τ min.	I Day	II Day	III Day
9.00 ⇓ 10.30	90'	Testing terminology. Why is testing necessary? How much testing is enough?	White and black boxes testing.	Types of CAST tool.
10.40 ⇓ 12.10	90'	Fundamental Test process. The psychology of testing. Re-testing and regression testing. Expected results.	Black boxes techniques	Tool selection.
12.20 ⇓ 13.40	80'	Prioritisation of the tests.	White boxes techniques	Tool implementation.
14.30 ⇓ 15.50	80'	Testing and the development lifecycle.	Errors guessing.	Summary.
16.00 ⇓ 17.10	70'	Process of testing modules.	Reviews and the test process. Types of review. Static analysis.	
17.25 ⇓ 18.10	45'		Test management. Organisation. Configuration Management. Test estimation, monitoring and control. Incident management. Standards for testing.	
Lecturer: Bogdan Bereza-Jarociński Software Konferencje.				

Program of the Environmental issues: EMAS (Environmental Management Audit Scheme), BAT (Best Available Techniques), BREF (Best available techniques Reference document) training.

Training program: Environmental issues: EMAS (Environmental Management Audit Scheme), BAT (Best Available Techniques), BREF (Best available techniques Reference document)

Duration: 3 days – 26 hours.

Time	τ min.	I Day	II Day	III Day
8.00 ⇓ 10.30	90'		Responsibilities of entrepreneurs in save of the air. Exercise: Check list preparation. Environmental Audits – visit in the company (briefing movie) + discussion	Integration permits – introduction Directive IPPC Law requirements of integration permits.
10.40 ⇓ 12.10	90'		Responsibilities of entrepreneurs in save of the water. Exercise: Check list preparation. Environmental Audits – summary (briefing movie) + discussion	Best Available Technique Best available techniques Reference document.
12.20 ⇓ 13.40	80'	Development of save environment conception Environmental Audits – targets, kinds Environmental Management Systems Standards – ISO 14015	Responsibilities of entrepreneurs in waste industry. Exercise: Check list preparation. Responsibilities of entrepreneurs in save against the noise and prevention breakdowns.	Relation between BAT and environmental management systems.
14.30 ⇓ 15.50	80'	Environmental Audits - Role of director (briefing movie) + discussion Standard ISO 14031, Standard ISO 19011	Regulation EMAS Differences between EMAS and ISO 14001	Sustainable development. (M. Sc. Eng. Dominik Wawrzyniak)
16.00 ⇓ 17.30	90'	Environmental Audits – Preparation to the audit (briefing movie) + discussion Environmental responsibilities of director in Poland.	Requirements EMAS in Poland.	
Lecturer: Robert Pochyluk – eko-net.pl				

V. Profile of Participants

- Representatives of small and medium-sized enterprises from automotive parts manufacturers sub-sector,
- Representatives of different sub-sector of polish economy from small and medium-sized enterprises from other manufacturing sectors could also participate, but as the second priority,
- Others.

VI. List of participants

Det Norske Veritas Poland

Security of IT information according to BS 7799-2:2002. Internal Auditor Training.

DURATION: 26-28 November
DUTY STATION: Warsaw
LECTURER: Marcin Majdecki

	SURNAME NAME	ADRESS
1.	Babuśka Łukasz	WUT, Ul. Plac wojska Polskiego 149/7, 05-075 Warszawa, NIP: 822-195-83-78 tel: (22) 603 959 732 e-mail: lukasz.babuska@wesola.3.pl
2.	Bacciarelli-Hallala Ewa	COMRUN Janusz Hallala ul. Górczewska 122a m. 34 01-460 Warszawa, NIP: 527-141-16-34 tel: (22) 837 53 97 e-mail: ewabacciarelli-hallala@o2.pl
3.	Blim Marek	European Network Security Institute Sp. z o.o. Al. Jana Pawła II 34 00-141 Warszawa NIP: 951-18-25-278 tel: (22) 620 12 00
4.	Byczkowski Maciek	European Network Security Institute Sp. z o.o. Al. Jana Pawła II 34 00-141 Warszawa NIP: 951-18-25-278 tel: (22) 620 12 00 e-mail: Maciej.Byczkowski@ensi.net
5.	Fidecki Jacek	DET NORSKE VERITAS POLAND Sp. z o.o. ul. Skrzetuskiego 16a 02-726 Warszawa tel: (22) 543 97 63
6.	Głowacki Wojciech	SYMAK Centrum Rozwoju Przedsiębiorczości ul. Rgielska 53a 62-100 Wągrowiec NIP: 972-095-17-68 tel: 509 416 031 e-mail: glowackiwoj@poczta.onet.pl
7.	Janiczek Marek	European Network Security Institute Sp. z o.o. Al. Jana Pawła II 34 00-141 Warszawa NIP: 951-18-25-278 tel: (22) 620 12 00

Security of IT information according to BS 7799-2:2002. Internal Auditor Training.

DURATION: 26-28 November
DUTY STATION: Warsaw
LECTURER: Marcin Majdecki

	SURNAME NAME	ADRESS
8.	Karczewska Joanna	ASKA s.c. Pl. Przymierza 4 m 9, 03-944 Warszawa NIP: 113-24-49-571 tel: 501 078 980 e-mail: telmena@poczta.onet.pl
9.	Kobyliński Marcin	DET NORSKE VERITAS POLAND Sp. z o.o. ul. Skrzetuskiego 16a 02-726 Warszawa tel: (22) 543 97 63
10.	Kozłowski Marek	CTPartners S.A. Ul. Robotnicza 3 02-261 Warszawa NIP 113-22-32-104 e-mail: marek.kozlowski@ctpartners.pl; MKozlo03@zi.centertel.pl
11.	Nowakowski Tomasz	Lack of data
12.	Ostaszewski Wiesław	Wiesław Ostaszewski ul. Marymoncka 34 m. 54 01-813 Warszawa NIP: 118-001-87-97 e-mail: Wieslaw_Ostaszewski@nik.gov.pl
13.	Pinkosz Roman	GETIN Bank SA ul. Pszczyńska 10 40-479 Katowice NIP: 634-019-45-90 tel: (32) 200-85-80
14.	Pozniak Jerzy	European Network Security Institute Sp. z o.o. Al. Jana Pawła II 34 00-141 Warszawa NIP: 951-18-25-278 tel: (22) 620 12 00
15.	Slawinski Marek	European Network Security Institute Sp. z o.o. Al. Jana Pawła II 34 00-141 Warszawa NIP: 951-18-25-278 tel: (22) 620 12 00

Security of IT information according to BS 7799-2:2002. Internal Auditor Training.

DURATION: 26-28 November
DUTY STATION: Warsaw
LECTURER: Marcin Majdecki

	SURNAME NAME	ADRESS
16.	Walczak Paweł	ArsFono Ewa Walczak Starej Baśni 10/56 01-853 Warszawa NIP: 118-020-01-64 e-mail: walczak@arsfono.com.pl
17.	Wojakowski Piotr	European Network Security Institute Sp. z o.o. Al. Jana Pawła II 34 00-141 Warszawa NIP: 951-18-25-278 tel: (22) 620 12 00:
18.	Wolak Marcin	European Network Security Institute Sp. z o.o. Al. Jana Pawła II 34 00-141 Warszawa NIP: 951-18-25-278 tel: (22) 620 12 00
19.	Wystub Sylwia	GETIN Bank SA ul. Pszczyńska 10 40-479 Katowice NIP: 634-019-45-90 tel: (32) 200-85-80; 601-910-698 e-mail: S.Wystub@GetinBank.pl

Quality management systems according to ISO 9001:2000. Internal Auditor Training.

DURATION: 3 – 5 December
DUTY STATION: Warsaw

	SURNAME NAME	ADRESS
1.	Babuśka Łukasz	WUT, Ul. Plac wojska Polskiego 149/7, 05-075 Warszawa, NIP: 822-195-83-78 tel: (22) 603 959 732 e-mail: lukasz.babuska@wesola.3.pl
2.	Borzym Andrzej	Biuro Usług Projektowych - Andrzej Borzym ul. Topazowa 3 05-500 Piaseczno NIP: 123-003-12-75 tel: 756 83 01; 602 243 274
3.	Bartkowska Agata	Komenda Powiatowa Policji w Otwocku ul. Pułaskiego 7A 05-400 Otwock tel: (22) 779 40 91
4.	Dziubińska Dorota	Komenda Powiatowa Policji w Otwocku ul. Pułaskiego 7A 05-400 Otwock tel: (22) 779 40 91
5.	Glinaka Wojciech	Komenda Powiatowa Policji w Otwocku ul. Pułaskiego 7A 05-400 Otwock tel: (22) 779 40 91
6.	Walczak Marek	Komenda Powiatowa Policji w Otwocku ul. Pułaskiego 7A 05-400 Otwock tel: (22) 779 40 91
7.	Żebrowski Robert	Komenda Powiatowa Policji w Otwocku ul. Pułaskiego 7A 05-400 Otwock tel: (22) 779 40 91
8.	Kubalski Jan	BusinessPoint S.A. Al. Krakowska 110/114 02-256 Warszawa NIP: 521-26-99-510 tel. (22) 868 57 30
9.	Głowacki Rafał	BusinessPoint S.A. Al. Krakowska 110/114 02-256 Warszawa NIP: 521-26-99-510 tel. (22) 868 57 30

Quality management systems according to ISO 9001:2000. Internal Auditor Training.

DURATION: 3 – 5 December
DUTY STATION: Warsaw

	SURNAME NAME	ADRESS
10.	Gałązka Marta	BusinessPoint S.A. Al. Krakowska 110/114 02-256 Warszawa NIP: 521-26-99-510 tel. (22) 868 57 30 e-mail: marta.galazka@kcp.pl
11.	Henig Paweł	Polska Wytwórnia Papierów Wartościowych ul. Sanguszki 1 00-222 Warszawa NIP: 525-000-10-90 tel: 53 02 227 e-mail: azawislak@pwpw.pl
12.	Gloza Elżbieta	Polska Wytwórnia Papierów Wartościowych ul. Sanguszki 1 00-222 Warszawa NIP: 525-000-10-90 tel: 53 02 227 e-mail: azawislak@pwpw.pl
13.	Sobieszek Rafał	Drukarnia Braci Kamińskich ul. Mickiewicza 5/7 97-500 Radomsko NIP: 772-010-13-71 tel: (44) 683 21 13; 683 20 60
14.	Stępień-Kamieniak Agata	Drukarnia Braci Kamińskich ul. Mickiewicza 5/7 97-500 Radomsko NIP: 772-010-13-71 tel: (44) 683 21 13; 683 20 60

Training on Software quality testing.

DURATION: 18 – 20 February
DUTY STATION: Warsaw
LECTURER: Bogdan Bereza-Jarociński

	SURNAME NAME	ADRESS
1.	Babuśka Łukasz	WUT, Ul. Plac wojska Polskiego 149/7, 05-075 Warszawa, NIP: 822-195-83-78 tel: (22) 603 959 732 e-mail: lukasz.babuska@wesola.3.pl
2.	Dąbrowski Marcin	PIMOT, Warszawa 03-254 Warszawa, ul. Turmoncka 22/602 tel: (22) 604 627 524 e-mail: marcin_dabrowski@wp.pl
3.	Dudek Danuta	Oriflame PP,Warszawa 05-804 Pruszków, Al. Wojska Polskiego 44/33 tel: (22) 501 016 068 e-mail: danusiadudek@wp.pl
4.	Dworczyk Ewa	SAP Projekt, Warszawa 01-554 Warszawa, Al. Wojska Polskiego 50/54 m 57 tel: (22) 608 466 344 e-mail: edworczyk@poczta.onet.pl
5.	Górecka Sylwia	GZF, Polfa, Grodzisk Maz 05-825 Grodzisk Maz, ul. Stolarska 16 tel: (22) 608 613 450 e-mail: sgorecka@grodzisk.rgnet.org
6.	Krzus Sabina	MPWiK, Wrocław 01-018 Warszawa, ul. Wolność 7/12 tel: (22) 507 005 813 e-mail: sabina_a@poczta.onet.pl
7.	Majewski Jan Konrad	ODiSz, Włocławek 87-800 Włocławek, ul. Cegłana 3 tel: (22) 605 055 616 e-mail: odis@bhp24.pl

Training on Software quality testing.

DURATION: 18 – 20 February
DUTY STATION: Warsaw
LECTURER: Bogdan Bereza-Jarociński

	SURNAME NAME	ADRESS
8.	Majewski Sebastian Radosław	ODiSz, Włocławek 87-800 Włocławek, ul. Ceglana 3 tel: (22) 601 140 014 e-mail: bhp24@bhp24.pl
9.	Oleksiak Bogdan	Główny Inspektorat Transportu Drogowego, Warszawa 00-928 Warszawa, ul. Chałubińskiego 4 tel: (22) 691 386 219 e-mail: b.oleksiak@wp.pl
10.	Osińska Anna	SS, Warszawa 03-436 Warszawa, ul. 11-go listopada 28 m.29 tel: (22) 503 672 055 e-mail: osania@poczta.onet.pl
11.	Urbańska Anna	Celon Pharme, Płońsk tel: (22) 604 599 818 e-mail: urbansia@go2.pl
12.	Ptasińska Agata Agnieszka	Megaus, Warszawa tel: (22) 504 064 169 e-mail: agataptasinska@o2.pl
13.	Prządka Paweł	Andra, Warszawa 02-226 Warszawa, ul. Pryzmaty 6/8 tel: (22) 603 660 994 e-mail: pprzadka@wp.pl
14.	Rosłoniec Mirosław	EURICO, Warszawa tel: (22) 600 430 186 e-mail: mirrosloniec@poczta.onet.pl
15.	Sosna Andrzej	PIMOT, Warszawa tel: (22) 692 530 537 e-mail: van_sosen@o2.pl
16.	Świder Wioletta	Flexofol Karczew tel: (22) 508 728 670 e-mail: brutalek1977@wp.pl

Training on Software quality testing.

DURATION: 18 – 20 February
DUTY STATION: Warsaw
LECTURER: Bogdan Bereza-Jarociński

	SURNAME NAME	ADRESS
17.	Trzciński Tomasz	Polmo, Łomianki 05-220 Zielonka, ul. Sowińskiego 16A tel: (22) 509 201 911 e-mail: tomasz.trzcinski@wp.pl
18.	Ziembiński Jerzy Zdzisław	SWJ System, Piaseczno 05-500 Piaseczno, Młynarska 17/18 tel: (22) 601 632 282 e-mail: jziembinski@swj.pl

RWTÜV POLSKA

Training on Environmental issues: EMAS (Environmental Management Audit Scheme), BAT (Best Available Techniques), BREF (Best available techniques Reference document).

DURATION: 4 – 6 March
DUTY STATION: Warsaw
LECTURER: Robert Pochyluk

	SURNAME NAME	ADRESS
1.	Augustyniak Ewa	Bio-Chic, Warszawa 96-500 Sochaczew, ul. Targowa 16/13 tel: 608 654 719 e-mail: ewaaugustyniak@interia.pl
2.	Babuśka Łukasz	WUT, Ul. Plac wojska Polskiego 149/7, 05-075 Warszawa, NIP: 822-195-83-78 tel: (22) 603 959 732 e-mail: lukasz.babuska@wesola.3.pl
3.	Dąbrowski Marcin	PIMOT, Warszawa 03-254 Warszawa, ul. Turmoncka 22/602 tel: (22) 604 627 524 e-mail: marcin_dabrowski@wp.pl
4.	Dudek Danuta	Oriflame PP,Warszawa 05-804 Pruszków, Al. Wojska Polskiego 44/33 tel: (22) 501 016 068 e-mail: danusiadudek@wp.pl
5.	Dworczyk Ewa	SAP Projekt, Warszawa 01-554 Warszawa, Al. Wojska Polskiego 50/54 m 57 tel: (22) 608 466 344 e-mail: edworczyk@poczta.onet.pl
6.	Górecka Sylwia	GZF, Polfa, Grodzisk Maz 05-825 Grodzisk Maz, ul. Stolarska 16 tel: (22) 608 613 450 e-mail: sgorecka@grodzisk.rgnet.org

RWTÜV POLSKA

Training on Environmental issues: EMAS (Environmental Management Audit Scheme), BAT (Best Available Techniques), BREF (Best available techniques Reference document).

DURATION: 4 – 6 March
DUTY STATION: Warsaw
LECTURER: Robert Pochyluk

	IMIĘ NAZWISKO	PODPIS
7.	Krzus Sabina	MPWiK, Wrocław 01-018 Warszawa, ul. Wolność 7/12 tel: (22) 507 005 813 e-mail: sabina_a@poczta.onet.pl
8.	Majewski Jan Konrad	ODiSz, Włocławek 87-800 Włocławek, ul. Ceglana 3 tel: (22) 605 055 616 e-mail: odis@bhp24.pl
9.	Majewski Sebastian Radosław	ODiSz, Włocławek 87-800 Włocławek, ul. Ceglana 3 tel: (22) 601 140 014 e-mail: bhp24@bhp24.pl
10.	Oleksiak Bogdan	Główny Inspektorat Transportu Drogowego, Warszawa 00-928 Warszawa, ul. Chałubińskiego 4 tel: (22) 691 386 219 e-mail: b.oleksiak@wp.pl
11.	Osińska Anna	SS, Warszawa 03-436 Warszawa, ul. 11-go listopada 28 m.29 tel: (22) 503 672 055 e-mail: osania@poczta.onet.pl
12.	Urbańska Anna	Celon Pharme, Płońsk tel: (22) 604 599 818 e-mail: urbansia@go2.pl
13.	Ptasińska Agata Agnieszka	Megaus, Warszawa tel: (22) 504 064 169 e-mail: agataptasinska@o2.pl

RWTÜV POLSKA

Training on Environmental issues: EMAS (Environmental Management Audit Scheme), BAT (Best Available Techniques), BREF (Best available techniques Reference document).

DURATION: 4 – 6 March
DUTY STATION: Warsaw
LECTURER: Robert Pochyluk

14.	Prządka Paweł	Andra, Warszawa 02-226 Warszawa, ul. Pryzmaty 6/8 tel: (22) 603 660 994 e-mail: pprzadka@wp.pl
15.	Rosłoniec Mirosław	EURICO, Warszawa tel: (22) 600 430 186 e-mail: mirrosloniec@poczta.onet.pl
16.	Sosna Andrzej	PIMOT, Warszawa tel: (22) 692 530 537 e-mail: van_sosen@o2.pl
17.	Świder Wioletta	Flexofol Karczew tel: (22) 508 728 670 e-mail: brutalek1977@wp.pl
18.	Trzciński Tomasz	Polmo, Łomianki 05-220 Zielonka, ul. Sowińskiego 16A tel: (22) 509 201 911 e-mail: tomasz.trzcinski@wp.pl
19.	Zabrocki Arkadiusz	Pakfol/Flexofol, Karczew tel: (22) 692 219 281 e-mail: arkadiusz_zabrocki@poczta.onet.pl
20.	Ziembiński Jerzy Zdzisław	SWJ System, Piaseczno 05-500 Piaseczno, Młynarska 17/18 tel: (22) 601 632 282 e-mail: jziembinski@swj.pl

VII. Brief overview of the trainings

1. Security of IT information according to BS 7799-2:2002. Internal Auditor Training has been carried out by Det Norske Veritas Poland.

   - Three days training course (26 H),
   - 19 participants.
   - 26 – 28 November 2004.
   - Lecturer Marcin Majdecki.
   - Duration Warsaw

For this training, the contractor used his own training materials. At the end of course Det Norske Veritas Poland (Scandinavian certification body operating in Poland) gave certificates.

2. Quality management systems according to ISO 9001:2000 - Internal auditors training.

   - Three days training course (26 H),
   - 14 participants.
   - 3 - 5 December 2004.

For this training, the contractor used his own training materials. At the end of course Zetom Katowice (partner of the Transfer Technology Centre of the Warsaw University of Technology) gave certificates.

3. Training on software quality testing.

   - Three days training course (26 H),
   - 18 participants.
   - 18 - 20 February 2005.
   - Lecturer Bogdan Bereza-Jarociński.

- Duration Warsaw.

For this training, the contractor used his own training materials. At the end of course Software Konferencje (the new training organization delivering very innovative training on testing of software quality) gave certificates.

4. Environmental issues: EMAS (Environmental Management Audit Scheme), BAT (Best Available Techniques), BREF (Best available techniques Reference document) training.

- Three days training course (26 H),
- 20 participants.
- 4 - 6 March 2005.
- Lecturer Robert Pochyluk.
- Duration Warsaw.

For this training, the contractor used his own training materials. At the end of course RWTUV (the best certification body in Poland, accreditation concerning persons and, management systems, partner of the Production Engineering Faculty of the Warsaw University of Technology in quality managers trainings since 1997) gave certificates.

VIII. Methodology of the trainings

1. Security of IT information according to BS 7799-2:2002 – Internal auditors trainings. The methodology of the training is based on the methods including: case study, skills training, work in the task group, presentation, interactive lectures and simulation of the real work situation.

   "Information is key to the growth and success of a company. A certified Information Security Management System demonstrates to customers that your information is suitably protected — whether stored on paper, electronically, or in the minds of employees.

   An Information Security Management System will help identify and reduce critical security risks, as it helps you focus your information security efforts and protect your information.

   The ability to discover strengths, weaknesses, and improvement opportunities is crucial to successfully managing security risks. With our Risk Based Certification™ approach, DNV auditors assess how well your Information Security Management System supports the areas of greatest importance to you, in addition to measuring compliance against elected standards.

   Information security is much more than information technology. With an Information Security Management System you can ensure proper handling of your information and prevent leaks.

   With the increase of technical solutions that are tailored to easy and quick sharing of information, leaks are becoming more widespread. The increased migration of workers between competing companies means you risk losing significant knowledge each time someone walks out the door. A systematic approach to information security can help you manage your information flow. Moving away from ad hoc processes gives you an overview that makes your

internal processes easier to **manage, measure**, and **improve**. It is the first step on a journey toward continual business improvement.

Three-dimensional protection of your information

With a management system you can establish, implement, operate, monitor, review, maintain, and improve your information security. You will have a tool to identify your critical assets and then protect them. While providing confidence for employees, customers, owners, and the society in general, it will also strengthen your organisation's ability to meet strategic objectives.

You will be able to protect your information with regard to three dimensions:

- **Confidentiality** ensures that information is accessible only to those authorised to have access.

- **Integrity** safeguards the accuracy and completeness of information and processing methods.

- **Availability** ensures that authorised users have access to information and associated assets when required.

Putting your security issues first

The purpose of information security management is to ensure business continuity and reduce business damage by preventing and minimising the impact of security incidents. The Audit Commission Update report (1998) shows that fraud or cases of IT abuse often occur due to absence of basic control, with one-half of all detected frauds found by accident. Ensuring the storage of your knowledge capital, and protecting it through a management system, will strengthen the competitive edge of your company"[www.dnv.com].

2. Quality management systems according to ISO 9001:2000 - Internal auditors training. The methodology of the training such as in the case of BS 7799:2002 – Internal auditor training is based on the methods including: case study, skills training, work in the task group, presentation, interactive lectures and simulation of the real work situation.

3. Training on software quality testing. The methodology is based on the following methods:

- case study,
- skills training,
- work in the task group,
- presentation,
- interactive lectures,
- simulation of the real work situation.

The training was composed of the following parts:

- **Introduction,**
- **Principles of testing,**

  Terminology; why testing is necessary; fundamental test process; psychology of testing; re-testing and regression testing; expected results and prioritisation.
- ***Testing throughout the lifecycle,***

  Models for testing; economics of testing; high level test planning; acceptance testing; integration testing in the large function and non-functional system; integration testing in the small; component testing and maintenance testing.
- **Dynamic testing techniques,**

  Black and white box testing; black and white box techniques; and error guessing.
- **Static testing,**

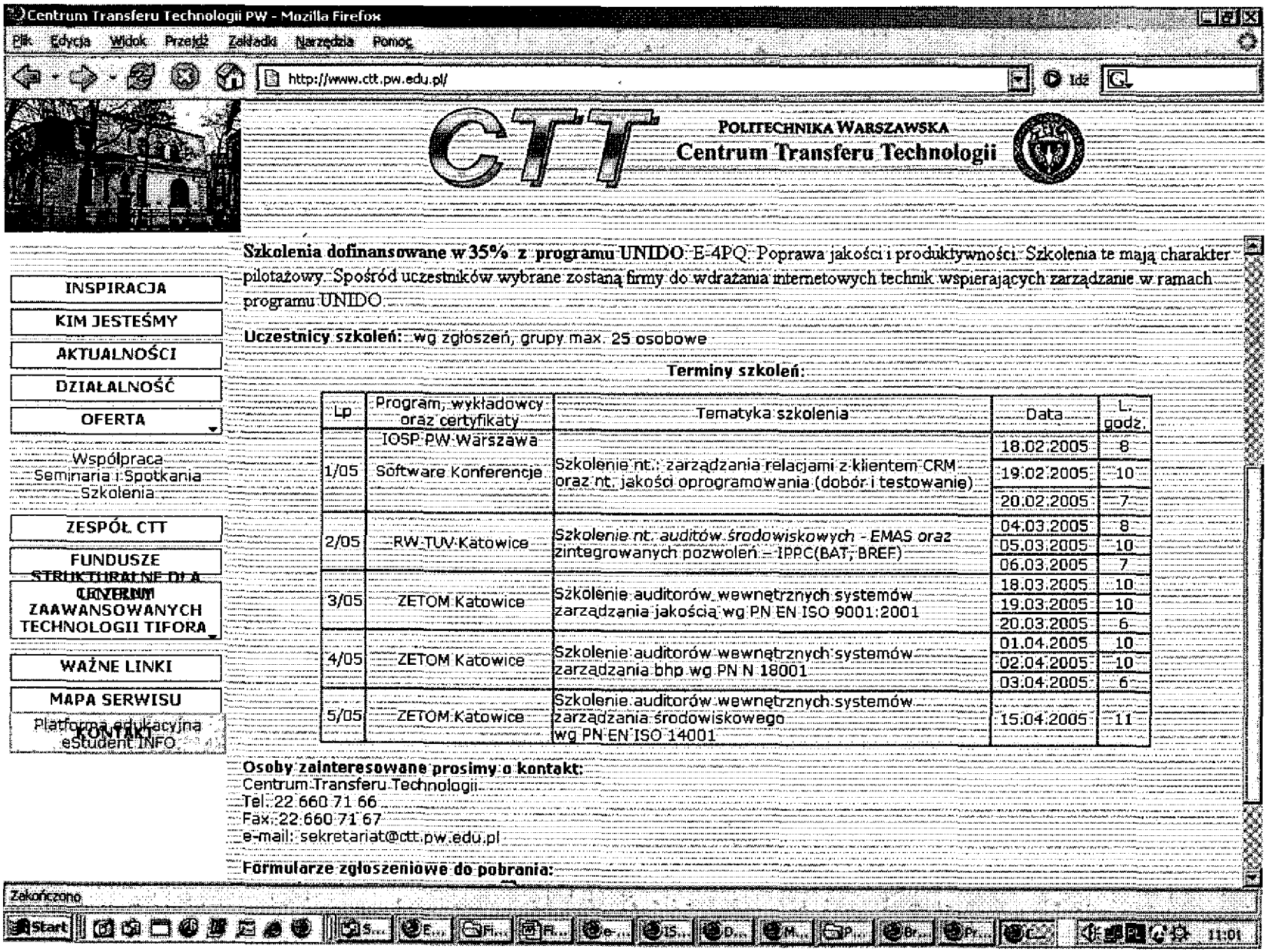
  Reviews and the test process; types of review; and static analysis.
- **Test Management,**

  Organisation and configuration management; test estimation; monitoring and control; incident management; and standards for testing.
- **Tool Support for Testing,**

  Types of CAST tool (Computer-Aided Software Testing); tool selection and implementation.

4. Environmental issues: EMAS (Environmental Management Audit Scheme), BAT (Best Available Techniques), BREF (Best available techniques Reference document) training methodology. **EMAS**, European Union Eco-Management

and Audit Scheme, is an instrument which all kinds of organizations can fix and improve their internal and external environmental. Environmental is key in activity of the company. Organisation has to aim to minimize environmental effects. The methodology of the EMAS training is based on the activity methods such as: case study, skills training, work in the task group, presentation, interactive lectures and simulation of the real work situation.


Centrum Transferu Technologii PW - Mozilla Firefox
Plik Edycja Widok Przejdź Zakładki Narzędzia Pomoc
http://www.ctt.pw.edu.pl/
Idź
CTT
POLITECHNIKA WARSZAWSKA
Centrum Transferu Technologii
INSPIRACJA
KIM JESTEŚMY
AKTUALNOŚCI
DZIAŁALNOŚĆ
OFERTA
Współpraca
Seminaria i Spotkania
Szkolenia
ZESPÓŁ CTT
FUNDUSZE STRUKTURALNE DLA
CENTRUM ZAAWANSOWANYCH TECHNOLOGII TIFORA
WAŻNE LINKI
MAPA SERWISU
Platforma edukacyjna eStudent INFO
KONTAKT
Szkolenia dofinansowane w 35% z programu UNIDO E-4PQ: Poprawa jakości i produktywności. Szkolenia te mają charakter pilotażowy. Spośród uczestników wybrane zostaną firmy do wdrażania internetowych technik wspierających zarządzanie w ramach programu UNIDO.
Uczestnicy szkoleń: wg zgłoszeń, grupy max. 25 osobowe
Terminy szkoleń:
Lp
Program, wykładowcy oraz certyfikaty
Tematyka szkolenia
Data
L. godz.
IOSP PW Warszawa
1/05
Software Konferencje
Szkolenie nt.: zarządzania relacjami z klientem CRM oraz nt. jakości oprogramowania (dobór i testowanie)
18.02.2005
19.02.2005
20.02.2005
8
10
7
2/05
RW TUV Katowice
Szkolenie nt. auditów środowiskowych - EMAS oraz zintegrowanych pozwoleń - IPPC(BAT, BREF)
04.03.2005
05.03.2005
06.03.2005
8
10
7
3/05
ZETOM Katowice
Szkolenie auditorów wewnętrznych systemów zarządzania jakością wg PN EN ISO 9001:2001
18.03.2005
19.03.2005
20.03.2005
10
10
6
4/05
ZETOM Katowice
Szkolenie auditorów wewnętrznych systemów zarządzania bhp wg PN N 18001
01.04.2005
02.04.2005
03.04.2005
10
10
6
5/05
ZETOM Katowice
Szkolenie auditorów wewnętrznych systemów zarządzania środowiskowego wg PN EN ISO 14001
15.04.2005
11
Osoby zainteresowane prosimy o kontakt:
Centrum Transferu Technologii
Tel: 22 660 71 66
Fax: 22 660 71 67
e-mail: sekretariat@ctt.pw.edu.pl
Formularze zgłoszeniowe do pobrania:
Zakończono
Start
11:01

Brief information has been sent to the companies presented below.

Company	Street	Zip-cod	Town	e - mail	tel.
1. **APE Auto Power Electronic**	Zbożowa 12	45-837	Opole	ape@ape.com.pl	(077) 474-56-74
2. **AutoLinka, Henryk Frydziński**	Janki, al. Krakowska 26	05-090	Raszyn	office@autolinka.com.pl	(022) 720 05 62
3. **Hak-Hol**	Brzegowa 90	58-200	Dzierżoniów	biuro@hakhol.com.pl	(074) 831 28 51
4. **Iławskie Zakłady Naprawy Samochodów S.A.**	Grunwadzka 13	14-200	Iława	izns@izns.com.pl	(0 89) 648 21 31
5. **P.P.H. Polauto, Jan Freitag**	Hawelańska 7	61-625	Poznań	polauto@polbox.com	(0 61) 823 88 61
6. **JANMOR**	Polna 12	95-200	Pabianice	biuro@janmor.pl	(0 42) 213 12 52
7. **KAMPOL s. j. Adam i Mieczysław Kopczyńscy**	pl. Sportowy 10	07-220	Kamieńczyk	kampolsc@poczta.onet.pl	(0 22) 781 36 34
8. **P.P.U.H. KAROS**	Wiosenna 57	05-092	Łomianki	karos@karoslomianki.com.pl	(0 22) 751 11 96
9. **MARETA s.c.**	Longinusa 2	05-230	Kobyłka	kontakt@maretabrakes.pl	(0 22) 786 33 34
10. **MOTO-SZLIF, Urbanek & Leszczyński**	11-go Listopada 3	91-370	Łódź	moto-szlif@mojagielda.pl	(0 42) 659 21 28
11. **MOTGUM**	Sikorskiego 137	05-420	Józefów	motgum@motgum.com	(0 22) 789 47 58
12. **P.P.W. "NABOR"**	Fabryczna 8	23-210	Kraśnik	nabor@nabor.pl	(0 81) 825 77 44
13. **PARADOWSCY AMP s.j.**	K. Jagiellończyka 1	02-496	Warszawa	marketing@paradowscy.pl	(0 22) 662 48 00
14. **PROKOM Sp.z.o.o.**	Mieszka I nr 21	71-007	Szczecin	prokom@inet.com.pl	(0 91) 482 03 41
15. **POZGUM s.j. H.P.D. Paproccy**	Nad Wierzbakiem 1	60-604	Poznań	info@pozgum.pl	(0 61) 851 99 96
16. **SENTECH**	Spacerowa 6/8	95-200	Pabianice	sentech@sentech.pl	(0 42) 227 56 50
17. **Spółdzielnia Inwalidów "ODRODZENIE"**	A. Struga 2/6	80-116	Gdańsk	odrodzenie@odrodzenie.pl	(0 58) 302 30 71
18. **SPINKO Sp. Z o.o.**	Okrężna 20	64-100	Leszno	jakosc@spinko.com.pl	(0 65) 525 88 00
19. **Przedsiębiorstwo Prywatne TOLIN**	Łęg Witoszyn	87-811	Fabianki	tolin@tolin.com.pl	(0 54) 237 11 16
20. **TORSTAR**	3 Maja 48	05-230	Kobyłka	biuro@torstar.com.pl	(0 22) 786 33 23
21. **Stowarzyszenie Producentów Części Motoryzacyjnych**	Jagiellońska 55	03-301	Warszawa	spcm@spcm.org.pl	(0 22) 814 62 49
22. **BIAZET EI Sp. Zo.o.**	Gen. Andersa 38	15-113	Białystok	sm@biazetei.pl	(0 85) 664 40 06
23. **CENTRA**	Gdyńska 31/33	61-016	Poznań	TomkowiakK@exide.pl	(0 61) 878 61 00
24. **Dunaj Stanisław, Zakład Pracy Chronionej**	Armii Ludowej 26a	57-120	Wiązów	biuro@dunaj.com.pl	(0 71) 393 11 40
25. **HSW - Zakład Zepołów Napędowych Sp. z o.o.**	Kwiatkowskiego 1	37-450	Stalowa Wola	zzn@hsw-zzn.com.pl	(0 15) 843 54 13
26. **HYDROTOR SA Przedsiębiorstwo Hydrauliki Siłowej**	Chojnicka 72	89-500	Tuchola	hydrotor@hydrotor.com.pl	(0 52) 336 36 00

27. **"Inprodus" Spółdzielnia Inwalidów ZPCh**	Piastowska 3	59-400	Jawor	marketing@inprodus.com.pl	(0 76) 729 46 81
28. **ISKRA Zakłady Precyzyjne Sp. Z o.o.**	Mielczarskiego 47	25-709	Kielce	info@iskra-kielce.pl	(0 41) 345 74 10
29. **Kirchhoff Polska Sp. z o.o.**	Wojska Polskiego 3	39-300	Mielec	r.czahor@kirchhoff.pl	(0 17) 788 56 40
30. **KOMETAL Wytwórnia Części Samochodowych Sp. z o.o.**	Bohaterów Warszawy 24/28	75-211	Koszalin	info@kometal.pl	(0 94) 342 48 58
31. **LINEX P.P.H.**	Rejtana 15	42-200	Częstochowa	linex@linex.com.pl	(0 34) 363 25 64
32. **MAGNET - ELEKTROMET Spółdzielnia Pracy**	Promenada 1/3	00-778	Warszawa	zarzad@magnet.pl	(0 22) 841 00 91
33. **Omag Sp. z o.o.**	Górnicza 8	32-610	Oświęcim	omag@omag.pl	(0 33) 843 00 81
34. **PLANDEX**	Kwiatowa 12	62-060	Stęszew	plandex@plandex.pl	(0 61) 813 54 94
35. **POLMO Kalisz, Zakład Sprzętu Motoryzacyjnego Sp. z o.o.**	Złota 20a	62-800	Kalisz	polmoinf@polmo.com.pl	(0 62) 75 70 600
36. **POLMO Łomianki S.A.**	Warszawska 31	05-092	Łomianki	sekretariat@polmosa.com.pl	(0 22) 751 30 31
37. **POLMO S.A. Zakłady Sprzętu Motoryzacyjnego**	Lidzbarska 15	87-300	Brodnica	zsm@polmo.pl	(0 56) 491 22 84
38. **PRIMA S.A. Fabryka Pierścieni Tłokowych**	Liściasta 17	91-357	Łódź	info@fpt-prima.com.pl	(0 42) 617 41 23
39. **PZL Sędziszów Wytwornia Filtrów**	Fabryczna 4	39-120	Sędziszów Młp.	wf@wf-sedziszow.com.pl	(0 17) 221 65 02
40. **Spółdzielnia Inwalidów "OGNIWO" ZPCh**	Cisowa 11	20-703	Lublin	info@ogniwo.com.pl	(0 81) 533 32 51
41. **STEINHOF Zakład Mechaniczny**	Przemysłowa 27a	33-100	Tarnów	firma@steinhof.pl	(0 14) 627 32 05
42. **WSK Gorzyce S.A.**	Odlewników 52	39-432	Gorzyce	alicja_piechnik@eu.fmo.com	(0 15) 836 01 01
43. **Wytwórnia Wkładów Filtracyjnych s.c.**	Złocha 10	63-507	Kobyla Góra	info@wwf.com.pl	(0 62) 731 63 66
44. **YAZDA - Producent Tarcz Sprzęgła**	Piwonii 8	43-300	Bielsko-Biała	yazda@yazda.pl	(0 33) 822 83 92
45. **Zakład Mechaniczny Grodzisk Maz.**	Żydowska 2A	05-825	Grodzisk Mazowiecki	jaro@zlom-jaro.pl	(0 22) 755 53 56
46. **Zakład Mechaniczny Suchy Las**	Graniczna 27	62-002	Suchy Las	biuro@szczublewski.poznan.pl	(0 61) 812 55 19
47. **"ZJEDNOCZENIE" Spółdzielnia Inwalidów**	Słowackiego 1a	39-460	Nowa Dęba	siz@pro.onet.pl	(0 15) 846 26 31

X. Finance

Generally payments from participants and contract price (10,175 Euro which is a 35 % all costs of project) allowed us for conducting of training on quality improvement. The sum of project allowed particularly for pay: accommodation, food, conducting of courses by certifications bodies:

- Det Norske Veritas,
- ZETOM Katowice,
- Software Konferencje,
- RWTUV.

XI. Feedback from participants

At the end of trainings everybody was questioned but some of the participants did not feedback a questionnaire (See Annex C). Example of the questionnaire is hereunder.

UNITED NATIONS INDUSTRIAL DEVELOPMENT ORGANIZATION
ORGANIZACJA NARODÓW ZJEDNOCZONYCH DS. ROZWOJU PRZEMYSŁOWEGO
E4PQ. Regionalny program wysokiej technologii zwiększania przemysłowej e-produktywności i jakości w krajach Europy Środkowowschodniej/Wspólnoty Niepodległych Państw

KWESTIONARIUSZ OCENY SZKOLENIA PRZEZ UCZESTNIKÓW

Nazwa szkolenia.....

Miejsce i data.....

1. Informacje otrzymane przed rozpoczęciem kursu

1.a Jak ocenia Pan/Pani wstępne informacje o programie kursu otrzymane przed jego rozpoczęciem ? *(proszę wpisać ocenę w odpowiedniej rubryce)*

	doskonałe		dobre			wystarczające			złe	
	10	9	8	7	6	5	4	3	2	1
- Cel szkolenia										
- Poziom programu										
- Treść programu										

Czy powinny być dostarczone bardziej szczegółowe informacje? Jeśli tak, proszę wymienić, jakich informacji brakowało:

1.b Na ile tygodni przed rozpoczęciem kursu szkoleniowego były dostarczone poniższe informacje?

	Ponad 4 tygodnie	*2 do 4 tygodni*	*Mniej niż 2 tygodnie*
Informacje na temat programu	[ ]	[ ]	[ ]
Potwierdzenie przyjęcia na kurs	[ ]	[ ]	[ ]

Uwagi:

2. Jakość i przydatność treści programu szkoleniowego

	doskonałe 10	9	dobre 8	7	6	wystarczające 5	4	3	słabe 2	1
2.a Program odpowiadał warunkom Państwa firmy/ instytutu										
2.b Jakość materiałów szkoleniowych										

2.c Jakie tematy programu były najwartościowsze?

2.d Jakie tematy programu były najmniej wartościowe?

2.e Jakiemu tematowi (–om) poświęcono zbyt mało uwagi?

2.f Jaki był ogólny poziom szkolenia?

[ ] za wysoki [ ] odpowiedni [ ] za niski

Uwagi:

3. *Organizacja szkolenia*

3.a Długość kursu:
[ ] za długi [ ] odpowiednio długi [ ] za krótki

Uwagi:

3.b Dzienny plan zajęć:
[ ] zbyt przeładowany [ ] odpowiedni [ ] za mało intensywny

Uwagi:

3.c Wielkość grupy uczestników:

[ ] za duża [ ] odpowiednia [ ] za mała

3.d Skład grupy był:
[ ] jednorodny (pod względem zawodu, wieku, etc.) w pozytywnym sensie
[ ] zbyt jednorodny
[ ] zbyt zróżnicowany (pod względem kwalifikacji, wieku, doświadczenia zawodowego, poziomu , itp.)
[ ] zróżnicowany, ale oceniam to pozytywnie

3.e Czy Pan/Pani czuł(-a) się zintegrowany(-a) z grupą? [ ] Tak [ ] Nie
Jeśli nie, dlaczego?

3.f Sugestie co do wprowadzenia zmian w programie:

4. Jakość szkolenia

4.a Stosowane metody szkolenia:

	doskonałe		dobre			wystarczające			złe	
	10	9	8	7	6	5	4	3	2	1
- Teoria										
- Praktyka (np. studia przypadków, ćwiczenia, itp.)										
- Dyskusje, prezentacje wygłaszane przez uczestników, itp.										

Uwagi:

4.b Sugerowane zmiany w metodach szkolenia:

	pozostawić bez zmian	zwiększyć	zmniejszyć
Wykłady	[ ]	[ ]	[ ]
Prace w grupach	[ ]	[ ]	[ ]
Prezentacje	[ ]	[ ]	[ ]
Studia przypadków	[ ]	[ ]	[ ]

Uwagi:

4.c Poziom prezentowany przez wykładowców i prezenterów studiów przypadków

Prowadzący..
....

	doskonały		dobry			wystarczający			słaby	
	10	9	8	7	6	5	4	3	2	1
- Przygotowanie merytoryczne										
- Sposób prowadzenia zajęć										
- Umiejętność odwoływania się do praktyki										

Prowadzący..
....

	doskonały		dobry			wystarczający			słaby	
	10	9	8	7	6	5	4	3	2	1
- Przygotowanie merytoryczne										
- Sposób prowadzenia prezentacji										
- Ogólna ocena samej prezentacji										

Prowadzący..
....

	doskonały		dobry			wystarczający			słaby	
	10	9	8	7	6	5	4	3	2	1
- Przygotowanie merytoryczne										
- Sposób prowadzenia prezentacji										
- Ogólna ocena samej prezentacji										

Prowadzący..
....

	doskonały		dobry			wystarczający			słaby	
	10	9	8	7	6	5	4	3	2	1
- Przygotowanie merytoryczne										
- Sposób prowadzenia prezentacji										
- Ogólna ocena samej prezentacji										

Uwagi:

4.d Czy było dość czasu na wymianę poglądów na tematy zawodowe?

	Tak	Nie
Z wykładowcami	[ ]	[ ]
Z uczestnikami	[ ]	[ ]

4.e Korzyści płynące z wymiany poglądów z:

	wykładowcami	**uczestnikami szkolenia**
Bardzo duże	[ ]	[ ]
Duże	[ ]	[ ]
Średnie	[ ]	[ ]
Niewielkie	[ ]	[ ]
Żadne	[ ]	[ ]

Uwagi:

	doskonałe 10 9	dobre 8 7 6	wystarczające 5 4 3	słabe 2 1
4.f Dostępność i jakość materiałów szkoleniowych				
4.g Zastosowanie tradycyjnych pomocy szkoleniowych				
4.h Zastosowanie technik audio-wizualnych				
4.i Zgodność przebiegu kursu z programem				

5. *Osiągnięte rezultaty*

	bardzo wysokie 10 9	wysokie 8 7 6	niskie 5 4 3	nieznaczne 2 1
5.a Korzyści zawodowe zdobyte w trakcie szkolenia				

Uwagi:

	bardzo wysoka 10 9	wysoka 8 7 6	niska 5 4 3	niewielka 2 1
5.b Możliwość zastosowania nowo zdobytej wiedzy w obecnej praktyce zawodowej				

Jakie trudności mogą być napotkane?

5.c Możliwość przekazania zdobytej wiedzy i umiejętności innym

bardzo wysoka		wysoka			średnia			niska	
10	9	8	7	6	5	4	3	2	1

5.d Jak to przekazanie się odbędzie?

[ ] w codziennej pracy - kolegom i podwładnym
[ ] w ramach usług doradczych świadczonych na rzecz MŚP
[ ] na specjalnie zorganizowanych szkoleniach

Jakich trudności można się spodziewać?

5.e Czy Państwa zdaniem istnieje potrzeba zorganizowania podobnych kursów w przyszłości, np. w innych regionach Polski?

6. *Administracja i logistyka*

6.a Czy sala wykładowa i pomoce naukowe były zadowalające?

[ ] Tak [ ] Nie

Uwagi:

7. Ogólna ocena kursu szkoleniowego

Wysoce zadowalająca		Zadowalająca, zgodnie z oczekiwaniami, dobra			Zadowalająca, chociaż poniżej oczekiwań			Niezadowalająca	
10	9	8	7	6	5	4	3	2	1

Uwagi:

8.a Proszę podać, jakie nowe umiejętności Państwo zdobyli na tym kursie?

8.b Dodatkowe uwagi odnośnie do spraw/problemów pominiętych w tym kwestionariuszu lub propozycje do realizacji:

***Imię, nazwisko, stanowisko**

* . Jeśli chcą Państwo zachować anonimowość, podawanie nazwiska nie jest konieczne

XII. Evaluation of the questionnaires

On the based of questionnaires from participants we can to conclude:

- Trainings lecturers have been evaluated very good (minimum 5 and maximum 10),
- Quality of the trainings have been evaluated very good (from 5 to 10),
- General valuation of the trainings to range from 5 to 10.

At the same time we can say that participants would like much more exercises, simulation of the real work situation, case studies and work in the task group.

The conclusion is that trainings have fulfilled expectations.

More detailed view at the trainings is:

- **Security of IT information according to BS 7799-2:2002 – Internal Auditor Training**

From among 19 participants we got 11 questionnaires back. On the based of questionnaires we can say that training has fulfilled expectations. Marcin Majdecki received very high range (largely 10). He has very good competence to provide this kind of the training. He is worker one of the best certification body in Poland. Materials were very good quality. Objectives of the trainings were achievement.

- **Quality management systems according to ISO 9001:2000 – Internal Auditor Training**

From among 14 participants we got 10 questionnaires back. On the based of questionnaires we can say that training has fulfilled expectations. ZETOM Katowice as a partner of Warsaw University of Technology received high note (largely 8 and 9). ZETOM Katowice has a large experience in auditing of the quality management systems (from 1899). Thankfully competences and experience training was very interesting.

- **Software quality testing**

From among 18 participants we got 11 questionnaires back. Bogdan Bereza-Jarociński as a lecturer provided very high level of the training. He has very good competences and experience to provide this kind of the training. On the based of questionnaires we can say that training has fulfilled expectations.

- **Environmental issues: EMAS (Environmental Management Audit Scheme), BAT (Best Available Techniques), BREF (Best available techniques Reference document)**

From among 20 participants we got 16 questionnaires back. On the based of questionnaires we can say that training has fulfilled expectations. EMAS in Poland is very new term and it was observable during the training. Robert Pochyluk deals the topic of Environmental Management and Audit Scheme already several years but for participants it was something new. After training all of the participants know how prepare documentations for EMAS and what is EMAS.

XIII. Case studies

Dabrowski Marcin – case study

I am a worker of the certification department in Automotive Industry Institute (PIMOT).

The Automotive Industry Institute (PIMOT) was founded by virtue of the Resolution No. 218 of the Council of Ministers dated August 11, 1972, as the central unit in the system of Polish automotive industry research and development facilities.

PIMOT was set up by transformation of:

- POLMO Automotive Industry Head Research and Development Centre and
- POLMO Automotive Industry Research and Development Centre.

The Institute continues long traditions, dated back to the period between the two World Wars, of the former automotive industry research and development units in Poland and employs highly qualified and experienced personnel.

The founding organ of the Institute is the Ministry of Economy, Labour, and Social Policy.

In general, Institute's lines of operation cover

- Scientific, research, and development work in the field of automotive industry problems.

PIMOT is a technical unit authorized by:

- Ministry of Infrastructure to carry out type-approval tests for conformity with selected UN-ECE Regulations;
- Polish Accreditation Centre to issue certificates of the right to label automotive products with the 'B' safety mark and certificates for special vehicles (armoured bank vehicles and cash carrying vehicles) – Accreditation Certificate of a Product Certifying Unit No. AC 001 (to Polish National Standard No. PN-EN 45011:2000);
- Polish Committee for Standardization (PKN – Polski Komitet Normalizacyjny) to grant manufacturers product conformity certificates that would entitle manufacturers to provide their products with a mark of conformity with Polish Standards – License No. PN-013;

- Polish Accreditation Centre to validate automotive exhaust-gas analysers – Accreditation Certificate No. AP 025 (to Polish National Standard No. PN-EN ISO/IEC 17025:2001);
- Central Measure Bureau to revalidate automotive exhaust-gas analysers – Authorization Certificate No. L 22/2003.

PIMOT also issues certificates for automotive vehicle repair and maintenance services.

The scope of Institute's activities includes:

- Tests and inspections carried out for the purposes of type-approval and certification of vehicles and vehicle component parts;
- Product development and modernization work;
- Engineering design and making of vehicle prototypes, component parts, and accessories as well as test apparatus and test stands;
- Automotive product standardization activities;
- Organization of scientific conferences and training courses.

The above activities are conducted at numerous Institute's laboratories as well as research and development departments and centres.

The following PIMOT units have been granted Accreditation Certificate No. AB 082 (PN-EN ISO/IEC 17025:2001) issued by the Polish Accreditation Centre:

- Vehicle Acoustics Laboratory,
- Vehicle Safety Laboratory,
- Research Equipment, Electrotechnics and Electronics Laboratory,
- Braking Systems Laboratory,
- Metallic Materials Laboratory,
- Non-Metallic Materials Laboratory,
- Engine Testing Laboratory,
- Field Tests Laboratory,
- Vehicle Components Testing Laboratory,
- Simulation Tests Laboratory,
- Measuring and Research Equipment Management Department.

Accreditation Certificate No. AP 025 (PN-EN ISO/IEC 17025:2001) issued by the Polish Accreditation Centre has been granted to:

- Automotive Exhaust-Gas Analyser Measuring Section at the Engine Testing Laboratory.

The Institute also undertakes the following tasks within its range of activities:

- Prepares analyses, expert's opinions, forecasts, and reviews concerning the automotive industry;
- Takes part in the development of regulations and procedures related to the assessment of products and operation of business units;
- Takes part in international cooperation in the field of type approval and standardization;
- Provides information and educational services for the manufacturers of vehicles and automotive products (in such fields as invention, patent protection, European systems of testing, certification of products and services, or Polish and foreign normative acts).

EMAS (Eco Management and Audit Scheme) training gave me a wide view about environmental management systems. I hope that during my work I will use a knowledge from training.

Trzcinski Tomasz – case study

I am a Quality Manager in POLMO ŁOMIANKI S.A.

POLMO ŁOMIANKI S.A. company's registered office is based outskirts of Warsaw at Łomianki, by Gdańsk route – the main communication way connecting South with North of Poland.

The Company's substructures consist of two other companies ltd., joined at 1949. Since 1965 the Company is known as powder metal components manufacturer, named Fabryka Wyrobów z Proszków Spiekanych. At the 60's two production departments present manufacturing profiles as follows:

- Powder metallurgy,
- Automotive electrotechnics.

Within second half of the 70's a modernization of the factory took place. Two new production buildings, sewage-treatment plant, water-treatment station, and access roads were constructed. The 90's cover intensified modernization and overhauls, processing modifications, new products launching, and work conditions improvement. In January 1995, new Company arose on base of the state enterprise, that is to say, staff company named Fabryka Wyrobów z Proszków Spiekanych POLMO S.A. The employee share ownership consisted of 402 persons. In July 1996, the firm assumed its name of POLMO ŁOMIANKI S.A.

Since very beginning of its activity the Company developed and modernized production of plastic components as a distinguishable organizational structure. The development of engineering and processing for plastic and powder metal components becomes general direction in the Company's development.
According to state of 31 Dec. 2001, shareholders equity belongs to 204 shareholders, with an employment for 297 persons.
EMAS (Eco Management and Audit Scheme) training allowed me for better understanding differences between 14001 and EMAS. In the future I will try to use captured knowledge for preparing a documentation of environmental management.

Sosna Andrzej – case study

I am a worker of the type approval department in Automotive Industry Institute (PIMOT).
The Automotive Industry Institute (PIMOT) was founded by virtue of the Resolution No. 218 of the Council of Ministers dated August 11, 1972, as the central unit in the system of Polish automotive industry research and development facilities.
PIMOT was set up by transformation of:

- POLMO Automotive Industry Head Research and Development Centre and
- POLMO Automotive Industry Research and Development Centre.

The Institute continues long traditions, dated back to the period between the two World Wars, of the former automotive industry research and development units in Poland and employs highly qualified and experienced personnel.
The founding organ of the Institute is the Ministry of Economy, Labour, and Social Policy.
In general, Institute's lines of operation cover

- Scientific, research, and development work in the field of automotive industry problems.

PIMOT is a technical unit authorized by:

- Ministry of Infrastructure to carry out type-approval tests for conformity with selected UN-ECE Regulations;
- Polish Accreditation Centre to issue certificates of the right to label automotive products with the 'B' safety mark and certificates for special vehicles (armoured bank vehicles and cash carrying vehicles) – Accreditation

Certificate of a Product Certifying Unit No. AC 001 (to Polish National Standard No. PN-EN 45011:2000);

- Polish Committee for Standardization (PKN – Polski Komitet Normalizacyjny) to grant manufacturers product conformity certificates that would entitle manufacturers to provide their products with a mark of conformity with Polish Standards – License No. PN-013;
- Polish Accreditation Centre to validate automotive exhaust-gas analysers – Accreditation Certificate No. AP 025 (to Polish National Standard No. PN-EN ISO/IEC 17025:2001);
- Central Measure Bureau to revalidate automotive exhaust-gas analysers – Authorization Certificate No. L 22/2003.

PIMOT also issues certificates for automotive vehicle repair and maintenance services.

The scope of Institute's activities includes:

- Tests and inspections carried out for the purposes of type-approval and certification of vehicles and vehicle component parts;
- Product development and modernization work;
- Engineering design and making of vehicle prototypes, component parts, and accessories as well as test apparatus and test stands;
- Automotive product standardization activities;
- Organization of scientific conferences and training courses.

The above activities are conducted at numerous Institute's laboratories as well as research and development departments and centres.

The following PIMOT units have been granted Accreditation Certificate No. AB 082 (PN-EN ISO/IEC 17025:2001) issued by the Polish Accreditation Centre:

- Vehicle Acoustics Laboratory,
- Vehicle Safety Laboratory,
- Research Equipment, Electrotechnics and Electronics Laboratory,
- Braking Systems Laboratory,
- Metallic Materials Laboratory,
- Non-Metallic Materials Laboratory,
- Engine Testing Laboratory,
- Field Tests Laboratory,
- Vehicle Components Testing Laboratory,

- Simulation Tests Laboratory,
- Measuring and Research Equipment Management Department.

Accreditation Certificate No. AP 025 (PN-EN ISO/IEC 17025:2001) issued by the *Polish Accreditation Centre has been granted to:*

- Automotive Exhaust-Gas Analyser Measuring Section at the Engine Testing Laboratory.

The Institute also undertakes the following tasks within its range of activities:

- Prepares analyses, expert's opinions, forecasts, and reviews concerning the automotive industry;
- Takes part in the development of regulations and procedures related to the assessment of products and operation of business units;
- Takes part in international cooperation in the field of type approval and standardization;
- *Provides information and educational services for the manufacturers of* vehicles and automotive products (in such fields as invention, patent protection, European systems of testing, certification of products and services, or Polish and foreign normative acts).

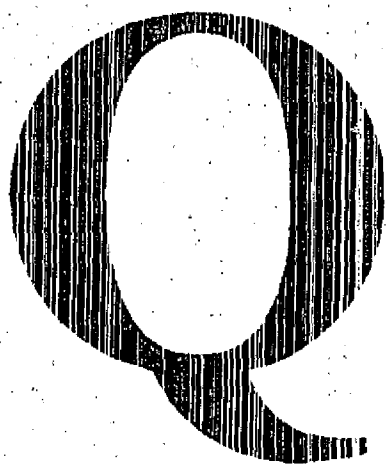
EMAS (Eco Mangement and Audit Scheme) informed me how major is proper environmental management in companies. It is foundation take caring about our common environmental. Training allowed me for better understanding clients of our firm.

ZETOM® Katowice od 1899 r.

Zakłady Badań i Atestacji „ZETOM"
im. Profesora Fryderyka Stauba w Katowicach
Institutions for Research and Certification **"ZETOM"**

„AUDITOR WEWNĘTRZNY SYSTEMU JAKOŚCI"

ISO 9001:2000

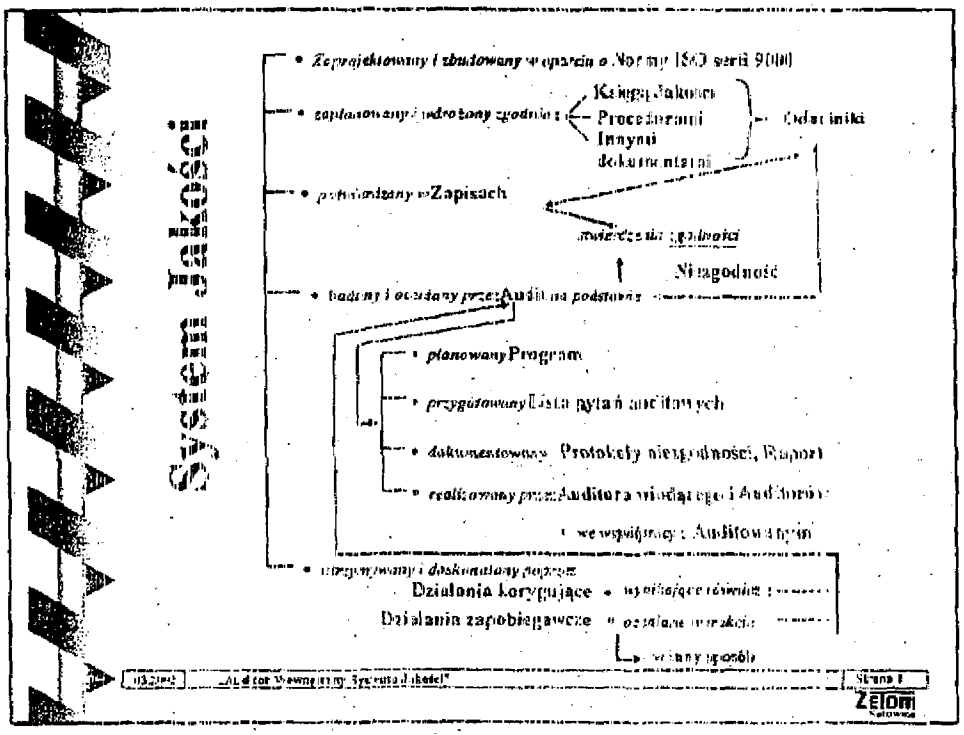


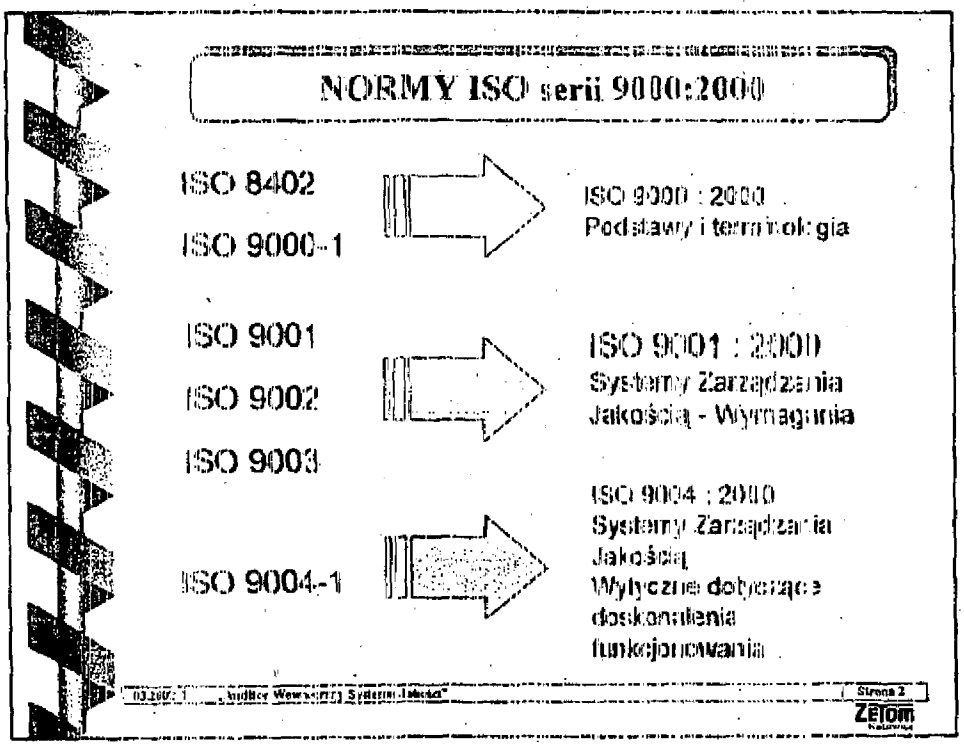
Materiały szkoleniowe

KATOWICE 2004 r.

SPIS TREŚCI

CZĘŚĆ I
SYSTEM JAKOŚCI

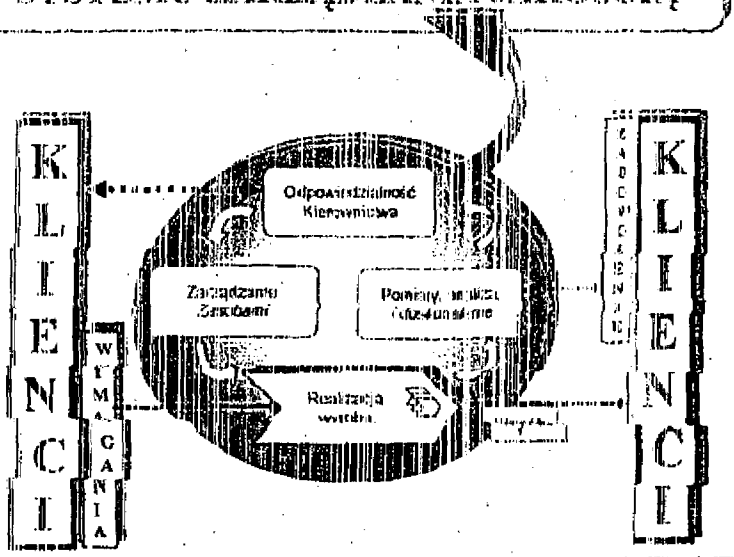

Zaprojektowany i zbudowany w oparciu o Normy ISO serii 9000
Księga Jakości
Procedurami
Innymi dokumentami
Odwołuje się do
Zapisach
Niezgodność
Planowany Program
Przygotowany Lista pytań auditowych
Dokumentowany Protokoły niezgodności, Raport
Auditora
Auditowanym
Działania korygujące
Działania zapobiegawcze
Strona 1
ZETOM

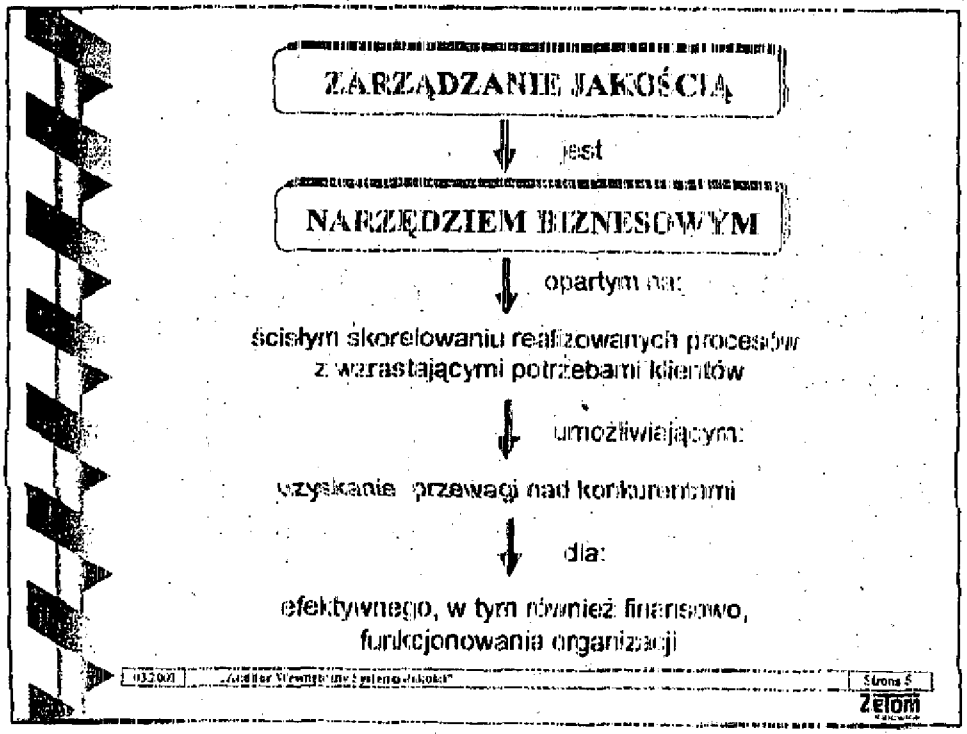

NORMY ISO serii 9000:2000
ISO 8402
ISO 9000-1
ISO 9000 : 2000
Podstawy i terminologia
ISO 9001
ISO 9002
ISO 9003
ISO 9001 : 2000
Systemy Zarządzania
Jakością - Wymagania
ISO 9004-1
ISO 9004 : 2000
Systemy Zarządzania
Jakością
Wytyczne dotyczące
doskonalenia
funkcjonowania
Strona 2
ZETOM

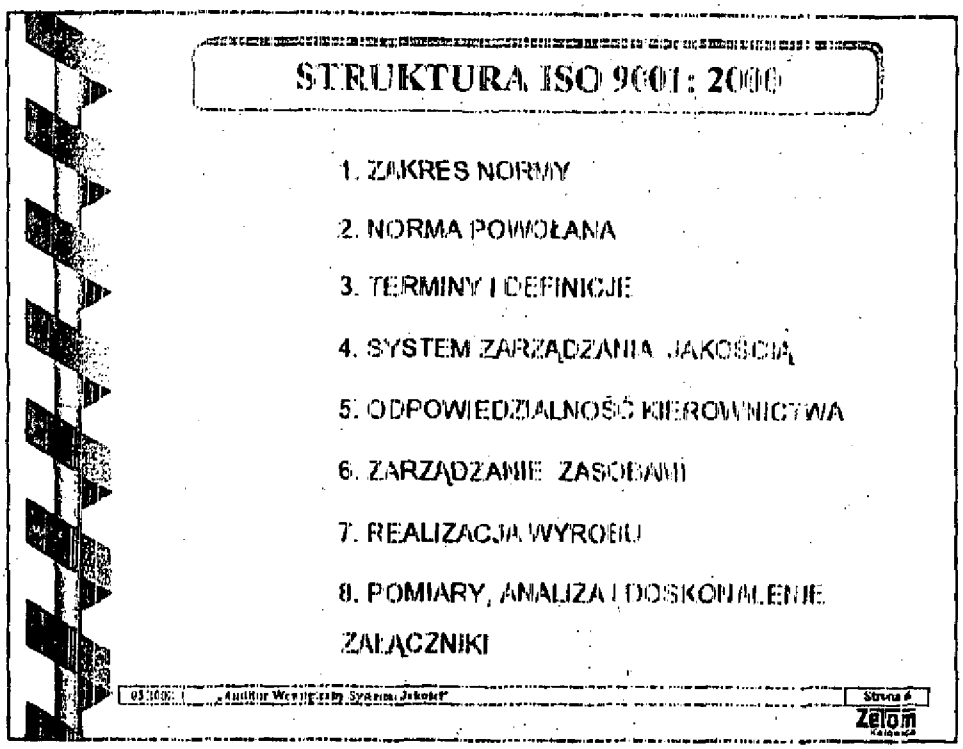
ZASADY ZARZĄDZANIA JAKOŚCIĄ WG ISO 9000:2000

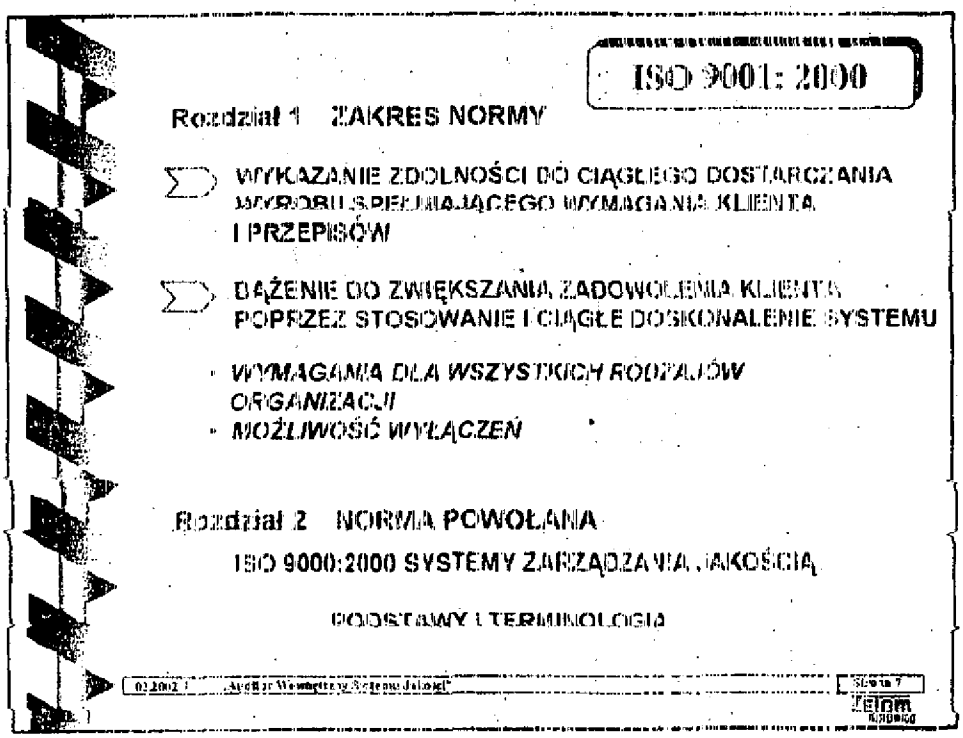
- ORIENTACJA NA KLIENTA
- PRZYWÓDZTWO
- ZAANGAŻOWANIE LUDZI
- PODEJŚCIE PROCESOWE
- PODEJŚCIE SYSTEMOWE DO ZARZĄDZANIA
- CIĄGŁE DOSKONALENIE
- PODEJMOWANIE DECYZJI NA PODSTAWIE FAKTÓW
- WZAJEMNIE KORZYSTNE POWIĄZANIA Z DOSTAWCAMI

CIĄGŁE DOSKONALENIE SYSTEMU ZARZĄDZANIA JAKOŚCIĄ




ZARZĄDZANIE JAKOŚCIĄ
jest
NARZĘDZIEM BIZNESOWYM
opartym na:
ścisłym skorelowaniu realizowanych procesów
z wzrastającymi potrzebami klientów
umożliwiającym:
uzyskanie przewagi nad konkurentami
dla:
efektywnego, w tym również finansowo,
funkcjonowania organizacji
Strona 5
Zelom


STRUKTURA ISO 9001: 2000
1. ZAKRES NORMY
2. NORMA POWOŁANA
3. TERMINY I DEFINICJE
4. SYSTEM ZARZĄDZANIA JAKOŚCIĄ
5. ODPOWIEDZIALNOŚĆ KIEROWNICTWA
6. ZARZĄDZANIE ZASOBAMI
7. REALIZACJA WYROBU
8. POMIARY, ANALIZA I DOSKONALENIE
ZAŁĄCZNIKI
Strona 6
Zelom


ISO 9001: 2000
Rozdział 1 ZAKRES NORMY
WYKAZANIE ZDOLNOŚCI DO CIĄGŁEGO DOSTARCZANIA WYROBU SPEŁNIAJĄCEGO WYMAGANIA KLIENTA I PRZEPISÓW
DĄŻENIE DO ZWIĘKSZANIA ZADOWOLENIA KLIENTA POPRZEZ STOSOWANIE I CIĄGŁE DOSKONALENIE SYSTEMU
WYMAGANIA DLA WSZYSTKICH RODZAJÓW ORGANIZACJI
MOŻLIWOŚĆ WYŁĄCZEŃ
Rozdział 2 NORMA POWOŁANA
ISO 9000:2000 SYSTEMY ZARZĄDZANIA JAKOŚCIĄ
PODSTAWY I TERMINOLOGIA


ISO 9001: 2000
Rozdział 3 TERMINY I DEFINICJE
łańcuch powiązań
DOSTAWCA
ORGANIZACJA
KLIENT
zastępuje dotychczasowe
PODWYKONAWCA
DOSTAWCA
KLIENT

PROCES ISO 9001: 2000

ZBIÓR DZIAŁAŃ WZAJEMNIE
POWIĄZANYCH
LUB
WZAJEMNIE ODDZIAŁYWUJĄCYCH,
KTÓRE PRZEKSZTAŁCAJĄ
WEJŚCIA W WYJŚCIA

ISO 9001: 2000

Rozdział 4 SYSTEM ZARZĄDZANIA JAKOŚCIĄ (1/5)

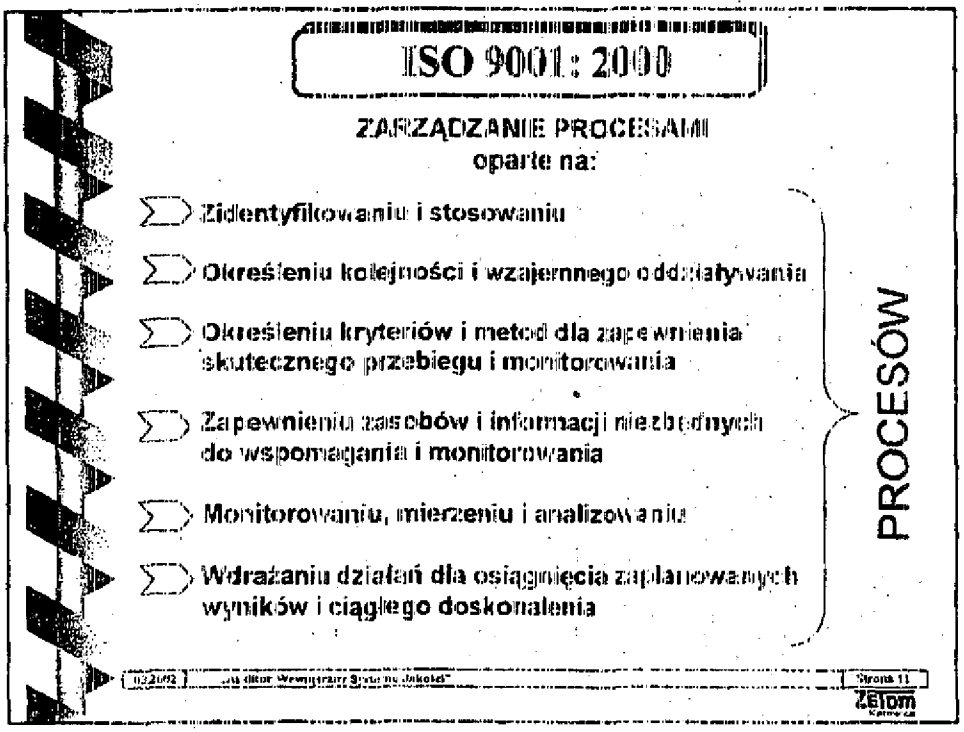
4.1 Wymagania ogólne

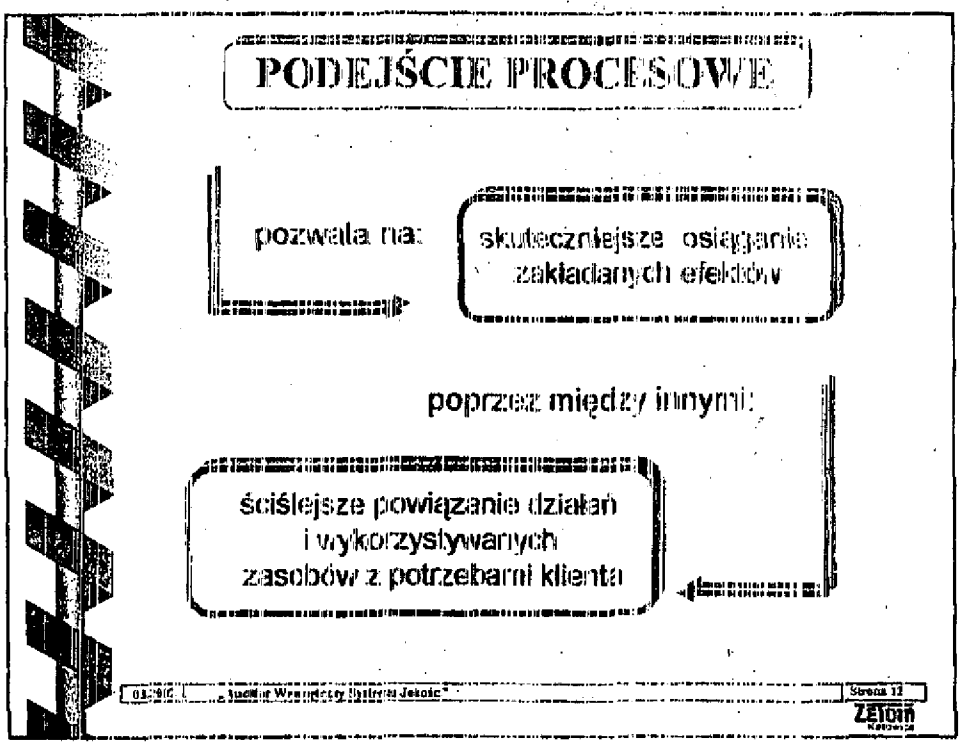
Należy:

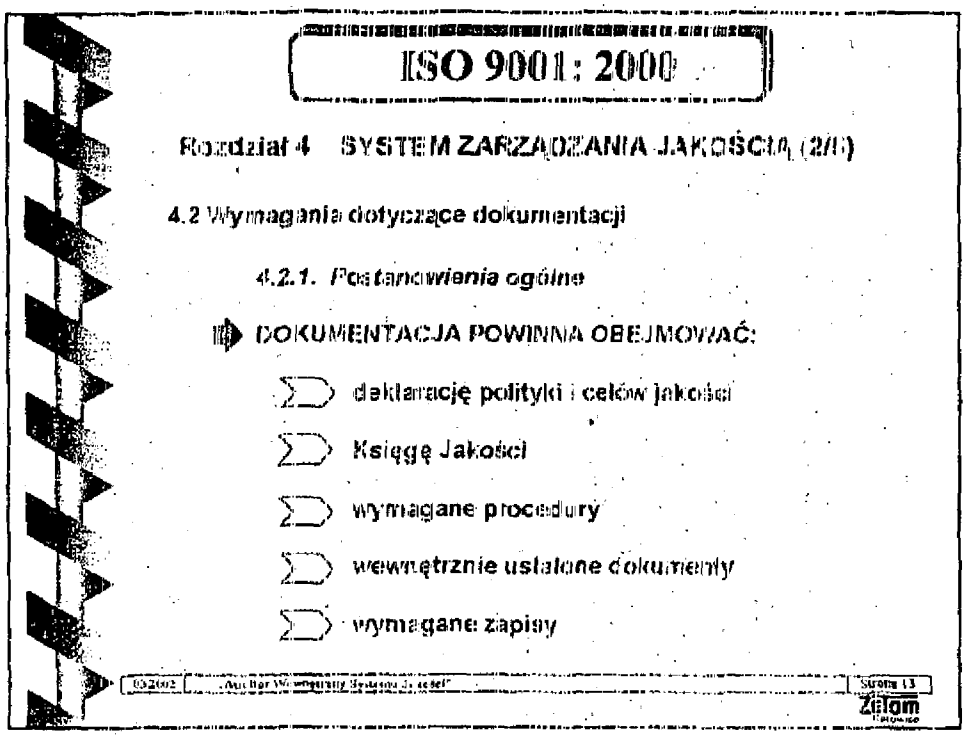
- ustanowić
- udokumentować
- wdrożyć
- utrzymywać i doskonalić

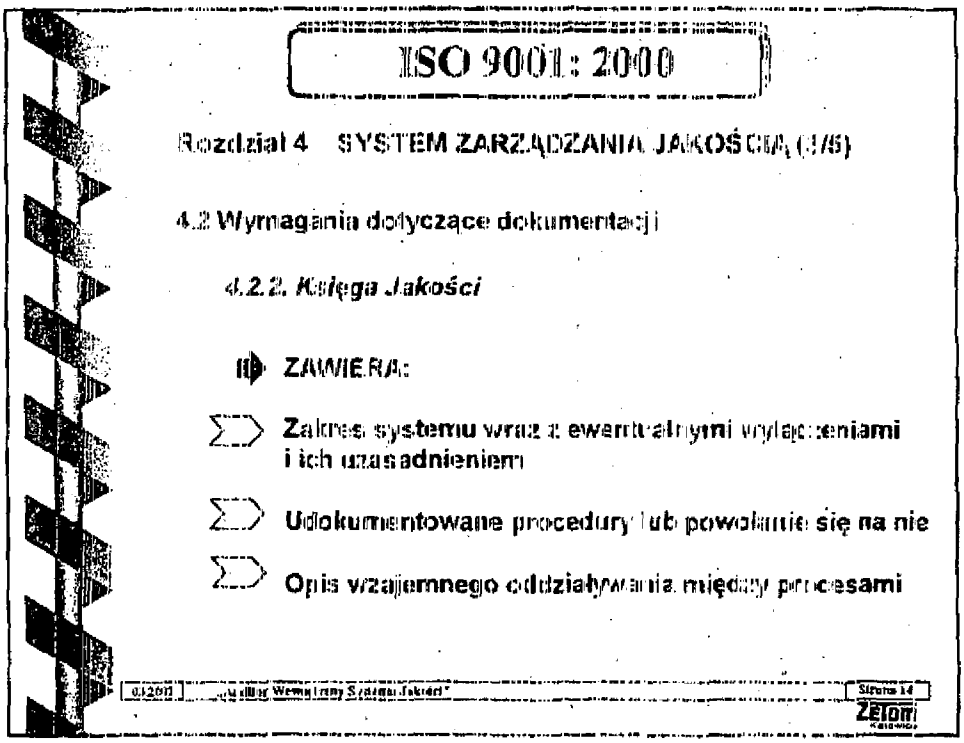
System Zarządzania Jakością zgodny z wymaganiami

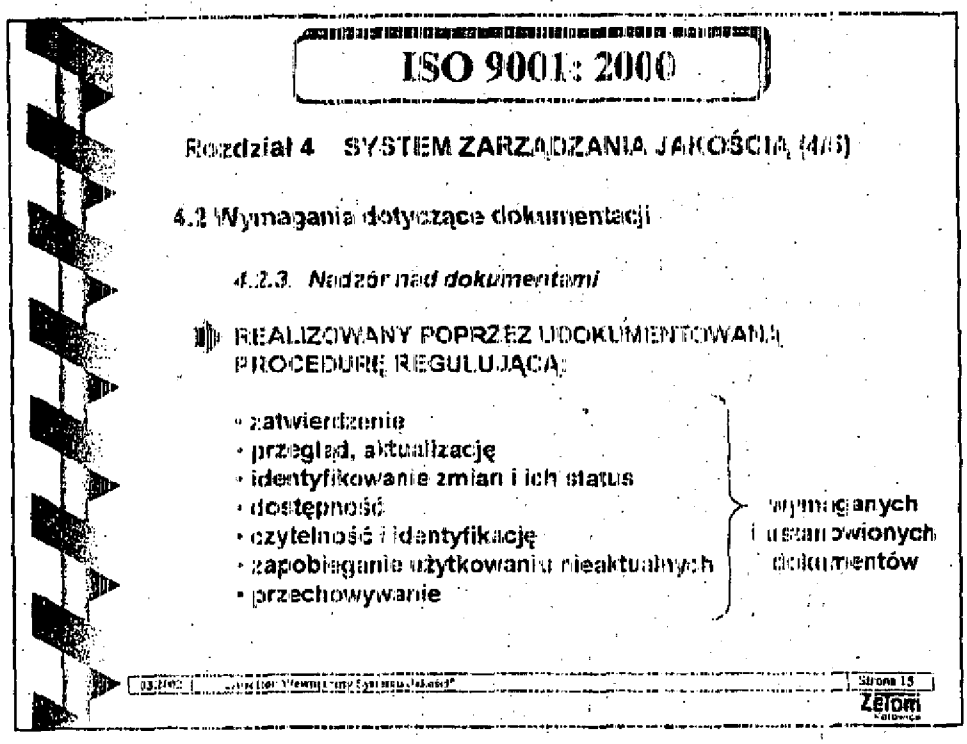
POPRZEZ ZARZĄDZANIE PROCESAMI

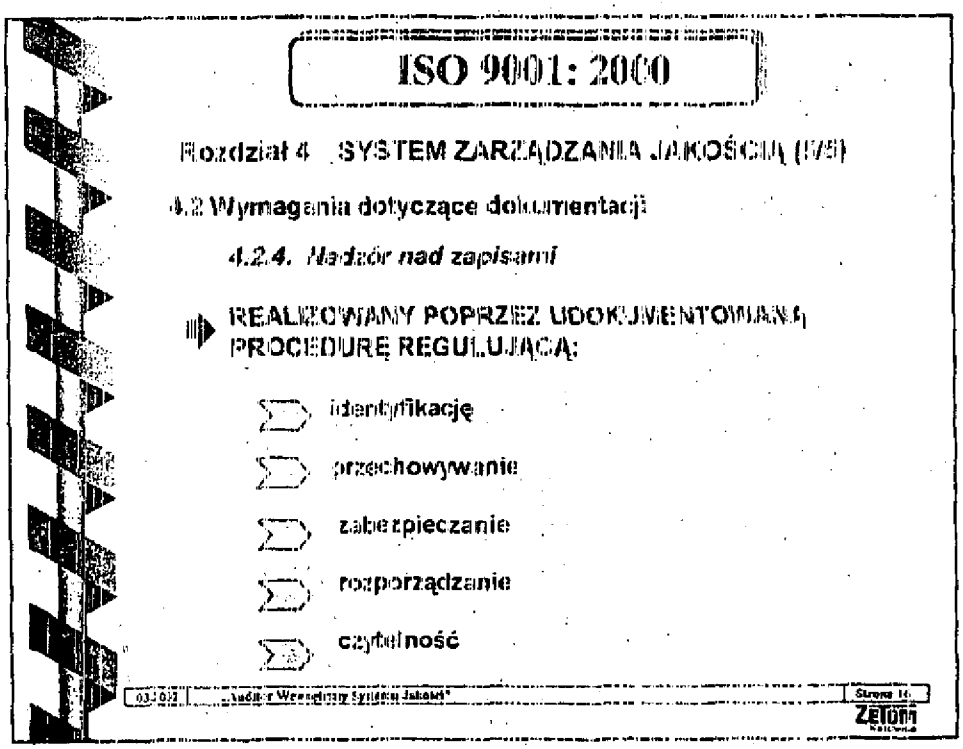

ISO 9001: 2000
ZARZĄDZANIE PROCESAMI
oparte na:
Zidentyfikowaniu i stosowaniu
Określeniu kolejności i wzajemnego oddziaływania
Określeniu kryteriów i metod dla zapewnienia skutecznego przebiegu i monitorowania
Zapewnieniu zasobów i informacji niezbędnych do wspomagania i monitorowania
Monitorowaniu, mierzeniu i analizowaniu
Wdrażaniu działań dla osiągnięcia zaplanowanych wyników i ciągłego doskonalenia
PROCESÓW
Strona 11
Zetom

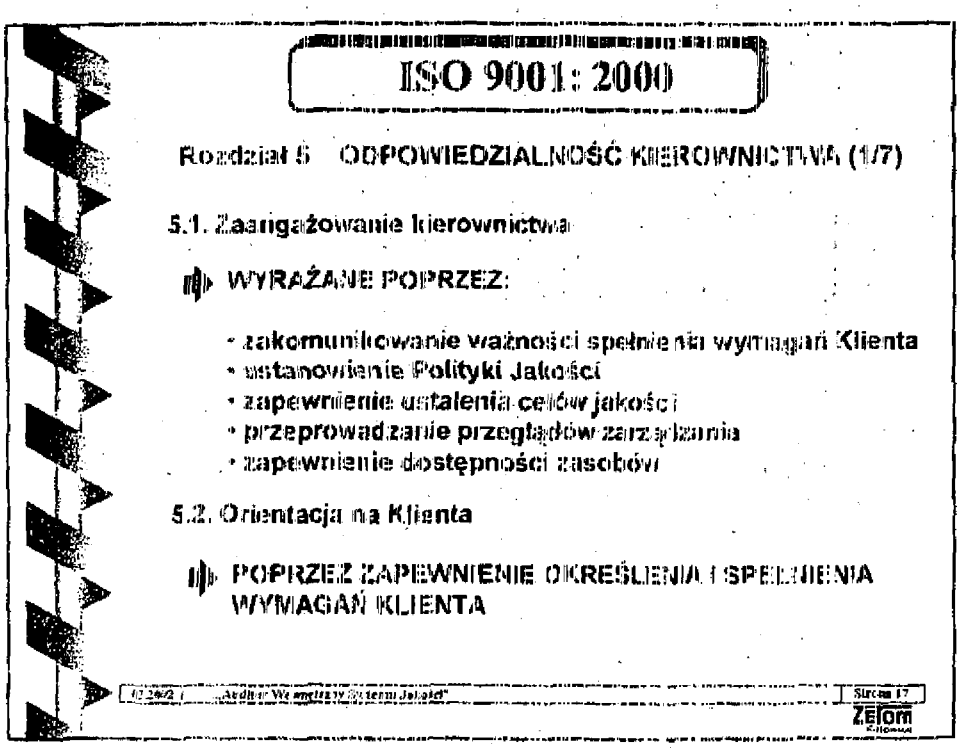

PODEJŚCIE PROCESOWE
pozwala na:
skuteczniejsze osiąganie zakładanych efektów
poprzez między innymi:
ściślejsze powiązanie działań i wykorzystywanych zasobów z potrzebami klienta
Strona 12
Zetom

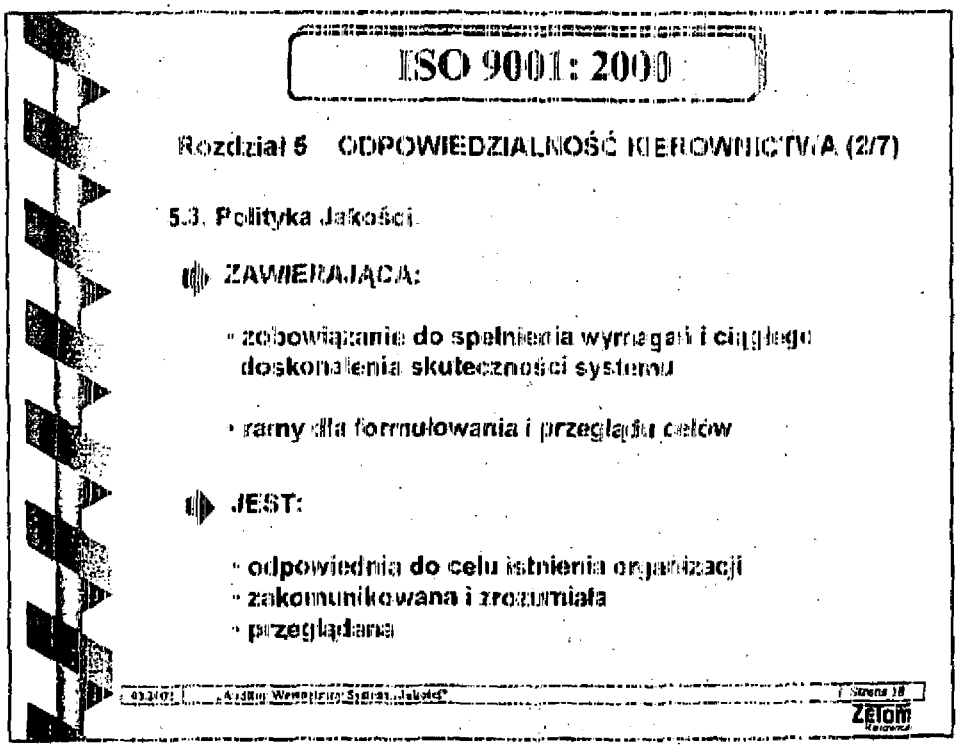

ISO 9001: 2000
Rozdział 4 SYSTEM ZARZĄDZANIA JAKOŚCIĄ (2/5)
4.2 Wymagania dotyczące dokumentacji
4.2.1. Postanowienia ogólne
DOKUMENTACJA POWINNA OBEJMOWAĆ:
deklarację polityki i celów jakości
Księgę Jakości
wymagane procedury
wewnętrznie ustalone dokumenty
wymagane zapisy
Strona 13
Zetom

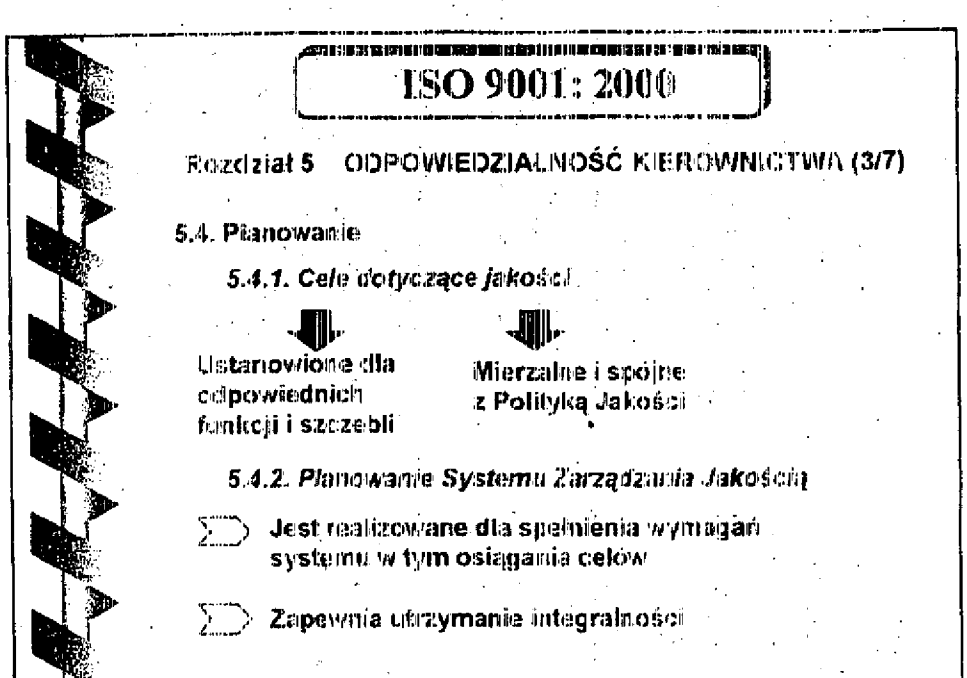

ISO 9001: 2000
Rozdział 4 SYSTEM ZARZĄDZANIA JAKOŚCIĄ (3/5)
4.2 Wymagania dotyczące dokumentacji
4.2.2. Księga Jakości
ZAWIERA:
Zakres systemu wraz z ewentualnymi wyłączeniami i ich uzasadnieniem
Udokumentowane procedury lub powołanie się na nie
Opis wzajemnego oddziaływania między procesami
Strona 14
Zetom

