

ISO 27001:2005 Sustav upravljanja informacijskom sigurnošću

ISO 27001:2005

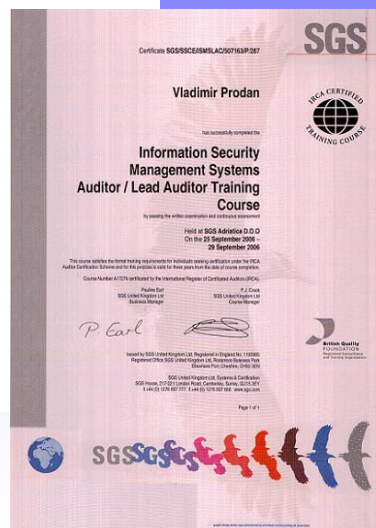
Information Technologies System Security Day

www.adriakon.hr

ISO 27001:2005 Sustav upravljanja informacijskom sigurnošću

Vladimir Prodan, dipl. ing. elek.

**Microsoft Certified System Engineer
TÜV Lead Auditor ISO 9001
SGS Lead Auditor ISO 27001**



ISO 27001:2005 Sustav upravljanja informacijskom sigurnošću

VLADIMIR PRODAN: ISO 9001, ISO 14001, ISO 27001, ...

Reference iz područja sustava kvalitete (ISO 9001, ISO 14001 – više od 60 poduzeća u Hrvatskoj):

Istra Informatički Inženjering d.o.o.	Pula	(informatika)
ARBOR INFORMATIKA d.o.o.	Rijeka	(informatika)
INFODESIGN d.o.o.	Varaždin	(informatika)
ABIT d.o.o.	Varaždin	(informatika)
COMPAK d.o.o.	Varaždin	(informatika)
DIALOG d.o.o.	Đakovo	(informatika)
INFOPROJEKT d.o.o.	Rijeka	(informatika)
PAKEL d.o.o.	Zadar	(informatika)
KLINIČKA BOLNICA MERKUR	Zagreb	(zavodi: radiologija, klinička kemija, interna kl.)
CHROMOS, Boje i lakovi d.d.	Zagreb	(boje i lakovi)
ZAGREBACKA VELETRŽNICA d.o.o.	Zagreb	(veletržnica)
DOKING d.o.o.	Zagreb	(razminiranje, strojevi za razminiranje)
LANAC d.o.o.	Zagreb	(željezni proizvodi i lanci)
PARTING d.o.o.	Zagreb	(upravljanje nekretninama)
TELEFON-GRADNJA d.o.o.	Zagreb	(cestovne instalacije)
...		
LİPOVICA	Popovača	(tvornica radijatora i ljevaonica)
VİROBETON d.d.	Vinkovci	(betonske konstrukcije)
...		
ĐRVOPLAST d.d.	Buzet	(namještaj, plastični profili)
GRADING KUK d.d. + ISO 14001	Buzet	(građenje)
FEROPLAST d.o.o. + ISO 14001	Buje	(žičani proizvodi)
AR-METAL d.o.o. + ISO 14001	Rijeka	(metalne konstrukcije)
Riječki uslužni servis d.o.o. + ISO 14001	Rijeka	(čišćenje)
ISTARSKA CIGLANA d.d. + ISO 14001	Rijeka	(betonska galanterija)
SIGURNOST-BOLJUN i DR. J.T.D.	Cerovlje	(zaštitarske djelatnosti)
GEOPROJEKT d.d.	Pula	(geodezija i projektiranje)
KAVAIMPEX d.o.o.	Opatija	(pržionica kave)
PK d.o.o.	Boljun	(ugradnja kamionskih dizalica)
NARODNO SVEUČILIŠTE d.o.o.	Rijeka	(obrazovanje)
...		

ISO 27001:2005 Sustav upravljanja informacijskom sigurnošću

Information Security Management System

ISO/IEC 17799 and BS 7799-2 and ISO 27001

1989 – BS PD 0003, A code of practice for information security management

1995 – Updated and re-issued as BS 7799

1998 – Part 2 of BS 7799 issued

1999 – First major revision to BS 7799-1

2000 – ISO 17799 was identical in technical content to BS7799-1

2002 – Major revision to BS 7799-2

2005 – ISO 27001

BS 7799-1 = ISO 17799

BS 7799-2 = ISO 27001

4 Information security management system

4.1 General requirements

4.2 Establishing and managing the ISMS

4.2.1 Establish the ISMS **ANNEX A**

4.2.2 Implement and operate the ISMS

4.2.3 Monitor and review the ISMS

4.2.4 Maintain and improve the ISMS

4.3 Documentation requirements

4.3.1 General

4.3.2 Control of documents

ISO 9001

ISO 14001

4.3.3 Control of records

5 Management responsibility

5.1 Management commitment

5.2 Resource management

5.2.1 Provision of resources

5.2.2 Training, awareness and competence

6 Internal ISMS audit

7 Management review of the ISMS

7.1 General

7.2 Review input

7.3 Review output

8 ISMS improvement

8.1 Continual improvement

ISO 9001

8.2 Corrective action

ISO 14001

8.3 Preventive action

Annex A Control objectives and controls

ISO 27001:2005 Sustav upravljanja informacijskom sigurnošću

Aneks A	Engl.
5	Security Policy
6	Organization of information security
6.1	Internal organization
6.2	External parties
7	Asset management
7.1	Responsibility for assets
7.2	Information classification
8	Human resources security
8.1	Prior to employment
8.2	During employment
8.3	Termination or change of employment
9	Physical and environmental security
9.1	Secure areas
9.2	Equipment security
10	Communications and operations management
10.1	Operational procedures and responsibilities
10.2	Third party service delivery management
10.3	System planning and acceptance
10.4	Protection against malicious software

