

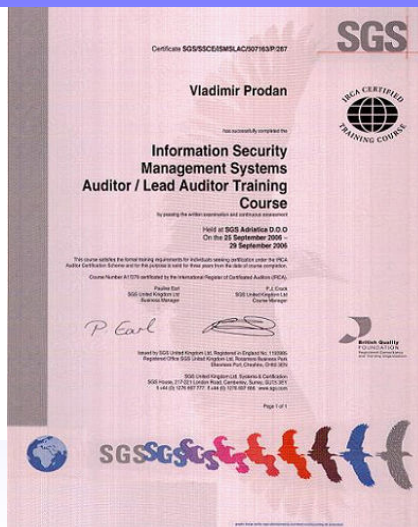
# ISO 27001:2005

## Information Technologies System Security Day

[www.adriakon.hr](http://www.adriakon.hr)

**Vladimir Prodan, BSEE**

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



## 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

**ISO 27001:2005 Information Security Management System**

- 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 Information Security Management System**

<b>Aneks A</b>	<b>Engl.</b>
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

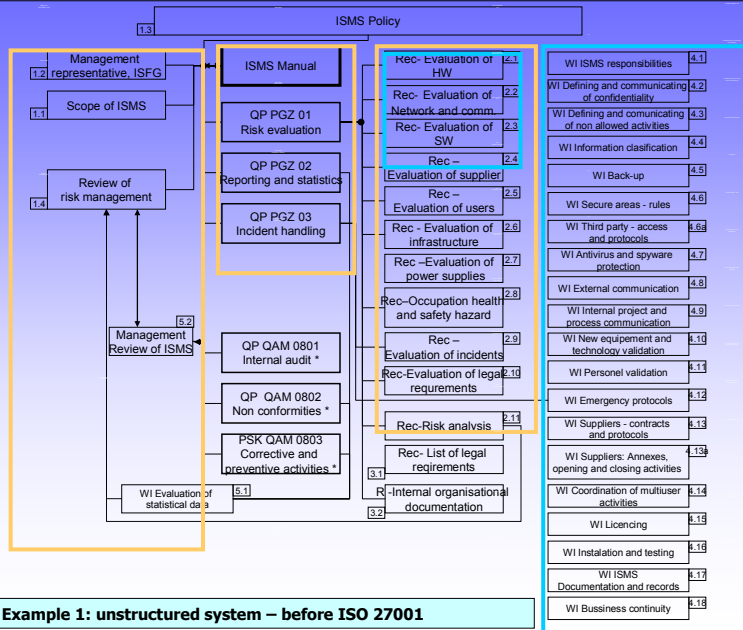
### ISO 27001:2005 Information Security Management System

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 Information Security Management System

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 Information Security Management System