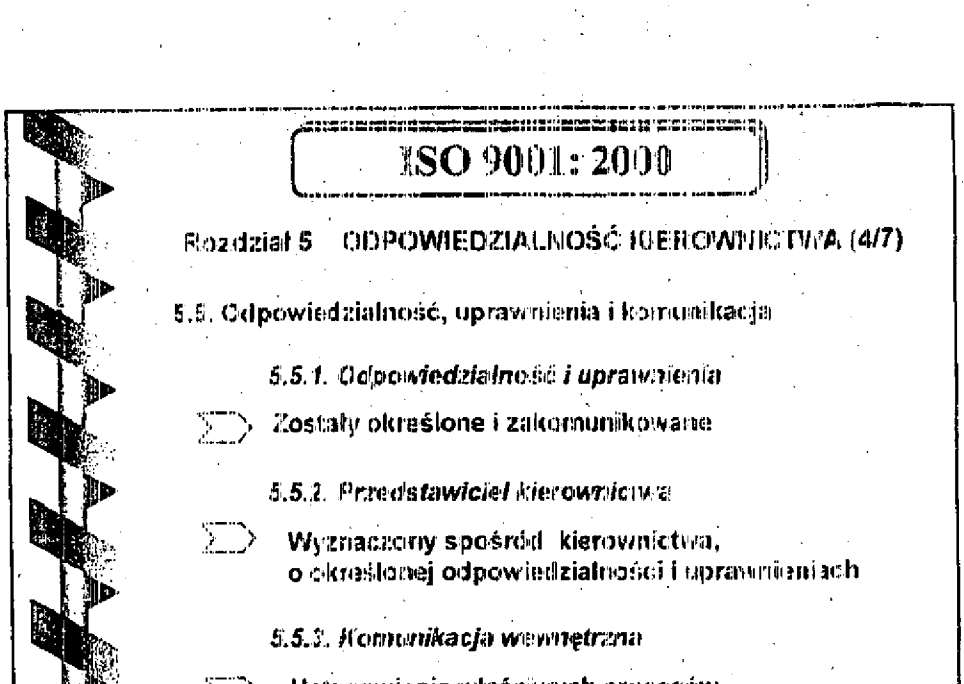

ISO 9001: 2000
Rozdział 4 SYSTEM ZARZĄDZANIA JAKOŚCIĄ (4/5)
4.2 Wymagania dotyczące dokumentacji
4.2.3. Nadzór nad dokumentami
REALIZOWANY POPRZEZ UDOKUMENTOWANĄ PROCEDURĘ REGULUJĄCĄ:
• zatwierdzenie
• przegląd, aktualizację
• identyfikowanie zmian i ich status
• dostępność
• czytelność i identyfikację
• zapobieganie użytkowaniu nieaktualnych
• przechowywanie
wymaganych i ustanowionych dokumentów
Strona 15
Zetom


ISO 9001: 2000
Rozdział 4 SYSTEM ZARZĄDZANIA JAKOŚCIĄ (5/5)
4.2 Wymagania dotyczące dokumentacji
4.2.4. Nadzór nad zapisami
REALIZOWANY POPRZEZ UDOKUMENTOWANĄ PROCEDURĘ REGULUJĄCĄ:
identyfikację
przechowywanie
zabezpieczanie
rozporządzanie
czytelność
Strona 16
Zetom


ISO 9001: 2000
Rozdział 5 ODPOWIEDZIALNOŚĆ KIEROWNICTWA (1/7)
5.1. Zaangażowanie kierownictwa
WYRAŻANE POPRZEZ:
• zakomunikowanie ważności spełnienia wymagań Klienta
• ustanowienie Polityki Jakości
• zapewnienie ustalenia celów jakości
• przeprowadzanie przeglądów zarządzania
• zapewnienie dostępności zasobów
5.2. Orientacja na Klienta
POPRZEZ ZAPEWNIENIE OKREŚLENIA I SPEŁNIENIA WYMAGAŃ KLIENTA
Zetom


ISO 9001: 2000
Rozdział 5 ODPOWIEDZIALNOŚĆ KIEROWNICTWA (2/7)
5.3. Polityka Jakości
ZAWIERAJĄCA:
• zobowiązanie do spełnienia wymagań i ciągłego doskonalenia skuteczności systemu
• ramy dla formułowania i przeglądu celów
JEST:
• odpowiednia do celu istnienia organizacji
• zakomunikowana i zrozumiała
• przeglądana
Zetom


ISO 9001: 2000
Rozdział 5 ODPOWIEDZIALNOŚĆ KIEROWNICTWA (3/7)
5.4. Planowanie
5.4.1. Cele dotyczące jakości
Ustanowione dla odpowiednich funkcji i szczebli
Mierzalne i spójne z Polityką Jakości
5.4.2. Planowanie Systemu Zarządzania Jakością
Jest realizowane dla spełnienia wymagań systemu w tym osiągania celów
Zapewnia utrzymanie integralności
Strona 19
ZETOM


ISO 9001: 2000
Rozdział 5 ODPOWIEDZIALNOŚĆ KIEROWNICTWA (4/7)
5.5. Odpowiedzialność, uprawnienia i komunikacja
5.5.1. Odpowiedzialność i uprawnienia
Zostały określone i zakomunikowane
5.5.2. Przedstawiciel kierownictwa
Wyznaczony spośród kierownictwa, o określonej odpowiedzialności i uprawnieniach
5.5.3. Komunikacja wewnętrzna
Ustanowienie właściwych procesów komunikacyjnych w organizacji oraz w odniesieniu do skuteczności systemu
Strona 20
ZETOM

ISO 9001: 2000

Rozdział 5 ODPOWIEDZIALNOŚĆ KIEROWNICTWA (6/7)

5.6. Przegląd zarządzania

5.6.1. Postanowienia ogólne

- Przeglądy przeprowadzane w zaplanowanych odstępach czasu
- Obejmujące ocenę możliwości doskonalenia i potrzebę zmian w systemie, łącznie z polityką jakości i celami jakości

ISO 9001: 2000

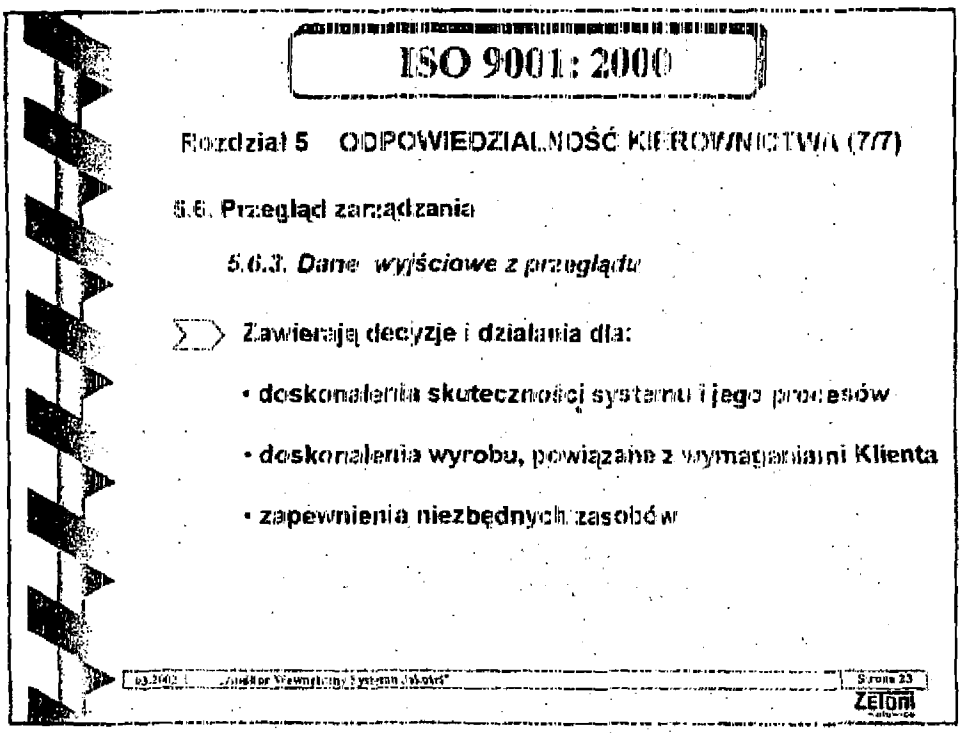
Rozdział 5 ODPOWIEDZIALNOŚĆ KIEROWNICTWA (6/7)

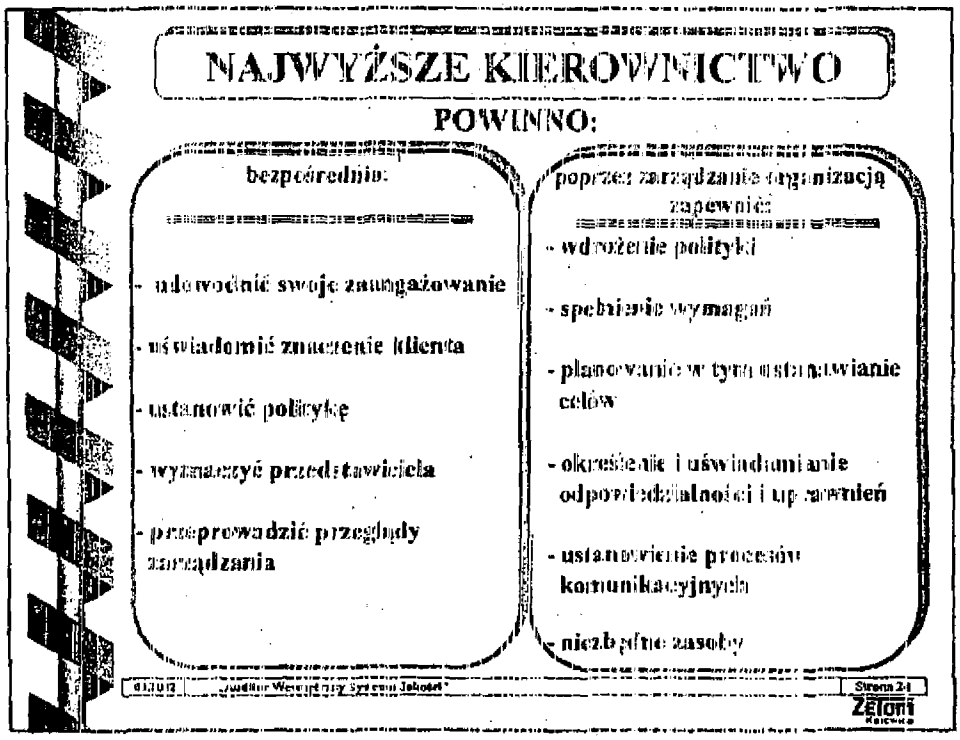
5.6. Przegląd zarządzania

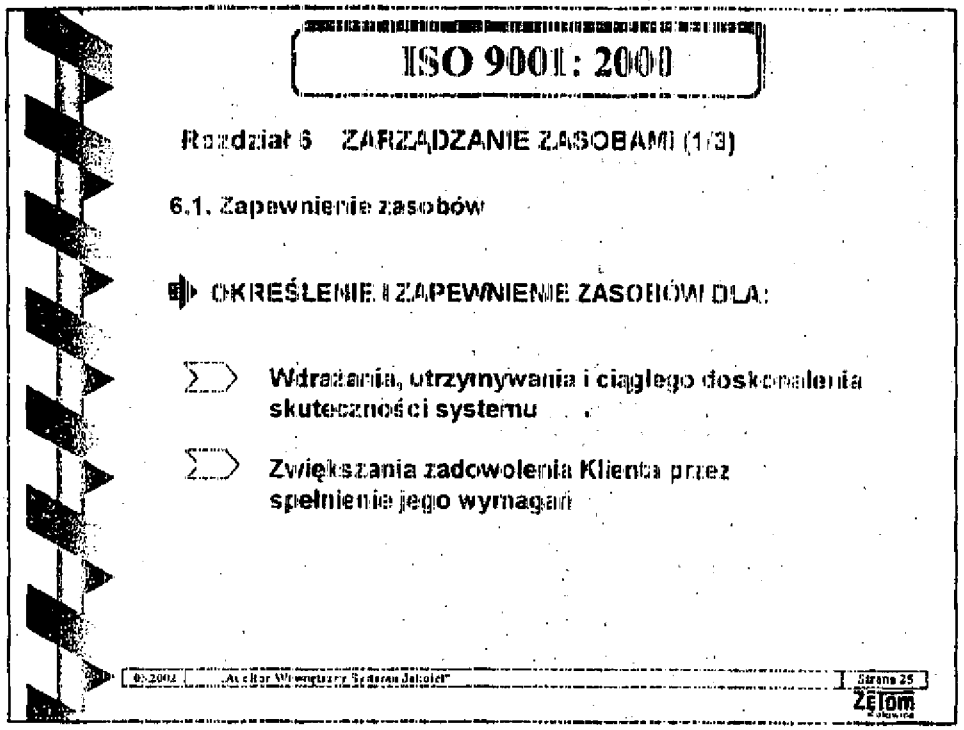
5.6.2. Dane wejściowe do przeglądu

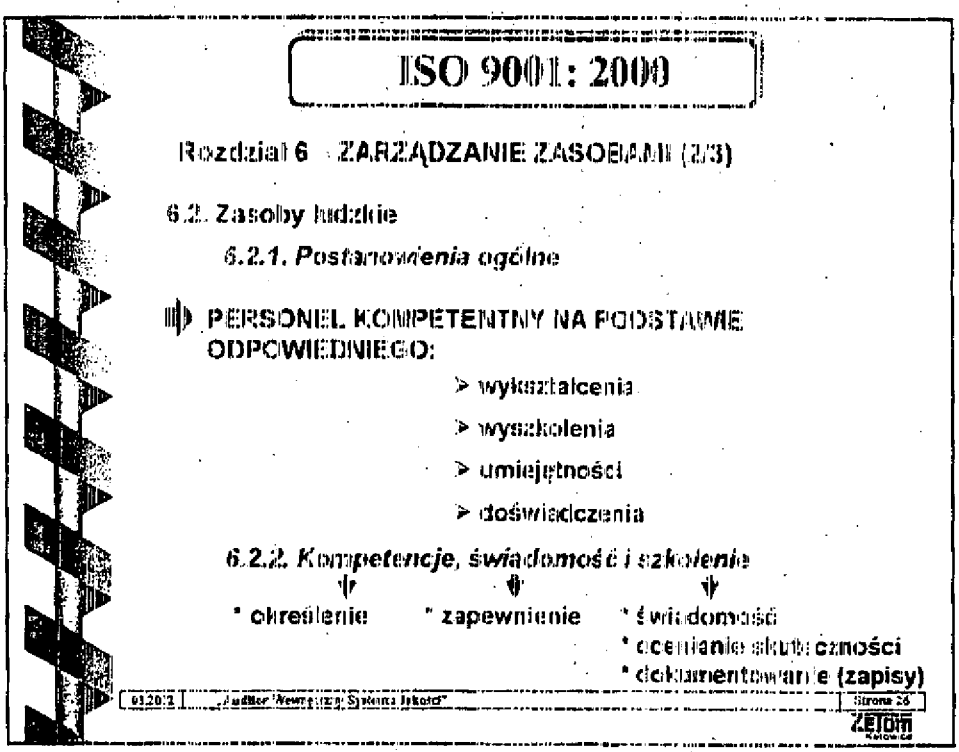
OBEJMUJĄ

- Informacje dotyczące:
  - wyników auditów
  - klientów
  - procesów i wyrobu
  - statusu działań doskonalących
  - realizacji działań wynikających z wcześniejszych przeglądów
  - zaplanowanych zmian
  - zaleceń dla doskonalenia


ISO 9001: 2000
Rozdział 5 ODPOWIEDZIALNOŚĆ KIEROWNICTWA (7/7)
5.6. Przegląd zarządzania
5.6.3. Dane wyjściowe z przeglądu
Zawierają decyzje i działania dla:
• doskonalenia skuteczności systemu i jego procesów
• doskonalenia wyrobu, powiązane z wymaganiami Klienta
• zapewnienia niezbędnych zasobów
Strona 23
ZETOM


NAJWYŻSZE KIEROWNICTWO
POWINNO:
bezpośrednio:
- udowodnić swoje zaangażowanie
- uświadomić znaczenie klienta
- ustanowić politykę
- wyznaczyć przedstawiciela
- przeprowadzić przeglądy zarządzania
poprzez zarządzanie organizacją zapewnić:
- wdrożenie polityki
- spełnienie wymagań
- planowanie w tym ustanawianie celów
- określenie i uświadamianie odpowiedzialności i uprawnień
- ustanowienie procesów komunikacyjnych
- niezbędne zasoby
Strona 24
ZETOM


ISO 9001: 2000
Rozdział 6 ZARZĄDZANIE ZASOBAMI (1/3)
6.1. Zapewnienie zasobów
OKREŚLENIE I ZAPEWNIENIE ZASOBÓW DLA:
Wdrażania, utrzymywania i ciągłego doskonalenia skuteczności systemu
Zwiększania zadowolenia Klienta przez spełnienie jego wymagań
Strona 25
ZETOM


ISO 9001: 2000
Rozdział 6 ZARZĄDZANIE ZASOBAMI (2/3)
6.2. Zasoby ludzkie
6.2.1. Postanowienia ogólne
PERSONEL KOMPETENTNY NA PODSTAWIE ODPOWIEDNIEGO:
wykształcenia
wyszkolenia
umiejętności
doświadczenia
6.2.2. Kompetencje, świadomość i szkolenie
* określenie
* zapewnienie
* świadomości
* oceniania skuteczności
* dokumentowanie (zapisy)
Strona 26
ZETOM

ISO 9001: 2000

Rozdział 6 ZARZĄDZANIE ZASOBAMI (3/3)

6.3. Infrastruktura

- OKREŚLENIE, ZAPEWNIENIE I UTRZYMYWANIE
  - zabudowania, przestrzeń, instalacje
  - wyposażenie procesu (sprzęt, oprogramowanie)
  - usługi pomocnicze (transport, łączność)

6.4. Środowisko pracy

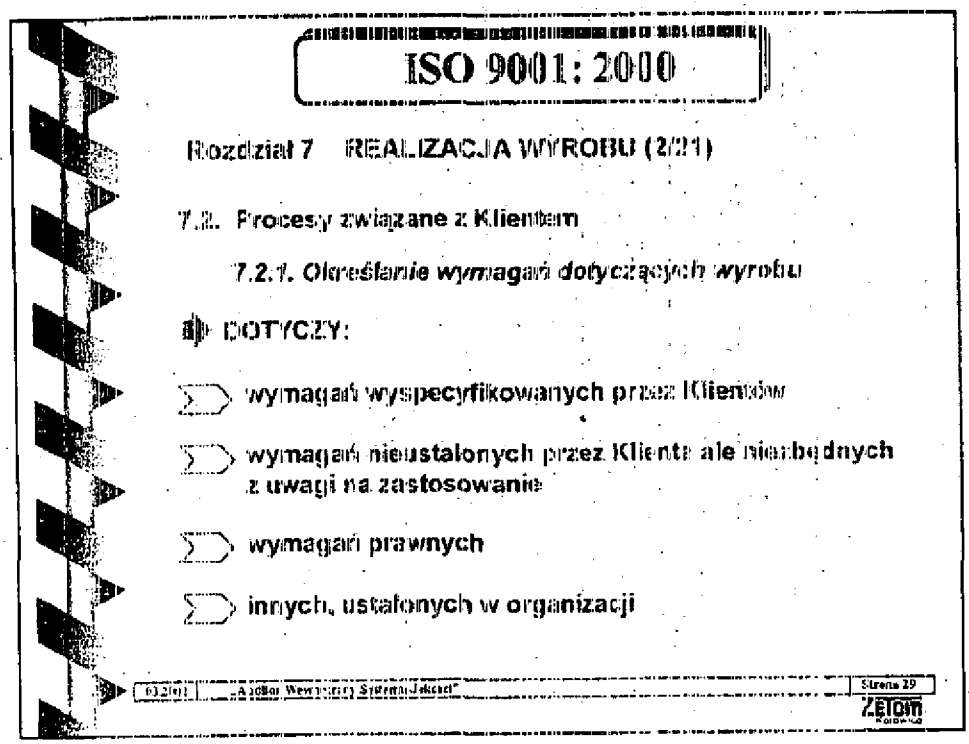
- OKREŚLONE I ZARZĄDZANE DLA:
  osiągnięcia zgodności z wymaganiami dot. wyrobu

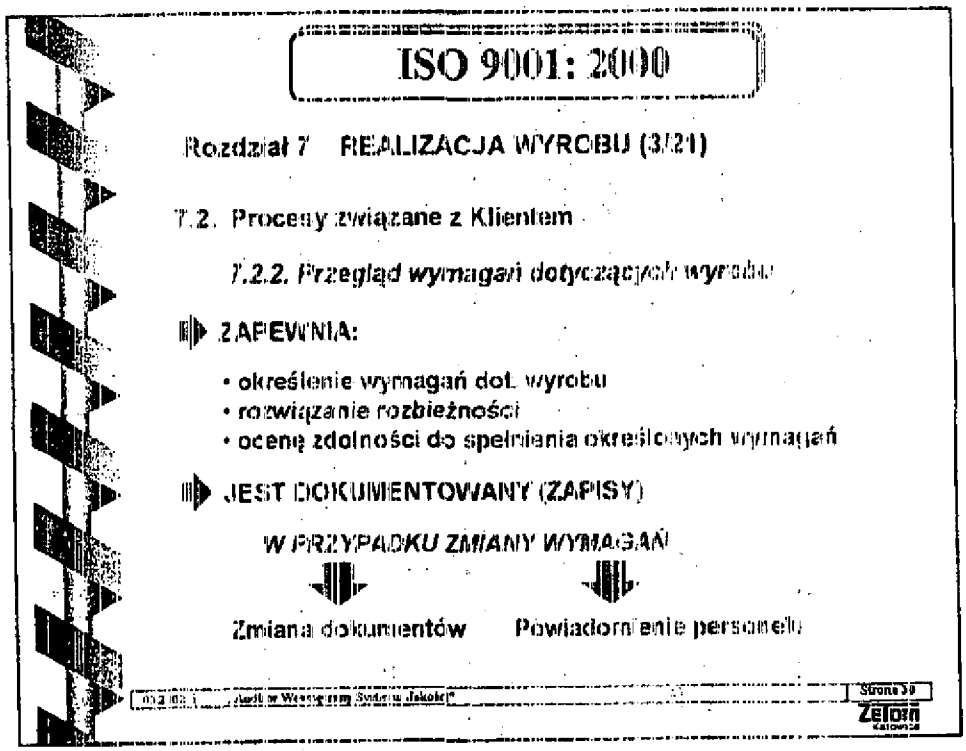
ISO 9001: 2000

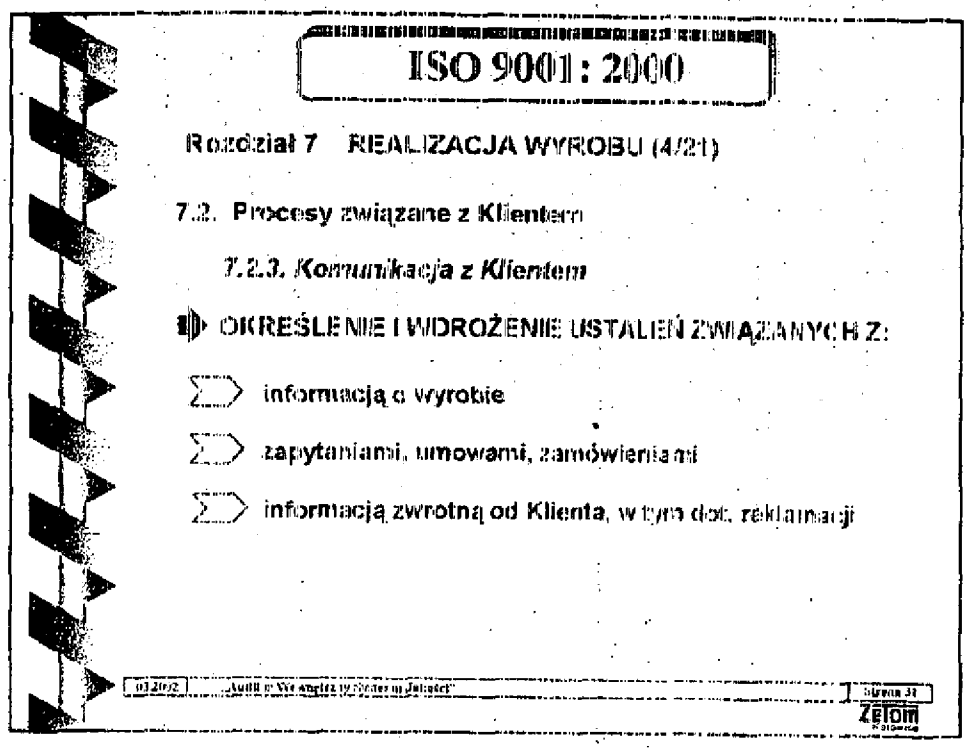
Rozdział 7 REALIZACJA WYROBU (1/21)

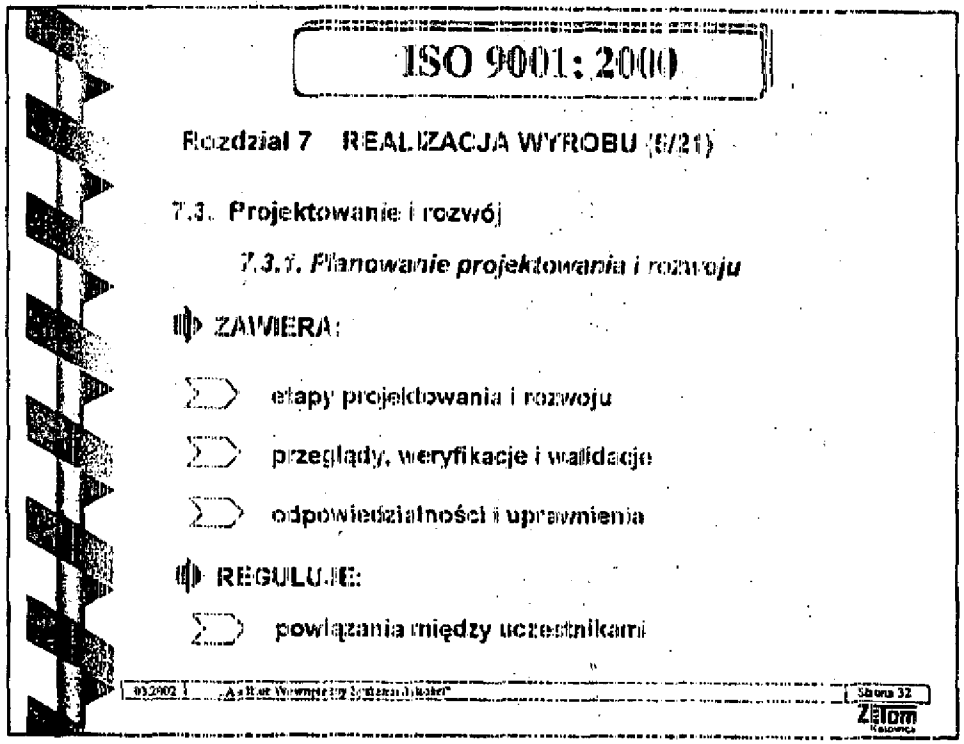
7.1. Planowanie realizacji wyrobu

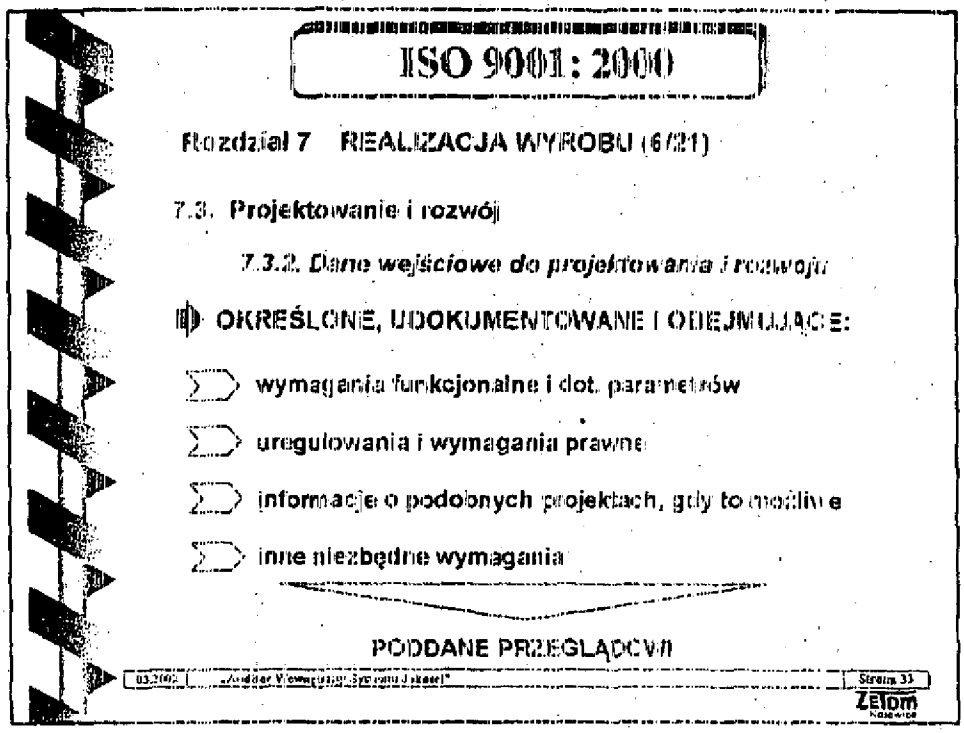
- Planowanie i opracowywanie procesów niezbędnych dla realizacji wyrobu.
- Planowanie realizacji wyrobu zachowuje spójność z innymi procesami systemu i odpowiednio obejmuje:
  - cele dot. jakości wymagania dla wyrobu
  - potrzeby dotyczące procesów, dokumentów i zasobów
  - specyficzne działania dot. weryfikacji, walidacji, monitorowania, kontroli i badań oraz kryteria przyjęcia
  - niezbędne zapisy

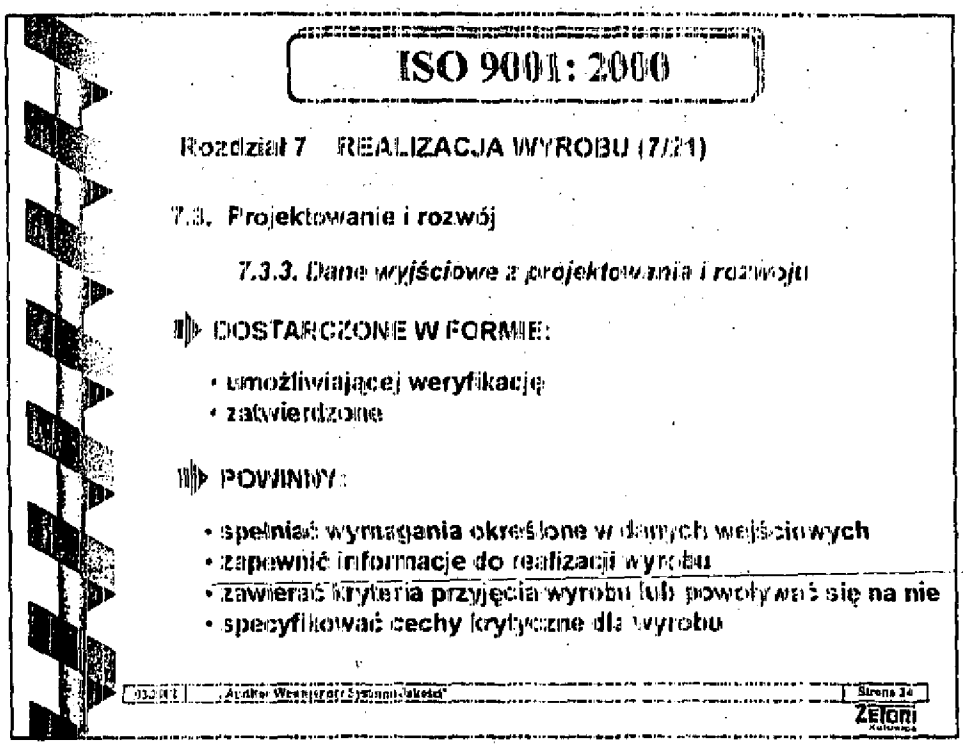

ISO 9001: 2000
Rozdział 7 REALIZACJA WYROBU (2/21)
7.2. Procesy związane z Klientem
7.2.1. Określanie wymagań dotyczących wyrobu
DOTYCZY:
wymagań wyspecyfikowanych przez Klientów
wymagań nieustalonych przez Klienta ale niezbędnych z uwagi na zastosowanie
wymagań prawnych
innych, ustalonych w organizacji
Strona 29
ZETOM

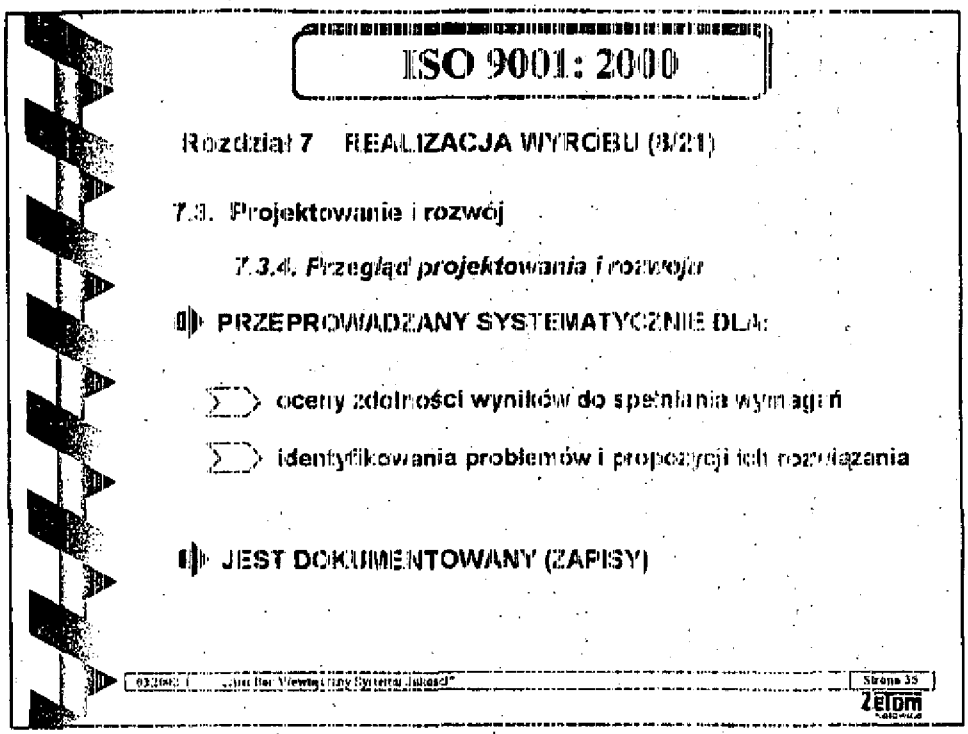

ISO 9001: 2000
Rozdział 7 REALIZACJA WYROBU (3/21)
7.2. Procesy związane z Klientem
7.2.2. Przegląd wymagań dotyczących wyrobu
ZAPEWNIA:
• określenie wymagań dot. wyrobu
• rozwiązanie rozbieżności
• ocenę zdolności do spełnienia określonych wymagań
JEST DOKUMENTOWANY (ZAPISY)
W PRZYPADKU ZMIANY WYMAGAŃ
Zmiana dokumentów
Powiadomienie personelu
Strona 30
ZETOM

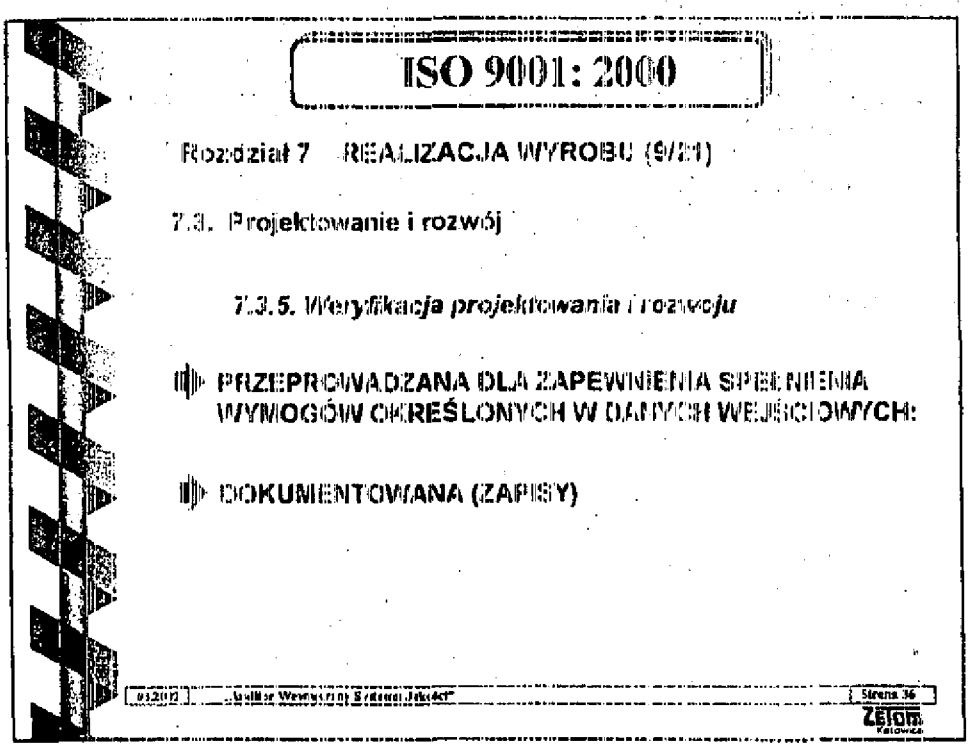

ISO 9001: 2000
Rozdział 7 REALIZACJA WYROBU (4/21)
7.2. Procesy związane z Klientem
7.2.3. Komunikacja z Klientem
OKREŚLENIE I WDROŻENIE USTALEŃ ZWIĄZANYCH Z:
informacją o wyrobie
zapytaniami, umowami, zamówieniami
informacją zwrotną od Klienta, w tym dot. reklamacji
Zetom

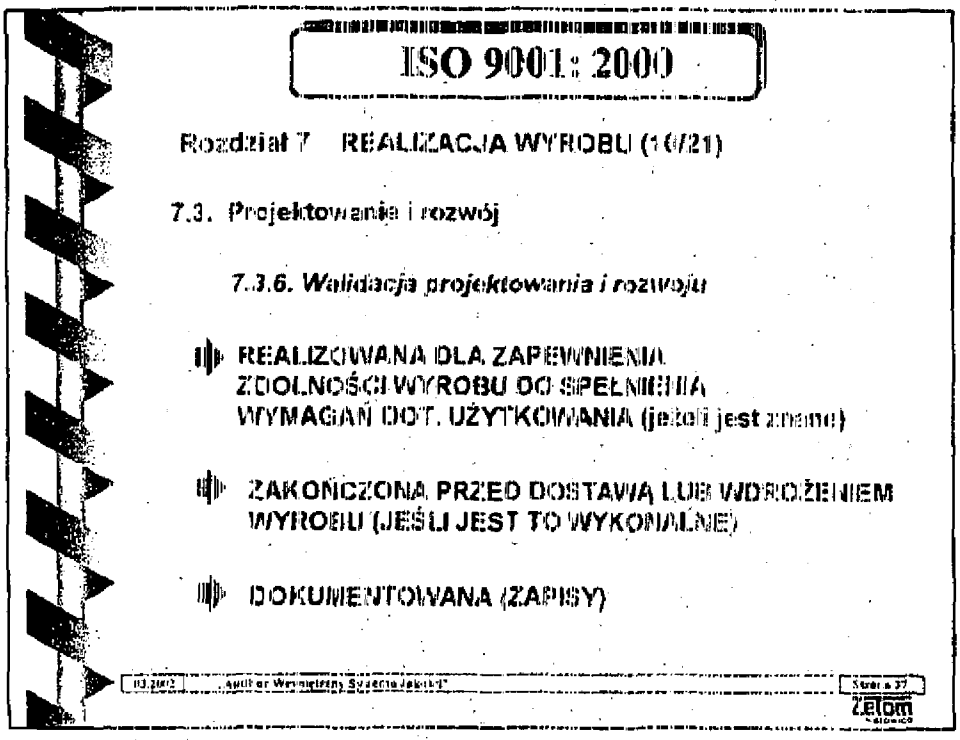

ISO 9001: 2000
Rozdział 7 REALIZACJA WYROBU (5/21)
7.3. Projektowanie i rozwój
7.3.1. Planowanie projektowania i rozwoju
ZAWIERA:
etapy projektowania i rozwoju
przeglądy, weryfikacje i walidacje
odpowiedzialności i uprawnienia
REGULUJE:
powiązania między uczestnikami
Zetom

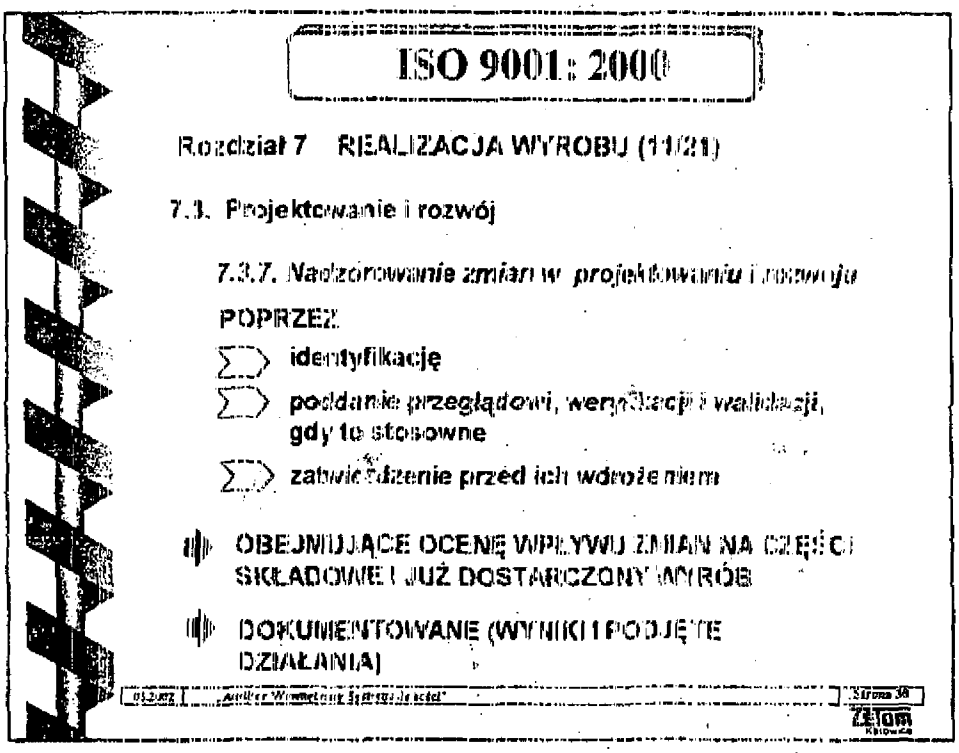

ISO 9001: 2000
Rozdział 7 REALIZACJA WYROBU (6/21)
7.3. Projektowanie i rozwój
7.3.2. Dane wejściowe do projektowania i rozwoju
OKREŚLONE, UDOKUMENTOWANE I ODEJMUJĄCE:
wymagania funkcjonalne i dot. parametrów
uregulowania i wymagania prawne
informacje o podobnych projektach, gdy to możliwe
inne niezbędne wymagania
PODDANE PRZEGLĄDOM
Strona 33
Zetom

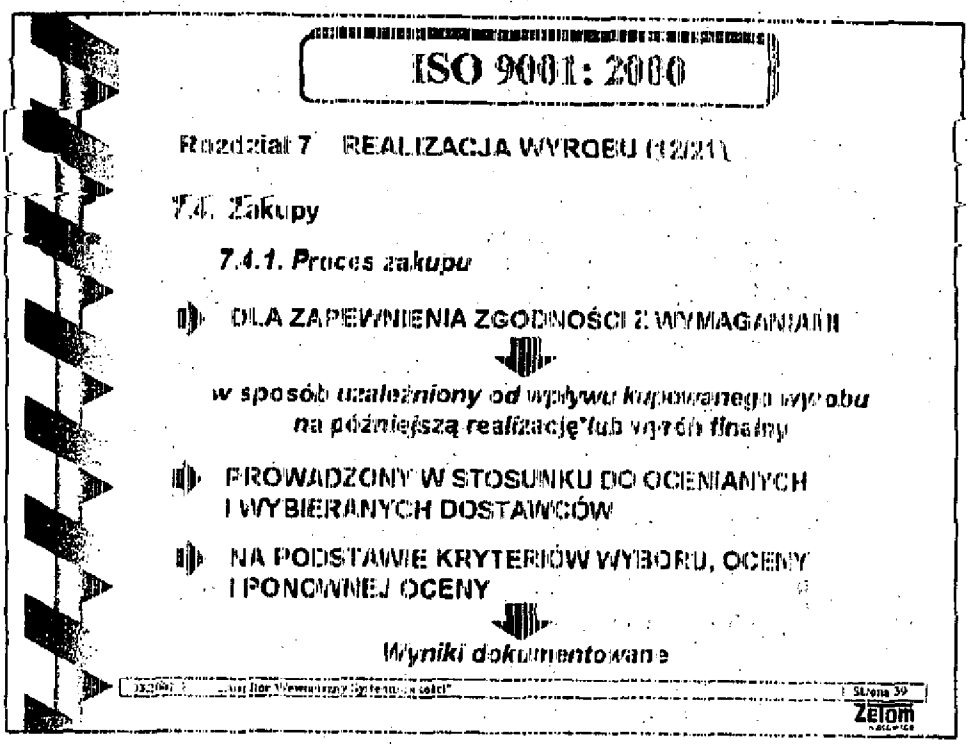

ISO 9001: 2000
Rozdział 7 REALIZACJA WYROBU (7/21)
7.3. Projektowanie i rozwój
7.3.3. Dane wyjściowe z projektowania i rozwoju
DOSTARCZONE W FORMIE:
umożliwiającej weryfikację
zatwierdzone
POWINNY:
spełniać wymagania określone w danych wejściowych
zapewnić informacje do realizacji wyrobu
zawierać kryteria przyjęcia wyrobu lub powoływać się na nie
specyfikować cechy krytyczne dla wyrobu
Strona 34
Zetom

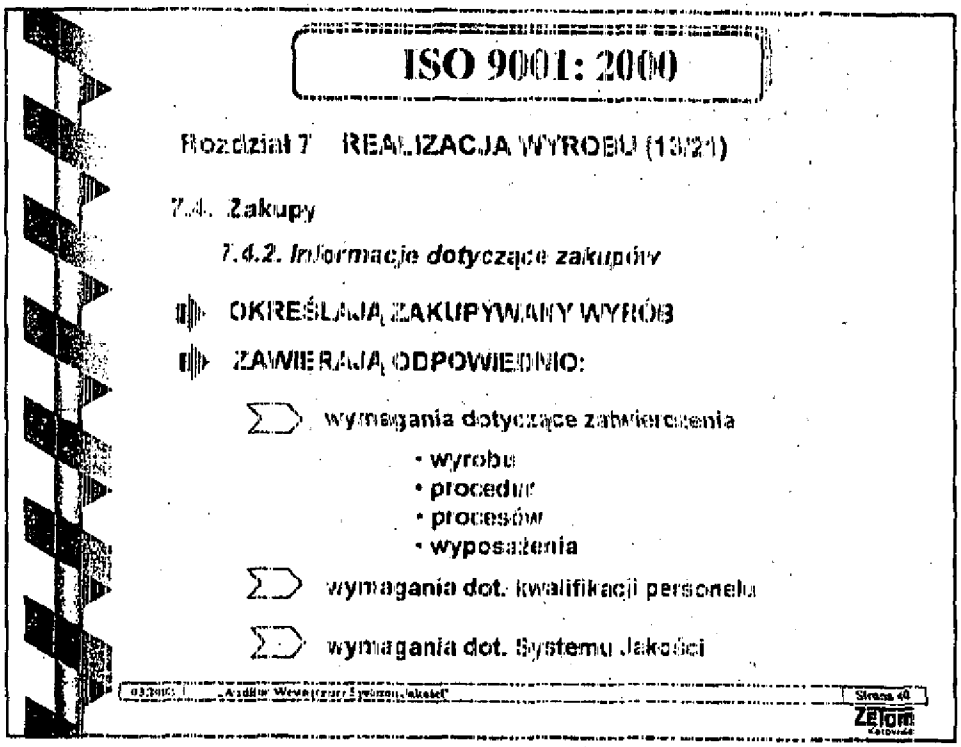

ISO 9001: 2000
Rozdział 7 REALIZACJA WYROBU (8/21)
7.3. Projektowanie i rozwój
7.3.4. Przegląd projektowania i rozwoju
PRZEPROWADZANY SYSTEMATYCZNIE DLA:
oceny zdolności wyników do spełniania wymagań
identyfikowania problemów i propozycji ich rozwiązania
JEST DOKUMENTOWANY (ZAPISY)
Strona 35
Zetom

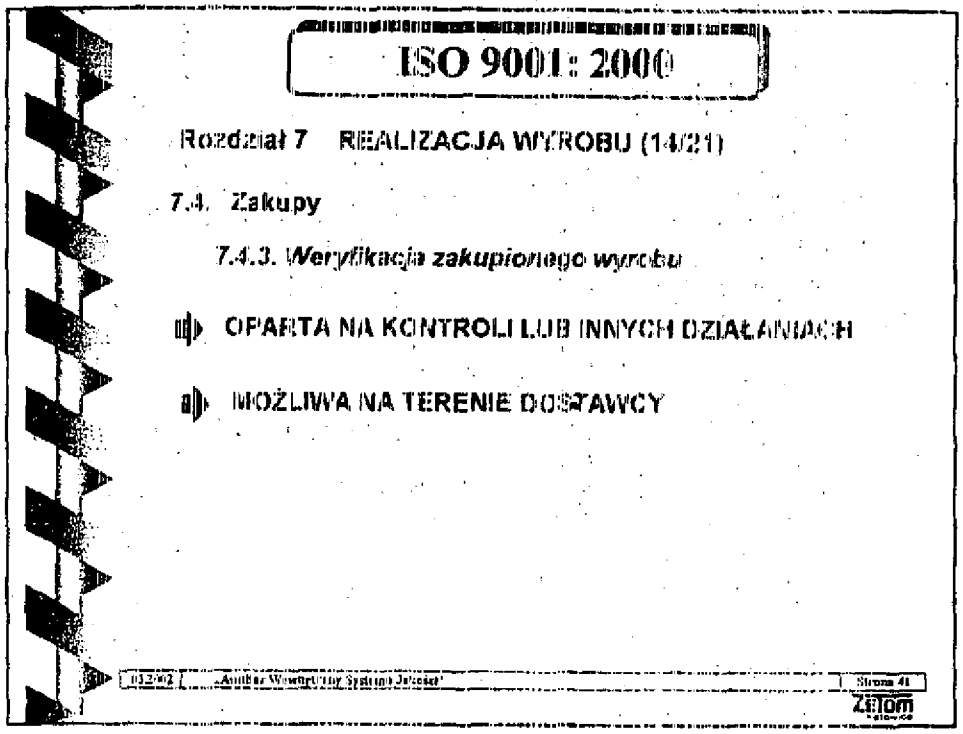

ISO 9001: 2000
Rozdział 7 REALIZACJA WYROBU (9/21)
7.3. Projektowanie i rozwój
7.3.5. Weryfikacja projektowania i rozwoju
PRZEPROWADZANA DLA ZAPEWNIENIA SPEŁNIENIA WYMOGÓW OKREŚLONYCH W DANYCH WEJŚCIOWYCH:
DOKUMENTOWANA (ZAPISY)
Strona 36
Zetom

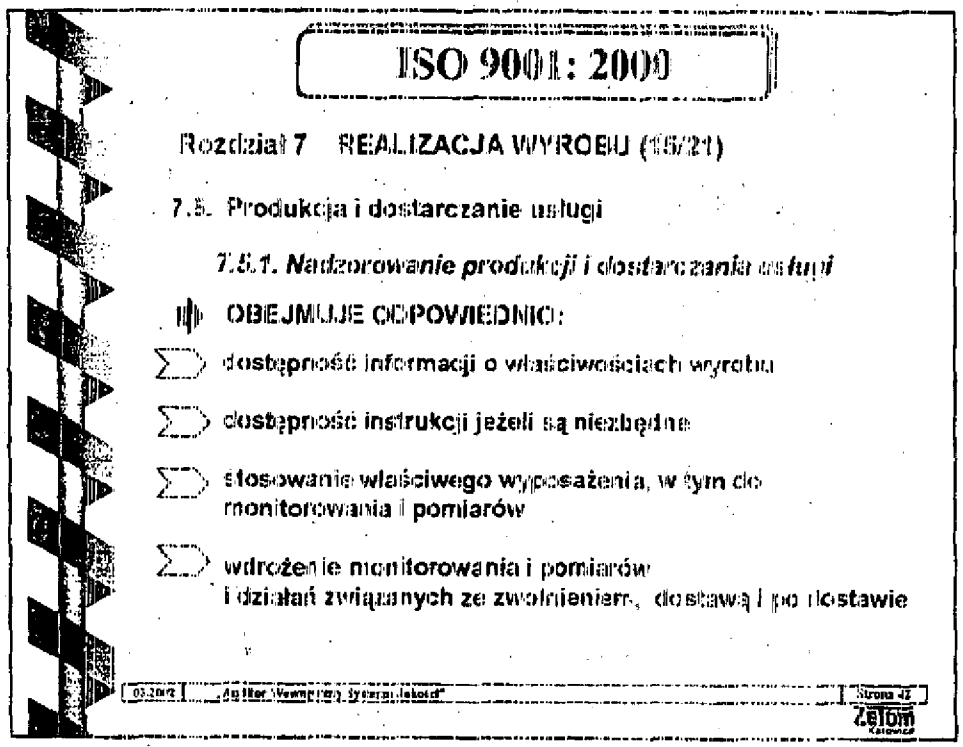

ISO 9001: 2000
Rozdział 7 REALIZACJA WYROBU (10/21)
7.3. Projektowanie i rozwój
7.3.6. Walidacja projektowania i rozwoju
REALIZOWANA DLA ZAPEWNIENIA ZDOLNOŚCI WYROBU DO SPEŁNIENIA WYMAGAŃ DOT. UŻYTKOWANIA (jeżeli jest znane)
ZAKOŃCZONA PRZED DOSTAWĄ LUB WDROŻENIEM WYROBU (JEŚLI JEST TO WYKONALNE)
DOKUMENTOWANA (ZAPISY)

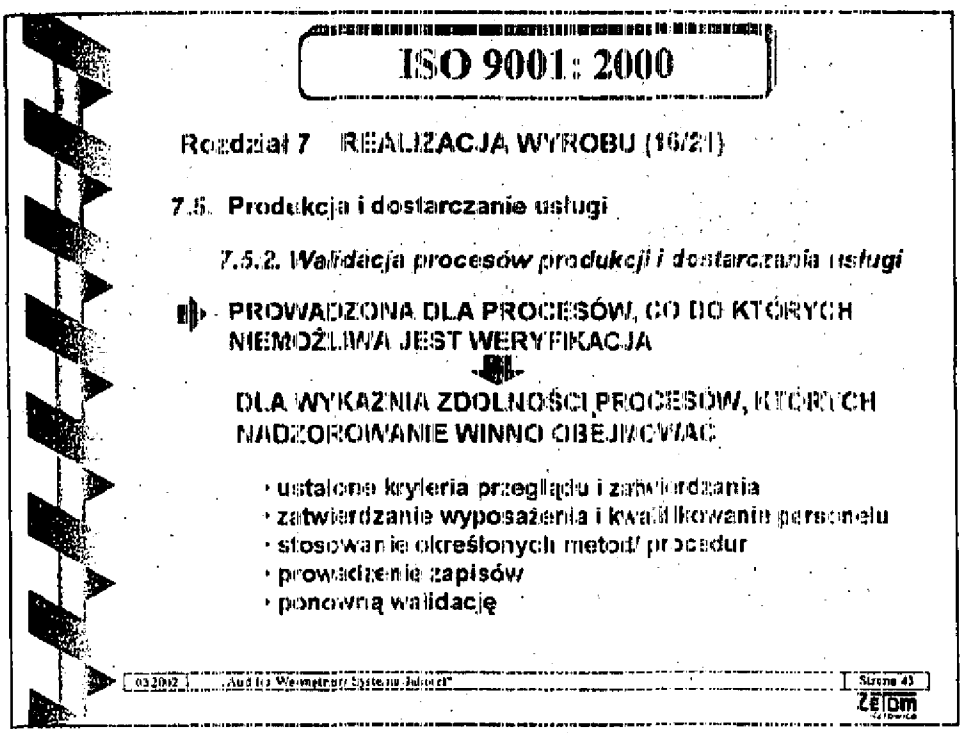

ISO 9001: 2000
Rozdział 7 REALIZACJA WYROBU (11/21)
7.3. Projektowanie i rozwój
7.3.7. Nadzorowanie zmian w projektowaniu i rozwoju
POPRZEZ
identyfikację
poddanie przeglądowi, weryfikacji i walidacji, gdy to stosowne
zatwierdzenie przed ich wdrożeniem
OBEJMUJĄCE OCENĘ WPŁYWU ZMIAN NA CZĘŚCI SKŁADOWE I JUŻ DOSTARCZONY WYRÓB
DOKUMENTOWANE (WYNIKI I PODJĘTE DZIAŁANIA)

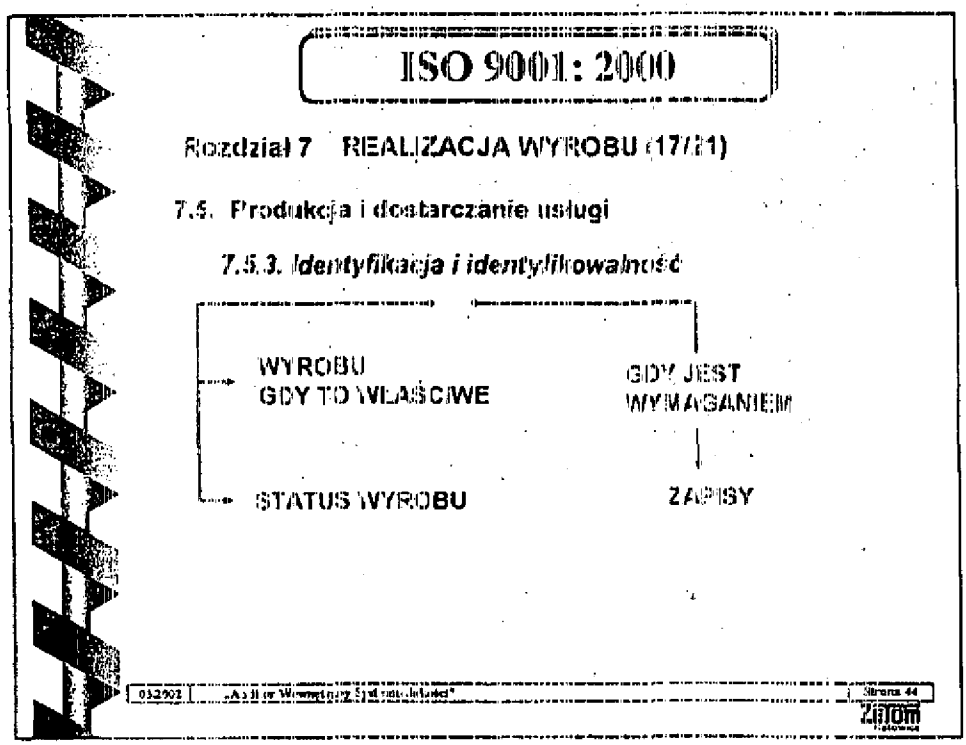

ISO 9001: 2000
Rozdział 7 REALIZACJA WYROBU (12/21)
7.4. Zakupy
7.4.1. Proces zakupu
DLA ZAPEWNIENIA ZGODNOŚCI Z WYMAGANIAMI
w sposób uzależniony od wpływu kupowanego wyrobu na późniejszą realizację lub wyrób finalny
PROWADZONY W STOSUNKU DO OCENIANYCH I WYBIERANYCH DOSTAWCÓW
NA PODSTAWIE KRYTERIÓW WYBORU, OCENY I PONOWNEJ OCENY
Wyniki dokumentowane
Strona 39
Zetom

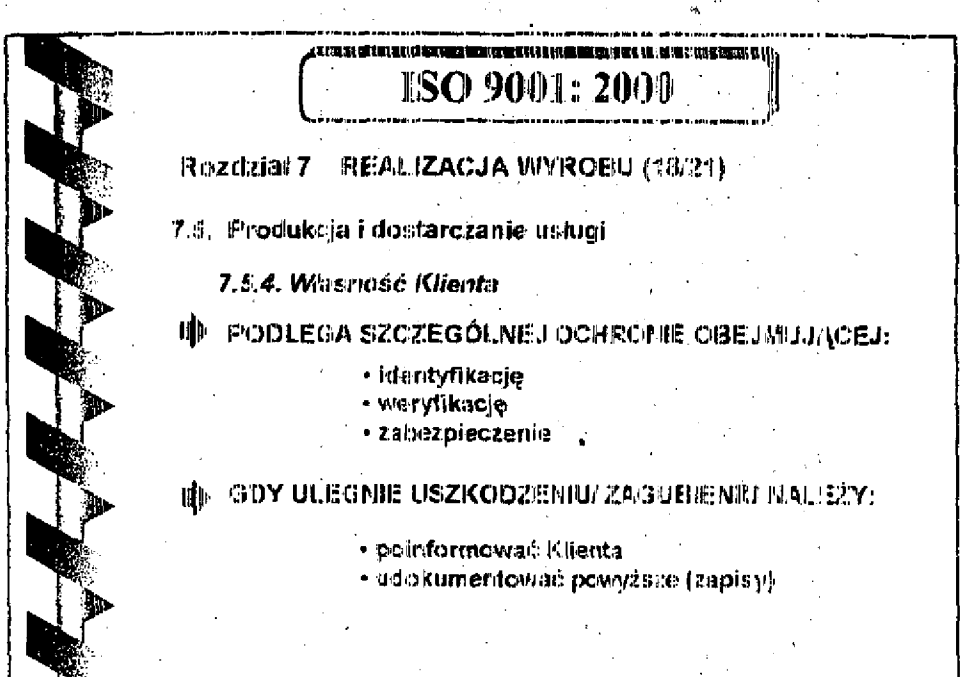

ISO 9001: 2000
Rozdział 7 REALIZACJA WYROBU (13/21)
7.4. Zakupy
7.4.2. Informacje dotyczące zakupów
OKREŚLAJĄ ZAKUPYWANY WYRÓB
ZAWIERAJĄ ODPOWIEDNIO:
wymagania dotyczące zatwierdzenia
• wyrobu
• procedur
• procesów
• wyposażenia
wymagania dot. kwalifikacji personelu
wymagania dot. Systemu Jakości
Strona 40
Zetom

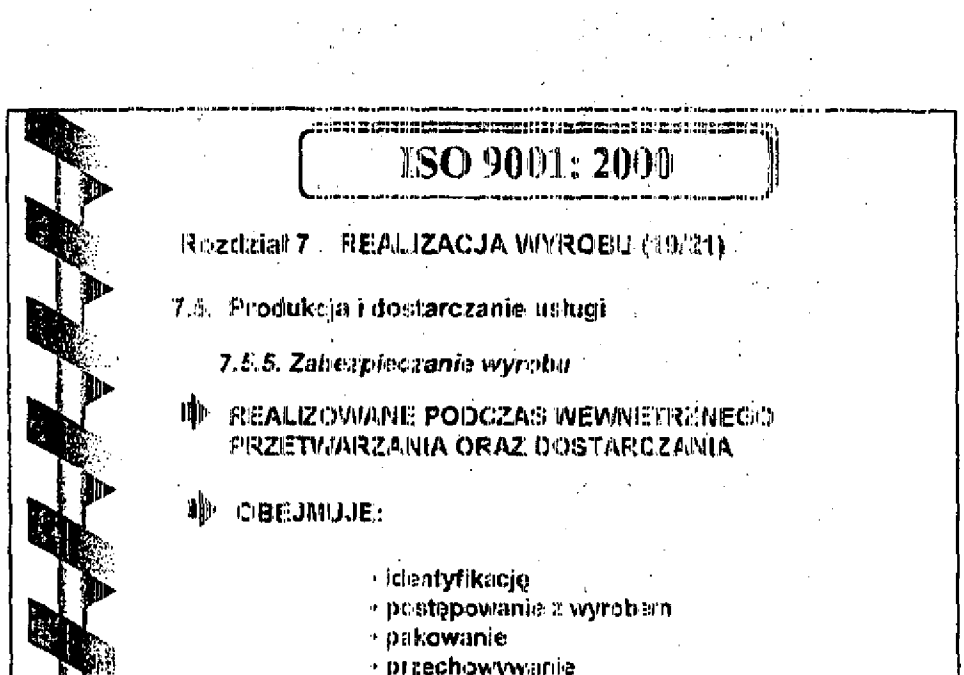

ISO 9001: 2000
Rozdział 7 REALIZACJA WYROBU (14/21)
7.4. Zakupy
7.4.3. Weryfikacja zakupionego wyrobu
OPARTA NA KONTROLI LUB INNYCH DZIAŁANIACH
MOŻLIWA NA TERENIE DOSTAWCY
Strona 41
Zetom

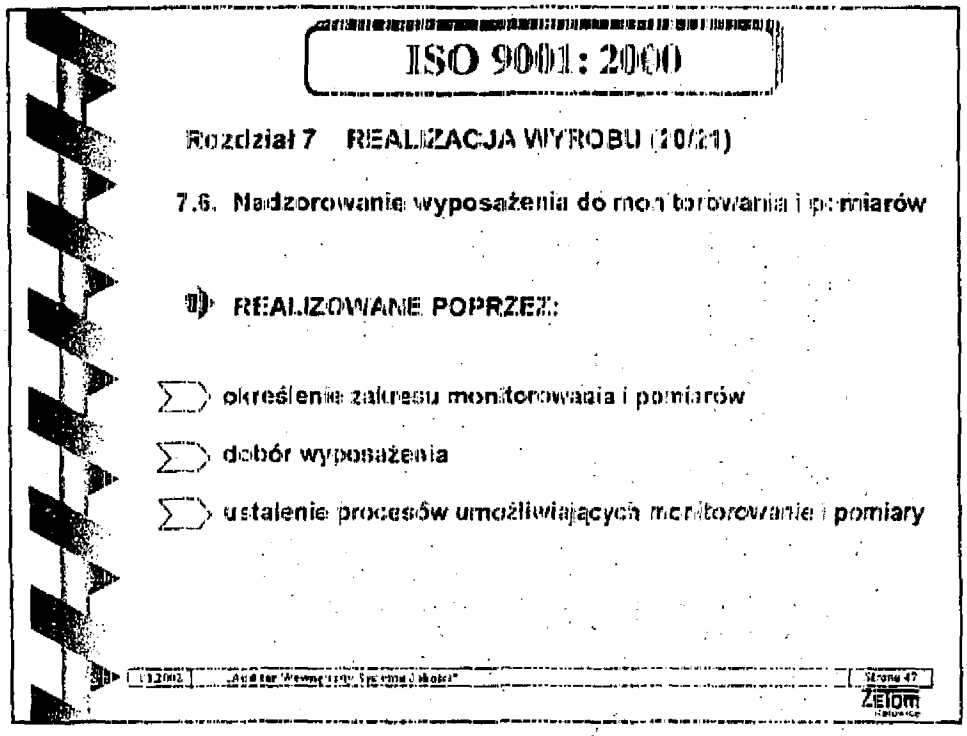

ISO 9001: 2000
Rozdział 7 REALIZACJA WYROBU (15/21)
7.5. Produkcja i dostarczanie usługi
7.5.1. Nadzorowanie produkcji i dostarczania usługi
OBEJMUJE ODPOWIEDNIO:
dostępność informacji o właściwościach wyrobu
dostępność instrukcji jeżeli są niezbędne
stosowanie właściwego wyposażenia, w tym do monitorowania i pomiarów
wdrożenie monitorowania i pomiarów i działań związanych ze zwolnieniem, dostawą i po dostawie
Strona 42
Zetom

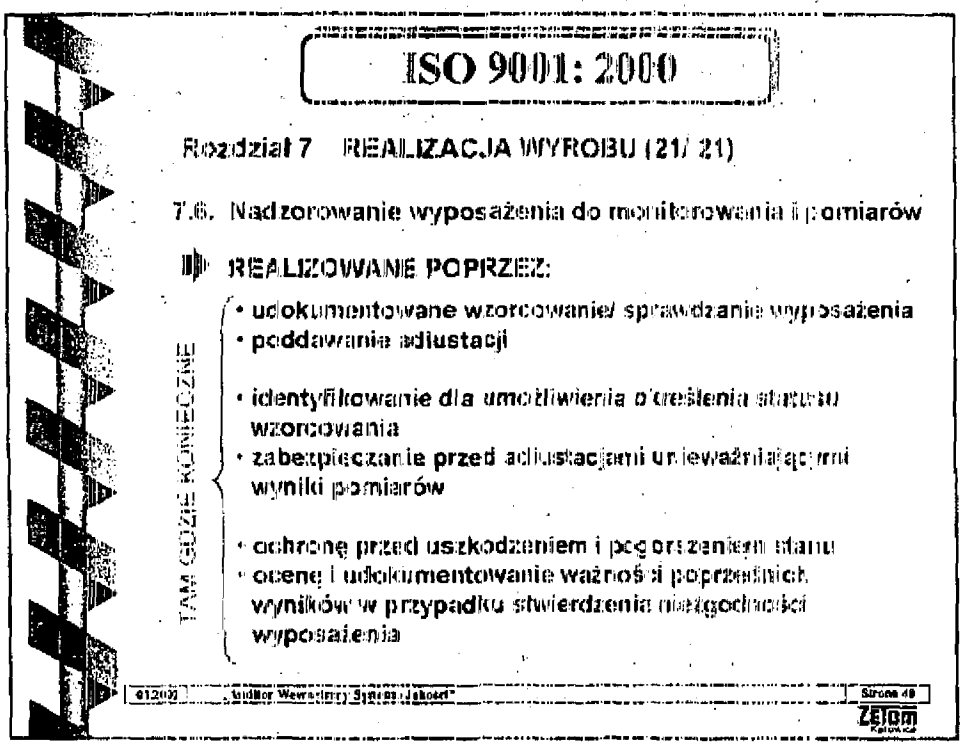

ISO 9001: 2000
Rozdział 7 REALIZACJA WYROBU (16/21)
7.5. Produkcja i dostarczanie usługi
7.5.2. Walidacja procesów produkcji i dostarczania usługi
PROWADZONA DLA PROCESÓW, CO DO KTÓRYCH NIEMOŻLIWA JEST WERYFIKACJA
DLA WYKAZNIA ZDOLNOŚCI PROCESÓW, KTÓRYCH NADZOROWANIE WINNO OBEJMOWAĆ
• ustalone kryteria przeglądu i zatwierdzania
• zatwierdzanie wyposażenia i kwalifikowanie personelu
• stosowanie określonych metod/ procedur
• prowadzenie zapisów
• ponowną walidację

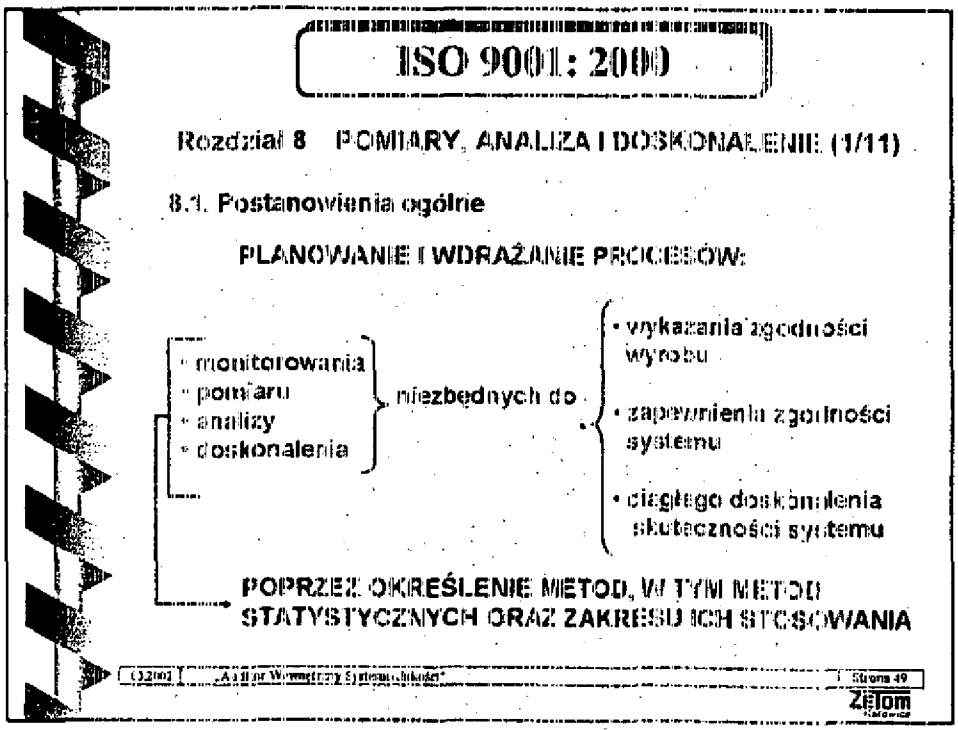

ISO 9001: 2000
Rozdział 7 REALIZACJA WYROBU (17/21)
7.5. Produkcja i dostarczanie usługi
7.5.3. Identyfikacja i identyfikowalność
WYROBU
GDY TO WŁAŚCIWE
GDY JEST WYMAGANIEM
STATUS WYROBU
ZAPISY

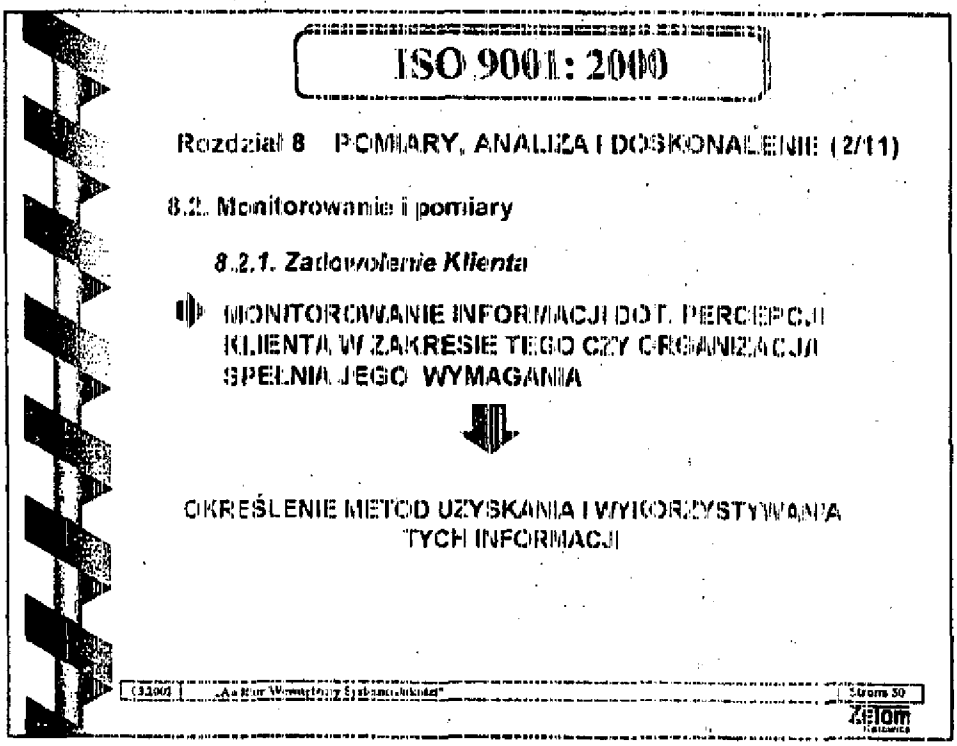

ISO 9001: 2000
Rozdział 7 REALIZACJA WYROBU (16/21)
7.5. Produkcja i dostarczanie usługi
7.5.4. Własność Klienta
PODLEGA SZCZEGÓLNEJ OCHRONIE OBEJMUJĄCEJ:
• identyfikację
• weryfikację
• zabezpieczenie
GDY ULEGNIE USZKODZENIU/ ZAGUBIENIU NALEŻY:
• poinformować Klienta
• udokumentować powyższe (zapisy)
Strona 45
Zetom

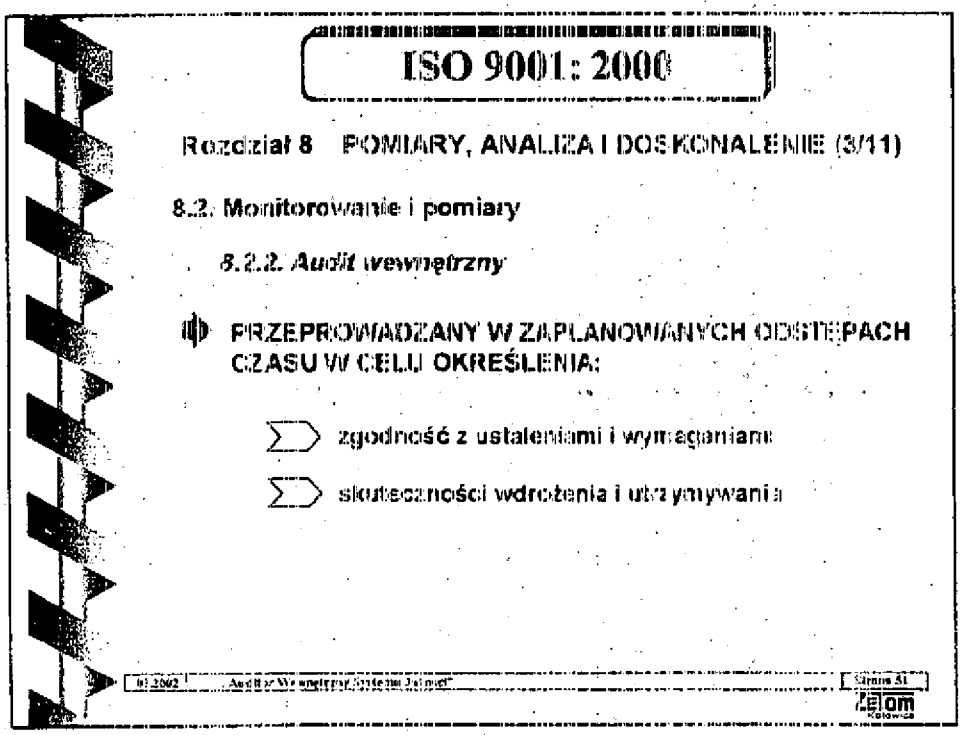

ISO 9001: 2000
Rozdział 7 REALIZACJA WYROBU (16/21)
7.5. Produkcja i dostarczanie usługi
7.5.5. Zabezpieczanie wyrobu
REALIZOWANE PODCZAS WEWNĘTRZNEGO PRZETWARZANIA ORAZ DOSTARCZANIA
OBEJMUJE:
• identyfikację
• postępowanie z wyrobem
• pakowanie
• przechowywanie
• ochronę
Strona 46
Zetom

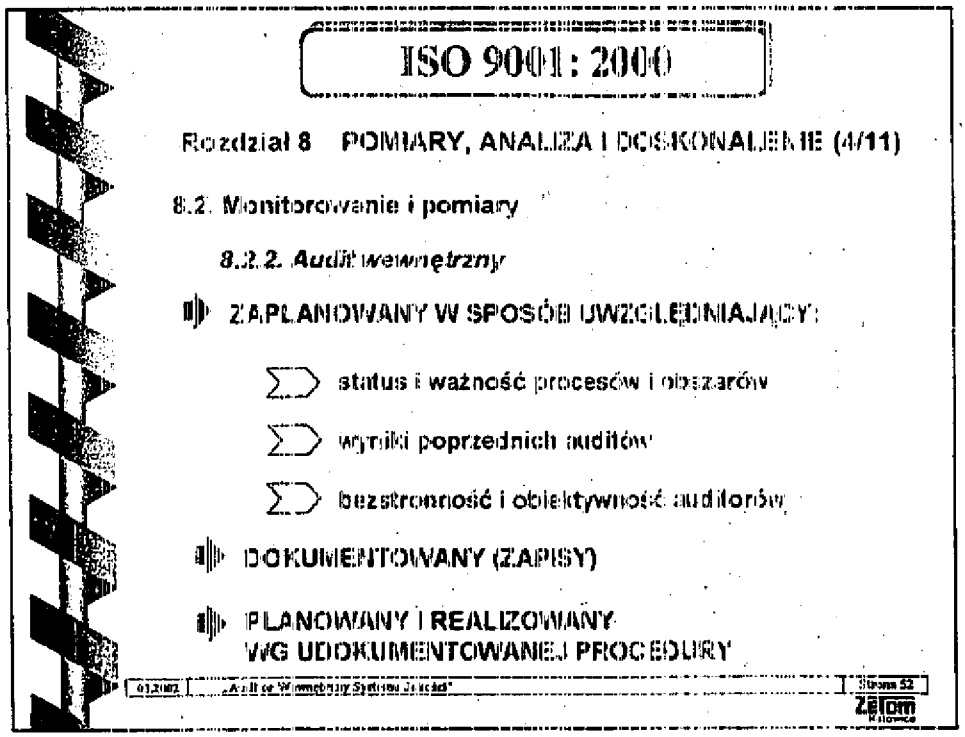

ISO 9001: 2000
Rozdział 7 REALIZACJA WYROBU (20/21)
7.6. Nadzorowanie wyposażenia do monitorowania i pomiarów
REALIZOWANIE POPRZEZ:
określenie zakresu monitorowania i pomiarów
dobór wyposażenia
ustalenie procesów umożliwiających monitorowanie i pomiary
Strona 47
Zetom

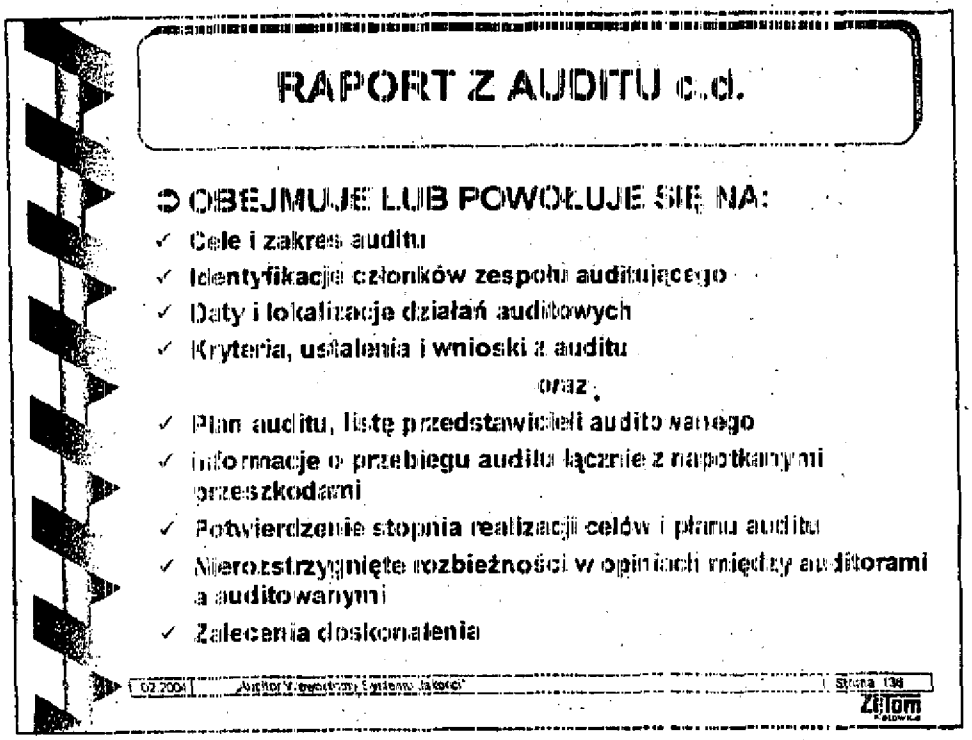

ISO 9001: 2000
Rozdział 7 REALIZACJA WYROBU (21/ 21)
7.6. Nadzorowanie wyposażenia do monitorowania i pomiarów
REALIZOWANIE POPRZEZ:
TAM GDZIE KONIECZNE
• udokumentowane wzorcowanie/ sprawdzanie wyposażenia
• poddawanie adiustacji
• identyfikowanie dla umożliwienia określenia statusu wzorcowania
• zabezpieczanie przed adiustacjami unieważniającymi wyniki pomiarów
• ochronę przed uszkodzeniem i pogorszeniem stanu
• ocenę i udokumentowanie ważności poprzednich wyników w przypadku stwierdzenia niezgodności wyposażenia
Strona 48
Zetom

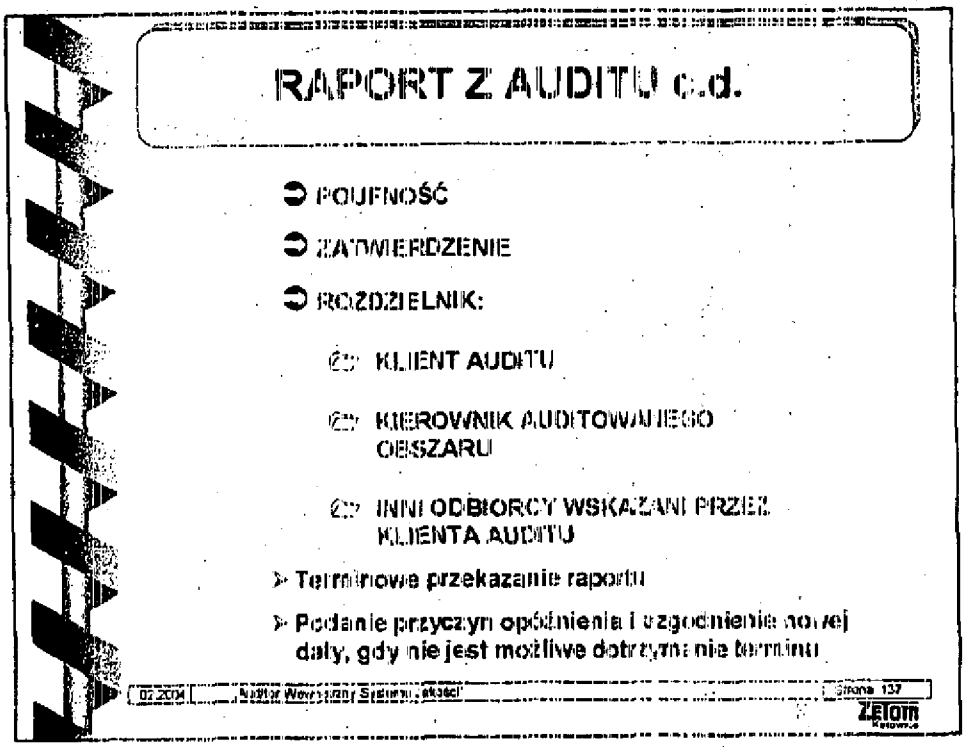

ISO 9001: 2000
Rozdział 8 POMIARY, ANALIZA I DOSKONALENIE (1/11)
8.1. Postanowienia ogólne
PLANOWANIE I WDRAŻANIE PROCESÓW:
• monitorowania
• pomiaru
• analizy
• doskonalenia
niezbędnych do
• wykazania zgodności wyrobu
• zapewnienia zgodności systemu
• ciągłego doskonalenia skuteczności systemu
POPRZEZ OKREŚLENIE METOD, W TYM METOD STATYSTYCZNYCH ORAZ ZAKRESU ICH STOSOWANIA
Strona 49

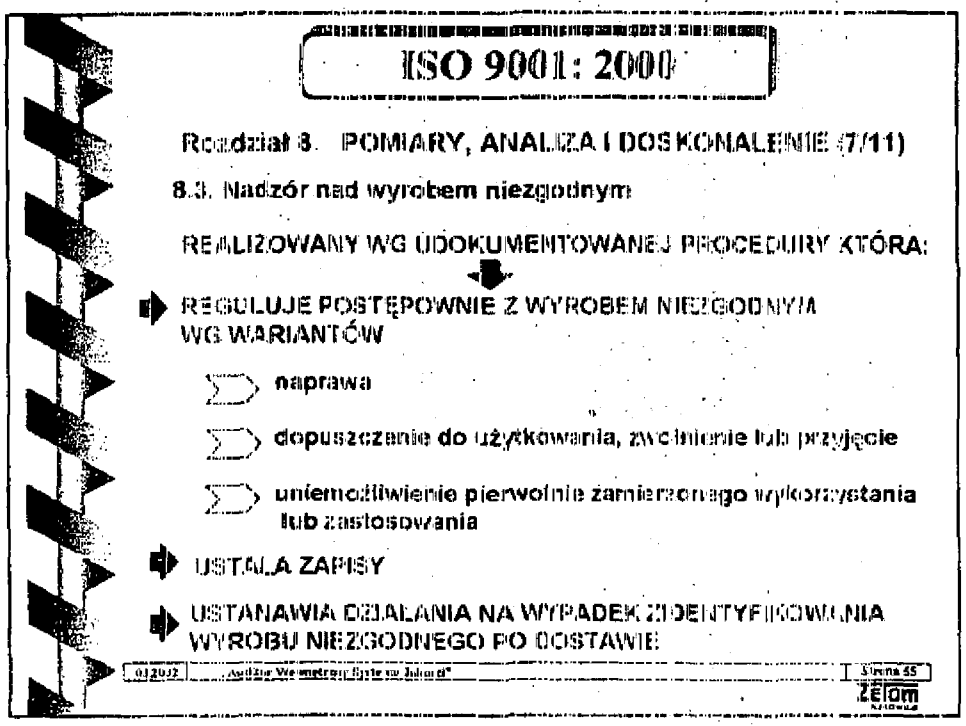

ISO 9001: 2000
Rozdział 8 POMIARY, ANALIZA I DOSKONALENIE (2/11)
8.2. Monitorowanie i pomiary
8.2.1. Zadowolenie Klienta
MONITOROWANIE INFORMACJI DOT. PERCEPCJI KLIENTA W ZAKRESIE TEGO CZY ORGANIZACJA SPEŁNIA JEGO WYMAGANIA
OKREŚLENIE METOD UZYSKANIA I WYKORZYSTYWANIA TYCH INFORMACJI
Strona 50

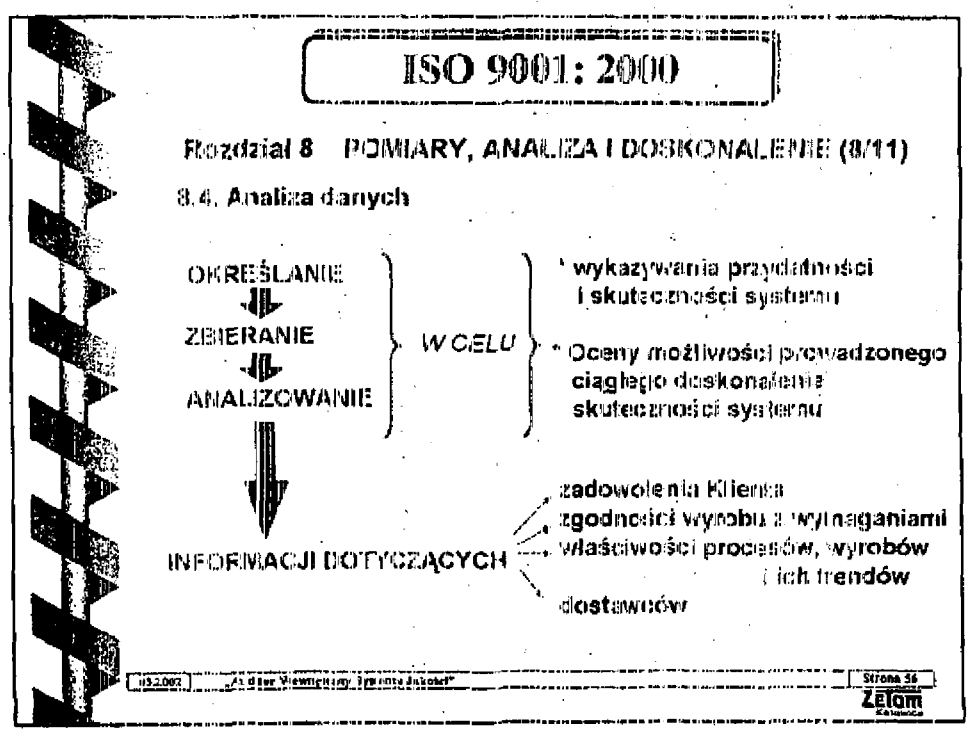

ISO 9001: 2000
Rozdział 8 POMIARY, ANALIZA I DOSKONALENIE (3/11)
8.2. Monitorowanie i pomiary
8.2.2. Audit wewnętrzny
PRZEPROWADZANY W ZAPLANOWANYCH ODSTĘPACH CZASU W CELU OKREŚLENIA:
zgodność z ustaleniami i wymaganiami
skuteczności wdrożenia i utrzymywania

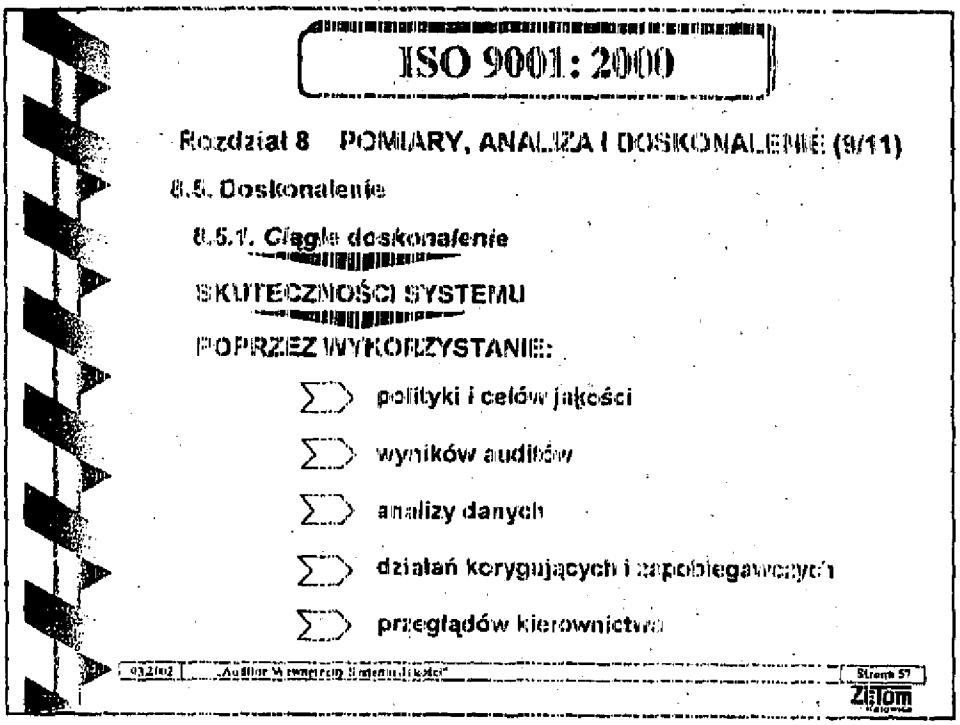

ISO 9001: 2000
Rozdział 8 POMIARY, ANALIZA I DOSKONALENIE (4/11)
8.2. Monitorowanie i pomiary
8.2.2. Audit wewnętrzny
ZAPLANOWANY W SPOSÓB UWZGLĘDNIAJĄCY:
status i ważność procesów i obszarów
wyniki poprzednich auditów
bezstronność i obiektywność auditorów
DOKUMENTOWANY (ZAPISY)
PLANOWANY I REALIZOWANY WG UDOKUMENTOWANEJ PROCEDURY

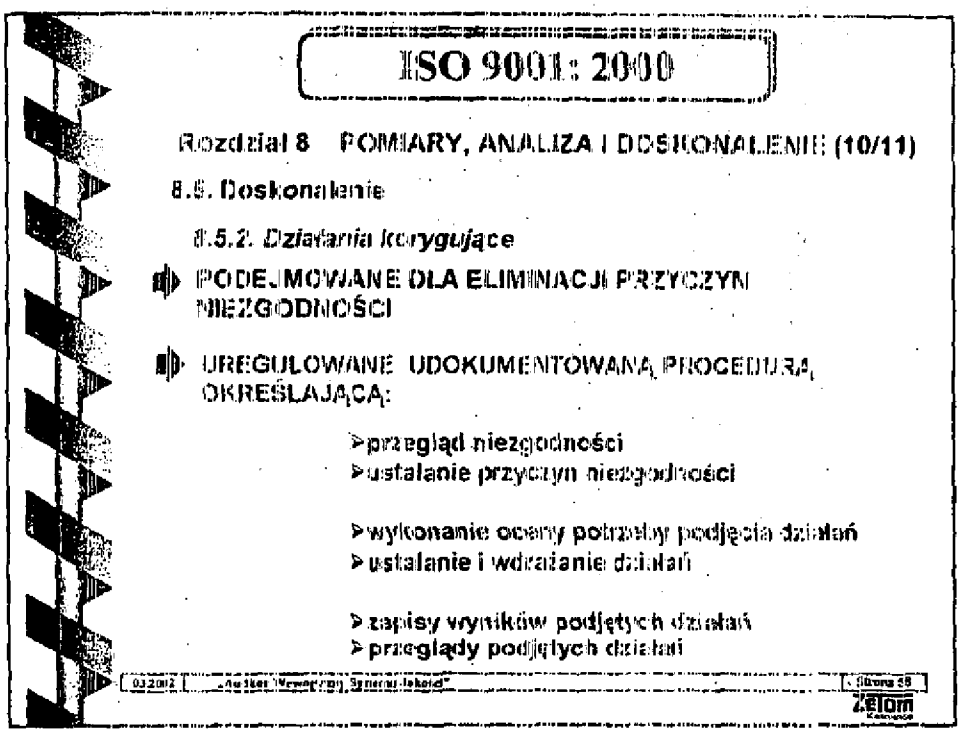

RAPORT Z AUDITU c.d.
OBEJMUJE LUB POWOŁUJE SIĘ NA:
Cele i zakres auditu
Identyfikacje członków zespołu auditującego
Daty i lokalizacje działań auditowych
Kryteria, ustalenia i wnioski z auditu
oraz:
Plan auditu, listę przedstawicieli auditowanego
Informacje o przebiegu auditu łącznie z napotkanymi przeszkodami
Potwierdzenie stopnia realizacji celów i planu auditu
Nierozstrzygnięte rozbieżności w opiniach między auditorami a auditowanymi
Zalecenia doskonalenia
02.2004
Strona 136
Zetom


