

Contents

Contents	1
Legislation.....	2
Standards Related to Information Security	3
General Principles	5
Information Security Management Recommendations.....	6
1) Introduce Risk Management as a Part of Information Security Management	6
2) Have a Security Policy:.....	7
3) Managing Information Security	7
4) Managing Assets	8
5) Paying Sufficient Attention to Personnel Security.....	8
6) Resolving Physical Security.....	8
7) Managing Communications and Operations.....	8
8) Managing Access to Systems.....	8
9) Paying Sufficient Attention to Procurement, Development and Maintenance	9
10) Resolving Security Incidents and Insufficiencies	9
11) Managing Continuity Administration	9
12) Ensuring Compliance with Standards and Legislation	9
Implementing Information Security Management Systems.....	10
Other Recommendations.....	12
Main Processes for Managing the Life-Cycle of Security Documentation	12
Types of Documentation.....	13
IS Security Plans	14

Legislation

The most important Czech legislation related to information security includes:

Constitutional Act No. 23/1991 Coll.,

Which introduces the Charter of Fundamental Rights and Freedoms.

Act No. 101/2000 Coll.,

On data protection and amendments to certain acts, as amended.

Act No. 106/1999 Coll.,

On free access to information, as amended.

Act No. 140/1961 Coll.,

The Criminal Code, as amended.

Act No. 513/1991 Coll.,

The Commercial Code, as amended.

Act No. 499/2004 Coll.,

On archive and registration services, and amendments to certain acts.

Act No. 337/1992 Coll.,

On tax and charges administration, as amended .

Act No. 551/1991 Coll.,

On the General Health Insurance Company of the Czech Republic, as amended .

Act No. 365/2000 Coll.,

On public administration information systems and amendments to certain acts, as amended.

Act No. 127/2005 Coll.,

On electronic communications and amendments to certain related acts (the Electronic communications act).

Act No. 227/2000 Coll.,

On electronic signatures and amendments to certain other acts (the Electronic signatures act), as amended.

Act No. 480/2004 Coll.,

On information society services.

Government Resolution No. 624 of 20 June 2001,

On the rules, principles and methods of auditing the use of computer programmes.

Constitutional Act No. 110/1998 Coll.,

On CR security, as amended.

Act No. 148/1998 Coll.,

On protection of classified information and amendments to certain other acts, as amended .

NBÚ Decree No. 56/1999 Coll.,

On security for information systems processing classified information, their accreditation and certification matters.

Act No. 240/2000 Coll.,

On crisis management and amendments to certain other acts (the Crisis act), as amended by the Act No. 320/2002 Coll.

Government Regulation 462/2000 Coll.,

On implementing Section 27 para. 8 and Section 28 para. 5 Act No. 240/2000 Coll., on crisis management and amendments to certain other acts (the Crisis Act).

Act No. 239/2000 Coll.,

On the integrated emergency system and amendments to certain other acts, as amended.

Act No. 121/2000 Coll.,

On copyrights and related rights and amendments to certain other acts (the Copyright Act).

Act No. 89/1995 Coll.,

On the National Statistical Service, as amended .

Act No. 552/1991 Coll.,

On state audits, as amended by Audit Regulations.

Act No. 166/1993 Coll.,

On the Supreme Audit Office, as amended .

Government Resolutions:

Resolution No. 2/1993 Coll.,

On the Declaration of the Charter of Fundamental Rights and Freedoms as a Part of the Constitutional Order of the Czech Republic.

Government Resolution No. 271 dated 21st March 2001,

On Communications infrastructure services for the Public Administration Information System (PAIS).

The most important European Union legislation for information security is as follows:

- **Directive 1997/66/EC** on data protection in the telecommunications sector.
- **Directive 1995/46/EC** on personal data protection.
- **Directive 2002/58/EC** on privacy and electronic communications.
- **Directive 1999/93/EC** on community framework for electronic signatures.
- **Directive 2002/58/EC** on the processing of personal data and privacy protection.
- **Regulation 2001/45/EC** on personal protection in personal data processing by authorities and institutions.
- **Council Directive 1991/250/EEC** on the legal protection of computer programmes.
- **Council Directive 2001/264/EC** on the protection of classified information.

Development guidelines are set out in action programmes and plans:

- **Interchange of Electronic Data between Administrations [member states] (IDA).**
- eEurope 2005: *An information society for all.*
- *Multiannual Community programme to stimulate the establishment of the information society in Europe.*
- *A user-friendly information society.*
- *Safer Internet.*

Standards Related to Information Security

The most important (generally most supported) standards for information security are:

CSN ISO/IEC 17799:2001

Information technology– Procedures for information security management.

CSN BS 7799-2:2004

Information security management systems – Specifications with instructions for use.

(Note: This originally British standard – BS 7799 has become the most recognised standard for information security management due to its high quality and intelligibility.)

Guidelines issued by the British Standards Institution closely related to BS 7799:

- *PD 3001:2002* *Preparing for BS 7799-2 certification,*
- *PD 3002:2002* *Guide to BS 7799 risk assessment,*
- *PD 3003:2002* *Compliance assessment workbook,*
- *PD 3004:2002* *Guide to the implementation and auditing of BS 7799 controls,*
- *PD 3005:2002* *Guide on the selection of BS 7799 controls.*

CSN ISO/IEC TR 13335-1:1999

Information technology- Management of information and communications technology security – Part 1: Concepts and models for IT security.