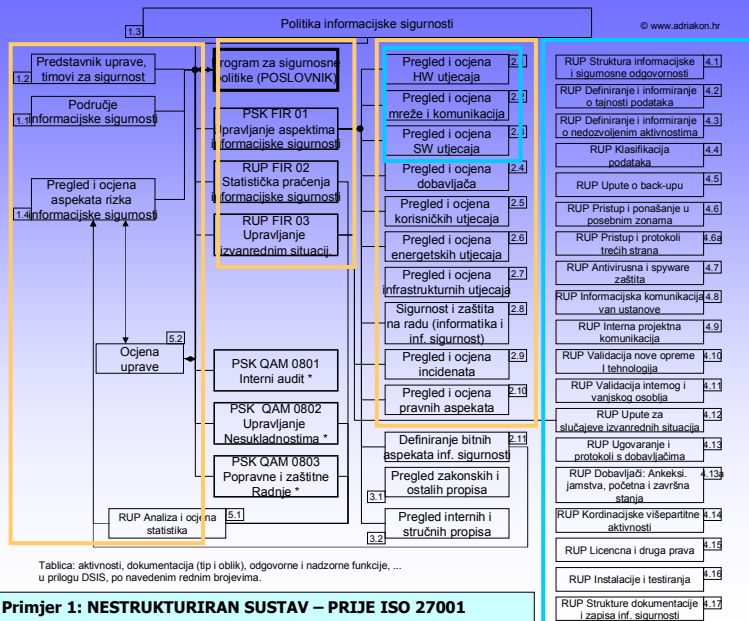
ISO 27001:2005 Sustav upravljanja informacijskom sigurnošću

10.5	Back-up
10.6	Network Security management
10.7	Media handling
10.8	Exchange of information
10.9	Electronic commerce services
10.1	Monitoring
11	Access Control
11.1	Business requirement for access control
11.2	User access management
11.3	User responsibilities
11.4	Network access control
11.5	Operating system access control
11.6	Application and information access control
11.7	Mobile computing and teleworking
12	Information systems acquisition, development and maintenance
12.1	Security requirements of information systems
12.2	Correct processing in applications
12.3	Cryptographic controls
12.4	Security of system files
12.5	Security in development and support processes

ISO 27001:2005 Sustav upravljanja informacijskom sigurnošću

12.6	Technical Vulnerability Management
13	Information security incident management
13.1	Reporting information security events and weaknesses
13.2	Management of information security incidents and improvements
14	Business continuity management
14.1	Information security aspects of business continuity management
15	Compliance
15.1	Compliance with legal requirements
15.2	Compliance with security policies and standards, and technical compliance
15.3	Information systems audit considerations

ISO 27001:2005 Sustav upravljanja informacijskom sigurnošću



ISO 27001:2005 Sustav upravljanja informacijskom sigurnošću

STRUKTURIRAN SUSTAV - zapisi:

Information security policy	- Politika - opća
IT Resources Use Policy	o politika resursa
Electronic mail policy	o politika e-maila
Confidentiality statement policy	o politika o tajnosti podataka
...	o ...
ISMS Objectives	- Ciljevi
Statement of Applicability	- Izjava o primjenjivosti
Risk assesment	- Ocjena rizika sumarna
Risk treatment plan	- Plan upravljanja rizicima
Statistics	- Statistike
Nonconf. and corr. act. list – intern. audit	- Nesukladnosti i popravne radnje audita
Nonconf. and corr. act. list - process	- Nesukladnosti i popravne radnje procesi
List of preventive acivities	- Zaštitne radnje
Annual revision	- Revizija
Annual revision - questionnaire	o revizijska lista
Annual revision - summary overview	o sumarna ocjena
...	...