RAPORT Z AUDITU c.d.
POUFNOŚĆ
ZATWIERDZENIE
ROZDZIELNIK:
KLIENT AUDITU
KIEROWNIK AUDITOWANEGO OBSZARU
INNI ODBIORCY WSKAZANI PRZEZ KLIENTA AUDITU
Terminowe przekazanie raportu
Podanie przyczyn opóźnienia i uzgodnienie nowej daty, gdy nie jest możliwe dotrzymanie terminu
02.2004
Strona 137
Zetom


ISO 9001: 2000
Rozdział 8. POMIARY, ANALIZA I DOSKONALENIE (7/11)
8.3. Nadzór nad wyrobem niezgodnym
REALIZOWANY WG UDOKUMENTOWANEJ PROCEDURY KTÓRA:
REGULUJE POSTĘPOWNIE Z WYROBEM NIEZGODNYM WG WARIANTÓW
naprawa
dopuszczanie do użytkowania, zwolnienie lub przyjęcie
uniemożliwienie pierwotnie zamierzonego wykorzystania lub zastosowania
USTALA ZAPISY
USTANAWIA DZIAŁANIA NA WYPADEK ZIDENTYFIKOWANIA WYROBU NIEZGODNEGO PO DOSTAWIE
Strona 55
Zelom


ISO 9001: 2000
Rozdział 8 POMIARY, ANALIZA I DOSKONALENIE (8/11)
8.4. Analiza danych
OKREŚLANIE
ZBIERANIE
ANALIZOWANIE
W CELU
wykazywania przydatności i skuteczności systemu
Oceny możliwości prowadzonego ciągłego doskonalenia skuteczności systemu
INFORMACJI DOTYCZĄCYCH
zadowolenia Klienta
zgodności wyrobu z wymaganiami
właściwości procesów, wyrobów i ich trendów
dostawców
Strona 56
Zelom


ISO 9001: 2000
Rozdział 8 POMIARY, ANALIZA I DOSKONALENIE (9/11)
8.5. Doskonalenie
8.5.1. Ciągłe doskonalenie
SKUTECZNOŚCI SYSTEMU
POPRZEZ WYKORZYSTANIE:
polityki i celów jakości
wyników audytów
analizy danych
działań korygujących i zapobiegawczych
przeglądów kierownictwa
Strona 57
Zetom


ISO 9001: 2000
Rozdział 8 POMIARY, ANALIZA I DOSKONALENIE (10/11)
8.5. Doskonalenie
8.5.2. Działania korygujące
PODEJMOWANE DLA ELIMINACJI PRZYCZYN NIEZGODNOŚCI
UREGULOWANE UDOKUMENTOWANĄ PROCEDURĄ, OKREŚLAJĄCĄ:
przegląd niezgodności
ustalanie przyczyn niezgodności
wykonanie oceny potrzeby podjęcia działań
ustalanie i wdrażanie działań
zapisy wyników podjętych działań
przeglądy podjętych działań
Zetom

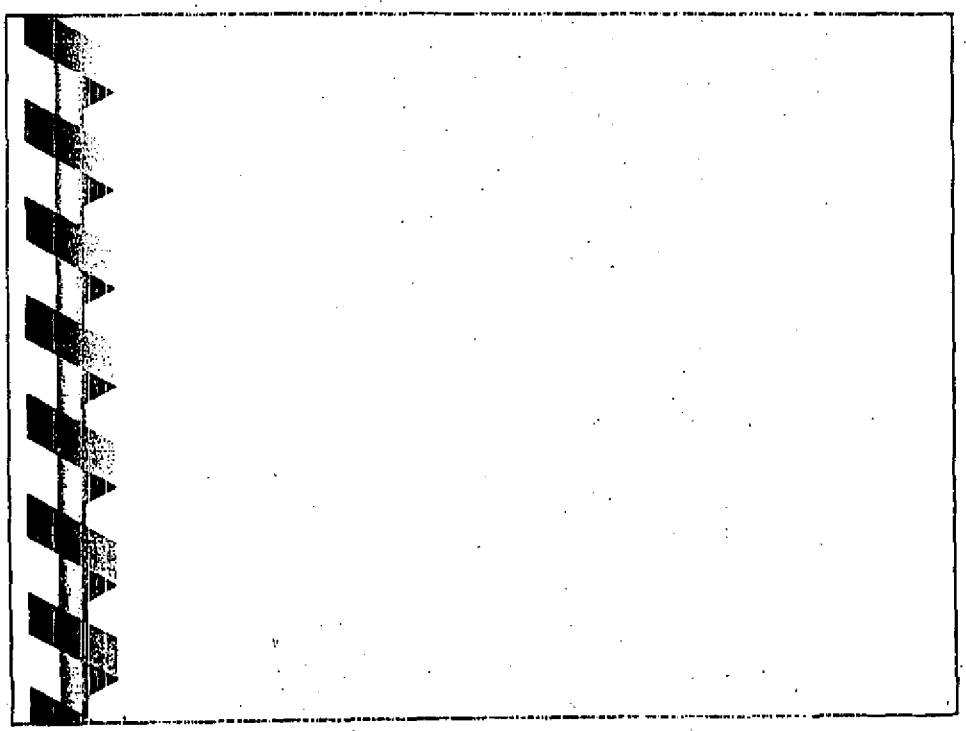
ISO 9001: 2000

Rozdział 8 POMIARY, ANALIZA I DOSKONALENIE (11/ 11)

8.5. Doskonalenie

8.5.3. *Działania zapobiegawcze*

- PODEJMOWANE DLA ELIMINACJI PRZYCZYN POTENCJALNYCH NIEZGODNOŚCI
- UREGULOWANE UDOKUMENTOWANĄ PROCEDURĄ OKREŚLAJĄCĄ:
  - ustalenie potencjalnych niezgodności i ich przyczyn
  - wykonanie oceny potrzeby podjęcia działań
  - ustalanie i wdrażanie podjętych działań
  - zapisy wyników podjętych działań
  - przeglądy podjętych działań

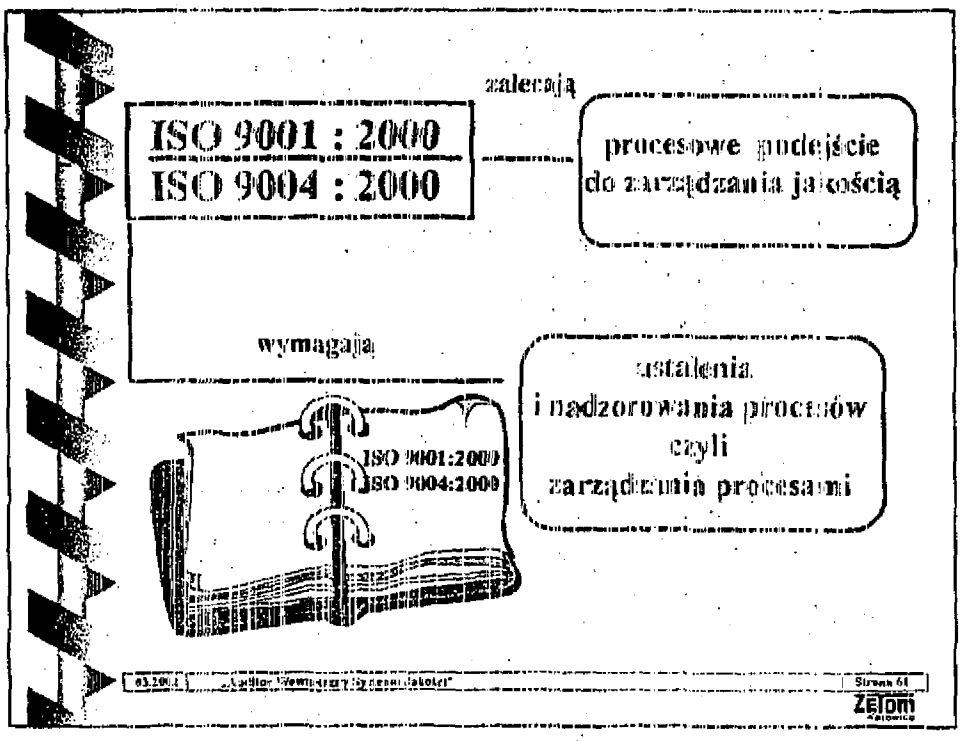


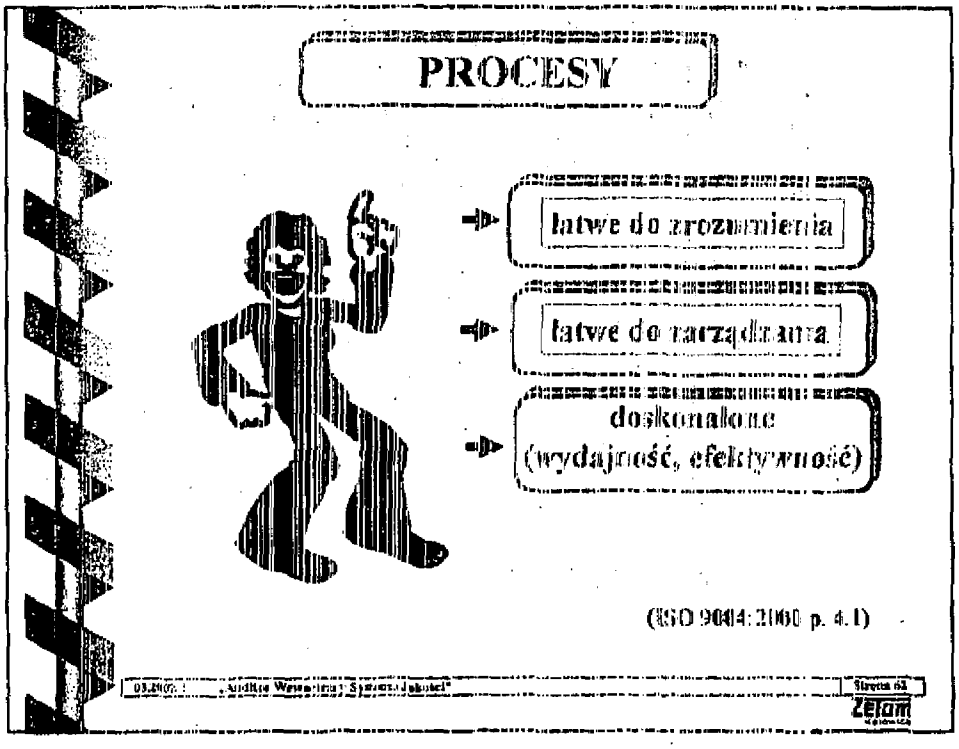
CZĘŚĆ II
ZARZĄDZANIE PROCESAMI W ASPEKCIE AUDITOWANIA

CZĘŚĆ II

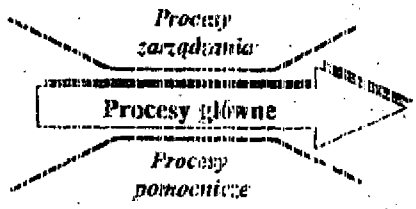
PODSTAWOWE ZASADY PODEJŚCIA PROCESOWEGO

1. Celem organizacji jest tworzenie wartości dla klienta.
2. Wartości dla klienta tworzona jest w procesach.
3. Sukces organizacji zależy od jej procesów.
4. Zaprojektowane procesy, zespoły wykonawców, środowisko pracy – wymagania dla zapewnienia funkcjonowania procesów


ISO 9001 : 2000
ISO 9004 : 2000
zalecają
procesowe podejście
do zarządzania jakością
wymagają
ustalenia
i nadzorowania procesów
czyli
zarządzania procesami
ISO 9001:2000
ISO 9004:2000

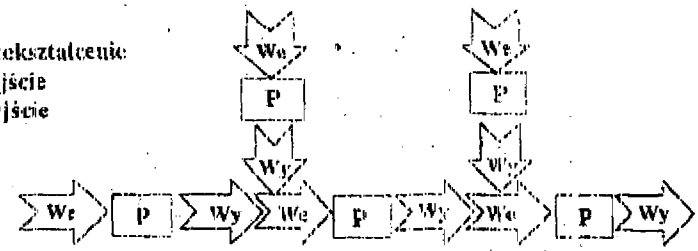

PROCESY
łatwe do zrozumienia
łatwe do zarządzania
doskonałone
(wydajność, efektywność)
(ISO 9004:2000 p. 4.1)

RODZAJE PROCESÓW



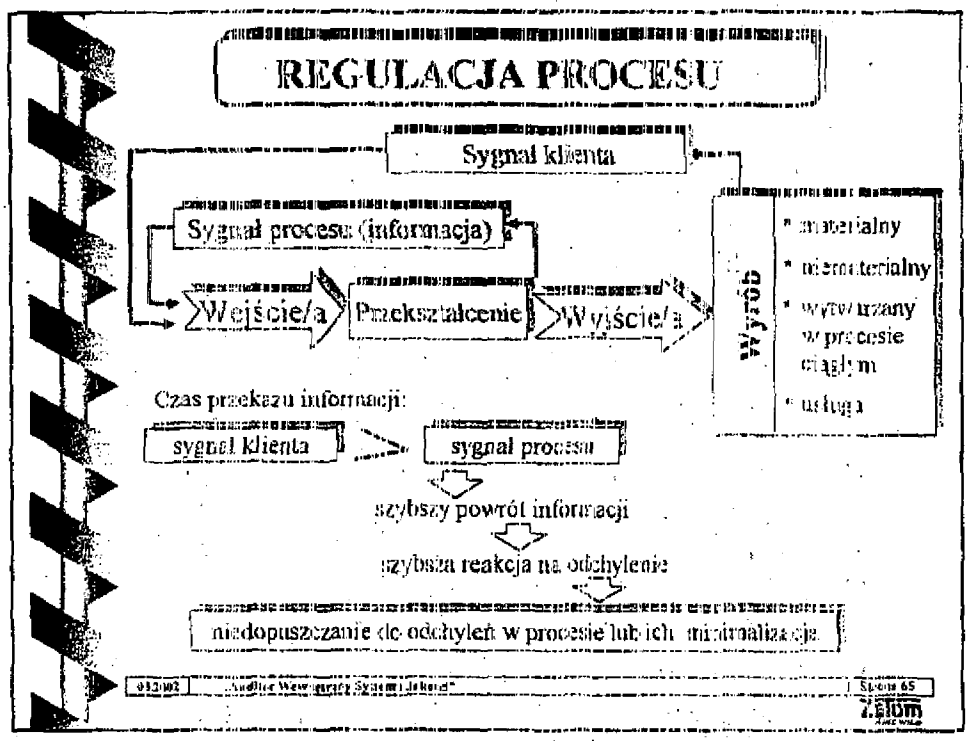
PROCESY SĄ ZAZWYCZAJ POWIĄZANE TWORZĄC ŁAŃCUCH PROCESÓW

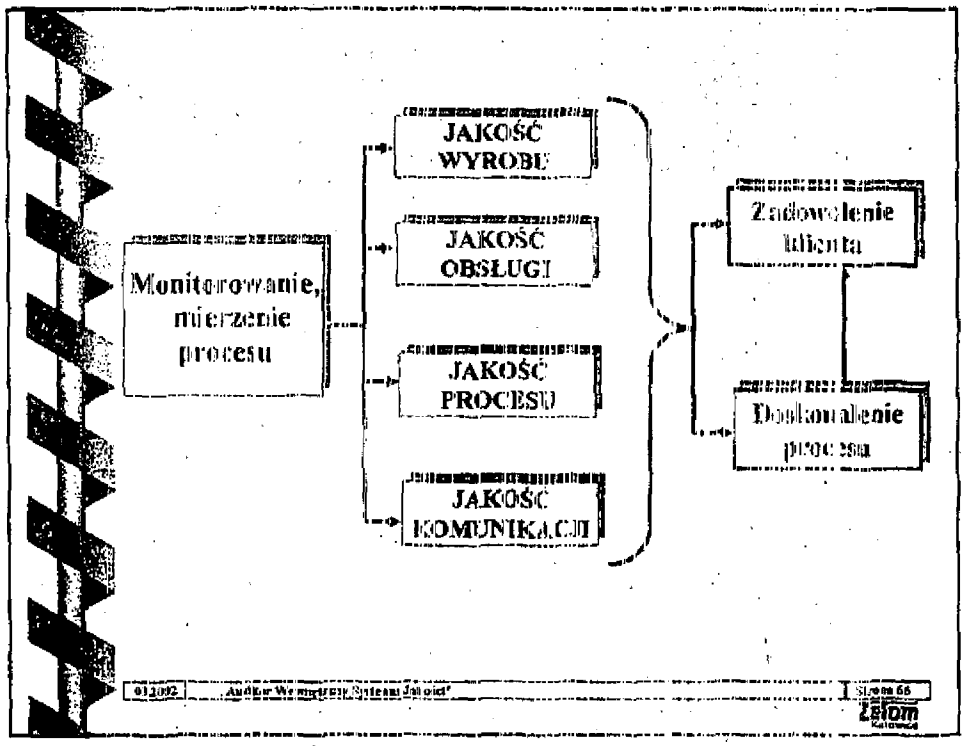
P - przekształcenie
We - wejście
Wy - wyjście



IDENTYFIKOWANIE PROCESU

- *Cele do osiągnięcia*
- *Klienci i dostawcy*
- *Początek i koniec*
- *Dane wejściowe i wyjściowe*
- *Właściciel*
- *Realizowane czynności*


REGULACJA PROCESU
Sygnał klienta
Sygnał procesu (informacja)
Wejście/a
Przekształcenie
Wyjście/a
Wyrób
* niematerialny
* niematerialny
* wytwarzany w procesie ciągłym
* usługa
Czas przekazu informacji:
sygnał klienta
sygnał procesu
szybszy powrót informacji
szybsza reakcja na odchylenie
niedopuszczanie do odchyleń w procesie lub ich minimalizacja


Monitorowanie, mierzenie procesu
JAKOŚĆ WYROBU
JAKOŚĆ OBSŁUGI
JAKOŚĆ PROCESU
JAKOŚĆ KOMUNIKACJI
Zadowolenie klienta
Doskonalenie procesu

POMIARY I MONITOROWANIE PROCESÓW WG ISO 9004:2000

DOTYCZY:

- zdolności
- czasu reakcji
- czasu cyklu lub przepustowości
- mierzalnych aspektów niezawodności
- wydajności
- efektywności i skuteczności pracowników organizacji
- wykorzystania technologii
- redukcji odpadów
- alokacji i redukcji kosztów

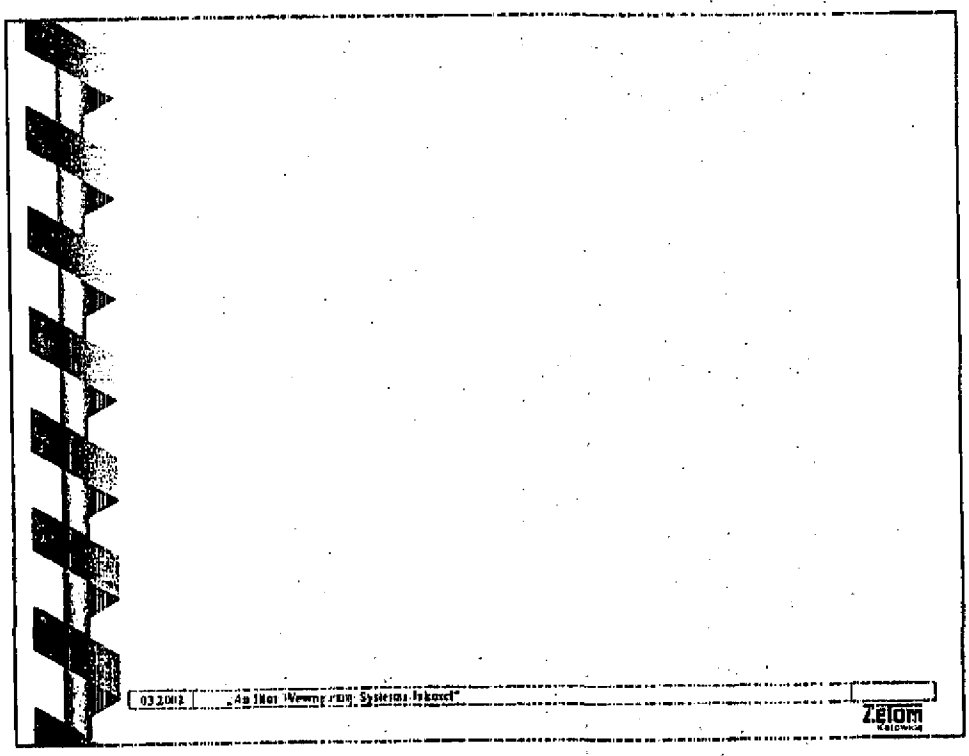
WSKAŹNIKI

BAZA DLA WYZNACZANIA / MIERZENIA CELÓW czyli: ULEPSZANIA

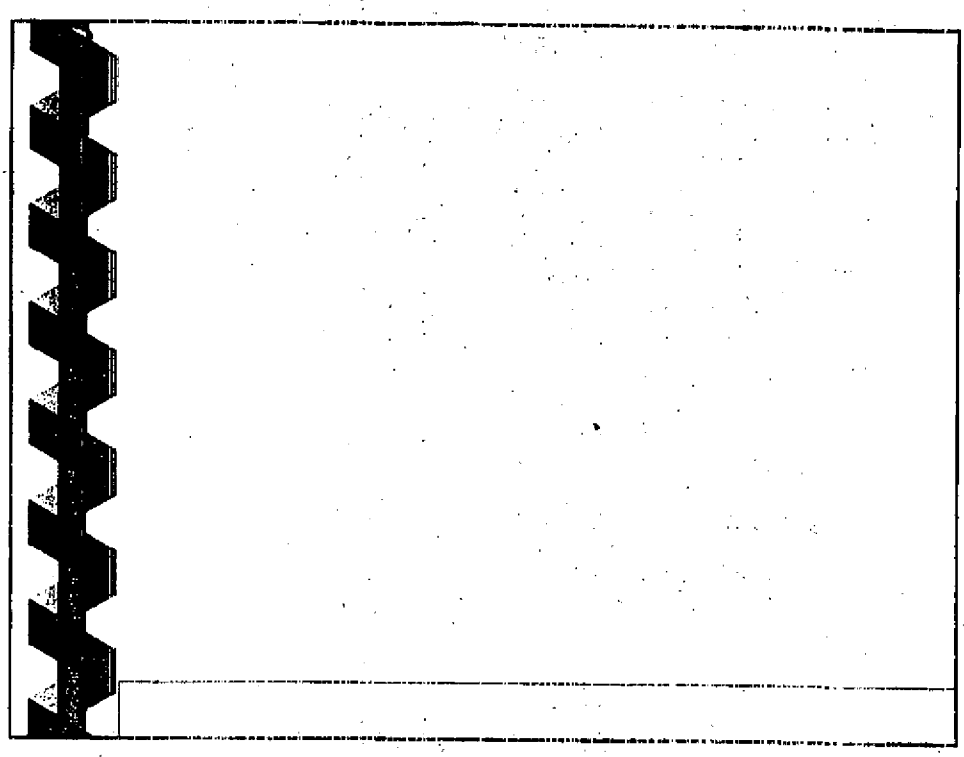
SYSTEMOWEGO PROGNOZOWANIA I OCENY WYNIKÓW ORGANIZACJI

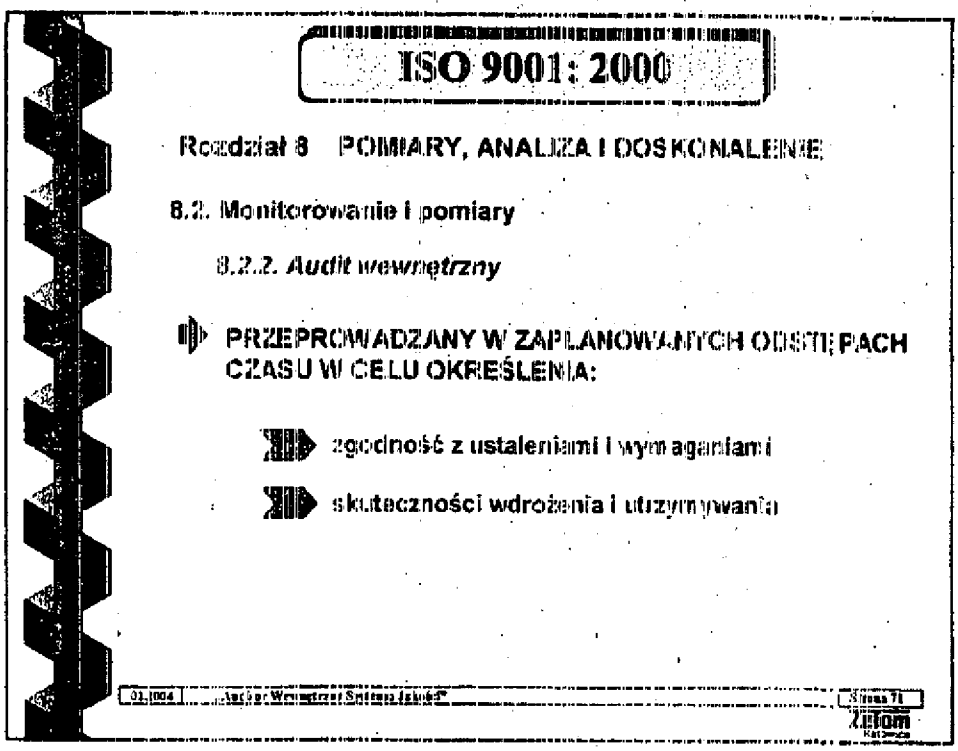
ZALETY SYSTEMU WSKAŹNIKÓW

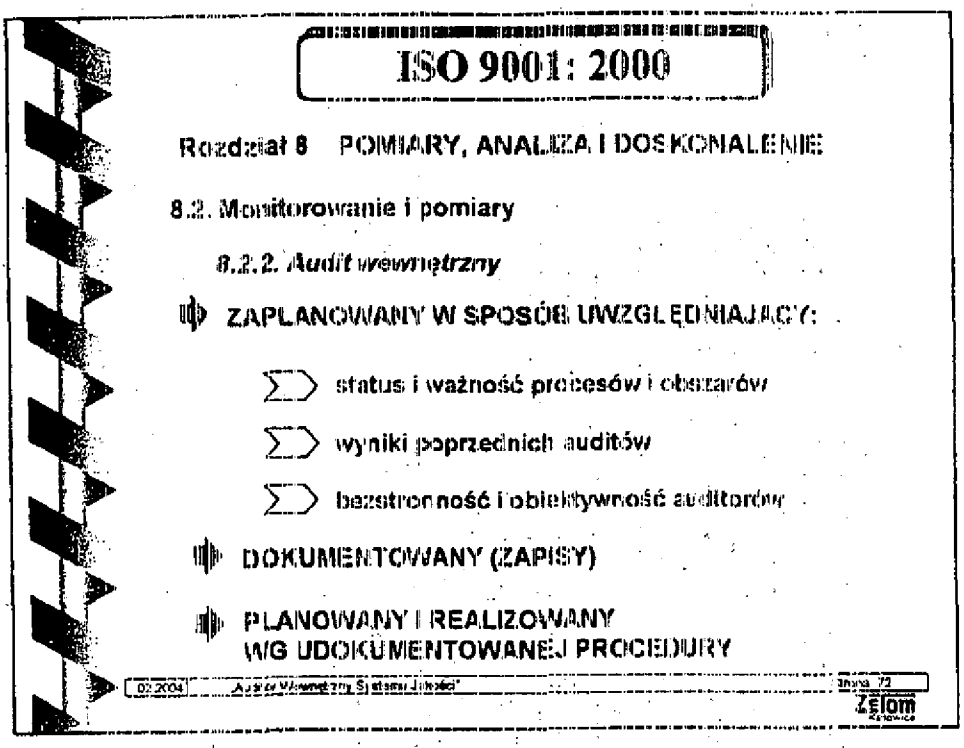
- są oparte na rzeczywistych danych
- szybka możliwość zareagowania
- obserwowanie trendów
- gwarancja rozpoznania efektów procesu
- kaskadowe powiązanie z wizją, misją i polityką
- koncentracja na najważniejszych parametrach

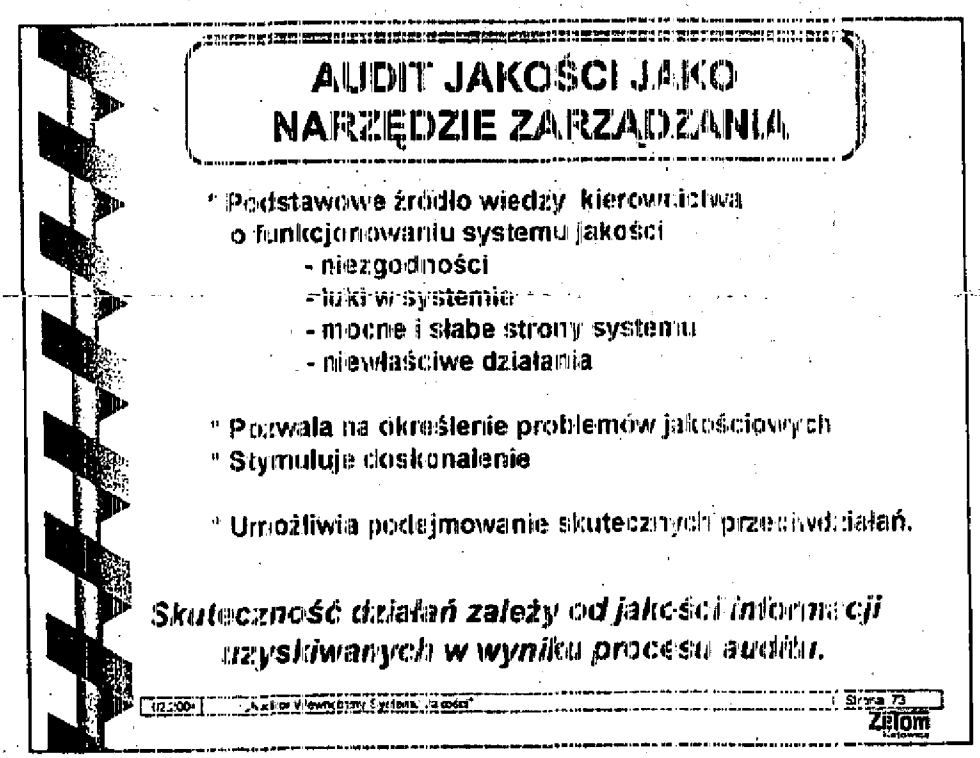


CZĘŚĆ III
AUDIT WEWNĘTRZNY




ISO 9001: 2000
Rozdział 8 POMIARY, ANALIZA I DOSKONALENIE
8.2. Monitorowanie i pomiary
8.2.2. Audit wewnętrzny
PRZEPROWADZANY W ZAPLANOWANYCH ODSTĘPACH CZASU W CELU OKREŚLENIA:
zgodność z ustaleniami i wymaganiami
skuteczności wdrożenia i utrzymywania


ISO 9001: 2000
Rozdział 8 POMIARY, ANALIZA I DOSKONALENIE
8.2. Monitorowanie i pomiary
8.2.2. Audit wewnętrzny
ZAPLANOWANY W SPOSÓB UWZGLĘDNIAJĄCY:
status i ważność procesów i obszarów
wyniki poprzednich auditów
bezstronność i obiektywność auditorów
DOKUMENTOWANY (ZAPISY)
PLANOWANY I REALIZOWANY
WG UDOKUMENTOWANEJ PROCEDURY
Zielom


AUDIT JAKOŚCI JAKO
NARZĘDZIE ZARZĄDZANIA
Podstawowe źródło wiedzy kierownictwa
o funkcjonowaniu systemu jakości
- niezgodności
- luki w systemie
- mocne i słabe strony systemu
- niewłaściwe działania
Pozwala na określenie problemów jakościowych
Stymuluje doskonalenie
Umożliwia podejmowanie skutecznych przeciwdziałań.
Skuteczność działań zależy od jakości informacji
uzyskiwanych w wyniku procesu auditu.
Zielom

NIEZGODNOŚCI

NIEZGODNOŚĆ – stan przeciwstawny jakości

pogwałcenie wymagań:

- ✓ normy systemu zarządzania jakością
- ✓ księgi jakości
- ✓ procedur / innych dokumentów systemu
- ✓ kontraktu, zewnętrznych przepisów prawnych
- ✓ innych przyjętych regulacji i ustaleń

OCENA SYSTEMU

na podstawie
LISTY NIEZGODNOŚCI

niezgodności/ spostrzeżeń dot. *planowania*

niezgodności/ spostrzeżeń dot. *wdrażania*

niezgodności/ spostrzeżeń dot. *skuteczności*

niezgodności w każdym obszarze

niezgodności względem poszczególnych elementów normy systemu

identyfikacja słabych elementów systemu

ujawnienie obszaru/ procesu wymagającego poprawy

NIEZGODNOŚĆ:
NIESPEŁNIENIE USTALONYCH WYMAGAŃ

Występuje gdy:

- ✓ nie są spełnione wszystkie wymagania
- ✓ stan wymagany i rzeczywisty nie są zgodne

Jako niezgodność można potraktować tylko to, co rzeczywiście zostało stwierdzone, tzn. poparte obiektywnym dowodem/ami.

NIEZGODNOŚCI:

* przypadkowe
* systematyczne

AUDITOR NIE MOŻE:

- ➢ wyciągać żadnych uogólniających wniosków na podstawie pojedyńczych przypadków,
- ➢ wnosić żadnych dodatkowych osobistych lub domniemanych wymagań

W przypadkach wątpliwych poszerzenie próby wyrywkowej poprzez dodatkowe badanie tego samego elementu systemu jakości.

KATEGORIE NIEZGODNOŚCI

NIEZGODNOŚCI SYSTEMATYCZNE

- Wada w systemie np.
  - ✓ nie opisany / nie wdrożony element systemu
  - ✓ brak prowadzenia wymaganych przeglądów projektu
  - ✓ brak prowadzenia wymaganych zapisów
  - ✓ część wyposażenia pomiarowego nie jest wzorcowana
  - ✓ wytyczne do sprawdzania rysunków istnieją, ale nie są przestrzegane.

KATEGORIE NIEZGODNOŚCI

NIEZGODNOŚCI PRZYPADKOWE

- Odizolowany przypadek - nie spełnienie wymagań bez większych konsekwencji np.
  - ✓ brak identyfikacji statusu jednego aparatu pomiarowego
  - ✓ jeden pomiar nie zapisany
  - ✓ jedna paleta nie jest oznakowana zgodnie z instrukcją

Uwaga: kilka takich niezgodności w tym samym obszarze / procesie tworzy ryzyko wady systemu

OCENA NIEZGODNOŚCI

MAŁA (M)	2	niezgodność przypadkowa
DUŻA (D)	3	niezgodność systematyczna

należy sporządzić

PROTOKOŁY NIEZGODNOŚCI

Znaczenie niezgodności oraz jej skutków należy wyjaśnić:

- na miejscu badania
- podczas spotkania zamykającego

ZAPISY DOTYCZĄCE NIEZGODNOŚCI

- Dokładnie opisać fakty
  - co wykryto ?
  - gdzie to znaleziono ?
  - na jakiej podstawie ?
  - jakie są dowody ?
- Zaszeregować niezgodność wobec normy / księgi jakości / procedury/ innego dokumentu
- Określić kategorię niezgodności
- Stosować właściwą terminologię

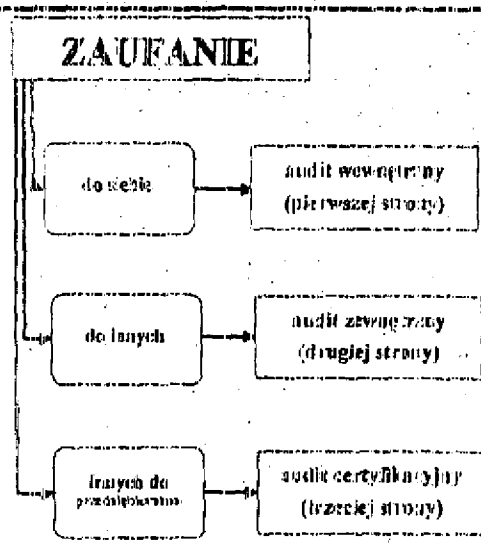
AUDIT JAKOŚCI wg ISO 9000:2000

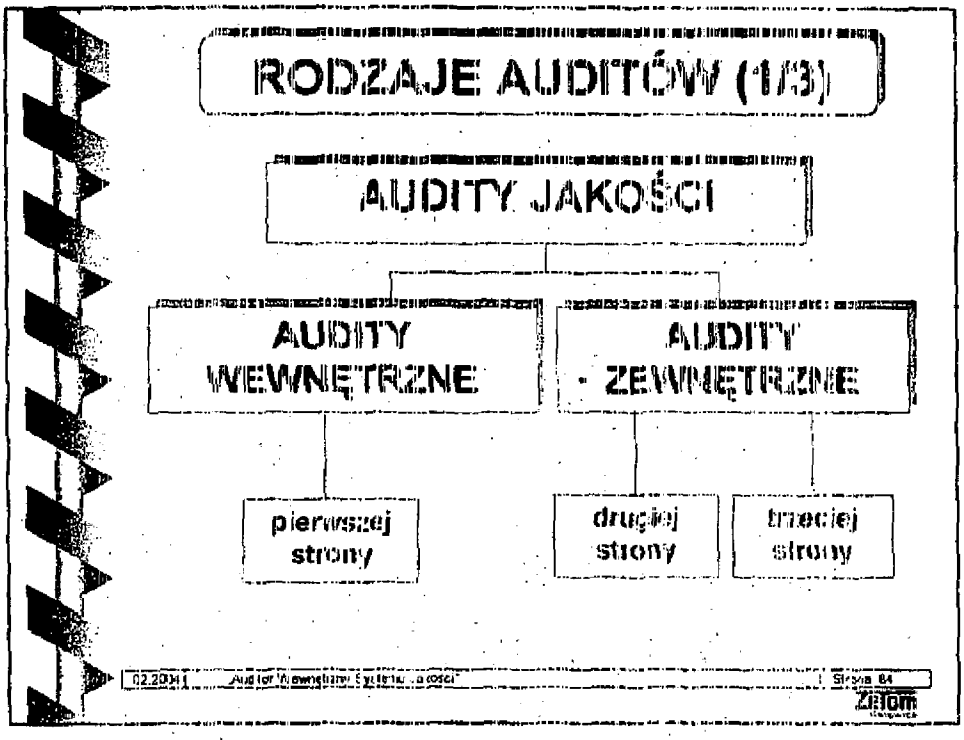
Systematyczny, niezależny i udokumentowany proces uzyskiwania dowodu z audytu oraz jego obiektywnej oceny w celu określenia stopnia spełnienia kryteriów audytu

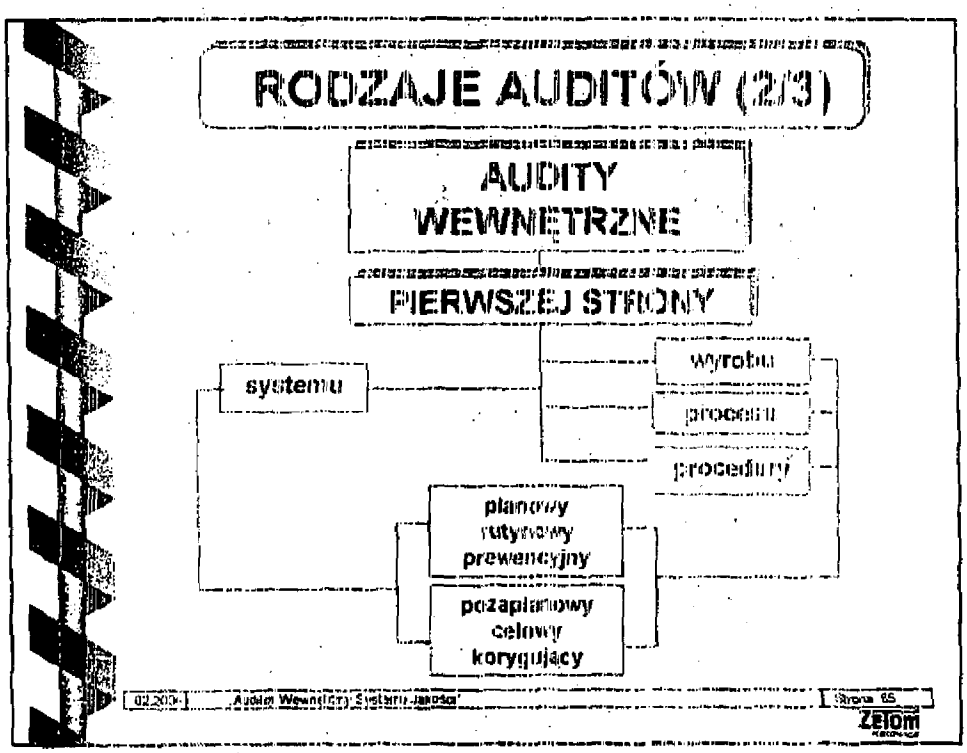
DOWÓD Z AUDITU – zapisy, stwierdzenia faktu lub inne informacje, które są istotne dla kryteriów auditu i możliwe do zweryfikowania

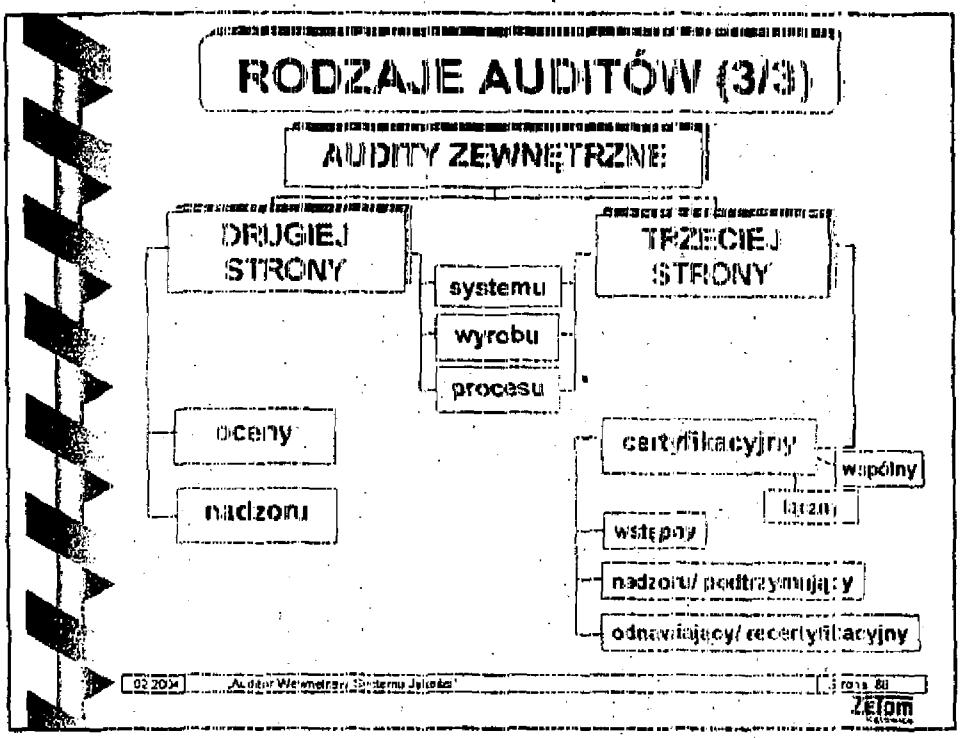
KRYTERIA AUDITU- zestaw polityk, procedur lub wymagań stosowanych jako odniesienie

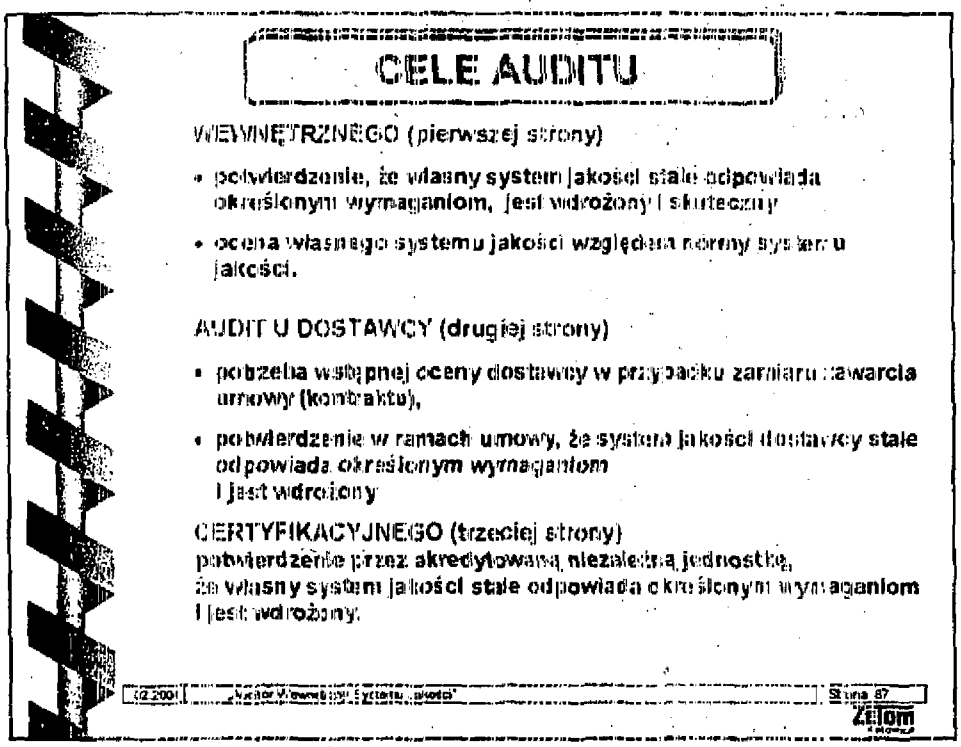
AUDIT NARZĘDZIEM POMIARU ZAUFANIA




RODZAJE AUDITÓW (1/3)
AUDITY JAKOŚCI
AUDITY WEWNĘTRZNE
AUDITY ZEWNĘTRZNE
pierwszej strony
drugiej strony
trzeciej strony


RODZAJE AUDITÓW (2/3)
AUDITY WEWNĘTRZNE
PIERWSZEJ STRONY
systemu
wyrobu
procesu
procedury
planowy
rutynowy
prewencyjny
pozaplanowy
celowy
korygujący


RODZAJE AUDITÓW (3/3)
AUDITY ZEWNĘTRZNE
DRUGIEJ STRONY
TRZECIEJ STRONY
systemu
wyrobu
procesu
oceny
nadzoru
certyfikacyjny
wspólny
wstępny
nadzoru/ podtrzymujący
odnawiający/ recertyfikacyjny


CELE AUDITU
WEWNĘTRZNEGO (pierwszej strony)
• potwierdzenie, że własny system jakości stale odpowiada określonym wymaganiom, jest wdrożony i skuteczny
• ocena własnego systemu jakości względem normy systemu jakości.
AUDIT U DOSTAWCY (drugiej strony)
• potrzeba wstępnej oceny dostawcy w przypadku zamiaru zawarcia umowy (kontraktu),
• potwierdzenie w ramach umowy, że system jakości dostawcy stale odpowiada określonym wymaganiom i jest wdrożony
CERTYFIKACYJNEGO (trzeciej strony)
potwierdzenie przez akredytowaną niezależną jednostkę, że własny system jakości stale odpowiada określonym wymaganiom i jest wdrożony.

AUDIT SYSTEMU JAKOŚCI

SYSTEMATYCZNA ANALIZA

- zgodności z kryteriami auditu
- skuteczności
- efektywność

WYBRANYCH ELEMENTÓW SYSTEMU JAKOŚCI

w całej organizacji lub w poszczególnych obszarach/ procesach

AUDIT SYSTEMU JAKOŚCI

DZIAŁALNOŚĆ FORMALNA

prowadzona na podstawie ustalonych kryteriów

- NORMY SYSTEMU ZARZĄDZANIA JAKOŚCIĄ
- KSIĘGI JAKOŚCI / POLITYKI JAKOŚCI
- PROCEDUR/ INSTRUKCJI/ INNYCH DOKUMENTÓW

w których organizacja określa jak będzie zajmować się jakością, poprzez

BEZSTRONNĄ ANALIZĘ OBIEKTYWNYCH DOWODÓW I WERYFIKACJĘ ZGODNOŚCI Z OKREŚLONYMI WYMAGANIAMI

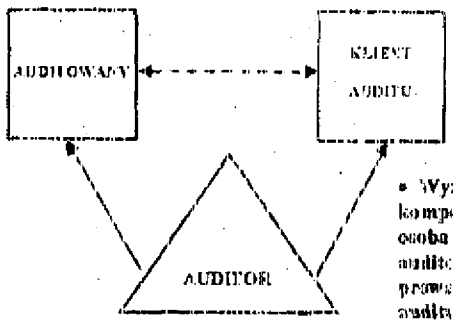
- AUDIT JEST PRÓBĄ LOSOWĄ

POWODY PROWADZENIA AUDITÓW WEWNĘTRZNYCH

- ☑ norma sytemu zarządzania jakością
- ☑ program auditów
- ☑ reklamacje klientów
- ☑ sygnały o wystąpieniu problemów
- ☑ zmiany w organizacji i zarządzaniu

PODZIAŁ RÓL W AUDICIE WEWNĘTRZNYM

- Organizacja lub osoba zlecająca wykonanie auditu
- Kierownictwo programowe auditów
- Szefowie komórek organizacyjnych
- Obszar systemu
- Organizacja auditowana



- Wyznaczona kompetentna osoba z listy auditorów do przeprowadzenia auditu

PN-EN ISO 19011:2003

„Wytyczne dotyczące auditowania systemów zarządzania jakością i/lub zarządzania środowiskowego"

TERMINY I DEFINICJE WG NORMY PN-EN ISO 19011

AUDIT – systematyczny, niezależny i udokumentowany proces uzyskiwania dowodu z auditu oraz jego obiektywnej oceny w celu określenia stopnia spełnienia *kryteriów auditu*

KRYTERIA AUDITU – zestaw polityk, procedur lub wymagań, kryteria są stosowane jako odniesienie, z którym porównuje się *dowody z auditu*

DOWODY Z AUDITU – zapisy, stwierdzenia faktu lub inne informacje, które są istotne ze względu na kryteria auditu *i możliwe do zweryfikowania*

TERMINY I DEFINICJE WG NORMY PN-EN ISO 19011

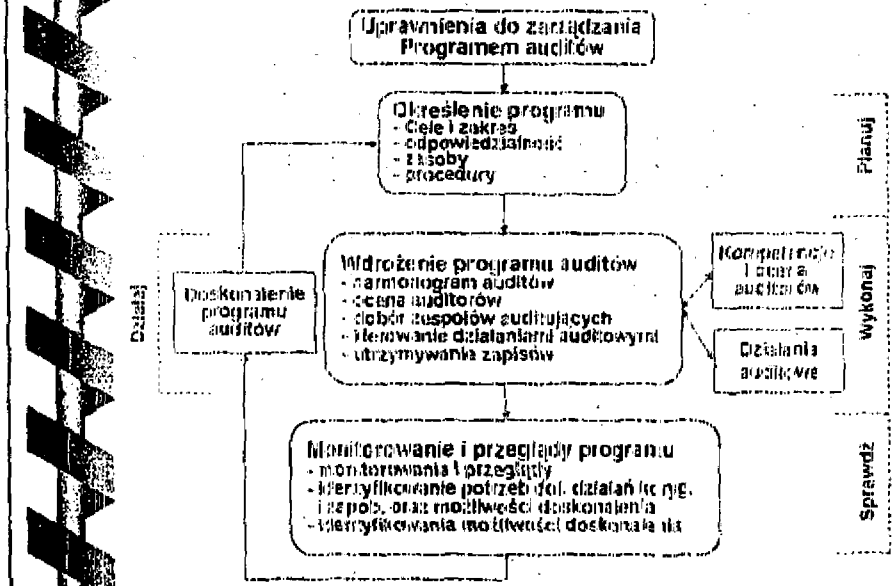
USTALENIA Z AUDITU – wyniki oceny zebranych dowodów z auditu w stosunku do *kryteriów auditu*

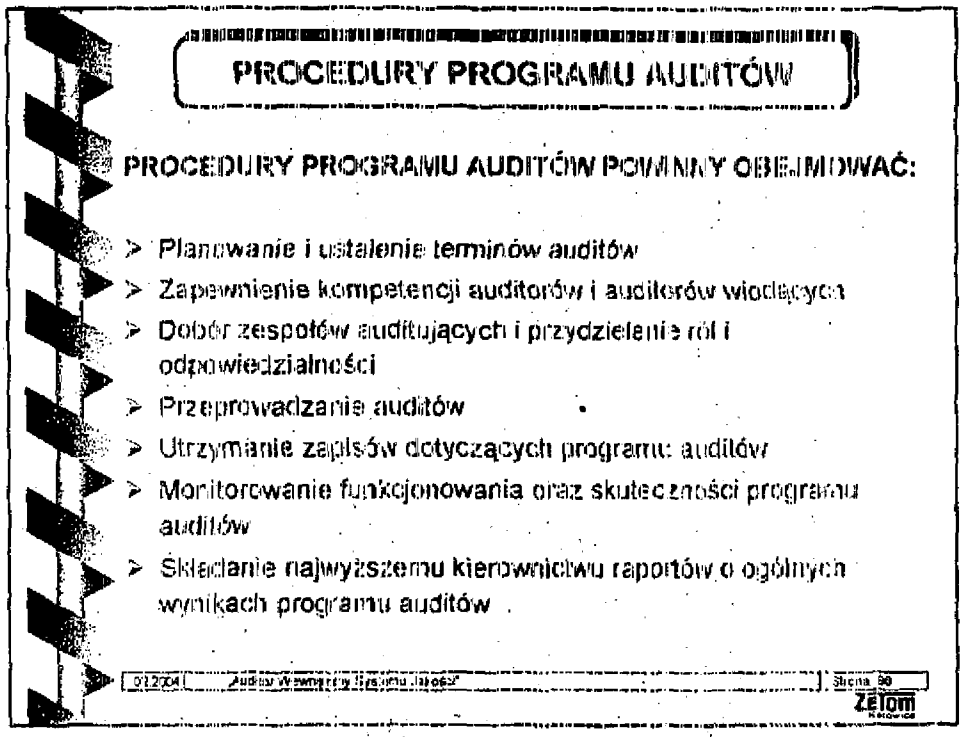
WNIOSEK Z AUDITU – *wynik auditu*, przedstawiony przez zespół auditujący po rozważeniu celów auditu i wszystkich ustaleń z auditu

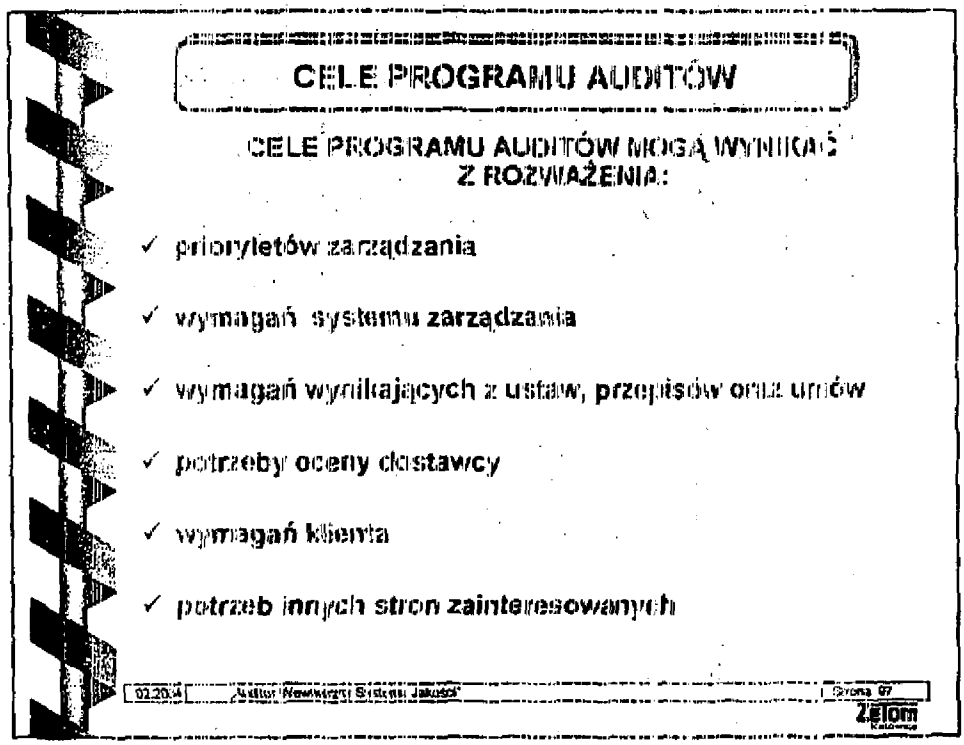
PROGRAM AUDITU – *zestaw auditów, jednego lub więcej zaplanowanych* w określonych ramach czasowych i mających określony cel

PLAN AUDITU – *opis działań oraz ustaleń organizacyjnych związanych z auditem*

PRZEBIEG PROCESU ZARZĄDZANIA PROGRAMEM AUDITÓW




PROCEDURY PROGRAMU AUDITÓW
PROCEDURY PROGRAMU AUDITÓW POWINNY OBEJMOWAĆ:
➢ Planowanie i ustalenie terminów auditów
➢ Zapewnienie kompetencji auditorów i audytorów wiodących
➢ Dobór zespołów auditujących i przydzielenie ról i odpowiedzialności
➢ Przeprowadzanie auditów
➢ Utrzymanie zapisów dotyczących programu auditów
➢ Monitorowanie funkcjonowania oraz skuteczności programu auditów
➢ Składanie najwyższemu kierownictwu raportów o ogólnych wynikach programu auditów


CELE PROGRAMU AUDITÓW
CELE PROGRAMU AUDITÓW MOGĄ WYNIKAĆ Z ROZWAŻENIA:
✓ priorytetów zarządzania
✓ wymagań systemu zarządzania
✓ wymagań wynikających z ustaw, przepisów oraz umów
✓ potrzeby oceny dostawcy
✓ wymagań klienta
✓ potrzeb innych stron zainteresowanych

ODPOWIEDZIALNOŚĆ ZA PROGRAM AUDITÓW

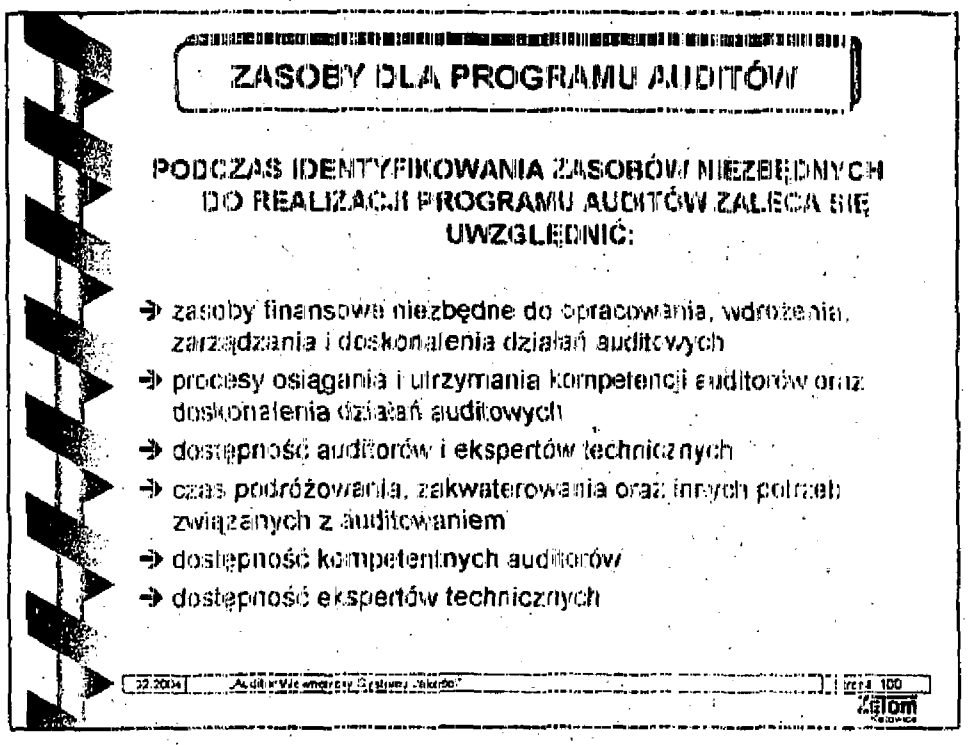
OSOBA/OSOBY ODPOWIEDZIALNE ZA ZARZĄDZANIE PROGRAMAMI AUDITÓW POWINNY:

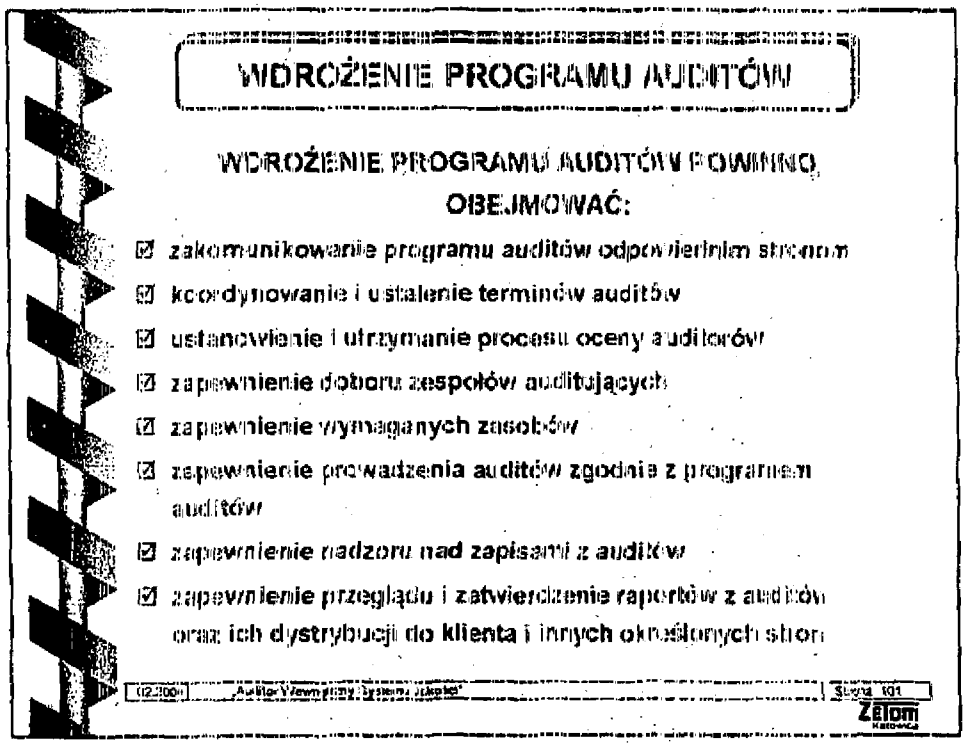
- ustalić cele i zakres programu auditów
- ustalić odpowiedzialność i procedury oraz zapewnić dostępność zasobów
- zapewnić wdrożenie programu auditów
- zapewnić utrzymanie odpowiednich zapisów z programu auditów
- monitorować, przeglądać i doskonalić program auditów

ZAKRES PROGRAMU AUDITÓW

ZALEŻY OD WIELKOŚCI, CHARAKTERU ORAZ ZŁOŻONOŚCI ORGANIZACJI ORAZ OD:

- ✓ zakresu, celu i czasu trwania każdego auditu, który ma być przeprowadzony
- ✓ częstość auditów, które mają być przeprowadzone
- ✓ liczby, ważności, złożoności, podobieństwa oraz lokalizacja działań które mają być auditowane
- ✓ wymagań norm, ustaw, przepisów oraz umów i innych kryteriów auditu
- ✓ wyników poprzednich auditów
- ✓ znaczących zmian w organizacji lub jej działaniach


ZASOBY DLA PROGRAMU AUDITÓW
PODCZAS IDENTYFIKOWANIA ZASOBÓW NIEZBĘDNYCH DO REALIZACJI PROGRAMU AUDITÓW ZALECA SIĘ UWZGLĘDNIĆ:
zasoby finansowe niezbędne do opracowania, wdrożenia, zarządzania i doskonalenia działań auditowych
procesy osiągania i utrzymania kompetencji auditorów oraz doskonalenia działań auditowych
dostępność auditorów i ekspertów technicznych
czas podróżowania, zakwaterowania oraz innych potrzeb związanych z auditowaniem
dostępność kompetentnych auditorów
dostępność ekspertów technicznych
12.2004
Slajd 100


WDROŻENIE PROGRAMU AUDITÓW
WDROŻENIE PROGRAMU AUDITÓW POWINNO OBEJMOWAĆ:
zakomunikowanie programu auditów odpowiednim stronom
koordynowanie i ustalenie terminów auditów
ustanowienie i utrzymanie procesu oceny auditorów
zapewnienie doboru zespołów auditujących
zapewnienie wymaganych zasobów
zapewnienie prowadzenia auditów zgodnie z programem auditów
zapewnienie nadzoru nad zapisami z auditów
zapewnienie przeglądu i zatwierdzenie raportów z auditów oraz ich dystrybucji do klienta i innych określonych stron
12.2004
Slajd 101

ZAPISY DOTYCZĄCEPROGRAMU AUDITÓW

- ZAPISY Z POSZCZEGÓLNYCH AUDITÓW:
  - ✓ plany auditu
  - ✓ raporty z auditu
  - ✓ raporty niezgodności
  - ✓ raporty z działań korygujących i zapobiegawczych
  - ✓ raporty z działań poauditowych, jeśli ma to zastosowanie
- WYNIKI PRZEGLĄDU PROGRAMU AUDITÓW
- ZAPISY DOTYCZĄCE PERSONELU AUDITUJĄCEGO
  - ✓ ocena kompetencji i działania auditora
  - ✓ kryteria doboru zespołu auditującego
  - ✓ utrzymanie i doskonalenie kompetencji

MONITOROWANIE I PRZEGLĄDY PROGRAMU AUDITÓW

ZALECA SIĘ MONITOROWANIE ORAZ PROWADZENIE PRZEGLĄDÓW WDROŻENIA PROGRAMU AUDITÓW ABY ZIDENTYFIKOWAĆ MOŻLIWOŚCI DOSKONALENIA

WSKAŹNIKI WYKONAWCZE DO MONITOROWANIA:

- ➢ możliwości realizacji planu auditów przez zespoły auditujące
- ➢ zgodność realizacji z programami auditów
- ➢ informacje zwrotne od klientów auditu, auditowanych i auditorów

- ✓ wyniki z monitorowania i zaobserwowane trendy
- ✓ zgodność z procedurami
- ✓ zmieniające się potrzeby i oczekiwania zainteresowanych stron
- ✓ alternatywne lub nowe praktyki auditowania

Przykład formularza:
PROGRAM AUDITÓW WEWNĘTRZNYCH NA 200...

Obszar \ Miesiąc	I	II	III	IV	V	VI	VII	VIII	IX	X	XI	XII	UWAGI
Dyrekcja													
Sprzedaż													
Administracja													
Projektowanie													
Planowanie produkcji													
Zaopatrzenie													
Produkcja													
Magazynow. i wysyłka													
Serwis													

Data: .....

Sporządził: .....

Zatwierdził: .....

- planowana data auditu
- audit przeprowadzono, raport sporządzono, niezgodności
- audit przeprowadzono, raport sporządzono, zaległości
- działania korygujące ustalono
- działania korygujące wprowadzono
- działania korygujące osiągnięto

Zetom Katowice

ETAPY PROCESU AUDITU WEWNĘTRZNEGO

INICJOWANIE AUDITU (ETAP I)

PRZEPROWADZENIE PRZEGLĄDU DOKUMENTÓW (ETAP II)

PRZYGOTOWANIE DZIAŁAŃ AUDITOWYCH REALIZOWANYCH NA MIEJSCU (ETAP III)

PROWADZENIE DZIAŁAŃ AUDITOWYCH NA MIEJSCU (ETAP IV)

PRZYGOTOWANIE, ZATWIERDZENIE I ROZPOWSZECHNIANIE RAPORTU Z AUDITU (ETAP V)

ZAKOŃCZENIE AUDITU (ETAP VI)

Zetom Katowice

INICJOWANIE AUDITU
(pierwszy etap auditu)

- Wyznaczenie auditora wiodącego
- Określenie celu auditu, który może obejmować:
  - ✓ zgodność audytowanego systemu / części z kryteriami auditora
  - ✓ ocena zdolności systemu do zapewnienia zgodności z ustawami, przepisami lub wymaganiami umowy
  - ✓ ocenę skuteczności systemu w osiąganiu zaplanowanych celów (wskaźników)
  - ✓ identyfikację obszarów potencjalnego doskonalenia
- Określenie zakresu auditu – obszaru i granic auditu, działań i procesów jednostek organizacyjnych, które mają być audytowane

INICJOWANIE AUDITU
(pierwszy etap auditu) c.d.

- Określenie wykonalności auditu – czas, zasoby, możliwość współpracy z auditowanym
- Wyznaczenie zespołu auditującego:
  - ✓ 1 auditor – auditor wiodący
  - ✓ udział auditora wiodącego w doborze członków zespołu
  - ✓ włączenie ekspertów technicznych
  - ✓ udział auditorów szkolących się w uzgodnieniu z auditowanym
- Nawiązanie I-go kontaktu z auditowanym z udziałem:
  - ✓ zarządzającego programem
  - ✓ auditora wiodącego

NIEZALEŻNOŚĆ AUDITORÓW WEWNĘTRZNYCH

wg ISO 9001:2000

AUDITOR NIE POWINIEN AUDITOWAĆ WŁASNEJ PRACY

wg ISO 19011:2002

AUDITOR JEST NIEZALEŻNY OD DZIAŁALNOŚCI PODDANEJ AUDITOWI

SCHEMAT PROCESU ZBIERANIA I ANALIZY INFORMACJI PODCZAS AUDITU wg ISO 19011

Źródło informacji

Zbieranie i selekcja (poprzez przegląd dokumentów, wywiad, obserwacje itp.)

Informacja

Weryfikacja

Dowód z auditu

Ocena względem kryteriów auditu

Ustalenia z auditu

Przegląd

Wnioski z auditu

PRZYGOTOWANIE AUDITU

- PRZEGLĄD DOKUMENTÓW ZWIĄZANYCH Z AUDITOWANYM OBSZAREM
- OPRACOWANIE PLANU AUDITU
- PRZYGOTOWANIE DOKUMENTÓW ROBOCZYCH
  - lista pytań audiowych
  - formularze do zapisywania informacji

PRZEPROWADZENIE PRZEGLĄDU DOKUMENTÓW (drugi etap audytu)

Ocena dokumentacji na zgodność z kryteriami auditu

wynik oceny pozytywny

wynik oceny negatywny

powiadomienie klienta auditu

- zarządzającego programem auditu
- auditowanego

Decyzja klient / auditor wiodący

- kontynuowanie auditu
- zawieszenie do czasu rozwiązania kwestii związanych z dokumentacją

PRZYGOTOWANIE DZIAŁAŃ AUDITOWYCH REALIZOWANYCH NA MIEJSCU (trzeci etap auditu)

- Przygotowanie planu auditu
- Przydzielenie pracy zespołowi auditującemu
- Przygotowanie dokumentów roboczych
  - ✓ listę listy kontrolnej
  - ✓ plan pobierania próbek (plan auditu)
  - ✓ formularze
  - ✓ notatki
- Poufne dokumenty powinny być zabezpieczone na czas auditu

PRZYGOTOWANIE AUDITU

Plan auditu wewnętrznego

Opracowany przez auditora wiodącego i zaakceptowany przez klienta auditu.

Przygotowany elastycznie, w sposób umożliwiający:

- dokonanie zmian w zakresie auditu wynikających z informacji zebranych w trakcie auditu

Szczegółowość planu auditu zależy od zakresu oraz złożoności auditu

Zastrzeżenia auditowanego wobec któregoś z elementów planu auditu powinny być wyjaśnione z auditorem wiodącym i klientem auditu, przed rozpoczęciem działań auditowych.

PLAN AUDITU WEWNĘTRZNEGO powinien zawierać:

- ✓ identyfikację obszarów/ procesów objętych auditem,
- ✓ cele i zakres auditu,
- ✓ identyfikację przedstawiciela auditowanego dla potrzeb auditu,
- ✓ kryteria auditu i identyfikację wszystkich odnośnych dokumentów (norma, księga jakości i procedury),
- ✓ identyfikację członków zespołu auditorów,
- ✓ datę i miejsce wykonania auditu,
- ✓ przewidywany czas rozpoczęcia i trwania każdej ze znaczniejszych czynności podczas auditu.

PLAN AUDITU WEWNĘTRZNEGO

ORGANIZACJA	PLAN AUDITU WEWNĘTRZNEGO	AUDIT: RUTYNOWY ☐ CELOWY ☐
NUMER ZLECENIA:		OBSZAR/PROCES AUDITOWANY:
CEL AUDITU:		
ZAKRES AUDITU:		
ZESPÓŁ AUDITORÓW		
KRYTERIA AUDITU:		

DATA/ GODZINA:	KOMÓRKA ORGANIZACYJNA	PROCESY:	CZYNNOŚCI/ ELEMENT NORMY:
			Spotkanie otwierające
			Spotkania zespołu auditorów
			Spotkanie zamykające
AUDITOR WIODĄCY:		KIEROWNIK KOMÓRKI AUDITOWANEJ:	

LISTA PYTAŃ AUDITOWYCH

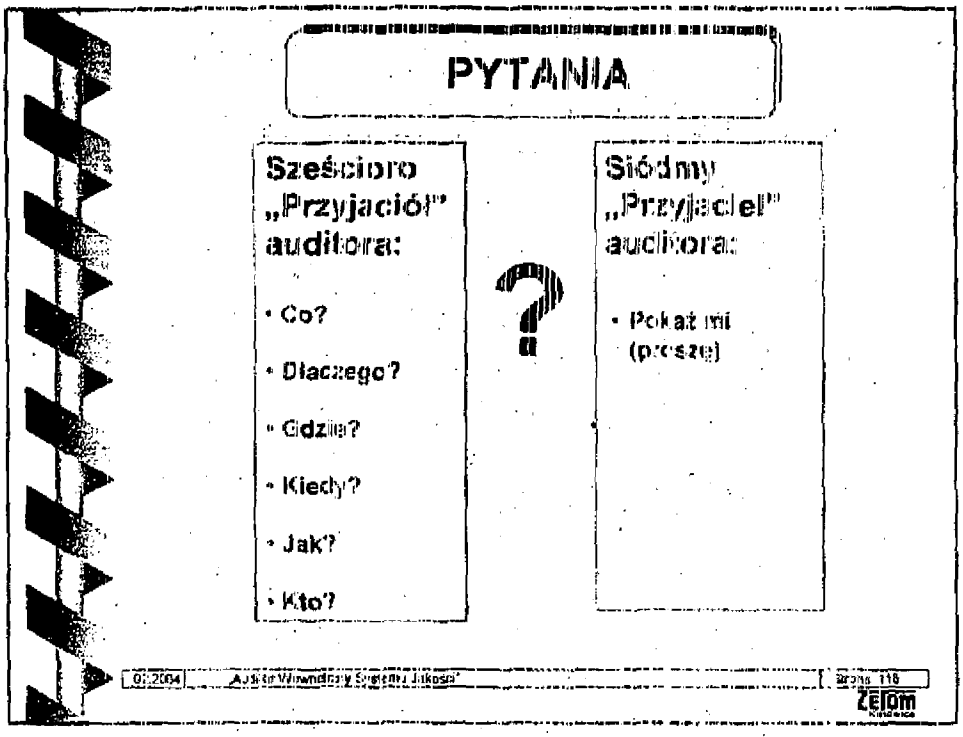
SKĄD POCHODZĄ PYTANIA?

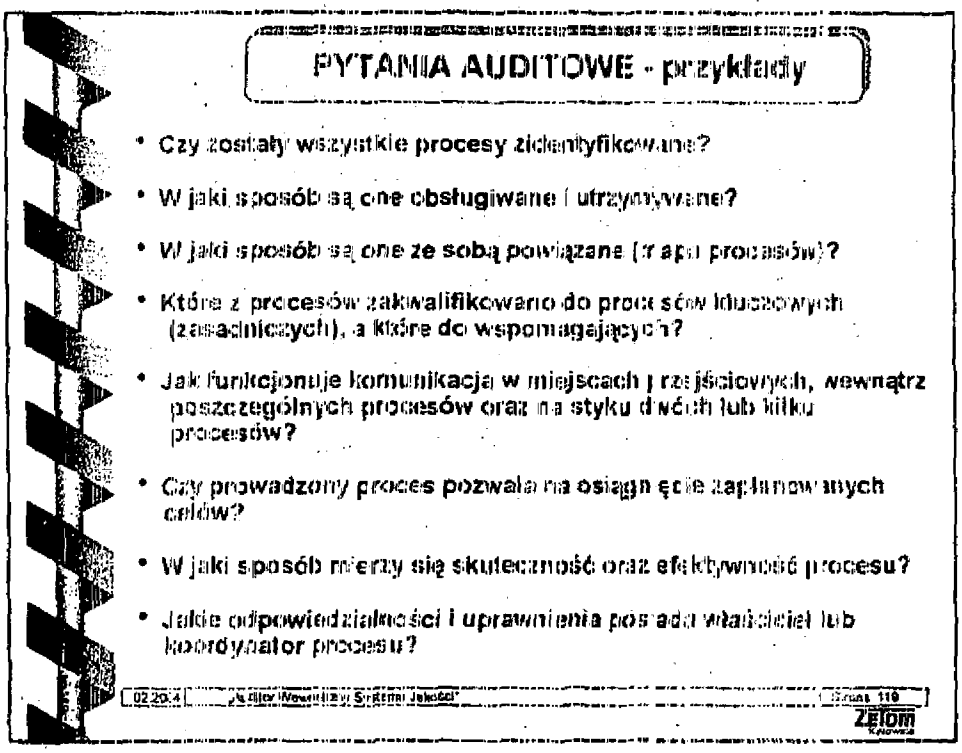
- z norm
- z Księgi Jakości
- z procedur i innych dokumentów systemu jakości
- z poprzednich auditów
- ze znajomości wyrobów, procesów, usług
- z doświadczenia auditora
- z informacji o organizacji
- z informacji od klienta

LISTA PYTAŃ AUDITOWYCH c.d.

KORZYŚCI

- jasne określenie celu auditu
- dowód planowania
- utrzymanie tempa i ciągłości auditu
- redukcja stronniczości auditora
- zmniejszenie obciążenia podczas auditu
- zapewnienie auditowanego o fachowości auditora


PYTANIA
Sześcioro „Przyjaciół" audytora:
• Co?
• Dlaczego?
• Gdzie?
• Kiedy?
• Jak?
• Kto?
?
Siódmy „Przyjaciel" audytora:
• Pokaż mi (proszę)
02.2004
Audyt Wewnętrzny Systemu Jakości
Strona 118
Zetom


PYTANIA AUDITOWE - przykłady
• Czy zostały wszystkie procesy zidentyfikowane?
• W jaki sposób są one obsługiwane i utrzymywane?
• W jaki sposób są one ze sobą powiązane (mapa procesów)?
• Które z procesów zakwalifikowano do procesów kluczowych (zasadniczych), a które do wspomagających?
• Jak funkcjonuje komunikacja w miejscach przejściowych, wewnątrz poszczególnych procesów oraz na styku dwóch lub kilku procesów?
• Czy prowadzony proces pozwala na osiągnięcie zaplanowanych celów?
• W jaki sposób mierzy się skuteczność oraz efektywność procesu?
• Jakie odpowiedzialności i uprawnienia posiada właściciel lub koordynator procesu?
02.2004
Audyt Wewnętrzny Systemu Jakości
Strona 119
Zetom

STOSOWANIE LISTY PYTAŃ AUDITOWYCH I FORMULARZY

NIE MOŻE OGRANICZAĆ ZAKRESU DZIAŁAŃ AUDITOWYCH KTÓRY MOŻE SIĘ ZMIENIAĆ W WYNIKU INFORMACJI ZEBRANYCH PODCZAS AUDITU

Przykład formularza: LISTA PYTAŃ AUDITOWYCH
- Nr zlecenia auditu .....

OBSZAR AUDITOWANY	*Opracował auditor:*	*Audytowany:*	*Data:* *Strona:*
Kryteria auditu	L.p.	Pytanie auditowe	Notatki auditowe

PRZEPROWADZENIE DZIAŁAŃ AUDITOWYCH NA MIEJSCU (czwarty etap auditu)

- SPOTKANIE OTWIERAJĄCE
- METODYCZNE BADANIE - ZBIERANIE I WERYFIKOWANIE INFORMACJI
- SPOTKANIE ZAMYKAJĄCE

SPOTKANIE OTWIERAJĄCE

- Przedstawienie uczestników oraz określenie ich roli
- Cel, zakres i kryteria auditu; metody i procedury auditu
- Plan auditu - przegląd, potwierdzenie/ dokonanie dodatkowych uzgodnień
- Potwierdzenie kanałów komunikowania się oraz poinformowanie, że audit jest próbą losową
- Uzgodnienia co do dyspozycyjności auditowanych
- Potwierdzenie dostępności zasobów i wyposażenia niezbędnego dla zespołu auditującego
- Wyjaśnienie ewentualnych niejasności (pytania)
- Potwierdzenie daty i godziny spotkania zamykającego oraz wszelkich spotkań w trakcie auditu

METODYCZNE BADANIE

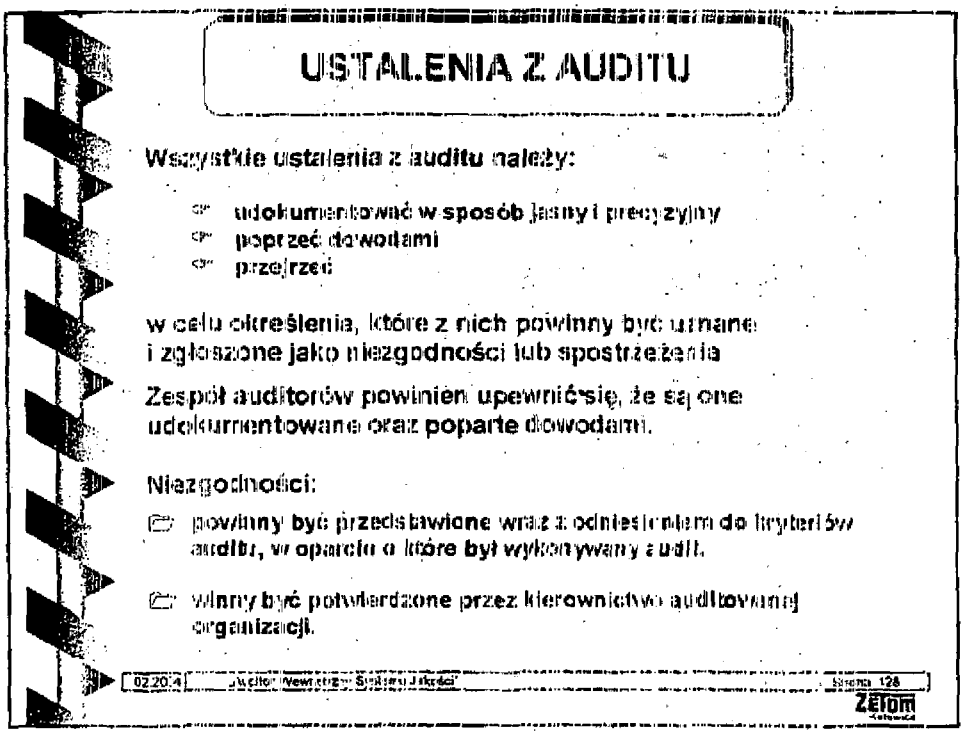
Jest przeprowadzone w rzeczywistych warunkach codziennej pracy przedsiębiorstwa

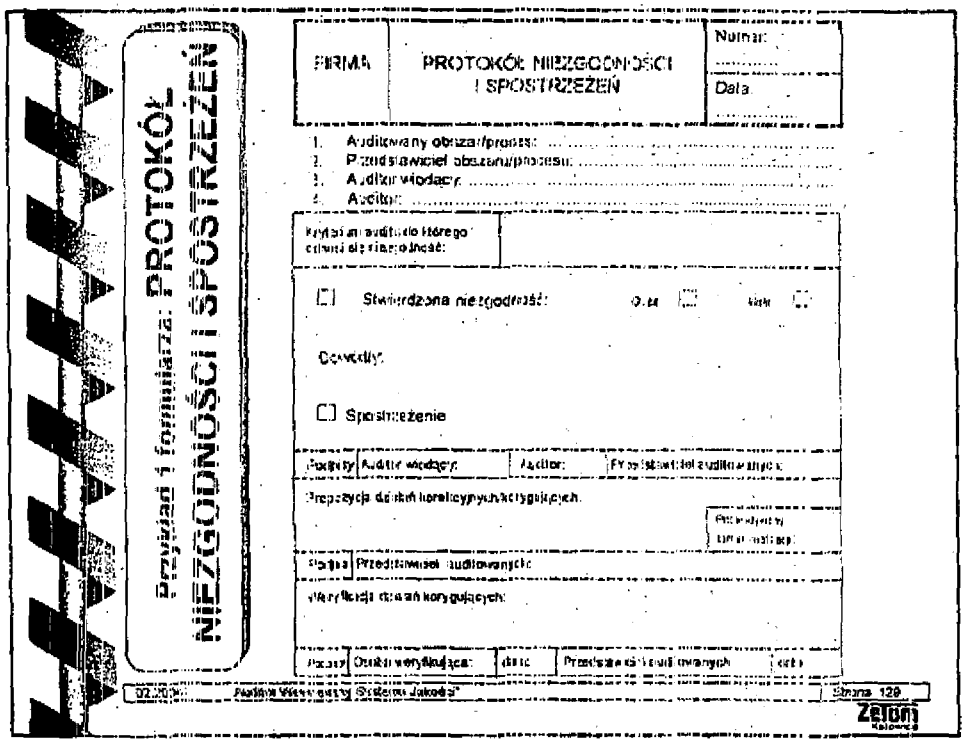
- ✓ Tworzy obraz systemu
- ✓ Polega na zbieraniu informacji „krok po kroku" poprzez:
  - wywiad auditowy - KTO, GDZIE, KIEDY, NA JAKIEJ PODSTAWIE, JAK?
  - obserwację działań
  - przegląd dokumentów
  - weryfikację informacji
  - zapisywanie - notatki spostrzeżeń oraz dowodów zgodności i niezgodności

METODYCZNE BADANIE c.d.

- ✓ *Spotkania przeglądowe* pod koniec każdego dnia - przejrzenie ustaleń
- ✓ *Sporządzanie zapisów* - protokołów spostrzeżeń i niezgodności
- ✓ *Spotkanie zespołu auditującego* w celu uzgodnienia i przygotowania wniosków z auditu

Jest prowadzone we współpracy z auditowanymi


USTALENIA Z AUDITU
Wszystkie ustalenia z auditu należy:
udokumentować w sposób jasny i precyzyjny
poprzeć dowodami
przejrzeć
w celu określenia, które z nich powinny być uznane i zgłoszone jako niezgodności lub spostrzeżenia
Zespół auditorów powinien upewnić się, że są one udokumentowane oraz poparte dowodami.
Niezgodności:
powinny być przedstawione wraz z odniesieniem do kryteriów auditu, w oparciu o które był wykonywany audit.
winny być potwierdzone przez kierownictwo auditowanej organizacji.
02.20.4
Strona 128
Zetom


Przykład formularza: PROTOKÓŁ NIEZGODNOŚCI I SPOSTRZEŻEŃ
FIRMA
PROTOKÓŁ NIEZGODNOŚCI I SPOSTRZEŻEŃ
Numer:
Data:
1. Auditowany obszar/proces:
2. Przedstawiciel obszaru/procesu:
3. Auditor wiodący:
4. Auditor:
Kryterium auditu do którego odnosi się niezgodność:
Stwierdzona niezgodność:
Dowody:
Spostrzeżenie
Podpis
Auditor wiodący:
Auditor:
Przedstawiciel auditowanych:
Propozycja działań korekcyjnych/korygujących:
Termin realizacji:
Podpis
Przedstawiciel auditowanych:
Weryfikacja działań korygujących:
Podpis
Osoba weryfikująca:
data:
Przedstawiciel auditowanych
data
02.20.5
Strona 129
Zetom

USTALENIA Z AUDITU

WYNIKI OCENY ZEBRANYCH DOWODÓW Z AUDITU W STOSUNKU DO KRYTERIÓW AUDITU

MOGĄ WSKAZYWAĆ NA:

- ZGODNOŚĆ LUB NIEZGODNOŚĆ
- /LUB MOŻLIWOŚĆ DO DOSKONALENIA

WNIOSKI Z AUDITU

WYNIK AUDITU PRZEDSTAWIONY PRZEZ ZESPÓŁ AUDITUJĄCY PO ROZWAŻENIU:

- *CELÓW AUDITU*
- *I WSZYSTKICH USTALEŃ Z AUDITU*

WNIOSKI Z AUDITU c.d.

MOGĄ DOTYCZYĆ:

- ZAKRESU ZGODNOŚCI SYSTEMU ZARZĄDZANIA Z KRYTERIAMI AUDITU
- SKUTECZNOŚCI WDROŻENIA I UTRZYMANIA SYSTEMU
- ZDOLNOŚCI PROCESU PRZEGLĄDU ZARZĄDZANIA

WNIOSKI Z AUDITU MOGĄ PROWADZIĆ DO ZALECEŃ ZWIĄZANYCH Z DOSKONALENIEM, RELACJAMI Z BIZNESEM, CERTYFIKACJĄ LUB PRZYSZŁYMI DZIAŁANIAMI AUDITOWYMI

SPOTKANIE ZAMYKAJĄCE

- CELEM SPOTKANIA JEST PRZEDSTAWIENIE KIEROWNICTWU AUDITOWANYCH OBSZARÓW USTALEŃ I WNIOSKÓW Z AUDITU
- JEST PROWADZONE PRZEZ AUDITORA WIODĄCEGO
- ZAWIERA NASTĘPUJĄCE ELEMENTY:
  - *INFORMACJA O PRZEBIEGU AUDITU*
  - *PRZEDSTAWIENIE USTALEŃ I WNIOSKÓW Z AUDITU (NIEZGODNOŚCI, DOWODY, UWAGI)*
  - *POTWIERDZENIE AUDITOWANEGO*
  - *UZGODNIENIE TERMINU PRZEDSTAWIENIA PLANU DZIAŁAŃ KORYGUJĄCYCH PRZEZ AUDITOWANEGO*
  - *ROZWIĄZANIE ROZBIEŻNYCH OPINII POMIĘDZY AUDITORAMI A AUDITOWANYMI (BRAK ROZWIĄZANIA – D. PYT.)*
  - *PRZEDSTAWIENIE ZALECEŃ W ZAKRESIE DOSKONALENIA, JEŚLI TO BYŁO OKREŚLONE W CELACH AUDITU*

UWAGA PRAKTYCZNA

Na życzenie auditowanego *auditor może* udzielić *nie wiążących* zaleceń dotyczących działań korygujących.

Określenie, zaplanowanie i przeprowadzenie działań korygujących *należy do auditowanego*.

PRZYGOTOWANIE, ZATWIERDZENIE I ROZPOWSZECHNIANIE RAPORTU Z AUDITU

- PRZYGOTOWANY POD KIERUNKIEM AUDITORA WIODĄCEGO
- AUDITOR WIODĄCY JEST ODPOWIEDZIALNY ZA TREŚĆ ORAZ DOKŁADNOŚĆ I KOMPLETNOŚĆ RAPORTU

ISO 9001: 2000

Rozdział 8 POMIARY, ANALIZA I DOSKONALENIE (6/11)

8.2. Monitorowanie i pomiary

8.2.3. Monitorowanie i pomiary procesów

- POPRZEZ STOSOWANIE ODPOWIEDNICH METOD:

WYKAZUJĄ ZDOLNOŚĆ PROCESÓW DO OSIĄGANIA ZAPLANOWANYCH WYNIKÓW

Przykład formularza: **RAPORT Z AUDITU WEWNĘTRZNEGO** str. 1/2

Organizacja	RAPORT Z AUDITU WEWNĘTRZNEGO	AUDIT: WYNIKOWY / CELOWY	NUMER: ..... DATA: ..... Strona / z ilu stron

OBSZAR / PROCES AUDITOWANY: | [illegible]:

CEL AUDITU:

ZAKRES AUDITU: ☐ ☐

DATA PRZEPROWADZENIA AUDITU: .....

OCZEKIWANCY AUDITU

ZESPÓŁ AUDITORÓW	PODLEGŁE KIEROWNICTWU AUDYTOWANEGO
1. AUDYTOR WIODĄCY:	1. .....
2.	2.
3.	3.
4.	4.

KRYTERIA AUDITU

.....

.....

02.2004 | Audytor Wewnętrzny / System Jakości | Strona 138

Zetom

Przykład formularza: **RAPORT Z AUDITU WEWNĘTRZNEGO** str. 2/2

Organizacja	RAPORT Z AUDITU WEWNĘTRZNEGO	AUDIT: WYNIKOWY / CELOWY	NUMER: ..... DATA: ..... Strona / z ilu stron

USTALENIA Z AUDITU:

WNIOSKI Z AUDITU:

ZAŁĄCZNIKI DO RAPORTU:

AUDYTOR WIODĄCY: .....

ROZDZIELNIK RAPORTU:

☐ ☐

02.2004 | Audytor Wewnętrzny / System Jakości | Strona 139

Zetom

ZAKOŃCZENIE AUDITU
(szósty etap auditu)

Audit jest zakończony, jeżeli wszystkie działania ujęte w planie auditu zostały zakończone i zatwierdzony raport został rozesłany.

PRZEKAZANIE RAPORTU:
- zlecającemu audit
- auditowanemu

ZACHOWANIE DOKUMENTÓW

Dokumenty z auditu są zachowane zgodnie z uzgodnieniami między stronami uczestniczącymi oraz zgodnie z procedurą auditów i mającymi zastosowanie przepisami i umowami.

POAUDITOWE DZIAŁANIA KORYGUJĄCE

- Odpowiedzialność auditora JEDYNIE za zidentyfikowanie niezgodności
- Odpowiedzialność auditowanego za:
  - Określenie
  - Przeprowadzenie w uzgodnionym terminie działań korygujących mieszczących się w jego kompetencjach
- Weryfikacja działań korygujących
  - *audit celowy (pozaplanowy)*
  - *audit rutynowy (planowy)*
  - *inny sposób określony przez zarządzającego programem auditów*

KOMPETENCJE AUDITORÓW wg ISO 19011:2002

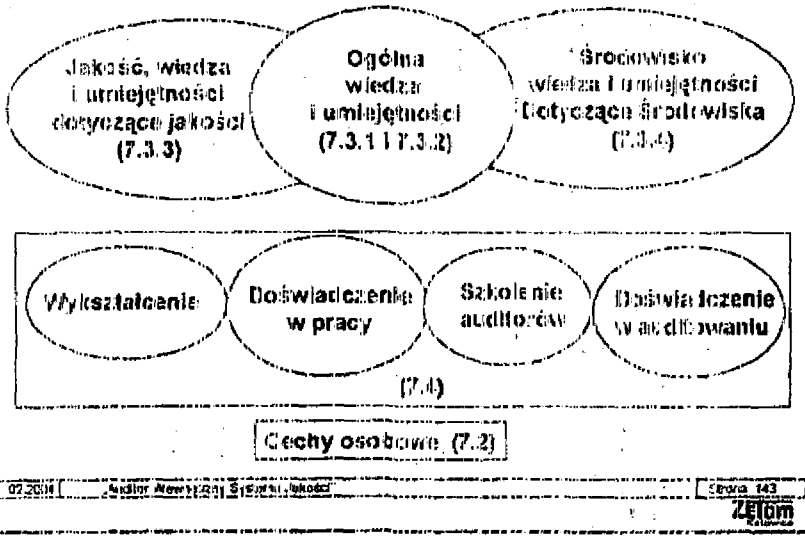
ZALECA SIĘ ABY OSOBA KTÓRA MA BYĆ AUDITOREM:

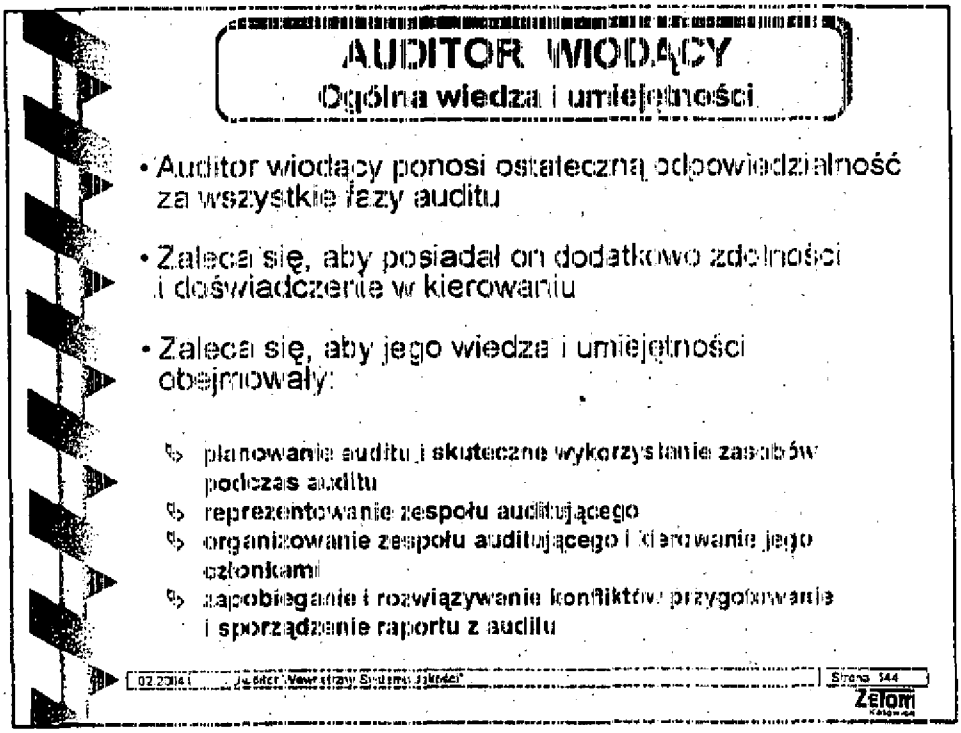
- posiadała odpowiednie cechy osobowe
- wykazała zdolność do stosowania wiedzy i umiejętności, które są niezbędne do prowadzenia auditów

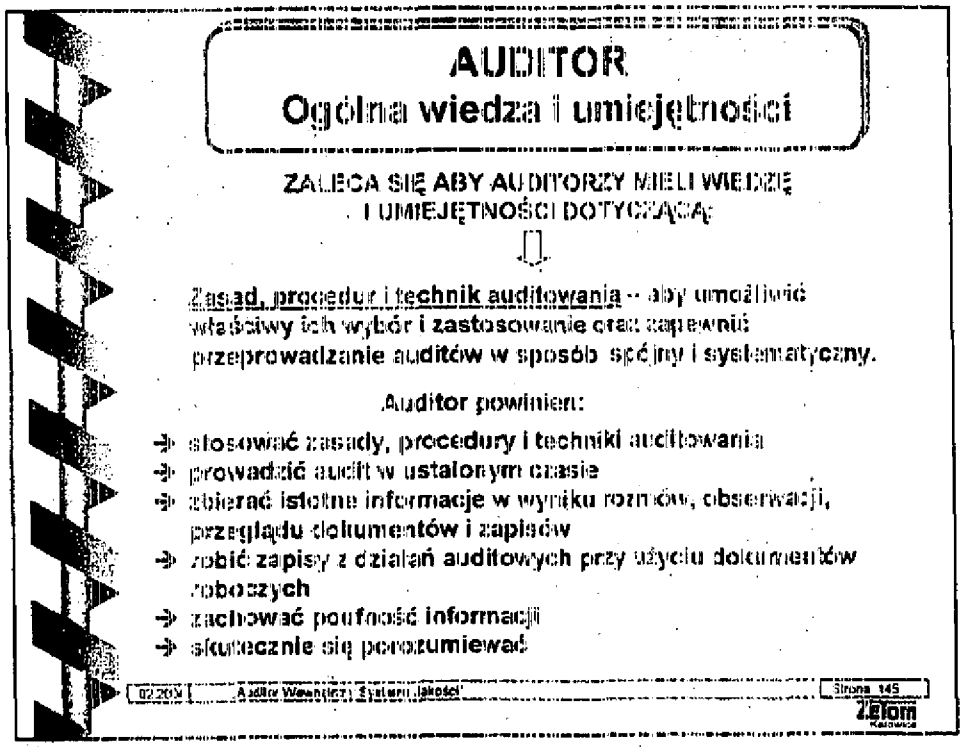
Wykształcenie, doświadczenie w pracy, szkolenie auditora oraz doświadczenie w auditowaniu są środkami, dzięki którym osoba nabywa wiedzę i umiejętności, aby stać się auditorem.