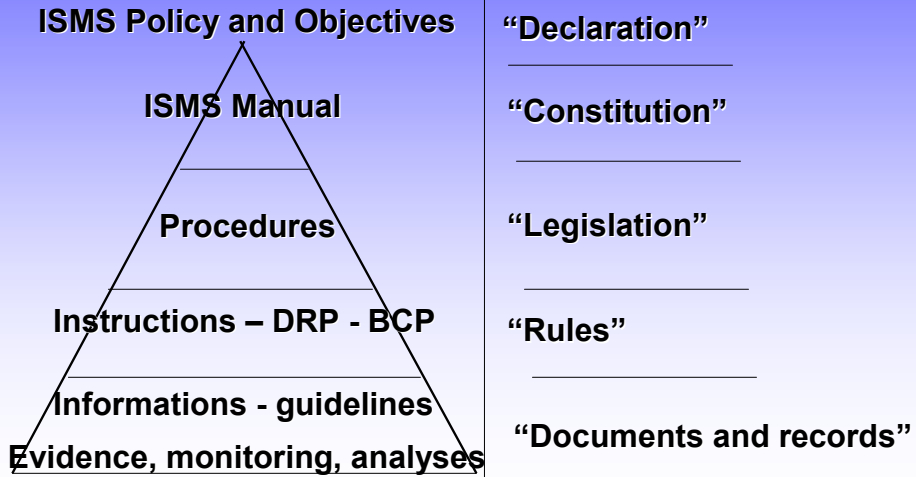


## ISO 27001:2005 Information Security Management System

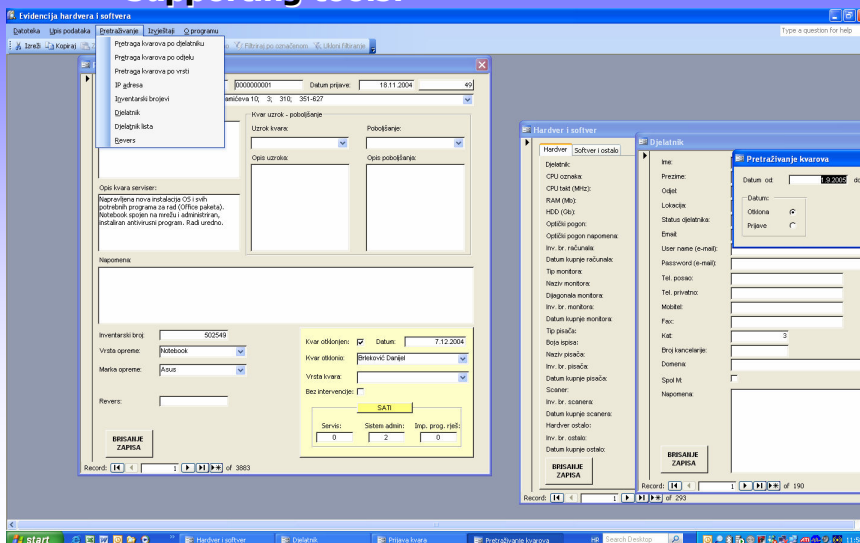
### STRUCTURED SYSTEM - records:

- Information security policy
- IT Resources Use Policy
- Electronic mail policy
- Confidentiality statment policy
- ...
- ISMS Objectives
- Statement of Applicability
- Risk assesment
- Risk treatment plan
- Statistics
- Nonconf. and corr. act. list – intern. audit
- Nonconf. and corr. act. list - process
- List of preventive activities
- Annual revision
- Annual revision - questionnaire
- Annual revision - summary overview
- ...

STRUCTURE OF DOCUMENTATION ISO 27001:



Supporting tools:



## ISO 27001:2005 Information Security Management System

The screenshot displays the Admin DISK application interface. The main window shows a list of activities with columns for ID, Aktivnost, Datum, and OPIS. A callout bubble points to the 'Aktivnost' column, stating: 'Filter activities based on user who is logged to application. (my tasks – active tasks)'. Another callout bubble points to the 'Aktivnost' column, stating: 'Filter activities based on type of activity (incident, solution, risk, etc...)'. A third callout bubble points to a specific activity entry, stating: 'Detailed form of activity'. The detailed form shows a form with various fields and a 'Završi' button.

ID	Aktivnost	OPIS	Grupa korisnika	odjeljenje/ostava
1863	Zapocetak		Svi	
1872	Zapoceti radovi	Napraven backup po-a listiran	Svi	
1893	Zapoceti radovi	Igor 045 26.12.2006 26.12.2006 Napraven backup po-a listiran	Supervizi	
2738	Zapocetak	26.12.2006 26.12.2006 Test veze		
		31.1.2007 22:55 1.2.2007 Aktivnost 2		
2247				
2731				
2187				
1853				
0				