ISO 27001:2005 Sustav upravljanja informacijskom sigurnošću

STRUKTURA DOKUMENTACIJE ISO 27001:



RIZICI

Upravljanje rizikom Risk Management

Procjena rizika Risk Assessment

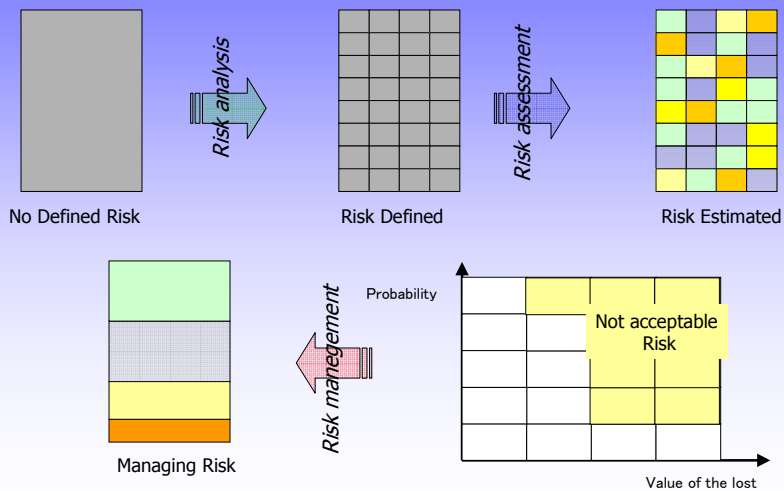
Analiza rizika Risk Analysis

Proračun rizika Risk Evaluation

Prihvatanje rizika Risk Acceptance

Postupanje rizikom Risk Treatment

Risk Assessment & Management



- **Risk management – upravljanje rizicima**
- **Data recovery – povrat podatka**
- **Business continuity plan – plan stalnosti poslovanja**

ISO 13335 "Guidelines for the Management of Information Security"
ISO 13569 "Banking and Related Financial Services – Information Security Guidelines"
ISO 15408 "Evaluation Criteria for IT Security (Common Criteria)"

USA NIST's 800 Series
USA GAO's Federal Information Systems Controls Audit Manual (FISCAM)
German BSI "IT Baseline Protection Manual"

ISF's Standard of Good Practice
SEI's OCTAVE
SEI's SW-CMM
ISACA's COBIT
FFIEC IT Examination Handbooks
ISSA's GAISP

...

RIZICI – APEKTI – PROCJENA - uobičajene greške

	Važnost (1-10):		
	Back-up	Antivirus	Tajnost
1. Proizvodno poduzeće	5	3	8
2. Novinska kuća	8	8	8
3. Trgovačko poduzeće	5	3-8	5
4. Financijska ustanova	5	3	9
5. Turistička ustanova	3	7	9

...,zatvoreni sustavi, real-time sustavi,...

RIZICI HW - primarna selekcija

Utjecaj:

ograničen na radno mjesto
unutar organizacije
šire
zaštita u okviru tekućih troškova
treba dodatna sredstva

Vlastita ocjena:

važan
nepoznato
samostalni nadzor moguć
potrebna vanjska usluga

Važnost:

za tim za sigurnost
za korisnika
za korisnikov odjel
za ustanovu

Zainteresirane strane:

pritužba (korisnika, ...)
medijska ili pravna reakcija moguća
Nepoznato

Zakonski zahtjev:

jasan
naslućuje
nepoznat
nema

RIZICI SOFTWARE

- | | |
|-------------------|--------------------------|
| ... | ... |
| -Uredski programi | -virusi |
| -E-mail programi | -spyware |
| -Internet | -greške u korištenju |
| -Aplikacije | -pogrešan unos |
| -Sistemska SW | -neovlaštene instalacije |
| ... | -privatna upotreba |
| | -poslovna tajna |
| | -lozinke |
| | -E-mail |
| | -internet |
| | ... |

RIZICI DOBAVLJAČI

- Podaci/aktivnost/oprema
- Dobavljač
- Trajanje ugovora
- Ugovoren odziv
- Procjena rizika
- Zastoj kod kvara izražen u vremenu
- Zastoj kod kvara izražen u vrijednosti
- Protokoli kod prekida suradnje
- Postupci kod incidenta
- Lista odobrenog osoblja
- Ograničenje pristupa

RIZICI OSTALO

...

- požar
- poplava
- krađa
- energetika i instalacije
- el. ometanja
- neovlašteni pristupi
- greške trećih strana (dobavljači,...)

...

PRAVNI ASPEKTI:

Interni:

- tajnost podatka – pravila ponašanja (osoblje)
- strukture podataka (službeno, interno, javno)
- kvalifikacija – procjena osoblja

Dobavljači:

- tajnost podatka – pravila
- prava pristupa
- prijelazni period (otkaz)
- odgovornost za štetu

Treće strane:

- tajnost podataka – pravila ponašanja
- kvalifikacija - procjena osoblja

Zakonska regulativa: ...

Sigurnost nije stanje nego proces.

%	TIP INCIDENTA	MJESTA POBOLJŠANJA
30	neznanje, neorganiziranost...	ORGANIZACIJA
20	greške korisnika (virus, e-mail, ...)	OBRAZOVANJE
10	greške u komunikaciji kod uvođenja novih aplikacija	TEHNOLOGIJE,ORG,OBR
10	nove tehnologije i prijelazna stanja	TEHNOLOGIJE
10	dobavljači i treće strane	PRAVNO, ORG
9	oprema (*)	TEHNOLOGIJE
8	energenti	ORG, TEH
3	namjerna vanjska opasnost	OBR,ORG,TEH,PRA

DOSTUPNOST, POVJERLJIVOST, INTEGRITET:

**Alat kojim,
koristeći razne metode i tehnološka rješenja,
rizik informacijske sigurnosti svodimo na minimum.**