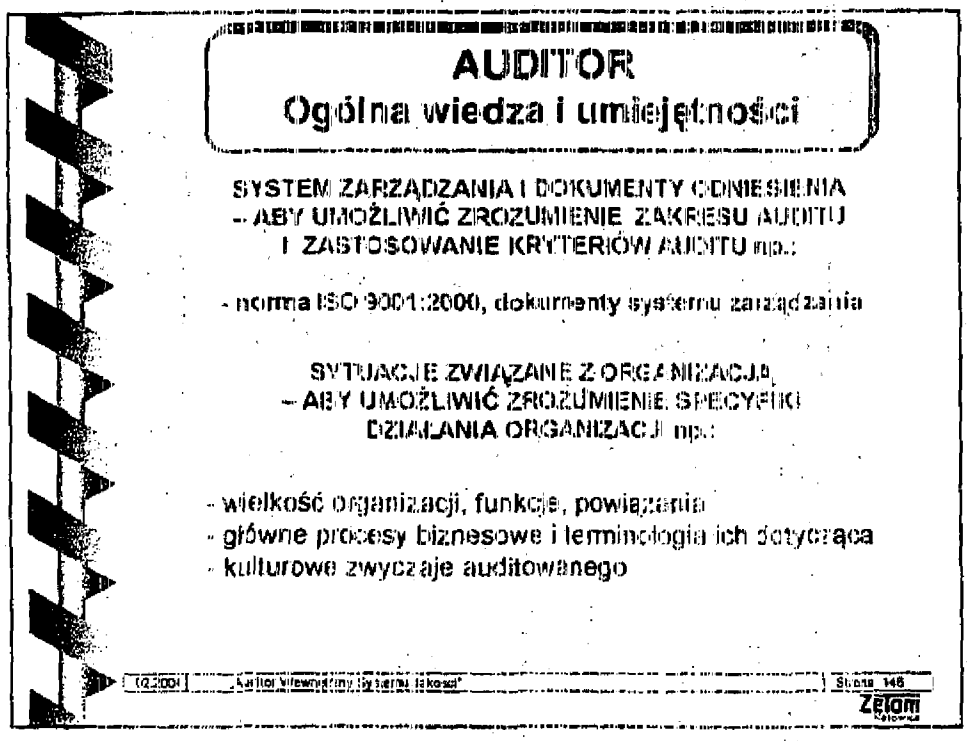
SĄ TO WSKAŹNIKI KOMPETENCJI

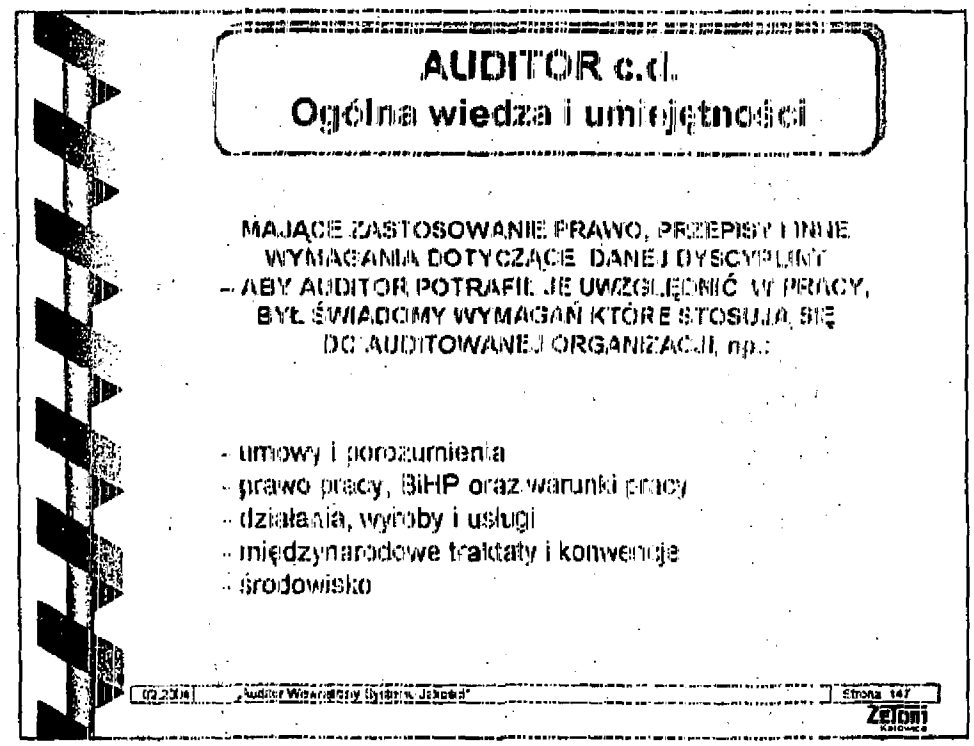
KOMPETENCJE




AUDITOR WIODĄCY
Ogólna wiedza i umiejętności
• Auditor wiodący ponosi ostateczną odpowiedzialność za wszystkie fazy auditu
• Zaleca się, aby posiadał on dodatkowo zdolności i doświadczenie w kierowaniu
• Zaleca się, aby jego wiedza i umiejętności obejmowały:
planowanie auditu i skuteczne wykorzystanie zasobów podczas auditu
reprezentowanie zespołu auditującego
organizowanie zespołu auditującego i kierowanie jego członkami
zapobieganie i rozwiązywanie konfliktów przygotowanie i sporządzenie raportu z auditu
Strona 144
Zelom


AUDITOR
Ogólna wiedza i umiejętności
ZALECA SIĘ ABY AUDITORZY MIELI WIEDZĘ I UMIEJĘTNOŚCI DOTYCZĄCĄ:
Zasad, procedur i technik auditowania – aby umożliwić właściwy ich wybór i zastosowanie oraz zapewnić przeprowadzanie auditów w sposób spójny i systematyczny.
Auditor powinien:
stosować zasady, procedury i techniki auditowania
prowadzić audit w ustalonym czasie
zbierać istotne informacje w wyniku rozmów, obserwacji, przeglądu dokumentów i zapisów
zrobić zapisy z działań auditowych przy użyciu dokumentów roboczych
zachować poufność informacji
skutecznie się porozumiewać
Strona 145
Zelom


AUDITOR
Ogólna wiedza i umiejętności
SYSTEM ZARZĄDZANIA I DOKUMENTY ODNIESIENIA
– ABY UMOŻLIWIĆ ZROZUMIENIE ZAKRESU AUDITU
I ZASTOSOWANIE KRYTERIÓW AUDITU np.:
- norma ISO 9001:2000, dokumenty systemu zarządzania
SYTUACJE ZWIĄZANE Z ORGANIZACJĄ
– ABY UMOŻLIWIĆ ZROZUMIENIE SPECYFIKI
DZIAŁANIA ORGANIZACJI np.:
- wielkość organizacji, funkcje, powiązania
- główne procesy biznesowe i terminologia ich dotycząca
- kulturowe zwyczaje auditowanego
Strona 146


AUDITOR c.d.
Ogólna wiedza i umiejętności
MAJĄCE ZASTOSOWANIE PRAWO, PRZEPISY I INNE
WYMAGANIA DOTYCZĄCE DANEJ DYSCYPLINY
– ABY AUDITOR POTRAFIŁ JE UWZGLĘDNIĆ W PRACY,
BYŁ ŚWIADOMY WYMAGAŃ KTÓRE STOSUJĄ SIĘ
DO AUDITOWANEJ ORGANIZACJI, np.:
- umowy i porozumienia
- prawo pracy, BiHP oraz warunki pracy
- działania, wyroby i usługi
- międzynarodowe traktaty i konwencje
- środowisko
Strona 147

AUDITOR

Specyficzna wiedza i umiejętności w zakresie Systemu Zarządzania Jakością

Zaleca się, aby auditorzy mieli wiedzę i umiejętności z zakresu:

METOD I TECHNIK ZWIĄZANYCH Z JAKOŚCIĄ – W CELU UMOŻLIWIENIA AUDITOROWI BADANIA S.Z.J. I OPRACOWANIE ODPOWIEDNICH USTALEŃ I WNIOSKÓW Z AUDITU, np.:

- terminologia z zakresu jakości
- zasady zarządzania jakością
- narzędzia zarządzania jakością i ich zastosowanie (statystyczne sterowanie procesem, FMEA itp.)

AUDITOR c.d.

Specyficzna wiedza i umiejętności w zakresie Systemu Zarządzania Jakością

WYROBÓW, W TYM USŁUG ORAZ PROCESÓW OPERACYJNYCH – ABY UMOŻLIWIĆ AUDITOROWI ZROZUMIENIE ZAGADNIEŃ TECHNICZNYCH, KTÓRE MAJĄ ZWIĄZEK Z AUDITEM, np.:

- terminologia specyficzna dla sektora
- charakterystyka techniczna procesów i wyrobów, w tym usług
- procesy i praktyki specyficzne dla sektora

KOMPETENCJE AUDITORA WEWNĘTRZNEGO

WYKSZTAŁCENIE
wystarczające do zdobycia wiedzy i umiejętności (określonych w Rozdz. 7.2)

DOŚWIADCZENIE W PRACY
na technicznym, kierowniczym lub innym stanowisku związanym z wykonywaniem oceny, rozwiązywaniem problemów i komunikacją z personelem kierowniczym, wykonawczym oraz klientami i innymi stronami.

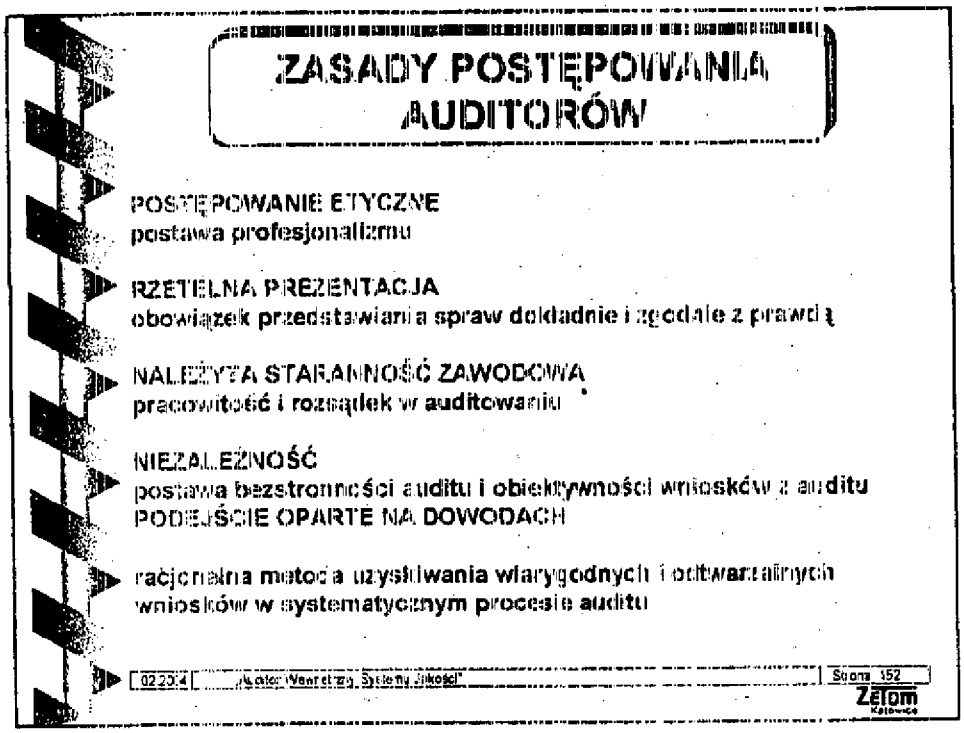
SZKOLENIE AUDITORÓW
pozwalające nabyć wiedzę i umiejętności (określone w Rozdz. 7.2.1)

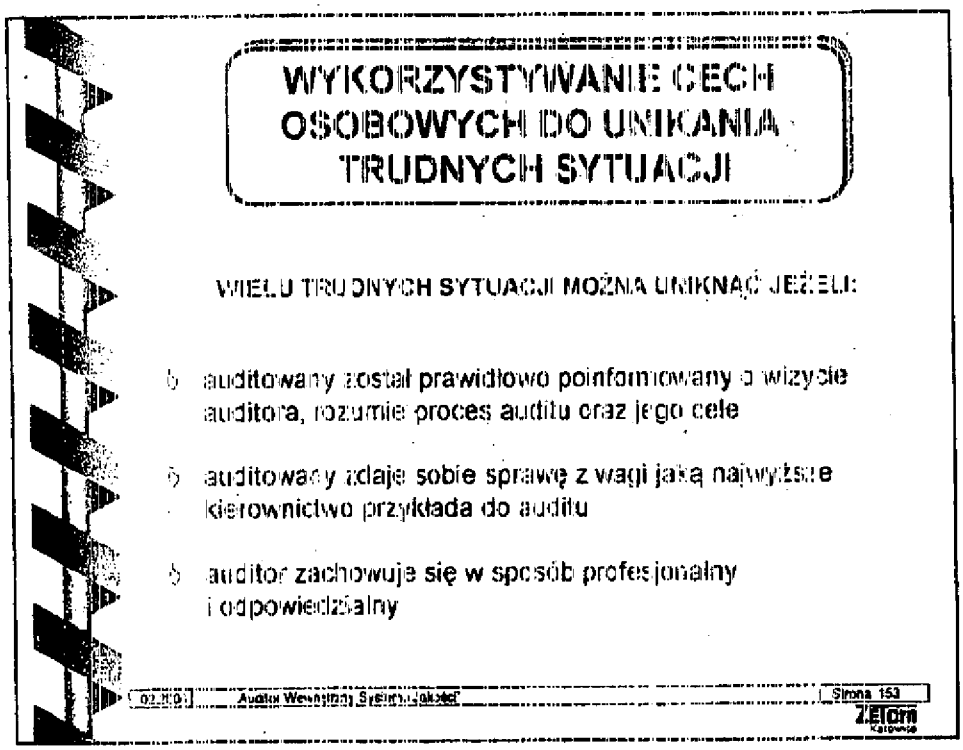
DOŚWIADCZENIE W AUDITOWANIU
nabyte pod nadzorem i kierunkiem auditora wiodącego, obejmujące pełny proces auditu oraz pełny zakres normy

KOMPETENCJE AUDITORA WEWNĘTRZNEGO c.d.

CECHY OSOBOWE – zaleca się, aby auditor był:

- etyczny
- otwarty
- dyplomatyczny
- obserwatorem
- percepcyjny
- elastyczny
- wytrwały
- zdecydowany
- niezależny


ZASADY POSTĘPOWANIA AUDITORÓW
POSTĘPOWANIE ETYCZNE
postawa profesjonalizmu
RZETELNA PREZENTACJA
obowiązek przedstawiania spraw dokładnie i zgodnie z prawdą
NALEŻYTA STARANNOŚĆ ZAWODOWA
pracowitość i rozsądek w auditowaniu
NIEZALEŻNOŚĆ
postawa bezstronności auditu i obiektywności wniosków z auditu
PODEJŚCIE OPARTE NA DOWODACH
racjonalna metoda uzyskiwania wiarygodnych i odtwarzalnych wniosków w systematycznym procesie auditu
02.2004
Auditor Wewnętrzny Systemu Jakości
Strona 152
Zelom


WYKORZYSTYWANIE CECH OSOBOWYCH DO UNIKANIA TRUDNYCH SYTUACJI
WIELU TRUDNYCH SYTUACJI MOŻNA UNIKNĄĆ JEŻELI:
auditowany został prawidłowo poinformowany o wizycie auditora, rozumie proces auditu oraz jego cele
auditowany zdaje sobie sprawę z wagi jaką najwyższe kierownictwo przykłada do auditu
auditor zachowuje się w sposób profesjonalny i odpowiedzialny
02.2004
Auditor Wewnętrzny Systemu Jakości
Strona 153
Zelom

GŁÓWNE CZYNNIKI ZACHOWAŃ na które auditor powinien zwrócić uwagę

- Język ciała
- Kontakt wzrokowy
- Głos
- Śledzenie wypowiedzi
- Zachęcanie do mówienia

SZKOLENIE KANDYDATÓW NA AUDITORÓW

...p. w zakresie:

- znajomości i rozumienia norm, na podstawie których mogą być przeprowadzane audity
- technik oceny dotyczących badania, formułowania pytań, formułowania ustaleń i wniosków oraz sporządzania raportów
- dodatkowych umiejętności wymaganych do kierowania auditem, takich jak planowanie, organizowanie, komunikowanie się

Wykazanie umiejętności

- podczas egzaminów pisemnych lub ustnych lub
- w inny odpowiedni sposób

UTRZYMANIE I DOSKONALENIE KOMPETENCJI AUDITORÓW

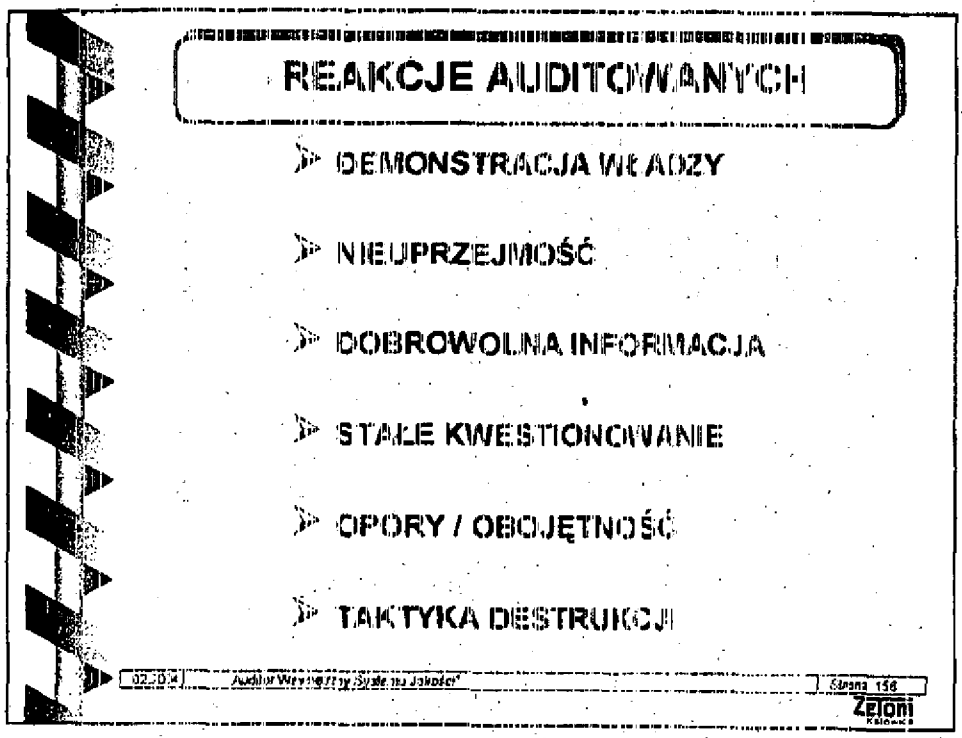
POPRZEZ

- stałe uaktualnianie swojej wiedzy i znajomości procedur i praktyk auditowania
- uczestniczenie w szkoleniach odnawiających umiejętności oraz ciągły udział w auditach S.Z.J.
- przedkładanie do przeglądu przez zespół oceniający wyników swojej pracy
- systematyczna ocena kompetencji auditorów - lista kwalifikowanych auditorów

AUDITOWANY

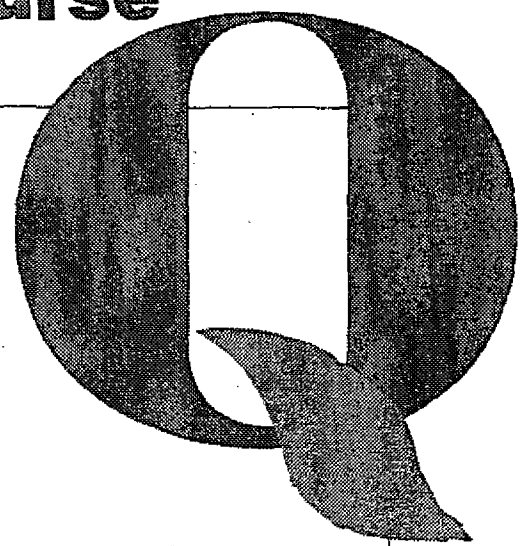
KIEROWNICTWO AUDITOWANEJ ORGANIZACJI POWINNO:

- informować personel, którego dotyczy audit, o jego celach i zakresie;
- wyznaczyć odpowiednich pracowników, którzy towarzyszyliby członkom zespołu auditującego;
- dostarczyć auditorom wszystkich niezbędnych środków do zapewnienia prawidłowego przebiegu auditu;
- zapewnić, na żądanie auditorów, dostęp do urządzeń oraz dowodów materialnych;
- współpracować z auditorami w celu osiągnięcia celów auditu;
- określać i rozpoczynać działania korygujące na podstawie raportu z auditu.


REAKCJE AUDITOWANYCH
DEMONSTRACJA WŁADZY
NIEUPRZEJMOŚĆ
DOBROWOLNA INFORMACJA
STAŁE KWESTIONOWANIE
OPORY / OBOJĘTNOŚĆ
TAKTYKA DESTRUKCJI
Strona 156
Zeloni

ANNEX A

ISEB Software Testing Foundation Certificate Training Course



Course Binder Version R2.2, 22 January 2005
Contents Responsible: ***bbjTest***, **www.bbj.com.pl**
Author: Bogdan Bereza-Jarociński

bbj Test

ISEB Software Testing Foundation Certificate Training Course

bbj Test

Bogdan Bereza-Jarociński
www.bbj.com.pl

bbj Test

Prerequisites of SW Testing

- **In more mature industries testing is *built into* development process**
- **Software development deceptively easy:**
  - no "production errors"
  - no physical constraints, easy to re-design
  - huge functionality increase possible
  - therefore "no testing necessary"
- **But SW products notoriously unreliable**

bbj Test

History of SW Testing

- **Discoveries:**
  - SW changes must be carefully verified
  - lack of physical constraints a benefit but hindrance as well (poor visibility)
  - testing effort 30-60% of project effort
- **Testing maturity:**
  - testing "to prove that it works" counterproductive
  - test is not the same as "debugging"
  - test requires specialised know-how
  - test is risk-based

bbj Test

Certification in SW Engineering

- **Numerous vendor certification schemes**
- **SW Engineering mostly post-graduate**
- **IEEE: CSDP** — Europe
- **ASQ: Certified Reliability Engineer** — USA
- **QAI: Certified Quality Analyst, Certified Software Test Engineer** — Australia, Poland, Switzerland, Europe
- **Other areas:**
  - project management, change management, requirements analysis

bbj Test

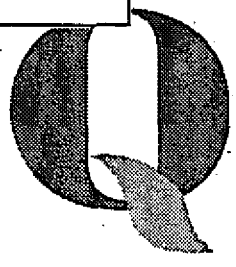
Benefits of Certification

- **For the profession:**
  - *specialised* testing skills enhanced
  - tester status
  - accepted body of knowledge
  - terminology
- **For employers:**
  - easier hiring process and career for testers
- **For testers:**
  - body of knowledge, career, acknowledgement, role clarification

bbj Test

Certification "Drawbacks"

- **Cannot replace thinking**
- **Poor agreement on what "body of knowledge" is**
- **Difficult without standards**
- **Too theoretical**
- **Terminology-focused examination**
- **Destroys diversity (testing = test + domain + CM + requirements knowledge)**



ISEB Certification 1/2

- **BCS: www.bcs.org.uk**
- **ISEB: www.bcs.org.uk/iseb/st**
- **History:**
  - BCS SIGIST (http://www.sigist.org.uk/)
  - BS 7925-2, Software Component Testing
  - BS 7925-1, Software Testing Vocabulary
  - ISEB Software Testing Foundation Certificate started 1998

ISEB Certification 2/2

- **Three levels:**
  - SW Testing Foundation Certificate (since 1998)
  - SW Testing Practitioner Certificate (since 2002)
  - SW Testing Practitioner Diploma (planned)
- **More than 18.000 participants in Foundation Certificate training courses**
- **Growing popularity outside Great Britain**
- **Growing demand for international scheme**

International Certification 1/3

- **ISTQB (www.istqb.org) started Nov. 2002**
- **Co-operation of a number of national organisations:**
  - *October 2003:* American Testing Board, Swedish Testing Board, Danish Testing Board, Polish Testing Board, Austrian Testing Board, German Testing Board, Swiss Testing Board, Finnish Testing Board, UK Testing Board, Dutch Testing Board

International Certification 2/3

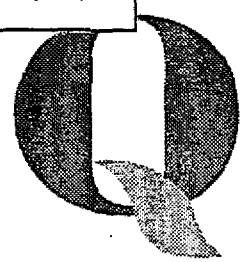
- **Goal: common syllabus and examination in a number of languages**
- **National accreditation boards**
- **International glossary of terms**
  - defines the terminology relevant for ISTQB Certified Tester Examinations in the several languages - currently in English, German and Dutch
- **TBOK (Testing Body of Knowledge)**
  - a basis for the ISTQB syllabi

International Certification 3/3

- **Organisation of examinations and certification process can be organised by national bodies themselves, or hired (currently from ISEB or ASQF, www.asqf.de)**

In Poland

- **Stowarzyszenie Jakości Systemów Informatycznych** *(Association for SW Systems Quality)*: **www.sjsi.org**
- **Polish SW Testing Board (ISTQB member): www.sjsi.org/pstb**
- **July 2002 - July 2003: *more than 200* participants, 160 took Foundation Certificate exam, 76% pass level**



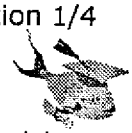
bbj Test

Training Providers

- Must be accepted by appropriate accreditation body
- Lists of accredited providers are available at accreditation bodies' sites
- Accreditation bodies check providers' facilities, inspect training material and verify tutors' credentials (professional and pedagogical)

bbj Test

Foundation Examination 1/4



- 40 multi-choice questions
- Exactly 60 minutes
- 25 correct answers passing minimum
- Only one correct answer (4 alternatives) per question
- All questions have equal weight (1 point)
- No minus points for incorrect answers

bbj Test

Foundation Examination 2/4

- No material except English dictionary (not electronic) is allowed
- Polish – English terminology list – if included in the course material - is *not* allowed
- Overseen by ISEB's invigilator
- All rules are explained in detail (in local language) by invigilator before examination
- Provider (tutor) not present
- Questions not known by provider

bbj Test

Foundation Examination 3/4

- Answer sheets gathered by invigilator and sent to ISEB for marking
- Questions cannot be kept by students, must be sent back to ISEB
- Examination results and certificates are sent from ISEB directly to candidates
- Careful spelling of non-English names!
- Complaints: invigilator - provider - ISEB

bbj Test

Foundation Examination 4/4

- Examination fee non-refundable
- New fee must be paid for new exam
- Participation in training course is not obligatory but advisable
- Public exams available in London - see ISEB page
- Public exams may be "imported"
- It is up to training providers to allow public examinees

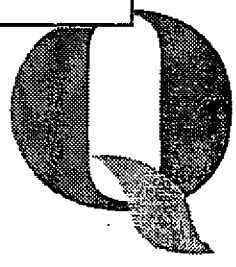
bbj Test

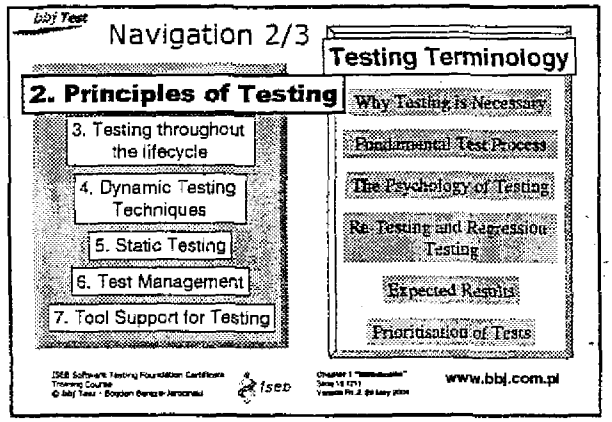
Navigation 1/3

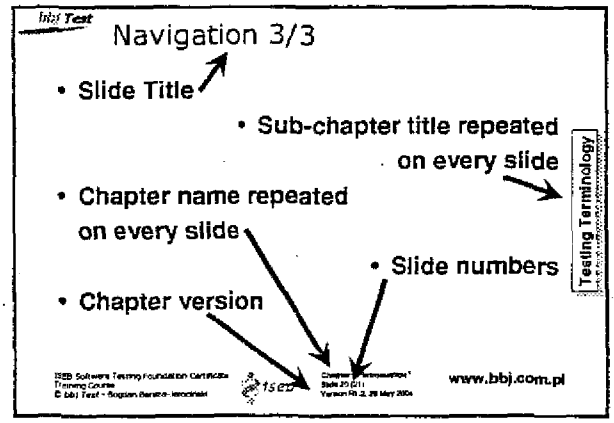
2. Principles of Testing
3. Testing throughout the lifecycle
4. Dynamic Testing Techniques
5. Static Testing
6. Test Management
7. Tool Support for Testing

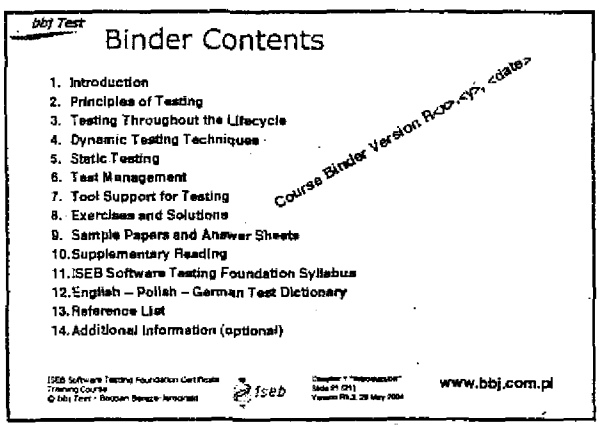
← Six main chapters

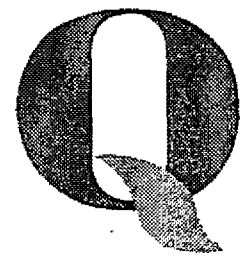
Each chapter is in a separate part of the course binder

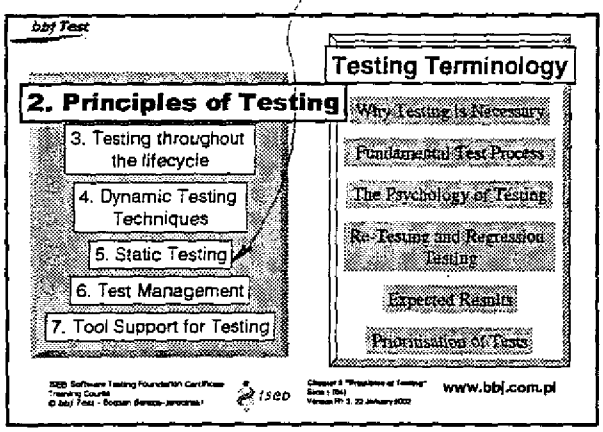


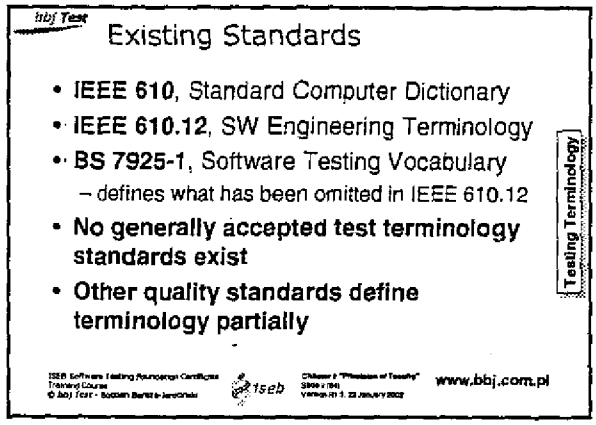

bbj Test
Navigation 2/3
Testing Terminology
2. Principles of Testing
3. Testing throughout the lifecycle
4. Dynamic Testing Techniques
5. Static Testing
6. Test Management
7. Tool Support for Testing
Why Testing is Necessary
Fundamental Test Process
The Psychology of Testing
Re-Testing and Regression Testing
Expected Results
Prioritisation of Tests
www.bbj.com.pl

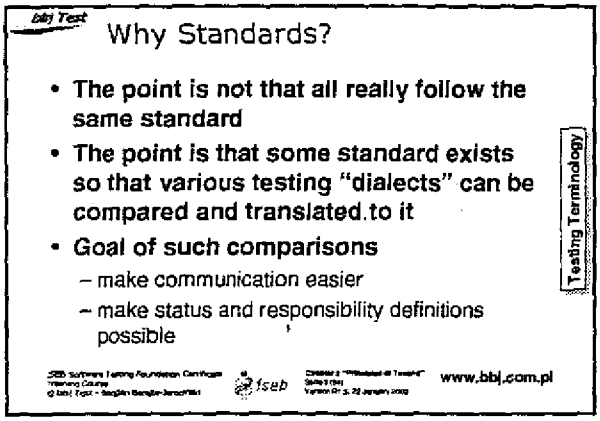

bbj Test
Navigation 3/3
• Slide Title
• Sub-chapter title repeated on every slide
• Chapter name repeated on every slide
• Slide numbers
• Chapter version
Testing Terminology
www.bbj.com.pl

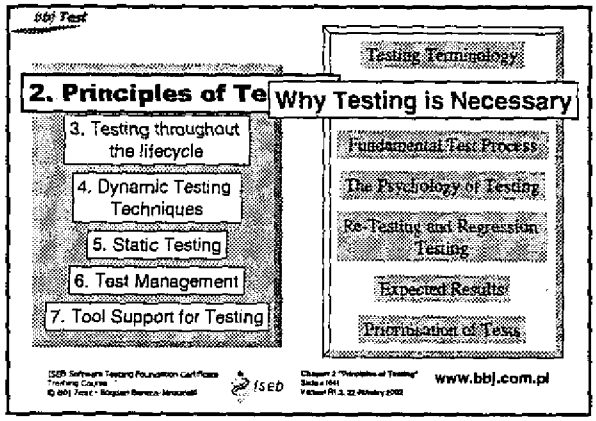

bbj Test
Binder Contents
1. Introduction
2. Principles of Testing
3. Testing Throughout the Lifecycle
4. Dynamic Testing Techniques
5. Static Testing
6. Test Management
7. Tool Support for Testing
8. Exercises and Solutions
9. Sample Papers and Answer Sheets
10. Supplementary Reading
11. ISEB Software Testing Foundation Syllabus
12. English – Polish – German Test Dictionary
13. Reference List
14. Additional Information (optional)
Course Binder Version Rxx.<y>, <date>
www.bbj.com.pl

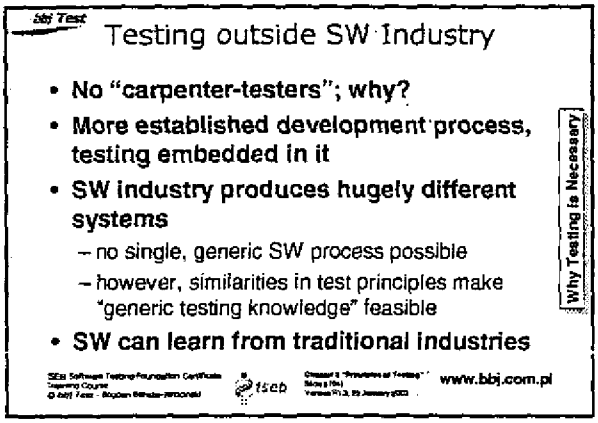


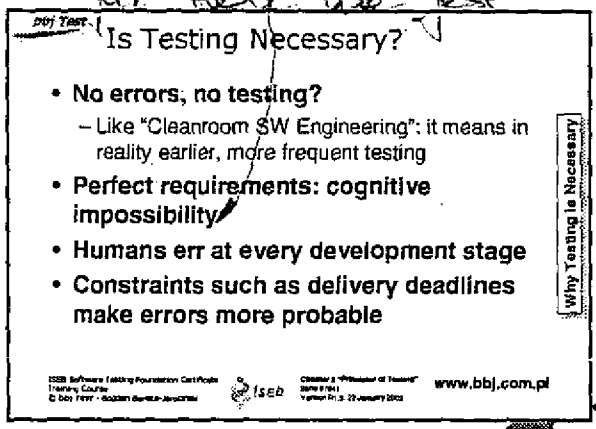

bbj Test
Testing Terminology
2. Principles of Testing
3. Testing throughout the lifecycle
4. Dynamic Testing Techniques
5. Static Testing
6. Test Management
7. Tool Support for Testing
Why Testing is Necessary
Fundamental Test Process
The Psychology of Testing
Re-Testing and Regression Testing
Expected Results
Prioritisation of Tests
www.bbj.com.pl

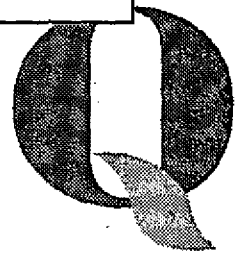

bbj Test
Existing Standards
• IEEE 610, Standard Computer Dictionary
• IEEE 610.12, SW Engineering Terminology
• BS 7925-1, Software Testing Vocabulary
– defines what has been omitted in IEEE 610.12
• No generally accepted test terminology standards exist
• Other quality standards define terminology partially
Testing Terminology
www.bbj.com.pl


bbj Test
Why Standards?
• The point is not that all really follow the same standard
• The point is that some standard exists so that various testing "dialects" can be compared and translated to it
• Goal of such comparisons
– make communication easier
– make status and responsibility definitions possible
Testing Terminology
www.bbj.com.pl


bbj Test
Testing Terminology
2. Principles of Te
Why Testing is Necessary
3. Testing throughout the lifecycle
4. Dynamic Testing Techniques
5. Static Testing
6. Test Management
7. Tool Support for Testing
Fundamental Test Process
The Psychology of Testing
Re-Testing and Regression Testing
Expected Results
Prioritisation of Tests
www.bbj.com.pl


bbj Test
Testing outside SW Industry
• No "carpenter-testers"; why?
• More established development process, testing embedded in it
• SW industry produces hugely different systems
– no single, generic SW process possible
– however, similarities in test principles make "generic testing knowledge" feasible
• SW can learn from traditional industries
Why Testing is Necessary
www.bbj.com.pl


bbj Test
Is Testing Necessary?
• No errors, no testing?
– Like "Cleanroom SW Engineering": it means in reality earlier, more frequent testing
• Perfect requirements: cognitive impossibility
• Humans err at every development stage
• Constraints such as delivery deadlines make errors more probable
Why Testing is Necessary
www.bbj.com.pl



bbj Test

Purpose of Testing

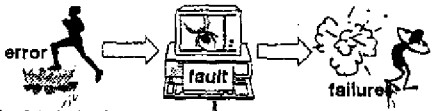
- **Testing = debugging**
- **To "prove" that SW works correctly**
- **To try to prove that is does not work**
- **To estimate risks**
- **To estimate product quality and its reliability**
- **Reliability:** "the probability that software will not cause the failure of a system for a specified time under specified conditions" (BS 7925-1)

Why Testing is Necessary

bbj Test

Error, Fault, Failure 1(2)

- **Error: the "mistake" (human, process or machine) that introduces fault into software**
- **Fault: "bug" or "defect", a faulty piece of code or HW**
- **Failure: when faulty code is executed, it may lead to incorrect results, i.e. to failure**



Why Testing is Necessary

bbj Test

Error, Fault, Failure 2(2)

Typically, only a *chain* of circumstances results in system failure in operation

Why Testing is Necessary

bbj Test

Why Errors Occur? 1(2)

- **Software and system complexity**
- **Cognitive limitations**
- **SW can be embedded - mechanical and production faults possible**
- **SW has human users - misunderstandings and misuse possible**
- **Project constraints: deadlines, resources, unrealistic requirements**

Why Testing is Necessary

bbj Test

Why Errors Occur? 2(2)

- **SW is tempting, very flexible media for development of new functionality**
  - *over-ambitious goals*
  - *over-reliance on the ability to "fix" SW faults instead of careful planning*
- **No natural constraints**
- **Invisibility of SW**
- **Psychological and social factors**

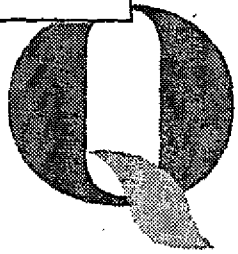
Why Testing is Necessary

bbj Test

Cost of Failures

- **Vary dramatically**
  - *from almost nothing (just re-start the program)*
  - *to many billions ("Arianne" 1996)*
- **Hard to measure**
  - loss of customer confidence
  - gradual loss of business
- **"Invisible" - outside project budget**
- **Cost of conformance < non-conformance**

Why Testing is Necessary



bbj Test

Exhaustive Testing 1(2)

- For simple algorithms, their correctness may be *proved* mathematically
- For complex algorithms it is impossible
- Correctness of an *implementation* can never be proved
  - other software
  - interaction SW/HW/OS
  - compiler 100% fault-free?

Why Testing is Necessary

bbj Test

Exhaustive Testing 2(2)

- # of remaining faults can sometimes be statistically estimated
- # of possible input combinations * states * interactions huge or infinite
- Example: "GUI calculator"
- In most SW products, even those considered as reliable, there are numerous faults and failures occur

Why Testing is Necessary

bbj Test

How much to Test?

- "Test is never ready" - true
- It depends on the risks involved (which in turn are the function of SW 'integrity levels')
- Unnecessary testing can cost you lost business
- Too little testing can cost you lost business
- Correct estimation crucial

Why Testing is Necessary

bbj Test

Risk-Based Testing 1/2

- The amount of testing depends on risks involved.
  - up to some level "quality is free" (i.e. higher cost of QA is offset by lower cost of failures)
  - above that level more testing does not result in significantly lower failure costs
  - finding this optimal level requires both testing and domain knowledge
  - it will be different for different systems

Why Testing is Necessary

bbj Test

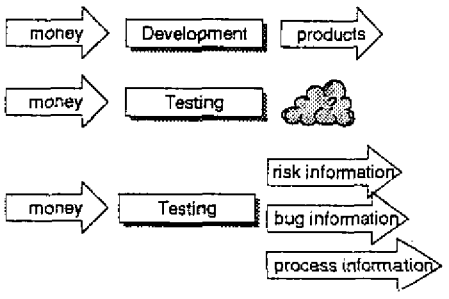
Risk-Based Testing 2/2

- Risk: probability * consequence (cost)
- Low-cost, very high probability: high risk
  - statistical testing helps address this area
- Very high-cost, low probability: high risk
  - some standards help us address this area, e.g. Standards for safety-critical systems
- Risk estimation crucial for successful test
- Correlation between more test / lower risk crucial for successful test planning

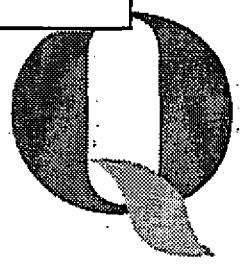
Why Testing is Necessary

bbj Test

Test Products



Why Testing is Necessary



bbj Test

Test Finds Faults

- Testing identifies faults...
- ... which can be removed and thus remove the risk of failures
- Therefore, an attitude question is that "successful test discovers faults"
- Test case suites must be constantly updated so that they keep up with new types of faults and find them

Why Testing Is Necessary

bbj Test

Test Measures Quality

- Test execution that does not find any faults is not wasted time, however
- It allows you to estimate product quality
- Product quality is the risk of its failure in operation
- This knowledge allows us to make better *business decisions*

Why Testing Is Necessary

bbj Test

Quality Attributes

- *Quality is not just* software functionality (*what* it does)...
- ... but even its attributes (*how* it does what it does)
- Some quality attributes are almost routinely forgotten in requirements specifications...
- ... therefore much depends on testing

Why Testing Is Necessary

bbj Test

Product Quality Criteria

- Estimation of product quality...
- ... based on criteria such as:
  - number of known remaining faults (unresolved incident reports) for the product
  - estimated number of unknown remaining faults in the product
  - number of test cases executed on it
- ... allow for estimation of its reliability and the cost of its expected failures

Why Testing Is Necessary

bbj Test

Test Quality Criteria

- How significant are your estimations of product quality...
- ... depends on test quality
- Quality of testing can be measured as its *coverage*: how well your test case suite cover all possible uses of the system
- *Exhaustive testing is not possible...*
- ... but representative coverage measures exist

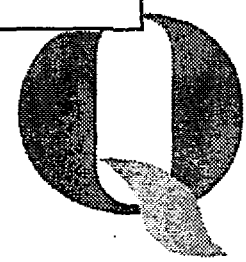
Why Testing Is Necessary

bbj Test

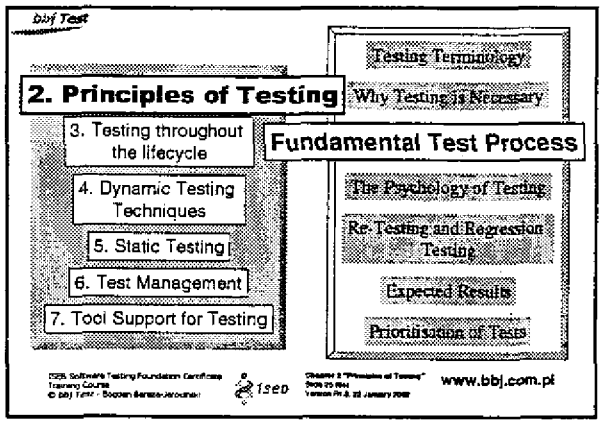
Legal Requirements

- For some industries, legal requirements for quality may exist
- The maybe embraced by industry-specific quality standards
- To prove their fulfilment may be necessary to achieve product certification *(e.g. for safety-critical)*
- Otherwise, proving non-negligent practice may always be required

Why Testing Is Necessary



bbj Test



bbj Test

Fundamental Test Process

Planning → Specification → Execution → Recording → Checking for Completion

- Basic test process - basic model of many existing test processes
- Not a full process to implement
- Describes the fundamental elements all test real processes must be composed of and their inter-dependencies

Fundamental Test Process

bbj Test

Test Planning

Planning → Specification → Execution → Recording → Checking for Completion

- Test strategy + project plan = project test plan (or any other test plan)
- Exceptions to test strategy may be introduced for each project
- Test plan is the result of this phase
- More on test plan in Chapter 3. "Testing throughout the Lifecycle"

Fundamental Test Process

bbj Test

Test Specification

Planning → Specification → Execution → Recording → Checking for Completion

- The result of test specification phase is a document called *test specification*
- Test specification is a *list of test cases* - basic building blocks describing what to test
- The level of detail of test specifications is varies, as does their relation to *test data*

Fundamental Test Process

bbj Test

Test Case Elements

Planning → Specification → Execution → Recording → Checking for Completion

- Unique test case identifier
- Short title, easily understandable by human reader
- Preconditions
- Action (typically, input values)
- Expected outcome
- Post-conditions

Fundamental Test Process

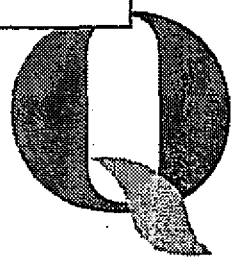
bbj Test

Test Execution

Planning → Specification → Execution → Recording → Checking for Completion

- Test cases described in test specification are executed (i.e. test inputs applied on SUT or other activities performed)
- Test cases may need to be executed many times, as new versions of SUT are delivered to test (with fault corrections or with added functionality)

Fundamental Test Process



Test Recording

Planning → Specification → Execution → Recording → Checking for Completion

- Identities and versions of the SUT, test specification and test environment are unambiguously recorded
- Actual outcomes are recorded
- *If discrepancy between actual and expected outcome exists, it is logged to facilitate fault localisation*
- Logging of what happens during test execution; incident tracking

Fundamental Test Process

Coverage Measurement

Planning → Specification → Execution → Recording → Checking for Completion

- During test recording, coverage (functional or structural) is recorded in order to be used in the next phase against coverage *criteria established in* the test plan as test completion criteria
- During test recording, *test records* and, possibly, *test logs* are created

Fundamental Test Process

Test Completion Criteria 1(2)

Planning → Specification → Execution → Recording → Checking for Completion

- Completion Criteria = Exit Criteria
- Completion criteria are best defined in advance and stated in test plan
- In case completion criteria are not met, testing must be started again from appropriate point in the process (re-planning, more test cases or new execution)

Fundamental Test Process

Test Completion Criteria 2(2)

Planning → Specification → Execution → Recording → Checking for Completion

- Some example test completion criteria
  - *all test cases executed*
  - all test cases executed on the last release
  - all test cases passed
  - no unresolved incident reports
  - no unresolved serious incident reports
  - number of faults found
  - estimated number of remaining faults low enough

Fundamental Test Process

Checking Test Completion

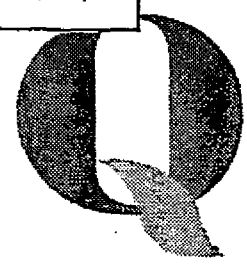
- Test completion criteria are based on *estimated product quality*
- The quality of this estimation (its significance) depends on the estimation of *test* quality
- More on test and product quality
  - slide "Product Quality Criteria" (slide 22)
  - slide "Test Quality Criteria" of this chapter (slide 23)

Fundamental Test Process

2. Principles of Testing

- 3. Testing throughout the lifecycle
- 4. Dynamic Testing Techniques
- 5. Static Testing
- 6. Test Management
- 7. Tool Support for Testing

- Testing Terminology
- Why Testing is Necessary
- Fundamental Test Process
- The Psychology of Testing
- Re-Testing and Regression Testing
- Expected Results
- Prioritisation of Tests



"Hostile Intent"

- **The main goal of testing is finding faults**
  - this can appear counter-productive (finding faults "delays" project)
  - this can appear destructive (why try "negative" or "illegal" input data values?)
  - this can appear disloyal to programmers and project management
- **The mindset of tester's role should be different to developer's**

The Psychology of Testing

Communication

- **Communication and co-operation between testers & developers is crucial**
  - developers inform testers of all recent changes
  - testers provide helpful information to facilitate reproducing failures and locating faults
- **Effective CM and incident reporting help:**
  - testers need not 'hunt' programmers for news on latest versions and changes
  - testers need not 'pester' programmers about found faults and correction plans

The Psychology of Testing

Test Diplomacy

- **Appropriate way to present faults to managers and programmers**
  - talk numbers and risk levels
  - do not adopt posture of "moral superiority"
  - remember release decision is business decision and show your understanding
  - do not 'gloat' over found faults (remembering they may be testing errors helps)
  - present found faults as common success

The Psychology of Testing

Independent Testing

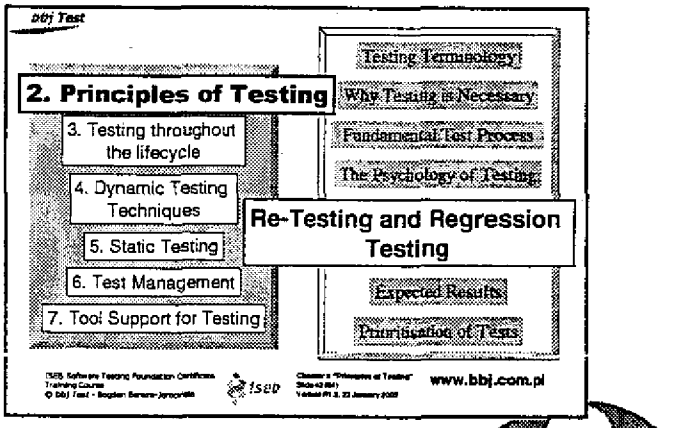
- **Independent testing is believed as more effective; its benefits are:**
  - no cognitive bias (wrong assumptions)
  - no vested interest in pretending there are no faults
  - no emotional bias ("cognitive dissonance")
- **Risks with independence:**
  - lower knowledge of implementation details
  - risk for conflict between testers & programmers

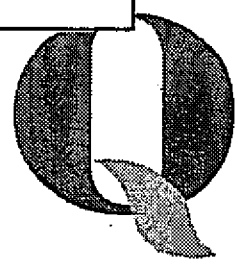
The Psychology of Testing

Levels of Independence

- **Test cases are designed by the person(s) who writes the software under test**
- **Test cases are designed by another person(s)**
- **Test cases are designed by a person(s) from a different section**
- **Test cases are designed by a person(s) from a different organisation**
- **Test cases are not chosen by a person**

The Psychology of Testing





Repetitive Tests

- **During development, it is seldom the case that test cases are executed only once**
- **Due to re-work and changes most test cases need be executed more than once**
- **Repetitive test execution is often very time-consuming**
- **Repetitive testing fosters boredom & frustration**

Re-Testing and Regression Testing

Re-testing

BS 7925-1

"Re-running of test cases that caused failures during previous execution, after the (supposed) cause of failure (i.e. fault) has been corrected, to ensure that it really has been removed successfully"

– re-testing cannot be planned (it is not known in advance how many faults will be found), but it is generally less time-consuming than regression testing

Re-Testing and Regression Testing

Regression Testing

BS 7925-1

"Re-testing of a previously tested program following modification to ensure that faults have not been introduced or uncovered as a result of the changes made"

– Regression testing can be more or less planned, but it is often the single most time-consuming activity in development projects

Re-Testing and Regression Testing

Debugging

BS 7925-1

"The *process of finding and removing* the causes of failures in software"

- **After (presumably) successful debugging has been performed**
  - re-testing is done to verify correction
  - regression testing is done to ensure no new faults have been unintentionally introduced while removing the old fault

Re-Testing and Regression Testing

Reasons for Regression Tests

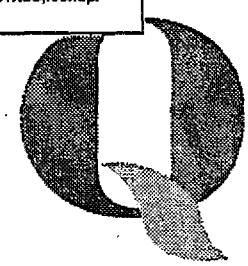
- **Regression due to fault correction**
  - unexpected side effects, new bugs introduced
- **Regression due to added new functionality**
- **Regression due to new platform**
- **Regression due to new configuration or after the customisation**
- **Regression and delivery planning**

Re-Testing and Regression Testing

Test Suite Selection

- **As test in general, the extent of regression test suite depends on risk**
- **Principles of regression test selection:**
  - new, unstable functionality
  - functionality with interface to changed functionality
  - components affected by configuration changes
  - components affected by platform modification
  - basic functionality from "everywhere"

Re-Testing and Regression Testing



Automatyzacja szkolenia wymagane testy regresji

Regression and Automation

- **Regression tests verify functionality already checked - less prone to changes**
- **Automation pays best in regression testing (lower cost of test program modifications)**
- **To identify possible automation areas investigate which test cases are used most frequently**
- **"Boredom" may be a good indicator, too**

Re-Testing and Regression Testing

Faster Regression 1(2)

- **Pruning regression test suite:**
  - old, stable components (but remember "Arianne" and risk factor)
  - components with no connection to changes (good system knowledge required)
  - statistical sampling of test cases
  - only most important test cases or "smoke test"
  - less basic functionality
  - accepting higher risk level

Re-Testing and Regression Testing

ryzykowne to jest

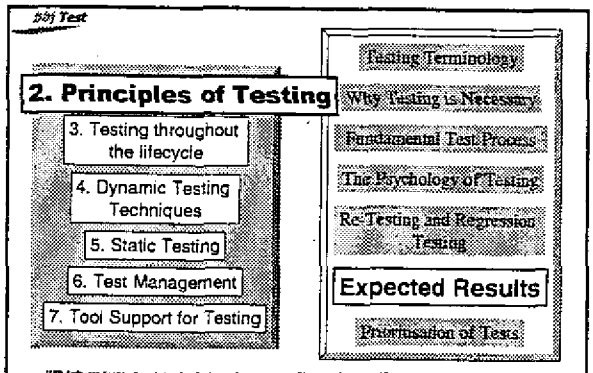
Faster Regression 2(2)

- **Faster execution of existing regression test suite:**
  - parallel testing
  - test automation
  - less frequent deliveries to test (i.e. more changes and corrections gathered in one delivery)
  - "round-robin" (not all test suit test cases executed on every delivery)

wykonujemy nie wszystkie

Re-Testing and Regression Testing

z wcześniej przygotowanych



Outcomes, results, outputs

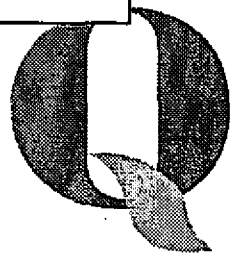
- **Test outcomes = test results**
- **Actual outcomes/results versus expected outcomes/results**
- **Outputs are often used as outcomes because:**
  - they are by definition easily accessible
  - they often *are* outcomes
- **For some tests, output are not outcomes or not the only outcomes**

Expected Results

Why Specify in Advance?

- **To avoid tester mistakes if:**
  - results are erroneous but plausible
  - due to boredom in regression testing
  - due to other psychological factors that cause errors
- **For objective result evaluation**
- **To avoid "political" pressures on test results**
- **To ensure testing defined requirements**

Expected Results



bbj Test

Outcome Types

- **Outputs**
- **State transitions**
- **Data changes**
- **Simple and compound results**
- **"Long-time" results**
- **Quality attributes (time, size etc)**
- **Side-effects**

Expected Results

bbj Test

Oracle

- **"Oracle" is a funny name used for various sources of expected outcomes:**
  - tester's intuition
  - requirements
  - specifications
  - business knowledge
  - existing system
  - other similar systems
  - standards
  - *not* the source code

Expected Results

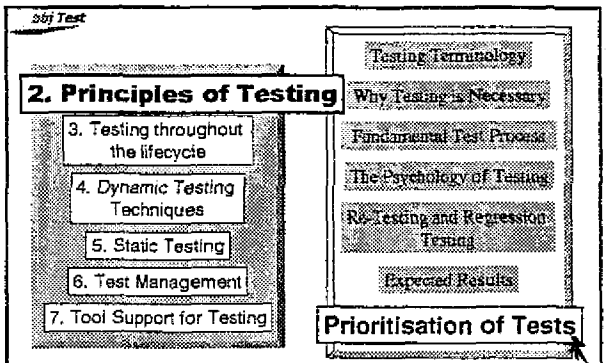
bbj Test

Outcomes & Test Data

- **Expected outcomes are part of test data (together with input data)**
- **Expected outcomes should be:**
  - under *configuration management*
  - checked for correctness
- **Expected outcomes may be difficult and expensive to obtain**

Expected Results

bbj Test



bbj Test

Why Never Enough Time?

- **Exhaustive testing not possible**
- **Test cases are always a subset of:**
  - all theoretically possible system inputs
  - all system uses it will be subject to during its lifetime
- **There is always probability that *not all* faults have been found**
- **Therefore, prioritisation (selection of more important tests cases) is necessary**

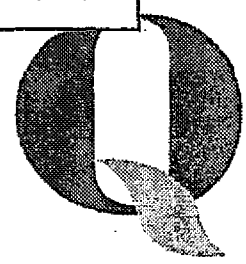
Prioritisation of Tests

bbj Test

Test Priorities and Risk

- **Selection test cases that fit into available time frame means risk-taking**
- **The more test cases are selected, the lower the risk**
- **The more important (high-priority) test *cases are selected, the lower the risk***
- **If more important test cases are executed first, risk is lower if tests abort prematurely**

Prioritisation of Tests



Prioritisation Goals

- **Selection of test cases into test suites**
  - for new functionality
  - for regression
- **Make incident report decisions easier (high-priority test cases cause high-priority incident reports)**
- **Ensure that high priority test cases are executed first in case there is not enough time to execute all**

Prioritisation of Tests

Prioritisation Criteria 1(2)

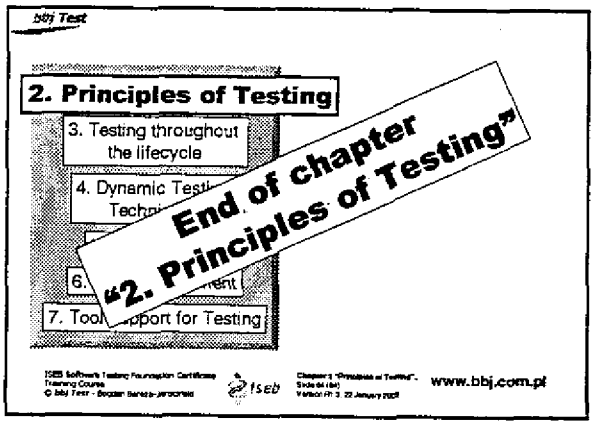
- **A list of sample criteria:**
  - Severity (failure)
  - Urgency - feedback to development
  - Probability / frequency
  - Visibility
  - Requirements priorities
  - What the customer wants
- **Some criteria overlap**

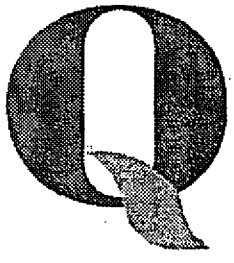
Prioritisation of Tests

Prioritisation Criteria 2(2)

- **Sample criteria for finding test areas:**
  - infected areas
  - complex code
  - change intensity
  - new technology or methods
  - people factors
  - project factors (time pressure, localisation)

Prioritisation of Tests





bbj Test

2. Principles of Testing

3. Testing throughout the lifecycle

4. Dynamic Testing Techniques

5. Static Testing

6. Test Management

7. Tool Support for Testing

Models for Testing

Economics of Testing

High Level Test Planning

Acceptance Testing

Integration Testing in the Large

Non-Functional System Testing

Functional System Testing

Integration Testing in the Small

Component Testing

Maintenance Testing

bbj Test

Verification

BS 7925-1

"The process of evaluating a system or component to determine whether the products of the given development phase satisfy the conditions imposed at the start of that phase"

- i.e. control whether you *build the system right, e.g. whether implementation of a* certain function complies with its specification

Models for Testing

bbj Test

Validation

BS 7925-1

"Determination of the correctness of the products of software development with respect to the user needs and requirements"

- i.e. control whether you *build the right system, e.g. whether customer* requirements are fulfilled
- Validation is not a test phase but a goal, realised in different phases

Models for Testing

bbj Test

Testing

BS 7925-1

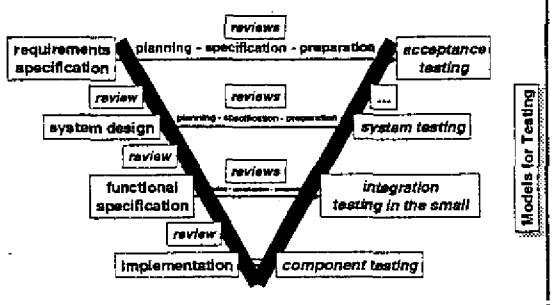
The process of exercising software, other system components and other artefacts created during system development to verify that they satisfy specified requirements, to detect faults and to estimate their reliability

[BS 7925-1, modified]

Models for Testing

bbj Test

V-model & testing in the lifecycle



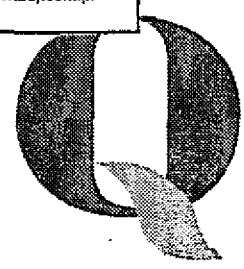
Models for Testing

bbj Test

V-model & Other Models

- Waterfall: encourages "testing-at-the-end" approach, does not allow for re-work nor parallelism among phases
- Incremental: supports parallelism, provides for requirements changes
- Spiral/iterative: supports early testing, prototyping, gradual refinement of requirements

Models for Testing



bbj Test

V-model Baselines

- Requirements engineering = preparations for acceptance testing
- Requirements break-down and system-level design = system test planning
- Functional specification = preparation for component testing
- Requirement and design baselines are basis for preparation of testing

Models for Testing

bbj Test

Testing in V-model

- Connections between corresponding development and test phases visible
- Early test design encouraged
- Early test planning and preparation encouraged
- The necessity to test (review and inspect) between development phases made visible

Models for Testing

bbj Test

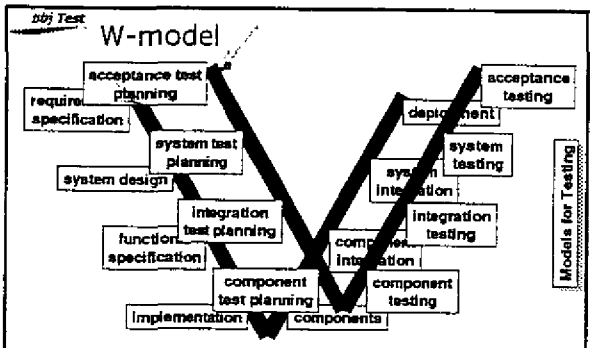
V-model: Deliverables

- Each development phase ends with a baseline which:
  - is the basis for the next phase
  - is the basis for the verification of next phase's final product
  - is the basis for planning, design and preparation of corresponding testing phase
- To accommodate iterative development, use a number of V:s in sequence

Models for Testing

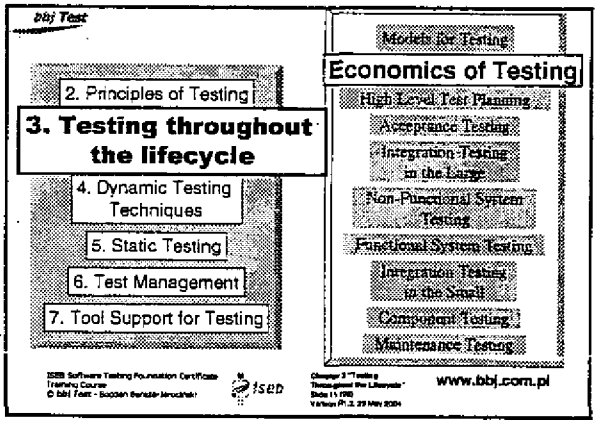
bbj Test

W-model



Models for Testing

bbj Test

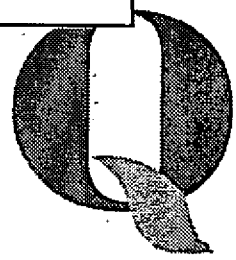


bbj Test

Cost of Failures

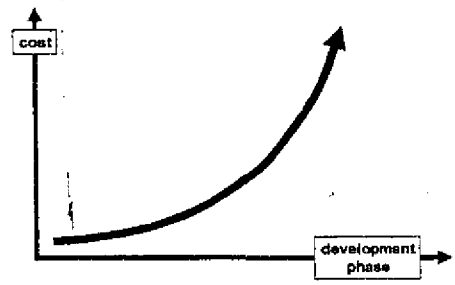
- Can be huge - see Huckle, Th. *Collection of Software Bugs*,
- Examples:
  - "Arianne" disaster (1996)
  - AA: new booking system failure (1988)
- Can be ethical
  - Therac 25 overdoses caused many deaths
- Can work slowly: loss of customer confidence

Economics of Testing



bbj Test

Cost of Fault Correction



Economics of Testing

bbj Test

Why Fault Cost Escalation?

- **Fault multiplication**
- **Faulty architecture, harder to remove faults**
- **Harder to localise faults**
- **More extensive impact analysis**
- **More extensive regression testing**
- **Re-work of documentation**
- **Re-installation and re-deployment**

Economics of Testing

bbj Test

Total Cost of Development

- **For constant testing cost:**
  - moving some resources from e.g. acceptance test to component test results in lower overall cost because of lower rework costs...
  - ... even if 'pure' test cost may be somewhat higher and there is re-organisation cost
- **"Quality is free": higher test cost results in lower overall cost - up to a certain level**

Economics of Testing

bbj Test

Fault Multiplication

- **One erroneous sentence in RS may result in:**
  - wrong system design and architecture
  - faulty code in many places
  - faulty component invoked by many other components
  - faulty class definition inherited by many classes
  - faulty documentation on many levels
  - "failure multiplication": one fault causes many

Economics of Testing

bbj Test

Early Test

- **In principle, earlier testing always decreases cost. However:**
  - not all faults can be discovered early: some "late test" is always necessary
  - test on different levels should have different focus and "net size" to avoid redundancy
  - for certain faults, discovery rates in early phases may be low and test cost high
  - testing on many levels adds some overhead costs

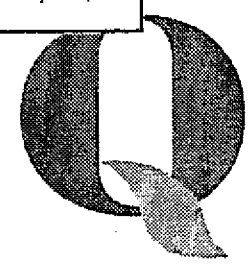
Economics of Testing

bbj Test

Early Test Design

- **Triple benefits:**
  - enables early testing: less expensive
  - early test planning and preparation: less dramatic when actual test execution arrives
  - facilitates verification and validation of requirements and other specifications - prevents fault multiplication
- **Design of system tests during requirements preparation brings to light faults in RS**

Economics of Testing



bbj Test

Techniques for Early Test

- **Reviews and inspections**
  - the only option available for most documents
- **Modelling**
  - using e.g. formal languages, which makes verification (and even validation) easier
- **Prototyping**
  - e.g. early test of usability, validation of user requirements
- **Static analysis**

Economics of Testing

bbj Test

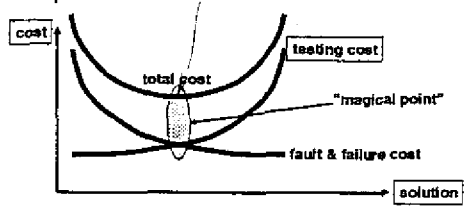
Missing Figures

- **Actual figures that show how early test and test design decrease costs are**
  - often not measured in companies
  - if measured, often not available for the public
- **The actual impact of improvements hard to measure and prove**
  - many variables involved
  - hard to distinguish correlation from causal relationship

Economics of Testing

bbj Test

Optimal Cost Level



- **"Magical point" depends on product, project and risk levels**
- **Its identification experience-based**

Economics of Testing

bbj Test

High Level Test Planning

2. Principles of Testing
3. Testing throughout the lifecycle
4. Dynamic Testing Techniques
5. Static Testing
6. Test Management
7. Tool Support for Testing

Models for Testing
Economics of Testing
Acceptance Testing
Integration Testing in the Large
Non-Functional System Testing
Functional System Testing
Integration Testing in the Small
Component Testing
Maintenance Testing

bbj Test

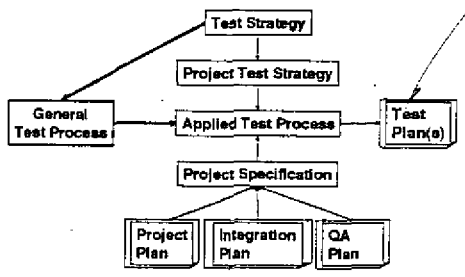
Goal of Test Planning

- **Product: document called *test plan***
- **Identification of necessary activities and resources**
- **Preparation of time schedule for testing**
- **Communication of planned test scope**
- **Choice of test methods to be used**
- **Basis for future monitoring and control**
- **Preparation of testing procedures**

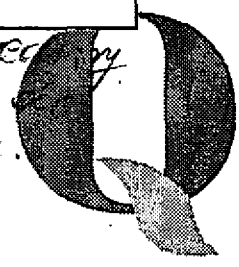
High Level Test Planning

bbj Test

Plan, Process, Strategy



High Level Test Planning



Levels in Test Planning

- **High level test planning: for the whole project (test co-ordination)**
- **Depending on project complexity:**
  - **test plans** for various levels (acceptance, system, integration, component etc.)
  - **test plans** form various sub-systems and components
  - **test plans** for various test types (functional, performance, attribute)

High Level Test Planning

IEEE 829-1998

- **IEEE/ANSI normative standard "SW Test *Documentation*"**
- **Extensive list of documents and their contents**
- **For many projects too complex**
- **It is best used as checklist for test process preparation (for document templates)**
- **Drawback: lack of process aspects**
- **Applicable on all test levels**

High Level Test Planning

Test Plan Contents 1 (5)

1. **Test plan identifier**
   - e.g. document number and version
2. **Introduction**
   - abstract, references to higher-level test plans and other source documents
3. **Test items**
   - detailed identification of those system components and attributes to which this test plan applies

High Level Test Planning

Test Plan Contents 2 (5)

4. **Features to be tested**
   - functions or high-level functions (features) which will be tested
5. **Features *not* to be tested**
   - important to communicate planned limitations in test scope
6. **Approach**
   - methods, techniques, tools (most subjects from other chapters of this course)

High Level Test Planning

Test Plan Contents 3 (5)

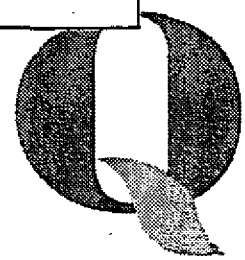
7. **Item pass/fail criteria**
   - = "test completion criteria" for each item
8. **Suspension and resumption criteria**
   - dependencies between test cases, items and levels
   - too low quality: suspension
   - entry criteria: resumption
9. ***Test deliverables***
   - all planned testware (& tested products?)

High Level Test Planning

Test Plan Contents 4 (5)

10. **Testing tasks**
    - all activities: from planning itself, through preparation, training, procurement to execution and follow-up
11. **Environmental needs**
    - detailed description of test environment(s)
12. **Responsibilities**
    - *roles and responsibilities within test project as well as test-related outside the project*

High Level Test Planning



Test Plan Contents 5 (5)

13. Staffing and training needs
- skills needed and training required

14. Schedule
- time plan

15. Risks and contingencies
- risk identification and prevention; contingency plans in case risks become true

16. Approvals
- signatures; test manager's insurance!

High Level Test Planning

Other Documents

- **IEEE 829 identifies other test documents**
  - test design specification
  - test case specification
  - test procedure specifications
  - test item transmittal reports
  - test logs
  - test incident reports
  - test summary reports

High Level Test Planning

Why Many Test Levels?

- **Risk of testing "at the end only"**
  - if there are many faults, their correction becomes very difficult
  - faults may have become so "embedded" that their correction would require extensive rework
  - the "end-of-project" drama makes testing harder
  - fault correction more expensive later
- **How many levels?** There is no single answer, it depends on the company, project and integrity requirements

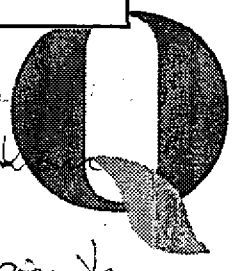
Why Many Test Levels?

Definition

BS 7925-1

"Formal testing conducted to enable a user, customer, or other authorised entity to determine whether to accept a system or component"

Acceptance Testing



bbj Test

About The Definition

- The main goal is acceptance - by someone (so that vendor can send the bill)
- Usually with end-users and other customer representatives closely involved
- For custom systems, usually as part of the deployment process
- In operational or similar test environment

Acceptance Testing

bbj Test

Practical Solutions 1 (2)

- Outsourcing - for certification or third-party acceptance
- Performed by <X> at <Y> premises
  - by the customer at his premises
  - by the vendor at customer's premises
  - by the customer at vendor's premises
  - by the vendor at his premises
- In operational environment with production (i.e. real) data

Acceptance Testing

bbj Test

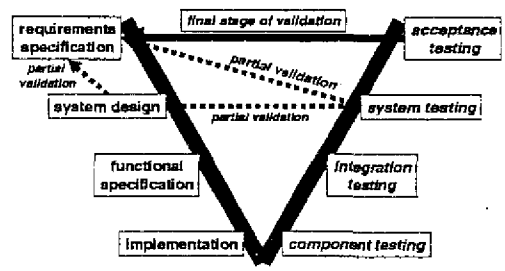
Practical Solutions 2 (2)

- Two levels of acceptance:
  - technical (system works technically)
  - organisational (system supports business)
- No customer-side acceptance testing: trusted vendor
- Pre-deployment, during deployment and post-deployment
  - all three alternative have advantages and disadvantages

Acceptance Testing

bbj Test

Final Stage of Validation



Acceptance Testing

bbj Test

Purposes and Goals

- No longer mainly fault finding, but demonstration and confidence building
- Its scope and form should have been defined in advance (and stipulated in contract)
- Acceptance testing against RS or against "what the customer really wants"?
  - what if not the same? RS validation. Customer involvement earlier. Difference "wants/needs"

Acceptance Testing

bbj Test

Customer Involvement

- At least in acceptance testing - but customer should have been closely involved much earlier
- Business process based testing
- Good for training of customer's end users and O&M personnel
- Temporary work-around can be found
- If not at customer's premises, then a "model office" can be a good option

Acceptance Testing

bbj Test

Contractual Testing

- **The only phase of testing where both vendor's and customer's lawyers should perhaps be present**
- **Contract**
  - are scope and details on acceptance testing specified in it?
  - are acceptance criteria specified in it?
  - **troublesome customer:** new requirements
  - **troublesome vendor:** no signature, no support

Acceptance Testing

bbj Test

Alpha Testing

BS 7925-1

- **Previous slides mostly applicable to custom-made systems**
- **What about "shrink-wrap" / COTS?**
- **Traditional terms "α" and "β" adopted**

"Simulated or actual operational testing at an in-house site not otherwise involved with the software developers"

  - e.g. by another department of vendor's company

Acceptance Testing

bbj Test

Beta Testing

BS 7925-1

"Operational") testing at a site not otherwise involved with the software developers"

*) *Operational testing* = testing conducted to evaluate a system or component in its operational environment

- **Great - a lot of end-users performs free testing for you at their homes!**
- **Not so great: hard to find incentives for incident reporting, low-quality reports**

Acceptance Testing

bbj Test

2. Principles of Testing

3. Testing throughout the lifecycle

4. Dynamic Testing Techniques

5. Static Testing

6. Test Management

7. Tool Support for Testing

Models for Testing

Economics of Testing

High Level Test Planning

Acceptance Testing

Integration Testing in the Large

Non-Functional System Testing

Functional System Testing

Integration Testing in the Small

Component Testing

Maintenance Testing

bbj Test

Definition

Testing the integration of systems and packages; testing interfaces to external organisations

- **File and database format**
- **Communication protocols**
- **Access rights**
- **Manual interfaces (i.e. documentation) to legacy systems**

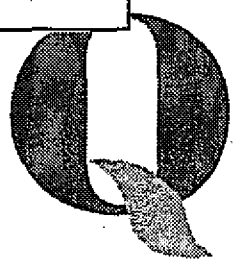
Integration Testing in the Large

bbj Test

Examples

- **Tables can be shared between a spreadsheet and word processor**
- **Mobile phone from one vendor works with Radio Base Station from another**
- **"Configuration testing": application on different platforms and configurations (e.g. Internet)**
- **Shared resources like printers, databases etc.**

Integration Testing in the Large



bbj Test

Strategies

- **Integration heuristics:**
  - one interface at a time
  - integrate each pair of systems only once
- **Incremental approach**
  - allows partial integration in the large before the system is complete
  - allows gradual integration
- **Non-incremental approach**
  - faster if successful

Integration Testing in the Large

bbj Test

Risk and Fault Localisation

- **Risk with interfaces to other systems**
  - protocol listeners/analysers may be necessary
  - no access to inner workings (nor source code) of other systems
  - security considerations when non-secure systems interface to security-critical
- **Fault localisation**
  - complex system interconnections: 3-tier Internet systems

Integration Testing in the Large

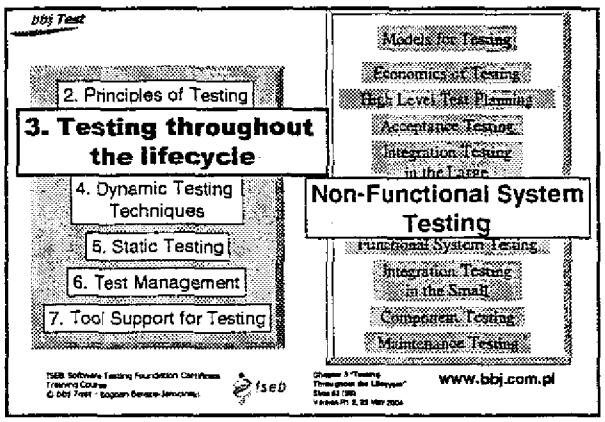
bbj Test

Test in O&M (Operation & Management)

- **Test training mainly focused on testing during development at vendor's side**
- **However, much testing is performed at customer's side during O&M of IT systems**
  - new disks installed - does all work as before?
  - new DLL, patches, versions
  - re-configuring systems
  - other changes (new resources, users etc.)

Integration Testing in the Large

bbj Test



bbj Test

Definitions

- **Testing of those requirements that do not relate to functionality, i.e. performance, usability, etc.**
- **IEEE 830 (SW RS) distinguishes:**
  - functional requirements
  - performance requirements
  - external interface requirements
  - project constraints
  - *quality attributes*

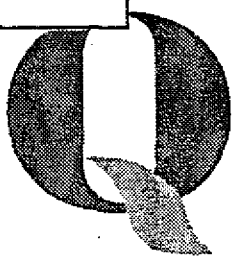
Non-Functional System Testing

bbj Test

Why on System Test Level?

- **Full non-functional testing cannot be performed before SUT is complete**
  - but partial non-functional testing is recommended as early as possible
- **Most extensive non-functional testing at system test level**
  - it is however done in acceptance and maintenance testing as well
- **The answer: for pedagogical reason**

Non-Functional System Testing



bbj Test

Quality Attributes

- **IEEE std 1061 and ISO std 9126:**
  - **efficiency** (time economy, resource economy)
  - **functionality** (completeness, correctness, security, compatibility, interoperability)
  - **maintainability** (correctability, expandability, testability)
  - **portability** (HW independence, SW independence, installability, reusability)
  - **reliability** (error tolerance, availability)
  - **usability** (understandability, ease of learning, operability, communicativeness)

Non-Functional System Testing

bbj Test

Load Testing

BS 7925-1

"Testing conducted to evaluate the compliance of a system or component with specified work load requirements"

- **Verification that SUT can:**
  - handle expected workload
  - handle expected workload over time
  - perform it's tasks while handling expected workload ("background testing")
  - where "workload" is transactions, bytes, users etc.

Non-Functional System Testing

bbj Test

Performance Testing

BS 7925-1

"Testing conducted to evaluate the compliance of a system or component with specified performance requirements"

- **End-to-end response times**
- **Internal response times**
- **Transaction processing times**
- **Load / performance dependency**

Non-Functional System Testing

bbj Test

Stress Testing

BS 7925-1

"Testing conducted to evaluate a system or component at or beyond the limits of its specified requirements"

- **service quality and level need not be provided**
- **does system crash or destroy data?**
- **does system require manual reset?**
- **What happens when load decreases?**

Non-Functional System Testing

bbj Test

Security Testing

- **Security: no illegal entry or activity beyond ones privileges must be allowed**
- **(Safety: system cannot cause harm)**
- **Security is part functionality:**
  - password functionality implemented
  - transaction refused when not enough money
- **Security is characteristics too:** no unintended "security holes" in passwords, encryption, firewalls, levels of access etc.

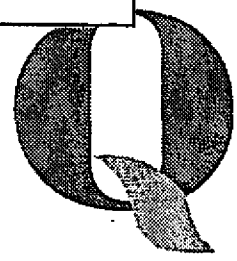
Non-Functional System Testing

bbj Test

Usability Testing

- **Four levels of "usability"**
  - user interface ergonomy
  - compliance with interface standard
  - applicability for its intended usage
  - compliance with psychological expectations of all stakeholders
- **Usability testing**
  - representative stakeholders
  - reviews, quality lab (plus SUMI)

Non-Functional System Testing



bbj Test

Storage and Volume Test

BS 7925-1

"Testing whether the system meets its specified storage objectives"

– memory management, memory size, security, access times, maintenance (e.g. fragmentation)

"Testing where the system is subjected to large volumes of data"

– e.g. full databases, large objects in memory, maximum size of protocol packages

– often combined with load and performance test

Non-Functional System Testing

bbj Test

Installability Testing

- **Installability often neglected because infrequently used**
- **Enters other non-functional areas:**
  - usability of installation procedure
  - correctness of installation documentation
  - *functional correctness*
- **Installability in various configurations**
- **How SW can be uninstalled**

Non-Functional System Testing

bbj Test

Documentation Testing

- **Usability:**
  - ease of use for different stakeholders and user levels
  - ease of learning
- **Correctness**
- **Today, documentation is very much part of the application:**
  - on-line help, context-sensitive help, application's Web site

Non-Functional System Testing

bbj Test

Recovery Testing

- **Handling of failures caused by external factors (power, mechanical, fire, memory failure etc.)**
  - what happens with interrupted transactions?
  - can data be restored from back-up?
  - remains system secure during and after failure?
  - do failure protections work (doubled, tripled systems)?
  - performance of recovery process

Non-Functional System Testing

bbj Test

2. Principles of Testing

3. Testing throughout the lifecycle

4. Dynamic Testing Techniques

5. Static Testing

6. Test Management

7. Tool Support for Testing

Models for Testing

Economics of Testing

High-Level Test Planning

Acceptance Testing

Integration Testing in the Large

Non-Functional System Testing

Functional System Testing

Integration Testing in the Small

Component Testing

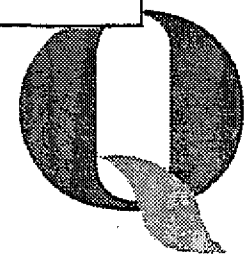
Maintenance Testing

bbj Test

Definition

- **Testing of functional requirements as specified in high-level, system RS**
- **System testing is concerned with the behaviour of a whole system. The majority of functional failures should have been already identified during unit and integration testing (TBOK)**

Functional System Testing



Goals and Purposes 1 (2)

- **First time the functionality of complete system can be tested**
- **Both verification and validation purpose**
- **Focus:**
  - end-to-end functionality
  - user perspective (user features)
  - functions that require complete system
  - recommended before integration in the large is started

Functional System Testing

Goals and Purposes 2 (2)

- **Integration of sub-systems, SW & HW**
- **Test case selection for system test is often based on models (state transition, transaction, syntax) to hide complexity**
- **Path testing**
- **Quality measures:**
  - requirements coverage
  - functional coverage
  - risk coverage

Functional System Testing

Requirements-based Test

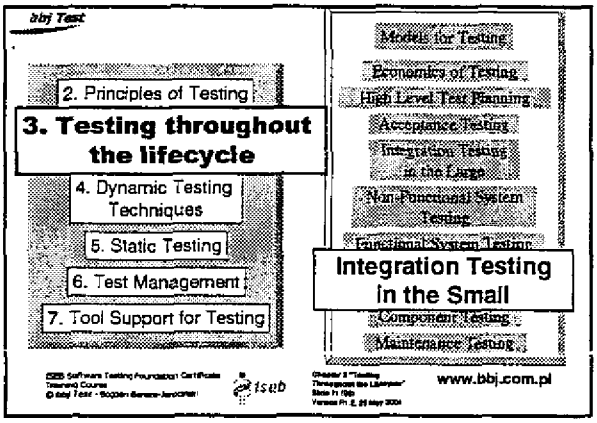
- **Is there a difference between requirements- and business-based test?**
  - depends on how requirements are described (e.g. if RS is use cases, no difference)
  - depends on what level RS is tested against (user RS or technical RS)
- **Requirements-based test:** one system function at a time, testing technical aspects, performed by vendor's test team

Functional System Testing

Business-process Testing

- **Use cases that mirror expected real usage of the system**
- **Performed by end-users or according to test scenarios prepared by end-users**
- **May comprise elements of integration testing in the large**
- **More readily performed in user environment or in model office**

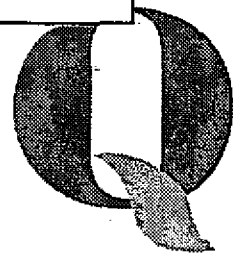
Functional System Testing



Goals and Levels

- **Two basic goals**
  - testing new wholes of integrated components
  - testing interfaces prior to integration
- **Precondition**
  - more than one tested components
- **Happens on many levels for complex systems**
- **Note: integration is development, integration test is test**

Integration Testing in the Small



Stubs and Drivers

- **Stub**
  - "a skeletal or special-purpose implementation of a software module, used to develop or test a component that calls or is otherwise dependent on it"
  - i.e. replacement for a **called function**
- **Test driver**
  - "a program or test tool used to execute software against a test case suite"
  - i.e. replacement for a **caller**

Integration Testing in the Small

Big-Bang Integration

"Integration testing where no incremental testing takes place prior to all the system's components being combined to form the system"

- ***i.e. all components at once***
- **Benefits**
  - fast if successful; no need for stubs or drivers
- **Risks**
  - first integration test happens late, if many faults localisation is difficult, rework may be necessary

Integration Testing in the Small

Top-down Integration

"Integration testing where the component at the top of the component hierarchy is tested first, with lower level components being simulated by stubs"

- ***i.e. "main program" first***
- **Benefits**
  - basic functionality first, can be used for prototyping, good monitoring and control
- ***Risks***
  - requires stubs, critical low-level functionality hidden

Integration Testing in the Small

Bottom-up Integration

"Integration testing where the lowest level components are tested first, then used to facilitate the testing of higher level components"

- ***i.e. low-level components integrated first***
- **Benefits**
  - critical low-level functionality first, hard-to-localise low-level faults easier to find one by one
- ***Risks***
  - stubs and drivers required, whole system late

Integration Testing in the Small

Functional Incrementation

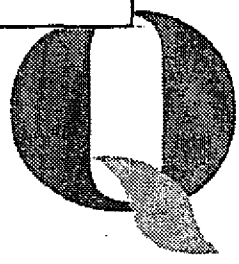
- **Like used in incremental development:**
  - only one "functional slice" (one feature) is integrated at one time, but it comprises full functionality from top to bottom
- **Benefits**
  - sensible compromise between "big bang" and stepwise methods; whole visible early
- **Risks**
  - basic functionality may be large

Integration Testing in the Small

Tips and Hints

- **Integration plan determines build and integration test order**
- **Find proper balance between goals:**
  - minimise support software
  - integrate only a small number of components at a time
- **First test basic functionality, then negative**
- **Many found faults indicate poor component testing**

Integration Testing in the Small



bbj Test

2. Principles of Testing

3. Testing throughout the lifecycle

4. Dynamic Testing Techniques

5. Static Testing

6. Test Management

7. Tool Support for Testing

Models for Testing

Economics of Testing

High Level Test Planning

Acceptance Testing

Integration Testing in the Large

Non-Functional System Testing

Functional System Testing

Integration Testing in the Small

Component Testing

Maintenance Testing

bbj Test

Names and Definitions

- Known as well as *unit*, *module*, *program*, *developer*, *basic* testing
- Usually done by programmers themselves, or a tester in a development team, or by another programmer ("buddy testing", pair programming)
- Quite often informal, undocumented and with no incident reporting
- However, it has a standard, BS 7925-2

Component Testing

bbj Test

Goals and Techniques 1(2)

- First opportunity for dynamic testing
- As net for catching bugs, it should have smallest holes
- If neglected it usually results in many faults found in integration and system testing
- Localising and removing faults relatively unexpensive

Component Testing

bbj Test

Goals and Techniques 2(2)

- Obvious area for static testing and code coverage measurements
- For testing, drivers (and sometimes stubs) are necessary
- There exist tools for creation of test drivers and function calls to achieve coverage
- Typically lack sufficient resources

Component Testing

bbj Test

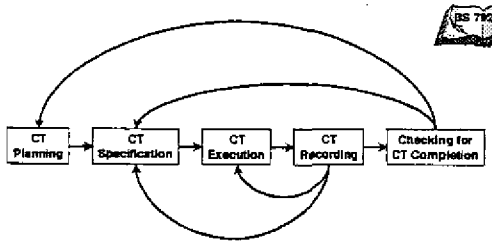
BS 7925-2

- Standard for Software *Component Testing* (BCS SIGIST)
- Comprises:
  - Process description and Guidelines
  - Test Case Design & Measurement Techniques (with Guidelines)
  - Discussion of test technique effectiveness
- Some similarities to IEEE 1008, *Software Unit Testing*

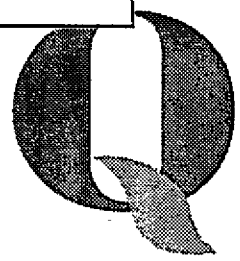
Component Testing

bbj Test

Component Test (CT) Process

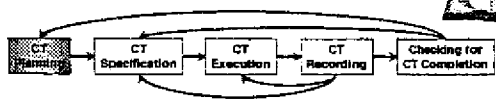


Component Testing



bbj Test

Component Test Planning

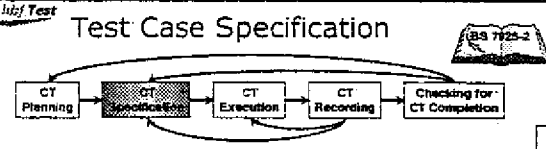


- Project component test plan specifies the dependencies between component tests and their sequence
- Component test plan specifies how the component test strategy and project component test apply to the given component under test

Component Testing

bbj Test

Test Case Specification

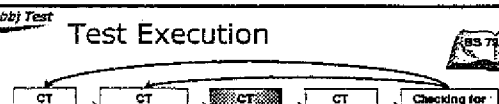


- Test cases are designed using the test case design techniques selected in the test planning activity

Component Testing

bbj Test

Test Execution

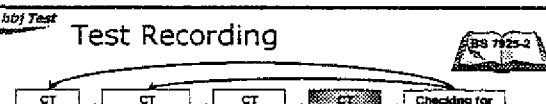


- Each test case is executed, and its outcome recorded

Component Testing

bbj Test

Test Recording

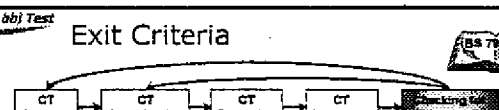


- Test record for each test case records identities and versions of the CUT and the TS
- The actual outcome is recorded
- The actual outcome is compared against the expected outcome, discrepancies logged
- The test coverage levels recorded

Component Testing

bbj Test

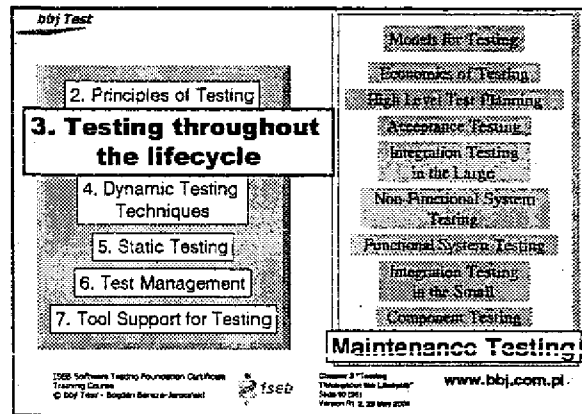
Exit Criteria

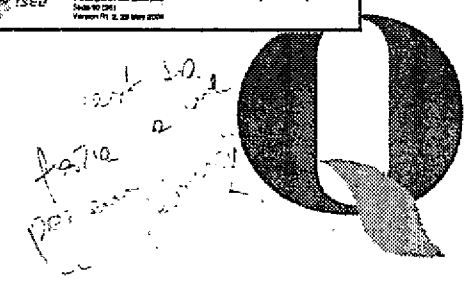


- Test records are be checked against the previously specified test completion criteria. If they are not met, the test process is restarted from appropriate point
- It may be necessary to repeat the Test Specification activity to design further test cases to meet a test coverage target

Component Testing

bbj Test





bbj Test

Definitions

- **Vendor testing during maintenance phase, i.e. after the initial release or deployment of SW product**
- **Technically, no different from testing during development**
- **The goal of maintenance testing is to preserve the level of quality achieved (regression testing) and verify changes and corrections (re-testing)**

Maintenance Testing

bbj Test

Testing "Old Code"

- **The actual age of the code tested during maintenance may vary, but it is nevertheless "old" in some sense:**
  - project structure to support its development and test no longer exists
  - any missing documentation creates difficulties as implementation details fade from project members' memories
  - it is important that old development and test environments are preserved

Maintenance Testing

bbj Test

Scope of Testing Old Code

- **Same reasoning as for regression testing in general**
  - the less is known, the larger regression scope is required
  - more extensive regression required for more extensive changes
- **If there is not enough time**
  - prioritisation
  - continue testing even after update delivery

Maintenance Testing

bbj Test

Impact Analysis

- **What can impact of code changes be? Not obvious due to:**
  - lack of fresh memory of technical details
  - missing (lost or never produced) documentation
  - missing source code (!)
- **Therefore, even the impact of "trivial" changes must be carefully analysed**
- **Exploratory testing techniques may help**

Maintenance Testing

bbj Test

Customer and Vendor

- **Maintenance testing done by the vendor**
  - fault corrections and new/modified functionality
  - if possible, a number of changes should be combined into maintenance release
- **Maintenance testing done by the customer**
  - testing in operation of SW from many vendors present in one's own environment
  - still more impact analysis and exploration required

Maintenance Testing

bbj Test

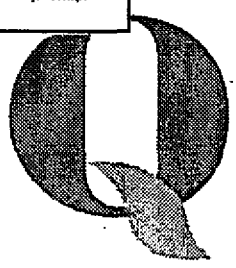
2. Principles of Testing

3. Testing throughou... the lifecyc...

4. Dynamic...

7. To... of Testing

End of chapter "3. Testing throughout the Lifecycle"



bbj Test

2. Principles of Testing
3. Testing throughout the lifecycle
4. Dynamic Testing Techniques
5. Static Testing
6. Test Management
7. Tool Support for Testing

Black and White Box Testing
Black Box Techniques
White Box Techniques
Error-Guessing

bbj Test

Dynamic?