## ISO 27001:2005 Information Security Management System

### RISK

**Risk Management**

**Risk Assessment**

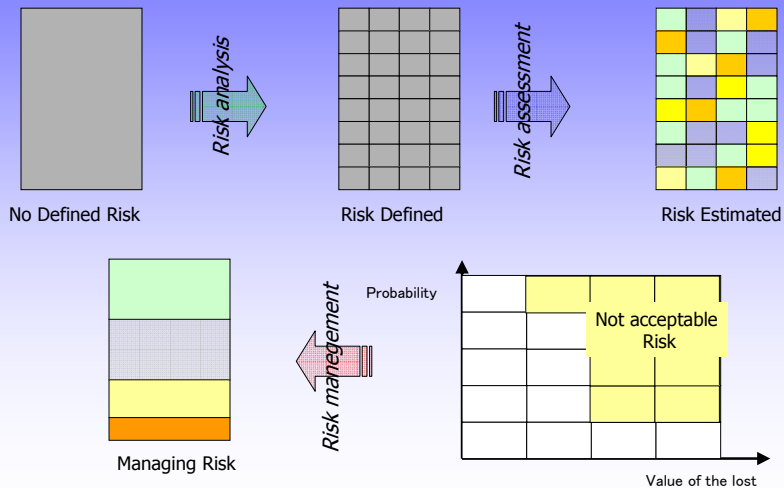
**Risk Analysis**

**Risk Evaluation**

**Risk Acceptance**

**Risk Treatment**

### Risk Assessment & Management



- Risk management
- Data recovery
- Business continuity plan

**ISO 27001:2005 Information Security Management System**

---

**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**  
...

**ISO 27001:2005 Information Security Management System**

---

**RISK – ASPECTS – EVALUATION - usual omission**

	Importance (1-10):		
	Back-up	Antivirus	Confidentiality
<b>1. Production company</b>	<b>5</b>	<b>3</b>	<b>8</b>
<b>2. Newspaper or publishing</b>	<b>8</b>	<b>8</b>	<b>8</b>
<b>3. Retail</b>	<b>5</b>	<b>3-8</b>	<b>5</b>
<b>4. Financial</b>	<b>5</b>	<b>3</b>	<b>9</b>
<b>5. Tourism</b>	<b>3</b>	<b>7</b>	<b>9</b>
..., real-time systems,...			

## RISK HW - primary selection

### Influence:

Limited to workplace  
Inside company  
Wide area  
Expences in planed framework  
Additional or external help necessary

### Intereseted parties:

Complaint (user, ...)  
Juridical or media response  
Unknown

### Legislative requirements:

Clear  
Possible  
Unknown  
Absence

### Self assesment:

Importance significant  
Unknown importance  
Internal supervision suficient  
External help necesarily

### Importance:

For ISMS team  
For user  
For department  
For company

## RISK SOFTWARE

...  
-Office application  
-E-mail  
-Internet  
-Applications  
-System SW  
...

...  
-Viruses  
-Spyware  
-Use errors  
-Entry errors  
-Unauthorised instalations  
-Unauthorised use of assets  
-Confidentiality  
-Passwords  
-Web  
-Interanet  
...

## **RISK - SUPPLIERS**

**Data/Activities/Equipment**  
**Contract terms**  
**Response procedures**  
**Supplier risk evaluation**  
**Failure delay – in time**  
**Failure delay – in value**  
**Incident procedures**  
**Authorised personnel list**  
**Access restriction**  
**Contract termination protocols**

## **RISK - other**

...  
**-Fire**  
**-Flood**  
**-Theft**  
**-Energetics and infrastructure**  
**-Interferences and obstructions**  
**-Unauthorised access**  
**-Third party failure (suppliers,...)**  
...

**LEGAL ASPECTS:**

**Internal:**

- confidentiality – code of conduct (personnel)
- data structures (officially, internal, public)
- qualification – evaluation of personnel

**Suppliers:**

- confidentiality – rules
- access and assets rights
- transition period (contract termination)
- error, malfunction or incident responsibilities

**Third party:**

- confidentiality – rules
- qualification – evaluation of personnel

**Legal requirements: ...**

**Information security is not a condition but a process.**

<b>%</b>	<b>INCIDENT TYPE</b>	<b>IMPROVEMENTS</b>
<b>30</b>	<b>unadequate organisation, ignorance, ...</b>	<b>organisational</b>
<b>20</b>	<b>users error (virus, e-mail, ...)</b>	<b>educational</b>
<b>10</b>	<b>organisational communication problems - new technologies</b>	<b>technologies, org., edu.</b>
<b>10</b>	<b>new technologies and transition stages</b>	<b>technologies</b>
<b>10</b>	<b>suppliers and third parties</b>	<b>legal, org.</b>
<b>9</b>	<b>equipment (*)</b>	<b>technologies</b>
<b>8</b>	<b>energetic and infrastructure</b>	<b>org., tech.</b>
<b>3</b>	<b>intentional external threat</b>	<b>edu., org., tech., leg.</b>

**AVAILABILITY, CONFIDENTIALITY, INTEGRITY:**

**Tool for decreasing information security risk by use  
of various methodologies and technologies.**