- **"Dynamic testing techniques"**: test design techniques used for dynamic testing, i.e. testing performed during execution of SUT or its parts
- **Are there "static testing techniques"?**
  - in a way (e.g. checklists for reviews and inspections, types of faults searched during static analysis), but they are different from techniques used for design of executable test and difference between black- & white-box is less distinct

Black and White Box Testing

bbj Test

Definitions and Names

- **Names:**
  - **black-box** = functional = behavioural testing = = requirements-based
  - **white-box** = structural = glass-box testing
- **Black-box:** "test case selection that is based on an analysis of the specification of the component without reference to its internal workings"
- **White-box:** "test case selection that is based on an analysis of the internal structure of the component"

Black and White Box Testing

bbj Test

Differences

System Under Test

- **Black-box**
  - SUT treated - for the purpose of test case generation - as a "black-box", i.e. The correctness of pairs stimulus-behaviour is verified
- **White-box**
  - ideas on what to test are found through analysis of system inner workings, its structure
- **Expected outcomes:** not from source code

Black and White Box Testing

bbj Test

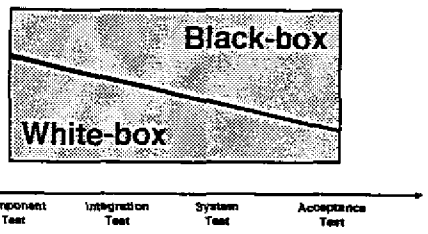
Focus and "Grey Box"

- **Specific techniques – can sometimes be used for either black-box or white-box**
  - e.g. syntax testing for user interface or internal protocol
- **The main difference is in focus: black-box from end-user perspective, white-box from technical knowledge**
- **"Grey box": some but limited knowledge about structure is assumed**

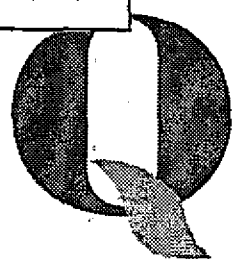
Black and White Box Testing

bbj Test

Black & White in Lifetime



Black and White Box Testing



bbj Test

No Black without White

- **If only black-box testing were used:**
  - insufficient knowledge about the quality of used test suite
  - increased risk of not testing "special cases" or "negative test cases"
  - tests designed specifically to address failures caused by design and implementation faults would not exist
  - "stupid" coding faults would be found only late

Black and White Box Testing

bbj Test

No White without Black

- **If only white-box testing were used:**
  - 100% code coverage does not guarantee 100% requirements coverage
  - user perspective omitted from tests
  - use case-based test cases and business-process-based tests would not exist
  - functional, requirement, transaction, state transition testing (& coverage) - unknown
  - users would soon discover "obvious" faults

Black and White Box Testing

bbj Test

Systematic Techniques

- **Testing is 33% art, 33% craft and 33% science (systematic, formal techniques)**
- **Art + craft = error guessing typically very effective for fault detection**
- **Systematic techniques necessary for quality estimates (confidence) of product and tests**
- **Systematic techniques provide control and minimise avoidable omissions**

Black and White Box Testing

bbj Test

Black & White Process

- **Begin with black-box test suite**
- **Measure structural coverage**
- **Complete black-box test suite**
- ***Add more white-box test cases***
- **Measure coverage, both structural and functional**
- **Estimate test suite quality**
- **Estimate product (SUT) quality**

Black and White Box Testing

bbj Test

Measurement & Coverage

- **"Coverage" is a measure of test suite quality**
- **There are different coverage measures: for black-box & for white-box testing**
- **White-box coverage is mainly code coverage**
- **Coverage measurement is not testing, but test quality assessment & improvement**

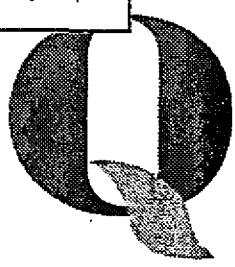
Black and White Box Testing

bbj Test

Using Tools

- **Tools for test design = tools for test generation**
- **Test generation for functional testing - difficult**
- **Tools for code coverage measurement:**
  - necessary for efficient measurements
  - tools exist for automatic generation of test drivers designed to achieve coverage for tested modules

Black and White Box Testing



bbj Test

2. Principles of Testing
3. Testing throughout the lifecycle
4. Dynamic Testing Techniques
5. Static Testing
6. Test Management
7. Tool Support for Testing

Black and White Box Testing
Black Box Techniques
White Box Techniques
Error-Guessing

bbj Test

List of Techniques 1/2

BS 7925-2

- **Equivalence Partitioning**
- **Boundary Value Analysis**
- **State Transition Testing**
- **Cause-Effect Graphing**
- **Syntax Testing**
- **Random Testing**
- **Syntax & random testing can produce ∞ # of test cases - no coverage metrics**

Black Box Techniques

bbj Test

List of Techniques 2/2

BS 7925-2

- **Cause-Effect Graphing:** "model of the logical relationships between causes and effects for the component", represented as a graph, from which test cases are derived
- **Syntax Testing:** "uses a model of the formally-defined syntax of the inputs to a component", or meta-language. E.g. for interface or protocol tests
- **Random Testing:** random generation of values from component's input domain; e.g. for stability testing

Black Box Techniques

bbj Test

Focus of This Chapter

- **Equivalence Partitioning**
  - described in some detail, exercises provided, appears among exam questions
- **Boundary Value Analysis**
  - described in some detail, exercises provided, appears among exam questions
- **State Transition Testing**
  - described shortly, no exercises nor examination questions on this technique

Black Box Techniques

bbj Test

Domain Testing

- **Test technique, applied on input or output domain(s):**
  - values inside domain assumed to be processed in the same way
  - test whether domain values are processed correctly
  - testing whether correct values belong to the domain (mainly on or near boundaries)
  - domains can be multi-dimensional
- **1-dimensional domain discussed here**

Black Box Techniques

bbj Test

Equivalence Partitioning

BS 7925-1

Equivalence class (partition): a portion of the component's input or output domains for which the component's behaviour is assumed to be the same from the component's specification

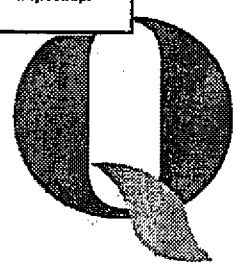
- **Example - testing a calculator**

  If 17 + 48 yields correct result, do you need to test 19 + 54 as well?

  What about $10^{33} + 10^{24}$?

  Equivalence class assumptions often require white-box knowledge

Black Box Techniques



bbj Test

EP: More Examples

- **Input domain**
  - register person with age 0 - 120
  - message length 10 - 50 bytes
  - voltage 0 - 1000 V
- **Output domain**
  - name printout 4 - 30 characters
  - attachment size 0 - 4 Mbytes
  - record field size 1byte - 127 bytes

Black Box Techniques

bbj Test

Boundary Value Analysis

BS 7925-1

A test case design technique for a component in which test cases are designed which include representatives of boundary values...
... which are input or output values either on boundaries between equivalence classes, or an incremental distance on either side of the boundary

- **Are EC boundaries correct?**
  - RS (Requirements Specification) faults due to unclear difference between "greater" and "greater or equal"
  - implementation faults between ">" and "<"

Black Box Techniques

bbj Test

BVA: Examples

- **Zero or nil value**
- **Values immediately outside EC boundaries**
- **Additional difficulties for floating-point values**
- **"register person with age 0 - 120"**
  - interesting values are e.g. -1, 0, 1, 119, 120, 121

Black Box Techniques

bbj Test

EP & BVA in Practice

- **Intuitive, aren't they?**
- **BVA requires more test cases than EP**
- **In practice, EP without BVA useless**
  - you would "test whether domain values are processed correctly" but not "whether correct values belong to the domain"
- **How thorough a boundary test should be: three test cases per boundary (lower, boundary and higher) guarantee its correctness (BS 7925-2)**

Black Box Techniques

bbj Test

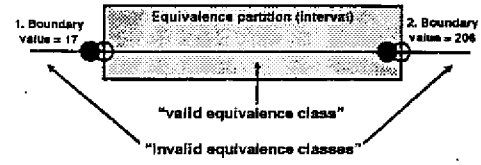
Open and Closed Boundaries
(not required for Foundation level)

17: open boundary (boundary value outside equivalence class); term "exclusive"
206: closed boundary (boundary value inside equivalence class); term "inclusive"
Example: `if (v > 17 && v <= 206)`
`equivalence class`

Black Box Techniques

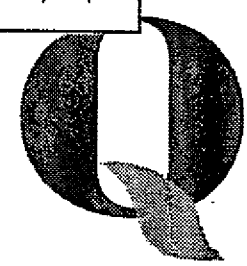
bbj Test

Valid and Invalid EP



Note: this (and following on other slides) diagrams could be simplified by showing boundaries on the edge of the class, disregarding „open" and „closed" boundaries

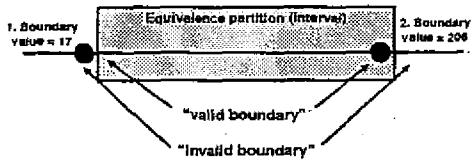
Black Box Techniques



Egzamin V – Grupa słownik, wnioski

bbj Test

Valid and Invalid Boundaries



- "valid boundary" = boundary value (for closed boundaries) or a value near the boundary (for open boundaries) inside EP
- "invalid boundary" = boundary value (for open bousdaries) or a value near the boundary (for closed boundaries) outside EP

Black Box Techniques

bbj Test

Calculation Example 1 (2)

- Test case for valid EP: e.g. 115
- Test cases for invalid EP:s: e.g. 5 and 300
- Test cases for valid BD:s: e.g. 18 and 206
- Test cases for invalid BD:s: e.g. 17 & 207
- Test cases for both valid and invalid EP:s: e.g. 5, 115, 300

Black Box Techniques

bbj Test

Calculation Example 2 (2)

- The number of test cases:
  - for valid EP only: e.g. 115
  - for valid BV only: 18 and 206
  - in this case, #TC for BVA = 2 * (#TC for EC)
  - for valid & invalid EP:s: e.g. 12, 103, 210
  - for valid & invalid BV: 17, 18, 206, 207
  - full BV test: 16, 17, 18, 205, 206, 207

Black Box Techniques

bbj Test

State Transition Testing

BS 7925-1

"A test case design technique in which test cases are designed to execute state transitions"

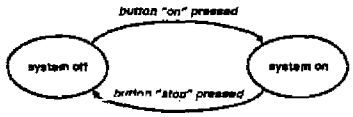
"State transition: a transition between two allowable states of a system or component"

Black Box Techniques

bbj Test

State Transition Model

- Model of the behaviour of a system (SW, SW & HW, HW, mechanical, organisational, legal, biological...)
- Expressed as *states* and *transitions* between states



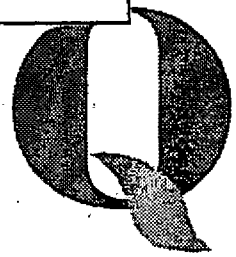
Black Box Techniques

bbj Test

Using Model for Testing

- Creating model (for test purposes) from textual RS finds often many RS faults
- Test cases (sequences of *events causing transitions between states*) can be derived from state transition model
  - to achieve a given state coverage
  - to achieve a given transition coverage ("0-switch")
  - to achieve a given coverage of transition pairs ("1-switch")

Black Box Techniques



bbj Test

2. Principles of Testing
3. Testing throughout the lifecycle
4. Dynamic Testing Techniques
5. Static Testing
6. Test Management
7. Tool Support for Testing

Black and White Box Testing
Black Box Techniques
White Box Techniques
Error-Guessing

bbj Test

White Box - General Approach

- **Test cases are <selected / designed / derived / generated> using <design / code / structure> information, e.g.**
  - there is an input buffer, let's check how it copes with high input load
  - tests to check whether load balancer distributes load correctly
  - there is a loop allocating dynamic memory in this code, let's execute it many times

White Box Techniques

bbj Test

White Box - Code Coverage

- **Systematic, algorithmic approach exists only for *code* coverage**
- **Testing based on code coverage: measure "how much code" is executed running test suite**
- **If too little - expand test suite**
- **Iterate until satisfactory coverage is achieved**

White Box Techniques

bbj Test

Statement Coverage Example 1

```
if (a = 3)
  print "a is 3"
else
  print "a is not 3"
end
if (b = 7)
  print "b is 7"
end
```

TC1: a = 3, b = 5
Coverage = 5/8 = = 62.5%

White Box Techniques

bbj Test

Statement Coverage Example 2

```
if (a = 3)
  print "a is 3"
else
  print "a is not 3"
end
if (b = 7)
  print "b is 7"
end
```

TC1: a = 3, b = 7
Coverage = 6/8 = = 75%

White Box Techniques

bbj Test

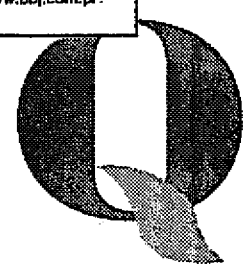
Statement Coverage Example 3

```
if (a = 3)
  print "a is 3"
else
  print "a is not 3"
end
if (b = 7)
  print "b is 7"
end
```

TC1: a = 3, b = 5
TC2: a = 7, b = 7

TC1 + TC2 yield 100% statement coverage

White Box Techniques



bbj Test

Benefits of Code Coverage

- Needed but missing TC:s identified
- Code difficult to test identified - can be inspected instead
- Code difficult to test but not important enough for inspection: risk known
- "Dead code" identified
- Encourages module/developer testing
- Connection TC - code (maintenance)

White Box Techniques

bbj Test

Limitations of Code Coverage

- 100% code coverage:
  - no guarantee that all requirements implemented
  - not all paths through code tested
  - can create false sense of security
- Instrumented code for coverage measurements - tests must be repeated
- Slower test execution
- Difficult on embedded systems

White Box Techniques

bbj Test

Code Coverage Measures 1/3: List of White Box Techniques

- Statement Testing
- Branch/Decision Testing

} described in some detail here

- Data Flow Testing
- Branch Condition Testing
- Branch Condition Combination Testing
- Modified Condition Decision Testing
- LCSAJ Testing

White Box Techniques

bbj Test

Code Coverage Measures 2/3

Branch Testing, Branch Condition Testing & Branch Condition Combination Testing

```
if ((c1) && (c2))
  print "OK!"
end
```

Branch Testing:
- TC1: (c1 && c2) FALSE
- TC2: (c1 && c2) TRUE

Branch Condition Testing:
- TC1: (c1 && c2) FALSE, c1 FALSE, c2 FALSE
- TC2: (c1 && c2) TRUE, c1 TRUE, c2 TRUE

Branch Condition Combination Testing: all combinations thereof

White Box Techniques

bbj Test

Code Coverage Measures 3/3

- **Data Flow Testing:** "test cases are designed based on variable usage within the code"
- **Modified Condition Decision Testing:** "test cases are designed to execute branch condition outcomes that *independently* affect a decision outcome"
- **LCSAJ Testing:** "Linear Code Sequence And Jump; LCSAJ is the start of the linear sequence of executable statements, the end of the linear sequence, and the target line [after jump]"

White Box Techniques

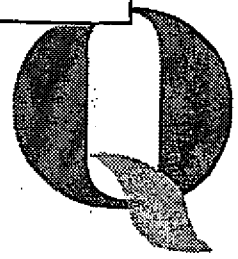
bbj Test

Branch Coverage Example 1/3

```
if (a = 3) //c1
  print "a is 3"
else
  print "a not 3"
end
if (b = 7) //c2
  print "b is 7"
end
```

TC1: a = 3, b = 7
TC2: a = 7, b = 7
TC1 + TC2 yield 100% statement coverage
c1: true & false
c2: true & true
TC1 + TC2 yield 75% branch coverage

White Box Techniques



bbj Test

Branch Coverage Example 2/3

- For sequential code not difference between statement and branch coverage
- If there is code for all control flow paths, the # of test cases needed for SC = # of test cases needed for branch coverage
- If above not true, then the # of test cases needed for SC < # of test cases needed for branch coverage

White Box Techniques

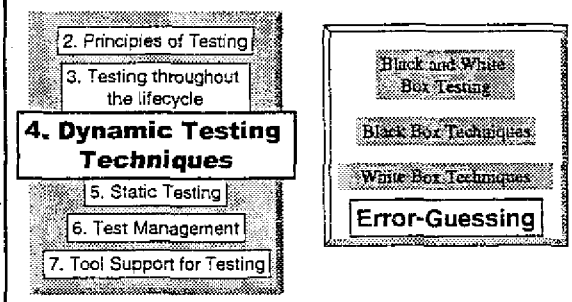
bbj Test

Branch Coverage Example 3/3

- Drawing a control flow graph may make calculating # test cases easier
- Calculating McCabe (cyclomatic complexity) index may give a hint, too:
  - the minimum number of test cases needed to achieve branch coverage of a component is less or equal McCabe index for this component (i.e. never more TC than McCabe index, but sometimes fewer... not very helpful)

White Box Techniques

bbj Test



bbj Test

What Is Error Guessing?

- *Misleading name*
  - should rather be "fault guessing"
  - heuristic, non-systematic test design technique based on previous experience, both usage, technical and project related
- Similar concept to "exploratory testing"
- Relies on testing "art & craft"
- Should be used as complement to systematic techniques

Error Guessing

bbj Test

Enlightened Guesses 1/4

- Visible areas
  - failures which occur in most visible areas are worth detecting, therefore good hunting ground
- Frequently used features
  - faults present in most frequently used areas are more likely to result in failures, therefore it pays to test those areas extra
- Infected areas
  - more faults is likely where many faults already found

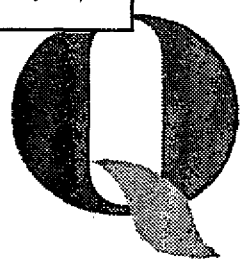
Error Guessing

bbj Test

Enlightened Guesses 2/4

- Complex code
  - e.g. with high McCabe cyclomatic complexity index seem more likely to contain faults; however, no conclusive evidence exists.
- Change intensity
  - relationship between amount of changes and fault intensity exists
  - change management can provide statistics on which areas are most changed

Error Guessing



bbj Test

Enlightened Guesses 3/4

- **New technology**
  - where new solutions, technology or development methods have been introduced, errors and faults are more likely
- **# of people involved**
  - organisational complexity
- **Turnover factor**
  - projects with high (internal or external) personnel turnover

Error Guessing

bbj Test

Enlightened Guesses 4/4

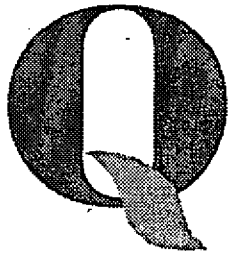
- **Time pressure**
- **Heavily optimised areas (!)**
- **History of numerous defects**
- **Geographically distributed projects**
- **History of user incident reports**
- **Local factors: organisational, social, psychological and cognitive factors**
- **Error guessing = detective work!**

Error Guessing

bbj Test

2. Principles of Testing
3. Testing throughout the lifecycle
4. Dynamic Testing
5. ...
6. Test ...
7. Tool Support for Testing

End of chapter "4. Dynamic Testing Techniques"



bbj Test

2. Principles of Testing
3. Testing throughout the lifecycle
4. Dynamic Testing Techniques
5. Static Testing
6. Test Management
7. Tool Support for Testing

Reviews and the Test Process
Types of Review
Static Analysis

bbj Test

Why Reviews?

- **Faults found earlier are much cheaper to remove – reviews can be performed early when only documents are available**
- **Early testing - using reviews - ensures less faults and failures in late phases: less "dramatic" system testing**
- **Reviews provide additional benefits:**
  - participation of various stakeholders, consensus, information exchange, engagement

Reviews and the Test Process

bbj Test

Caveats of Reviews 1/2

- **Not all reviews are equally effective - some faults (e.g. GUI, source code) may be cheaper to *find* with dynamic testing**
- **The type of review must be suitable for its goal:**
  - no inspection for preliminary sketch
  - no informal review for final architecture review
- **Reviews can be subject to harmful group dynamics**

Reviews and the Test Process

bbj Test

Caveats of Reviews 2/2

- **Reviews can be used as substitute for insufficient communication**
- **Some experts may get overloaded with reviewing**
- **Reviews are dropped when not planned**
- **Reviews may be treated as hinder for "proper work"**
- **Reviews are cognitively demanding**

Reviews and the Test Process

bbj Test

What to Review?

- **Anything:**
  - documentation
  - rough sketches, ideas "on a napkin"
  - source code
  - models, anatomy charts, sequence diagrams
  - user manuals, on-line help
  - test data, test configuration, test specifications
  - test results and logs
- **But it must be somehow written/recorded**

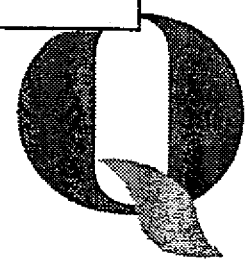
Reviews and the Test Process

bbj Test

How to Perform Reviews 1/2

- **Relatively often - otherwise:**
  - overwhelmingly large documents to review
  - faults get build-in
  - serious faults stay undetected too long
  - subject-matter quickly forgotten
  - too many faults found during one review have demoralising effect
- **Realistic amount - perhaps no more than 15% of total project costs**

Reviews and the Test Process



bbj Test

How to Perform Reviews 2/2

- Some types of large documents can be divided into smaller parts
- Random sampling can be used for some
- Review meetings not too long
- Chosen review type must be followed - requires discipline and commitment
- Appropriate mix of experiences among reviewers; not too many reviewers

Reviews and the Test Process

bbj Test

Review Costs 1/2

- Like testing cost:
  - not the cost of creating objects of reviews
  - the cost of training in review technique(s)
  - the cost of *all* review meetings
  - the cost of individual preparation
  - the cost of result gathering and analysis
  - not the cost of removing faults from the reviewed document
  - the cost of process improvement analysis (if included)

Reviews and the Test Process

bbj Test

Review Costs 2/2

- To keep review costs down:
  - do not waste time by reviewing too early: use entry criteria when appropriate (e.g inspections)
  - do not waste time on inefficient review meetings: cancel if participants not prepared
  - ensure training in review method
- Reviews are not replacement for inefficient communication channels

Reviews and the Test Process

bbj Test

More Review Benefits 1/2

- (see even slide 2 "Why Reviews?")
- Reviews assure documentation quality, which is "traditionally" sloppy as regards quality
- Reviews apply formal, systematic QA procedures on less structured project activities

Reviews and the Test Process

bbj Test

More Review Benefits 2/2

- Review Goals:
  - verification
  - validation
  - consensus
  - improvements
  - fault finding
- Reviews applicable for requirement validation, usability assessment and other "untestable" activities

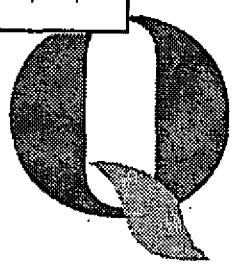
Reviews and the Test Process

bbj Test

Reviews & Process: Summary

- Reviews must be planned to work
- Reviews required trained personnel
- Reviews must not replace other processes (communication, distribution)
- Appropriate review types must be used
- Reviews are the first test method, applicable before any dynamic testing can be used

Reviews and the Test Process



bbj Test

2. Principles of Testing
3. Testing throughout the lifecycle
4. Dynamic Testing Techniques
5. Static Testing
6. Test Management
7. Tool Support for Testing

Reviews and the Test Process
Types of Review
Static Analysis

bbj Test

Review Types and Goals

- **Different review types applicable for different goals, e.g.**
  - formal acceptance: **inspection**
  - early concept checking: **walkthrough**
  - buy-in of an idea: **walkthrough**
  - finding technical faults: **peer review**
  - technical brainstorming: **technical review or walkthrough**
  - quick check: **informal review**
  - decision making: **inspection**

Types of Review

bbj Test

Similarities and Differences

- **All are *reviews***
  - no specific machine support
  - reading (or listening) and controlling
  - comprise a *number of human participants*
  - mainly for documents
- **There are differences in goals and used techniques - see following slides**

Types of Review

bbj Test

Basis of Review Classification

- **Level of formality**
- **Existence or lack of specified roles**
- **Requirements on individual preparation**
- **Requirements on formal procedures (criteria, checklists, roles, documents)**
- **Role of review meeting**
- **Applicable goals**
- **Deliverables**

Types of Review

bbj Test

Walkthroughs

- **The author explains his/her idea going through the document**
- **Reviewers: peer group**
- **Example uses:**
  - dry runs (code reviews)
  - scenarios (e.g. use cases)
- **The author must be well prepared**
- **Reviewers need not be prepared.**

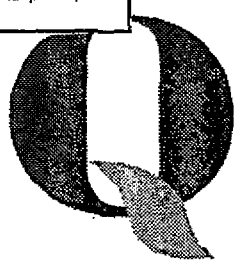
Types of Review

bbj Test

Informal Reviews

- **Undocumented**
- **No formal process need be followed**
- **Benefits:**
  - fast
  - cheap
  - useful to check if the author is on track
- **Dangers:**
  - if more formal review is required, but not used

Types of Review



bbj Test

Technical (Peer) Reviews

- Documented
- Defined process for fault-finding...
- ... but few rules outside fault-finding
- Reviewers: peers and technical experts
- Goal: improvement and quality estimation of a technical document
- No management participation (to avoid "decision pressure")
- Example: CCB (Change Control Board)

Types of Review

bbj Test

Inspection - Definition

Definition of *inspection* according to Gilb & Graham:

"A group review and quality improvement process for written material. It consists of two aspects; product (document itself) improvement and process improvement (of both document production and inspection)"

Types of Review

bbj Test

Inspection - Goals

- Inspection (formal review) - history
  - "Fagan inspections" (1970-s, IBM)
  - Gilb & Graham: enhanced (process improvement added)
- Verification and validation against
  - source specifications
  - standards
- Achieving consensus
- Process improvement proposals

Types of Review

bbj Test

Inspection - Activities 1/2

- Planning
  - "project plan" for the inspection is prepared by the inspection leader
- Overview meeting ("kick off")
  - circa 1 week before review meeting
  - information & distribution: review object, roles, schedule, checklists, other rules
- Individual preparation
  - basic activity, requires most time

Types of Review

bbj Test

Inspection - Activities 2/2

- Review meeting
  - participants' roles clear
  - all participants prepared, else cancelled
- Editing (correction of the document)
- Follow-up
  - verification of corrections, done by insp. leader
- Metrics' analysis
- Process improvement proposals

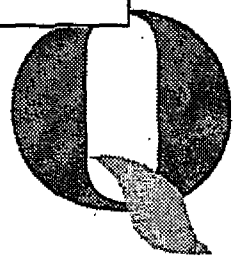
Types of Review

bbj Test

Inspection - Roles 1/2

- Moderator
  - experienced in inspection techniques
  - conducts the meeting
  - often the same person as inspection leader
- Author
  - usually even responsible for secretarial work during inspection meeting and editing the inspected document afterwards

Types of Review



bbj Test

Inspection - Roles 2/2

- **Reviewer (inspector)**
  - main responsibility: individual preparation
- **Manager**
  - "Inspection owner": provides budget and resources for inspections; often PM of the project using inspections
- **Review manager (inspection leader)**
  - "Inspection PM": responsible for planning and control of current inspection

Types of Review

bbj Test

Inspection - Deliverables

- **Product changes**
  - some faults discovered in inspected document (e.g. RS) may lead to product changes
- **Document changes**
  - document faults corrected
- **Source document changes**
  - faults in source documents can be corrected
- **Process improvement proposals**
- **Consensus - decision(s)**

Types of Review

bbj Test

Inspection - Pitfalls 1/2

- **Lack of training**
  - not all participants understand (or accept) the inspection process and "sabotage" it
- **Lack of documentation**
  - some source documents missing (e.g. Integration Plan when Test Plan is inspected)
  - some source documents not yet inspected and approved
  - other review types applicable in such situation

Types of Review

bbj Test

Inspection - Pitfalls 2/2

- **Lack of management support**
  - inspections require considerable resources
- **Failure to improve process**
  - metrics not gathered, "brainstorming" session not performed or its results ignored
- **Group dynamics and organisational politics overshadows inspection**
  - possible lack of motivation among inspection participants

Types of Review

bbj Test

Review Types - Summary

	led by the author	no mgmnt. participation	include technical criteria	fault detection process	undocumented	entry/exit criteria	formal process	include metrics	defined roles	led by moderator
informal review					O					
walkthrough	O									
technical review		O	O	O						
inspection						O	O	O	O	O

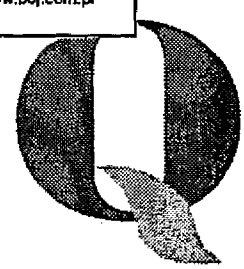
Types of Review

bbj Test

Types of Review: Reality

- **"Pure" inspections seldom used**
- **Companies often have own review classification schemes (and names)**
- **Some standards (e.g. for safety critical systems) require inspection-like reviews**
- **CMM uses the term "peer reviews" for structured and formal reviews**
- **Potential for improvements is large!**

Types of Review



bbj Test

2. Principles of Testing
3. Testing throughout the lifecycle
4. Dynamic Testing Techniques
5. Static Testing
6. Test Management
7. Tool Support for Testing

Reviews and the Test Process
Types of Review
Static Analysis

bbj Test

Definition (BS7925-1)

"Analysis of a program carried out without executing the program"

Static Analysis

bbj Test

Benefits and Limitations

- **Benefits**
  - can be used prior to dynamic testing
  - encourages developer testing
  - can be used to enforce local standards
  - finds potential faults that can be difficult to locate later, especially during maintenance
- **Limitations**
  - many types of faults invisible for static analysis
  - finds mostly "suspected faults", not faults

Static Analysis

bbj Test

Results 1/3

- **Some of these are found by compilers (depends on the language)**
- **Unreachable ("dead") code**
- **Parameter type mismatches**
- **Array bound violations**
- **Faults found by compilers**
- **Program complexity**
- **% of the source code changed**

Static Analysis

bbj Test

Results 2/3

- **Undeclared variables**
- **Uncalled procedures**
- **Graphical representation of code properties:**
  - control flow graph
  - call trees
  - sequence diagrams
  - class diagrams

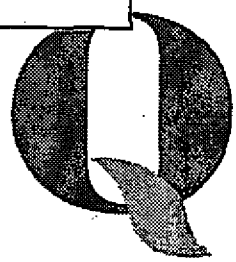
Static Analysis

bbj Test

Results 3/3

- **Data Flow Analysis**
  - definitions with no intervening use (of a variable or another resource like file, device)
  - use of a variable after it is killed
  - use of a variable before it has been assigned any value
  - two value assignments without any intervening use
  - type mismatch in assignments
  - type mismatch in use

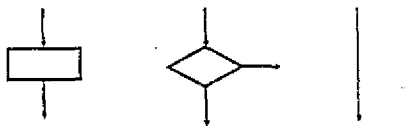
Static Analysis



bbj Test

Flow Charts

Sequential Code | Decision / Branch | Jump

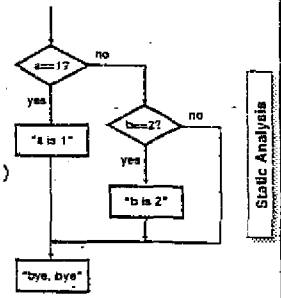


Static Analysis

bbj Test

Flow Chart - Example

```
if (a == 1)
  print("a is 1")
else
  if (b == 2)
    print("b is 2")
  end
end
print("bye, bye")
```



Static Analysis

bbj Test

Complexity Indices

- Lines of Code (LoC) - trivial but useful
- Mc Cabe's Cyclomatic Complexity Index is calculated from a graph of the flow chart of the module:
- General formula: CC = E - N + p
  - E = the number of edges of the graph
  - N = the number of nodes of the graph
  - p = the number of connected components
- Simplified formula: CC = E – N + 1

Static Analysis

bbj Test

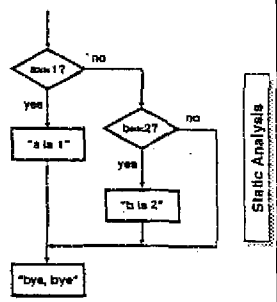
McCabe CCI - Example

CC = E - N + p =
= 4 - 2 + 1 = 3

Simplified formula for graphs where all nodes have 2 edges ("if-branches" only):

CC = # nodes + 1

CC = 2 + 1 = 3



Static Analysis

bbj Test

Complexity - Nesting Levels

```
if (x>5)                    // One nesting level
  print 'big';
else
  print 'small';
endif;

if (x>5)
  if (x<10)
    print 'big unit'; // Two nesting levels
  endif
else
  if (x != 0)
    print 'small unit'; // Two nesting levels
  endif;
endif;
```

Two nesting levels

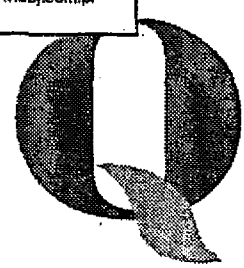
Static Analysis

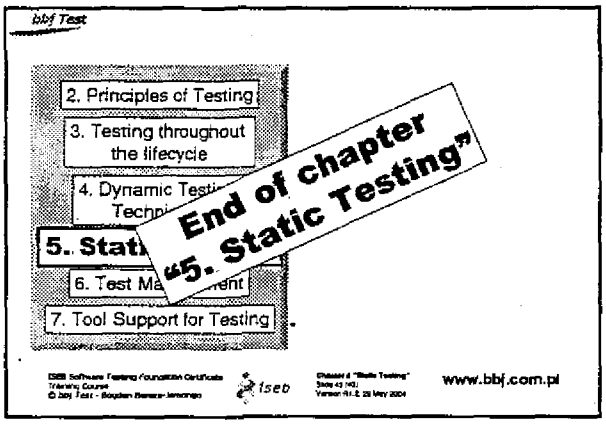
bbj Test

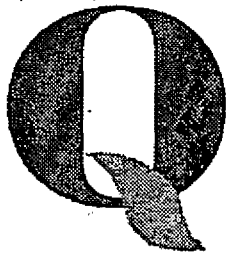
Complexity: Fan-in & Fan-out

- Fan-in: the number of callers (how many procedures call this procedure)
- Fan-out: the number of called procedures
- Procedure with high both fan-in and fan-out
  - changes require considerable regression test
  - *may be bad architecture*

Static Analysis




bbj Test
2. Principles of Testing
3. Testing throughout the lifecycle
4. Dynamic Testi
Techni
5. Stati
6. Test Ma ent
7. Tool Support for Testing
End of chapter
"5. Static Testing"
www.bbj.com.pl



bbj Test

2. Principles of Testing
3. Testing throughout the lifecycle
4. Dynamic Testing Techniques
5. Static Testing
6. Test Management
7. Tool Support for Testing

Organisation
Configuration Management
Test Estimation, Monitoring and Control
Incident Management
Standards for Testing

bbj Test

Different Organisations

- **There is no single 'perfect' test organisation; it depends on**
  - product structure
  - project organisation
  - product's integrity level
- **Defining and implementing better test organisation is part of test process improvement**

Organisation

bbj Test

Developer Testing

- **Programmers test their own code**
- **Benefits**
  - intimate knowledge of implementation details
  - one-person responsibility
- **Disadvantages**
  - *cognitive problems (once mistaken, twice mistaken)*
  - interest conflict (I get promoted for writing code)
  - goal conflict (I want to get rid of this)

Organisation

bbj Test

"Buddy Testing"

- **Programmers test one another's code**
- **Benefits:**
  - code knowledge more spread among programmers
  - mitigated cognitive conflicts
- **Disadvantages**
  - still possible interest conflict
  - still similar focus and perspective
- **Special case: XP (programming in pairs)**

Organisation

bbj Test

One-man Orchestra

- **Tester in programmers' team**
- **Benefits**
  - still more cognitive independence
  - close contact - good communication
- **Risks**
  - group pressure, loyalty conflict
  - lack of peer support for the tester
  - test planning, test specification, testing... too much!

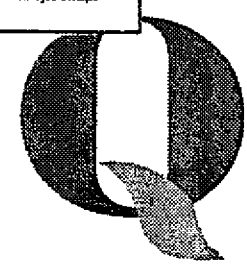
Organisation

bbj Test

Test Team & Consultants

- **Test team**
  - solution typical for system testing
  - allows for rational division of labour
  - provides good experience & knowledge mix
  - risk: insufficient communication
- **Consultants (internal or external)**
  - provide test team with some specialist knowledge part-time (test tool, automation, techniques, user representatives)

Organisation



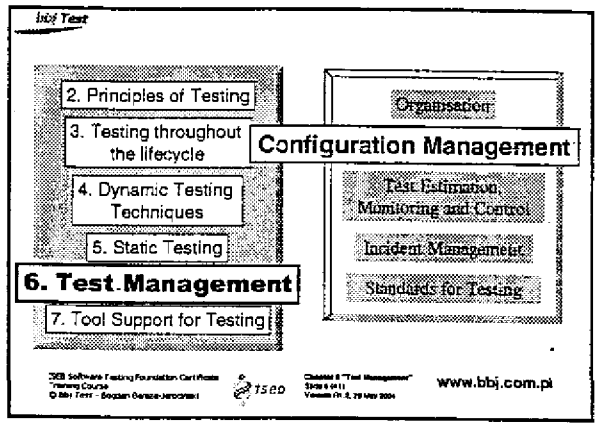
bbj Test

Multi-disciplinary Team

- **A number of various knowledge profiles required (sometimes part-time)**
  - test manager
  - test analyst
  - test automation expert
  - database administrator or designer
  - user interface experts
  - test environment manager
  - test technique experts
  - test tool experts
  - domain expert

Organisation

bbj Test



bbj Test

Symptoms of Poor CM 1/2

- **Which source code version created this object code?**
- **Which compiler version did we use three months ago?**
- **What is the difference between 2.3 and 2.4 source code versions?**
- **Simultaneous (unsynchronised) changes made in source code by 2 programmers**

Configuration Management

bbj Test

Symptoms of Poor CM 2/2

- **Recurrence of bugs**
  - some days later someone uses old code version for linking
- **Conflicting changes**
  - module-A(params1), module-B(params2)
  - change request
  - module-A(params2), module-B(params1)
- **Unauthorised changes**
  - programmer makes a change and does not tell anybody (not the tester, anyway)

Configuration Management

bbj Test

Configuration Items

- **Configuration items examples:**
  - source code file
  - source code file pair (*.h and *.cc)
  - test specification
- **CI identification**
  - unique labels consisting of CI:s name, version number and status indication
  - baseline identification build of CI:s identifications

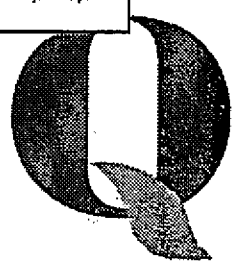
Configuration Management

bbj Test

Configuration Control

- **Maintenance of CI:s in libraries with controlled access**
- **Recording how CI:s change**
- **Establishment of baselines**
  - what CI:s with what versions belong to a particular baseline
- **Change control**
  - who is allowed to make what changes, when and why.

Configuration Management



bbj Test

Status Accounting

- **Change management and tracking**
  - establishing and maintenance of change management procedures (including incident reports) and tools
  - how many change requests exist?
  - what is the status of active change requests?
  - how many change requests / incident reports concerning this CI exist?
  - what is the status of this baseline?

Configuration Management

bbj Test

Configuration Auditing

- **Complete control over status and compliance of all CI:s at all times is not always feasible**
- **Therefore, periodical *configuration audits* may be a better solution**
  - correctness of all CI:s in CM library
  - appropriate status of all relevant CI:s
  - compliance with internal and external standards
  - compliance with CM procedures

Configuration Management

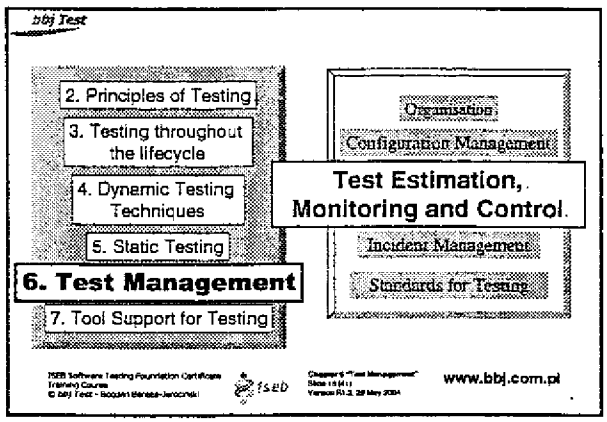
bbj Test

CM in Complex Environments

- **Testware too must be under CM control:**
  - test documentation, test data, test programs, test environment including test tools
- **Complex environments:**
  - distributed development
  - many test environments (each with own versions)
  - distributed change management
  - many product increments and versions

Configuration Management

bbj Test



bbj Test

Test Estimation ≈ Planning 1/2

- **Identify test activities**
- **Estimate time for each activity**
- **Identify resources and skills needed**
- **In what order should the activities be performed?**
- **Identify for each activity**
  - start and stop date
  - resources to perform the job

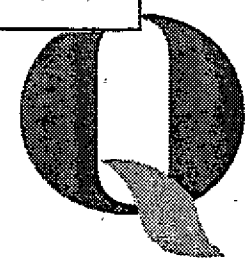
Test Estimation, Monitoring and Control

bbj Test

Test Estimation ≈ Planning 2/2

- **Unknown number of found faults**
  - require time-consuming localisation
  - may require access to test environment
- **Re-test and regression test needed**
  - number of deliveries to test
  - time required for unplanned-for regression testing
- **Quality of tested SW**
  - if too low testing itself takes longer time

Test Estimation, Monitoring and Control



bbj Test

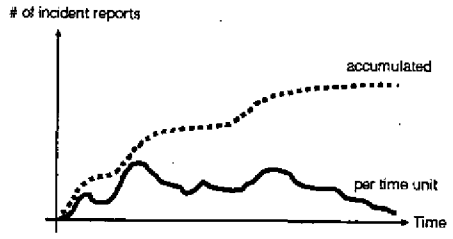
Test Monitoring: Metrics

- **What will be measured**
  - measurement means cost and difficulties
  - metrics easy to get but useless
- **Measurement method**
  - must not be too time-consuming
  - appropriate tool may help
- **Tools**
  - test management tools, incident report statistics, spreadsheet for more metrics

Test Estimation, Monitoring and Control

bbj Test

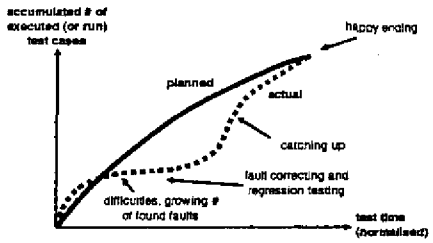
Test Measurements 1/3



Test Estimation, Monitoring and Control

bbj Test

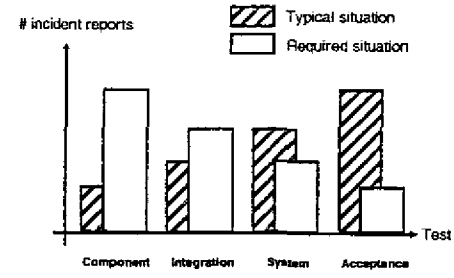
Test Measurements 2/3



Test Estimation, Monitoring and Control

bbj Test

Test Measurements 3/3



Test Estimation, Monitoring and Control

bbj Test

Reporting Deviations

- **Graphs and diagrams more efficient than numbers**
- **Accumulated values more informative than numbers per time unit**
- **False conclusions if calendar time is used instead of normalised**
- **Different granularity of reporting, depending on organisational level**

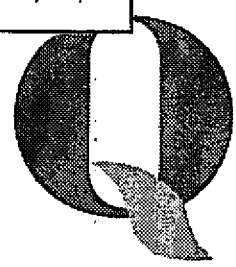
Test Estimation, Monitoring and Control

bbj Test

POWER: Test Control 1/3

- **Waiting for late delivery**
  - reviews of test specifications
  - test environment improvement
- **No faults found**
  - improving test case suite?
  - stopping testing before planned date?
- **Bermuda triangle**
  - time - quality - functionality

Test Estimation, Monitoring and Control



bbj Test

POWER: Test Control 2/3

- **Re-organisation - examples**
  - testers help developers debug
  - developers help testers configure and test
  - almost no time left - do exploratory testing
- **Time plan changes - examples**
  - test case prioritisation and partial execution
  - release / delivery delayed
  - testing in increment 1 only, increment 2 will have to wait longer

Test Estimation, Monitoring and Control

bbj Test

POWER: Test Control 3/3

- **Test environment changes - examples**
  - parallel testing on double environment
  - adding tools for easier fault localisation
  - execution with / on simulator instead
- **Regression test modifications**
  - less frequent deliveries to testing
  - not full regression test suite for every delivery
  - higher entry criteria with "smoke test"

Test Estimation, Monitoring and Control

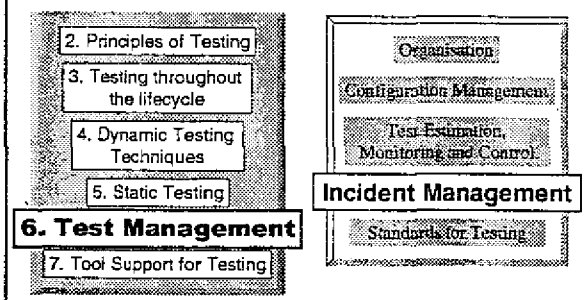
bbj Test

Test Lead / Manager

- **Test Lead**
  - manages a test subproject
  - planning, estimation, monitoring and control
  - post-project analysis
- **Test Manager**
  - manages test department
  - distribute resources among projects
  - ensure training
  - ensure tools, competence and environment

Test Estimation, Monitoring and Control

bbj Test



bbj Test

What Are 'Incidents'?

"An incident is any significant, unplanned event that occurs during testing that requires subsequent investigation and/or correction"

- **Incidents are raised when expected and actual test results differ**
- **Incidents may depend on many factors: from SW fault to tester error**

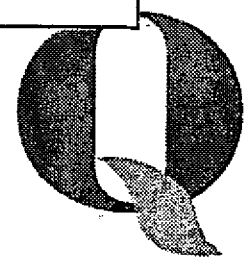
Incident Management

bbj Test

When & against Whom?

- **Anytime, i.e. from the beginning of the project (and not only after dynamic testing has begun)**
- **Can be raised against:**
  - SUT, testware, test environment, all documents
- **Should be logged when someone other than the author of the SUT performs the testing**

Incident Management



bbj Test

Incident Analysis

- **Possible decisions on an incident report:**
  - this is not a SUT fault, tester's error
  - this is not a SUT fault, test fault - re-classify this report
  - cannot be reproduced - investigate
  - this was not a failure, re-classify report to indicate RS fault
  - correct and verify
  - postpone

Incident Management

bbj Test

Contents of Incident Reports 1/2

- **Detailed incident description**
- **Product version**
- **Test specification version**
- **Test environment version and configuration**
- **Failure cause - detailed fault description**
- **Decision concerning fault**

Incident Management

bbj Test

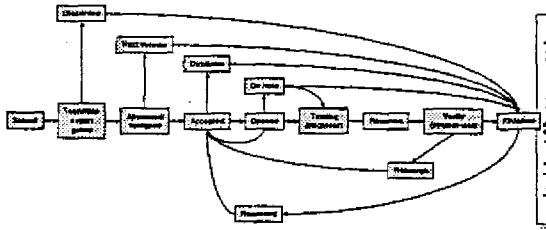
Contents of Incident Reports 2/2

- **Who and when corrects the fault....**
- **... or other decisions**
- **Correction performed?**
- **Re-test result**
- **Regression test result**
- **Connections to other incident reports?**
- **Log, screen dumps etc.**

Incident Management

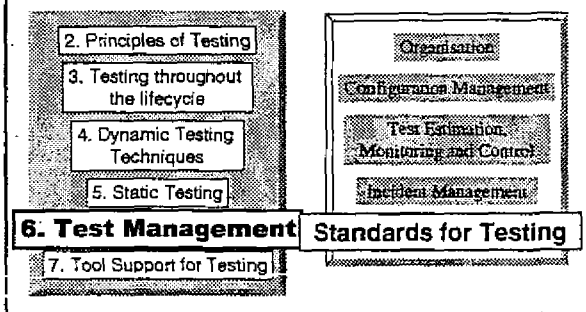
bbj Test

Incident Tracking - Example



Incident Management

bbj Test

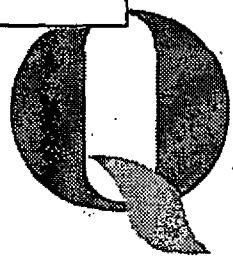


bbj Test

How To Use Standards

- **Unless compliance with a standard is required, it need not be a goal in itself**
- **Standards are good as checklists for creating own test process**
- **Appropriate standards should be used**
  - e.g. not a standard for safety-critical systems used for testing low-integrity, local software
- **Remember standards are not consistent and often overlap**

Standards for Testing



bbj Test

Terminology Standards

- **IEEE 610**, Standard Computer Dictionary
  - very comprehensive, over 200 pages of definitions
- **IEEE 610.12**, Software Engineering Terminology
- **BS 7925-1**, Software Testing Vocabulary
  - British standard, defines what has been omitted in IEEE 610.12

Standards for Testing

bbj Test

QA Standards 1/2

Contain only little about SW testing!

- **ISO 9000-3**
  - application of ISO 9000 to information systems
- **ISO 9001**, Quality systems
- **IEEE 730**, Software Quality Assurance Plans
- **ISO 12207**, Software life cycle processes

Standards for Testing

bbj Test

QA Standards 2/2

- **IEEE 1044**, Classification for Software Anomalies (faults, failures)
- **IEEE 1209**, Recommended Practice for the Evaluation and Selection of CASE Tools
- **IEC 60300-3-9**, Dependability management
  - this part refers to risk analysis
- **ISO 15026**, System and software integrity levels
  - how to define integrity levels

Standards for Testing

bbj Test

Testing Standards

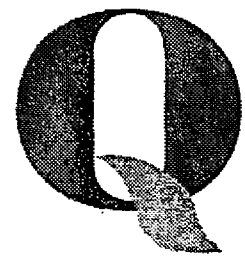
- **IEEE 1008**, Software Unit Testing
  - BS 7925-2 is more complete and modern
- **IEEE 1012**, Software Verification and Validation
  - general standard for verification and validation
- **IEEE 829**, Test Documentation
- **IEEE 1028**, Software Reviews
  - describes various review methods and techniques

Standards for Testing

bbj Test

2. Principles of Testing
3. Testing throughout the lifecycle .
4. Dynamic Testi... Techni...
5. ...
6. Test ...gement
7. Tool Support for Testing

End of chapter "6. Test Management"



bbj Test

2. Principles of Testing
3. Testing throughout the lifecycle
4. Dynamic Testing Techniques
5. Static Testing
6. Test Management
7. Tool Support for Testing

Types of CAST Tools
Tool Selection and Implementation

bbj Test

Requirements Testing Tools

- **Requirements modelling**
  - easier requirements validation if appropriate model used
- **Requirements (model) verification (consistency, animation)**
- **Requirements tracking**
  - between various requirements levels
  - between requirements and test cases
  - between requirements and product versions

Types of CAST Tools

bbj Test

Static Analysis Tools

- **Example: warnings from compilers**
- **Data flow faults and "suspects"**
- **Dead code**
- **Access outside array boundaries**
- **Complexity measurements**
- **Models, graphical presentations:**
  - class diagrams, call trees, control flow, sequence diagrams

Types of CAST Tools

bbj Test

Test Design Tools

- **Test case generation from requirements specification / model**
- **From source code: generation of**
  - stubs
  - drivers
  - harnesses
- **Generation of test programs from (formal) test specifications**

Types of CAST Tools

bbj Test

Test Data Preparation Tools

- **Large amounts of input and expected output data**
  - both for manual and automatic testing
- **Generation of random data**
- **Manipulation and editing of data**
- **Extracting data from existing databases**
- **Data conversion between various formats**

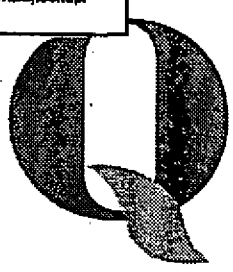
Types of CAST Tools

bbj Test

Test Running Tools

- **For automatic test execution, controlled by programs ("scripts")**
- **Comprise:**
  - application of test inputs
  - registration of actual outputs produced by SW under test
  - comparison of actual and expected outputs
  - logging of activities and registration of test results
- **Commercial or custom-developed**

Types of CAST Tools



bbj Test

Capture-replay Tools 1/2

- "Capture-replay" or "capture-playback"
- Comprise two parts:
  - test running tool (the "replay" part)
  - generation of test programs by recording (capturing) of manually performed tests (both inputs and chosen actual outputs)
- Most popular commercial test tools
- Typically for standard GUI

Types of CAST Tools

bbj Test

Capture-replay Tools 2/2

- Four levels of test program architecture:
  - captured
  - structured
  - data-driven
  - keyword-driven
- When to use "capture"
  - when lead time at the beginning is essential
  - when no programmers are available
  - when very little maintenance is expected

Types of CAST Tools

bbj Test

Character-based Running Tools

- For dumb-terminal applications (still quite common in some businesses)
- Captures keystrokes
- Captures screen responses and stores them as expected outputs for future comparisons
- Captured procedures stored in programmable programs ("scripts")
- Data in programs or separate files

Types of CAST Tools

bbj Test

GUI Test Running Tools

- Captures, then simulates:
  - mouse movements and clicks, keyboard inputs
- Captures, then recognises:
  - GUI objects (buttons, windows, fields, lists)
  - Statuses of GUI objects (like active, inactive)
  - bitmap images
- Which GUI objects are stored and used in comparisons can be chosen during recording

Types of CAST Tools

bbj Test

Test Harnesses and Drivers

- Test driver: running tests by direct invocation of function(s) or subsystem(s)
- Test harness: enables unattended running of groups of test programs
  - which means test harness is somewhere between typical test running program and test management program
- Simulators: enable testing when parts of SUT (SW or HW) are missing or when target testing is dangerous or expensive

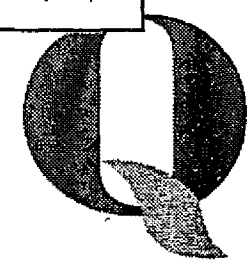
Types of CAST Tools

bbj Test

Performance Test Tools 1/2

- Performance testing:
  - load generation
  - performance measurement (response, transaction times)
- Load generation:
  - through interface(s)
  - using drivers
  - simulating many simultaneous users
  - simulating different user profiles

Types of CAST Tools



bbj Test

Performance Test Tools 2/2

- **Performance measurements:**
  - end-to-end response times
  - internal processing times
- **Graphs load / performance**
- **Performance test tools used during:**
  - pre-system testing to verify architecture
  - system test to validate performance requirements
  - during operation for performance monitoring

Types of CAST Tools

bbj Test

Dynamic Analysis Tools

- **Used for monitoring execution (during test or operation)**
- **May be part of OS (resource monitoring: memory, processes, CPU, I/O)**
- **Testing for absence of „unintended side-effects" such as:**
  - missing de-allocation of memory (memory leaks)
  - unassigned pointers
  - illegal memory accesses

Types of CAST Tools

bbj Test

Debugging Tools

- **Tools that allow during execution:**
  - changing and examining memory contents
  - setting instruction breakpoints
  - setting data access breakpoints (HW debugger)
- **Mainly programming tools used for fault localisation ("debugging")**
- **Can be useful for module testing**
- **Can be used as simulators**

Types of CAST Tools

bbj Test

Comparison Tools

- **To detect differences between actual and expected outcomes**
- **Commercial test running tools usually have built-in comparison tools**
- **Often custom-built to perform comparisons on custom data formats**
- **Filtering capabilities for "advanced" comparisons (only part of data compared)**

Types of CAST Tools

bbj Test

Test Management Tools 1/2

- **Testware management:**
  - creation and control of test documentation
  - storage and management of test result documentation (logs and reports)
- **Test project management:**
  - task scheduling
  - result logging
  - result statistics, graphs (i.e. # of runs versus planned tests, # incident reports)

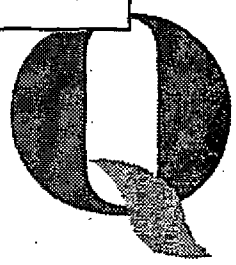
Types of CAST Tools

bbj Test

Test Management Tools 2/2

- **Incident management tools**
  - archiving of incident reports
  - statistics of incident reports
  - status tracking, assignment and monitoring of incident reports
- **Commercial test management tools**
  - work with test running tools from same vendor
  - support test case structuring (levels, dependencies)

Types of CAST Tools



bbj Test

Coverage Measurement Tools

- Three-step tools
  - target program instrumentation
  - logging coverage data during execution
  - analysis and presentation of logged coverage data
- Language and coverage type dependent
- Slow down test execution
- Tests run to measure coverage must be re-run without instrumentation
- Special tools for embedded systems

Types of CAST Tools

bbj Test

bbj Test

Which Activities to Automate?

- Repeatable (like regression testing)
- Stable (i.e. when SUT does not change)
- Time-consuming (multiple data entry)
- Error-prone (e.g. file comparison)
- In other words, "boring" activities!
- In other words, where investment in automation is profitable
- Not necessarily test execution

Tool Selection and Implementation

bbj Test

"CAST Readiness"

- Established test process
- Existing test specifications
- When considering execution automation:
  - incident reporting already uses tools
  - CM using tools
  - (partially) automated build
- Otherwise: "automated chaos becomes more and faster chaos"!

Tool Selection and Implementation

bbj Test

Tool Benefits

- Faster test execution
- Continuous test execution (24x7x52)
- Stable quality of test execution (no human factors - like boredom - involved)
- More exact measurements possible
- "Invisible" outcomes can be measured
- Liberation of human testing resources
- Require disciplined test process

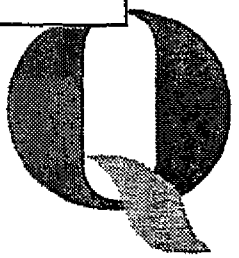
Tool Selection and Implementation

bbj Test

Dangers of Automation

- Underestimated deployment costs:
  - licences, training courses, gaining experience, unexpected technical difficulties
- Underestimated cost of test programs maintenance
- Lack of programming knowledge
- Lack of resources - initially more work during tool introduction than before

Tool Selection and Implementation



bbj Test

Tool Requirements 1/2

- **Tool execution platform**
- **HW requirements and their cost**
- **Integration with existing tools**
- **Integrated toolkits offered by many vendors:**
  - maybe very good
  - maybe unnecessary
  - integration *between* vendors may be an option

Tool Selection and Implementation

bbj Test

Tool Requirements 2/2

- **Integration with existing test process**
- **Interfaces, standard or custom components**
- **Asynchronous execution, interrupt and failure handling**
- **The way tool will be used (once, in many projects?) and programming capabilities (language, captured, structured etc.)**

Tool Selection and Implementation

bbj Test

Tool Selection Process 1/2

- **Creation of a candidate tool shortlist**
  - considering too many similar tools may be a major and expensive undertaking
  - vendors' descriptions not easily comparable
  - describe tools in own terms to facilitate this
- **Arranging demos - preferably:**
  - in your test environment
  - with your real application
  - with technical expertise on your and vendor's side

Tool Selection and Implementation

bbj Test

Tool Selection Process 2/2

- **Evaluation(s) of selected tool(s)**
  - evaluation licences may be a good option
  - let it take enough time
  - ensure participation of all your stakeholders
- **Review and select tool**
  - sometimes, building own custom tool is better
  - consider even non-technical factors: licence policy, availability of support, vendor stability
  - consider long-term profit and repercussions

Tool Selection and Implementation

bbj Test

Pilot Project

- **To minimise loss in case procurement decisions was actually wrong**
- **Teething problems: limit their impact on schedules**
- **Create knowledge base for future reference**
- **Identify necessary test process changes**
- **Asses benefits and costs again**

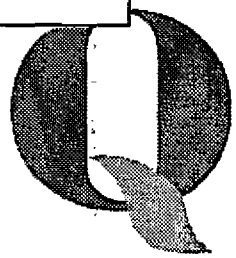
Tool Selection and Implementation

bbj Test

Tool Roll-out

- **Based of successful pilot project**
- **Pilot project success must be advertised**
- **... to ensure resources and management and user support and commitment**
- **Knowledge gathered during pilot must be made easily available**
  - internal hands-on training can be beneficial
- **Prepare support organisation ->**

Tool Selection and Implementation



bbj Test

Tool Maintenance

- → **support organisation:**
  - receive and manage produced testware
  - make routine library available and documented
  - support projects with expertise to minimise automation overhead
- **Methodology development beyond project scope:**
  - keyword driven automation?
  - gathering metrics to assess automation success

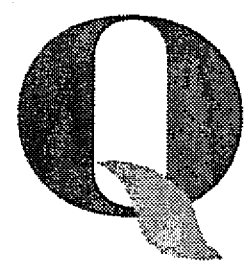
Tool Selection and implementation

bbj Test

2. Principles of Testing
3. Testing throughout the lifecycle
4. Dynamic Testi… Techni…
…ent

End of chapter "7. Tool Support for Testing"

7. T… Support for Testing



Technical Guidance Note S0.01
IPPC General Sector Guidance

2.11 Likwidacja zakładu

Plan likwidacji zakładu powinien zawierać:

- sposób usunięcia niebezpiecznych substancji ze zbiorników i rurociągów oraz ich całkowitego opróżnienia;
- sposób uzgadniania z Agencją planów rozmieszczenia wszystkich zbiorników i rurociągów podziemnych oraz ich aktualizacji;
- metody i środki niezbędne do oczyszczenia łagun;
- metody zapewnienia, że składowiska odpadów zlokalizowane na terenie zakładu będą spełniać wymagania equivalent of surrender conditions;
- usunięcie azbestu i innych potencjalnie szkodliwych materiałów, chyba, że nastąpią uzgodnienia z następnym właścicielem;
- metody rozbiórki budynków i innych konstrukcji
- badania gruntu prowadzone w celu ustalenia stopnia w jakim działanie zakładu spowodowało jego zanieczyszczenie oraz ewentualnej potrzeby przeprowadzenia rekultywacji do stanu zapisanego w raporcie stanu środowiska.

Technical Guidance Note S0.01
IPPC General Sector Guidance

2.12 Zagadnienia ogólne

Możliwe działania są uzależnione od typu prowadzonej działalności i warunków lokalnych. Mogę obejmować:

- uwzględnienie ekonomii skali i wprowadzenie skojarzonej produkcji energii (elektrociepłownie);
- wykorzystanie odpadów o wysokiej wartości opałowej i budowa wspólnej instalacji do ich wykorzystania energetycznego;
- wykorzystania odpadów wytwarzanych przez jednego operatora jako surowców dla pozostałych operatorów;
- wykorzystanie oczyszczonych ścieków wytwarzanych przez jednego operatora jako źródła zaopatrzenia w wodę dla pozostałych operatorów;
- budowa wspólnej oczyszczalni ścieków umożliwiającej wyższy stopień oczyszczania;
- wspólne działania mające na celu eliminowanie ryzyka wystąpienia sytuacji awaryjnej mogącej mieć wpływ na pozostałych operatorów;
- działania mające na celu eliminowanie sytuacji, w których zanieczyszczenia gruntu przez jednego z operatorów wpływają na pozostałych – odpowiednie ekonomizowania w zakresie własności gruntu.

Technical Guidance Note S0.01
IPPC General Sector Guidance

2.10 Monitorowanie

2.10. 2. Monitorowanie stanu środowiska

Należy monitorować emisje odpadów i zapisywać następujące informacje:

- fizyczny i chemiczny skład odpadów;
- charakterystyka szkodliwości odpadów;
- środki ostrożności i substancje, z którymi określone odpady nie powinny być mieszane.

- Jeżeli odpady są bezpośrednio składowane w ziemi, np. rozrzucanie osadów ściekowych lub składowiska odpadów, należy opracować programy *monitorowania w przypadku uwzględniające potencjalne zanieczyszczenia i* ścieżki migracji zanieczyszczeń z ziemi do wód gruntowych, wód powierzchniowych lub łańcucha pokarmowego.

eko-net.pl

Technical Guidance Note S0.01
IPPC General Sector Guidance

2.10 Monitorowanie

2.10. 3. Monitorowanie parametrów procesu

Parametry procesu, które mają potencjalny związek z oddziaływaniem na środowisko powinny zostać zidentyfikowane i odpowiednio monitorowane. Przykładami mogą być:

- monitorowanie surowców pod względem zawartości substancji zanieczyszczających;
- wydajność zakładu tam, gdzie ma to związek z oddziaływaniem na środowisko;
- zużycie energii w zakładzie i w poszczególnych miejscach zużycia zgodnie z planem energetycznym.
- zużycie wody pitnej w całym zakładzie i w poszczególnych punktach poboru powinno być monitorowane jako część planu wydajności zużycia wody.

eko-net.pl

Technical Guidance Note S0.01
IPPC General Sector Guidance

2.11 Likwidacja zakładu

Działania, które należy podjąć na etapie projektowania i budowy:

- należy unikać budowy zbiorników i rurociągów podziemnych a gdy nie jest to możliwe trzeba wyposażyć je w podwójny płaszcz lub odpowiedni program nadzoru.;
- w projektowaniu należy uwzględnić możliwość całkowitego opróżnienia i wyczyszczenia zbiorników i rurociągów przed rozbiórką;
- projektowanie lagun i składowisk odpadów stałych powinno uwzględniać ich *zamknięcie i zagospodarowanie;*
- należy stosować materiały izolacyjne dające się łatwo usunąć bez emisji pyłów i zagrożenia dla pracowników;
- należy stosować materiały nadające się do odzysku

eko-net.pl

Technical Guidance Note S0.01
IPPC General Sector Guidance

2.8 Sytuacje awaryjne i ich skutki

Operator powinien zidentyfikować zagrożenia dla środowiska, jakie stwarza instalacja. Przede wszystkim należy uwzględnić (ale nie ograniczać się tylko do nich) następujące obszary:

- przenoszenie substancji (np. załadunek i rozładunek zbiorników)
- przepełnianie zbiorników,
- awarie instalacji i/lub urządzeń (np.: zbyt wysokie ciśnienie w zbiornikach i rurociągach, niedrożność kanalizacji);
- awarie urządzeń chroniących przed rozlewami (np. obwałowań lub studzienek kanalizacyjnych),
- możliwość zatrzymania wód pogaśniczych;
- niewłaściwe podłączenia do kanalizacji lub innych instalacjach;
- zapobieganie kontaktom substancji stanowiących zagrożenie w przypadku zmieszania się ze sobą;
- niepożądane reakcje i/lub reakcje niekontrolowane;
- zrzut ścieków przed sprawdzeniem ich składu chemicznego;
- skutki wandalizmu.

Technical Guidance Note S0.01
IPPC General Sector Guidance

2.9 Hałas i wibracje

Operator powinien przedstawić następujące informacje:

- Główne źródła hałasu i wibracji
- Okresowe źródła hałasu i wibracji
- Najbliższe lokalizacje wrażliwe na hałas
- Szczegóły dotyczące pomiarów hałasu w środowisku
- Techniki nadzoru nad emisją hałasu

Technical Guidance Note S0.01
IPPC General Sector Guidance

2.10 Monitorowanie

2.10. 1. Monitorowanie emisji zanieczyszczeń

2.10. 1.1. Monitorowanie emisji zanieczyszczeń do kanalizacji i wód

Dla większości zakładów zrzucających ścieki do wód i kanalizacji należy prowadzić pomiary przynajmniej następujących parametrów:

- Natężenie przepływu
- Odczyn [pH]
- Temperatura
- ChzT/BzT
- Ogólny węgiel organiczny
- Mętność
- Tlen rozpuszczony

Technical Guidance Note S0.01
IPPC General Sector Guidance

2.10 Monitorowanie

2.10. 1. Monitorowanie emisji zanieczyszczeń

2.10. 1.1. Monitorowanie emisji zanieczyszczeń do kanalizacji i wód cd.

Ponadto operator powinien przeprowadzać pełniejszą analizę obejmującą szerokie spektrum substancji w celu ustalenia czy wszystkie istotne substancje zostały uwzględnione podczas określania dopuszczalnych parametrów ścieków. Pomiary te powinny być prowadzone przynajmniej raz w roku.

Również inne, nie wymienione substancje, które mogą zagrażać środowisku w wyniku prowadzonej działalności, powinny podlegać regularnemu monitoringowi. Dotyczy to przede wszystkim pestycydów i metali ciężkich.

Technical Guidance Note S0.01
IPPC General Sector Guidance

2.10 Monitorowanie

2.10. 1. Monitorowanie emisji zanieczyszczeń

2.10. 1.2. Monitorowanie emisji zanieczyszczeń do powietrza

Istnieje wiele zróżnicowanych emisji do powietrza i dokładna informacje można znaleźć w istniejących wytycznych technicznych. Ogólnie:

- ciągle monitorowanie jest konieczne tam, gdzie emisje są znaczące oraz tam, gdzie jest to niezbędne dla utrzymania nadzoru nad emisjami;
- aby odnieść stężenia do ładunku zanieczyszczeń niezbędny jest pomiar (lub inny sposób jego określania) przepływu gazów odlotowych;
- aby odnieść wyniki pomiarów do warunków normowych należy określać i odnotowywać następujące parametry:
  - temperatura
  - zawartość tlenu tam, gdzie emisje są wynikiem procesów spalania
  - zawartość pary wodnej tam, gdzie emisje są wynikiem procesu spalania lub w przypadku występowania wilgotnych gazów odlotowych. Nie jest to konieczne w przypadku, gdy zawartość pary wodnej nie może przekroczyć 3% objętościowo lub wtedy, gdy techniki pomiarowe pozwalają uzyskać wynik niezależnie od wilgotności gazów odlotowych.

Technical Guidance Note S0.01
IPPC General Sector Guidance

2.10 Monitorowanie

2.10. 1. Monitorowanie emisji zanieczyszczeń

2.10. 1.3. Monitorowanie odpadów.

- Należy monitorować emisje odpadów i zapisywać następujące informacje:
  - fizyczny i chemiczny skład odpadów;
  - charakterystyka szkodliwości odpadów;
  - środki ostrożności i substancje, z którymi określone odpady nie powinny być mieszane.
- Jeżeli odpady są bezpośrednio składowane w ziemi, np. rozrzucanie osadów ściekowych lub składowiska odpadów, należy opracować programy monitorowania w przypadku uwzględniające potencjalne zanieczyszczenia i ścieżki migracji zanieczyszczeń z ziemi do wód gruntowych, wód powierzchniowych lub łańcucha pokarmowego.

koszt

Pozwolenia zintegrowane

Art. 210. 1. Warunkiem rozpatrzenia wniosku o wydanie pozwolenia zintegrowanego jest wniesienie opłaty rejestracyjnej na wyodrębniony rachunek bankowy prowadzony przez ministra właściwego do spraw środowiska.

3. Wysokość opłaty rejestracyjnej nie może być wyższa niż 3.000 EURO.

4. Minister właściwy do spraw środowiska określi, w drodze rozporządzenia, wysokość opłat rejestracyjnych, kierując się zakresem dokumentacji niezbędnej do wydania pozwolenia ze względu na skalę i rodzaj działalności prowadzonej w instalacjach oraz koniecznością zgromadzenia środków umożliwiających wykonywanie zadań, o których mowa w art. 206 i 212.

eko-net.pl

Pozwolenia zintegrowane

Wysokość opłaty rejestracyjnej, z zastrzeżeniem § 3, oblicza się według następującego wzoru:

$$O = B \times W_R / W_P$$

gdzie:

O – oznacza wysokość opłaty rejestracyjnej,

B – oznacza wysokość bazowej stawki opłaty dla danego rodzaju instalacji,

W_R – oznacza maksymalną teoretyczną (możliwą teoretycznie do osiągnięcia) wielkość parametru charakteryzującego skalę działalności prowadzonej w danej instalacji,

W_P – oznacza progową wielkość parametru charakteryzującego skalę działalności prowadzonej w instalacji danego rodzaju.

eko-net.pl

Pozwolenia zintegrowane

Dla przetwórstwa mleka

B = 700 Euro

W_P = 500 t/dobę

Jeżeli na terenie zakładu położona jest więcej niż jedna instalacja tego samego rodzaju, to wskaźnik (W_R) określa się jako sumę maksymalnych teoretycznych wielkości parametrów charakteryzujących skalę działalności poszczególnych instalacji.

Jeżeli wielkość wskaźnika (W_R) jest mniejsza bądź równa wielkości wskaźnika (W_P), to wysokość opłaty rejestracyjnej jest równa bazowej stawce opłaty.

Jeżeli obliczona wysokość opłaty rejestracyjnej jest wyższa niż 3.000 euro, to opłatę wnosi się w wysokości równoważnej 3.000 euro.

eko-net.pl

Pozwolenia zintegrowane

Organem właściwym do wydawania pozwoleń zintegrowanych jest:

wojewodą - dla instalacji, która jest kwalifikowana jako przedsięwzięcie mogące znacząco oddziaływać na środowisko, dla którego sporządzenie raportu o oddziaływaniu przedsięwzięcia na środowisko jest obowiązkowe,

starosta - w pozostałych przypadkach. (art. 378)

Dokumenty Referencyjne BAT

Szczegółowe wytyczne opisujące Najlepsze Dostępne Techniki opracowywane są przez Europejskie Biuro IPPC (EIPPCB) w Sewilli. Dokumenty referencyjne BAT (BREFs, BREF Notes, BAT Reference Notes) mają w skali UE dawać podstawę do sporządzania wniosków o wydanie pozwolenia zintegrowanego.

Dokumenty Referencyjne BAT

- *Komisja Europejska zleciła European IPPC Bureau* w Sewilli opracowanie wytycznych (tzw. BAT Reference Notes-BREF) dla poszczególnych procesów podlegających Dyrektywie.
- W tym celu EIPPCB analizuje informacje dotyczące prowadzenia procesów przemysłowych na całym świecie.
- Dokumenty BREF mają zawierać szczegółowe informacje pozwalających na określenie bieżących poziomów BAT i odpowiadających im limitów emisyjnych.

Technical Guidance Note S0.01
IPPC General Sector Guidance

2.5. Gospodarka odpadami

Ogólne zasady dotyczące określania ilości, składowania i zagospodarowywania odpadów:

- Należy wprowadzić i utrzymywać system rejestrowania ilości, właściwości, pochodzenia oraz (gdzie to uzasadnione) przeznaczenia, częstotliwości zbiórki, środków transportu i metod unieszkodliwiania odpadów przeznaczonych do gospodarczego wykorzystania lub unieszkodliwienia.
- W każdym przypadku, kiedy jest to możliwe odpady powinny być segregowane. Dla każdego rodzaju odpadu należy określić drogę unieszkodliwienia, która powinna być jak najkrótsza tj. najbliższa punktowi wytwarzania odpadów;
- Informacje o wszystkich odpadach wysłanych poza teren zakładu powinny być rejestrowane;
- Miejsca składowania odpadów powinny być zlokalizowane z dala od cieków wodnych i granic obszarów wrażliwych np. obszarów użyteczności publicznej i zabezpieczone przez wandalizmem;
- Obszary składowania odpadów powinny być wyraźnie wyznaczone i oznakowane, a pojemniki powinny być wyraźnie opisane;

Technical Guidance Note S0.01
IPPC General Sector Guidance

2.5. Gospodarka odpadami

Ogólne zasady dotyczące określania ilości, składowania i zagospodarowywania odpadów (cd.)

- Należy określić maksymalną objętość magazynowania dla obszarów składowania odpadów, która nie powinna być przekroczona. Należy także określić maksymalne okresy magazynowania pojemników;
- Należy zapewnić odpowiednie urządzenia do magazynowania szczególnych odpadów np. substancji łatwopalnych, wrażliwych na ciepło lub światło. Poszczególne rodzaje odpadów powinny być składowane osobno;
- Pojemniki służące do przechowywania odpadów powinny być zamknięte stosownymi pokrywami, zamknięciami, zaworami zabezpieczającymi. *Dotyczy to również pustych pojemników.*
- Pojemniki te powinny podlegać regularnym inspekcjom;
- Należy opracować procedury postępowania w przypadku wykrycia uszkodzonego lub nieszczelnego pojemnika;
- Należy podjąć właściwe kroki, aby zapobiec emisji (np. cieczy, pyłów, lotnych związków organicznych i zapachów) ze składowania i magazynowania odpadów (patrz sekcje 2.3.3, 2.3.4, 2.3.5)

Technical Guidance Note S0.01
IPPC General Sector Guidance

2.6. Wykorzystanie i unieszkodliwianie odpadów

- Agencja zobowiązuje operatorów instalacji do przedstawienia opisu każdego rodzaju odpadu wytwarzanego przez instalację niezależnie od tego czy dany rodzaj odpadu jest wykorzystywany czy składowany.
- Jeżeli operator proponuje składowanie odpadów, jest zobowiązany przedstawić dowody na to, że wykorzystanie odpadów jest technicznie lub ekonomicznie nieuzasadnione oraz że podejmuje działania mające na celu wyeliminowanie bądź ograniczenie wpływu na środowisko.

Technical Guidance Note S0.01
IPPC General Sector Guidance

2.7. Oszczędność energii

Techniki poprawiające efektywność energetyczną:

- odzyskiwanie ciepła z różnych operacji należących do procesu;
- wysokowydajne techniki odwadniania służące minimalizacji zużycia energii do suszenia;
- minimalizacja zużycia wody i systemy zamkniętych obiegów wody;
- dobra izolacja cieplna;
- odpowiednie lokalizowanie urządzeń pozwalające zmniejszyć odległości przepompowywania;
- ograniczenie zapotrzebowania na moc bierną, optymalizacja fazy sterowania elektronicznego silnikami; phase optimisation of electronic control motors;
- ponowne użycie wód chłodniczych (o podwyższonej temperaturze) w celu odzysku ciepła;
- przenoszenie taśmowe zamiast pneumatycznego (należy uwzględnić możliwość większej emisji niezorganizowanej);
- wprowadzenie ciągłych procesów produkcyjnych.

Technical Guidance Note S0.01
IPPC General Sector Guidance

2.7. Oszczędność energii cd.

Techniki stosowane w produkcji energii:

- stosowanie produkcji skojarzonej (energia elektryczna i cieplna);
- odzyskiwanie ciepła z odpadów;
- używanie mniej zanieczyszczających paliw.

Technical Guidance Note S0.01
IPPC General Sector Guidance

2.8 Sytuacje awaryjne i ich skutki

Zarządzanie sytuacjami awaryjnymi składa się z trzech elementów:

- **identyfikacja zagrożeń** związanych z działaniem instalacji;
- **ocena ryzyka** (niebezpieczeństwo x prawdopodobieństwo) zaistnienia sytuacji awaryjnej i możliwych skutków;
- wdrożenie **działań mających na celu obniżenie ryzyka** związanego z wystąpieniem sytuacji awaryjnych wypadków i opracowanie planów działania w przypadku ich wystąpienia.

Technical Guidance Note S0.01
IPPC General Sector Guidance

2.3.3. Nadzór nad niezorganizowanymi zrzutami ścieków do wód powierzchniowych, kanalizacji i wód gruntowych

Instalacje podziemne

- przebieg instalacji kanalizacyjnych powinien być ustalony i zapisany;
- przebieg wszystkich rurociągów podziemnych powinien być ustalony i zapisany;
- wszystkie podziemne studzienki i zbiorniki powinny zostać zidentyfikowane;
- instalacje powinny być wykonane w sposób ograniczający możliwość wycieków oraz możliwość ich szybkiego wykrycia szczególnie w przypadku wycieków substancji niebezpiecznych;
- dla rurociągów, studzienek i zbiorników podziemnych należy wykonać odpowiednie obudowy i zapewnić możliwość wykrywania nieszczelności;
- dla wszystkich instalacji podziemnych należy opracować program inspekcji i konserwacji np. testy ciśnieniowe lub wykorzystanie telewizji przemysłowej;.

Technical Guidance Note S0.01
IPPC General Sector Guidance

2.3.3. Nadzór nad niezorganizowanymi zrzutami ścieków do wód powierzchniowych, kanalizacji i wód gruntowych

Uszczelnienie terenu:

- należy przygotować opisy techniczne, sposób wykonania i użytkowania wszystkich powierzchni, na których prowadzona jest działalność;
- należy opracować program inspekcji i konserwacji wszystkich nieprzepuszczalnych powierzchni i barier chroniących przed rozlewami;
- należy uzasadnić przypadki, gdzie powierzchnie operacyjne nie zostały wyposażone w :
  - nieprzepuszczalną powierzchnię,
  - bariery chroniących przed rozlewami,
  - uszczelnianie złącz konstrukcyjnych,
  - podłączenia do zamkniętej instalacji kanalizacyjnej.

Technical Guidance Note S0.01
IPPC General Sector Guidance

2.3.3. Nadzór nad niezorganizowanymi zrzutami zanieczyszczeń do wód powierzchniowych, kanalizacji i wód gruntowych

Wszystkie zbiorniki z płynami, które mogą oddziaływać na środowisko, powinny być obwałowane. Obwałowanie powinno:

- być nieprzepuszczalne i odporne na działanie magazynowanych materiałów;
- nie mieć żadnych wylotów (tj. drenów czy. spustów) chyba, że do zamkniętego zbiornika zbiorczego;
- być wyposażone w rurociągi poprowadzone w sposób zapewniający szczelność obwałowań;
- być zaprojektowane w sposób zapewniający wyłapanie wycieków ze zbiorników i urządzeń;
- mieć objętość odpowiadającą większej wartości z wymienionych: 110% największego z obwałowanych zbiorników lub 25% całkowitej objętości zbiorników;
- być przedmiotem regularnych inspekcji celem zapewnienia, że każde odpompowanie lub usuwanie zawartości jest prowadzone pod nadzorem po przeprowadzeniu pomiarów zanieczyszczeń;

Technical Guidance Note S0.01
IPPC General Sector Guidance

2.3.3. Nadzór nad niezorganizowanymi zrzutami ścieków do wód powierzchniowych, kanalizacji i wód gruntowych

Wszystkie zbiorniki z płynami, które mogą oddziaływać na środowisko, powinny być obwałowane. Obwałowanie powinno (cd.):

- być nieprzepuszczalne i odporne na działanie magazynowanych materiałów;
- jeśli inspekcje nie są częste, obwałowanie winno być wyposażone we wskaźnik napełnienia i/lub instalację alarmową;
- mieć wlew umieszczony wewnątrz obwałowania a jeśli to niemożliwe odpowiednie zabezpieczenie miejsca wlewu przed rozlewem;
- być przedmiotem zaplanowanych inspekcji obejmujących badanie wody, jeżeli szczelność obwałowania budzi wątpliwości.

Technical Guidance Note S0.01
IPPC General Sector Guidance

2.3.4. Zapachy

Operator jest zobowiązany do opracowania i utrzymywania planu działania dotyczącego emisji zapachów, który powinien uwzględniać dwa możliwe przypadki:

- Emisja jest określona w pozwoleniu – tj. pozwolenie sankcjonuje emisję zapachu z określonego procesu a jako BAT uznaje się określony poziom *dyspersji pomiędzy źródłem a receptorem zapewniający brak uciążliwości* dla otoczenia.
- Emisja nie jest określona w pozwoleniu – tzn. że w normalnych warunkach emisji zapachu można zapobiec lub ograniczyć do terenu zakładu przez stosowanie BAT takich jak uszczelnianie procesów, dobrą praktykę i wyłapywanie zapachów.

- Dla każdego z wymienionych przypadków zapewnić, że w normalnych warunkach nie będzie problemu zapachów.
- Dla każdego z wymienionych przypadków określić działania, które zostaną podjęte w wypadku sytuacji nietypowych lub w warunkach, w których mogą wystąpić uciążliwości zapachowe.

Technical Guidance Note S0.01
IPPC General Sector Guidance

2.4. Emisje zanieczyszczeń do wód gruntowych

Warunki pozwolenia IPPC muszą spełniać następujące wymagania:

- Generalnie pozwolenie nie może wydane w przypadku bezpośredniego zrzutu zanieczyszczeń z Listy I do gruntu (wyjątki dopuszczalne w określonych okolicznościach).
- *Jeśli pozwolenie dopuszcza stosowanie i/lub unieszkodliwianie substancji z* listy I lub inne działania, które mogą prowadzić do pośredniego uwalniania zanieczyszczeń wymienionych na liście I, warunkiem jego uzyskania jest przeprowadzenie odpowiednich badań. Pozwolenie nie może być wydane, *jeśli analiza wskazuje na możliwość* pośredniego przedostawania się do gruntu substancji z listy I. Konieczne jest wprowadzenie działań zabezpieczających przed przedostaniem się tych zanieczyszczeń do gruntu.
- W przypadku substancji z listy II, pozwolenie na bezpośrednie lub pośrednie uwalnianie zanieczyszczeń nie może być wydane bez przeprowadzenia odpowiednich analiz i spełnienia warunków zapobiegających zanieczyszczeniu wód gruntowych.

Technical Guidance Note S0.01
IPPC General Sector Guidance

2.2.3 Zużycie wody

Zużycie wody do mycia może być minimalizowane poprzez:

- *stosowanie technik podciśnieniowych, zgarnianie, ścieranie w miejsce spłukiwania powierzchni;*
- określenie możliwości powtórnego użycia wody;
- zastosowanie ręcznych zwalniaczy wypływu wody na wszystkich wężach, lancach itp.

Technical Guidance Note S0.01
IPPC General Sector Guidance

2.3 Działanie instalacji i techniki ochrony środowiska

Operator powinien dostarczyć odpowiedni opis procesów oraz proponowanych urządzeń ochrony środowiska i sposobu ich nadzorowania. Opis powinien zawierać :

- *schemat technologiczny procesu;*
- rysunki tych elementów instalacji, które mają związek z oddziaływaniem na środowisko, np. uszczelnienie składowiska odpadów, komora spalania spalami odpadów, urządzenia ochrony środowiska itp.
- szczegóły dotyczące wszystkich reakcji chemicznych wraz z ich kinetyką/bilansem energetycznym;
- koncepcję systemu nadzoru i sposób w jaki system kontroli wykorzystuje informacje z monitoringu środowiskowego,
- informacje dotyczące rocznej produkcji, bilansu masy i bilansu energetycznego;
- opis rozwiązań zapobiegających awariom instalacji;
- streszczenie istniejących procedur operacyjnych i konserwacyjnych;
- opis działania ochrony w nietypowych warunkach pracy takich jak rozruch, zatrzymanie i czasowe przerwy.

Technical Guidance Note S0.01
IPPC General Sector Guidance

2.3.1. Ograniczanie emisji do powietrza ze źródeł punktowych

Operator powinien odnieść się we wniosku do zagadnień przedstawionych poniżej:

- opis urządzeń ograniczających emisje z działalności;
- identyfikacja głównych składników chemicznych emisji (w szczególności dla *mieszanin lotnych związków organicznych*) i wpływ tych substancji na środowisko;
- działania zapewniające, że parametry oczyszczania są zgodne z wymaganiami;
- działania zapewniające wystarczającą dyspersję emisji w celu zapobiegania przekroczeniom norm imisyjnych krajowych i związanych z zapobieganiem transgranicznemu przepływowi zanieczyszczeń w odniesieniu do najbardziej wrażliwych receptorów, którymi mogą być *zdrowie ludzkie, gleba lub* ekosystemy leśne.

Technical Guidance Note S0.01
IPPC General Sector Guidance

2.3.2. Ograniczenie emisji zanieczyszczeń ze źródeł punktowych do wód powierzchniowych i kanalizacji

Nadzór emisji zanieczyszczeń do wód powinien być oparty na stosowaniu określonych niżej zasad w następującej kolejności:

- zużycie wody powinno być ograniczane a ścieki powinny być wykorzystywane ponownie. Nie zanieczyszczone wody opadowe zebrane z dachów i powierzchni utwardzonych, które nie mogą być wykorzystywane na miejscu, nie powinny być mieszane z innymi ściekami.
- W większości przypadków nadmiar wody wymaga podczyszczenia aby spełnić wymogi BAT (a także wymagań prawnych i innych) Oczyszczanie ścieków jest bardziej efektywne, jeżeli różne rodzaje ścieków są oczyszczane osobno. Jednak w przypadku, gdy wykorzystanie określonych cech ścieków pozwala uniknąć dodawania innych substancji chemicznych dla oczyszczenia ścieków, należy wykorzystać taką możliwość (np. neutralizacja ścieków kwaśnych i alkalicznych).
- Należy unikać sytuacji, w których część strumienia ścieków omija instalację oczyszczającą.

Technical Guidance Note S0.01
IPPC General Sector Guidance

2.3.3. Nadzór nad emisjami niezorganizowanymi do powietrza

Pyły:

W zależności od warunków następujące działania powinny znaleźć zastosowanie:

- przykrywanie zbiorników;
- unikanie gromadzenia materiałów na nie przykrytych hałdach i stosach (gdzie to możliwe);
- tam, gdzie to nieuniknione, używanie zraszaczy, środków wiążących, barier wiatrowych i podobnych technik;
- czyszczenie kół i dróg (zapobieganie przenoszenia zanieczyszczeń do wody lub przenoszenia ich przez wiatr);
- stosowanie zamkniętych przenośników taśmowych, przenośników pneumatycznych (uwzględniając wyższe zapotrzebowanie na energię);
- regularne działania porządkowe.

Technical Guidance Note S0.01
IPPC General Sector Guidance

2.3.3. Nadzór nad emisjami niezorganizowanymi do powietrza

Lotne związki organiczne:

- w trakcie przetaczania łatwo parujących cieczy, powinno stosować się następujące techniki – napełnianie podpowierzchniowe przez rury doprowadzone do dna zbiornika, wyrównywanie ciśnienia par poprzez instalacje odprowadzające pary z napełnianego do opróżnianego zbiornika lub zastosowanie systemów zamkniętych, w których pary są odprowadzane do odpowiedniego urządzenia ochrony powietrza;
- stosowanie odpowiednio dobranych systemów wentylacyjnych w celu redukcji emisji z odpowietrzania (np. ciśnieniowe/próżniowe zawory) a tam, gdzie to możliwe stosowanie knock-out pots w powiązaniu z odpowiednim urządzeniem ochrony powietrza;
- dla instalacji takich jak rafinerie lub niektóre zakłady chemiczne należy opracować program wykrywania nieszczelności i prowadzenia napraw .

Technical Guidance Note S0.01
IPPC General Sector Guidance

2.1 **Techniki zarządzania cd.**

Wymagania dotyczące systemu zarządzania:

- włączenie kwestii ochrony środowiska... : (cd.)
  - planowania i kosztorysowania;
  - włączenie aspektów środowiskowych do normalnych procedur operacyjnych;
  - polityki zakupów;
  - stosowania metod księgowych polegających na wiązaniu kosztów ochrony środowiska z procesami a nie jako kosztów ogólnych;

Technical Guidance Note S0.01
IPPC General Sector Guidance

2.1 **Techniki zarządzania cd.**

Wymagania dotyczące systemu zarządzania:

Operator powinien wykazać, w jaki sposób w praktyce system zarządzania odnosi się do następujących aspektów działalności:

- dobór surowców
- wydajność zużycia wody
- zmniejszenie ilości wytwarzanych odpadów
- nadzór nad emisjami zorganizowanymi i niezorganizowanymi;
- gospodarka odpadami
- energia
- hałas i wibracje
- monitorowanie

Technical Guidance Note S0.01
IPPC General Sector Guidance

2.2 **Zużycie materiałów**

Podstawowe zasady, których stosowanie operator powinien zademonstrować to:

- **redukcja** zużycia chemikaliów i innych materiałów
- **zastępowanie** materiałów szkodliwych materiałami mniej uciążliwymi dla środowiska lub takimi, których działanie może być łatwiej ograniczone lub które mogą być przekształcone w substancję, którą można łatwiej utylizować;
- **zrozumienie** przepływu produktów ubocznych i substancji zanieczyszczających oraz ich oddziaływania na środowisko

Technical Guidance Note S0.01
IPPC General Sector Guidance

2.2.1. Dobór surowców

Operator powinien posiadać szczegółowy rejestr surowców i materiałów zużywanych w zakładzie. Lista głównych surowców powinna być dołączona do wniosku. Powinna ona zawierać:

- skład chemiczny surowców, gdzie jest to istotne;
- ilości zużywane w zakładzie;
- strumienie przepływu surowca/materiału (tj. przybliżone wartości procentowe ilości surowca/materiału wprowadzane do produktu i do każdego komponentu środowiska);
- oddziaływanie na środowisko (np. okres rozkładu, potencjał bioakumulacyjny, toksyczność dla określonych gatunków);
- alternatywne surowce/materiały, które mogą mieć mniejszy wpływ na środowisko włączając te, *(ale nie wyłącznie), które zostały* opisane jako alternatywne w istniejących wytycznych.

Technical Guidance Note S0.01
IPPC General Sector Guidance

2.2.2 Ograniczanie ilości wytwarzanych odpadów (minimalizacja *zużycia* surowców

Pod nazwą "minimalizacja odpadów" mieści się wiele rodzajów stosowanych technik, od zwykłego utrzymywania porządku poprzez techniki pomiarów statystycznych, aż po wprowadzanie czystszych technologii.

Charakterystycznymi cechami minimalizacji odpadów jest:

- Ciągła identyfikacja i wdrażanie działań mających na celu zapobieganie powstawaniu odpadów;
- Aktywne uczestnictwo i zaangażowanie pracowników wszystkich szczebli np. system wykorzystywania pomysłów formułowanych przez pracowników;
- Monitorowanie i raportowanie zużycia surowców/materiałów a *także ich porównywanie z określonymi wskaźnikami.*

Technical Guidance Note S0.01
IPPC General Sector Guidance

2.2.3 Zużycie wody

W celu ograniczenia zużycia wody należy kierować się *następującymi zasadami*:

- techniki oszczędzania wody powinny być stosowane "u źródła", jeśli jest to możliwe;
- woda powinna być wykorzystywana w obiegu zamkniętym w tym samym procesie po wcześniejszym podczyszczeniu, jeśli jest to konieczne. Jeśli nie jest to możliwe, powinna być wykorzystywana w innych procesach, w których wymagania w stosunku do jakości wody *są niższe.*
- Należy podjąć działania mające na celu ograniczenia ryzyka zanieczyszczenia wody w procesie oraz wód powierzchniowych.

Technical Guidance Note S0.01
IPPC General Sector Guidance

- 2.1 Techniki zarządzania
- 2.2. Zużycie materiałów
  - 2.2.1 Dobór surowców
  - 2.2.2 Ograniczanie ilości wytwarzanych odpadów (minimalizacja zużycia surowców)
  - 2.2.3 Zużycie wody
- 2.3. Działalnie instalacji i ochrona środowiska
  - 2.3.1 Ograniczanie emisji do powietrza za źródeł punktowych
  - 2.3.2 Ograniczenie emisji zanieczyszczeń za źródeł punktowych do wód powierzchniowych i kanalizacji
  - 2.3.3 Nadzór nad emisjami niezorganizowanym do powietrza
  - 2.3.4 Nadzór nad niezorganizowanym zrzutami ścieków do wód powierzchniowych, kanalizacji i wód gruntowych
  - 2.3.4 Zapachy
- 2.4. Emisje zanieczyszczeń do wód gruntowych
- 2.5 Gospodarka odpadami
- 2.6 Wykorzystanie i składowanie odpadów
- 2.7. Energia
- 2.8. Sytuacje awaryjne i ich skutki
- 2.9. Hałas i wibracje
- 2.10. Monitoring
- 2.11. Likwidacja instalacji
- 2.12. Zagadnienia ogólne

Technical Guidance Note S0.01
IPPC General Sector Guidance

2.1 Techniki zarządzania

Wymagania dotyczące systemu zarządzania:

- Identyfikacja kluczowych oddziaływań na środowisko wywołanych prowadzoną działalnością;
- Cele i mierzalne zadania w zakresie wyników działań na rzecz środowiska;
- Program działań dotyczących realizacji celów i zadań;
- Regularne monitorowanie oddziaływania instalacji na środowisko;
- Sprzężenie zwrotne między wynikiem monitorowania a ustalaniem celów oraz zobowiązanie do realizacji kolejnych celów, jeśli jest to możliwe.;
- Regularne audity wewnętrzne i zewnętrzne – prowadzone przez niezależne jednostki;
- Regularne raporty środowiskowe dotyczące wyników działań na rzecz środowiska (roczne lub powiązane z cyklem auditów) opracowywane w celu:
  - przedłożenia rocznego raportu środowiskowego Agencji
  - publicznego przedstawienia tych danych (preferowane);

Technical Guidance Note S0.01
IPPC General Sector Guidance

2.1 Techniki zarządzania cd.

Wymagania dotyczące systemu zarządzania:

- *jasno określone zakresy odpowiedzialności za wyniki*, w szczególności za spełnianie wymagań pozwolenia IPPC;
- system monitorowania i nadzoru w celu:
  - zapewnienia funkcjonowania instalacji zgodnie z założeniami;
  - wykrycia błędów i operacji nie zamierzonych;
  - wykrycia powolnych zmian parametrów działania wskazujących na konieczność podjęcia działań zapobiegawczych;
- procedury analizy błędów i zapobiegania ich powtórnemu wystąpieniu;

Technical Guidance Note S0.01
IPPC General Sector Guidance

2.1 **Techniki zarządzania cd.**

Wymagania dotyczące systemu zarządzania:

- opracowanie odpowiednich procedur i szkoleń dla załogi, które powinny obejmować następujące obszary:
  - jednoznaczne wymagania w zakresie umiejętności i kompetencji niezbędnych do wykonywnia pracy na danym stanowisku;
  - świadomość wpływu wymagań wynikających z pozwolenia IPPC na wykonywane działania i sposób ich wykonywania przez pracowników;
  - świadomość wszystkie potencjalnych oddziaływań na środowisko spowodowanych działalnością w warunkach normalnych i wyjątkowych;
  - zapobieganie awaryjnym emisjom zanieczyszczeń i wskazywanie działań, jakie powinny być podjęte w wypadku ich wystąpienia;

Technical Guidance Note S0.01
IPPC General Sector Guidance

2.1 **Techniki zarządzania cd.**

Wymagania dotyczące systemu zarządzania:

- opracowanie odpowiednich procedur i szkoleń dla załogi, które powinny obejmować następujące obszary: (cd.)
  - wprowadzenie i utrzymywanie dokumentacji szkoleń pracowników operacyjnych;
  - zapewnienie, że poziom wiedzy, wyszkolenia i kwalifikacji kadry kierowniczej i technicznej, będzie uzależniony od wykonywanych zadań i ich roli w utrzymywaniu zgodności działania instalacji z prawem. Może być to oceniane według norm przyjętych w danej branży.
- programy prewencyjnych przeglądów określonych urządzeń;
- procedury dokumentowania, analizowania i prowadzenia działań korygujących w odpowiedzi na skargi związane z oddziaływaniem na środowisko;

Technical Guidance Note S0.01
IPPC General Sector Guidance

2.1 **Techniki zarządzania cd.**

Wymagania dotyczące systemu zarządzania:

- włączenie kwestii ochrony środowiska we wszystkie pozostałe aspekty działalności przedsiębiorstwa w zakresie w jakim jest to wymagane przez Dyrektywę IPPC, a w szczególności:
  - nadzoru nad zmianami procesów na instalacji;
  - projektowania i przeglądów nowych urządzeń, konstrukcji i innych inwestycji;
  - zatwierdzenia środków kapitałowych przeznaczonych na te inwestycje;
  - alokacji zasobów i środków;

SZS a nie certyfikat jest BAT ; jest wpisany w BAT

Najlepsza Dostępna Technika - BAT

WNIOSKI:

Stosowanie BAT będzie wymagać od wszystkich zainteresowanych:

- **śledzenia bieżących zmian w zakresie BAT**
- **lepszej koordynacji w zakresie wszystkich komponentów środowiska i uwzględniania oddziaływania na środowisko jako całość**
- **zwrócenia większej uwagi na zagadnienia efektywności energetycznej i materiałowej**
- **zwrócenia baczniejszej uwagi na zagadnienia natury organizacyjnej oraz sposobu likwidacji instalacji**

eko-net.pl

Najlepsza Dostępna Technika - BAT

WNIOSKI:

Stosowanie BAT będzie wymagać od instytucji wydających pozwolenia zintegrowane:

- **określenia realnych terminów w jakich operator będzie zobowiązany do wprowadzenia BAT**

programy dostosowawcze

eko-net.pl

Najlepsza Dostępna Technika - BAT

WNIOSKI:

Stosowanie BAT będzie wymagać od operatorów instalacji :

Nowych:

- **dokonywania doboru najwłaściwszych rozwiązań spośród dostępnych w trakcie projektowania i budowy**

Istniejących:

- **poszukiwania wszystkich możliwości ograniczenia wpływu na środowisko**
- ***realizacji działań niskonakładowych natychmiast***
- **planowanie działań wymagających znaczących nakładów**

eko-net.pl

Najlepsza Dostępna Technika - BAT

WNIOSKI:

Wymaganie stosowania BAT nie oznacza ujednolicenia rozwiązań technicznych w podobnych instalacjach. Konieczne jest uwzględnienie faktu, że instalacje:

- **są/były budowane w różnym czasie**
- **pod różnymi rygorami prawnymi**

BAT nie będzie więc oznaczał tego samego w *każdym* zakładzie.

eko-net.pl

Najlepsza Dostępna Technika - BAT

WNIOSKI:

- **w przypadku instalacji nowych istnieje możliwość wykorzystania procedur OOS**
- **wymagane będzie stosowanie najlepszych dostępnych rozwiązań w czasie projektowania i budowy**
- **w przypadku instalacji istniejących może wystąpić konieczność ustalania warunków BAT na poziomie zakładu a nie branży**
- **ustalanie BAT na poziomie zakładu wymaga nie tylko wiedzy technicznej, ale również zdolności negocjacyjnych.**

eko-net.pl

Technical Guidance Note S0.01
IPPC General Sector Guidance

- 2.1 Techniki zarządzania
- 2.2. Zużycie materiałów
  - 2.2.1 Dobór surowców
  - 2.2.2 Ograniczanie ilości wytwarzanych odpadów (minimalizacja zużycia surowców)
  - 2.2.3 Zużycie wody
- 2.3. Działalnie instalacji i ochrona środowiska
  - 2.3.1 Ograniczanie emisji do powietrza ze źródeł punktowych
  - 2.3.2 Ograniczenie emisji zanieczyszczeń ze źródeł punktowych do wód powierzchniowych i kanalizacji
  - 2.3.3 Nadzór nad emisjami niezorganizowanymi do powietrza
  - 2.3.4 Nadzór nad niezorganizowanymi zrzutami ścieków do wód powierzchniowych, kanalizacji i wód gruntowych
  - 2.3.4 Zapachy
- 2.4. Emisje zanieczyszczeń do wód gruntowych
- 2.5 Gospodarka odpadami
- 2.6 Wykorzystanie i składowanie odpadów
- 2.7. Energia
- 2.8. Sytuacje awaryjne i ich skutki
- 2.9. Hałas i wibracje
- 2.10. Monitoring
- 2.11. Likwidacja instalacji
- 2.12. Zagadnienia ogólne

eko-net.pl

Dokumenty Referencyne BAT

STATUS NOT BREF

- Noty BREF nie wymagają stosowania konkretnych technik ani wartości granicznych emisji zanieczyszczeń ale przedstawiają informacje pomagające określać warunki pozwoleń zintegrowanych.
- BREF muszą więc być brane pod uwagę na równi z pozostałymi czynnikami wymienionymi w załączniku IV
- Kraje członkowskie nie są więc obowiązane do stosowania wszystkich standardów określonych w BREF.

Dokumenty Referencyne BAT

- Większość krajów członkowskich UE planuje opracowanie własnych wytycznych uwzględniających BREF.
- Wytyczne krajowe przedstawiające technicznie i ekonomicznie uzasadnione techniki umożliwiające ochronę środowiska i poprawę jego stanu mają na celu wsparcie osób wydających decyzje administracyjne.

Dokumenty Referencyne BAT

ZAWARTOŚĆ NOT BREF

- Streszczenie
- Wstęp

1. Ogólne informacje dotyczące grupy procesów
2. Obecnie stosowane techniki
3. Obecny poziom zużycia materiałów/surowców i emisji zanieczyszczeń
4. Techniki analizowane pod kątem określenia BAT
5. **Techniki uznane jako BAT**
6. Techniki na etapie doświadczeń
7. Wnioski i zalecenia

Dokumenty Referencyne BAT

Aktualne informacje dot. BAT

Strona Internetowa Biura w Sewilli
http://eippcb.jrc.es

zawiera informacje nt.:

- programu prac
- kontakty do członków TWG
- dokumentów wykorzystywanych do opracowanie Not BREF
- pełny tekst Not BREF
- możliwość pobrania dokumentów (wersja angielska).

Inne dokumenty określające BAT

Wielka Brytania

ENVIRONMENT AGENCY

Strona internetowa Agencji Ochrony Środowiska
http://www.environment-agency.gov.uk

zawiera wytyczne techniczne ogólne i dla sektorów

- możliwość „ściągnięcia" dokumentów

Inne dokumenty określające BAT

ENVIRONMENT AGENCY

Składając wniosek o pozwolenie zintegrowane należy opierać się na następujących dokumentach:

- Wytyczne branżowe IPPC
- Wytyczne ogólne IPPC (jeżeli brak branżowych)
- Istniejące wytyczne branżowe IPC
- Istniejące wytyczne dot. gospodarki odpadami

Dokumenty Referencyjne BAT

Praca European IPPC Bureau w Sewilli opiera się na wymianie informacji między członkami grup roboczych

- *Dla każdego dokumentu powołano Techniczną Grupę Roboczą*
  - koordynacja - pracownik Biura
  - członkowie - pracownicy władz i przemysłu
  - określenie zakresu prac nad branżą lub zagadnieniem
  - analiza dostępnych materiałów
  - projekt noty BREF
  - publikacja na stronie internetowej
  - opiniowanie i weryfikacja
  - publikacja pełnej wersji dokumentu

Dokumenty Referencyjne BAT

- Prace nad notami BREF dla wszystkich branż mają być rozpoczęte do końca 2002 r.

Dokumenty Referencyjne BAT

Noty BREF - opublikowane

Produkcja papieru i celulozy	BREF, grudzień 2001
Produkcja żelaza i stali	BREF, grudzień 2001
Produkcja cementu i wapna	BREF, grudzień 2001
Przemysłowe systemy chłodzące	BREF, grudzień 2001
Elektrolityczne uzyskiwanie chloru	BREF, grudzień 2001
Obróbka metali żelaznych	BREF, grudzień 2001
Obróbka metali nieżelaznych	BREF, grudzień 2001
Wytwarzanie szkła	BREF, grudzień 2001
Garbowanie skór	BREF, luty 2003
Rafinerie	BREF, luty 2003
Wielkotonażowa produkcja związków organicznych	BREF, luty 2003
Instalacje oczyszczania ścieków i oczyszczania gazów odlotowych i systemy zarządzania nimi w przemyśle chemicznym	BREF, luty 2003
Obróbka tkanin	BREF, lipiec 2003
Systemy monitorowania	BREF, lipiec 2003
Intensywna hodowla zwierząca	BREF, lipiec 2003

Dokumenty Referencyjne BAT

Noty BREF - zakończone

Ubojnie zwierząt i zakłady utylizacji odpadów pochodzenia zwierzęcego	BREF, listopad 2003
Zagospodarowywanie odpadów w górnictwie surowców mineralnych	BREF, lipiec 2004
Kuźnie i odlewnie	BREF, lipiec 2004
Emisje związane ze składowaniem masowym lub materiałów niebezpiecznych	BREF, styczeń 2004

eko-net.pl

Dokumenty Referencyjne BAT

final draft

Noty BREF - projekty

Zagadnienia ekonomiczne i ogólne związane z IPPC	FD, listopad 2004
Duże instalacje energetycznego spalania paliw	FD, listopad 2004
Utylizacja i wykorzystanie odpadów	D2, styczeń 2004
Przemysł spożywczy i przetwórstwo mleka	D2, maj 2003
Duże zakłady chemii nieorganicznej - azotowe, kwasy, nawozy	D2, marzec 2004
Spalanie odpadów	D2, marzec 2004
Obróbka powierzchniowa metali	D2, kwiecień 2004
Produkcja wysokowartościowych substancji organicznych	D1, marzec 2004
Obróbka powierzchniowa z użyciem rozpuszczalników	D1, maj 2004
Produkcja ceramiki	D1, październik 2004
Produkcja specjalnych substancji nieorganicznych	D1, wrzesień 2004
Produkcja polimerów	D1, wrzesień 2004
Duże zakłady chemii nieorganicznej - produkty stałe i inne	D1, sierpień 2004

eko-net.pl

Dokumenty Referencyne BAT

Noty BREF - planowane

Efektywność energetyczna	2003

eko-net.pl

Typy Wskaźników

- bezwzględne
  - liczba ton CO2 wyemitowanych w ciągu roku
  - liczba ton odpadów powstałych w ciągu roku
  - liczba litrów wody zużytej do chłodzenia
- względne
  - emisja CO2 na jednostkę produkcji
  - procent samochodów wyposażonych w katalizator
- agregowane
  - liczba przejechanych kilometrów
- ważone

Przykłady wskaźników względnych

- UDZIAŁY

  energia wytworzona z gazu (MWh)

  całkowite zużycie energii MWh

- RELACJE

  zużycie energii (MWh)

  wielkość produkcji (kg)

Przykłady wskaźników ważonych

	emisja na jednostkę produkcji	Waga	Emisja ważona
Emisja A	200	4	800
Emisja B	5000	2	10000
Emisja C	700	10	7000
Emisja D	4000	1	4000
Emisja E	400	8	3200
Emisja F	900	3	2700
			27700

Przykłady wskaźników ważonych

Wskaźnik poprawy

rok bieżący - 27700
rok poprzedni - 32440

27700/32440 = 0,854

	Produkcja	Zużycie materiałów	Zużycie energii	Zużycie wody	Liczba pracowników	roboczogodzin	roboczogodziny	powierzchnia/kubatura budynków	sprzedaż	koszty produkcji
Zużycie materiałów	X									
Opakowania	X	X								
Środki czyszczące								X		
Zużycie energii	X				X			X		
Zużycie wody	X				X					
Odpady	X	X								
Ścieki	X			X						
Emisje do pow.	X		X							
Transport	X				X					
Wypadki przy pracy					X	X	X			
Skargi						X				
Szkolenia					X	X				
Koszty ochr. środ.									X	X

Przykłady wskaźników materiałowych

WSKAŹNIK	OPIS	jedn.
Całkowite zużycie surowca		t
Efektywność wykorzystania	zużycie materiału/wlk. produkcji	%
Całkowita ilość opakowań		t
Względna ilość opakowań	ilość opakowań/wlk. produkcji	%
Udział opakowań zwrotnych	opakowania zwrotne/wszystkie opakowania	%
Liczba substancji niebezp.		liczba
Masa substancji niebezp.		kg
Udział surowców wtórnych	surowce wtórne/całk. ilość surowców	%
Koszty materiałowe		zł
Koszt opakowań		zł
Udział opakowania w cenie	koszt opakowań/wlk. produkcji	zł/jedn. produkcji

Przykłady wskaźników energetycznych

WSKAŹNIK	OPIS	jedn.
Całkowite zużycie energii		kWh
Względne zużycie energii	zużycie energii/wlk. produkcji	kWh/j.p..
Udział nośnika energii	zuż. nośnika/całk. zuż. energii	%
Wzgl. zużycie energii na produkt (proces)	zużycie energii na produkt (proces)/całk. zużycie energii	%
Udział energii odnawialnej	energia odnawialna/całk. zużycie	%
Względne zużycie energii cieplnej	zuż. en. cieplnej/m3 obiektów	kWh/m3
Całk. koszt energii		zł
Względny koszt energii	całk. koszt energii/koszty produkcji	%
Względny koszt energii z danego źródła	koszt en. ze źródła/zużycie tego źródła	%
Wielkość oszczędności		zł

Przykłady wskaźników zużycia wody

WSKAŹNIK	OPIS	jedn.
Całkowite zużycie wody		m3
Udział źródeł wody	zużycie wody ze źródła/całk. zuż. wody	%
Względne zużycie wody	całk. zużycie wody/wielkość produkcji	m3/ j.p.
Wzgl. zapotrzebowanie na wodę	zużycie wody na produkt (proces)/całk. zużycie wody	%
Całk. koszt wody		zł
Względny koszt wody	całk. koszt wody/koszty produkcji	%

Przykłady wskaźników odpadowych

WSKAŹNIK	OPIS	jedn.
Całkowita ilość odpadów		t
względna ilość rodzaju odpadu	ilość rodzaju odpadów/wlk. produkcji	kg/j.p.-
odpady do zagospodarowania		t
odpady do składowania		t
udział recyklingu	ilość odpadów zagospodarowanych/całk. ilość odpadów	%
udział składowania	ilość odpadów do składowania/całk. ilość odpadów	
ilość odpadów niebezpiecznych		t
udział odpadów niebezpiecznych	ilość odp. niebezp./całk. ilość odpadów	%
koszt zagospodarowania i utylizacji	koszt en. ze źródła/zużycie tego źródła	%
względny koszt	koszt rodzaju odpadu/całk. koszt odpadów	zł

Przykłady wskaźników emisji

WSKAŹNIK	OPIS	jedn.
Całkowita wielkość emisji		m3
Ładunek emitowanych substancji	np. ładunek CO2, NOx,SO2, VOC	kg
względny ładunek *emitowanych substancji*	np. ładunek CO2, NOx,SO2, VOC/wielkość produkcji	kg/j.p.
koszt oczyszczania		zł
względny koszt oczyszczania	koszt oczyszczania/całk. koszt produkcji	%

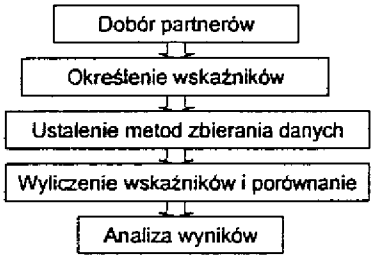
Dlaczego stosować wskaźniki?

- Kontrola zgodności z przepisami
- Nadzór nad ciągłą poprawą i skutecznością przeprowadzonych działań
- ocena realizacji celów środowiskowych
- ogólny nadzór nad funkcjonowaniem przedsiębiorstwa
- usprawnienie przepływu informacji między przedsiębiorstwem a otoczeniem

BENCHMARKING

Benchmarking jest **procesem**,na drodze którego zakłady identyfikują i oceniają najlepsze rozwiązania **wewnątrz i na zewnątrz** swej organizacji skupiając się na tych dziedzinach, w których *zamierzają poprawić swe osiągnięcia*

Benchmarking



BENCHMARKING

KORZYŚCI :

- **przełamanie istniejącego oporu przed poprawą przez wykazanie, że innym organizacjom udaje się osiągnąć lepsze wyniki;**
- **porównanie swoich osiągów z innymi w branży lub z normami, co prowadzi albo do potwierdzenia dobrej ścieżki postępowania lub do wytyczenia obszarów, w których należy działać w celu osiągnięcia poprawy;**
- **dostarczenie podstaw empirycznych do wyznaczania celów do osiągnięcia, a przez to zwiększenia zaufania co do trafności dobranych celów i zwiększenie prawdopodobieństwa ich osiągnięcia;**
- **wytworzenie danych i pomysłów, nawiązanie kontaktów poprzez dialog z innymi organizacjami.**

BENCHMARKING

Przykłady oceny znaczenia aspektów środowiskowych poprzez zastosowanie uproszczonej metody benchmarkingu.

Źródło:
D. Hunt, C. Johnson: "Environmental Management Systems. Principles and Practice", McGraw-Hill Book Company

A031 - wskaźniki dla porównania

BENCHMARKING

Przykład oceny znaczenia zużycia energii elektrycznej:
Firma produkcyjna ma roczne obroty 45 mln GBP
i jej roczne zużycie energii elektrycznej wynosi 310 GWh:

Zużycie energii elektrycznej w firmie: 310 GWh
Zużycie energii elektrycznej przez przemysł w UK: 273 000 GWh

Względne zużycie energii elektrycznej w firmie:
310/273000= **0,0011**

Obroty firmy: 45 mln GBP
Produkt Krajowy Brutto w UK: 543 000 mln GBP
Względna wielkość firmy: 45/543000= **0,000083**

Czynnik określający względne znaczenie zużycia energii:
0,0011/0,000083= 13
Czy badana działalność jest energochłonna? Lepiej by było posiadać dane dla sektora.

BENCHMARKING

Przykład oceny znaczenia emisji CO_2
Firma zatrudnia 530 pracowników i emituje (głównie z uwagi na ogrzewanie) około 1470 ton dwutlenku węgla rocznie:

Emisja firmy: 1470 ton
Emisja w UK z przemysłu: 158 mln ton
Względny udział firmy: 1470/158mln= **0,0000093**

Liczba zatrudnionych w firmie: 530
Liczba zatrudnionych w UK: 25 mln
Względna wielkość organizacji: 530/25mln= **0,000021**

Czynnik określający znaczenie badanego oddziaływania:
0,0000093/0,000021= **0,44**

Czy badana działalność wiąże się nierozłącznie z emisją CO_2?
Lepiej by było posiadać dane dla sektora.

PODSTAWOWE INFORMACJE O WYMAGANIACH PRAWA OCHRONY ŚRODOWISKA W POLSCE

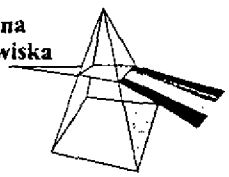
ŚRODOWISKO

ogół elementów przyrodniczych, w tym także przekształconych w wyniku działalności człowieka, w szczególności :

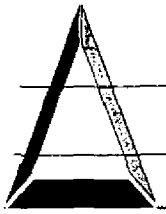
- **powierzchnia ziemi,**
- **kopaliny,**
- **wody,**
- **powietrze,**
- **zwierzęta i rośliny,**
- **krajobraz i klimat.**

PRAWO OCHRONY ŚRODOWISKA

Ochrona środowiska



- ☑ prawo finansowe,
- ☑ prawo administracyjne
- ☑ prawo cywilne
- ☑ prawo karne
- ☑ prawo pracy
- ☑ .....

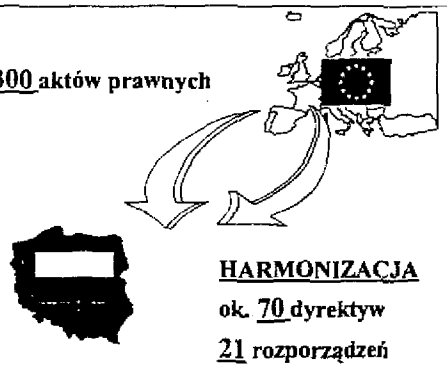


poziomy tworzenia prawa ochrony środowiska

prawo międzynarodowe konwencje i umowy	ratyfikowane umowy międzynarodowe mają pierwszeństwo przed ustawami
ustawodawstwo krajowe ustawy i rozporządzenia	wymóg zgodności z Konstytucją
prawo miejscowe, stanowione przez: - wojewodów - sejmiki województwa - rady powiatów - rady gmin	wydawane na podstawie upoważnień ustawowych i w sytuacjach zagrożenia; powszechnie obowiązujące ale w granicach określonych regionów; najważniejsze - plany zagospodarowania przestrzennego, przestrzenne formy ochrony przyrody

ENVIRONMENTAL ACQUIS

ok. 300 aktów prawnych



HARMONIZACJA

ok. 70 dyrektyw

21 rozporządzeń

CO ZNACZĄ OBECNIE ŚRODOWISKOWE DYREKTYWY WSPÓLNOTY EUROPEJSKIEJ

Z chwilą przystąpienia Polski do Unii Europejskiej:

- rozporządzenia Rady weszły bezpośrednio do prawa polskiego, zastępując sprzeczne z nimi przepisy ustaw i aktów wykonawczych;
- polski ustawodawca *związany jest celami działań* wyznaczonymi w dyrektywach i ma obowiązek stworzenia przepisów krajowych zgodnych z daną dyrektywą, posiadając jednak *swobodę co do sposobu prowadzenia wyznaczonych* działań
- w szczególnych, uzasadnionych przypadkach polskie normy będą mogły być bardziej rygorystyczne od przepisów unijnych

Prawo ochrony środowiska

- Liczba stron Dziennika Ustaw 2001

- Liczba stron Dziennika Ustaw 2002

13000

16000

Prawo ochrony środowiska

Liczba stron Dziennika Ustaw 2003

17000

ZASADY OGÓLNE PRAWA OCHRONY ŚRODOWISKA

r.pr. Michał Behnke

PRAWO OCHRONY ŚRODOWISKA

⇕

? Co nie jest zabronione jest dozwolone

? Nieznajomość i niedbałość co do prawa szkodzi

ćwiczenie

Wyrok Sądu Najwyższego - Izba Administracyjna Pracy i Ubezpieczeń Społecznych

z dnia 09.06.1999 r. III RN 12/99

„Obowiązek należytego oraz wyczerpującego informowania stron przez organ administracyjny o okolicznościach faktycznych i prawnych, mogących wpływać na ustalenie ich praw i obowiązków będących przedmiotem postępowania **(art.9 kpa) nie zwalnia przedsiębiorcy prowadzącego profesjonalną działalność gospodarczą z obowiązku znajomości przepisów prawnych i dołożenia należytej staranności w zakresie jej prowadzenia."**

⇩

ZARZĄDZANIE ŚRODOWISKOWE

ZASADY TWORZENIA PRAWA OCHRONY ŚRODOWISKA

- **Techniki zapobiegawcze: Przepisy**

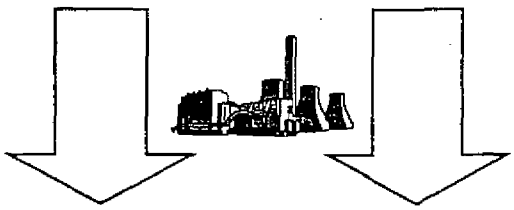
R

  - **Ustanawianie standardów, norm**
    - Standardy imisji - standardy jakości środowiska (jego komponentów).
    - Standardy emisji - określenie ilości zanieczyszczenia dopuszczalnego do emisji w odniesieniu do jednostki czasu, jednostki produkcji itp.
    - Standardy procesowe - określenie postępowania przy wykonywaniu operacji i procesów technologicznych.
    - Normy dotyczące produktów - określenie np.: (1) fizycznego i/lub chemicznego składu produktu (przykłady: lekarstwa, detergenty), (2) procedur postępowania z produktem, jego pakowania i oznakowania (przykład: substancje toksyczne), (3) ilości zanieczyszczeń, które mogą zostać uwolnione w czasie użytkowania (przykład: nośniki energii, farby).

NOWE STANDARDY ŚRODOWISKA (2001)

- ☑ standardy jakości gleby (o)
- ☑ standardy jakości ziemi (f)
- ☑ standardy zapachowej jakości powietrza (f)
- ☑ pięć klas, dla prezentowania stanu ekologicznego i stanu chemicznego wód powierzchniowych oraz stanu ilościowego i chemicznego wód podziemnych (o)

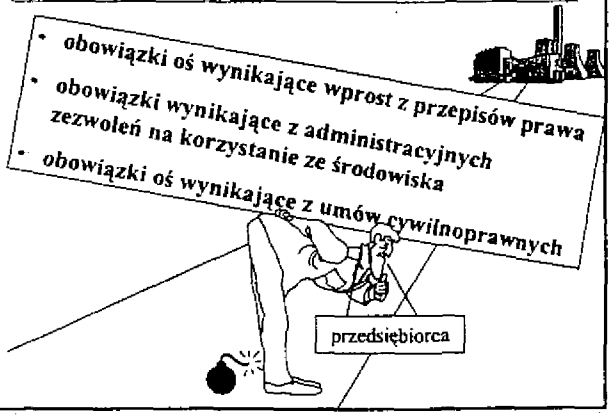
ZRÓŻNICOWANIE WYMAGAŃ



FAZA INWESTYCYJNA

FAZA EKSPLOATACJI

ŹRÓDŁA WYMAGAŃ ŚRODOWISKOWYCH



USTAWA Z DNIA 27 KWIETNIA 2001 R. PRAWO OCHRONY ŚRODOWISKA

PRYNCYPIA

WYKONYWANIE OCHRONY ŚRODOWISKA

Art. 82.

Ochrona zasobów środowiska jest realizowana w szczególności poprzez:

1) określenie standardów jakości środowiska oraz kontrolę ich osiągania, a także podejmowanie działań służących ich nieprzekraczaniu lub przywracaniu,

- STANDARDY JAKOŚCI ŚRODOWISKA,
- STREFOWANIE
- PUBLICZNE PROGRAMY OCHR. ŚRODOWISKA

2) ograniczanie emisji,

- standardy: INSTALACJI, SUBSTANCJI, PRODUKTÓW

USTAWA PRAWO OCHRONY ŚRODOWISKA

Tytuł III Przeciwdziałanie zanieczyszczeniom

Dział I Przepisy ogólne (Art. 137-140)
Dział II Instalacje, urządzenia, substancje oraz produkty
Rozdział 1 Instalacje i urządzenia (Art. 141-157)
Rozdział 2 Substancje (Art. 158-165)
Rozdział 3 Produkty (Art. 166-172)
Dział III Drogi, linie kolejowe, linie tramwajowe, lotniska oraz porty(Art. 173-179)
Dział IV Pozwolenia na wprowadzenie do środowiska substancji lub energii
Dział V Przeglądy ekologiczne(Art. 237-242)

KLUCZOWE SPOJRZENIE

INSTALACJA - rozumie się przez to:
a) stacjonarne urządzenie techniczne,
b) zespół stacjonarnych urządzeń technicznych powiązanych technologicznie, do których tytułem prawnym dysponuje ten sam podmiot i położonych na terenie jednego zakładu,
c) ~~obiekty budowlane~~ budowle nie będące urządzeniami technicznymi ani ich zespołami,
których eksploatacja może spowodować emisję,

ZAKŁAD - rozumie się przez to jedną lub kilka instalacji wraz z terenem, do którego prowadzący instalacje posiada tytuł prawny, oraz znajdującymi się na nim urządzeniami,

a nie przewodzenie

emisje to CO_2 a nie czynność wprowadzania

NOWE DEFINICJE LEGALNE

EMISJA - ~~wprowadzane~~ **bezpośrednio lub pośrednio, w wyniku działalności człowieka, do powietrza, wody, gleby lub ziemi:**
a) substancje,
b) energie, takie jak ciepło, hałas, wibracje lub pola elektromagnetyczne,

ZANIECZYSZCZENIE- emisja, która może być ~~jest~~ szkodliwa dla zdrowia ludzi lub stanu środowiska, ~~powoduje~~ może powodować szkodę w dobrach materialnych, może pogarszać ~~pogarsza~~ walory estetyczne środowiska lub może kolidować ~~koliduje~~ z innymi, uzasadnionymi sposobami korzystania ze środowiska,

SYSTEM POZWOLEŃ NA WPROWADZANIE DO ŚRODOWISKA SUBSTANCJI LUB ENERGII

PRAWO OCHRONY ŚRODOWISKA

Art. 180.

Eksploatacja instalacji powodująca:

1) wprowadzanie gazów lub pyłów do powietrza,
2) wprowadzanie ścieków do wód lub do ziemi,
3) wytwarzanie odpadów,
4) emitowanie hałasu,
5) emitowanie pól elektromagnetycznych,

jest dozwolona po uzyskaniu pozwolenia, jeżeli jest ono wymagane.

GRANICE ODDZIAŁYWANIA NA ŚRODOWISKO

Art. 144. 1. Eksploatacja instalacji nie powinna powodować przekroczenia standardów jakości środowiska.

2. Eksploatacja instalacji powodująca wprowadzanie gazów lub pyłów do powietrza, emisję hałasu oraz wytwarzanie pól elektromagnetycznych nie powinna, z zastrzeżeniem ust. 3, powodować przekroczenia standardów jakości środowiska poza terenem, do którego prowadzący instalację ma tytuł prawny.

3. Jeżeli w związku z funkcjonowaniem instalacji utworzono obszar ograniczonego użytkowania, eksploatacja instalacji nie powinna powodować przekroczenia standardów jakości środowiska poza tym obszarem.

STREFY OCHRONNE

ustawa o zmianie ustawy o ochronie i kształtowaniu środowiska 1997

Jednostki organizacyjne, które posiadają wydane na podstawie dotychczasowych przepisów decyzje w sprawie stref ochronnych, obowiązane są w terminie do 2005 r. do ograniczenia szkodliwego oddziaływania na środowisko do terenu, do którego posiadają tytuł prawny.

- ⇨ Obowiązek zmniejszenia zasięgu oddziaływania albo
- ⇨ Obowiązek nabycia prawa do terenu (≠ terenu) do granic zasięgu oddziaływania

POWIETRZE

Wybrane aspekty prawa ochrony środowiska w Polsce

SANDARDY EMISYJNE

dla:

- procesu energetycznego spalania paliw,
- procesu spalania i współspalania odpadów,
- procesu produkcji lub obróbki wyrobów azbestowych,
- procesu produkcji dwutlenku tytanu w przypadku stosowania do rafinacji dwutlenku tytanu, reakcji sulfonowania lub chlorowania,
- procesów, w których używane są rozpuszczalniki organiczne.

W pozostałym zakresie o dopuszczalności i wielkości emisji decyduje zasadniczo lokalny, aktualny stan jakości powietrza.

Wybrane aspekty prawa ochrony środowiska w Polsce

Podstawowe wymagania w zakresie ochrony powietrza kształtują się następująco:

(a) Wprowadzanie pyłów lub gazów do powietrza wymaga **pozwolenia**.

(b) W drodze rozporządzenia zostaną określone przypadki, w których wprowadzanie gazów lub pyłów do powietrza nie będzie wymagało pozwoleń.

(c) W przypadku, gdy nie jest wymagane pozwolenie na wprowadzanie gazów lub pyłów do powietrza, ale instalacja może negatywnie oddziaływać na środowisko, wymagane może być zgłoszenie faktu wprowadzania gazów lub pyłów do powietrza staroście. Rodzaje instalacji, z których emisja nie wymaga pozwolenia, a których eksploatacja wymaga zgłoszenia zostały określone w *rozporządzeniu Ministra Środowiska z dnia 20.11.2001 r.* w sprawie rodzajów instalacji, których eksploatacja wymaga zgłoszenia (Dz.U. *Nr 140, poz. 1585*).

W przypadku, gdy pozwolenie na wprowadzanie gazów lub pyłów do powietrza jest wymagane, w celu jego uzyskania należy złożyć wniosek o wydanie pozwolenia na wprowadzanie gazów lub pyłów do powietrza.

PRAWO OCHRONY ŚRODOWISKA

NIE WYMAGA POZWOLENIA WPROWADZANIE GAZÓW LUB PYŁÓW DO POWIETRZA Z INSTALACJI:

INFORMACJE AKTUALNE, ALE NIEOBECNE JUŻ W USTAWIE

1) z których wprowadzanie gazów lub pyłów do powietrza odbywa się w *sposób niezorganizowany, bez pośrednictwa przeznaczonych do tego celu* środków technicznych,
2) wentylacji grawitacyjnych,
3) energetycznych:
a) opalanych węglem kamiennym o łącznej nominalnej mocy do 5 MWt,
b) opalanych koksem, drewnem, słomą, olejem napędowym i opałowym o łącznej nominalnej mocy do 10 MWt,
c) opalanych paliwem gazowym o łącznej nominalnej mocy do 15 MWt,

POWIETRZE

PRAWO OCHRONY ŚRODOWISKA

NIE WYMAGA POZWOLENIA WPROWADZANIE GAZÓW LUB PYŁÓW DO POWIETRZA Z INSTALACJI:

INFORMACJE AKTUALNE, ALE NIEOBECNE JUŻ W USTAWIE

4) innych niż energetyczne o łącznej nominalnej mocy do 1 MWt, opalanych węglem kamiennym, koksem, drewnem, słomą, olejem napędowym i opałowym, paliwem gazowym,
5) do przetaczania paliw płynnych,
6) do suszenia zboża,
7) w lakierniach zużywających na dobę mniej niż 3 kg lakierów wodnych i lakierów o wysokiej zawartości cząstek stałych,
8) stosowanych w gastronomii,
9) w oczyszczalniach ścieków,
10) w zbiornikach bezodpływowych kanalizacji lokalnej,
11) w przechowalniach owoców i warzyw,
12) stosowanych w hutach szkła - o wydajności mniejszej niż 1 tona na dobę,

POWIETRZE

PRAWO OCHRONY ŚRODOWISKA

NIE WYMAGA POZWOLENIA WPROWADZANIE GAZÓW LUB PYŁÓW DO POWIETRZA Z INSTALACJI:

INFORMACJE AKTUALNE, ALE NIEOBECNE JUŻ W USTAWIE

13) stosowanych w fermach hodowlanych, z wyłączeniem instalacji zaliczonych do przedsięwzięć mogących znacząco oddziaływać na środowisko, o których mowa w art. 51 ust. 1,
14) do suszenia, brykietowania i mielenia węgla - o mocy przerobowej mniejszej niż 30 ton surowca na godzinę,
15) stosowanych w młynach spożywczych,
16) do produkcji wapna palonego - przy wydajności mniejszej niż 10 ton na dobę.

POWIETRZE

Wybrane aspekty prawa ochrony środowiska w Polsce

OBOWIĄZEK ZGŁOSZENIA

Rodzaje instalacji, z których emisja nie wymaga pozwolenia, a których *eksploatacja wymaga zgłoszenia zostały określone w rozporządzeniu Ministra Środowiska z dnia 20.11.2001 r. w sprawie rodzajów instalacji, których eksploatacja wymaga zgłoszenia (Dz.U. Nr 140, poz.1585)*:

Instalacje niewymagające pozwolenia na wprowadzanie gazów lub pyłów do powietrza, których eksploatacja wymaga zgłoszenia z uwagi na wprowadzanie gazów lub pyłów do powietrza:

1) energetyczne:
- opalane węglem kamiennym o łącznej nominalnej mocy od 0,5 MWt do 5 MWt,
- opalane koksem, drewnem, słomą, olejem napędowym i opałowym o łącznej nominalnej mocy od 1 MWt do 10 MWt,
-opalane paliwem gazowym o łącznej nominalnej mocy od 1 MWt do 15 MWt

2) inne niż energetyczne o łącznej nominalnej mocy od 0,5 MWt do 1 MWt, opalane węglem kamiennym, koksem, drewnem, słomą, olejem napędowym i opałowym, paliwem gazowym

3) do przetaczania paliw płynnych

4) stosowane do suszenia zboża, o wydajności większej niż 30 Mg na godzinę

POWIETRZE

Wybrane aspekty prawa ochrony środowiska w Polsce

OBOWIĄZEK ZGŁOSZENIA

POWIETRZE

5) w lakierniach zuzywajacych na dobe mniej niz 3 kg lakierów wodnych i lakierów o wysokiej zawartosci czastek stalych

6) stosowane w gastronomii, przystosowanej do obslugi wiecej niz 500 osób na dobe

7) w przechowalniach owoców i warzyw, przystosowanych do jednoczesnego przechowywania owoców lub warzyw w ilosci wiekszej niz 50 Mg

8) stosowane w hutach szkla o wydajnosci mniejszej niz 1 Mg na dobe

9) stosowane w fermach hodowlanych, zaliczane do przedsiewziec mogacych znaczaco oddzialywac na srodowisko, dla których sporzadzenie raportu o oddzialywaniu przedsiewziecia na srodowisko moze byc wymagane

10) do suszenia, brykietowania i mielenia wegla o mocy przerobowej mniejszej niz 30 Mg surowca na godzine

11) stosowane w mlynach spozywczych

12) do produkcji wapna palonego o wydajnosci mniejszej niz 10 Mg na dobe

Wybrane aspekty prawa ochrony środowiska w Polsce

W związku z wprowadzaniem pyłów lub gazów do powietrza na przedsiębiorcy ciąży obowiązek wnoszenia kwartalnych **opłat za korzystanie ze środowiska**

na rachunek urzędu marszałkowskiego właściwego ze względu na miejsce korzystania ze środowiska.

W przypadku wprowadzania gazów lub pyłów do powietrza, wynikającego z eksploatacji urządzeń, opłaty te wnosi się

na rachunek urzędu marszałkowskiego właściwego ze względu na miejsce rejestracji podmiotu korzystającego ze środowiska.

EWIDENCJA / OPŁATY

Wybrane aspekty prawa ochrony środowiska w Polsce

- W terminie wniesienia opłaty, marszałkowi województwa należy również przedstawić **wykaz danych**, na podstawie których została wyliczona opłata.
- W razie korzystania ze środowiska bez uzyskania wymaganego pozwolenia lub innej decyzji korzystający ze środowiska ponosi opłatę podwyższoną o 100%,
- a w przypadku korzystania ze środowiska z przekroczeniem lub naruszeniem warunków określonych w pozwoleniu lub innej decyzji, oprócz opłaty ponosi on także karę pieniężną.

Pomiary wielkości emisji : wstępne, okresowe i ciągłe.

Wstępnych pomiarów wielkości emisji dokonuje się w przypadku instalacji nowo zbudowanej lub zmienionej w istotny sposób, z której emisja wymaga pozwolenia. Przypadki, w których jest wymagany ciągły pomiar emisji z instalacji oraz przypadki, w których są wymagane okresowe pomiary emisji z instalacji albo urządzenia, oraz częstotliwości prowadzenia tych pomiarów określa Rozporządzenie Ministra Środowiska z dnia 13 czerwca 2003 r. w sprawie wymagań w zakresie prowadzenia pomiarów wielkości emisji (Dz.U. Nr 110, poz. 1057).

Analyt.
standard emisyjne czy jest (emisyjne, pyłów, TO_2, rozpuszczalniki organiczne).
2. Czy wymagane jest pomiarowe czy przy zgłoszeniu
3. Jeśli pomiarowe to odpowiedzialny
4. Czy wymagane były pomiary?

ODPADY

Wybrane aspekty prawa ochrony środowiska w Polsce

Podstawowym aktem prawnym regulującym to zagadnienie jest ustawa z dnia 27 kwietnia 2001 r. o odpadach.

Wymagania w zakresie gospodarki odpadami w uproszczeniu kształtują się następująco:

§ Zasadą jest, że na tym, kto wytwarza odpady spoczywa obowiązek:

- uzyskania **pozwolenia** na wytwarzanie odpadów,
(jeżeli wytwarza powyżej 1 Mg odpadów niebezpiecznych rocznie lub powyżej 5 tys. Mg odpadów innych niż niebezpieczne rocznie)

- uzyskanie **decyzji zatwierdzającej program gospodarki odpadami niebezpiecznymi**,
(jeżeli wytwarza odpady niebezpieczne w ilości powyżej 0,1 Mg rocznie)

- **przedłożenie informacji** o wytwarzanych odpadach oraz o sposobach gospodarowania wytworzonymi odpadami.
(jeżeli wytwarza odpady niebezpieczne w ilości do 0,1 Mg rocznie albo powyżej 5 Mg rocznie odpadów innych niż niebezpieczne)

Wybrane aspekty prawa ochrony środowiska w Polsce

§ Przedsiębiorca wytwarzający odpady może zlecić wykonanie obowiązku gospodarowania odpadami innemu posiadaczowi odpadów.

Może je jednak przekazywać wyłącznie podmiotom, które uzyskały zezwolenie właściwego organu na prowadzenie działalności w zakresie gospodarki odpadami polegające na:
- odzysku odpadów,
- unieszkodliwianiu odpadów,
- zbieraniu odpadów,
- transporcie odpadów.

Jeżeli bowiem odpad zostanie przekazany podmiotowi, który nie posiada wymaganego zezwolenia, to przekazujący odpady (np. przedsiębiorca) ponosi dalej odpowiedzialność za przekazane odpady i za działania podmiotu, który przejął odpady.

Posiadaczem odpadów jest ta firma, która aktualnie ma te odpady mowa firma transportowa

Wybrane aspekty prawa ochrony środowiska w Polsce

§ Posiadacz odpadów jest obowiązany na bieżąco **prowadzić ich ilościowa i jakościowa ewidencje,** a przekazując odpady odbiorcy odpadów musi za każdym razem **wypełnić odpowiedni formularz karty przekazania odpadu.**

§ Do końca marca musi również sporządzić zbiorcze zestawienie dotyczące ilości odpadów wytworzonych w minionym roku.

EWIDENCJA

Wybrane aspekty prawa ochrony środowiska w Polsce

§ Na wytwarzających odpady spoczywa obowiązek ponoszenia następujących opłat:

- opłaty za składowanie odpadów (za umieszczenie odpadów na składowisku odpadów) – dotyczy zarządzających składowiskami odpadów,
- opłaty podwyższone za nieprawidłowe magazynowanie odpadów w przedsiębiorstwach,
- opłaty podwyższone za składowanie odpadów w miejscu na ten cel nieprzeznaczonym,
- opłaty produktowe za nieosiągnięcie wymaganego przepisami poziomu odzysku i recyklingu odpadów opakowaniowych i poużytkowych.

WZÓR KARTY EWIDENCJI ODPADU

KARTA EWIDENCJI ODPADU | Nr karty | Rok prowadzenia

Kod odpadu

Rodzaj odpadu

Posiadacz odpadów | Adres

Nr REGON | Telefon/fax

Przeznaczenie odpadów: Wł | Za | Tr | Od | Un

Miesiąc	Masa wytworzonych odpadów [Mg]	Masa przyjętych odpadów [Mg]	Nr karty przekazania odpadu	Charakterystyka odpadów: we własnym zakresie – Masa [Mg]	Metoda odzysku R	Metoda unieszkodliwiania D	odpady przekazane innemu posiadaczowi odpadów – Masa [Mg]	Nr karty przekazania odpadu	Podpis osoby sporządzającej dane

ODPADY

WZÓR KARTY PRZEKAZANIA ODPADÓW

ODPADY

KARTA PRZEKAZANIA ODPADU	Nr karty	Rok ewidencji
Posiadacz odpadów, który przekazuje odpad[1]	Posiadacz odpadów, który przejmuje odpad[1]	
Adres[1]	Adres[1]	
Telefon/fax	Telefon/fax	
Nr REGON	Nr REGON	
Kod odpadu / Rodzaj odpadu		
Potwierdzam przekazanie odpadu data, pieczęć i podpis	Potwierdzam przyjęcie odpadu data, pieczęć i podpis	

Data/miesiąc[1]	Masa przekazanych odpadów [Mg][1]	Numer rejestracyjny pojazdu, przyczepy lub naczepy[1]

formularz dwustronny W Rozporządzeniu, więc Każdy posiada taki Sam Sporządzony jest w dwóch egz. (przekazał, odebrał)

WODA

ŚCIEKI

Wybrane aspekty prawa ochrony środowiska w Polsce

VI. GOSPODARKA WODNO-ŚCIEKOWA

Podstawowymi aktami prawnymi w tym zakresie są:

§ ustawa z dnia *18 lipca 2001 r. – Prawo wodne*,
§ ustawa z 7 czerwca 2001 r. o zbiorowym zaopatrzeniu w wodę i zbiorowym odprowadzaniu ścieków.

Wybrane aspekty prawa ochrony środowiska w Polsce

- Korzystanie z wód przez przedsiębiorców ma status szczególnego korzystania z wód i wymaga **pozwolenia wodnoprawnego**.
Korzystaniem takim jest w szczególności:
(a) pobór oraz odprowadzanie wód powierzchniowych lub podziemnych,
(b) wprowadzanie ścieków do wód lub do ziemi,
(c) przerzuty wody oraz sztuczne zasilanie wód podziemnych,
(d) piętrzenie oraz retencjonowanie śródlądowych wód powierzchniowych,
(e) korzystanie z wód do celów energetycznych,
(f) korzystanie z wód do celów żeglugi oraz spławu,
(g) wydobywanie z wód kamienia, żwiru, piasku oraz innych materiałów, a także wycinanie roślin z wód lub brzegu,
(h) rybackie korzystanie ze śródlądowych wód powierzchniowych.

Pozwolenie wodnoprawne należy uzyskać zanim będzie się ubiegać o pozwolenie na budowę.

W szczególnych przypadkach może być wymagane pozwolenie wodnoprawne na odprowadzanie ścieków do kanalizacji

Wybrane aspekty prawa ochrony środowiska w Polsce

=> Pobór wód z wodociągów i odprowadzanie ścieków do kanalizacji regulują umowy w sprawie zaopatrzenia w wodę i odprowadzania ścieków zawierane z przedsiębiorcami wodociągowo-kanalizacyjnymi.
=> Dla oceny, czy ścieki odprowadzane do wód odpowiadają wymaganym warunkom konieczne jest porównanie z wartościami parametrów zanieczyszczeń określonymi w pozwoleniu wodnoprawnym.
=> Przedsiębiorcy obowiązani są do rejestracji ilości pobieranej wody oraz ilości i jakości ścieków odprowadzanych do środowiska, czyli do wód lub do ziemi oraz **wnoszenia opłat za gospodarcze korzystanie ze środowiska**.

EWIDENCJA

=> Pobór wód z wodociągu oraz odprowadzanie ścieków do kanalizacji podlega opłatom określonym w umowie pomiędzy zakładem, a przedsiębiorstwem wodociągowo-kanalizacyjnym.

OPAKOWANIA

Wybrane aspekty prawa ochrony środowiska w Polsce

VII. WYMAGANIA ZWIĄZANE Z WPROWADZANIEM NA RYNEK TOWARÓW W OPAKOWANIACH

Podstawowymi aktami prawnymi w tym zakresie są dwie *ustawy z dnia 11 maja 2001 r.:*

§ *o opakowaniach i odpadach opakowaniowych*

§ *o obowiązkach przedsiębiorców w zakresie gospodarowania niektórymi odpadami oraz o opłacie produktowej i opłacie depozytowej.*

Wybrane aspekty prawa ochrony środowiska w Polsce

Przepisy tych ustaw dotyczą:

•przedsiębiorców wprowadzających na rynek krajowy produkty w opakowaniach wymienionych w załączniku nr 1 do *ustawy o obowiązkach przedsiębiorców w zakresie gospodarowania niektórymi odpadami oraz o opłacie produktowej i opłacie depozytowej* i produkty wymienione w załącznikach nr 2 i 3 do tej ustawy
[w tym - przedsiębiorców, którzy zlecili wytworzenie produktu lub produktu w opakowaniu oraz którego oznaczenie zostało umieszczone na produkcie lub produkcie w opakowaniu],

•przedsiębiorców prowadzących jednostkę handlu detalicznego o powierzchni handlowej powyżej 500 m2, sprzedających produkty tam pakowane,

•przedsiębiorców prowadzących więcej niż jedną jednostkę handlu detalicznego o łącznej powierzchni handlowej powyżej 5000 m2, bez względu na powierzchnię pojedynczej jednostki, sprzedających produkty w tych jednostkach pakowane,

Wybrane aspekty prawa ochrony środowiska w Polsce

Przepisy tych ustaw dotyczą (c.d.):

•przedsiębiorców wprowadzających na rynek krajowy w drodze importu towary, których częściami składowymi lub przynależnościami są produkty wymienione w załącznikach nr 2 i 3 do *ustawy o obowiązkach przedsiębiorców w zakresie gospodarowania niektórymi odpadami oraz o opłacie produktowej i opłacie depozytowej,*
[importerzy - także importerzy importujący towary na potrzeby własne; nie uważa się za importerów przedsiębiorców, którzy dokonują eksportu importowanych uprzednio produktów lub produktów w opakowaniach],

•przedsiębiorców, którzy pakują produkty wytworzone przez innego przedsiębiorcę i wprowadzają je na rynek krajowy.

Wybrane aspekty prawa ochrony środowiska w Polsce

Przedsiębiorca obowiązany jest **zgłosić** fakt rozpoczęcia (30 dni wcześniej) i likwidacji (14 dni wcześniej) działalności podlegającej zapisom ustawy marszałkowi województwa właściwemu ze względu na siedzibę

obowiązek odzysku i recyklingu odpadów opakowaniowych na poziomie określonym w przepisach na dany rok. Obowiązek ten można realizować samodzielnie albo poprzez tzw. organizacje odzysku.

Jeżeli nie zaangażowano organizacji odzysku, a przedsiębiorcy nie uda się osiągnąć wymaganego poziomu odzysku i recyklingu odpadów, obowiązany jest on ustalić i uiścić na konto urzędu marszałkowskiego tzw. **opłatę produktową**.

Wybrane aspekty prawa ochrony środowiska w Polsce

•Przedsiębiorca ponadto ma obowiązek składać **sprawozdanie roczne**, na formularzach określonych rozporządzeniami

•Sprawozdania te składane są marszałkowi województwa w terminie do dnia 31 marca następnego roku.

•Roczne sprawozdanie powinno zawierać informację:
- o wysokości należnej opłaty produktowej,
- o masie wytworzonych, przywiezionych z zagranicy oraz wywiezionych za granicę opakowań.

Istnieje również obowiązek prowadzenia ewidencji opakowań wprowadzanych do obrotu wraz z produktami; ewidencja ta jest podstawą dla wspomnianych sprawozdań składanych corocznie marszałkowi województwa na temat realizacji obowiązku odzysku i recyklingu oraz należnej opłaty produktowej.

EWIDENCJA

GLEBA

ZIEMIA

Wybrane aspekty prawa ochrony środowiska w Polsce

VIII. WYMAGANIA W ZAKRESIE OCHRONY GLEBY I ZIEMI

Najważniejsze przepisy w tym zakresie znajdują się w ustawie z dnia 27 kwietnia 2001 r. Prawo ochrony środowiska oraz ustawie o ochronie gruntów rolnych i leśnych z 1995 r.

Sankcjonują one działania polegające na:
- niekorzystnym przekształceniu ukształtowania terenu,
- zanieczyszczeniu gleby lub ziemi,
- spowodowaniu utraty albo ograniczenia wartości użytkowej gruntów rolnych.

Wybrane aspekty prawa ochrony środowiska w Polsce

Władający powierzchnią ziemi, na której występuje zanieczyszczenie gleby lub ziemi albo niekorzystne przekształcenie naturalnego ukształtowania terenu jest obowiązany do przeprowadzenia ich rekultywacji.

Władający powierzchnią ziemi może się zwolnić od odpowiedzialności tylko w takiej sytuacji, w której wykaże, że ww. zanieczyszczenie albo *niekorzystne przekształcenia spowodował inny, wskazany podmiot. Jeżeli* jednak do takiego niedozwolonego zanieczyszczenia czy przekształcenia doszło za wiedzą lub zgodą władającego powierzchnią ziemi, będzie on obowiązany do rekultywacji na równi ze sprawcą.

Jeśli przedsiębiorca działa na terenie zakupionym od innego podmiotu, albo włada nim w jakiś inny sposób, to dobra praktyka nakazywałaby:
- zbadać grunt,
- w przypadku stwierdzenia zanieczyszczenia – do 30 czerwca 2004 r. zgłosić właściwemu staroście fakt zanieczyszczenia gruntu w przeszłości.

Wybrane aspekty prawa ochrony środowiska w Polsce

Rekultywacja w związku z niekorzystnym przekształceniem naturalnego ukształtowania terenu polega na jego przywróceniu do stanu poprzedniego.

Rekultywacja zanieczyszczonej gleby lub ziemi polega na ich przywróceniu do stanu wymaganego standardami jakości.

Standardy te określa *Rozporządzenie Ministra Środowiska z dnia 9 września 2002 r. w sprawie standardów jakości gleby oraz standardów jakości ziemi (Dz.U. 2002.165.1359 z dnia 4 października 2002 r.).*

HAŁAS

Wybrane aspekty prawa ochrony środowiska w Polsce

IX. OCHRONA PRZED HAŁASEM

Zasadnicze znaczenie dla tej materii mają przepisy ***ustawy Prawo ochrony środowiska z 2001 r.,*** która definiuje hałas jako dźwięki o częstotliwości od 16 Hz do 16 000 Hz.

Traktowany jest on na gruncie tej ustawy jako emisja rozumiana jako wprowadzana bezpośrednio lub pośrednio, w wyniku działalności człowieka, do powietrza energia.

Wybrane aspekty prawa ochrony środowiska w Polsce

Obowiązki przedsiębiorcy:

Na etapie inwestycyjnym przedsiębiorca powinien zadbać, aby w fazie planowania i budowy swojego zakładu zagadnienia związane z hałasem zostały uwzględnione przez projektanta, który powinien zapewnić, że poziom hałasu nie będzie przekraczał dopuszczalnych norm (norm środowiskowych).

Na etapie eksploatacji, przedsiębiorca nie musi z góry uzyskiwać pozwolenia na emitowanie hałasu.

Na etapie eksploatacji przedsiębiorca powinien dbać o odpowiedni poziom hałasu w środowisku pracy, czyli o ten poziom hałasu, który ma przede wszystkim wpływ na pracowników.

Przedsiębiorca powinien również dbać o to, by poziom hałasu „na granicy działki zakładu" nie przekraczał limitów określonych dla różnego rodzaju terenów (zasadniczo ciszej musi być tam, gdzie mieszkają ludzie, a głośniej może być tam, gdzie ludzie pracują, handlują, jeżdżą samochodami).

Wybrane aspekty prawa ochrony środowiska w Polsce

W przypadku przekroczenia poziomu hałasu poza granicą działki zakładu i stwierdzenia tego przekroczenia przez wojewódzkiego inspektora ochrony środowiska lub inną upoważnioną służbę kontrolną, przedsiębiorca otrzyma ze starostwa (albo z urzędu wojewódzkiego) postanowienie, z którego będzie wynikał obowiązek wystąpienia o pozwolenie na emisję hałasu.

Zakład występuje o pozwolenie na emisję hałasu przygotowując odpowiedni wniosek.

Po otrzymaniu pozwolenia na emisję hałasu, za każde przekroczenie przez przedsiębiorcę dopuszczalnego poziomu hałasu, będzie on zmuszony płacić surowe kary.

DRZEWA

KRZEWY

W trakcie realizacji inwestycji, ale również w trakcie eksploatacji obiektów, może powstać konieczność **usunięcia drzew lub krzewów.**

W takim przypadku przedsiębiorca musi zawczasu uzyskać niezbędne zezwolenie i wnieść opłaty.

DRZEWA LUB KRZEWY

KARY

Wybrane aspekty prawa ochrony środowiska w Polsce

X. KARY ZA NIEWYKONYWANIE OBOWIĄZKÓW OCHRONY ŚRODOWISKA

Odpowiedzialność za nieprzestrzeganie wymogów w zakresie ochrony środowiska istnieje niezależnie od wystąpienia skutku w postaci zanieczyszczenia środowiska.
Fakt spowodowania zagrożenia dla środowiska (w tym zdrowia ludzi) w następstwie działań lub zaniechań przedsiębiorców może skutkować skumulowaną odpowiedzialnością:
- **cywilną** (np. żądanie przywrócenia stanu zgodnego z prawem i podjęcia środków zapobiegawczych, w szczególności przez zamontowanie instalacji lub urządzeń zabezpieczających przed zagrożeniem lub naruszeniem),
- **administracyjną** (np. nakaz wstrzymania działalności przedsiębiorstwa),
- **karną**.

Jeżeli chodzi o odpowiedzialność karną, to należy zauważyć, że nowe przepisy z zakresu ochrony środowiska znacznie zwiększyły katalog obowiązków zagrożonych karami, a w obowiązującym Kodeksie Karnym znalazł się rozdział obejmujący przestępstwa przeciwko środowisku.

Wybrane aspekty prawa ochrony środowiska w Polsce

Do najważniejszych przestępstw przeciwko środowisku, które powiązane są z działalnością gospodarczą, należą:

§ składowanie, usuwanie, przerabianie, unieszkodliwianie albo przewóz wbrew przepisom, choćby nieumyślnie, odpadów lub substancji w takich warunkach lub w taki sposób, że może to zagrozić życiu lub zdrowiu wielu osób lub spowodować zniszczenie w świecie roślinnym lub zwierzęcym w znacznych rozmiarach; także - dopuszczanie wbrew obowiązkowi do popełnienia ww. czynu,
§ wywóz wbrew przepisom za granicę odpadów niebezpiecznych,
§ sprowadzanie wbrew przepisom z zagranicy, choćby nieumyślnie, odpadów lub substancji zagrażających środowisku bądź też dopuszczanie wbrew obowiązkowi do popełnienia ww. czynu,
§ nie utrzymywanie w należytym stanie lub nie używanie wbrew obowiązkowi, choćby nieumyślnie, urządzeń zabezpieczających wodę, powietrze lub ziemię przed zanieczyszczeniem,
§ powodowanie, choćby nieumyślnie, zniszczenia w świecie roślinnym lub zwierzęcym w znacznych rozmiarach,

Wybrane aspekty prawa ochrony środowiska w Polsce

§ wznoszenie nowego lub powiększanie wbrew przepisom istniejącego obiektu budowlanego na terenie objętym ochroną ze względów przyrodniczych lub krajobrazowych albo w otulinie takiego terenu, albo prowadzenie tam działalności gospodarczej zagrażającej środowisku,
§ uniemożliwianie lub utrudnianie korzystania z wody do zwalczania poważnych awarii, klęsk żywiołowych, pożarów albo innych miejscowych zagrożeń lub do zapobieżenia poważnemu niebezpieczeństwu grożącemu życiu, zdrowiu osób lub mieniu znacznej wartości,
§ wykonywanie w pobliżu urządzeń wodnych robót lub czynności zagrażających tym urządzeniom,
§ niszczenie lub uszkadzanie brzegów śródlądowych wód powierzchniowych, tworzących brzeg wody budowli lub murów nie będących urządzeniami wodnymi oraz gruntów pod śródlądowymi wodami powierzchniowymi albo utrudnianie przepływu wody w związku z wykonywaniem lub utrzymywaniem urządzeń wodnych.

Wybrane aspekty prawa ochrony środowiska w Polsce

Czyny powyższe zagrożone są karą pozbawienia wolności najczęściej w rozmiarze

od 3 miesięcy do lat 5,
a w razie ich nieumyślności – do lat 2.

Jeżeli jednak wyrządzana jest szkoda w znacznych rozmiarach zagrożenie karne wzrasta do przedziału

od 6 miesięcy do lat 8.

Najwyższa kara przewidziana jest w przypadku, gdy następstwem *nieprawidłowej gospodarki odpadami jest śmierć człowieka* lub ciężki uszczerbek na zdrowiu wielu osób –

od lat 2 do 12.

EMAS

eko-net.pl

EMAS I (nieaktualny)

Rozporządzenie Rady Wspólnot Europejskich w sprawie dopuszczenia do dobrowolnego udziału przedsiębiorstw sektora przemysłowego Wspólnoty w systemie eko-zarządzania i eko-auditów".

Rozporządzenie EMAS zostało przyjęte 29 czerwca 1993 roku, a 10 lipca 1993 zostało opublikowane w Dzienniku Ustaw Wspólnoty Europejskiej.

W oryginale nazwa rozporządzenia brzmi: "Council Regulation (EEC) No. 1836/93 of 29 June 1993 allowing voluntary participation by companies in the industrial sector in a Community Eco-Management and Audit scheme, Official Journal of the European Communities, 10 July, 1993.

eko-net.pl

EMAS I (nieaktualny)

- Rozporządzenie EMAS składa się z 21 artykułów i 5 załączników.
- EMAS wszedł w życie w kwietniu 1995. W ciągu 21 miesięcy od publikacji rozporządzenia do jego wejścia w życie każde państwo członkowskie UE miało obowiązek:
  - powołać jednostkę kompetentną odpowiedzialną za ustanowienie systemu i administrowanie systemem EMAS w danym kraju;
  - wyznaczyć organizację akredytacyjną, akredytującą i nadzorującą akredytowanych weryfikatorów środowiskowych.

eko-net.pl

zeszyty się wyjęte i tam
zwiększyć się wymagania
w przeciwieństwie do ISO
14001

EMAS nowela

NOWELIZACJA ROZPORZĄDZENIA EMAS

Na początku lipca 1999 roku Komisja Europejska przedłożyła Parlamentowi Europejskiemu i Radzie Europejskiej propozycję nowelizacji rozporządzenia EMAS. Główne proponowane zmiany są następujące:

- udostępnienie systemu EMAS dla wszystkich organizacji, a nie tylko dla przedsiębiorstw przemysłowych;
- przyjęcie normy EN ISO 14001: 1996 jako specyfikacji wymagań dla systemu zarządzania środowiskowego w ramach EMAS;
- dodanie wymagania pełnego włączenia pracowników w proces wdrażania EMAS;
- utworzenie mechanizmów umożliwiających szersze uczestnictwo MŚP w systemie EMAS.

eko-net.pl

EMAS nowela

Podstawowe dwie informacje, jakie płyną po analizie nowelizacji EMAS są następujące:

- **wdrożenie SZŚ zgodnego z wymaganiami normy ISO 14001 jest naturalnym krokiem w kierunku EMAS;**
- **stworzone zostaną warunki dla MŚP, które zachęcą je do wdrażania EMAS, a więc coraz więcej przedsiębiorstw będzie działać zgodnie z zasadami systemu zarządzania środowiskowego.**

eko-net.pl

EMAS II

„Rozporządzenie (UE) nr 761/2001 Parlamentu Europejskiego i Rady z 19 marca 2001 r. w sprawie dopuszczenia do dobrowolnego udziału organizacji we Wspólnotowym systemie eko-zarządzania i eko-auditów".

Rozporządzenie EMAS zostało przyjęte 19 marca 2001 r. roku, a 24 kwietnia 2001 r. zostało opublikowane w Dzienniku Ustaw Wspólnoty Europejskiej.

W oryginale nazwa rozporządzenia brzmi:
"Regulation (EC) No. 761/2001 of the European Parliament and of the Council of 19 March 2001 allowing voluntary participation by organisations in a Community eco-management and audit scheme (EMAS)
Official Journal of the European Communities, 24.04.2001.

eko-net.pl

EMAS II

18 artykułów

8 załączników

eko-net.pl

EMAS II

Rejestracja w schemacie EMAS:

- **Przeprowadzenie przeglądu środowiskowego zgodnie z wymaganiami zawartymi w Załączniku 7**
  - (w zasadzie zbieżny z wytycznymi z ISO 14004 —> prawo, aspekty, istniejące procedury, poprzednie wypadki
  - + rejestr znaczących aspektów środowiskowych
  - + opis sposobu wyboru znaczących aspektów środowiskowych)

  uwzględniając zagadnienia zawarte w Załączniku 6
  - (w zasadzie zbieżny z wytycznymi z ISO 14004 —> bezpośrednie i pośrednie aspekty środowiskowe oraz kryteria istotności aspektów).

Nie trzeba przeprowadzać przeglądu, jeśli istniejący/funkcjonujący certyfikowany SZŚ wg ISO14001 dostarcza odpowiednie informacje, tzn. zawarte w Załączniku 6.

- **Wdrożenie SZŚ zgodnego z wymaganiami zawartymi w Załączniku 1**
  - A (w głównej części tożsamy z EN ISO 14001
  - B w drugiej części ogólne uwagi: nacisk na zgodność z przepisami, na zmniejszanie obciążenia środowiska, na komunikację zewnętrzną oraz na włączanie pracowników w realizację procesu ciągłego doskonalenia).

eko-net.pl

EMAS II

Rejestracja w schemacie EMAS:

- **Przeprowadzenie wewnętrznego auditu SZŚ zgodnie z wymaganiami zawartymi w Załączniku 2**
  - typowe wymagania dot. odpowiedniego przygotowania auditu, odpowiedniej organizacji auditu, zwrócenia uwagi na zgodność z przepisami, na zmniejszanie obciążenia środowiska, dokumentowania auditu, cyklu auditu (3 lata).

- **Przygotowanie oświadczenia (raportu) środowiskowego zgodnie z wymaganiami zawartymi w Załączniku 3**
  - OMÓWIONE NA OSOBNYCH SLAJDACH.

- **Poddanie weryfikacji przez akredytowanego weryfikatora następujących elementów:**
  - **przeglądu środowiskowego,**
  - **systemu zarządzania środowiskowego,**
  - **auditów wewnętrznych,**
  - **oświadczenia (raportu) środowiskowego.**

eko-net.pl

EMAS II

Rejestracja w schemacie EMAS:

- **Wysłanie zweryfikowanego raportu do organu rejestrującego.**
- **Wniesienie odpowiedniej opłaty.**

eko-net.pl

EMAS II

Akredytacja weryfikatorów zgodnie z Załącznikiem 5.

Organ rejestrujący:
- **rejestracja organizacji,**
- **lista weryfikatorów.**

Po zarejestrowaniu w schemacie EMAS można stosować LOGO EMAS:
- **na reklamach,**
- ***na papierze firmowym,***
- **NIE na produktach i opakowaniach (z zastrzeżeniami - żeby nie było wątpliwości, że nie jest to EKO-ZNAK).**

eko-net.pl

EMAS II

Załącznik 3:
Przekazanie informacji zainteresowanym stronom.
Jasna i zwarta forma - również w wersji drukowanej.

Minimalne wymagania dot. informacji zawartej w raporcie:
- przejrzysty opis organizacji, krótka charakterystyka działalności, wyrobów, usług, powiązań z jednostką nadrzędną;
- polityka środowiskowa i krótki opis SZŚ;
- opis wszystkich bezpośrednich i pośrednich aspektów środowiskowych (Załącznik 6);
- opis celów i zadań środowiskowych;
- zestawienie informacji i danych dotyczących obciążenia środowiska wskutek działalności organizacji (w odniesieniu do znaczących aspektów środowiskowych); informacje te mogą obejmować dane dotyczące m.in.:
  - emisji do powietrza,
  - wytwarzania odpadów,
  - zużycia surowców,
  - zużycia wody,
  - zużycia energii,
  - emisji hałasu.

eko-net.pl

EMAS II

Załącznik 3:

- **inne zagadnienia dotyczące obciążenia środowiska wskutek działania organizacji oraz zagadnienia związane osiąganiem zgodności z wymaganiami prawnymi;**
- **nazwa (nazwisko) akredytowanego weryfikatora, numer akredytacji weryfikatora oraz data weryfikacji.**

Coroczna aktualizacja informacji w raporcie (wraz z jej weryfikacją).

Różne inne rodzaje przekazu informacji, utworzenie raportów kierowanych do specyficznego odbiorcy (w oparciu o pełen raport) - może być logo EMAS, jeśli jest to informacja zweryfikowana.

Dostępność publiczna.

Dla MSP - jeśli nie ma zmian to ciągu roku to nie musi publikować

Logo

Version 1

EMAS

VERIFIED ENVIRONMENTAL MANAGEMENT

REG NO

Version 2

EMAS

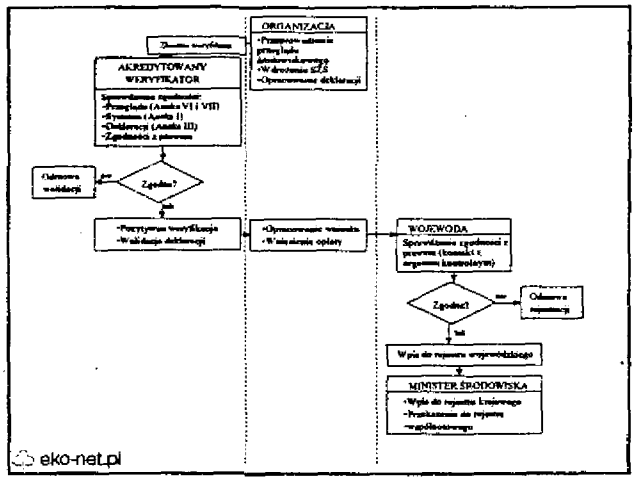
VALIDATED INFORMATION.

REG.NO.

EMAS w Polsce

W Polsce system rejestracji w systemie EMAS opiera sie (poza samym Rozporzadzeniem EMAS) na:

- ustawie z dnia 12 marca 2004 r. o krajowym systemie ekozarzadzania, audytu (EMAS); oraz
- rozporzadzeniu Ministra Srodowiska z dnia 23 kwietnia 2004 r. w sprawie wzoru wniosku o wpis podmiotu do rejestru weryfikatorów srodowiskowych oraz wzorów dokumentów, formy, czestotliwosci i *terminów przekazywania informacji z rejestru wojewódzkiego do rejestru* krajowego ().
- rozporzadzeniu Ministra Srodowiska z dnia 23 kwietnia 2004 r. w sprawie zakresu danych, które zawiera rejestr wojewódzki oraz wzoru wniosku o rejestracje organizacji w rejestrze wojewódzkim.
- rozporzadzeniu Mlnistra Srodowiska z dnia 23 kwietnia 2004 r. w sprawie współczynników róznicujacych wysokosc oplaty rejestracyjnej w krajowym systemie ekozarzadzania i audytu (EMAS)



eko-net.pl

E M A S w Polsce

Opłata rejestracyjna

- Wysokość podstawowa - 1000 zł.
- Współczynniki zmniejszające dla:
  - organizacji pożytku publicznego, placówek oświatowo-wychowawczych i jednostek sektora finansów publicznych - 0,005.
  - podmiotów gospodarczych zatrudniających:
    - do 5 osób – 0,10
    - od 6 do 20 – 0,15
    - od 21 do 50 – 0,25
    - od 51 do 250 – 0,35
    - od 251 do 500 – 0,50.

eko-net.pl

Raporty środowiskowe wg EMAS II

Wymagania minimum:

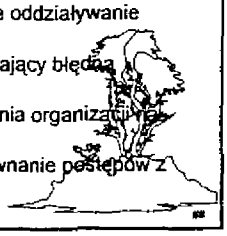
- opis działalności przedsiębiorstwa
- polityka środowiskowa i opis problemów środowiskowych
- opis znaczących aspektów środowiskowych i związanych oddziaływań na środowisko
- cele i zadania
- podsumowanie wyników w zakresie ochrony środowiska umożliwiające porównanie z wcześniejszymi okresami
- inne czynniki w tym zgodność z wymaganiami prawa
- nazwisko (nazwa) i numer akredytacyjny weryfikatora oraz data potwierdzenia

eko-net.pl

Raporty środowiskowe wg EMAS II

Raport może być oznaczony logo EMAS, jeśli dane w nim zawarte zostały zweryfikowane przez upoważnioną osobę oraz spełniają następujące warunki:

- są dokładne i obiektywne
- potwierdzone i weryfikowalne
- odpowiednie dla organizacji i użyte we właściwym kontekście,
- stanowią prawdziwe odzwierciedlenie oddziaływanie organizacji na środowisko
- przedstawione w sposób uniemożliwiający błędną interpretację
- istotne z punktu widzenia oddziaływania organizacji na środowisko
- informacje powinny umożliwiać porównanie postępów z wcześniejszymi raportami



Pozwolenia zintegrowane

Pozwolenia zintegrowane

•Obowiązująca od 1 października 2001r. ustawa ***Prawo ochrony rodowiska*** wprowadziła do polskiego systemu prawnego obowiązek uzyskania pozwolenia zintegrowanego dla instalacji, których działanie wiąże się ze znacznym oddziaływaniem na środowisko.

•Obowiązek ten jest konsekwencją transpozycji do polskiego prawa unijnej Dyrektywy 96/61/WE w sprawie zintegrowanego zapobiegania i ograniczania zanieczyszczeń (**IPPC**).

DYREKTYWA IPPC

Dyrektywa IPPC nakłada na operatorów wybranych typów instalacji obowiązek:

- **uzyskiwania *zintegrowanego pozwolenia* – warunkującego możliwość podejmowania i prowadzenia wybranych rodzajów działalności przemysłowej (określonych w Aneksie I do Dyrektywy 96/61/WE);**
- **dostosowywania się do wymagań BAT (Najlepszej Dostępnej Techniki), jako warunku uzyskania *zintegrowanego pozwolenia;***
- **optymalizowania oddziaływań w celu zapewnienia wysokiego stopnia ochrony środowiska jako całości;**
- **unikania ochrony jednego komponentu środowiska, kosztem zwiększenia zanieczyszczenia innego.**

DYREKTYWA IPPC

23 ARTYKUŁY + 4 ZAŁĄCZNIKI

1. **Kategorie działalności przemysłowej, o których mowa w artykule 1**
2. **Lista dyrektyw WE, o których mowa w artykułach 18 (2) i 20**
3. **Lista głównych substancji zanieczyszczających, które mają być uwzględniane przy ustalaniu granicznych wielkości emisji**
4. **Zagadnienia, które należy wziąć pod uwagę ogólnie lub w konkretnych przypadkach przy określaniu najlepszych dostępnych technik, zgodnie z Artykułem 2 (11), mając na *względzie prawdopodobne koszty i zyski wynikające* z zastosowania metod i zasad przezorności i zapobiegania**

DYREKTYWA IPPC

Artykuł 1. Cel i zakres

Osiągnięcie zintegrowanego zapobiegania i ograniczania zanieczyszczeń związanych z rodzajami działalności wymienionymi w Załączniku 1.

Rodzaje działalności wymienione w Załączniku 1

na następnym slajdzie

DYREKTYWA IPPC

Aneks I do Dyrektywy IPPC:

1. **Przemysł energetyczny**
2. **Produkcja i obróbka metalu**
3. **Przemysł mineralny**
4. **Przemysł chemiczny**
5. **Gospodarka odpadami**
6. **Inne rodzaje działalności**

DYREKTYWA IPPC

Priorytety:

- Zapobieganie powstawaniu zanieczyszczeń (oddziaływań, uciążliwości);
- Ograniczanie oddziaływań, którym nie można w racjonalny sposób zapobiegać;
- Minimalizowanie oddziaływania na poszczególne komponenty środowiska oraz na środowisko jako całość;

oraz

- spełnianie wymagań wynikających z *najlepszej dostępnej techniki*

DYREKTYWA IPPC

KORZYŚĆ DLA PRZEMYSŁU:

- **Jedno pozwolenie na korzystanie ze środowiskowa.**
- **Jednokrotne przejście zakładu przez procedurę i pozwolenie wydane kompleksowo na wszystko, co dotyczy ochrony środowiska.**

KORZYŚĆ DLA OCHRONY ŚRODOWISKA:

- **Eliminacja ochrony jednego komponentu środowiska kosztem innego.**
- **Standardy automatycznie zmienne w czasie.**
- **Objęcie regulacją obszarów dotychczas nieregulowanych.**

DYREKTYWA IPPC

Terminy:

dla nowych instalacji wymagania Dyrektywy stosuje się od wejścia dyrektywy w życie (30 X 1999 r. - w Polsce wejście w życie odpowiednich przepisów ustawy POŚ - 1 I 2002 r.),

dla istniejących instalacji - okres dostosowawczy do 30 X 2007 r.

eko-net.pl

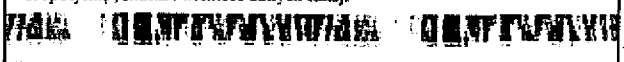
28

DYREKTYWA IPPC

Załącznik IV do Dyrektywy:

Określając najlepsze dostępne techniki ogólnie lub w konkretnych przypadkach uwzględniając prawdopodobne koszty i korzyści wynikające z zastosowania określonego rozwiązania oraz zasady przezorności i zapobiegania należy wziąć pod uwagę następujące zagadnienia :

1. wykorzystanie technologii nisko odpadowych
2. wykorzystanie mniej niebezpiecznych substancji
3. wzrost stopnia odzysku i recyklingu substancji wytwarzanych i wykorzystywanych w procesach oraz odpadów
4. porównywalne procesy, urządzenia lub metody działania, które sprawdziły się w użyciu na skalę przemysłową
5. postęp technologiczny i rozwój wiedzy
6. specyfikę , skutki i wielkość danych emisji



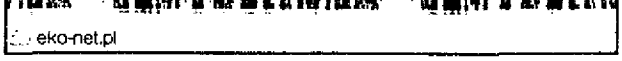
eko-net.pl

jeżeli coś udowodniono że jest niezbędne to dla a pk nie to z zatrucia jest szkodliwe

DYREKTYWA IPPC

Załącznik IV c.d.

7. terminy przekazania do eksploatacji nowych i istniejących instalacji
8. czas potrzebny do wprowadzenia najlepszej dostępnej techniki
9. wielkość zużycia i właściwości surowców (włączając wodę) wykorzystywanych w procesie oraz ich wydajność energetyczną
10. potrzebę zapobiegania lub redukcji do minimum całkowitego wpływu na środowisko oraz związanych z tym zagrożeń
11. potrzebę zapobiegania wypadkom oraz minimalizacji skutków dla środowiska.
12. informacje opublikowane przez Komisję zgodnie z Artykułem 16 (2) lub przez organizacje międzynarodowe



eko-net.pl

Podstawy prawne w Polsce

- Ustawa z dnia 27 kwietnia 2001 roku - Prawo ochrony środowiska (Dz. U. Nr 62, poz. 627 z pózn. zm.)
- Ustawa z dnia 27 lipca 2001 roku o wprowadzeniu ustawy - Prawo ochrony środowiska, ustawy o odpadach oraz o zmianie niektórych ustaw (Dz. U. Nr 100, poz. 1085 z pózn. zm.)
- Ustawa z dnia 27 kwietnia 2001 roku o odpadach (Dz. U. Nr (Dz. U. Nr 62, poz. 628 z pózn. zm.)
- Ustawa z dnia 18 lipca 2001 roku Prawo wodne (Dz. U. Nr 115 poz. 1229 z pózn. zm.);
- Akty wykonawcze do w/w ustaw

Podstawy prawne w Polsce

- Rozporządzenie Ministra Środowiska z dnia 26 lipca 2002 r w sprawie rodzajów instalacji mogących powodować znaczne zanieczyszczenie poszczególnych elementów przyrodniczych albo środowiska jako całości (Dz.U. Nr 122 poz. 1055)
- Rozporządzenie Ministra Środowiska z dnia 4 listopada 2002 r. w sprawie wysokości opłat rejestracyjnych (Dz.U. Nr 190, poz. 1591);
- Rozporządzenie Ministra Środowiska z dnia 8 kwietnia 2003r. w sprawie rodzajów instalacji, dla których prowadzący mogą ubiegać się o ustalenie programu dostosowawczego (Dz.U. Nr 80, poz. 731);
- Rozporządzenie Ministra Środowiska z dnia 26 września 2003 r. w sprawie późniejszych terminów do uzyskania pozwolenia zintegrowanego (Dz.U. Nr 177, poz. 1776).

Pozwolenia zintegrowane

Obowiązki prowadzącego instalacje wymagającą pozwolenia zintegrowanego:

- **zapobieganie lub *(jeżeli nie jest to możliwe) skuteczne* ograniczanie wprowadzania do środowiska substancji lub energii (art. 137 POŚ),**
- **nieprzekraczanie standardów emisyjnych (art.141 POŚ),**
- **niepogorszanie stanu środowiska w znacznych rozmiarach lub zagrożenia życia lub zdrowia ludzi (art.141 POŚ),**
- **nieprzekraczanie standardów jakości środowiska poza terenem, do którego ma tytuł prawny (art.144 POŚ),**

Pozwolenia zintegrowane

Obowiązki cd. :

- **zapewnienie, że emisja w warunkach normalnego funkcjonowania instalacji, nie będzie większa niż wynikająca z prawidłowej eksploatacji instalacji, dla poszczególnych wariantów funkcjonowania (art.188 POŚ),**
- **spełnianie wymagań *najlepszej dostępnej techniki (BAT)*, a zwłaszcza dotrzymywanie *granicznych wielkości emisyjnych* ustalonych w odniesieniu do wymagań BAT (art. 204 POŚ)**

Pozwolenia zintegrowane

Pozwolenie zintegrowane zastępuje następujące pozwolenia na wprowadzanie do środowiska substancji lub energii:

- na wprowadzanie gazów lub pyłów do powietrza
- na emitowanie hałasu do środowiska
- na wytwarzanie odpadów (wraz z zezwoleniami na odzysk, unieszkodliwianie, transport i gromadzenie odpadów)
- wodnoprawne na wprowadzanie ścieków do wód lub do ziemi (łącznie z określeniem warunków poboru wody)
- na emitowanie pól elektromagnetycznych.

Pozwolenia zintegrowane

Warunki emisji ustala się w *pozwoleniu zintegrowanym* na zasadach określonych dla poszczególnych oddziaływań na środowisko, określając:

- wielkość emisji gazów lub pyłów wprowadzanych do powietrza z instalacji;
- dopuszczalny poziom hałasu;
- warunki wytwarzania i sposoby postępowania z odpadami;
- warunki odprowadzania ścieków do wód lub do ziemi oraz warunki poboru wód;
- warunki odprowadzania ścieków do kanalizacji (jeżeli sytuacja taka ma miejsce);
- warunki emisji pól elektromagnetycznych (jeżeli instalacja spełnia w tym zakresie kryteria określone w ustawie);

Pozwolenia zintegrowane

Ponadto pozwolenie zintegrowane musi określać:

- *sposoby osiągania wysokiego poziomu ochrony środowiska jako całości*
- sposoby zapobiegania występowaniu i ograniczania skutków awarii oraz wymóg informowania o wystąpieniu awarii, jeżeli nie dotyczy to zakładów, o których mowa w art. 248 ust. 1,
- *sposoby postępowania w przypadku zakończenia eksploatacji* instalacji, w tym sposoby usunięcia negatywnych skutków powstałych w środowisku w wyniku prowadzonej eksploatacji, gdy są one przewidywane,
- sposoby zapewnienia efektywnego wykorzystania energii.

INSTALACJA

definicja z ustawy Prawo Ochrony Środowiska

Instalacja:

a) stacjonarne urządzenie techniczne,

b) zespół stacjonarnych urządzeń technicznych powiązanych technologicznie, do których tytułem prawnym dysponuje ten sam podmiot i położonych na terenie jednego zakładu,

c) budowle niebędące urządzeniami technicznymi ani ich zespołami,

których eksploatacja może spowodować emisję.

INSTALACJA

Interpretacja Ministerstwa Środowiska

- Zgodnie z definicją pozwolenie zintegrowane obejmuje wszystkie, zlokalizowane na terenie danego zakładu urządzenia, pomiędzy którymi ma miejsce powiązanie technologiczne – czyli wszystkie urządzenia od punktu dostarczania surowców lub półproduktów do miejsca odbioru produktów, zgodnie ze schematem, obejmującym wszystkie operacje i procesy potrzebne do produkcji wyrobów.
- Prowadzący instalację powinien sam określić zgodnie ze znajomością technologii produkcji jakie jest powiązanie technologiczne poszczególnych urządzeń tworzących instalację uwzględniając wszystkie etapy procesu produkcji od dostarczenia surowców lub półproduktów do miejsca odbioru produktów.

INSTALACJA

Interpretacja Ministerstwa Środowiska

Ustawa nie definiuje pojęcia *stacjonarny*. Dlatego pod tym pojęciem należy rozumieć, zgodnie z jego potocznym znaczeniem: nie zmieniający *miejsca położenia, pozostający na miejscu* (*Słownik języka polskiego*, Wydawnictwo Naukowe PWN Warszawa 1992 T. III s. 313). Stąd pod pojęciem *stacjonarnego* urządzenia technicznego lub zespołu urządzeń (art. 3 pkt. 6 lit. a i b ustawy - Prawo ochrony środowiska) należy rozumieć urządzenie (zespół urządzeń), które ze względu na swój charakter przeznaczone jest do użycia w określonym miejscu i w ramach jego zwykłej eksploatacji pozostaje ono w jednym miejscu (nie następują zmiany jego położenia). Trzeba zastrzec, iż instalacją w rozumieniu ustawy jest jedynie urządzenie stacjonarne (ich zespół), które mogą powodować emisje w rozumieniu art. 3 pkt. 4 ww. ustawy (art. 3 pkt. 6 *in fine* ustawy).

EMISJA

definicja z ustawy Prawo Ochrony Środowiska

emisja

wprowadzane bezpośrednio lub pośrednio, w wyniku działalności człowieka, do powietrza, wody, gleby lub ziemi:

a) substancje,

b) energie, takie jak ciepło, hałas, wibracje lub pola elektromagnetyczne,

PROWADZĄCY INSTALACJĘ

definicja z ustawy Prawo Ochrony Środowiska

prowadzący instalację:

podmiot uprawniony na podstawie określonego tytułu prawnego do władania instalacją w celu jej eksploatacji zgodnie z wymaganiami ochrony środowiska, na zasadach wskazanych w ustawie,

tytuł prawny:

prawo własności, użytkowanie wieczyste, trwały zarząd, ograniczone prawo rzeczowe albo stosunek zobowiązaniowy;

PROWADZĄCY INSTALACJĘ

definicja z ustawy Prawo Ochrony Środowiska

zakład:

jedna lub kilka instalacji wraz z terenem, do którego prowadzący instalacje posiada tytuł prawny, oraz znajdującymi się na nim urządzeniami

Pozwolenia zintegrowane

„Wiele mniejszych zakładów pracuje nieregularnie w zależności od zapotrzebowania rynku. Wielkość produkcji może być w tym przypadku niepewnym wskaźnikiem rzeczywistej wydajności instalacji oraz nie odzwierciedla rzeczywistego oddziaływania na środowisko instalacji. W związku z tym, zdaniem Komisji, jedynym technicznie logicznym określeniem "wydajności" w tym przypadku, jest zdolność produkcyjna instalacji. Zdolność ta powinna być określona przy założeniu, że istniejąca instalacja pracuje przez 24 godziny na dobę, jeżeli jest to technicznie możliwe „

Communication from the Commission to the Council, the European Parliament, the European Economic and Social Committee and the Committee of the Regions "On the Road to Sustainable Production, progress in implementing Council Directive 96/61/EC concerning integrated pollution prevention and control"

Pozwolenia zintegrowane

Art. 203. Instalacje, o których mowa w art. 201 ust. 1, położone na terenie jednego zakładu obejmuje się jednym pozwoleniem zintegrowanym.

Pozwolenia zintegrowane

Art. 365. 1. Wojewódzki inspektor ochrony środowiska wstrzyma, w drodze decyzji, użytkowanie instalacji:

1) eksploatowanej bez wymaganego pozwolenia zintegrowanego,
2) eksploatowanej z naruszeniem warunków pozwolenia zintegrowanego przez okres przekraczający 6 miesięcy.

Brak wymaganego pozwolenia zintegrowanego skutkuje wstrzymaniem działalności – jest to więc **rodzaj licencji na prowadzenie działalności.**

Pozwolenia zintegrowane

Art. 186. Organ właściwy do wydania pozwolenia odmówi jego wydania, jeżeli:

1) nie są spełnione wymagania, o których mowa w art. 141 ust. 2, art. 143 i 204 ust. 1 lub przepisach ustawy o odpadach,
2) eksploatacja instalacji powodowałaby przekroczenie dopuszczalnych standardów emisyjnych,
3) eksploatacja instalacji powodowałaby przekroczenie standardów jakości środowiska,

(Planowane są zmiany umożliwiające realizację działań dostosowawczych po uzyskaniu pozwolenia).

ISTOTNA ZMIANA INSTALACJI

definicja z ustawy Prawo Ochrony Środowiska

istotna zmiana instalacji:

taka zmiana sposobu funkcjonowania instalacji lub jej rozbudowa, która może powodować zwiększenie negatywnego oddziaływania na środowisko

Wg Ministerstwa Środowiska nie ma jednoznacznych kryteriów oceny „istotności" zmian. Każdy przypadek należy rozpatrywać indywidualnie.

Najlepsza Dostępna Technika - BAT

definicja z ustawy Prawo Ochrony Środowiska

Najbardziej efektywny oraz zaawansowany poziom rozwoju technologii i metod prowadzenia danej działalności, wykorzystywany jako podstawa ustalania granicznych wielkości emisyjnych, mających na celu eliminowanie emisji lub, jeżeli nie jest to praktycznie możliwe, ograniczanie emisji i wpływu na środowisko jako całość, z tym że pojęcie:

eko-net.pl

Najlepsza Dostępna Technika - BAT

definicja z ustawy Prawo Ochrony Środowiska

(a) "technika" oznacza zarówno stosowaną technologię, jak i sposób, w jaki dana instalacja jest *projektowana, wykonywana, eksploatowana oraz likwidowana*,

technika jest czymś szerszym niż technologia

eko-net.pl

Najlepsza Dostępna Technika - BAT

definicja z ustawy Prawo Ochrony Środowiska

b) "dostępne techniki" oznacza techniki o takim stopniu rozwoju, który umożliwia ich praktyczne zastosowanie w danej dziedzinie przemysłu, z uwzględnieniem warunków ekonomicznych i technicznych oraz rachunku kosztów inwestycyjnych i korzyści dla środowiska, a które to techniki prowadzący daną działalność może uzyskać,

[w projekcie ustawy było jeszcze (*na rozsądnych warunkach, niezależnie czy są one wykorzystywane lub oferowane na terenie kraju, czy poza jego granicami*)]

eko-net.pl

Najlepsza Dostępna Technika - BAT

definicja z ustawy Prawo Ochrony Środowiska

c) "najlepsza technika" oznacza najbardziej efektywną technikę w osiąganiu wysokiego ogólnego poziomu ochrony środowiska jako całości,

eko-net.pl

Najlepsza Dostępna Technika - BAT

BAT jest koncepcją *dynamiczną*, wymagania zmieniają się w czasie tzn. proces dostosowywania się do wymogów BAT ma charakter ciągły. Postęp technologiczny jest źródłem lepszych, efektywniejszych czy tańszych metod ochrony środowiska, opartych przede wszystkim na zasadzie prewencji, czyli *zapobieganiu powstawania zanieczyszcze u źródła*, w miejsce stosowanych urządzeń typu „końca rury", które również są często kosztowne.

eko-net.pl

Najlepsza Dostępna Technika - BAT

- Stosowanie BAT nie jest celem samym w sobie. Celem jest osiąganie maksymalnej możliwej ochrony środowiska jako całości, przy optymalnym zaangażowaniu środków.
- BAT - to nie wymóg zastosowania konkretnego rozwiązania technicznego, ale parametry ekologiczne i techniczne, które są wyznacznikiem dla osiągnięcia pożądanego poziomu oddziaływania na środowisko.

eko-net.pl

Najlepsza Dostępna Technika - BAT

- Ustalenie, co uznaje się za BAT stanowi zasadniczy krok do określenia konkretnych warunków pozwolenia, w szczególności granicznych wartości emisji.
- Wartości graniczne powinny być ustalane w odniesieniu do BAT, ale powinny uwzględniać takie czynniki jak:
  - techniczna charakterystyka rozpatrywanej technologii
  - lokalizacja geograficzna
  - lokalne warunki środowiskowe
- Dyrektywa IPPC nie określa konkretnych wymagań eksploatacyjnych, ustanawia natomiast ramy i zasady, które należy stosować przy wydawaniu pozwoleń.
- Kraje członkowskie mają dużą swobodę, zarówno w kwestii określania BAT jak i uwzględniania czynników lokalnych.
- Istotnym czynnikiem określania BAT jest możliwość pokrycia kosztów związanych z wprowadzeniem BAT przez przedsiębiorstwa w danym sektorze.
- Możliwości pokrycia kosztów przez konkretną firmę nie mogą być uwzględniane przy określaniu BAT.

eko-net.pl

Najlepsza Dostępna Technika - BAT

- **Art. 141.**.1. Eksploatacja instalacji lub urządzenia nie powinna powodować przekroczenia standardów emisyjnych.
- **Art. 144.** 1. Eksploatacja instalacji nie powinna powodować przekroczenia standardów jakości środowiska.

eko-net.pl

Najlepsza Dostępna Technika - BAT

- **Art. 143.** Technologia stosowana w nowo uruchamianych lub zmienianych w sposób istotny instalacjach i urządzeniach powinna spełniać wymagania, przy których określaniu uwzględnia się w szczególności:
  1) stosowanie substancji o małym potencjale zagrożeń,
  2) efektywne wytwarzanie oraz wykorzystanie energii,
  3) zapewnienie racjonalnego zużycia wody i innych surowców oraz materiałów i paliw,
  4) stosowanie technologii bezodpadowych i maloodpadowych oraz możliwość odzysku powstających odpadów,
  5) rodzaj, zasięg oraz wielkość emisji,
  6) wykorzystywanie porównywalnych procesów i metod, które zostały skutecznie zastosowane w skali przemysłowej,
  7) wykorzystanie analizy cyklu życia produktów,
  8) postęp naukowo-techniczny.

eko-net.pl

Najlepsza Dostępna Technika - BAT

Art. 204. 1. Instalacje wymagające pozwolenia zintegrowanego powinny spełniać wymagania ochrony środowiska wynikające z najlepszej dostępnej techniki, a w szczególności, z zastrzeżeniem art. 207 ust. 2, nie mogą powodować przekroczenia granicznych wielkości emisyjnych.

2. Przez graniczne wielkości emisyjne rozumie się takie dodatkowe standardy emisyjne, które nie mogą być przekraczane przez instalacje wymagające pozwolenia zintegrowanego.

Art. 205. Nieprzekraczanie wielkości emisji wynikającej z zastosowania najlepszej dostępnej techniki nie zwalnia z obowiązku dotrzymania standardów jakości środowiska.

eko-net.pl

Najlepsza Dostępna Technika - BAT

- Art. 207. 1. Najlepsza dostępna technika powinna spełniać wymagania, przy których określaniu uwzględnia się jednocześnie:

  1) rachunek kosztów i korzyści,
  2) czas niezbędny do wdrożenia najlepszych dostępnych technik dla danego rodzaju instalacji,
  3) zapobieganie zagrożeniom dla środowiska powodowanym przez emisje lub ich ograniczanie do minimum,
  4) podjęcie środków zapobiegających poważnym awariom przemysłowym lub zmniejszających do minimum powodowane przez nie zagrożenia dla środowiska.

- 1a. Przy określaniu najlepszej dostępnej techniki bierze się pod uwagę wymagania, o których mowa w art. 143, także w przypadku gdy instalacja nie jest nowo uruchamiana lub zmieniana w sposób istotny.

eko-net.pl

Najlepsza Dostępna Technika - BAT

Art. 206. 2. Odstępstwo od granicznych wielkości emisji jest dopuszczalne w zakresie progów tolerancji ustalonych na podstawie art. 206 ust. 2 pkt 3, pod warunkiem że:

1) będzie to z korzyścią dla środowiska jako całości,
2) nie zostaną naruszone standardy emisyjne.

3. Jeżeli graniczne wielkości emisyjne nie zostały określone na podstawie art. 206 ust. 2 pkt 1, dopuszczalną wielkość emisji z instalacji ustala się, uwzględniając potrzebę przestrzegania obowiązujących standardów emisyjnych.

eko-net.pl

Najlepsza Dostępna Technika - BAT

- Art. 206. 2. Minister właściwy do spraw środowiska, w porozumieniu z ministrem właściwym do spraw gospodarki, uwzględniając potrzebę zapewnienia jednolitego podejścia do wydawania zintegrowanych pozwoleń na obszarze całego kraju, może określić, w drodze rozporządzenia, minimalne wymagania wynikające z najlepszej dostępnej techniki, jakie muszą spełniać instalacje, o których mowa w art. 201 ust. 2, w tym:
  1) graniczne wielkości emisyjne,
  2) w uzasadnionych przypadkach wzajemne, wariantowe relacje pomiędzy granicznymi wielkościami emisyjnymi dotyczącymi wprowadzania gazów lub pyłów do powietrza, odprowadzania ścieków, wytwarzania odpadów i emitowania hałasu oraz pól elektromagnetycznych,
  3) progi tolerancji dla uzasadnionych odstępstw od ustalonych granicznych wielkości emisyjnych oraz czas ich stosowania,
  4) wymagania dotyczące energochłonności i materiałochłonności,
  5) inne niezbędne wymagania techniczne.

Najlepsza Dostępna Technika - BAT

- **Korzystając z wytycznych należy w każdym przypadku uwzględniać specyfikę zakładu, którego dotyczy decyzja, jego położenie i stan otaczającego go środowiska.**
- **Jeśli stosując BAT nie można dotrzymać norm stanu środowiska, pozwolenie powinno nałożyć dodatkowe obowiązki pozwalające osiągnąć wymagany stan środowiska.**
- **Pozwolenia IPPC muszą zawierać limity emisji zanieczyszczeń, które będą prawdopodobnie emitowane w znaczących ilościach ze szczególnym uwzględnieniem wymienionych w załączniku III (do dyrektywy IPPC).**

Najlepsza Dostępna Technika - BAT

- **Graniczne wielkości emisji mają być ustalane na podstawie BAT.**
- **Celem ustalenia BAT jest określenie limitów emisyjnych, które odzwierciedlają właściwe proporcje pomiędzy kosztami i zyskami.**
- **Graniczne wielkości emisji mogą być ustalane na szczeblu europejskim lub krajowym.**

Najlepsza Dostępna Technika - BAT

- **BAT powinna być wybierana w taki sposób, aby zapewnić emisję, która nie będzie powodowała przekroczenia standardów jakości środowiska (art. 143 POŚ).**
- **W przypadku, gdy możliwe jest osiągnięcie lepszych efektów środowiskowych poprzez zastosowanie BAT, która nie powodowałaby nadmiernych kosztów, należy ją zastosować.**

eko-net.pl

Najlepsza Dostępna Technika - BAT

Wymagania BAT w praktyce:

1 – dotrzymywanie wszystkich właściwych wymagań prawnych w zakresie ochrony środowiska, w tym zwłaszcza standardów emisyjnych;

2 – utrzymywanie standardów jakości środowiska na poziomie wymaganym przez prawo i lokalne programy;

3 – spełnianie wskaźnikowych parametrów BAT dotyczących wielkości emisji, energochłonności, materiałochłonności, gospodarki odpadami, procedur nadzoru, kontroli i monitoringu

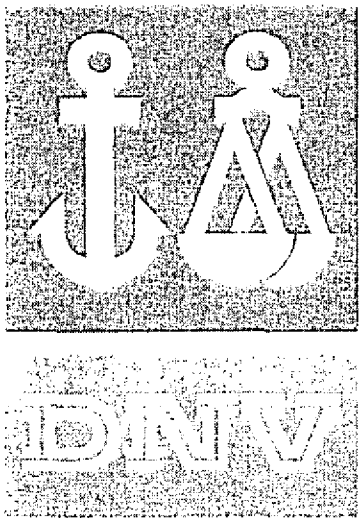
eko-net.pl

Pozwolenia zintegrowane

- Wymogi odnoszące się do poszczególnych instalacji określa się w sposób indywidualny, uwzględniając również – oprócz wymogów ogólnych – ich specyfikę, lokalne uwarunkowania środowiskowe, rachunek kosztów-korzyści, koszty ewentualnej modernizacji lub wdrożenia usprawnień technologii, porównanie z innymi zakładami z danej branży, odniesienie do dokumentów referencyjnych itp.)
- warunki korzystania *ze środowiska, ustalane w pozwoleniach* **nie mogą zalecać stosowania jednej konkretnej techniki lub technologii.**
- Za prawidłowe ustalenie wymogów BAT i ich odpowiednie przetransponowanie na wymogi *pozwolenia zintegrowanego* odpowiada organ wydający dane pozwolenie.

eko-net.pl

DET NORSKE VERITAS POLAND



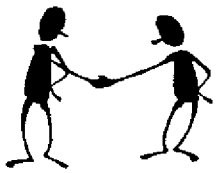
Auditor wewnętrzny systemu zarządzania bezpieczeństwem informacji wg normy BS7799-2:2002

DNV Poland 2004 r.

Kurs Audytora Wewnętrznego Systemu Zarządzania Bezpieczeństwem Informacji wg BS7799-2:2002

17799 - zgodność z wytycznymi
więc nie ma certyfikacji

Witamy na kursie Audytora Wewnętrznego



CEL KURSU

Przygotowanie uczestników do pełnienia roli audytorów wewnętrznych systemów zarządzania bezpieczeństwem informacji wg normy BS7799-2:2002

ZAKRES KURSU

- Podstawowe zagadnienia związane z normami serii 7799
- Co to jest audyt?
- Cele stosowania zabezpieczeń i zabezpieczenia
- Przygotowanie do audytu
- Szacowanie ryzyk
- Przeprowadzanie audytu
- Działania poaudytowe
- Proces certyfikacji
- Egzamin

PRZEDSTAWIAMY SIĘ

Imię i nazwisko
Stanowisko
Zakres odpowiedzialności (ogólnie)
Doświadczenie związane z ISMS
Oczekiwania dotyczące szkolenia

Bezpieczeństwo informacji - pojęcia

Informacja to jedno z najbardziej wartościowych aktywów organizacji.
Brak zapewnienia odpowiedniej ochrony może doprowadzić do jej:

- wyjawienia, przecieku lub ujawnienia w nieautoryzowany sposób,
- modyfikacji bez wiedzy użytkowników, czyniących ją mniej wartościową,
- utraty bez śladu lub nadziei na odzyskanie,
- niedostępności wtedy, gdy jest najbardziej potrzebna.

Bezpieczeństwo informacji - pojęcia

Bezpieczeństwo informacji – zabezpieczenie poufności, integralności i dostępności informacji

Poufność – zapewnienie, że informacja jest dostępna jedynie osobom upoważnionym

Integralność – zapewnienie dokładności i kompletności informacji oraz metod przetwarzania

Dostępność – zapewnienie, że osoby upoważnione mają dostęp do informacji i związanych z nią aktywów wtedy, gdy jest to potrzebne

MANAGING RISK

ICIA
Confidentiality – Poufność
Integrity – modyfikacje
na skutek błędu w procesie
Availability – co z tego, że
gdzieś jest, nie ma
dostępu

Bezpieczeństwo informacji - pojęcia

System Zarządzania Bezpieczeństwem Informacji (ISMS) część ogólnego systemu zarządzania organizacji, oparta o podejście uwzględniające analizę ryzyka biznesowego, w celu ustanowienia, wdrożenia, stosowania, monitorowania, przeglądania, utrzymywania i doskonalenia bezpieczeństwa informacji.

ISMS powinien być skuteczny jeśli ma być przydatny dla organizacji:

- powinien być integralną częścią ogólnego systemu zarządzania organizacji,
- powinien być postrzegany nie jako jednorazowa akcja (certyfikacja) lecz jako ciągły proces doskonalenia skuteczności,
- obszerność dokumentacji zależy od wielkości organizacji,
- złożoność procesów realizowanych w organizacji powinna mieć wpływ na planowanie ISMS.

MANAGING RISK

odpowiedzialność

Bezpieczeństwo informacji zależne Bezpieczeństwo
Podstawowe jest analiza ryzyka
organizacja – to firma musi wdrożyć,
kiedy wdrożyć i utrzymać system ISMS
nie odpowiedzieć na to dlaczego chcieć
się zmartwić
Norma 18000, mówi, że ma się
zastosować do wielkiej organizacji

Bezpieczeństwo informacji - pojęcia

System Zarządzania Bezpieczeństwem Informacji to:

- organizacja,
- struktura,
- polityki,
- planowanie działalności,
- odpowiedzialności,
- praktyki,
- procedury,
- zasoby.

MANAGING RISK

najpierw uporządkować, dlaczego tego
jest to co odpowiedzialny

Bezpieczeństwo informacji - pojęcia

System Zarządzania Bezpieczeństwem Informacji może obejmować:

- wszystkie systemy informacyjne organizacji,
- niektóre systemy informacyjne organizacji,
- określony system informacyjny organizacji.

może w tym wypadku nie być swobodnego przepływu informacji

17799 nie może się odbywać na podstawie tej normy

Historia norm serii 7799

1995 BS 7799-1 zainicjowana przez brytyjskie Ministerstwo Handlu i Przemysłu
1998 BS 7799-2
1999 nowa edycja BS 7799-1 i BS 7799-2
1999 SS 627799 części 1 i 2
1999 rozpoczyna się projekt ISMS w Hövik
2000 ISO 17799 (= BS 7799-1)
2002 BS 7799-2
2003 PN-ISO 17799 ~~Zasady dobrej praktyki~~
2004 ~~PN-I-7799:2004-???~~

wytyczne dla zbudowania ISMS
możliwość poddania się certyfikacji jak spełnie te wymagania to może być
~~certyfikat się nadaje dla tych części~~
mimo wytycznych /text niedostatek i w najlepszym razie ~~się~~ dobrze)

PN-I-07799:2004 - zostanie ustanowiona przez komitet i oparta na podpis przewodniczącego komitetu (termin wejścia w życie = termin

Nawarzie nie na PN-I-07799:2004 nie ma możliwości PCA może być podany nadanie przez PCA (może być w ogóle nie akredytowane).

Normy powołane

ISO 17799 odnosi się

ISO 9001:2000	**Systemy zarządzania jakością** Wymagania
ISO 17799:2000	**Technologia informacyjna** Praktyczne zasady zarządzania bezpieczeństwem informacji
ISO Guide 73:2002	**Zarządzanie ryzykiem** Słownictwo – Wskazówki stosowania

= ISO 17799:2000 - [illegible] pewne

ISO 19011 - zastąpiła ISO 10011 - czyli wytyczne dla audytów

tym wytyczne dotyczące zarządzania [illegible]

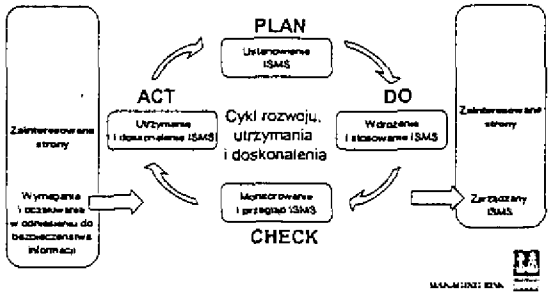
Akty prawne i normatywne

- **BS 7799-2:2002**
  Wymagania i specyfikacja ISMS
- **ISO 17799:2000 / PN-ISO/IEC 17799:2003**
  Praktyczne zasady zarządzania bezpieczeństwem informacji
- **ISO 13335 (część 1 - 5) GMITS**
  Wytyczne do zarządzania bezpieczeństwem systemów informatycznych
- **Ustawa z 22.01.1999**
  o ochronie informacji niejawnych
- **Ustawa z 29.08.1997**
  o ochronie danych osobowych

Układ normy BS7799-2:2002

0	Wprowadzenie	
1	Zakres	
2	Normy powołane	
3	Terminy i definicje	
4	System zarządzania bezpieczeństwem informacji	
5	Odpowiedzialność Kierownictwa	
6	Przegląd zarządzania ISMS	
7	Doskonalenie ISMS	
Załącznik A (normatywny)		Cele zabezpieczania i zabezpieczenia
Załącznik B (informacyjny)		Przewodnik stosowania normy
Załącznik C (informacyjny)		Powiązania między ISO 9001:2000, ISO 14001:1996 oraz BS 7799-2:2002
Załącznik D (informacyjny)		Zmiany w numeracji punktów normy

Model PDCA zaimplementowany do ISMS



Model PDCA zaimplementowany do ISMS

PLAN – ustanowienie ISMS
ustanowienie polityk bezpieczeństwa, zadań, celów, procesów i procedur odpowiednich dla zarządzania ryzykiem i doskonalenia bezpieczeństwa informacji w celu spełnienia postanowień polityki i celów organizacji

DO – wdrożenie i stosowanie ISMS
wdrożenie i zastosowanie polityk bezpieczeństwa, zabezpieczeń, procesów i procedur

CHECK – monitorowanie i przegląd ISMS
ocena i gdzie to możliwe monitorowanie wydajności procesów pod kątem spełnienia polityk bezpieczeństwa, celów i praktycznych doświadczeń: przedstawianie wyników Kierownictwu do przeglądu

ACT – utrzymywanie i doskonalenie ISMS
podejmowanie działań korygujących i zapobiegawczych na podstawie wyników przeglądów zarządzania w celu ciągłego doskonalenia ISMS

MANAGING RISK

Model PDCA – PLAN

- **Zdefiniowanie zakresu ISMS**
  - w zależności od charakteru działalności, organizacji, lokalizacji, aktywów i technologii
  - nie musi obejmować całej organizacji / wszystkich procesów,
  - wyłączenia wymagań punktów 4 – 7 są niedopuszczalne,
  - musi być precyzyjny i mówić prawdę,
  - powinien brać pod uwagę wszelkie okoliczności zewnętrzne, powiązania z innymi organizacjami, systemami czy dostawcami

MANAGING RISK

wdrożenie ≠ certyfikacja

nawet 9001 zakłada, że można wyłączyć, o ile w tej nie można wyłączać

audyt o jakiejś widzimy korporacji

Model PDCA – PLAN

- **Zdefiniowanie polityk ISMS**
  - w zależności od od charakteru działalności, organizacji, lokalizacji, aktywów i technologii
  - muszą uwzględniać wymagania prawne i kontraktowe,
  - powinny być zaakceptowane przez Kierownictwo,
  - powinny zawierać ramy do ustalania celów, wyznaczać kierunki działań, określać kontekst zarządzania ryzykiem i kryteria oceny ryzyka

MANAGING RISK

Model PDCA – PLAN

- **Określenie systematycznego podejścia do szacowania ryzyka**
  - identyfikacja najbardziej odpowiedniej metody dla ISMS organizacji,
  - powinna ona zawierać kryteria akceptowalności ryzyk i identyfikacji akceptowalnych poziomów ryzyk,
  - przyjęta metoda szacowania ryzyk powinna objąć swoim zasięgiem wszystkie obszary zabezpieczeń,
  - złożoność przyjętej metody szacowania ryzyk i ewentualne jej zautomatyzowanie zależy od złożoności ISMS organizacji.

Model PDCA – PLAN

- **Identyfikacja ryzyk**
  - określenie aktywów i ich gestorów
  - *identyfikacja zagrożeń i podatności dla każdego z aktywów,*
  - określenie skutków utraty poufności, integralności, dostępności informacji
- **Szacowanie ryzyk**
  - oszacowanie szkód organizacji w przypadku utraty poufności, integralności lub dostępności informacji
  - oszacowanie prawdopodobieństw zdarzenia się naruszenia bezpieczeństwa aktywów uwzględniając zagrożenia, podatności, konsekwencji i zastosowane zabezpieczenia
  - oszacowanie poziomu ryzyk oraz ustalenie kiedy ryzyka są akceptowalne lub wymagane są działania z nimi związane

Model PDCA – PLAN

- **Identyfikacja i ocena wariantów postępowania z ryzykiem**
  - zastosowanie odpowiednich zabezpieczeń,
  - unikanie ryzyk,
  - przeniesienie ryzyk (w całości lub w części) na inną organizację, np. ubezpieczyciel, dostawca
  - w sposób świadomy i obiektywny zaakceptowanie ryzyk.

Model PDCA – PLAN

- **Wybór celów zabezpieczania i zabezpieczeń jako metody postępowania z ryzykiem**
  - cele zabezpieczania i zabezpieczenia z listy zawartej w załączniku A do normy BS7799-2:2002,
  - może być konieczny wybór dodatkowych, nieujętych w załączniku A celów zabezpieczania i zabezpieczeń,
  - wybór uzasadniony w oparciu o wnioski wynikające z procesu szacowania ryzyka i postępowania z ryzykiem,
  - zastosowanie celów zabezpieczania i zabezpieczeń musi być ekonomicznie uzasadnione (koszt implementacji powinien być niższy niż strata powstała w wyniku incydentu)

Załącznik normatywny tzw. zał. A
musi zawierać 12 punktów
B, C, D – są informacyjne a A jest
normatywny. Jest możliwe wyłączenie
pewnych punktów ale tylko z A.
np. z kryptografii. Na bazie A
powstaje się deklarację zgodności.
Statement of Applicability ISO 17799 to
jest omówienie załącznika A do nas.

Model PDCA – PLAN

- **Przygotowanie Deklaracji Stosowania (SoA)**
  - obowiązkowy dokument ISMS,
  - powinien zawierać listę celów zabezpieczania i zabezpieczeń wybranych w wyniku procesu szacowania i postępowania z ryzykiem,
  - powody wyboru celów zabezpieczania i zabezpieczeń powinny być udokumentowane w deklaracji stosowania,
  - wszystkie cele zabezpieczania i zabezpieczenia wymienione w załączniku A mają zastosowanie w organizacji, chyba że na podstawie wyników szacowania ryzyka i kryteriów akceptacji zostanie pokazane, że specyficzne cele zabezpieczania i zabezpieczenia nie są celowe.

Lista tego co będziemy stosować, ~~że~~ uzasadnienie
~~których nie będziemy stosować~~

Nie mamy wpływu na to
stanowisko ale można to
uzasadnić.

Risk Treatment Plan

Model PDCA – DO

Wymagania zawarte w punkcie 4.2.2 mają na celu zapewnienie, że organizacja ustanowiła system procesów, którego celem jest wdrożenie i utrzymywanie ISMS zaplanowanego w fazie **PLAN**.

Jednym z elementów tego systemu jest plan postępowania z ryzykiem (RTP):

- w celu zarządzania zidentyfikowanymi i oszacowanymi ryzykami,
- zawierający zadania do realizacji, odpowiedzialności i ramy czasowe

Szczegóły to w jednym dokumencie
mamy odnośniki wiążące w innym
miejscu.

Efficiency Effective

Model PDCA – DO

Skuteczność jest słowem kluczowym przy rozpatrywaniu wdrożenia zabezpieczeń. Z założenia muszą one być skuteczne tak, aby spełnić cele zabezpieczania.

Należy rozważyć aspekt ekonomiczny wdrażania zabezpieczeń.

Należy wdrożyć programy uświadamiania i szkolenia.

- ilość i obszerność szkoleń zależy od świadomości personelu i jego kompetencji oraz złożoności procesów realizowanych w organizacji,
- zbyt obszerny plan szkoleń może doprowadzić do frustracji i obniżenia skuteczności działań mających na celu podniesienie świadomości.

Te warte uwagi o ważnym zjawisku nie dotyczą o implementacji o skuteczności BS 15... niż o dbałości o ... dobrej współpracy

Model PDCA – DO

Nie wolno zapominać o celu istnienia organizacji – ISMS nie może uniemożliwiać wykonywania obowiązków.

ISMS powinien umożliwiać realizowanie zadań w sposób skuteczny i efektywny.

Personel powinien szybciej zauważyć dobrze zaimplementowane praktyki ochrony informacji niż niedogodności wynikające z zastosowania zabezpieczeń.

Model PDCA – CHECK

Wymagania punktu 4.2.3 normy mają na celu zapewnienie, że organizacja ustanowiła system procesów, którego celem jest monitorowanie i przegląd ISMS wdrożonego w fazie DO.

Aby ISMS był skuteczny musi być poddawany przeglądowi i monitorowaniu wszelkich zmian mogących wpływać na ryzyka oddziałujące na organizację.

Zagrożenia, podatności, ryzyka, poziomy akceptowalności ryzyk, zabezpieczenia i cele zabezpieczania powinny być regularnie przeglądane w celu utrzymania ich ciągłej aktualności.

Model PDCA – CHECK

Zmiany zagrożeń, podatności i wpływów ze względu na:

- zmiany struktury organizacji,
- zmiany otoczenia organizacji (nowi kooperanci, dostawcy, klienci, ekspansja na inne rynki, kondycja rynku, nowa konkurencja),
- zmiany polityk i celów organizacji,
- zmiany technologii, infrastruktury, personelu, metod pracy, outsourcing,
- zmiany prawa i wymagań normatywnych.

Model PDCA – CHECK

Regularne przeglądy skuteczności ISMS:

- zgodność zakresu ISMS,
- zgodność z politykami i celami,
- przegląd i ocena skuteczności zabezpieczeń,
- zgodność i prawidłowe wykorzystywanie procedur,
- *zgodność obowiązków i uprawnień w ramach ISMS,*
- rezultaty audytów bezpieczeństwa,
- dokumentowanie i postępowanie z incydentami,
- sugestie oraz informacje zwrotne od zainteresowanych stron,
- aktualność procedur ciągłości działania.

Model PDCA – ACT

Wymagania punktu 4.2.4 normy mają na celu zapewnienie, że organizacja ustanowiła system procesów, którego celem jest utrzymywanie i doskonalenie ISMS zaimplementowanego w fazie **CHECK**.

- Identyfikacja obszarów wymagających doskonalenia
- Identyfikacja planów zmian aby zapobiec dezaktualizacji ISMS
- Identyfikacja zmian wymagających natychmiastowej reakcji

Model PDCA – ACT

Źródła potrzeb doskonalenia:

- polityki bezpieczeństwa informacji,
- cele zabezpieczania,
- wyniki audytów,
- wyniki przeglądów ISMS,
- analiza i monitorowanie procesów,
- informacje o incydentach
- działania korygujące,
- działania zapobiegawcze

cykl wytyczne dotyczące zakresu dokumentacji ISMS

Wymagania dotyczące dokumentacji

- Udokumentowane deklaracje polityk bezpieczeństwa oraz celów zabezpieczania,
- Zakres ISMS oraz procedury i zabezpieczenia służące realizacji ISMS,
- Raport z procesu szacowania ryzyka,
- Plan postępowania z ryzykiem,
- Udokumentowane procedury potrzebne organizacji do zapewnienia skutecznego planowania, utrzymywania i sterowania jej procesami bezpieczeństwa informacji,
- Zapisy wymagane przez normę,
- Deklaracja stosowania.

Wymagania dotyczące dokumentacji

Jeśli w niniejszej normie pojawia się termin „udokumentowana procedura", oznacza to, że procedura ta jest ustanowiona, udokumentowana, wdrożona i utrzymywana.

Zakres dokumentacji ISMS może być różny w organizacjach w zależności od wielkości organizacji i rodzaju działalności, zakresu i złożoności systemu i wymagań bezpieczeństwa informacji.

Dokumenty i zapisy mogą mieć dowolną formę lub dowolny rodzaj nośnika.

Wymagania dotyczące dokumentacji

Nadzór nad dokumentami

- zatwierdzanie przed wydaniem,
- przegląd i aktualizacja,
- identyfikacja zmian i statusu rewizji,
- dostępność aktualnych wersji w miejscach ich użytkowania,
- czytelność,
- dokumenty zewnętrzne,
- kontrolowany obieg dokumentów,
- ochrony przed niezamierzonym użyciem dokumentów nieaktualnych,
- odpowiednia identyfikacja, jeśli są przechowywane z jakiegokolwiek powodu.

Wymagania dotyczące dokumentacji

Nadzór nad zapisami

- dowód zgodności z wymaganiami i skuteczności ISMS,
- zgodny z *wymaganiami prawnymi*,
- czytelne, łatwe do zidentyfikowania i odszukania,
- identyfikowanie, przechowywanie, zabezpieczanie, wyszukiwanie, zachowywanie przez określony czas, niszczenie,
- ISMS powinien określać potrzebę i zakres zapisów.

Wymagania dotyczące dokumentacji

Dokument

informacja i jej nośnik

Zapis

dokument, w którym przedstawiono uzyskane wyniki lub dowody przeprowadzonych działań

Odpowiedzialność Kierownictwa

Dowód zaangażowania w ustanowienie, wdrożenie, monitorowanie, przegląd, utrzymywanie i doskonalenie skuteczności ISMS

- określenie polityk i celów ISMS,
- określenie ról i odpowiedzialności,
- informowanie o znaczeniu spełniania celów i zgodności z politykami bezpieczeństwa informacji,
- zapewnienie wystarczających zasobów,
- ustanawianie akceptowalnych poziomów ryzyk,
- przeprowadzanie przeglądów ISMS.

Odpowiedzialność Kierownictwa

Określenie i zapewnienie zasobów w celu:

- ustanowienia, wdrożenia, eksploatacji i utrzymania ISMS,
- zapewnienia, że procedury ISMS wspierają wymagania biznesowe,
- zidentyfikowania i odniesienia się do wymagań prawnych, normatywnych lub kontraktowych,
- utrzymania odpowiedniego bezpieczeństwa przez poprawne zastosowanie zabezpieczeń,
- przeprowadzania przeglądów oraz reagowania na ich wyniki,
- poprawy skuteczności ISMS.

Odpowiedzialność Kierownictwa

Kompetencje, świadomość, szkolenie

- określenie niezbędnych kompetencji
- spełnienie potrzeb (szkolenie lub inne działania),
- ocena skuteczności działań,
- utrzymywanie zapisów

Kompetencje wynikające z:

- wykształcenia
- wyszkolenia
- umiejętności
- doświadczenia

szkolenia, czy podnoszenie kompetencji

Przegląd zarządzania

- zaplanowane odstępy czasu,
- przydatność, adekwatność, skuteczność,
- okazja do doskonalenia systemu,
- potrzeba zmian systemu, polityk i celów,
- zapisy.

Przegląd zarządzania

Dane wejściowe

- wyniki audytów i przeglądów ISMS,
- informacja zwrotna od zainteresowanych stron,
- techniki, produkty i procedury, które mogą być zastosowane w celu poprawy funkcjonowania i skuteczności ISMS,
- status działań korygujących i zapobiegawczych,
- podatności lub zagrożenia, źle lub niezaadresowane w poprzednio realizowanym procesie szacowania ryzyka,
- działania podjęte w następstwie wcześniejszych przeglądów zarządzania,
- zmiany wpływające na ISMS,
- zalecenia dotyczące doskonalenia.

Przegląd zarządzania

Dane wyjściowe

Decyzje i działania związane z:

- doskonaleniem skuteczności ISMS,
- modyfikacją procedur ISMS, w celu reakcji na wewnętrzne lub zewnętrzne zdarzenia, w tym zmiany:
  - wymagań biznesowych,
  - wymagań bezpieczeństwa,
  - procesów biznesowych mających wpływ na istniejące wymagania biznesowe,
  - uwarunkowań prawnych lub uregulowań wewnętrznych,
  - poziomów ryzyka i/lub poziomów akceptacji ryzyka,
- potrzebnymi zasobami.

Audyt wewnętrzny

Zaplanowane odstępy czasu
W celu określenia, czy cele zabezpieczania, zabezpieczenia, procesy i procedury ISMS są:

- zgodne z wymaganiami niniejszej normy, odpowiednimi przepisami prawa oraz innymi regulacjami,
- zgodne z określonymi wymaganiami bezpieczeństwa informacji,
- skutecznie wdrożone i utrzymywane,
- realizowane w oczekiwany sposób.

Audyt wewnętrzny

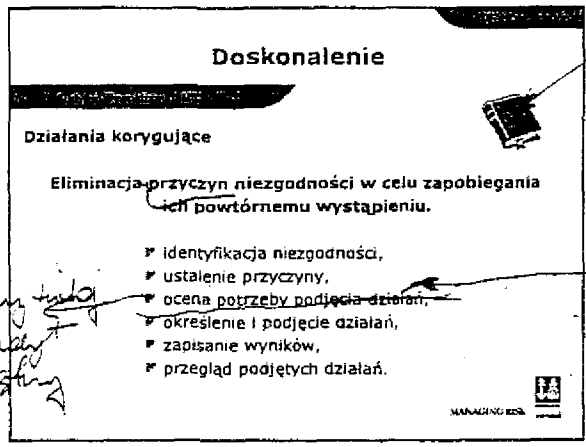
- zaplanowany (status i znaczenie procesów / obszarów,z uwzględnieniem wyników poprzednich audytów),
- zdefiniowane kryteria audytu, zakres, częstotliwość i metody,
- bezstronność i obiektywność audytora,
- działania korygujące (bez nieuzasadnionej zwłoki),
- weryfikacja działań poaudytowych.

E procesy ogólnie mogą zostać powinny być audytowane czas

Doskonalenie

Organizacja powinna w sposób ciągły poprawiać skuteczność ISMS poprzez:

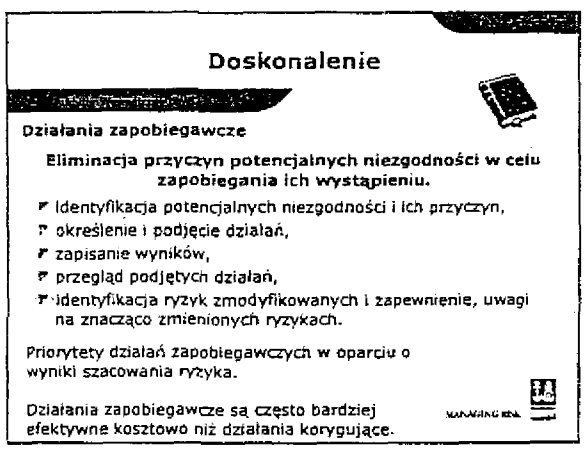
- stosowanie polityk bezpieczeństwa informacji,
- cele,
- wyniki audytów,
- analizy monitorowanych zdarzeń,
- działania korygujące i zapobiegawcze,
- przeglądy realizowane przez kierownictwo.



nowe wymaga poprawy

Dbałenie wyeliminowania to kwestia

po tym jak znajdziemy jakie działania podjąć



Często w firmach działania zapobiegawcze się podejmuje ale nie dokumentuje (jak coś robię to podnosimy)

Powinny być prowadzone zapisy bo jak ktoś wyjdzie z firmy to wyniesie ze sobą wiedzę.

CO TO JEST AUDYT?

Audyt

Systematyczny, niezależny i udokumentowany proces uzyskiwania dowodu z audytu oraz jego obiektywnej oceny w celu określenia stopnia spełnienia kryteriów audytu.

Audyt

CEL AUDYTU

Ocena stopnia zgodności systemu zarządzania bezpieczeństwem informacji z ustalonymi wymaganiami

Stopień zgodności z wymaganiami

Spełnienie wymagań BS7799-2

Dwa typy wymagań w BS7799-2:2002

- wymagania zawarte w *procesie ISMS (rozdziały 4-7)* normy BS7799-2:2002 – wyłączenia niedopuszczalne,
- cele zabezpieczania i zabezpieczenia wymienione w załączniku A – uzasadnienie wyłączeń w SoA

Audytor

ISO 19011

osoba mająca kompetencje do przeprowadzania audytu

audyty powinien przeprowadzać personel, który nie jest bezpośrednio odpowiedzialny za obszary podlegające audytowi

audytorzy powinni być bezstronni i nie powinni ulegać czynnikom mogącym mieć wpływ na ich obiektywność

(wewnętrzny musi zachować obiektywność)

Audytorzy muszą mieć podpisane tutaj

1 Deklaracje poufności
2 Deklaracje bezstronności

ISO 19011

Kompetencje

wykazane cechy osobowości i wykazana zdolność zastosowania wiedzy i umiejętności

Źródła kompetencji:

- wykształcenie,
- wyszkolenie,
- umiejętności,
- doświadczenie.

przy audytach jakości

Audyt

Zakres audytu
zasięg i granice audytu

Kryteria audytu
zestaw polityk, procedur lub wymagań, stosowanych jako odniesienie

Dowód z audytu
zapis, stwierdzenie faktu lub inna informacja, która jest związana z kryteriami audytu i może być zweryfikowana

Dowód obiektywny
dane potwierdzające istnienie lub prawdziwość czegoś

nie cała organizacja musi być poddana audytom

BS 7799 → może być a nie zawsze 17799, 2 wytyczne

Audytor jak nie jest pewny nie może przez 20 min się wydrapać to sprawdzi albo nie ma nie podejmuje kwestii

Audyt

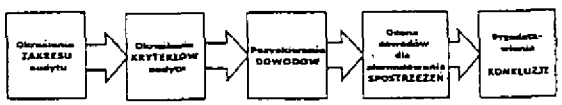
Spostrzeżenie audytowe
wynik oceny zebranych dowodów audytowych w odniesieniu do kryteriów audytu

Konkluzja z audytu
wynik audytu, przedstawiony przez zespół audytowy po rozważeniu celów audytu i wszystkich spostrzeżeń audytowych

nie musi mieć charakteru pochwalnego. Nie mylić spostrzeżenie z czymś negatywnym

Audyt

Kolejne kroki audytu



BS 7799 7
ISO 17799 } nie wiązanie ciała

Zewnętrzna audyty certyfikujący
o wdrożeniu

Jak jest źle można poinformować ze audyt zrobiony

IAF wydaje ISO Guide.
max 20 osób dni.

Audyt

Program audytu
jeden lub więcej audytów, zaplanowanych w określonym przedziale czasowym, dla zrealizowania określonego celu

Określone cele, np.
- spełnienie wymagań dla certyfikacji ISMS,
- sprawdzenie zgodności z wymaganiami kontraktu,
- pozyskanie i utrzymanie zaufania co do zdolności dostawcy,
- wkład w doskonalenie systemu zarządzania,
- ocena skuteczności systemu zarządzania

Plan audytu
opis czynności i uzgodnień dla audytu

Określenie programu to być jeden z planów wszystkich a w nim zamierzamy te strony dostawcę audytujemy (cel audytu) nie może podawać. Może tylko powiedzieć czy jest zgodny czy nie

Typy audytów

Audyty wewnętrzne

nazywane czasami audytami **strony pierwszej**, są przeprowadzane w celach wewnętrznych przez samą organizację lub w jej imieniu

Typy audytów

Audyty zewnętrzne

- audyty **strony drugiej** są przeprowadzane przez strony zainteresowane organizacją, takie jak klienci, lub przez inne osoby występujące w ich imieniu
- audyty **strony trzeciej** są przeprowadzane przez niezależne organizacje zewnętrzne. Organizacje takie prowadzą certyfikację na zgodność z wymaganiami

np. u naszego dostawcy chcemy audytować procesy kadrowe

Typy audytów

- planowy
- pozaplanowy
- systemu zarządzania
- procesu
- wyrobu

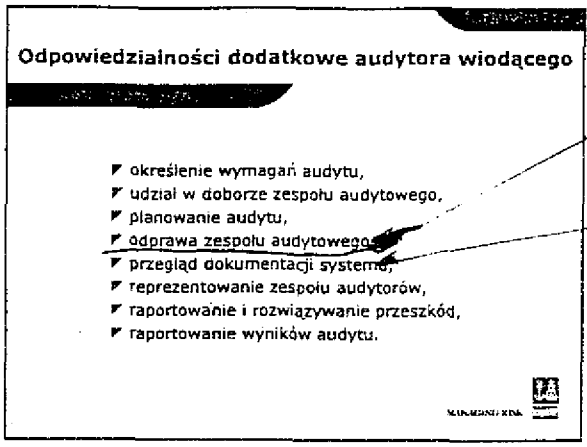
Powody przeprowadzania audytów wewnętrznych

- wymaganie normy BS7799-2:2002
- narzędzie pozwalające ocenić zgodność i skuteczność zarządzania bezpieczeństwem informacji
- narzędzie pozwalające poprawiać ISMS
- narzędzie pozwalające usprawniać ISMS

Odpowiedzialności członków zespołu audytowego

- przestrzeganie wymagań audytu,
- wyjaśnianie wymagań audytowanym,
- skuteczne i efektywne planowanie i realizacja zadań,
- przygotowywanie dokumentów roboczych,
- dokumentowanie spostrzeżeń,
- raportowanie wyników,
- ocena działań korygujących,
- zabezpieczanie dokumentów,
- wspieranie audytora wiodącego,
- przestrzeganie kodeksu postępowania.

IRCA



przewodniczący
do ... i za co mu
zwrócić uwagę
audytor wiodący przygotowuje
dokumentację ... i za co
będzie jego później ...
(wolności z błędami)

Jak nie ma dostępu możemy przerwać audyt.

CELE STOSOWANIA ZABEZPIECZEŃ I ZABEZPIECZENIA

To co w załączniku A i ISO 17799

Struktura celów

- A.1 Wprowadzenie
- A.2 Poradnik praktycznych zasad
- A.3 Polityka bezpieczeństwa
- A.4 Organizacja bezpieczeństwa
- A.5 Klasyfikacja i kontrola aktywów
- A.6 Bezpieczeństwo osobowe
- A.7 Bezpieczeństwo fizyczne i środowiskowe
- A.8 Zarządzanie systemami i sieciami
- A.9 Kontrola dostępu do systemu
- A.10 Rozwój i utrzymanie systemu
- A.11 Zarządzanie ciągłością działania
- A.12 Zgodność

A.3 Polityka bezpieczeństwa

A.3.1 Polityka bezpieczeństwa informacji

- Dokument polityki bezpieczeństwa informacji (A.3.1.1)

Prosty i precyzyjny.

Rozpowszechniony w organizacji.

Może to być zestaw polityk - w zależności od funkcji i szczebli w organizacji

Jak zdefiniowano bezpieczeństwo informacji?

Dlaczego jest ważne dla organizacji?

Jaka jest dostępność? Jakie zrozumienie?

- Przegląd i ocena (A.3.1.2)

Regularne przeglądy.

Przegląd i ocena w warunkach zachodzących zmian

Kiedy jest przeprowadzana? Czy plan przeglądów jest adekwatny do zmieniającego się ryzyka?

Jak organizacja reaguje na zmiany - incydenty, nowe podatności i zagrożenia, zmiany technologii, etc.?

PD 3001 - 3005

BSI wydaje dokumenty PD które mówią jak audytować czyli dla nas ważne zadania

A.4 Organizacja bezpieczeństwa

A.4.1 Infrastruktura bezpieczeństwa informacji

- Forum kierowania polityką bezpieczeństwa (A.4.1.1)
- Koordynowanie bezpieczeństwa informacji (A.4.1.2)

Kluczowe osoby z kierownictwa organizacji,

Zaangażowanie kierownictwa, zapewnienie odpowiednich zasobów,

Koordynacja wdrożenia różnych rodzajów zabezpieczeń,

Upowszechnianie wśród personelu świadomości bezpieczeństwa informacji,

Wszelkie decyzje i działania forum winny być udokumentowane

Kto wchodzi w skład forum?

Jakie uprawnienia mają poszczególni członkowie forum (wytyczne: ISO/IEC 17799:2000)?

Jak często, w jakich sytuacjach zwołuje się spotkania? Jak dokumentuje się ich przebieg?

W jaki sposób podejmowane decyzje przekładają się na działania w procesach?

A.4 Organizacja bezpieczeństwa

A.4.1 Infrastruktura bezpieczeństwa informacji

- Podział odpowiedzialności w zakresie bezpieczeństwa informacji (A.4.1.3)

Odpowiedzialność za ochronę poszczególnych aktywów jasno zdefiniowana i udokumentowana,

Może dotyczyć każdego pracownika,

Wskazane umieszczenie tych odpowiedzialności np. w opisie stanowiska pracy

Czy ustanowiono osobę odpowiedzialną za całokształt bezpieczeństwa informacji (np. officer bezpieczeństwa)?

W jaki sposób określono właścicieli poszczególnych aktywów?

Czy zdefiniowano odpowiedzialności pracowników za bezpieczeństwo informacji na wszystkich szczeblach?

W jaki sposób zapoznano pracownika z jego odpowiedzialnością w tym zakresie? Jakie są na to dowody?

A.4 Organizacja bezpieczeństwa

A.4.1 Infrastruktura bezpieczeństwa informacji

- Proces autoryzacji urządzeń służących do przetwarzania informacji (A.4.1.4)

Staranny wybór – niewłaściwe wyposażenie lub niemożność spełnienia wymagań przez dostawcę może osłabić bezpieczeństwo informacji,

Konieczne aprobaty: techniczna, jednostki organizacyjnej, osoby odpowiedzialnej za bezpieczeństwo,

Aprobaty i dopuszczenia winny być udokumentowane

W jaki sposób dokonywano wyboru urządzeń i ich dostawców?

Jak autoryzuje się urządzenia podczas modernizacji, rekonfiguracji, rozszerzeń i innych podobnych działań?

W jaki sposób zarządza się konfiguracją? Czy przeprowadzono stosowne walidacje? Jak to zostało udokumentowane?

Czy pracownicy mogą we własnym zakresie wprowadzać jakieś urządzenia? Jak dokonuje się ich autoryzacji?

A.4 Organizacja bezpieczeństwa

A.4.1 Infrastruktura bezpieczeństwa informacji

- Specjalistyczne doradztwo w dziedzinie bezpieczeństwa informacji (A.4.1.5)

Wysoka złożoność zagadnień, daleko posunięta specjalizacja wymagają poszukiwania wewnętrznych lub zewnętrznych ekspertów,

Dobór specjalistów winien być elementem każdego planu projektu, należy także przewidzieć na to środki,

Wewnętrzni i zewnętrzni doradcy winni być świadomi zagadnień związanych z bezpieczeństwem informacji,

Doradztwo to nie tylko ekspert – to także literatura, organizacje, dostawcy sprzętu etc.

W jaki sposób organizacja określa czy i jakiego doradztwa poszukiwać? Kto decyduje o wyborze?

Czy właściwie rozpoznano potrzeby? Czy są obszary, w których nie korzysta się z doradztwa, a jest ono potrzebne?

Czy wybrani doradcy są odpowiedni (kompetencje, wystarczający, ...)?

Jak zorganizowano autoryzację dostępu doradców do aktywów? Czy odnotowano jakieś incydenty z ich udziałem? Jakie działania podjęto?

A.4 Organizacja bezpieczeństwa

A.4.1 Infrastruktura bezpieczeństwa informacji

- Współpraca pomiędzy instytucjami (A.4.1.6)

Współpraca z zewnętrznymi instytucjami stanowiącymi przepisy i uregulowania prawne, z dostawcami usług, z innymi organizacjami,

Współpraca oficerów bezpieczeństwa, udział w grupach problemowych, uczestnictwo w komitetach normalizacyjnych, konferencjach etc.,

Internet jako bogate źródło wiedzy,

Wymiana doświadczeń – tak, ale pod kontrolą, by nie naruszyć bezpieczeństwa informacji

Z jakimi instytucjami nawiązano współpracę? Jaką mają do odegrania rolę?

Czy przewidziano współpracę w postępowaniu w sytuacjach awaryjnych? We wsparciu infrastruktury?

Jakie wymagania prawne, branżowe etc.. mają zastosowanie we współpracy? W jaki sposób monitoruje się ich przestrzeganie?

Czy przedstawiciele organizacji udzielają się w jakichś forach wymiany doświadczeń? Jak określono zasady tego udziału, zasady jego nadzorowania?

A.4 Organizacja bezpieczeństwa

A.4.1 Infrastruktura bezpieczeństwa informacji

- Niezależne przeglądy bezpieczeństwa informacji (A.4.1.7)

Praktyka w zakresie bezpieczeństwa informacji winny być okresowo poddawane przeglądom, o ile to możliwe – przez niezależną instytucję,

„Niezależną instytucją" może być także ktoś z wewnątrz organizacji, o ile posiada wystarczającą niezależność od jej kierownictwa (np. audyt wewnętrzny).

Audyt trzeciej strony, prowadzony przez uprawnioną jednostkę certyfikacyjną może być formą takiego przeglądu

Jakie formy przeglądów bezpieczeństwa informacji mają zastosowanie? Jak można ocenić ich rzeczywistą niezależność?

Jak często dokonuje się takich przeglądów?

W jaki sposób ich wyniki wpływają na analizę ryzyka i podejmowane działania?

Jak oceniana jest w nich skuteczność systemu zarządzania bezpieczeństwem informacji?

A.4 Organizacja bezpieczeństwa

A.4.2 Bezpieczeństwo dostępu osób trzecich

- Identyfikacja ryzyka wynikającego z dostępu osób trzecich (A.4.2.1)

Identyfikacja rodzajów dostępu (fizyczny, logiczny),

Analiza ryzyka związanego z dostępem osób trzecich,

Dostęp osób trzecich do aktywów organizacji dopiero po zawarciu umowy

Jakie osoby trzecie mają dostęp do aktywów organizacji? Jaki rodzaj i zakres dostępu? Serwery? Internet, intranet, ...? Dostęp fizyczny?

Jak oceniał się ryzyka z tym związane? Jakie zabezpieczenia wprowadzono, by je zminimalizować?

Jakie są zasady ponownej analizy ryzyka? Incydenty? Ewentualne działania?

A.4 Organizacja bezpieczeństwa

A.4.2 Bezpieczeństwo dostępu osób trzecich

- Wymagania bezpieczeństwa w umowach z osobami trzecimi (A.4.2.2)

Wymagania bezpieczeństwa wobec personelu osób trzecich – przynajmniej takie same jak wobec własnego personelu,

Analiza ryzyka i stosowane zabezpieczenia powinny uwzględniać wpływ braku bezpośredniego zwierzchnictwa nad tym personelem, odmienność kultury innej organizacji etc.,

Dobra umowa – co maksymalnie szczegółowa umowa (wytyczne: ISO/IEC 17799:2000)

Jakie wymagania odnośnie bezpieczeństwa zidentyfikowano w kontaktach ze stronami trzecimi? Jakie odzwierciedlenia znajduje to w umowach?

Jak zdefiniowano uprawnienia w organizacji (ale także w organizacji strony trzeciej) do zawierania umów?

Czy odnotowano jakieś odstępstwa? Jakie było uzasadnienie? W jaki sposób się je dokumentuje?

Jakie są zasady ponownej analizy ryzyka? Incydenty? Ewentualne działania?

A.4 Organizacja bezpieczeństwa

A.4.3 Zlecanie przetwarzania na zewnątrz *(outsourcing)*

- Wymagania bezpieczeństwa w umowach zlecania na zewnątrz (A.4.3.1)

Należy zapewnić bezpieczeństwo informacji również wtedy, gdy odpowiedzialność za jej przetwarzanie przekazuje się innej organizacji,

Uzgodnienia z zewnętrznymi stronami dot. zabezpieczania i zabezpieczeń, stosowanych rozwiązań i procedur winny obejmować się na ocenie ryzyka

Konieczna umowa (wytyczne: ISO/IEC 17799:2000)

Jakie ryzyko jest związane z faktem, że organizacja traci na niektórych etapach nadzór nad bezpieczeństwem informacji?

Jak zdefiniowano wymagania, zabezpieczenia i odpowiedzialności odnośnie bezpieczeństwa w umowach?

Jakie zagadnienia brano pod uwagę podczas konstruowania umów? Czy przeprowadzono analizę ryzyka?

A.5 Klasyfikacja i kontrola aktywów

A.5.1 Rozliczalność aktywów

- Inwentaryzacja aktywów (A.5.1.1)

Wszystkie ważne aktywa powinny być zinwentaryzowane i posiadać właściciela,

Posiadanie spisu inwentarza aktywów wynika również ze standardów dot. prowadzenia księgowości

Inwentaryzacja aktywów winna zawierać:
– dla aktywów fizycznych: producent, *model*, typ, *numer seryjny*, datę zakupu, *numer inwentarzowy*, nazwisko właściciela (użytkownika), zapisy o pozbyciu się aktywów
– dla aktywów informacyjnych: np. lista aplikacji, baz danych, dokumentów, planów, nośnik, miejsce przechowywania etc.

Regularna aktualizacja – przynajmniej raz w roku

Czy prawidłowo zidentyfikowano i sklasyfikowano aktywa?

Czy inwentaryzacja jest dokładna, kompletna i aktualna? Czy zawiera poprawne informacje?

Komu przypisano odpowiedzialność za inwentaryzację?

W jaki sposób przechowuje się spis inwentarza? Kopie zapasowe spisu? Zasady dostępu do spisu? Czas przechowywania?

Czy są zapisy z audytu inwentaryzacji aktywów?

MANAGING RISK

Rejestr - lista kto dysponuje aktywami (zasobami)

A.5 Klasyfikacja i kontrola aktywów

A.5.2 Klasyfikacja informacji

- Wytyczne do klasyfikacji (A.5.2.1)

Zróżnicowana waga informacji wymaga zróżnicowania sposobów ochrony oraz oznaczania informacji dla zapewnienia właściwego poziomu ochrony.

Schemat klasyfikacji – udokumentowany, zasady dostępu do niego – określone, ze szczególnym uwzględnieniem osób, które emitują dokumenty i dane.

Dla każdej klasy informacji – precyzyjnie zdefiniowanie zasady dostępu przez personel, przechowywania, pozbywania się,

Zasady klasyfikacji mogą być różne w różnych organizacjach; mogą nie być porównywalne – konieczna szczególna uwaga przy przyjmowaniu i wysyłaniu informacji z zewnątrz

W jaki sposób organizacja klasyfikuje informacje? Jak stopniuje się poziom ochrony?

Czy klasyfikacja uwzględnia wszystkie aktywa wchodzące w zakres ISMS?

Jakie uzgodnienia z innymi organizacjami poczyniono dla właściwego rozpoznawania klasy informacji wchodzącej / wychodzącej?

W jaki sposób przeklasyfikowuje się informacje?

Czy schemat i zasady klasyfikacji są *zrozumiałe dla personelu?*

MANAGING RISK

Jak nie ma napisane tajne to można je wynieść!

A.5 Klasyfikacja i kontrola aktywów

A.5.2 Klasyfikacja informacji

- Oznaczanie i postępowanie z informacją (A.5.2.2)

Ważne aktywa informacyjne winny być w sposób widoczny oznaczone, by zapewnić właściwy poziom ochrony,

Dla informacji w postaci elektronicznej – określenie reguł dostępu na poziomie systemu,

Reguły przesyłania informacji w zależności od jej zaklasyfikowania (techniki szyfrowania?),

Postępowanie z informacją po jej udowodnieniu – unikanie zbędnych kosztów ochrony

W jaki sposób oznacza się informacje z uwzględnieniem rodzaju nośnika? Czy system oznaczania jest zgodny z przyjętym sposobem klasyfikacji?

Czy sposób oznaczania informacji jest spójny dla różnej postaci danych (papierowe, elektroniczne, ...)? Czy jest zrozumiały dla personelu?

Jakie są zasady postępowania przy przesyłaniu informacji?

Czy oznaczenia aktywów są zawsze widoczne? Czy są w sposób trwały *związane z aktywami?*

MANAGING RISK

A.6 Bezpieczeństwo osobowe

A.6.1 Bezpieczeństwo przy określaniu zakresów obowiązków i zarządzaniu zasobami ludzkimi

- Uwzględnianie aspektu bezpieczeństwa w zakresach obowiązków przypisanych do stanowisk (A.6.1.1)

Odpowiedzialność za bezpieczeństwo informacji winna być brana pod uwagę przy rekrutacji, zapisana w kontraktach, w opisach stanowisk pracy i monitorowana w toku zatrudnienia,

Kandydaci na odpowiedzialne stanowiska winni podlegać sprawdzeniu,

Wszyscy pracownicy, także trzeciej strony, mający odpowiedzialność za bezpieczeństwo informacji – klauzule poufności

Czy wszyscy pracownicy posiadają opisy stanowisk pracy uwzględniające zagadnienia bezpieczeństwa? Czy podpisali je? Czy opisy te są spójne z politykami bezpieczeństwa? Z obowiązującymi procedurami?

Czy nowo zatrudnieni w pełni rozumieją swoje odpowiedzialności w zakresie bezpieczeństwa? Czy zakończono postępowanie wprowadzające?

Jakie są zasady postępowania wobec czasowo zatrudnionych? Czy mają opisy stanowisk pracy?

A.6 Bezpieczeństwo osobowe

A.6.1 Bezpieczeństwo przy określaniu zakresów obowiązków i zarządzaniu zasobami ludzkimi

- Sprawdzanie podczas naboru (A.6.1.2)

Sprawdzenia tożsamości, przegląd CV, ale nie tylko – poprzednie miejsca pracy, przerwy w zatrudnieniu, sprawdzenie dowodów dot. kwalifikacji,

Wszystkie zmiany, wywiady – udokumentowane, zasoby przechowywane przez cały czas zatrudnienia (i po),

Rozmiary sprawdzenia mogą być limitowane przez obowiązujące prawo

Jakie sprawdzenia przewidują procedury rekrutacji (wytyczne: ISO/IEC 17799:2000)?

Czy oprócz przeglądu CV praktykuje się jakieś inne formy wywiadu?

Jakie środki ochrony stosuje się wobec zpromadzonych danych osobowych?

W jaki sposób przełożeni nowo zatrudnionych monitorują wypełnianie przez nich nałożonych odpowiedzialności?

Nie można zbierać
świadectw niekaralności co
prz wszystkich z pracy

A.6 Bezpieczeństwo osobowe

A.6.1 Bezpieczeństwo przy określaniu zakresów obowiązków i zarządzaniu zasobami ludzkimi

- Umowy o zachowaniu poufności (A.6.1.3)

Zawarcie pisemnej umowy o zachowaniu poufności nie gwarantuje jej zachowania, ale jest wartościowym argumentem przed sądem,

przy rekrutacji podpisze ją każdy – bo chce dostać pracę,

Umowy o poufności winny obejmować nie tylko stały personel, ale i pracowników stron trzecich, personel tymczasowy, pracowników agencyjnych etc.

Czy wszyscy pracownicy, których działania są objęte ISMS podpisali umowę o zachowaniu poufności?

Co zawiera taka umowa? Jak chroni organizację i jej aktywa?

Czy personel jest świadomy, co wynika z podjętego zobowiązania?

Kto w organizacji dba o to, by wszystkie umowy były aktualne? Kto dba o podpisywanie umów o poufności przez odchodzących z firmy?

A.6 Bezpieczeństwo osobowe

A.6.1 Bezpieczeństwo przy określaniu zakresów obowiązków i zarządzaniu zasobami ludzkimi

- Warunki zatrudnienia (A.6.1.4)

Pracownicy winni być świadomi swojej odpowiedzialności za bezpieczeństwo posiadanych informacji oraz za właściwe wykorzystanie urządzeń do ich przetwarzania, dlatego powinna być ona opisana w warunkach zatrudnienia.

Odpowiedzialność ta obowiązuje również podczas pracy w domu, pracy u klienta, na spotkaniu służbowym w publicznym miejscu, ale także „po godzinach" - w życiu prywatnym

Czy warunki zatrudnienia jasno precyzują odpowiedzialności pracowników za bezpieczeństwo informacji?

Czy odnoszą się do wymagań prawnych?

Czy określają zasady obowiązujące podczas pracy poza normalnymi godzinami? Podczas pracy z oddali?

Czy określają działania, jakie będą podjęte w razie niespełnienia wymagań bezpieczeństwa?

Czy warunki zatrudnienia są aktualizowane w razie np. zmiany stanowiska, zmiany miejsca, zmian w dostępie do urządzeń etc.?

A.6 Bezpieczeństwo osobowe

A.6.2 Szkolenie użytkowników

- Szkolenie i kształcenie w zakresie bezpieczeństwa informacji (A.6.2.1)

Działania niewyszkolonego personelu są zagrożeniem dla organizacji,

Wszyscy pracownicy organizacji (także osoby trzecie, jeśli mają dostęp) powinni być przeszkoleni w zakresie obowiązujących polityk i procedur, także w zakresie posługiwania się urządzeniami i oprogramowaniem,

Zapisy ze szkoleń

Jakie szkolenia przeprowadzono? Kto w nich uczestniczył?

Czy program szkolenia był dostosowany do stanowiska i związanych z nim zadań?

Kto prowadzi szkolenia? Czy posiada odpowiednie kwalifikacje? Czy dostawcy szkoleń zostali zatwierdzeni?

Czy szkolenia są okresowo ponawiane?

Czy utrzymuje się zapisy? Materiały ze szkoleń?

A.6 Bezpieczeństwo osobowe

A.6.3 Reagowanie na naruszenia bezpieczeństwa i niewłaściwe funkcjonowanie systemu

- Zgłaszanie przypadków naruszenia bezpieczeństwa (A.6.3.1)

Wszelkie przypadki naruszenia bezpieczeństwa (także zagrożenia, słabości lub niewłaściwe funkcjonowanie) winny być zgłaszane właściwym czynnikom tak szybko, jak to możliwe,

Każdy pracownik może być tym pierwszym, który zauważy taki przypadek - wczesne powiadomienie może zminimalizować straty,

Kultura organizacji: „nie szukać winnego"

Jak zdefiniowano przypadki naruszenia bezpieczeństwa? Czy personel potrafi prawidłowo je rozpoznawać?

Jakie procedury zgłaszania obowiązują? Jakie są kanały przepływu informacji o zdarzeniach?

Jakie są reakcje na zgłaszane przypadki? Czy zidentyfikowano przyczyny takich zdarzeń? Jakie zapisy są utrzymywane?

Czy zgłaszający są informowani o podejmowanych działaniach?

A.6 Bezpieczeństwo osobowe

A.6.3 Reagowanie na naruszenia bezpieczeństwa i niewłaściwe funkcjonowanie systemu

- Zgłaszanie słabości systemu bezpieczeństwa (A.6.3.2)

Żaden system nie jest w 100% bezpieczny.

Każda zauważona słabość systemu winna być zgłaszana przełożonemu lub innym odpowiedzialnym osobom.

Zauważonych słabości nie wolno wykorzystywać, nawet w dobrej intencji

Jakie procedury zgłaszania obowiązują? Jakie są kanały przepływu informacji o słabościach?

Jakie są reakcje na zgłaszane słabości? Czy poddaje się je badaniu? Jakie zapisy są utrzymywane?

Czy zgłaszający są informowani o podejmowanych działaniach?

A.6 Bezpieczeństwo osobowe

A.6.3 Reagowanie na naruszenia bezpieczeństwa i niewłaściwe funkcjonowanie systemu

- Zgłaszanie niewłaściwego funkcjonowania oprogramowania (A.6.3.3)

Szkodliwe lub niewłaściwe funkcjonujące oprogramowanie jest najczęstszym zagrożeniem dla bezpieczeństwa.

Należy ustanowić i wdrożyć sposób postępowania w przypadku wykrycia.

Najczęściej to końcowi użytkownicy jako pierwsi zauważają wadliwe funkcjonowanie systemu

Jakie procedury zgłaszania obowiązują? Co zawierają zgłoszenia? Jakie są kanały przepływu informacji o wadliwym działaniu?

Jakie są reakcje na zgłoszenia? Czy poddaje się je badaniu?

Jakie działanie korygujące są podejmowane (w tym działania wobec dostawców oprogramowania)? Jakie zapisy są utrzymywane?

Czy zgłaszający są informowani o podejmowanych działaniach?

A.6 Bezpieczeństwo osobowe

A.6.3 Reagowanie na naruszenia bezpieczeństwa i niewłaściwe funkcjonowanie systemu

- Nauka płynąca z incydentów (A.6.3.4)

W uzupełnieniu do wykrywania i rozwiązywania incydentów oraz nieprawidłowych działań należy zliczać i monitorować ich rodzaje, rozmiary i koszty.

Nauka płynąca z doświadczeń pozwala zwiększać skuteczność ISMS w zapobieganiu sytuacjom niepożądanym.

Doskonały materiał do szkolenia użytkowników

W jaki sposób organizacja zlicza i mierzy incydenty? Czy podejmowane działania są skuteczne?

Gdy nie ma zbyt wielu raportów o incydentach i niezrawidłowych działaniach, może to świadczyć o słabości procedur zgłaszania

Jakie doświadczenia z zaistniałych zdarzeń uwzględnia się w planach działań i w procedurach? W materiałach szkoleniowych?

Lot's make another mistakes

A.6 Bezpieczeństwo osobowe

A.6.3 Reagowanie na naruszenia bezpieczeństwa i niewłaściwe funkcjonowanie systemu

- Postępowanie dyscyplinarne (A.6.3.5)

Naruszenie polityk bezpieczeństwa lub procedur postępowania wymagą formalnego postępowania dyscyplinarnego.

Postępowanie jest uzależnione od kultury organizacji, praktyk w zarządzaniu i świadomości personelu.

Niewłaściwie wdrożone może spowodować osłabienie systemu, odpływ personelu, może także zwiększyć ilość spraw w sądzie pracy.

Postępowanie dyscyplinarne winno być udokumentowane

Czy pracownicy są świadomi istnienia takiego mechanizmu?

Jakie są kryteria postępowania dyscyplinarnego?

Jakie postępowania były prowadzone? Czy zapewniają uczciwe i stosowne do rodzaju przewinienia traktowanie?

W jaki sposób przeprowadzone postępowania przyczyniają się do zwiększania skuteczności ISMS?

MANAGEMENT RISK

A.7 Bezpieczeństwo fizyczne i środowiskowe

Secure areas

A.7.1 Obszary bezpieczne

- Fizyczne obwody zabezpieczające (A.7.1.1)

Konieczna jest ochrona przed niepowołanym dostępem (z zewnątrz ale i z wewnątrz) do obszarów, gdzie przetwarzane są informacje.

Wyznaczenie fizycznych granic tych obszarów ma umożliwić nadzór nad wkraczaniem do nich i opuszczaniem ich

Wskazane jest by możliwa była rejestracja.

Rodzaj bariery i dodatkowe zabezpieczenia - analiza ryzyka (wytyczne: ISO/IEC 17799:2000)

W jaki sposób organizacja fizycznie chroni swe obiekty przed niepowołanym dostępem?

Jak monitoruje się dostęp do obiektów, w których przetwarzane są informacje?

Własna ocena audytora: czy są jakieś potencjalne luki (np. niezabezpieczone okno, schody, wzajemne pożyczanie przepustek, możliwość oszukania nadzoru, etc.)?

MANAGEMENT RISK

A.7 Bezpieczeństwo fizyczne i środowiskowe

A.7.1 Obszary bezpieczne

- Fizyczne zabezpieczenie wejścia (A.7.1.2)

W oparciu o analizę ryzyka - wydzielenie wejść do obszaru (obszarów) i określenie rodzaju zabezpieczeń (wytyczne: ISO/IEC 17799:2000).

Obszary różnego ryzyka mogą wymagać różnych poziomów zabezpieczeń

Jakie zabezpieczenia są stosowane? Czy rzeczywiście umożliwiają wejście tylko upoważnionym? Rejestry wejść / wyjść?

Czy pracownicy noszą identyfikatory? A goście? Co dzieje się z tymi, którzy nie noszą?

- Zabezpieczenie biur, pomieszczeń i urządzeń (A.7.1.3)

Analiza ryzyka: które obszary mają być bezpieczne.

Rozśrodkowanie aktywów.

Uwzględnienie zagrożeń takich jak pożar, zalanie, celowe działanie człowieka, oddziaływanie sąsiedztwa, etc. (wytyczne: ISO/IEC 17799:2000)

Czy poziom ochrony jest dostosowany do najbardziej wrażliwych aktywów w danym obszarze?

Czy oprócz zasad dostępu organizacja wzięła także pod uwagę np. zalanie, ochronę ppoż., inne zabezpieczenia?

MANAGEMENT RISK

A.7 Bezpieczeństwo fizyczne i środowiskowe

A.7.1 Obszary ~~bezpieczne~~ chronione Secure areas

- Praca w obszarach bezpiecznych (A.7.1.4)

Identyfikacja ewentualnych dodatkowych wymagań i zabezpieczeń, wynikających z rodzaju i wrażliwości przetwarzanych informacji,

(wytyczne: ISO/IEC 17799:2000)

Jakiego rodzaju działania wykonuje się w danym obszarze? Do jakiego stopnia wiedza o nich jest publiczna?

Jak zabezpieczone są wejścia / wyjścia? Jakie dodatkowe zabezpieczenia? Na ile łatwo jest wprowadzić / wyprowadzić informacje?

Czy w obszarze dozwala się na robienie zdjęć, filmów, nagrywanie? Czy akceptuje się posiadanie sprzętu audio / video?

Czy przewidziano jakieś zdwojenia zabezpieczeń?

A.7 Bezpieczeństwo fizyczne i środowiskowe

A.7.1 Obszary bezpieczne

- Izolowane obszary dostaw i załadunku (A.7.1.5)

Oddzielenie obszarów dostaw i wysyłek od obszarów bezpiecznych,

Nadzór nad przepływem aktywów między obszarami bezpiecznymi a obszarami dostaw i załadunku,

Przyjmowanie tylko spodziewanych dostaw i wydawanie wysyłek tylko uprawnionym odbiorcom,

Dostawcy i odbiorcy (o ile to możliwe) nie przekraczają granic obszarów bezpiecznych,

Nazwiska, numery pojazdów rejestrowane

Jakiego rodzaju zagrożenia mogą wiązać się z doszczętnymi do (wysyłanymi z) organizacji produktami? Z organizacją dostaw i wysyłek?

W jaki sposób uwzględniono te zagrożenia w analizie ryzyka?

Do jakich obszarów organizacji mają dostęp dostawcy i odbiorcy? Jak ich pobyt i poruszanie się w siedzibie są nadzorowane?

Jak odbywa się dystrybucja dostaw (kompletowanie wysyłek) wewnątrz organizacji?

A.7 Bezpieczeństwo fizyczne i środowiskowe

A.7.2 Zabezpieczenie sprzętu

- Rozmieszczenie sprzętu i jego ochrona (A.7.2.1)

Sprzęt powinien być chroniony przed zagrożeniami ze strony środowiska oraz przed nieuprawnionym dostępem,

Specjalna uwaga należy się sprzętom przenośnemu, szczególnie jeśli umożliwia dostęp do sieci.

Ochrona sprzętu obejmuje również te urządzenia, które pracują poza siedzibą organizacji (one też powinny być objęte inwentaryzacją aktywów – patrz A.5.1.1)

Jak organizacja chroni swój sprzęt? Czy jego rozmieszczenie zapewnia należytą ochronę przed niekorzystnym wpływem otoczenia (zapylenie, wilgoć, rozlana kawa..., ale też włamanie, podglądanie monitorów etc.)?

Czy obszary przyległe do tych, w których rozmieszczono sprzęt nie stwarzają zagrożenia? Czy uwzględniono to w analizie ryzyka?

A.7 Bezpieczeństwo fizyczne i środowiskowe

A.7.2 Zabezpieczenie sprzętu

- Zasilanie (A.7.2.2)

Mimo wysokiej niezawodności współczesnych systemów zasilania, zawsze możemy paść ofiarą jego braku (El Nino albo koparka za rogiem), a przecież elektryczność to podstawa wszelkiej działalności,

Analiza ryzyka powinna wskazywać te urządzenia, które dla zachowania ciągłości muszą mieć zasilanie awaryjne,

W jaki sposób organizacja określiła swoje potrzeby i wymagania w tym zakresie?

Jak zorganizowano zasilanie (podtrzymanie) awaryjne urządzeń? Czy zastosowane zabezpieczenia uwzględniają krytyczność urządzeń dla systemu?

Własna ocena audytora: czy zastosowane zasilanie (podtrzymanie) jest wystarczające? Czy jest utrzymywane i okresowo sprawdzane (testy)?

Czy zapewniono oświetlenie awaryjne na wypadek przerwy w zasilaniu?

A.7 Bezpieczeństwo fizyczne i środowiskowe

A.7.2 Zabezpieczenie sprzętu

- Bezpieczeństwo okablowania (A.7.2.3)

Kable zasilające i telekomunikacyjne, ich połączenia powinny być pewnie i bezpiecznie poprowadzone – zarówno dla bezpieczeństwa informacji, jak i dla bezpieczeństwa w ogóle,

Gniazda sieciowe: zabezpieczenia fizyczne, zabezpieczenia przed niepowołanym dostępem – analiza ryzyka,

Jak poprowadzono i umocowano okablowanie, jak wykonano połączenia (jakość wykonania)? Wytyczne: ISO/IEC 17799:2000

Jakie zagrożenia wiążą się z przesyłaniem informacji? Jakie są słabe punkty sieci (przejście do innych budynków, wrzące kable napowietrzne, szerzyny i studzienki energetyczne i telekomunikacyjne dostępne publicznie etc.?

A.7 Bezpieczeństwo fizyczne i środowiskowe

A.7.2 Zabezpieczenie sprzętu

- Konserwacja sprzętu (A.7.2.4)

Współczesny – choć zwykle niezawodny – sprzęt zawsze może ulec awarii, dlatego powinien być regularnie konserwowany,

Instrukcje obsługi i utrzymania sprzętu, dostarczane przez producentów, powinny być „wkomponowane" w procedury operacyjne,

Służby utrzymania winny posiadać odpowiednie kwalifikacje i wyposażenie, a ich praca winna być nadzorowana,

Zapisy dot. konserwacji, zapisy o awariach powinny być utrzymywane i analizowane

W jaki sposób zorganizowano utrzymanie i konserwację sprzętu? Czy podejmowane działania są zgodne z zaleceniami producentów? Czy uwzględniają natężenie i warunki pracy?

Jakie czynności z tego zakresu włączono do codziennych praktyk i procedur?

Czy personel dokonujący przeglądów i konserwacji jest odpowiednio wykwalifikowany i wyposażony?

Jak funkcjonuje mechanizm raportowania awarii i uszkodzeń? Analiza tych raportów w celu korygowania procedur konserwacji sprzętu?

A.7 Bezpieczeństwo fizyczne i środowiskowe

A.7.2 Zabezpieczenie sprzętu

- *Zabezpieczenie sprzętu poza siedzibą (A.7.2.5)*

Praca sprzętu poza siedzibą wymaga zatwierdzenia.

Należy przeprowadzić analizę ryzyka związanego z pracą sprzętu poza siedzibą organizacji oraz zapewnić, że pozostanie na swoim miejscu, pozostanie sprawny i nie stworzy niekontrolowanego ryzyka.

Szczególna uwaga w analizie ryzyka powinna być poświęcona sprzętowi przenośnemu, który – zwłaszcza w miejscach publicznych – narażony jest na kradzież.

Patrz także A.9.8: Komputery przenośne i praca na odległość

Jak zinwentaryzowano sprzęt pracujący poza siedzibą?

Jakie zagrożenia wiążą ze sobą praca tego sprzętu? Jakie wprowadzono zabezpieczenia? Czy są one przynajmniej tak dobre jak te stosowane wewnątrz organizacji?

Czy może się zdarzyć, że jakiś sprzęt w jakichś okolicznościach pozostaje bez nadzoru?

Czy – tam gdzie może to mieć zastosowanie – wprowadzono ubezpieczenia?

A.7 Bezpieczeństwo fizyczne i środowiskowe

A.7.2 Zabezpieczenie sprzętu

- Bezpieczne zbywanie sprzętu lub przekazywanie go do ponownego użycia (A.7.2.6)

Przed pozbyciem się sprzętu (złomowanie, sprzedaż itp.) lub przed przekazaniem go do ponownego użycia należy starannie usunąć gromadzone informacje.

Zwykłe skasowanie pliku z dysku to nic dla kogoś posiadającego odpowiednie narzędzia.

Nośniki pamięci są dziś na tyle tanie, że może warto je po prostu zniszczyć i zastąpić nowymi?

Jakie metody usuwania informacji są stosowane przy pozbywaniu się sprzętu?

Czy wszyscy pracownicy są świadomi zagrożeń pojawiających się w związku z pozbywaniem się sprzętu?

Jak organizacja zabezpiecza się podczas *pozbywania sprzętu do naprawy?*

A.7 Bezpieczeństwo fizyczne i środowiskowe

A.7.3 Ogólne zabezpieczenia

- Polityka czystego biurka i czystego ekranu (A.7.3.1)

Stosy papierów zalegające na biurku to wystawa ważnych informacji. Zwiedzają ją goście, dostawcy, klienci, osoby sprzątające biuro ...

Zwykły przeciąg lub ludzki błąd może doprowadzić do nieodwracalnych skutków.

Wygaszacz ekranu z hasłem to wygodne zabezpieczenie, kiedy trzeba odejść od komputera, a nie możemy go wyłączyć

Jakie zasady zabezpieczania wprowadzono do codziennej praktyki? Na ile pracownicy stosują się do nich?

Jakie są możliwości dostępu niepowołanych osób do tego co leży na biurku albo w szufladzie? Do sprzętu?

Jakie zabezpieczenia obowiązują po „normalnych" godzinach pracy, w nocy, w weekendy? Kto w tym czasie może pojawiać się i przebywać w organizacji?

A.7 Bezpieczeństwo fizyczne i środowiskowe

A.7.3 Ogólne zabezpieczenia

- Wynoszenie mienia (A.7.3.2)

Sprzęt, informacje lub oprogramowanie należące do organizacji nie powinny być wynoszone bez zezwolenia – być może właśnie ulegają kradzieży.

Tam, gdzie to możliwe należy wprowadzić oznaczenia sprzętu wskazujące na jego właściciela,

Pracownicy posługujący się przenośnym sprzętem (lub innymi przenośnymi nośnikami), pracujący w firmie i w terenie, powinni okazywać go na każde wezwanie organizacji.

Wnoszenie własnego przenośnego sprzętu przez odwiedzających winno być nadzorowane

Jakie są potrzeby organizacji w tym zakresie i jaka obowiązuje polityka?

Jakie zabezpieczenia są stosowane przy wyjściu (i wejściu)? Czy można „wynieść" mienia korzystając z technologii Internetu?

W jaki sposób nadzoruje się wynoszenie i wnoszenie tych nośników, które łatwo schować?

Zbyt/zu rezim, ale też zbyt/na pobłażliwość nieuchronnie prowadzą do naruszeń wprowadzonych zasad. Dlatego najwięcej zależy od uświadomienia pracowników.

A.8 Zarządzanie systemami i sieciami

A.8.1 Procedury eksploatacji oraz zakresy odpowiedzialności

- Dokumentowanie procedur eksploatacyjnych (A.8.1.1)

Dla zapewnienia poprawnego i bezpiecznego działania urządzeń do przetwarzania informacji, należy udokumentować i utrzymywać procedury eksploatacyjne identyfikowane w polityce bezpieczeństwa,

Zakres dokumentacji zależny od złożoności, wielkości organizacji i kompetencji personelu,

Gdy odpowiedzialność za eksploatację urządzeń jest zlecana innej organizacji, konieczne jest zawarcie szczegółowego kontraktu i zapewnienie, że ta organizacja także spełnia wymagania BS 7799-2

Jakie procedury zostały ustanowione i udokumentowane? Czy są adekwatne? Czy są zatwierdzone?

W jaki sposób dokonuje się przeglądu? Jak dokonywane są zmiany?

Jak funkcjonuje administrowanie sieci? Jakie ustanowiono procedury?

Jak uregulowano współpracę z ewentualnymi zewnętrznymi dostawcami? Jakie oni mają instrukcje? Jak są nadzorowane?

A.8 Zarządzanie systemami i sieciami

A.8.1 Procedury eksploatacji oraz zakresy odpowiedzialności

- Kontrola zmian w eksploatacji (A.8.1.2)

Zmiany w urządzeniach (zarówno w sprzęcie jak i w oprogramowaniu) winny być nadzorowane.

Dotyczy to nie tylko instalowania nowego sprzętu czy oprogramowania, ale również modernizacji istniejącego,

Procedury eksploatacji winny określać tryb wprowadzania (zatwierdzania) zmian i ewentualne kroki, jakie należy podjąć jeśli zmiana wywoła niepożądane skutki.

Jak zdefiniowano odpowiedzialność za wprowadzanie zmian? Jak regulują to procedury?

W jaki sposób monitoruje się przebieg zmian? Czy są utrzymywane stosowne zapisy?

Czy w procesie zatwierdzania zmian ocenia się możliwe straty? Jak procedury opisują postępowanie na wypadek nieprzewidzianych komplikacji?

W jaki sposób o zmianach informowany jest personel? Szkolenia?

A.8 Zarządzanie systemami i sieciami

A.8.1 Procedury eksploatacji oraz zakresy odpowiedzialności

- Procedury zarządzania incydentami związanymi z bezpieczeństwem (A.8.1.3)

Kierownictwo ponosi odpowiedzialność za to, by reakcja na incydenty była szybka, skuteczna i uporządkowana - procedury,

Wiele incydentów można zawczasu przewidzieć i podjąć kroki zapobiegawcze (choć jakże często się je lekceważy),

Dane na temat incydentów należy rejestrować, incydenty powinny podlegać przeglądom i analizie (przyczyny) – forum bezpieczeństwa

Jakie są procedury postępowania w reakcji na incydenty? Czy są spójne z procedurami zgłaszania przypadków naruszenia bezpieczeństwa (6.3)?

Jakie zapisy są utrzymywane? W jaki sposób analizuje się incydenty? Jakie działania podejmowane są w następstwie?

Czy przeprowadza się ćwiczenia postępowania na wypadek incydentów? Jakie wnioski płyną z tych ćwiczeń?

Rejestracje [illegible]

A.8 Zarządzanie systemami i sieciami

A.8.1 Procedury eksploatacji oraz zakresy odpowiedzialności

- Podział obowiązków (A.8.1.4)

Obowiązki i obszary odpowiedzialności należy rozdzielać, by ograniczyć ryzyko nieuprawnionej modyfikacji lub nadużyć (analiza ryzyka),

Podział obowiązków jest tradycyjnym sposobem zwiększania skuteczności nadzoru nad czynnościami, szczególnie tam gdzie monitorowanie jest utrudnione, także tam, gdzie w grę wchodzi wielka odpowiedzialność

Czy organizacja zidentyfikowała krytyczne obszary i procesy w swojej analizie ryzyka? Czy w tych obszarach zbyt duża odpowiedzialność i uprawnienia nie są gromadzone w jednym ręku?

Jakie niezależne sprawdzenia ustanowiono na poszczególnych etapach tych procesów?

Jak zorganizowano pracę w krytycznych obszarach na wypadek choroby, urlopu, delegacji etc.?

A.8 Zarządzanie systemami i sieciami

A.8.1 Procedury eksploatacji oraz zakresy odpowiedzialności

- Oddzielanie urządzeń będących w eksploatacji od przeznaczonych do prac rozwojowych (A.8.1.5)

Należy rozdzielać (fizycznie lub poprzez uprawnienia) urządzenia do prac rozwojowych od tych służących w eksploatacji,

Zasady przenoszenia oprogramowania z „rozwoju" do „eksploatacji" - określone i udokumentowane, spójne z 8.1.2 - kontrola zmian w eksploatacji

Jak zorganizowano rozdział? W jaki sposób zapobiega się mieszaniu zasobów będących w fazie tworzenia i testowania od tych, które służą do normalnej pracy?

Jeśli wprowadzenie fizycznego rozdziału nie było możliwe, to jak zorganizowano zasady dostępu?

Czy zasady przenoszenia oprogramowania są spójne z zasadami nadzorowania zmian w eksploatacji?

A.8 Zarządzanie systemami i sieciami

A.8.1 Procedury eksploatacji oraz zakresy odpowiedzialności

- Zewnętrzne zarządzanie urządzeniami (A.8.1.6)

Należy przeprowadzić analizę ryzyka przed zleceniem usługi zarządzania urządzeniami z zewnątrz.

Z wykonawcą należy uzgodnić szczegółowe zabezpieczenia i włączyć je do umowy, jednak żadna umowa nie jest gwarancją bezpieczeństwa

Jak przeprowadzono analizę ryzyka?

Jakie wymagania sformułowano w stosunku do zewnętrznego wykonawcy? Jak opisano to w umowie?

W jaki sposób monitoruje się wypełnianie postanowień umowy? Jaki wpływ ma organizacja w działaniu wykonawcy?

Jakie uregulowania własne obowiązują u wykonawcy? Czy pozostają w zgodności z wymaganiami BS 7799-2?

A.8 Zarządzanie systemami i sieciami

A.8.2 Planowanie i odbiór systemu

- Planowanie pojemności (A.8.2.1)

Dla minimalizacji ryzyka awarii systemów konieczne jest nie tylko monitorowanie bieżących potrzeb w zakresie pojemności, ale i przewidywanie przyszłych potrzeb.

Zmiany potrzeb co do pojemności systemów mogą być nagłe. Ich skutkiem może być znaczne ograniczenie wydolności.

Przewidywanie przyszłych potrzeb powinno być prowadzone cyklicznie

Co podlega monitorowaniu? Jakie „wąskie gardła" zostały zidentyfikowane?

W jaki sposób dane z monitorowania są wykorzystywane do planowania przyszłych potrzeb? Czy występują jakieś trendy?

Jak przebiega proces planowania? Jakie *inne przesłanki bierze się pod uwagę*?

Czy w planowaniu pojemności systemów uwzględnia się tzw. czynnik ludzki – potrzeby w zakresie personelu?

A.8 Zarządzanie systemami i sieciami

A.8.2 Planowanie i odbiór systemu

- Odbiór systemu (A.8.2.2)

Wdrażanie nowych urządzeń, systemów, nowych wersji, aktualizacji istniejących – wszystko co wymaga ustanowienia kryteriów odbioru i przeprowadzenia testów przed ich akceptacją.

Wszystkie przeprowadzane testy wymagają udokumentowania i zatwierdzenia

Jak zaplanowano wdrożenie? Jak zaplanowano czynności weryfikacyjne? Czy *staranność tych planów jest adekwatna* do skali wdrożenia i skali możliwych negatywnych skutków?

Jakie kryteria akceptacji zostały ustanowione? Czy są jednoznaczne?

Kiedy i jak przeprowadza się testowanie? Jakie są wyniki testów? Czy testy są odpowiednio udokumentowane?

A.8 Zarządzanie systemami i sieciami

A.8.3 Ochrona przed szkodliwym oprogramowaniem

- Zabezpieczenia przed szkodliwym oprogramowaniem (A.8.3.1)

Dla zapewnienia poufności, integralności i dostępności chronionych informacji należy wdrożyć środki wykrywania i ochrony (ISO/IEC 17799),

Kluczowe znaczenie ma świadomość personelu, kształcowanie nawyków,

Dynamiczny rozwój szkodliwego oprogramowania wymusza konieczność ciągłego uaktualniania stosowanych zabezpieczeń

Jak zorganizowano system wykrywania i ochrony? Jaką politykę stosuje się wobec przychodzącego oprogramowania?

Jakie są potencjalne możliwości wtargnięcia szkodliwego oprogramowania do systemu (systemów)?

Jakie zasady postępowania obowiązują pracowników? Jak są przestrzegane?

Jak postępuje się w przypadku zainfekowania systemu?

Jak często i w jaki sposób aktualizuje się zabezpieczenia?

MANAGING RISK

A.8 Zarządzanie systemami i sieciami

A.8.4 Procedury wewnętrzne

- Kopie zapasowe informacji (A.8.4.1)

Nośniki informacji ulegają uszkodzeniom; zapewnienie integralności i dostępności informacji wymaga posiadania zapasowych kopii,

Częstość wykonywania kopii zależy od tego jak krytyczna dla organizacji jest dana informacja (analiza ryzyka),

Kopie przechowywane w bezpiecznym miejscu,

Przy długoterminowym przechowywaniu konieczne zapewnienie sprzętu i oprogramowania, które potrafią odczytać dany nośnik,

Należy testować odtwarzanie kopii zapasowych

Czy organizacja sklasyfikowała informacje według ich znaczenia? Jak odzwierciedla to analiza ryzyka?

Jakie procedury postępowania w zakresie tworzenia, przechowywania i odtwarzania kopii zapasowych zostały ustanowione?

Jak często tworzy się kopie? Ile kopii? Jak są przechowywane? Czy przechowuje się jakieś kopie poza siedzibą? Jak są tam chronione?

Jakie stosuje się nośniki? Jaka jest ich trwałość? Czy organizacja jest w stanie je odtworzyć?

Czy przeprowadza się próby odtwarzania? Wyniki? Zapisy?

MANAGING RISK

16.09.2003 dn. wizyta
o godzinie

A.8 Zarządzanie systemami i sieciami

A.8.4 Procedury wewnętrzne

- Dzienniki operatorów (A.8.4.2), zapisywanie informacji o błędach (A.8.4.3)

Operatorzy winni prowadzić dzienniki wykonywanych przez siebie czynności,

Dzienniki powinny podlegać regularnej i niezależnej kontroli,

Wszelkie incydenty powinny być zapisywane,

Automatyczne lub ręczne zapisy działań operatorów są przydatne podczas analizy incydentów i reakcji na nie,

Należy przechowywać dziennik przez określony czas

Jakie dzienniki są wymagane przez procedury operacyjne: w normalnych działaniach, w reagowaniu na incydenty?

Jaka informacja zawarta jest w dziennikach?

Czy dzienniki są w sposób niezależny przeglądane? Jakie wnioski wypływają z tych przeglądów i kontroli?

W jaki sposób przechowuje się dzienniki? Czy można je zidentyfikować? Odtworzyć w razie potrzeby?

MANAGING RISK

A.8 Zarządzanie systemami i sieciami

A.8.5 Zarządzanie sieciami

- Zabezpieczenia sieci (A.8.5.1)

Sieci i ich infrastruktura – przez swą złożoność i mnogość włączonych urządzeń, poprzez łatwość popełnienia błędu w konfigurowaniu, są szczególnie podatne na zagrożenia,

Zarządzanie bezpieczeństwem sieciowym jest jednym z kluczowych elementów zarządzania bezpieczeństwem w ogóle,

Przepływ wrażliwych informacji przez sieci publicznie dostępne może wymagać dodatkowych zabezpieczeń,

W jaki sposób organizacja zaplanowała swoją sieć (sieci)? Jakie są możliwości jej penetracji i jakie przewidziano zabezpieczenia?

W jaki sposób używane sieci są udokumentowane?

W jaki sposób organizacja monitoruje bezpieczeństwo użytkowanych sieci?

Jak zapewnia się bezpieczeństwo na styku z sieciami publicznymi i w nich?

Incydenty?

A.8 Zarządzanie systemami i sieciami

A.8.6 Postępowanie z nośnikami i ich bezpieczeństwo

- Zarządzanie wymiennymi nośnikami komputerowymi (A.8.6.1)

Wymienne nośniki (taśmy, dyski, kasety etc.) winny być nadzorowane,

Przechowywanie, transport – zgodnie z zaleceniami producenta,

Wynoszenie, transport nośników - autoryzowane

Jak uwzględniono wymienne nośniki w analizie ryzyka?

Jakie ustanowiono procedury postępowania (przechowywanie, wynoszenie, transport, użytkowanie w innych środowiskach, logowanie)?

- Niszczenie nośników (A.8.6.2)

Niepotrzebny już nośnik jest uznawany za bezwartościowy. Ale zawiera dane!

Wyrzucony nośnik może doprowadzić do naruszenia poufności. Dlatego należy go zniszczyć w sposób bezpieczny i pewny

Jak postępuje się z niepotrzebnymi nośnikami?

Jeśli niszczy inna organizacja, to jak to robi? Jak zapewnia bezpieczeństwo?

A.8 Zarządzanie systemami i sieciami

A.8.6 Postępowanie z nośnikami i ich bezpieczeństwo

- Procedury postępowania z informacją (A.8.6.3)

Wszystkie wrażliwe informacje (także finansowe) winny być chronione przed nieuprawnionym dostępem lub nadużyciem.

Należy wyraźnie określić odpowiedzialność za ochronę, szczególnie przy przekazywaniu informacji,

Wyraźna identyfikacja osób: nadawcy i odbiorcy przesyłki, identyfikacja kuriera (przewoźnika etc.), potwierdzenia nadania i odbioru

Jak uwzględniono w analizie ryzyka wysyłane i odbierane informacje? Jakie stosuje się procedury?

Jak analiza ryzyka i procedury postępowania mają się do przyjętej klasyfikacji informacji?

Jakie są zasady identyfikacji osób nieznanych personelowi wysyłającemu i odbierającemu informacje (kurierzy, dostawcy, przewoźnicy etc.).

Jak monitoruje się postępowanie z informacją? Incydenty?

A.8 Zarządzanie systemami i sieciami

A.8.6 Postępowanie z nośnikami i ich bezpieczeństwo

- Bezpieczeństwo dokumentacji systemu (A.8.6.4)

Nieuprawniony dostęp do dokumentacji systemu stanowi poważne zagrożenie dla bezpieczeństwa informacji,

Szczególną ochroną należy otaczać dokumentacją opisującą obowiązujące zasady zarządzania bezpieczeństwem (procedury, instrukcje, także zapisy!).

Dokumentacja systemu winna również być sklasyfikowana, należy określić zasady dystrybucji, kopiowania i likwidowania dokumentacji

Jak nadzorowane są dokumenty systemowe? Jak je zaklasyfikowano? Jak są identyfikowane?

Jakie są zasady dostępu do dokumentów? Na jakich nośnikach występują? Jak nadzoruje się ich powielanie rozpowszechnianie?

Jak przebiega zatwierdzanie, zmiany, ponowne zatwierdzanie etc.?

Jak postępuje się z dokumentami nieaktualnymi?

A.8 Zarządzanie systemami i sieciami

A.8.7 Wymiana danych i oprogramowania

- Porozumienie dotyczące wymiany danych i oprogramowania (A.8.7.1)

Wymiana informacji między organizacjami (elektroniczna i ręczna) powinna być nadzorowana,

Organizacje powinny porozumieć się co do zasad wymiany informacji, z uwzględnieniem wymagań prawnych,

Porozumienia powinny być zatwierdzone na odpowiednim szczeblu organizacji, poddawane okresowym przeglądom,

Jeśli stosowane praktyki wymiany ulegają zmianom, powinno to zostać wprowadzone do porozumień

Jakie organizacje uczestniczą w wymianie informacji? Czy uzgodniono z nimi porozumienia?

Jak zdefiniowano poziomy bezpieczeństwa przy wymianie? Jak to się ma do klasyfikacji informacji?

Jakie zabezpieczenia stosowane są w tych organizacjach? (ISO/IEC 17799)

A.8 Zarządzanie systemami i sieciami

A.8.7 Wymiana danych i oprogramowania

- Zabezpieczenia nośników podczas transportu (A.8.7.2)

Transportowane nośniki winny być chronione przed nieuprawnionym dostępem, nadużyciem lub uszkodzeniem,

Analiza ryzyka winna dać odpowiedź co do wyboru środka transportu i stosowanych zabezpieczeń.

Wszystkie nadania winny być zarejestrowane i - tam gdzie to konieczne - zatwierdzane.

Czy zidentyfikowano wszystkie miejsca w organizacji, w których nośniki wydawane są do transportu?

Jakie są wyniki analizy ryzyka? Jakie metody i środki transportu wybrano? Według jakich kryteriów?

Jakie stosuje się zabezpieczenia?

Jeśli transport zleca się innej organizacji (poczta, firma kurierska, przewoźnik etc.) to jakie praktyki i zabezpieczenia są tam stosowane?

A.8 Zarządzanie systemami i sieciami

A.8.7 Wymiana danych i oprogramowania

- Bezpieczeństwo handlu elektronicznego (A.8.7.3)

W handlu prowadzonym drogą elektroniczną należy chronić nie tylko bezpieczeństwo informacji, ale też stosować zabezpieczenia przed oszustwami i sporami kontraktowymi,

Stosowanie zabezpieczeń (szyfrowanie, podpisy elektroniczne) winno być zgodne z obowiązującym prawem,

W organizacji należy ustanowić politykę dotyczącą uprawnień do handlu i monitorowania ich wykorzystania

Jakie działania handlowe są prowadzone? Jakie zamierza się prowadzić w przyszłości?

Kto jest uprawniony do działań? Jak przebiega autoryzacja?

Czy wprowadza się podział obowiązków lub inne formy dodatkowego nadzoru dla zmniejszenia ryzyka oszustwa?

Jakie zabezpieczenia transakcji? Jakie zabezpieczenia sieciowe przed atakami z zewnątrz?

A.8 Zarządzanie systemami i sieciami

A.8.7 Wymiana danych i oprogramowania

- Bezpieczeństwo poczty elektronicznej (A.8.7.4)

Należy ustanowić politykę używania poczty elektronicznej, zarówno w obrębie organizacji jak i na zewnątrz,

Świadomość personelu co do zawartości listów elektronicznych, nawet tych prywatnych, znaczenie przepisów prawa, odpowiedzialność sądowa,

Jeśli organizacje porozumiewają się pocztą elektroniczną – udokumentowane porozumienie określające status wiadomości,

Poczta elektroniczna jako furtka dla szkodliwego oprogramowania

Jakie informacje przesyła się pocztą elektroniczną? Jakie załączniki? Jak potwierdza się prawidłowość doręczenia?

W jaki sposób traktuje się pocztę przychodzącą? Techniki antywirusowe? Anti-spam?

Czy stosuje się techniki szyfrowania?

Polityka: czy uwzględnia aspekty prawne? Czy powstała w oparciu o analizę ryzyka?

W jaki sposób ruch pocztowy jest monitorowany? Inicjowany?

A.8 Zarządzanie systemami i sieciami

A.8.7 Wymiana danych i oprogramowania

- Bezpieczeństwo elektronicznych systemów biurowych (A.8.7.5)

Systemy biurowe, choć znacząco poprawiają efektywność pracy, stwarzają nowe zagrożenia dla bezpieczeństwa – analiza ryzyka,

Należy ustanowić politykę oraz wytyczne używania systemów biurowych (np. urządzeń do powielania i przesyłania informacji, kalendarzy i notatników elektronicznych, baz danych zawierających dane osobowe – adresy, numery telefonów etc.),

Należy ustanowić zasady dostępu do tych systemów

Jakie systemy biurowe funkcjonują? Jakie ryzyka wiążą się z nimi? Jakie polityki (procedury) obowiązują przy korzystaniu z nich?

Kto do jakich systemów ma dostęp? Jak korzystają z systemów pracownicy pracujący poza siedzibą?

Dostępność systemów dla gości, dostawców, klientów, etc.? Dla innych organizacji?

A.8 Zarządzanie systemami i sieciami

A.8.7 Wymiana danych i oprogramowania

- *Systemy publicznie dostępne (A.8.7.6)*

Zanim informacja zostanie publicznie udostępniona powinien nastąpić formalny proces jej autoryzacji,

Należy sprawdzić poprawność, kompletność, szczegółowość, należy rozważyć zgodność upowszechniania z prawem,

Po udostępnieniu należy zapewnić ochronę przed nieuprawnioną modyfikacją informacji,

Informacja przychodząca z systemów publicznych powinna być poddana weryfikacji

Jak przebiega proces autoryzacji? Kto posiada uprawnienia do umieszczania informacji w systemach publicznych?

Czy ktoś w organizacji regularnie sprawdza zawartość prezentowanych informacji?

Czy ktoś w organizacji nadzoruje stronę *prawną publikowania (lub pobierania z* systemów publicznych) informacji? Prawodawstwo kraju, w którym publikowana jest informacja?

Jakie zabezpieczenia stosuje się przed intruzami chcącymi wejść do systemów organizacji poprzez systemy publiczne?

A.8 Zarządzanie systemami i sieciami

A.8.7 Wymiana danych i oprogramowania

- Inne formy wymiany informacji (A.8.7.7)

Należy ustanowić i wdrożyć zasady ochrony wymiany informacji przy pomocy innych środków – ustnie, telefonicznie, faksem etc.,

Pracownicy muszą być świadomi, że rozmowa w miejscu publicznym, wiadomość pozostawiona na sekretarce, wysłany bez powiadomienia *fax*, źle wybrany numer, etc. mogą stanowić zagrożenie bezpieczeństwa,

Jakie są w organizacji zasady używania telefonów? Telefonów komórkowych? Automatycznych sekretarek? Faksu? Automatów poczty elektronicznej? Innych urządzeń i środków?

A.9 Kontrola dostępu do systemu

A.9.1 Potrzeby biznesowe związane z dostępem do systemu

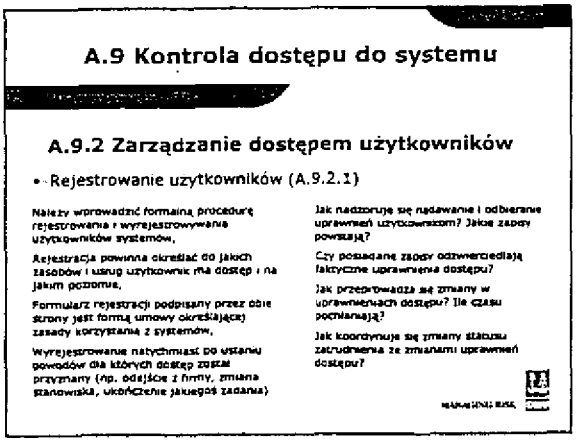
- Polityka kontroli dostępu (A.9.1.1)

Należy zdefiniować i udokumentować wymagania biznesowe odnośnie kontroli dostępu do informacji – polityka kontroli dostępu,

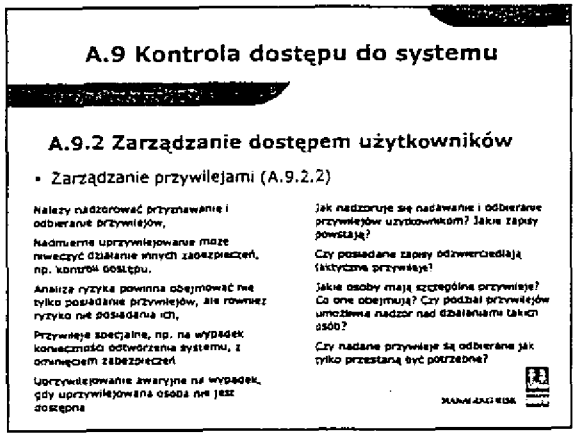
Wskazane jest tworzenie profili dostępu standardowych użytkowników.

Jak ustanowiono politykę kontroli dostępu? Na ile kontrola dostępu sterowana jest potrzebami biznesowymi?

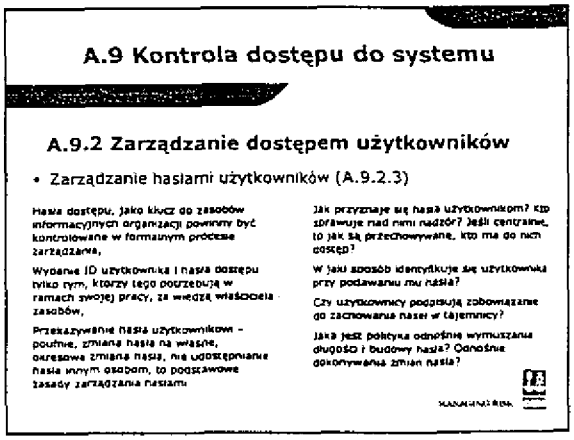
Na ile jednoznacznie określa ona możliwości dostępu do danych dla użytkowników różnych szczebli?



kogoś zmotywować zwolnieniem pracownikowi o wiele więcej by kosztowało niż dostęp do systemu
Zasada 4 oczu - czasu kubikiskat



W/g wprowadzonej DzU ~~Nr~~ Poz 1024/2004
czas życia hasła 30 dni



A.9 Kontrola dostępu do systemu

A.9.2 Zarządzanie dostępem użytkowników

- Przegląd praw dostępu użytkowników (A.9.2.4)

Kierownictwo powinno regularnie przeprowadzać formalny przegląd praw dostępu użytkowników,

Wynikiem przeglądu powinno być utrzymanie praw, jeśli potrzeby biznesowe wciąż istnieją, lub odebranie jeśli potrzeby ustały, a praw odebranych nie odebrano,

Przeglądy praw dostępu winny być dokumentowane, a prawa zatwierdzane przez uprawnioną osobę

Jak odbywają się przeglądy praw dostępu? Czy utrzymuje się zapisy?

Czy przeglądy obejmują zarówno uprawnienia dostępu jak i przywileje?

Czy bieżące prawa dostępu użytkowników są zgodne z postanowieniami podjętymi na przeglądzie?

Jak zarządza się zmianami praw dostępu w warunkach zmian kadrowych?

A.9 Kontrola dostępu do systemu

A.9.3 Zakres odpowiedzialności użytkowników

- Użycie haseł (A.9.3.1)

Dla zapobiegania nieuprawnionemu dostępowi użytkownicy powinni stosować się do dobrych, sprawdzonych praktyk bezpieczeństwa,

Wskazane jest, by organizacja na bieżąco uświadamiała użytkowników jakie praktyki są zalecane (ISO/IEC 17799),

Czy polityka zarządzania hasłami jest adekwatna do potrzeb organizacji w zakresie bezpieczeństwa? Czy jest adekwatna do poziomu świadomości personelu?

Jak użytkownicy przechowują swoje hasła dostępu? Czy udostępniają innym? Jak często je zmieniają? Czy jest to wymuszane? Czy można powtarzać hasła?

A.9 Kontrola dostępu do systemu

A.9.3 Zakres odpowiedzialności użytkowników

- Pozostawianie sprzętu użytkownika bez opieki (A.9.3.2)

Użytkownicy ponoszą odpowiedzialność za zapewnienie odpowiedniej ochrony sprzętu, gdy nie jest on używany,

Różne rodzaje zabezpieczeń wprowadzone przez organizację winny być stosowane przez użytkowników: zabezpieczenia organizacyjne, fizyczne, sprzętowe, logiczne.

Jakie procedury pozostawiania sprzętu obowiązują?

Czy są stosowane? Czy pracownicy mają świadomość możliwych następstw pozostawienia sprzętu bez wymaganego zabezpieczenia?

W jaki sposób winien być zabezpieczany sprzęt o szczególnym znaczeniu (np. serwery)? Jakie praktyki obserwuje się w tym zakresie?

A.9 Kontrola dostępu do systemu

A.9.4 Kontrola dostępu do sieci

- Polityka korzystania z usług sieciowych (A.9.4.1)

Użytkownicy powinni mieć dostęp tylko do tych usług, do których mają uprawnienia - konieczne jest jednoznaczne ich sprecyzowanie,

Nie jest wskazane eksponowanie pełnego wachlarza usług sieciowych,

Wskazane jest udostępnianie szczególnie wrażliwych usług tylko z wybranych terminali

Jaka jest topologia sieci? Jakiego rodzaju usługi sieciowe są realizowane?

Jak monitoruje się usługi sieciowe? Czy powstają zapisy? Czy odnotowuje się incydenty? Jakie działania z nich wynikają? Jak ocenia się ich skuteczność?

Jacy użytkownicy mają dostęp do jakich usług? Czy przyznany dostęp do usług nie pozostaje w sprzeczności z ustanowionymi uprawnieniami w dostępie do informacji?

A.9 Kontrola dostępu do systemu

A.9.4 Kontrola dostępu do sieci

- Wymuszenie dróg połączeń (A.9.4.2)

Tam gdzie to jest możliwe, użytkownicy powinni łączyć swój terminal z usługą poprzez wymuszoną drogę w sieci - routery, dedykowane linie logiczne lub fizyczne, dedykowane porty

Dodatkowym zabezpieczeniem może być udostępnienie danej usługi tylko z lokalizacji uznawanych za bezpieczne i nie udostępnianie jej gdy terminal łączy się z innej lokalizacji

Jeśli stosuje się politykę wymuszania dróg połączeń, to czy nie ma możliwości ominięcia ich?

Z jakich lokalizacji włączają się użytkownicy? Czy zasady udostępniania usług i dostępu do informacji są zgodne z polityką bezpieczeństwa?

Czy rozwiązania telekomunikacyjne zapewniają skuteczne polityki wymuszania dróg połączeń w różnych warunkach, np. przełączenia?

A.9 Kontrola dostępu do systemu

A.9.4 Kontrola dostępu do sieci

- Uwierzytelnianie użytkowników przy połączeniach zewnętrznych (A.9.4.3), uwierzytelnianie węzłów (A.9.4.4)

Zdalny dostęp i połączenia ze zdalnymi komputerami powinny być uwierzytelniane,

Dodatkowe zabezpieczenia (np. token) w uzupełnieniu do ID i hasła użytkownika, w połączeniach zdalnych redukują ryzyko do akceptowalnego poziomu,

Należy zidentyfikować wszystkie linie pozwalające „dodzwonić" się do systemu i ocenić ryzyko,

Należy także przeprowadzić analizę ryzyka związanego z wszystkimi węzłami sieci, w siedzibie organizacji i poza nią

Czy wszystkie linie, węzły sieci zostały zidentyfikowane? Czy przeprowadzono pełną, kompleksową analizę ryzyka?

Jak uwierzytelniają się użytkownicy przy połączeniach zewnętrznych? Czy sposób uwierzytelniania jest adekwatny do wrażliwości informacji, do których uzyskuje się dostęp?

Czy uzyskanie dostępu do przypisanych zasobów daje możliwość penetracji ponad przyznane uprawnienia?

A.9 Kontrola dostępu do systemu

A.9.4 Kontrola dostępu do sieci

- Ochrona zdalnych portów diagnostycznych (A.9.4.5)

Dostęp do portów diagnostycznych powinien być nadzorowany,

Należy rozważyć wdrożenie procedur wymuszających wyłączanie tych portów, gdy nie są w użyciu,

Każde wykorzystanie portu winno być poprzedzone uwierzytelnieniem i potwierdzone,

Czy organizacja zidentyfikowała wszystkie porty diagnostyczne? W jaki sposób są zabezpieczane?

Jakie są zasady korzystania z tych portów? *Kto ma do nich dostęp? Jakie są zasady uwierzytelniania?* Czy hasła fabryczne portów są zmieniane? Jakie zasady powstają?

Czy po wykorzystaniu porty są wyłączane? Jeśli nie to jakie wprowadzono zabezpieczenia? *Czy monitoruje się* aktywność portów?

MANAGING RISK

A.9 Kontrola dostępu do systemu

A.9.4 Kontrola dostępu do sieci

- Rozdzielanie sieci (A.9.4.6)

Wewnątrz sieci należy wprowadzić zabezpieczenia w celu rozdzielenia grup usług informacyjnych, użytkowników i systemów informacyjnych,

Podział na domeny fizyczne lub logiczne zmniejsza ryzyko, szczególnie w większych sieciach,

Analiza ryzyka powinna dostarczyć odpowiedzi na pytanie o poziom bezpieczeństwa każdej domeny,

Domeny i ich powiązania winny być szczegółowo udokumentowane

W jaki sposób dokonano podziału na domeny? Jak duże? Jak są od siebie oddzielone?

Jaki poziom ryzyka określono dla każdej z nich? Jakie stosuje się zabezpieczenia? Czy są one adekwatne do wymagań bezpieczeństwa?

Czy w ramach działalności operacyjnej realizuje się komunikację z sieciami innych organizacji (dostawcy, klienci, serwis)? Jakie zabezpieczenia?

Czy stosowane zabezpieczenia nie ograniczają funkcjonalności?

MANAGING RISK

A.9 Kontrola dostępu do systemu

A.9.4 Kontrola dostępu do sieci

- Kontrola połączeń sieciowych (A.9.4.7), kontrola routingu w sieciach (A.9.4.8)

We współużytkowanych sieciach możliwości połączeń pomiędzy poszczególnymi użytkownikami powinny być ograniczone do takiego poziomu, na jaki zezwalają uprawnienia dostępu każdego z nich do zasobów informacyjnych,

Jeśli sieci są współużytkowane przez różne organizacje, należy stosować zabezpieczenia kontrolowania tras (routery sieciowe). Sprawdzenie adresu nadawcy i odbiorcy znacząco redukuje poziom ryzyka,

Analiza ryzyka powinna dotyczyć każdego połączenia i być w pełni udokumentowana

W jaki sposób polityka uprawnień dostępu użytkowników znajduje odzwierciedlenie w możliwościach połączeniowych między nimi (szczególnie jeśli w grę wchodzi łączenie po publicznych łączach)?

Jeśli wymuszane trasy są kontrolowane przez inne organizacje, to jakie zabezpieczenia (także alternatywy na wypadek awarii, etc.) są dostępne?

Jeśli w grę wchodzi trasa po publicznych łączach, to czy brano pod uwagę alternatywne sposoby przesyłania informacji?

MANAGING RISK

A.9 Kontrola dostępu do systemu

A.9.4 Kontrola dostępu do sieci

- Bezpieczeństwo usług sieciowych (A.9.4.9)

Czy organizacja korzysta z usług sieciowych dostarczanych przez inne organizacje, należy zadbać o jasny opis cech bezpieczeństwa tych usług,

Oferowane cechy bezpieczeństwa powinny być poddane analizie ryzyka,

Czy organizacja otrzymała od dostawców usług sieciowych pełną informację o cechach bezpieczeństwa?

Czy oferowane cechy bezpieczeństwa są wystarczające w stosunku do potrzeb? Czy zapewniają poufność, integralność i dostępność?

W jaki sposób uwzględniono je w procedurach operacyjnych organizacji?

Czy dokonuje się okresowych przeglądów cech bezpieczeństwa usług?

A.9 Kontrola dostępu do systemu

A.9.5 Kontrola dostępu do systemów operacyjnych

- Automatyczna identyfikacja terminala (A.9.5.1), procedury rejestrowania terminala w systemie (A.9.5.2)

W celu uwierzytelniania połączeń z określonych miejsc i urządzeń przenośnych należy rozważyć automatyczną identyfikację terminala,

Dostęp do usług informacyjnych powinien być osiągany za pomocą procesu bezpiecznego rejestrowania (wytyczne: ISO/IEC 17799),

Procedura rejestrowania powinna być przyjazna, jednak im mniej informacji dostarcza, tym lepiej,

Procedura rejestrowania powinna być przedmiotem analizy ryzyka

Jeśli automatyczna identyfikacja jest stosowana, to w jaki sposób się ją sprawdza?

Czy oprócz identyfikacji terminala wymaga się ID i hasła użytkownika?

Czy oprócz podania ID i hasła stosuje się inne kroki w procedurze rejestracji?

Czy przewidziano blokadę dostępu po określonej liczbie nieudanych prób rejestracji? Czy oprócz blokady dostępu stosuje się inne restrykcje?

A.9 Kontrola dostępu do systemu

A.9.5 Kontrola dostępu do systemów operacyjnych

- Identyfikacja i uwierzytelnianie użytkowników (A.9.5.3)

Każdy użytkownik powinien mieć unikalny identyfikator użytkownika (user ID) do swojego osobistego i wyłącznego użytku (przypisanie działań i odpowiedzialność za nie),

Należy wybrać odpowiednią technikę uwierzytelniania dla potwierdzania tożsamości użytkownika,

Wskazana analiza ryzyka w przypadku wprowadzania użytkowników o specjalnych uprawnieniach (superusers)

Czy identyfikatory są unikalne, czy mogą być współużytkowane przez więcej osób? Jeśli tak, to co za tym przemawia? Jakie dodatkowe zabezpieczenia są wtedy stosowane?

W jaki sposób identyfikuje się użytkowników o krytycznym znaczeniu (np. administratorzy)? Czy prowadzone są zapisy?

Czy stosowane procedury identyfikacji i uwierzytelniania zapewniają odpowiednie bezpieczeństwo?

A.9 Kontrola dostępu do systemu

A.9.5 Kontrola dostępu do systemów operacyjnych

- System zarządzania hasłami (A.9.5.4)

System zarządzania hasłami powinien opierać się na efektywnych, interaktywnych mechanizmach, które są w stanie wymusić stosowanie haseł odpowiedniej jakości,

Jeżeli stosowane systemy nie przewidują automatycznych mechanizmów wymuszających jakość i częstotliwość zmiany hasła, należy wprowadzić dodatkowe zabezpieczenia (wytyczne: ISO/IEC 17799),

Czy jest ustanowiona jakaś polityka odnośnie stosowania haseł?

Jaka jest długość haseł, częstotliwość zmiany, używanie wspólnych haseł?

W jaki sposób przechowuje się hasła?

Czy nadawane są hasła domyślne? Jeśli tak to czy są zmieniane? Czy dozwala się na utrzymywanie starych haseł?

Czy utrzymuje się zapisy dotyczące zmian haseł?

A.9 Kontrola dostępu do systemu

A.9.5 Kontrola dostępu do systemów operacyjnych

- Użycie systemowych programów narzędziowych (A.9.5.5)

Używanie systemowych programów narzędziowych (jako tych, które mogą istotnie zagrozić integralności systemu bezpieczeństwa) winno być ograniczone i ściśle kontrolowane,

Należy zidentyfikować wszystkie systemowe programy narzędziowe i przeprowadzić analizę ryzyka,

Używanie programów narzędziowych winno być monitorowane (wytyczne ISO/IEC 17799)

Czy organizacja zidentyfikowała wszystkie programy narzędziowe będące w jej posiadaniu? Czy nie pominięto jakichś starych, „zapomnianych" programów?

Kto i w jakich sytuacjach może z nich korzystać?

W jaki sposób jest to nadzorowane / monitorowane?

Czy istnieje możliwość instalowania takich programów lokalnie, bez wiedzy administratora?

A.9 Kontrola dostępu do systemu

A.9.5 Kontrola dostępu do systemów operacyjnych

- Alarm przymusu stosowany do zabezpieczenia użytkowników (A.9.5.6)

Osoby pracujące ze szczególnie wrażliwymi zasobami mogą być celem ataku osób trzecich – należy przeprowadzić analizę ryzyka,

Alarm przymusu (zwany też antynapadowym – duress alarm) może być wzięty pod uwagę jako dodatkowe zabezpieczenie,

W przypadku stosowania alarmu przymusu należy określić odpowiedzialności i procedury postępowania, konieczne jest przeprowadzenie szkoleń i ćwiczeń

Jeśli organizacja stosuje to zabezpieczenie, to w jakich miejscach? Czy wszystkie miejsca, w których jest on potrzebny zostały nim objęte?

W jaki sposób alarm jest wzbudzany? Czy wymaga sięgnięcia po procedury?

Czy sposób wzbudzenia alarmu nie naraża personelu na niebezpieczeństwo?

Czy istnieje możliwość odwołania fałszywego alarmu?

A.9 Kontrola dostępu do systemu

A.9.5 Kontrola dostępu do systemów operacyjnych

- Wyłączanie terminala po określonym czasie (A.9.5.7), ograniczanie czasu trwania połączenia (A.9.5.8)

Nieaktywne terminale, usytuowane w miejscach o wysokim ryzyku powinny być automatycznie wyłączane po upływie określonego czasu, by chronić je przed dostępem nieuprawnionych osób.

Ograniczenie ryzyka można także uzyskać ograniczając czas trwania połączenia.

Należy przeprowadzić analizę ryzyka

Jeśli organizacja stosuje te zabezpieczenia, to w jakich miejscach? Czy wszystkie miejsca, w których są one potrzebne zostały nimi objęte?

Po jakim czasie terminale są wyłączane? Jakie limity czasowe połączeń wprowadzono? Czy nie stwarza to zagrożenia? Czy nie utrudnia działań?

Jakiego rodzaju wyłączenie jest stosowane (wygaszacz z hasłem, wylogowanie)?

A.9 Kontrola dostępu do systemu

A.9.6 Kontrola dostępu do aplikacji

- Ograniczanie dostępu do informacji (A.9.6.1)

Właściciel biznesowy aplikacji i informacji z nią związanych powinien określić politykę dostępu do informacji i funkcji systemowych aplikacji.

Dostęp użytkowników powinien być ograniczony do tego, co określa ta polityka.

Uprawnienia i poziomy dostępu winny być regularnie przeglądane i aktualizowane

Czy określony dostęp do informacji i funkcji aplikacji jest zgodny z przyznanymi uprawnieniami dostępu użytkowników (A.9.1)?

Czy niedostępne dla danego użytkownika funkcje systemowe aplikacji są wyświetlane w oknach menu? W podręcznikach obsługi aplikacji?

W jaki sposób kontrolowane jest używanie tych funkcji, które są przeznaczone dla administratorów?

Jakie uprawnienia przyznawane są użytkownikom aplikacji i udostępnianych informacji?

A.9 Kontrola dostępu do systemu

A.9.6 Kontrola dostępu do aplikacji

- Izolowanie systemów wrażliwych (A.9.6.2)

Systemy wrażliwe powinny być instalowane w dedykowanych (izolowanych) środowiskach przetwarzania – analiza ryzyka.

Należy wskazać jakie systemy (np. dokumentacja systemu, wyniki analizy ryzyka, niektóre systemy przetwarzania), ocenić ryzyko biorąc także pod uwagę konieczność normalnego funkcjonowania tych systemów oraz koszty izolacji.

Izolowanie może być stopniowe

Jakie systemy zostały zidentyfikowane do izolowania? Jakie są wyniki analizy ryzyka?

Jakie stopnie izolacji zostały wprowadzone? W jaki sposób izolowanie jest realizowane?

W jaki sposób jest to nadzorowane / monitorowane?

Czy izolowanie nie utrudnia prowadzenia działalności?

Jakie są plany na wypadek awarii?

A.9 Kontrola dostępu do systemu

A.9.7 Monitorowanie dostępu do systemu i jego użycia

- *Zapisywanie informacji o zdarzeniach (A.9.7.1)*

Systemy powinny być monitorowane by możliwe było wykrywanie nieuprawnionego dostępu.

Zdarzenia wyjątkowe związane z bezpieczeństwem winny być zapisywane i przechowywane, by umożliwić dochodzenia i kontrolę dostępu w przyszłości.

Zapisy – jako minimum – powinny zawierać ID użytkownika, działanie, datę, godzinę, lokalizację i wynik (np. odmowa dostępu)

W jakich systemach organizacji należy prowadzić monitorowanie i zapisywać jego wyniki?

Co organizacja traktuje jako zdarzenie (incydent)? Co jest zapisywane?

Jak długo i w jaki sposób przechowuje się zapisy? Czy zapobiega to nieuprawnionej zmianie ich treści (np. dla ukrycia niedozwolonych działań)?

W jaki sposób jest to nadzorowane / monitorowane?

MANAGING RISK

Nie sprawdzałem codziennie logów. Nie miałem z tym nic w bieżącej pracy to na długo niektóre tylko

A.9 Kontrola dostępu do systemu

A.9.7 Monitorowanie dostępu do systemu i jego użycia

- Monitorowanie użycia systemu (A.9.7.2)

Należy wprowadzić procedury monitorowania używania urządzeń do przetwarzania informacji, a wyniki monitorowania powinny być poddawane regularnym przeglądom.

Dzięki monitorowaniu możliwa jest ocena skuteczności działania pozostałych zabezpieczeń.

Poziom, rodzaj, częstotliwość monitorowania – w oparciu o analizę ryzyka.

Wytyczne do monitorowania – ISO/IEC 17799

Jakie urządzenia winny być monitorowane? Jakie zapisy? Jaka częstość przeglądów?

Czy zapewniona jest niezależność monitorującego od monitorowanego?

Czy stosuje się jakąś automatyzację monitorowania (np. filtrowanie) dla ułatwienia wyszukiwania zdarzeń wyjątkowych, dla ułatwienia późniejszych przeglądów?

Jakie działania podejmowane są w wyniku monitorowania?

MANAGING RISK

Np na linie potrzebnemy dzienników z godziną i w menu

A.9 Kontrola dostępu do systemu

A.9.7 Monitorowanie dostępu do systemu i jego użycia

- Synchronizacja zegarów (A.9.7.3)

Dla zapewnienia dokładnego rejestrowania zegary komputerów powinny być synchronizowane.

Dzięki synchronizacji zarówno jest ustalać przebieg zdarzeń, ich kolejność, ułatwia to prowadzenie dochodzeń, rozstrzyganie sporów.

W jaki sposób synchronizuje się zegary? Co przyjęte jako podstawę synchronizacji?

Jakimi środkami technicznymi dysponuje się organizacja? Jaka częstotliwość synchronizacji jest zapewniona?

W jaki sposób następuje przejście na czas letni / zimowy?

Jak synchronizowane są zegary urządzeń przenośnych, które nie są stale wpięte do sieci?

Jak synchronizuje się zegary np. wiszące na ścianach (o ile może co mieć znaczenie)?

MANAGING RISK

A.9 Kontrola dostępu do systemu

A.9.8 Komputery przenośne i praca na odległość

- Komputery przenośne (A.9.8.1)

Należy przyjąć formalną politykę postępowania uwzględniającą ryzyko związane z pracą z komputerami przenośnymi, szczególnie w miejscach pozbawionych ochrony.

Oprócz znajomości polityki, personel powinien być świadomy zagrożeń, jakie wiążą się z użyciem sprzętu przenośnego, w danym miejscu i w danym czasie.

Konieczne jest wdrożenie zabezpieczeń nie tylko identyfikujących sprzęt, ale również uwierzytelniających użytkownika.

Szczególne zabezpieczenia – ochrona antywirusowa, kopie zapasowe, szyfrowanie etc.

Jakie urządzenia przenośne są objęte tym zabezpieczeniem?

Jaka jest polityka postępowania z urządzeniami przenośnymi w różnych miejscach i czasie? Co wynika z analizy ryzyka?

Jak przebiega proces uwierzytelnienia?

Jakie zabezpieczenia wprowadzono dla fizycznej ochrony urządzeń przenośnych?

MANAGING RISK

A.9 Kontrola dostępu do systemu

A.9.8 Komputery przenośne i praca na odległość

- Praca na odległość (A.9.8.2)

Należy wprowadzić polityki, procedury i standardy umożliwiające autoryzowanie i kontrolowanie pracy wykonywanej na odległość.

Oddalone miejsce pracy (dom, lotnisko, hotel, etc.) nie zabezpieczają z reguły wymaganego poziomu bezpieczeństwa.

Świadomość personelu.

Wytyczne – ISO/IEC 17799

Jeśli w grę wchodzi praca na odległość, to jakie procedury postępowania mają zastosowanie?

Jakie zabezpieczenia (fizyczne, logiczne)? Jak przebiega uwierzytelnianie? Czy czas połączeń jest limitowany?

Czy przy pracy na odległość stosuje się jakieś dodatkowe ograniczenia w dostępie do informacji?

Czy dozwala się używać sprzęt do innych celów (gry, Internet, etc.)?

MANAGING RISK

A.10 Rozwój i utrzymanie systemu

A.10.1 Wymagania bezpieczeństwa systemów

- Analiza i opis wymagań bezpieczeństwa (A.10.1.1)

Wymagania biznesowe dla nowych systemów lub dla rozszerzania istniejących powinny uwzględniać wymogi bezpieczeństwa.

Należy rozpoznawać możliwe zagrożenia już od pierwszych kroków podejmowanych dla rozwoju systemów – analiza ryzyka.

Wytyczne – ISO/IEC 17799

Jak zagadnienia bezpieczeństwa są brane pod uwagę przy projektowaniu nowych i rozwijaniu istniejących systemów?

Jak to przebiega przy kupowaniu gotowych produktów „z półki", a jak przy „szyciu na miarę"?

W jaki sposób dokonuje się przeglądów i weryfikacji spełniania zidentyfikowanych wymagań na poszczególnych etapach?

W jaki sposób rozwiązuje się problemy (odstępstwa, rozbieżności)?

MANAGING RISK

A.10 Rozwój i utrzymanie systemu

A.10.2 Bezpieczeństwo systemów aplikacji

- Potwierdzanie ważności danych wejściowych (A.10.2.1), kontrola wewnętrznego przetwarzania (A.10.2.2)

Dane wejściowe do aplikacji powinny być potwierdzane co do ich poprawności, nieważkie dane mogą prowadzić do utraty integralności i dostępności,

Konieczna jest kontrola poprawności przetwarzania danych dla uniknięcia błędów spowodowanych uszkodzonym lub zmienionym w sposób nieuprawniony oprogramowaniem,

Analiza ryzyka winna wskazać miejsca, w których powinno się sprawdzać poprawność danych i poprawność ich przetwarzania oraz rodzaje zabezpieczeń

Jak wprowadza się dane do aplikacji (ręcznie, automatycznie)?

Jakie błędy są wykrywane? Jak chronione są rośniki, z których wpisuje się dane? Czy są na nich poprawki? Autoryzowane?

Jak są oznakowane nośniki? Czy przed wprowadzeniem sprawdza się ich stan i zawartość? Co dzieje się potem z tymi nośnikami?

MANAGING RISK

Wszystko na podstawie analizy ryzyka.

A.10 Rozwój i utrzymanie systemu

A.10.2 Bezpieczeństwo systemów aplikacji

- Uwierzytelnianie wiadomości (A.10.2.3)

Gdy wobec przesyłanych wiadomości istnieje wymaganie zachowania integralności, należy stosować ich uwierzytelnianie,

Uwierzytelnienie jest potwierdzeniem nadawcy, że przesłana wiadomość pochodzi na pewno od niego i że nie została ona zmieniona podczas transmisji,

Wytyczne – ISO/IEC 17799

Czy uwierzytelnianie wiadomości ma zastosowanie? W jakich wypadkach? Co wynika z analizy ryzyka?

W jaki sposób nadawca wiadomości się uwierzytelnia?

Wymiana dokumentów, wiadomości w transakcjach handlowych? Polecenia przelewów, zapłaty, etc.?

Technologia w tym zakresie rozwija się bardzo szybko.

MANAGING RISK

Podobnie jak dane wejściowe i samo przetwarzanie informacji, tak i dane wyjściowe z aplikacji winny być potwierdzane co do poprawności, dokładności i kompletności,

Wytyczne do potwierdzania – ISO/IEC 17799

Jakie stosuje się procedury potwierdzania prawidłowości danych wychodzących po przetworzeniu przez aplikację?

Czy jest możliwe przeprowadzenie testu potwierdzającego? Czy pracownicy wiedzą jak to robić?

Czy istnieje możliwość dokonywania zmian w wynikach testów?

MANAGING RISK

A.10 Rozwój i utrzymanie systemu

A.10.3 Zabezpieczenia kryptograficzne

- Polityka używania zabezpieczeń kryptograficznych (A.10.3.1)

Należy stworzyć politykę używania zabezpieczeń kryptograficznych, w której zalecana stosowania tych metod są zidentyfikowane, uzgodnione i stosowane w całej organizacji,

Należy przeprowadzić analizę ryzyka, by dobrać najwłaściwsze zasady i techniki, stosowne do wymagań bezpieczeństwa i do potrzeb biznesowych organizacji,

Zarządzanie kluczami (patrz A.10.3.5)

W jaki sposób polityka używania zabezpieczeń kryptograficznych realizowana jest w codziennej praktyce?

Jak rozdzielono odpowiedzialności i zadania w stosowaniu tych zabezpieczeń?

W jaki sposób przygotowano pracowników do posługiwania się tymi narzędziami? Świadomość? Stosowanie się do polityki?

Skuteczność zastosowanych metod (długość klucza, algorytm)?

A.10 Rozwój i utrzymanie systemu

A.10.3 Zabezpieczenia kryptograficzne

- Szyfrowanie (A.10.3.2), podpisy cyfrowe (A.10.3.3), usługi niezaprzeczalności (A.10.3.4)

Do ochrony informacji wrażliwych lub krytycznych należy zastosować szyfrowanie (np. wobec transakcji przesyłanych publicznymi sieciami, wobec wrażliwych informacji przechowywanych w komputerach przenośnych),

Do ochrony autentyczności i integralności informacji (np. handel, płatności, podpisywanie kontraktów) należy stosować podpisy elektroniczne,

Dla rozstrzygania sporów dotyczących wystąpienia lub nie wystąpienia jakiegoś zdarzenia lub działania należy stosować usługi niezaprzeczalności

W jakich sytuacjach używa się szyfrowania, podpisów elektronicznych, usług niezaprzeczalności? Czy jest to spójne z polityką bezpieczeństwa? Z wymaganiami biznesowymi?

Czy przy wyborze rodzaju zabezpieczenia kierowano się analizą ryzyka?

Czy zidentyfikowano wymagania prawne dotyczące szyfrowania? Czy są przestrzegane?

Jaka jest znajomość polityk wśród pracowników? Praktyka?

A.10 Rozwój i utrzymanie systemu

A.10.3 Zabezpieczenia kryptograficzne

- Zarządzanie kluczami (A.10.3.5)

Dla umożliwienia właściwego stosowania technik kryptograficznych, zgodnego z politykami w tym zakresie, należy wprowadzić system zarządzania kluczami,

Zarządzania kluczami zależne od przyjętej techniki kryptograficznej, typu klucza (publiczny czy tajny),

Do ochrony urządzeń używanych do generowania, przechowywania i archiwizowania klucy zaleca się stosowanie ochrony fizycznej,

Jako wytyczne – zestaw standardów i procedur w ISO/IEC 17799

Czy klucze tajne i prywatne są w należyty sposób chronione?

Jakie zabezpieczenia stosuje się w dostępie do kluczy? Czy jest to ochrona zarówno logiczna jak i fizyczna?

Czy wprowadzono inne procedury zarządzania kluczami, np. te wymienione w ISO/IEC 17799 (aktywowanie klucza, unieważnianie, certyfikacja klucza, etc.)?

Jak postępuje się w przypadku naruszenia bezpieczeństwa klucza?

Odtwarzanie klucza?

A.10 Rozwój i utrzymanie systemu

A.10.4 Bezpieczeństwo plików systemowych

- Kontrola eksploatowanego oprogramowania (A.10.4.1)

Należy zapewnić kontrolę wprowadzania oprogramowania do eksploatowanych systemów,

Wszystkie zmiany oprogramowania (nowsze wersje) powinny być kontrolowane i zatwierdzane przed wprowadzeniem,

Zaleca się zachowywać kopie zapasowe poprzednich konfiguracji,

Konieczne jest posiadanie ważnych licencji na stosowanie danego oprogramowania

W jaki sposób wprowadzane jest nowe oprogramowanie (nowe wersje) do zasobów systemowych? Czy przechowuje się wersje źródłowe?

Jakie zapisy zmian są utrzymywane?

W jaki sposób chroni się inne zasoby (pliki, biblioteki)?

Czy programiści i administratorzy są świadomi zagrożeń związanych z wprowadzeniem niesprawdzonego oprogramowania do systemu?

Jakie sprawdzenia, testy są stosowane?

Kopie zapasowe?

A.10 Rozwój i utrzymanie systemu

A.10.4 Bezpieczeństwo plików systemowych

- Ochrona systemowych danych testowych (A.10.4.2)

Należy chronić i kontrolować systemowe dane testowe,

Zaleca się by unikać stosowania jako dane testowe informacji zawierających dane rzeczywiste, dane osobowe,

Gdy dane rzeczywiste kopiowane są do zbiorów danych testowych należy uzyskać pozwolenie, po zakończeniu testowania wykasować je z testowych systemów aplikacji i utrzymywać zapisy tych działań,

Dostęp do systemów testowych powinien być chroniony tak dobrze, jak dostęp do systemów operacyjnych

W jaki sposób tworzone są dane testowe? Jak są przechowywane i chronione? Jakie są możliwości ich modyfikacji?

Czy są to dane fikcyjne, czy też do ich stworzenia wykorzystuje się dane rzeczywiste? Na ile wrażliwe informacje wchodzą w ich skład? Czy dane rzeczywiste są modyfikowane tak, by nie można ich było powiązać z rzeczywistymi informacjami, osobami, etc.?

Jak przechowuje się wyniki testowania?

Czy testowanie wprowadza do żywych baz danych jakieś informacje? Jak są usuwane?

A.10 Rozwój i utrzymanie systemu

A.10.4 Bezpieczeństwo plików systemowych

- Kontrola dostępu do bibliotek programów źródłowych (A.10.4.3)

Należy zapewnić ścisłą kontrolę dostępu do bibliotek programów źródłowych,

Biblioteki te są repozytorium systemów operacyjnych i szczegółowym opisem ich zabezpieczeń,

Wszelkie pobrania i wprowadzenia programów źródłowych winny być zatwierdzane i ściśle kontrolowane, a zapisy utrzymywane,

Jako wytyczne – zestaw zaleceń w ISO/IEC 17799

Gdzie przechowywane są biblioteki programów źródłowych? Czy jest możliwość ich penetracji z systemów eksploatowanych?

Jakie wprowadzono zasady dostępu do bibliotek? Czy stosuje się jakieś metody weryfikacji kodów (np. sumy kontrolne)?

Czy przechowuje się wydruki kodów?

Czy prowadzi się dziennik zdarzeń i rejestruje każdy dostęp?

Czy przechowuje się archiwalne wersje programów źródłowych?

A.10 Rozwój i utrzymanie systemu

A.10.5 Bezpieczeństwo w procesach rozwojowych i obsługi informatycznej

- Procedury kontroli zmian (A.10.5.1)

Wdrażanie zmian winno być ściśle kontrolowane i przebiegać według ustalonych, formalnych procedur zmian,

Na każdym etapie rozwoju zmiany powinny być wprowadzane w sposób skoordynowany od strony technicznej i biznesowej,

Zmiany powinny być planowane, podlegać zaplanowanym przeglądom, weryfikacjom i testom,

Jako wytyczne – zestaw standardów i procedur w ISO/IEC 17799

Czy istnieją formalne procedury wprowadzania zmian? Do jakich rodzajów zmian się odnoszą? Czy mają charakter procedur standardowych czy raczej planów jakości?

W jaki sposób zarządza się zmianami w systemach on-line? Czy są plany na wypadek niepowodzenia?

Czy wszystkie zmiany są przeglądane i zatwierdzane przez właściwe do tego osoby?

W jaki sposób testuje się wprowadzane zmiany?

MANAGING RISK

Przerwa się i wejdzie w 2005 roku
KO 20743

A.10 Rozwój i utrzymanie systemu

A.10.5 Bezpieczeństwo w procesach rozwojowych i obsługi informatycznej

- Techniczny przegląd zmian w systemie operacyjnym (A.10.5.2)

Po przeprowadzeniu zmian w systemach operacyjnych i aplikacyjnych należy poddawać je przeglądowi i testowaniu,

Należy ocenić wpływ zmian na zabezpieczenia aplikacji i na bezpieczeństwo w ogóle,

Organizacja powinna ustanowić i wdrożyć procedury dokonywania przeglądów zmian,

Jakie są procedury przeglądu i testowania zmian? *Kiedy są stosowane? Jakie są dane wejściowe i wyjściowe w przeglądzie?*

Jak ocenia się wyniki testowania? Jak ocenia się wpływ zmian na bezpieczeństwo?

Czy stosuje się jednoznaczną identyfikację wersji?

W jaki sposób powiadamia się o zmianach?

Czy wyniki przeglądu i testowania znajdują odzwierciedlenie w planach ciągłości biznesu?

MANAGING RISK

A.10 Rozwój i utrzymanie systemu

A.10.5 Bezpieczeństwo w procesach rozwojowych i obsługi informatycznej

- Ograniczenia dotyczące zmian w pakietach oprogramowania (A.10.5.3)

Należy unikać dokonywania zmian w pakietach oprogramowania; zaleca się używanie pakietów dostarczanych przez dostawcę, nie modyfikując ich,

Jeśli zmiany w pakietach są konieczne, należy ustanowić dodatkowe zabezpieczenia (analiza ryzyka),

Wskazane jest uzgadnianie z dostawcą dostarczenia nowej wersji całego pakietu – standardowa aktualizacja programu,

Jakie są procedury wprowadzania zmian? *Kiedy są stosowane? Jakie uzasadnienie do zmian są akceptowane?*

Jak organizacja ocenia wpływ zmian na funkcjonowanie i bezpieczeństwo oprogramowania? Czy potrafi jednoznacznie zidentyfikować i ocenić ryzyko?

Czy zmiany są jednoznacznie odzwierciedlane w dokumentacji oprogramowania?

Czy zmiany prowadzi się za wiedzą i w porozumieniu z dostawcą?

MANAGING RISK

A.10 Rozwój i utrzymanie systemu

A.10.5 Bezpieczeństwo w procesach rozwojowych i obsługi informatycznej

- Ukryte kanały i konie trojańskie (A.10.5.4)

Przy zakupie, modyfikowaniu i używaniu oprogramowania należy dokonywać sprawdzeń pod kątem występowania ukrytych kanałów i koni trojańskich,

Wskazane jest zakupywanie oprogramowania tylko z wiarygodnych źródeł, zakup programów w wersji źródłowej, używanie wcześniej sprawdzonych produktów,

Wskazane jest dobranie wysoko kwalifikowanego i zaufanego personelu do pracy w kluczowych systemach

Czy organizacja jest świadoma jakie ukryte kody występują w eksploatowanym oprogramowaniu? Czy potrafi określić ich przeznaczenie i szkodliwość?

W jaki sposób dobiera się dostawców oprogramowania? Jak sprawdza się zakupywane oprogramowanie?

Jak organizacja jest przygotowana do działania w przypadku wykrycia ukrytego kodu?

Czy posiada odpowiednio wykwalifikowany i świadomy personel?

A.10 Rozwój i utrzymanie systemu

A.10.5 Bezpieczeństwo w procesach rozwojowych i obsługi informatycznej

- Prace rozwojowe nad oprogramowaniem powierzane na zewnątrz (A.10.5.5)

Zlecanie prac rozwojowych nad oprogramowaniem firmie zewnętrznej wymaga stosowania zabezpieczeń,

Należy rozważyć wprowadzenie uzgodnień kontraktowych dot. licencji, własności kodu, certyfikacji jakości i dokładności, prawa audytu kodu, testowania przed instalacją, zaszczepienia powierniczwa kodu na wypadek niewypełnienia zobowiązań

Jak organizacja ocenia ryzyko związane ze zleceniem prac rozwojowych na zewnątrz?

W jakim środowisku i w jak zorganizowanych procesach toczyć się będą prace rozwojowe?

Jakie zabezpieczenia wprowadzono do kontraktu? Jak organizacja będzie egzekwować jakość, dokładność i terminowość?

Jak organizacja zabezpiecza się przed ukrytymi kanałami i innymi ryzykami utraty bezpieczeństwa?

A.11 Zarządzanie ciągłością działania

A.11.1 Aspekty zarządzania ciągłością działania

- Proces zarządzania ciągłością działania (A.11.1.1), ciągłość działania i analiza skutków dla działalności biznesowej (A.11.1.2)

Dla przeciwdziałania przerwom w działalności biznesowej i dla ochrony przed skutkami rozległych awarii lub katastrof należy wdrożyć w całej organizacji proces zarządzania ciągłością działania,

Podstawa: analiza ryzyka,

Należy przygotować plan (plany) zachowania ciągłości działania (lub odtworzenia) biznesu w warunkach zdarzeń losowych lub awarii, nie tylko w sferze IT,

Ważnym elementem planów ciągłości działania jest aspekt kosztów utrzymania (odtworzenia) działalności i kosztów ciężkiej czasowej „niedostępności" w biznesie

Jakie zdarzenia mogą zagrozić ciągłości firmy? Jakie mogą być ich konsekwencje dla biznesu?

Jak przebiega proces zarządzania ciągłością działania? Czy jest obecny w całej organizacji?

Czy tworzone są plany, warianty postępowania, czy są na bieżąco analizowane i uaktualniane?

Czy plany odnoszą się do wszystkich aspektów prowadzonej działalności, do wszystkich zasobów, nie tylko informatycznych lub informacyjnych?

A.11 Zarządzanie ciągłością działania

A.11.1 Aspekty zarządzania ciągłością działania

- Tworzenie i wdrażanie planów ciągłości działania (A.11.1.3)

Plany powinny zawierać szczegółowe opisy działań podejmowanych w następstwie awarii, katastrof lub innych przeszkód w prowadzeniu działalności wraz z przydziałem odpowiedzialności za te działania.

Plany należy uzgodnić w całej organizacji, wcześniej system szkoleń i budowania świadomości wśród personelu.

Konieczne jest regularne testowanie planów i ich uaktualnianie dla podniesienia ich skuteczności.

Czy ramy czasowe oraz przypisane zasoby są adekwatne do wymagań biznesowych? Czy są realistyczne?

Czy przypisanie odpowiedzialności jest jednoznaczne i nie pozostawia luk? Czy pracownicy są świadomi swoich zadań i odpowiedzialności?

Czy procedury postępowania zostały udokumentowane i są dostępne tam gdzie to potrzebne?

Czy przeprowadza się testowanie – ćwiczenia, próby? Czy wyniki są analizowane a plany uaktualniane?

A.11 Zarządzanie ciągłością działania

A.11.1 Aspekty zarządzania ciągłością działania

- Struktura planowania ciągłości działania (A.11.1.4)

Aby upewnić się, że wszystkie plany ciągłości działania są ze sobą zgodne oraz by zidentyfikować priorytety podczas testowania i utrzymania, należy zachować jednolitą strukturę tych planów.

Jednolita struktura to koordynacja planów, ustalenie priorytetów, organizacja ćwiczeń i skoordynowany rozwój i utrzymanie.

Konieczne jest regularne testowanie planów i ich uaktualnianie dla podniesienia ich skuteczności.

Czy poszczególne plany ciągłości działania, przygotowane dla poszczególnych oddziałów, obszarów, procesów etc. są spójne ze sobą?

Jakie typowe scenariusze uwzględniają te plany (atak wirusowy, hakerski, przerwa w zasilaniu, pożar, powódź, katastrofa ekologiczna, utrata kluczowego personelu, etc.)?

Czy określono priorytety działań?

Czy we wszystkich obszarach objętych planami są dostępne odpowiednie zasoby (instrukcje, wyposażenie, informacje, wyszkoleni ludzie)?

BCP BCP

A.11 Zarządzanie ciągłością działania

A.11.1 Aspekty zarządzania ciągłością działania

- Testowanie, utrzymywanie i ponowna ocena planów ciągłości działania (A.11.1.5)

Plany ciągłości działania winny być regularnie testowane, tak by zapewnić ich aktualność i skuteczność.

Dynamika zmian zachodzących we współczesnych organizacjach powoduje, że plany szybko się dezaktualizują, stają się niedokładne lub wręcz niebezpieczne.

Należy sporządzić plan aktualizowania planów ciągłości działania i utrzymywać dowody ich regularnych przeglądów.

Czy ustanowiono harmonogramy testowania planów ciągłości? Czy są realizowane?

Czy obrazowano kompleksowy plan wdrażania, utrzymania i rozwijania (aktualizacji) planów ciągłości?

Jak wypadają wyniki testów? Czy spełniają przyjęte założenia? Czy z kolejnych testów wynika poprawa sprawności w przeprowadzaniu działań?

Czy nowi pracownicy (lub ci przeniesieni na inne stanowiska) są przygotowywani do sprawnego realizowania zadań?

Zmiany w przepisach prawnych?

Robić tylko scenariusz działanie (inne mogą) bo później będzie się tylko modyfikować

A.12 Zgodność

A.12.1 Zgodność z przepisami prawa

- Określenie odpowiednich przepisów prawnych (A.12.1.1)

Aby uniknąć naruszeń prawa karnego i cywilnego, dla każdego systemu informacyjnego należy wyraźnie określić i udokumentować wszelkie wymagania wynikające z ustaw, zarządzeń (rozporządzeń) i umów,

Obejmuje to nie tylko identyfikację wymagań w kraju organizacji, ale również wymagań obowiązujących w krajach, w których organizacja prowadzi biznes,

Wskazane jest zasięgnięcie wsparcia eksperckiego - prawnicy,

Jakie działania są prowadzone w celu identyfikowania (i uaktualniania) obowiązujących przepisów prawa?

Czy organizacja ustanowiła i wdrożyła zabezpieczenia wymuszające respektowanie zidentyfikowanych wymagań?

Kto odpowiada za otrzymanie i przestrzeganie tych zabezpieczeń? Czy te osoby są świadome swojej odpowiedzialności?

A.12 Zgodność

A.12.1 Zgodność z przepisami prawa

- Prawo do własności intelektualnej (A.12.1.2)

Zaleca się wprowadzenie odpowiednich procedur, tak aby zapewnić zgodność z odpowiednimi uregulowaniami prawnymi dotyczącymi respektowania własności intelektualnej oraz użytkowaniem oprogramowania będącego przedmiotem praw własności,

Przynajmniej raz w roku należy przeprowadzać inwentaryzację dla uzyskania potwierdzenia, że obsługa użytkowanego oprogramowania jest objęta ważnymi licencjami (z uwzględnieniem liczby stanowisk, na jakie opiewają licencje),

Jakie przedmioty objęte prawami własności intelektualnej są użytkowane przez organizację? Jakie rodzaje praw mają zastosowanie? Jakiego rodzaju odpowiedzialność prawna wiąże się z tymi prawami?

Jakie procedury organizacja ustanowiła i stosuje dla respektowania praw do własności intelektualnej? Świadomość personelu?

Jak zarządza się licencjami oprogramowania?

W jaki sposób uregulowano kwestie modyfikacji?

A.12 Zgodność

A.12.1 Zgodność z przepisami prawa

- Zabezpieczanie dokumentów organizacji (A.12.1.3)

Ważne dokumenty organizacji należy chronić przed utratą, zniszczeniem lub sfałszowaniem.

Należy utrzymywać wykaz (rejestr) ważnych dokumentów: aktów własności różnych aktywów, praw do nich, dokumentów finansowych wymaganych przez prawo etc..

Przynajmniej raz w roku należy przeprowadzać inwentaryzację i odnotowywać jej wyniki

Czy organizacja jest świadoma, jakie dokumenty i jak długo należy przechowywać? Jakie są wymagania prawne własnego kraju i krajów, w których prowadzi się biznes?

Jak przechowuje się dokumenty? Czy sposób przechowywania spełnia wymogi prawne? Jak są chronione przed utratą, zniszczeniem? Kto ma do nich dostęp?

Czy przechowywane dokumenty są zinwentaryzowane? Czy sprawdza się ich zawartość? Jak często?

A.12 Zgodność

A.12.1 Zgodność z przepisami prawa

- Ochrona danych osobowych i prywatność informacji dotyczących osób fizycznych (A.12.1.4)

Należy chronić dane osobowe zgodnie z przepisami obowiązującego prawa.

Zaleca się opracowanie wytycznych dla personelu posługującego się danymi osobowymi, dotyczących indywidualnych zakresów odpowiedzialności oraz określonych procedur, które powinny być stosowane,

Przepisy prawa (np. Ustawa o ochronie danych osobowych) wymagają powoływania administratorów danych

Jakie dane osobowe są przechowywane? Czy wszystkie przechowywane dane są organizacji potrzebne?

Jak chroni się dane osobowe? Czy ustanowiono dla nich administratora?

Czy przechowywane dane są rejestrowane? Czy sprawdza się je i aktualizuje zawartość? Jak często?

Kto ma dostęp do danych osobowych i w jakim zakresie? Jaki użytek jest robiony z tych danych?

Postępowanie w razie naruszenia?

MANAGING RISK

A.12 Zgodność

A.12.1 Zgodność z przepisami prawa

- Zapobieganie nadużywaniu urządzeń przetwarzających informacje (A.12.1.5)

Używanie urządzeń przetwarzających dane powinno być autoryzowane przez kierownictwo, należy wprowadzić zabezpieczenia przed nieuprawnionym używaniem tych urządzeń,

Nieuprawnione użycie (przez nieuprawnione osoby lub w nieuprawniony sposób) powinno podlegać sankcjom dyscyplinarnym (A.6.3.5),

W niektórych przypadkach nieuprawnionego użycia można z mocy prawa mieć do czynienia z odpowiedzialnością karną

Czy kierownictwo zdefiniowało jasną politykę, z której jednoznacznie wynika jakie działanie są nadużyciem?

Czy pracownicy znają tę politykę? Czy formalnie potwierdzili zapoznanie się z nią?

Jak postępuje się w przypadku wykrycia przypadków celowych nadużyć?

Jeśli pracownikom wolno korzystać z Internetu, gier, instalować programy, etc., to czy na tych samych urządzeniach, na których przechowuje się ważne informacje?

MANAGING RISK

A.12 Zgodność

A.12.1 Zgodność z przepisami prawa

- Regulacje dotyczące zabezpieczeń kryptograficznych (A.12.1.6)

Dostęp do środków kryptograficznych (szyfrowanie, podpisy elektroniczne) i ich używanie powinny przebiegać w zgodności z regulacjami prawnymi w tym zakresie, regulacjami wewnętrznymi i umowami,

Należy uwzględniać zgodność z regulacjami prawnymi w kraju organizacji, w krajach gdzie prowadzi się biznes, a nawet w krajach, przez które informacja podróżuje

Jakie działania podjęto dla zidentyfikowania mających zastosowanie regulacji? Czy korzystano z porad prawnych w tym zakresie?

Jakie wprowadzono zabezpieczenia, działania? Czy są one udokumentowane?

Czy rzeczywiste praktyki stosowania narzędzi kryptograficznych są zgodne z wymaganiami (patrz też A.10.3)?

MANAGING RISK

A.12 Zgodność

A.12.1 Zgodność z przepisami prawa

- Gromadzenie materiału dowodowego (A.12.1.7)

Tam gdzie postępowanie jest związane z naruszeniem przepisów prawa, zarówno cywilnego jak i karnego, przedstawiany materiał dowodowy powinien odpowiadać zasadom gromadzenia materiałów dowodowych przyjętym w danej dziedzinie prawa lub zasadom przyjętym w określonym sądzie, w którym przypadek będzie rozpatrzony. Obejmuje to zgodność z daną opublikowaną normą lub praktycznymi zasadami dotyczącymi tworzenia materiału dowodowego,

Nigdy nie wiadomo, czy dany przypadek nie skończy się w sądzie...

W jaki sposób gromadzi się materiał dowodowy? Czy są na to jakieś procedury? Jakie standardy i kodeksy postępowania stosują?

Jak zapewnia się jakość i kompletność zebranego materiału? Jak można ją udowodnić?

W jaki sposób chroni się zebrany materiał dowodowy? Komu i w jakich okolicznościach może być udostępniany?

Audytor nie może zbierać dowodów. Należy to do pracowników ale służby odpowiedzialne. Mówi to czy to są dowody.

A.12 Zgodność

A.12.2 Przeglądy polityki bezpieczeństwa i zgodności technicznej

- Zgodność z polityką bezpieczeństwa (A.12.2.1)

Kierownictwo powinno przedsięwziąć kroki, aby zapewnić, że wszystkie procedury związane z bezpieczeństwem mieszczące się w zakresie ich odpowiedzialności są wykonywane poprawnie i wszystkie obszary w obrębie instytucji podlegają regularnym przeglądom w celu zapewnienia zgodności z zasadami i normami bezpieczeństwa.

Takie przeglądy winny się odbywać przynajmniej raz w roku (o ile z analizy ryzyka nie wynika ze częściej),

Należy utrzymywać zapisy z takich przeglądów, odnotowywać niezgodności, uzgodnione działania i oceniać ich skuteczność

Czy odbywają się regularne wewnętrzne audyty zgodności, a wyniki tych audytów poddaje się przeglądom? Czy personel audytujący posiada odpowiednie kwalifikacje?

Czy przy planowaniu częstotliwości i zakresu przeglądów i audytów bierze się pod uwagę poziom wymagań bezpieczeństwa wynikający z analizy ryzyka? Zmiany w organizacji? Zmiany w technologii?

Czy można polityki [illegible] zgodne z prawem
np. kontrola dostępu do [illegible]

A.12 Zgodność

A.12.2 Przeglądy polityki bezpieczeństwa i zgodności technicznej

- Sprawdzanie zgodności technicznej (A.12.2.2)

Systemy informacyjne powinny być regularnie sprawdzane pod kątem zgodności ze standardami wdrażania zabezpieczeń.

Nie wystarczy świadomość, że wszystkie potrzebne zabezpieczenia zostały wdrożone, konieczne są regularne ich przeglądy techniczne, w odstępach wynikających z analizy ryzyka,

Przeglądy powinny być przeprowadzane przez wykwalifikowany i doświadczony personel

Czy istnieje plan sprawdzeń zgodności technicznej? Czy określa co i jak ma podlegać sprawdzeniom? Jak często? Kto ponosi odpowiedzialność?

Kto dokonuje sprawdzeń? Jakie narzędzia znajdują zastosowanie? W jaki sposób sprawdza się narzędzia?

W jaki sposób przedstawia się wyniki sprawdzeń? Jakie działania są podejmowane jeśli wynik sprawdzenia jest niepomyślny?

A.12 Zgodność

A.12.3 Rozważania dotyczące audytu systemu

- Zabezpieczenia audytu systemu (A.12.3.1)

W celu minimalizowania ryzyka zakłóceń procesów biznesowych, należy starannie planować i uzgadniać działania i potrzeby związane z audytem, wymagające sprawdzania systemów operacyjnych.

Plany audytów powinny być uzgadniane, dokumentowane i zatwierdzane

W jaki sposób planuje się audyty systemu? Jak są one zatwierdzane?

W jaki sposób audyt może zakłócić działanie systemów operacyjnych? Czy przeprowadzenie audytu może doprowadzić do niezamierzonej zmiany chronionych danych?

Czy narzędzia do prowadzenia audytu podlegały wcześniejszej walidacji?

Czy działania związane z prowadzeniem audytu są rejestrowane tak jak wszystkie inne działania w systemach operacyjnych?

A.12 Zgodność

A.12.3 Rozważania dotyczące audytu systemu

- Ochrona narzędzi audytu systemu (A.12.3.1)

Aby zapobiec możliwym nadużyciom lub naruszeniu bezpieczeństwa, należy chronić dostęp do narzędzi audytu systemu, np. oprogramowania lub plików danych.

Każde użycie narzędzi audytu winno być rejestrowane i - jeśli zachodzi taka potrzeba - zatwierdzane przez kierownictwo odpowiedniego szczebla

W jaki sposób przechowuje się narzędzia audytu? Czy są przechowywane oddzielnie od systemów operacyjnych i testowych? Jeśli nie, to jakie zabezpieczenia przed niepowołanym dostępem zostały wprowadzone?

Jak chroni się podręczniki użytkownika dla narzędzi audytu? Kto ma do nich dostęp?

Czy narzędzia do prowadzenia audytu podlegają okresowym sprawdzeniom? Jakie są wyniki? Zapisy?

PRZYGOTOWANIE DO AUDYTU

Zalety dokumentacji ISMS

- pozytywna komunikacja,
- poprawa nadzoru nad czynnościami,
- zapewnienie ciągłości w zmieniających się okolicznościach,
- konsekwentne szkolenie personelu,
- dostarcza metody prezentacji,
- stanowi podstawę audytów.

Dokumentacja ISMS

- Udokumentowane deklaracje polityk bezpieczeństwa oraz celów zabezpieczania,
- Zakres ISMS oraz procedury i zabezpieczenia służące realizacji ISMS,
- Raport z procesu szacowania ryzyka,
- Plan postępowania z ryzykiem,
- Udokumentowane procedury potrzebne organizacji do zapewnienia skutecznego planowania, utrzymywania i sterowania jej procesami bezpieczeństwa informacji,
- Zapisy wymagane przez normę,
- Deklaracja stosowania.

Ocena dokumentacji

- zakres ISMS,
- stopień zgodności dokumentacji z wymaganiami,
- *zakres dokumentacji ISMS,*
- udokumentowane procedury,
- zapoznanie się ze sposobami dokumentowania ISMS,
- metoda szacowania ryzyk i wyniki
- wyłączenia opisane w Deklaracji Stosowania.

Plan audytu

- zakres audytu i kryteria
- tożsamość członków zespołu audytorów
- termin audytu
- spotkanie otwierające
- kolejność zdarzeń
- narady
- opracowanie raportu
- spotkanie zamykające

Żeby jednoznacznie wiedzieć co, gdzie, kiedy audytujemy.

Celu nie musi tylko jeden audytor badać, bywa

Dietanie kategorie i wagowanie

mają różne dziedziny.

Listy pytań kontrolnych

- jest przewodnikiem audytora
- zapewnia dokładność badania
- ułatwia kontrolowanie czasu
- ułatwia opracowanie raportu
- kierunkuje reakcje audytowanego
- dostarcza obiektywnych dowodów
- ułatwia zachowanie spójności i konsekwencji

Są różne opis można przygotować sobie samemu dostosować do danego zadania

Może zadać to samo pytanie w kilku dziedzinach i sprawdzić powiązania

Czasem listy te są przekazywane audytowanemu do zapoznania się

Listy pytań kontrolnych

Pytania powinny być:

- jasne
- precyzyjne
- pozbawione sugestii
- otwarte

Muszą mieć opis procesu a nie zdarzenia

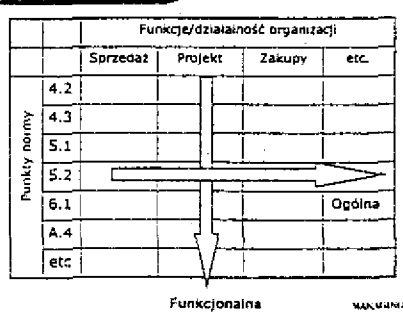
Pytanie sugerujące czy wartość jest dobra czy zła.

Listy pytań kontrolnych

Listy ogólne
Ogólna lista pytań kontrolnych koncentruje się na wymaganiach pojedynczego punktu normy

Listy funkcjonalne
Lista funkcjonalna koncentruje się dziale / funkcji / procesie w organizacji i odwołuje się do wymagań różnych, mających zastosowanie, punktów normy

Listy pytań kontrolnych



Zwykle pokaz z reklamy: 3-krokowej badanie check list

Listy pytań kontrolnych

Wskazane jest posługiwanie się metodą „trzech kroków":

Krok pierwszy
pytania zmierzające do ustalenia jak skuteczny jest proces:
- jaki jest cel procesu – co ma on osiągnąć?
- w jaki sposób proces oddziaływuje z innymi procesami?
- jakie kluczowe kroki są wykonywane w procesie?
- jakie są wejścia / wyjścia?
- w jaki sposób proces jest mierzony / monitorowany?
- jakie są cele dla doskonalenia procesu?

Listy pytań kontrolnych

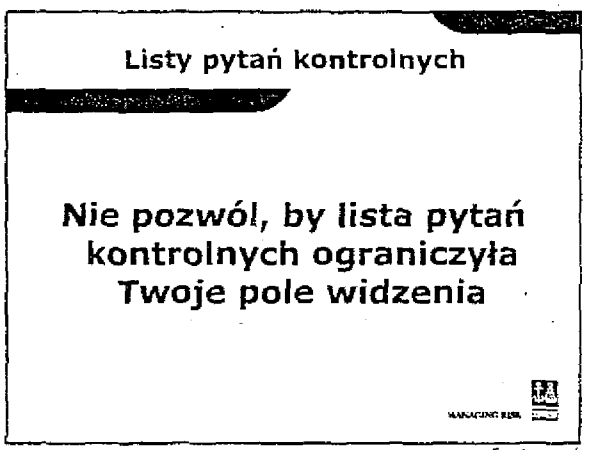
Krok drugi
Wymagania stawiane przez normę:
- wymagania poszczególnych punktów normy mających zastosowanie do procesu poddawanego audytowi,
- wymagania normy, które mają zastosowanie do wszystkich procesów

Krok trzeci
Pytania wynikające z innych przesłanek:
- z przeglądu dokumentów odnoszących się do danej funkcji / działalności (np. procedur),
- z uregulowań prawnych,
- z wymagań klienta.

Ngtawczy, że klient nie swoje oczekiwania dokumentach i musimy dostosować procedury

Przykład formularza listy pytań kontrolnych

DZIAŁ:	REFERENCJE:	LISTA Nr:	WERSJA / STRONA
Lp.	WYMAGANIE	Referencje	Zgodność (T/N)	Obserwacje
	Pytanie	Wolne przyp		



Audyt wewn. – może być – [illegible] – zdany ewidencji

- Nepiew to nadaje zdać
- Polityka bezpieczeństwa
- Struktura

= inspiracja
= zalecenia
– nagrobienie

Bezpieczeństwo:
fizyczne
osobowe
informacji
ciągłości działania

Dyrektywa zadań
– Normalne
– Fast Track

6 sprawdzeń
jest
znane
stosowane
wdrożone
udokumentowane
czy są znane wyniki

SZACOWANIE RYZYK

Szacowanie ryzyk

Organizacja powinna szacować ryzyka związane z możliwością utraty atrybutów bezpieczeństwa, uwzględniając wartość informacji funkcjonujących w obrębie systemów informacyjnych będących w zakresie ISMS.

Ogólnie, metody szacowania ryzyka mogą być stosowane do kompletnych lub pojedynczych systemów informacyjnych, komponentów systemu informacyjnego, urządzeń lub usług jeśli jest to praktyczne i użyteczne.

Szacowanie ryzyka bierze się z samej normy

ISO Guide - Stanisław

Szacowanie ryzyk

Szacowanie ryzyk wymaga systematycznego rozważania:

- **skutków** – szkód w organizacji które mogą powstać jako rezultat incydentu związanego z bezpieczeństwem informacji, biorąc pod uwagę potencjalne konsekwencje utraty lub naruszenia poufności, integralności i dostępności informacji
- **prawdopodobieństwa** – realnego prawdopodobieństwa utraty bezpieczeństwa informacji w świetle zagrożeń, podatności i zabezpieczeń

Zarządzanie ryzykiem – działania konieczne

- wybór metody szacowania ryzyk – najbardziej odpowiedniej dla ISMS organizacji,
- Identyfikacja wymagań prawnych, normatywnych i kontraktowych,
- określenie kryteriów akceptowalności ryzyk oraz identyfikacja akceptowalnych poziomów ryzyk,
- Identyfikacja i oszacowanie ryzyk,
- Identyfikacja i ocena opcji postępowania z ryzykiem,
- wybór celów zabezpieczania i zabezpieczeń w celu redukcji ryzyk do akceptowalnych poziomów,
- dla celów ~~certyfikacji~~ – ~~przygotowanie~~ Deklaracji Stosowania.

Szacowanie ryzyk

Proces szacowania ryzyk jest uzależniony bezpośrednio od:

- rodzaju prowadzonej działalności i Systemu zarządzania organizacji,
- rodzaju wykorzystywanych informacji dla celów biznesowych,
- otoczenia, w którym funkcjonuje ISMS,
- dostępnej ochrony dzięki zastosowanym zabezpieczeniom.

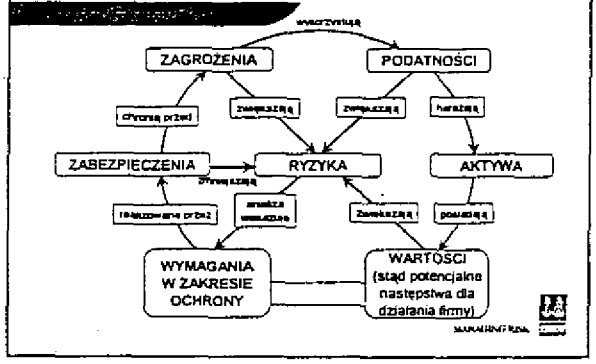
Bezpieczeństwo informacji - pojęcia

Aktywa [assets] – to wszystko co ma wartość dla organizacji
Następstwa [impacts] – rezultaty niepożądanego incydentu
Ryzyko szczątkowe [residual risk] – ryzyko, które pozostaje po zastosowaniu zabezpieczeń
Ryzyko [risk] – kombinacja prawdopodobieństwa i konsekwencji zdarzenia niepożądanego
Analiza ryzyka [risk analysis] – systematyczne wykorzystywanie informacji w celu identyfikacji zagrożeń oraz oceny ryzyk
Szacowanie ryzyka [risk assessment] – szacowanie zagrożeń i ich wpływu oraz podatności informacji i urządzeń do przetwarzania informacji oraz prawdopodobieństwa ich wystąpienia

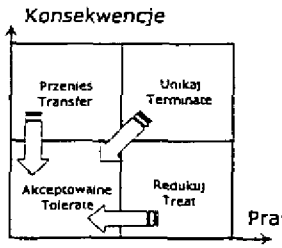
Bezpieczeństwo informacji - pojęcia

Postępowanie z ryzykiem [risk treatment] - proces wyboru i wdrażania zabezpieczeń w celu modyfikacji ryzyk
Zarządzanie ryzykiem [risk management] – skoordynowane działania mające na celu zarządzanie organizacją ze szczególnym uwzględnieniem ryzyk. Zazwyczaj obejmuje szacowanie ryzyk oraz postępowanie z ryzykiem.
Zagrożenie [threat] – potencjalna przyczyna niepożądanego incydentu, którego skutkiem może być szkoda dla systemu lub organizacji
Podatność [vulnerability] – słabość zasobu lub grupy zasobów, która może być wykorzystana przez zagrożenie

Bezpieczeństwo informacji - pojęcia

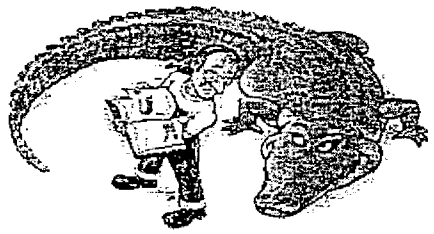


Opcje postępowania z ryzykiem



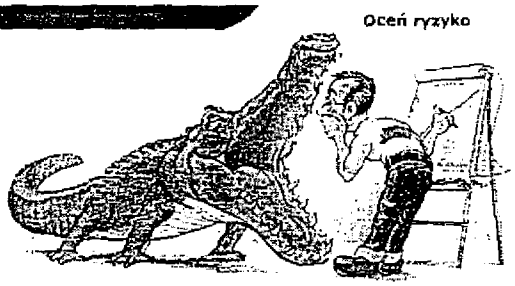
Opcje postępowania z ryzykiem

Zidentyfikuj zagrożenie



Opcje postępowania z ryzykiem

Oceń ryzyko

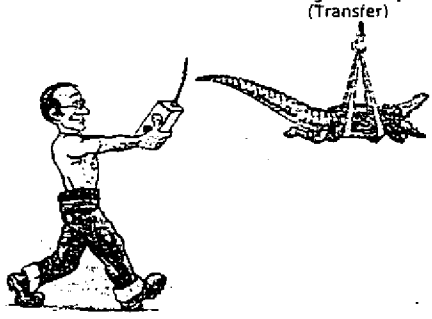


Opcje postępowania z ryzykiem

Wyeliminuj zagrożenie
(Terminate)

Opcje postępowania z ryzykiem

Przemieść zagrożenie poza Firmę
(Transfer)



Opcje postępowania z ryzykiem

Ogranicz prawdopodobieństwo wystąpienia zagrożenia
(Treat)

Opcje postępowania z ryzykiem

Zmniejsz skalę skutków
(Treat)

Opcje postępowania z ryzykiem

Toleruj zagrożenie (Tolerate)

Proces szacowania ryzyk - etapy

1. Identyfikacja aktywów,
2. Wycena aktywów,
3. Identyfikacja wymagań związanych z bezpieczeństwem informacji, t.j. zagrożeń, podatności, wymagań prawnych, kontraktowych i własnych,
4. Oszacowanie wagi wymagań związanych z bezpieczeństwem informacji,
5. Obliczenie ryzyk,
6. Identyfikacja i ocena opcji postępowania z ryzykiem,
7. Zastosowanie zabezpieczeń w celu redukcji ryzyk do poziomu akceptowalnego.

Proces szacowania ryzyk

1. Identyfikacja aktywów

- główna odpowiedzialność kadry zarządzającej wszystkich szczebli,
- przypisany właściciel i klasyfikacja.

Proces szacowania ryzyk

Przykłady aktywów:

- **Aktywa informacyjne** – bazy danych, pliki danych, dokumentacja systemu, podręczniki użytkowania, materiały szkoleniowe, procedury operacyjne i wspomagające, plany ciągłości, plany awaryjne
- **Dokumenty papierowe** – umowy, wytyczne, dokumentacja organizacji, raporty wynikowe
- **Oprogramowanie** – systemy operacyjne, aplikacje, narzędzia
- **Aktywa fizyczne** – sprzęt komputerowy i telekomunikacyjny, nieruchomości, nośniki danych
- **Ludzie** – personel, klienci, dostawcy
- **Usługi** – projektowania, przetwarzania, transmisji
- **Wizerunek firmy**

Materiał to zapis, ale zapisu nie można dotrzeć dotrzeć się ciągle z materiałem

Proces szacowania ryzyk

2. Wycena aktywów

- główna odpowiedzialność właścicieli aktywów,
- czynny udział właścicieli aktywów,
- uwzględniając ich wagę dla organizacji,
- powiązana z kosztem nabycia i utrzymania oraz wpływu utraty poufności, integralności lub dostępności dla organizacji,
- może mieć charakter ilościowy ($) lub jakościowy (wartość duża - mała),
- aktywa potężnej wartości dla jednej organizacji mogą mieć wartość pomijalną dla innej.

Nie można tak dać o ludzie ~~że~~ nie można od ~~ich~~ wymagać tych ~~rzeczy~~ rzeczy

kwantyfikatory: ilościowy, jakościowy

Proces szacowania ryzyk

3. Identyfikacja wymagań bezpieczeństwa informacji

Źródła wymagań:

- komplet zagrożeń i podatności mogących doprowadzić do znacznych strat organizacji w przypadku ich wystąpienia,
- ustawowe i kontraktowe,
- wymagania własne organizacji, polityki, zasady, cele i procedury

Proces szacowania ryzyk

4. Oszacowanie wagi wymagań bezpieczeństwa informacji

Metoda szacowania powinna być odpowiednia do metody szacowania ryzyka.
Aby nie komplikować procesu w wielu przypadkach wystarczy zastosować prostą trójstopniową skalę wagi wymagań:

- bardzo istotne
- istotne
- mało istotne

Proces szacowania ryzyk

Oszacowanie prawdopodobieństw wystąpienia zagrożeń i wykorzystania podatności

- *ocena prawdopodobieństwa wykorzystania podatności przez* zagrożenia,
- w zależności od metody ocena prawdopodobieństw *wystąpienia zagrożeń i wykorzystania podatności może być* dokonana łącznie lub rozdzielnie.

Proces szacowania ryzyk

Ocena prawdopodobieństwa wystąpienia zagrożeń

Zagrożenia permanentne:
- słaba motywacja,
- potencjał wymagany vs. rzeczywisty,
- zasoby narażone na potencjalny atak,
- postrzegana wartość aktywów

Zagrożenia incydentalne:
- jak często mogą wystąpić na podstawie doświadczenia, statystyki, etc.
- biorąc pod uwagę potencjalne błędy ludzkie i uszkodzenia sprzętu

Proces szacowania ryzyk

Prawdopodobieństwo incydentu jest funkcją podatności

Ocena prawdopodobieństwa wykorzystania podatności

- **bardzo prawdopodobne lub prawdopodobne** – podatności łatwe do wykorzystania z powodu braku lub zastosowania trywialnych zabezpieczeń,
- **możliwe** – podatność może być wykorzystana po obejściu zastosowanych zabezpieczeń
- **nieprawdopodobne lub niemożliwe** – zastosowano bardzo skuteczne zabezpieczenia

Proces szacowania ryzyk

Oszacowanie wag wymagań prawnych i kontraktowych

- Jak duży wpływ na organizację może mieć niespełnienie wymagań prawnych i kontraktowych?
- Jakie mogą być tego konsekwencje dla poszczególnych aktywów i całego ISMS?
- Jakie jest prawdopodobieństwo takiej sytuacji?

Proces szacowania ryzyk

5. Obliczenie ryzyk

Celem procesu szacowania ryzyk jest identyfikacja i ocena ryzyk na podstawie kroków 1 – 4

Kalkulacja ryzyk oparta jest o kombinację wartości aktywów i oszacowanych wag odpowiednich wymagań bezpieczeństwa informacji.

Jest wiele metod kalkulacji ryzyk opartych o zależność funkcyjną wartości zasobów, podatności, zagrożeń, wag wymagań prawnych i kontraktowych.

Najlepsze - tutaj podejście to Hiszpanii Margenit

Proces szacowania ryzyk

Metoda podstawowego poziomu bezpieczeństwa

Użycie tego samego sposobu podejścia do zabezpieczenia wszystkich aktywów, niezależnie od ryzyka jakie im zagraża używając prostej skali wartości aktywów i poziomu wymagań, np.

	Poziom wymagań	NISKI	WYSOKI
Wartość aktywów	NISKA	0	2
	ŚREDNIA	1	3
	WYSOKA	2	4

Proces szacowania ryzyk

Metoda podstawowego poziomu bezpieczeństwa

- \+ Minimalne zaangażowanie zasobów,
- \+ Metoda szybka i niskonakładowa,
- « Pozwala osiągnąć podstawowy poziom bezpieczeństwa,
- \- Jeśli poziom podstawowy zostanie określony zbyt wysoko, to istnieje ryzyko zastosowania nadmiaru zabezpieczeń,
- \- Jeśli poziom podstawowy zostanie określony zbyt nisko, to istnieje ryzyko słabego zabezpieczenia aktywów.

Formalne - są odpowiednie (podejście dlaczego to)

Nieformalne - [illegible]

Proces szacowania ryzyk

Podejście nieformalne

- Nie opiera się na metodach strukturalnych,
- Bazuje na wiedzy ekspertów,
- Koncentruje uwagę tylko na szczególnie wrażliwych elementach systemu

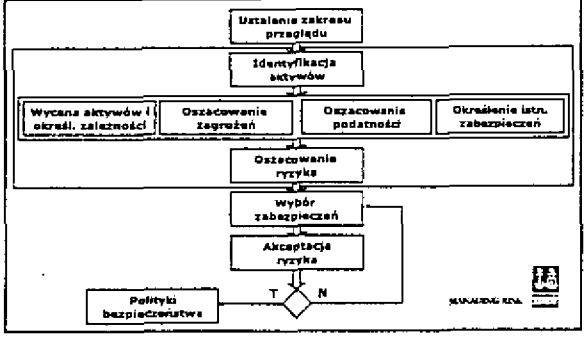
Proces szacowania ryzyk

Podejście nieformalne

+ Nie wymaga zbyt wielu zasobów i czasu,
- Duże prawdopodobieństwo pominięcia ważnych elementów systemu,
- Wymagany doświadczony personel,
- Subiektywizm oceny,
- Problem ponownej oceny, przy braku personelu, który poprzednio dokonywał oceny

Proces szacowania ryzyk

Szczegółowa analiza ryzyk



Proces szacowania ryzyk

Szczegółowa analiza ryzyk

+ Wysokie prawdopodobieństwo właściwego zabezpieczenia aktywów,
+ Wyniki łatwo wykorzystać w zarządzaniu zmianami związanymi z bezpieczeństwem,
- Metoda czasochłonna i pracochłonna,

Proces szacowania ryzyk

Podejście mieszane

Początkowo dokonanie szacowania ryzyk metodą podstawowego poziomu bezpieczeństwa dla wszystkich aktywów i elementów ISMS, a potem dla aktywów wycenionych wysoko, bądź szczególnie narażonych *dokonanie analizy szczegółowej.*

Zaczynamy od metod - analiza

Proces szacowania ryzyk

Podejście mieszane

+ Wysokie prawdopodobieństwo właściwego zabezpieczenia aktywów przy efektywnych nakładach,
- Ze względu na to, że początkowe analizy ryzyka prowadzone *są na wysokim poziomie ogólności, niektóre wrażliwe* aktywa mogą nie zostać zakwalifikowane do analizy szczegółowej.

Proces szacowania ryzyk

6. Identyfikacja i ocena opcji postępowania z ryzykiem

W zależności od rodzajów aktywów, potencjalnych konsekwencji i poziomu ryzyk akceptowalnych.

- zastosowanie zabezpieczeń w celu **redukcji** ryzyk,
- świadoma i obiektywna decyzja o **akceptowaniu** ryzyk,
- **unikanie** ryzyk,
- **przeniesienie** ryzyk na inną organizację

Plan postępowania z ryzykiem - powinien być w/g normy.

Proces szacowania ryzyk

Unikanie ryzyka

Wszelkie działania mające na celu przeniesienie aktywów z obszarów wysokiego ryzyka np.

- rezygnacja z pewnych działalności (np. zablokowanie możliwości pracy zdalnej z wrażliwymi aplikacjami),
- przeniesienie aktywów z obszarów ryzyka (np. zakaz przechowywania szczególnie cennych informacji w niezamykanych pomieszczeniach biura).

Proces szacowania ryzyk

Przeniesienie ryzyka

Może być najlepszą opcją kiedy nie da się ryzyka uniknąć, jest zbyt trudno lub zbyt drogo aby ryzyko zredukować.

- na ubezpieczyciela,
- na dostawcę (outsourcing),
- [poza zakres ISMS].

Proces szacowania ryzyk

7. Zastosowanie zabezpieczeń

W celu redukcji ryzyka do poziomu akceptowalnego.
Proces wyboru zabezpieczeń powinien bazować na rezultatach szacowania ryzyk.

Konieczna jest inwentaryzacja zabezpieczeń już funkcjonujących wraz z decyzją o ich pozostawieniu, usunięciu lub udoskonaleniu.

Koszt zabezpieczeń !!!

Firma działa tak to aby [illegible]

Proces szacowania ryzyk

Czynniki wyboru zabezpieczenia:

- łatwość implementacji zabezpieczenia,
- „przezroczystość" dla użytkownika,
- ułatwiające realizację procesów,
- skuteczność,
- funkcja realizowana przez zabezpieczenie:
  - ✓ zapobiegania,
  - ✓ odstraszania,
  - ✓ wykrywania,
  - ✓ odzyskiwania,
  - ✓ korygowania,
  - ✓ monitorowania,
  - ✓ uświadamiania.

Proces szacowania ryzyk

Redukcja ryzyk

- zmniejszenie prawdopodobieństwa
- zapewnienie spełnienia wymagań prawnych i normatywnych,
- redukcja następstw sytuacji niepożądanych jeśli wystąpią,
- wykrywanie sytuacji niepożądanych i reakcja

Proces szacowania ryzyk

Akceptacja ryzyk

- zawsze pozostanie ryzyko szczątkowe,
- może ono być na poziomie akceptowalnym lub nie


Opcje postępowania z ryzykiem
Jeśli nic się nie sprawdza: zmień biznes!!!

PRZEPROWADZENIE AUDYTU

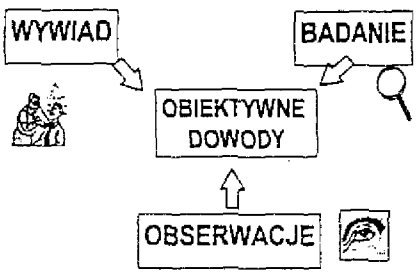
Przeprowadzenie audytu

Zdobywanie informacji

Jest wiele sposobów zdobywania informacji:

- rozmowy z pracownikami,
- badanie dokumentów,
- obserwacja działań i okoliczności.

Przeprowadzenie audytu



Pytania audytowe

CO?

DLACZEGO?

KIEDY?

JAK?

GDZIE?

KTO?

Proszę mi powiedzieć
Proszę mi pokazać

Spostrzeżenia

„Uwierz wyznaniu, ale sprawdź twierdzenie"

Należy dokonać przeglądu niezgodności z udziałem audytowanego dla uzyskania potwierdzenia, że dowody z audytu są dokładne i że niezgodności zostały zrozumiane

Sposoby przezwyciężania strachu u audytowanego

- pamiętaj audytujesz system a nie ludzi,
- buduj zaufanie,
- zapewnij poufność,
- zostaw uprzedzenia, bądź obiektywny,
- bądź życzliwy i spokojny,
- nie szukaj „dziury w całym",
- odrobina poczucia humoru nie zaszkodzi.

Proces wywiadu

- pytanie,
- słuchanie odpowiedzi,
- jednoczesna obserwacja (procesu, ale i tego, co dzieje się wokół),
- jeśli trzeba - prośba o powtórzenie lub uzupełnienie,
- podejmowanie decyzji,
- notowanie,
- upewnienie się, że audytowany rozumie o czym mówimy.

Uzyskiwanie informacji

Dwoje oczu

Dwoje uszu

Jedne usta

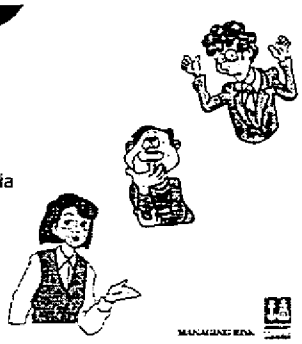
Próbkowanie

- populacja,
- próba losowa,
- próba reprezentatywna.

Ty określasz próbę,
ale to audytowany Ci ją podaje!

Język ciała

- oczy i brwi
- wyraz twarzy
- ręce
- postawa całego ciała



Zachowanie audytorów

Pracując nad swoim wizerunkiem, audytor powinien zawsze:

- stosownie się ubierać,
- zachowywać się etycznie,
- być punktualnym,
- być dobrze przygotowanym,
- być precyzyjnym i dokładnym,
- być zdecydowanym i bezpośrednim,
- być ludzkim i uczciwym,
- panować nad audytem i kontrolować czas,
- zachować spokój i uprzejmość,
- pozwolić audytowanemu odprężyć się,
- umieć pochwalić i wyrazić uznanie tam, gdzie się ono należy.

Źródła wymagań

- Norma
- Polityki Bezpieczeństwa
- Deklaracja Stosowania
- Analiza ryzyk
- Procesy organizacji
- Procedury organizacji
- Instrukcje robocze organizacji
- Zamówienie klienta
- Przepisy i wymogi prawa

Raporty niezgodności

- Raport niezgodności
- Protokół odstępstwa
- Wniosek o działanie korygujące
- Formularz potencjalnego udoskonalenia

Klasyfikacja niezgodności

Duża / Mała
Kategoria 1 / Kategoria 2
Punkt wstrzymujący / Możliwość poprawy

Klasyfikacja niezgodności

Kategoria 1

Brak lub nieskuteczne wdrożenie jednego lub większej ilości wymaganych elementów systemu, lub sytuacja która wzbudza poważne wątpliwości czy wyroby lub usługi spełnią ustalone wymagania,

lub

Grupa niezgodności kategorii 2 wskazujących na niewłaściwe wdrożenie systemu i odnoszących się do tego samego elementu normy

Klasyfikacja niezgodności

Kategoria 2

Uchybienie dyscypliny lub nadzoru podczas wdrażania wymagań systemowych/proceduralnych, które nie wskazuje na załamanie się systemu ani nie nasuwa wątpliwości, czy wyroby lub usługi spełnią wymagania

Dokumentowanie niezgodności

- **WYMAGANIE** (norma, dokument ISMS, procedura werbalna ...)
- **BŁĄD** (sytuacja, wypowiedź, brak zapisu ...)
- **DOWÓD** (wskazanie dowodu obiektywnego)

(stwierdzić brak zapisu ... nie przestrzegania zapisu)

tak zapisz wszystko bo to kawałek tekstu może przydać

Dokumentowanie niezgodności

Zapisy dotyczące niezgodności powinny być jasne, precyzyjne, łatwe do zweryfikowania, zatwierdzone przez audytora i potwierdzone przez audytowanego.

Zasady poszukiwania faktów

- Nie wyzbywaj się wątpliwości i pytaj o wszystko
- Poznaj różnice pomiędzy stwierdzeniami płynącymi z racjonalnych dowodów, a tymi, które są jedynie perswazją
- Bądź precyzyjny w słowach i oczekuj precyzji od innych
- Spodziewaj się błędów nawet w Piśmie Świętym

Piotr Abelard (1079-1142)

Cechy audytora

JAKI POWINIEN BYĆ AUDYTOR?

- Taktowny i dyplomatyczny
- Komunikatywny
- Otwarty i wolny od uprzedzeń
- Dojrzały
- Sprawiedliwy
- Zdolny do analizowania skomplikowanych sytuacji
- Nieustępliwy

Cechy audytora

JAKI NIE POWINIEN BYĆ AUDYTOR?

- Kłótliwy
- Zadufany
- Leniwy
- Podatny na wpływy
- Pochopnie wyciągający wnioski

Cechy audytora

„Typowy audytor to mężczyzna powyżej wieku średniego, szczupły, pomarszczony, inteligentny, zimny, pasywny, dyplomatyczny, z oczami dorsza, uprzejmy, ale równocześnie niekontaktowy, spokojny i irytująco zrównoważony jak betonowy słup lub odlew, ludzka skamieniałość z sercem jak głaz, bez krztyny uroku, litości, uczucia i poczucia humoru. Na szczęście nigdy się nie rozmnażają i w końcu idą do piekła."

Elbert Hubbard

Taktyki opóźniania audytu

- przewodnik porzuca audytora i nie wraca,
- pracownicy pełniący kluczowe funkcje są niedostępni lub spóźniają się,
- przewodnik nie zna pracowników funkcyjnych,
- brak dostępu do dokumentów,
- banalne rozmowy,
- przewodnik często prowadzi od działu do działu bardzo długą trasą,
- częste przerwy,
- telefony,
- prezentacje komputerowe.

Kategoria i tytuł zawodowy
Dostęp do informacji zapisanej

DZIAŁANIA POAUDYTOWE

Działania poaudytowe

- Opracowanie raportu
- Przekazanie raportu
- Działania korygujące / zapobiegawcze
- Weryfikacja wdrożenia działań korygujących i zapobiegawczych oraz ocena ich skuteczności

Raport
ISO gwiazdy mówią co powinno
się tam znaleźć

Kategoryzacja niezgodności

Wpisanie jest dobre — to niezgodność
lub uwaga ext. i wpisać

że mamy się dostosować.

Tabela Rozdział do nie są wymagane
europejskich akredytacji

EA 7/03 www.ea.
7/02 sprawdzić

Raport z audytu

- zakres i cele audytu,
- termin audytu,
- szczegóły różnych aspektów audytowanego systemu,
- tożsamość członków zespołu audytującego,
- tożsamość członków personelu z którymi prowadzono rozmowy,
- tożsamość dokumentów stanowiących podstawę audytu (norma odniesienia, polityki bezpieczeństwa organizacji, SoA, RTP, itp.),

Raport z audytu - cd

- raporty niezgodności w odniesieniu do przypadków niespełnienia wymagań,
- raporty obserwacji, dotyczące potencjalnych niezgodności lub aspektów, które zdaniem zespołu audytującego warto wyjaśnić,
- należy wykorzystać okazję do zasygnalizowania nie tylko słabych punktów, ale i zaobserwowanych mocnych stron,
- podsumowanie lub wynik audytu w postaci opinii zespołu audytującego na temat zgodności ISMS z kryteriami audytu,
- lista adresatów raportu.

Raport z audytu - załączniki

- raporty niezgodności,
- listy obecności,
- plan audytu

Raport z audytu

Nie należy poruszać:

- tematów drażliwych, o charakterze politycznym, będących przedmiotem szczególnej wrażliwości,
- spraw wybiegających poza zakres audytu,
- spraw, o których nie było wzmianki, lub które nie były omawiane podczas audytu.

Niezgodności i działania korygujące

- odpowiedzialnością **audytora** jest identyfikacja niezgodności
- odpowiedzialnością **audytowanego** jest działanie korygujące

nie identyfikujemy
problemu i nie podejmujemy
działań korygujących.

Jednostka certyfikacyjna
nie powinna bawić się
konsultingiem jeżeli nie chce
się precyzyjnie wiązać (to Pan
tak powiedział)

Działania korygujące

- identyfikacja przyczyn stwierdzonych niezgodności,
- decyzja dotycząca niezgodności,
- określenie niezbędnych działań korygujących,
- określenie oczekiwanych rezultatów działań korygujących,
- podjęcie działań korygujących,
- ocena skuteczności podjętych działań korygujących.

Nie powinno tak być że
tylko niezgodności z audytu
są poprawiane a inne już nie
Ciekawe jest tak że wtedy
się niezgodności z audytu

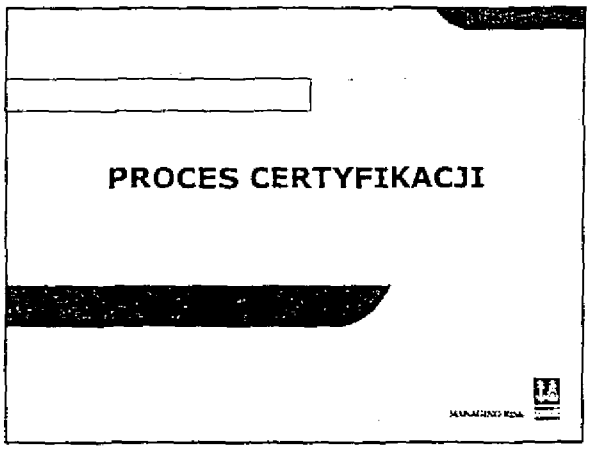
Niezgodności wynikające z audytu

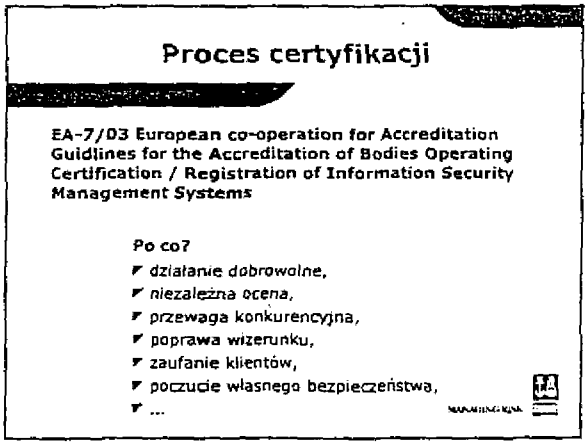
Różny punkt odbioru
organizacja zapobiegania

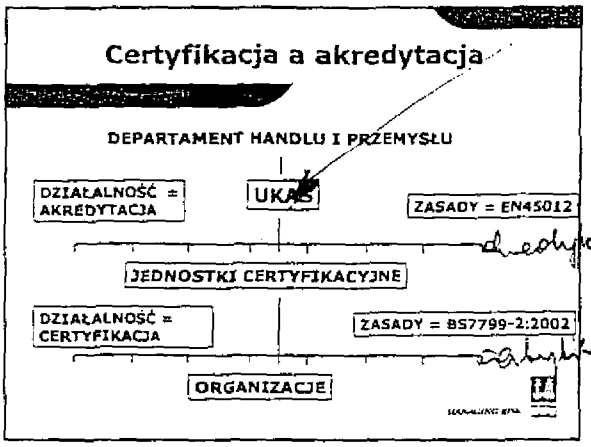
Działania korygujące

Przyczyną niezgodności

było jej wykrycie przez audytora


PROCES CERTYFIKACJI


Proces certyfikacji
EA-7/03 European co-operation for Accreditation Guidlines for the Accreditation of Bodies Operating Certification / Registration of Information Security Management Systems
Po co?
działanie dobrowolne,
niezależna ocena,
przewaga konkurencyjna,
poprawa wizerunku,
zaufanie klientów,
poczucie własnego bezpieczeństwa,
...


Certyfikacja a akredytacja
DEPARTAMENT HANDLU I PRZEMYSŁU
DZIAŁALNOŚĆ = AKREDYTACJA
UKAS
ZASADY = EN45012
JEDNOSTKI CERTYFIKACYJNE
DZIAŁALNOŚĆ = CERTYFIKACJA
ZASADY = BS7799-2:2002
ORGANIZACJE

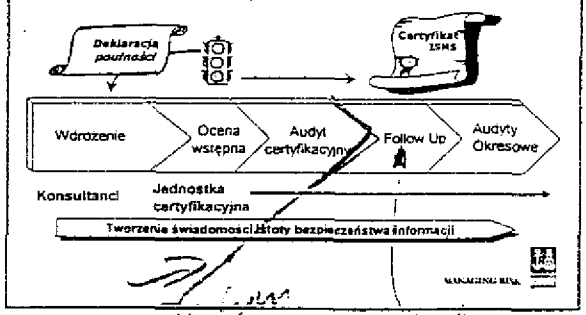
Proces certyfikacji

Warunki przystąpienia do procesu certyfikacji:

- co najmniej 6 miesięcy funkcjonowania systemu od momentu zakończenia procesu wdrażania,
- audyty wewnętrzne i przegląd wykonywany przez kierownictwo zostały przeprowadzone,
- dokonana analiza ryzyka,
- system obsługi niezgodności, reakcji na incydenty i inicjowania działań korygujących wykazuje, że proces ciągłego doskonalenia przebiega prawidłowo.

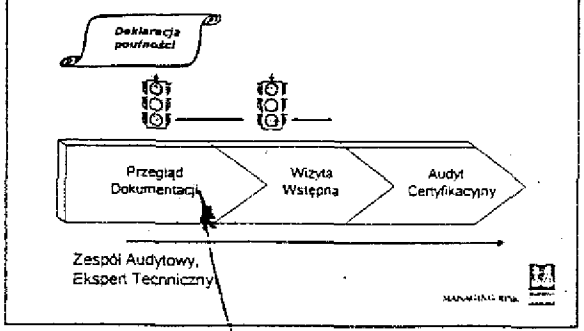
Audytor ma analizować system zarządzania a nie oklaskiwać...

Proces certyfikacji



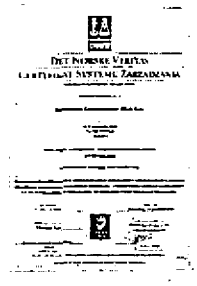
Audytorzy nie dojrzą dwa razy wstępna. Audytorzy, ... w ... można rozbierać na części recertyfikacyjne Audyty okresowe tutaj 6.9.17 kwestia

Proces certyfikacji



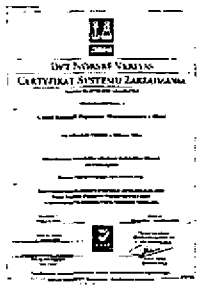
to co mamy porównywać z normą.

Certyfikacja DNV



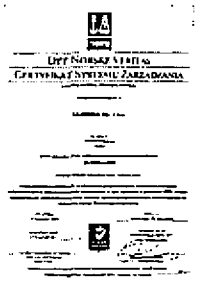
Doradztwo Gospodarcze
DGA S.A.

Certyfikacja DNV

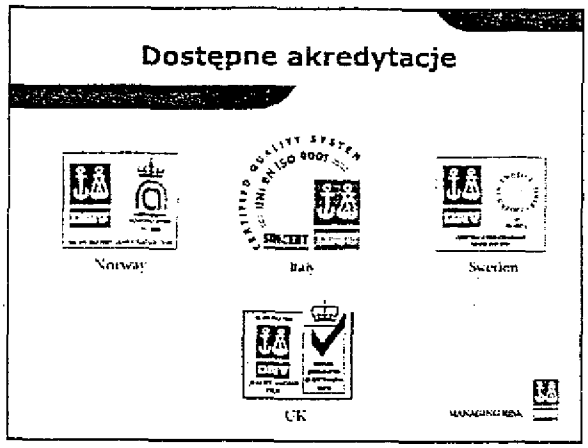


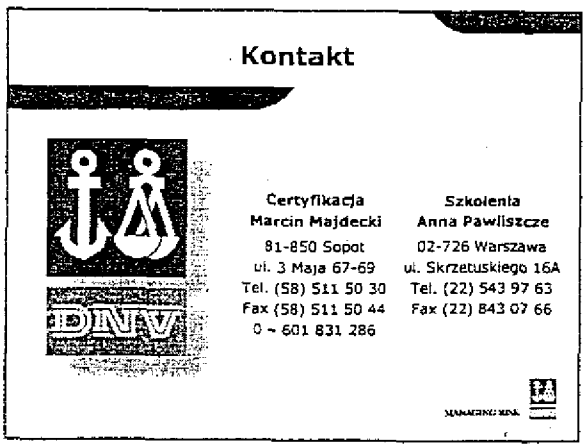
Urząd Komisji
Papierów Wartościowych
i Giełd

Certyfikacja DNV



LUMENA Sp. z o.o.





Nie może kogo sygnować certyfikacją wyników to my certyfikujemy system.

WWW.irca.org - international register of certificated auditors

Stopnie certyfikacji:
- ISMS Provisional Auditor

ISO 17043 ⇒ nie ma B a zamiast
z certyfikowanej usługi

akredytacja od GHITBiów

Delegowanie uprawnień | ABN - instytucja wydająca
nie wiem się z delegacją | WWW.in.gov.pl