CSN ISO/IEC TR 13335-2:2000

Information technology- Management of information and communications technology security – Part 2: Managing and planning IT security.

CSN ISO/IEC TR 13335-3:2000

Information technology- Management of information and communications technology security - Part 3: IT security equipment.

CSN ISO/IEC TR 13335-4:2002

Information technology- Management of information and communications technology security - Part 4: Selection of safeguards.

CSN ISO/IEC TR 13335-5 (not yet issued)

Information technology- Management of information and communications technology security - Part 5: Protective measures for external connections.

Other information security standards:

CSN ISO/IEC 15408-1:2001

Information technology- Security techniques - Evaluation criteria for IT security– Part 1: Introduction and general model.

CSN ISO/IEC 15408-2:2002

Information technology- Security techniques - Evaluation criteria for IT security– Part 2: Security functional requirements.

CSN ISO/IEC 15408-3:2002

Information technology- Security techniques - Evaluation criteria for IT security– Part 3: Security assurance requirements.

CSN ISO/IEC 15816:2003

Information technology- Security techniques - Security information objects for access control.

CSN ISO/IEC 9126-1:2002

Software engineering – Product quality - Part 1: Quality model.

CSN ISO/IEC 14598-1:2000

Information technology- Software product evaluation - Part 1: General overview.

CSN ISO/IEC 14598-2:2002

Software engineering - Product evaluation - Part 2: Planning and management.

CSN ISO/IEC 14598-3:2001

Software engineering - Product evaluation - Part 3: Process for developers.

CSN ISO/IEC 14598-4:2001

Software engineering - Product evaluation - Part 4: Process for acquirers.

CSN ISO/IEC 14598-5:1999

Information technology- Software product evaluation - Part 5: Process for evaluators.

CSN ISO/IEC 14598-6:2002

Software engineering - Product evaluation - Part 6: Documentation of evaluation models.

CSN ISO/IEC 12207:1997(2003 print change)

Information technology- Software life cycle processes.

CSN ISO/IEC 12119:1996

Information technology- Software packages – Quality requirements and testing.

CSN ISO/IEC 2382-8:2001

Information technology– Vocabulary – Part 8: Security.

CSN ISO/IEC TR 14 516:2004

Information technology- Security techniques - Guidelines for the use and management of Trusted Third Party services.

CSN ISO/IEC 10736:1998

Information technology- Telecommunication and information exchange between systems – transport layer security protocol.

CSN ISO/IEC 10181-1:1998

Information technology- Open Systems Interconnection - Security frameworks for open systems: Overview.

CSN ISO/IEC 10181-2:1998

Information technology- Open Systems Interconnection - Security frameworks for open systems: Authentication framework.

CSN ISO/IEC 10181-3:1998

Information technology- Open Systems Interconnection - Security frameworks for open systems: Access control framework.

CSN ISO/IEC 10181-4:1999

Information technology- Open Systems Interconnection - Security frameworks for open systems: non-repudiation framework.

CSN ISO/IEC 10181-5:1999

Information technology- Open Systems Interconnection - Security frameworks for open systems: Confidentiality framework.

CSN ISO/IEC 10181-6:1999

Information technology- Open Systems Interconnection - Security frameworks for open systems: Integrity framework.

CSN ISO/IEC 10181-7:1999

Information technology- Open Systems Interconnection - Security frameworks for open systems: Security audit and alarms framework.

CSN ISO/ IEC 9797:1997

Information technology- Security techniques – Data integrity mechanisms using cryptographic control functions with algorithm blocking ciphers.

CSN ISO IEC 9797-1:2001

Information technology- Security techniques - Message authentication codes (MACs) - Part 1: Mechanisms using a block cipher.

CSN ISO/IEC 9798-1:1997

Information technology- Security techniques - Entity authentication – Part 1: General.

CSN ISO/IEC 9798-2:2000

Information technology- Security techniques - Entity authentication - Part 2: Mechanisms using symmetric encipherment algorithms.

CSN ISO/IEC 9798-3:1997

Information technology- Security techniques - Entity authentication - Part 3: Entity authentication using public key algorithms.

CSN ISO/IEC 9798-4:2001

Information technology- Security techniques - Entity authentication - Part 4: Mechanisms using a cryptographic check function.

CSN ISO/IEC 9798-5:2001

Information technology- Security techniques - Entity authentication - Part 5: Mechanisms using zero-knowledge techniques.

CSN ISO/IEC 11770-1:1998

Information technology- Security techniques - Key management - Part 1: Framework.

CSN ISO/IEC 11770-2:1999

Information technology- Security techniques - Key management - Part 2: Mechanisms using symmetric techniques.

CSN ISO/IEC 11770-3:2002

Information technology- Security techniques - Key management - Part 3: Mechanisms using asymmetric techniques.

CSN ISO/IEC 15945:2004

Information technology- Security techniques - Specification of TTP services to support the application of digital signatures.

CSN ISO/IEC 13888-1:2001

Information technology- Security techniques - Non repudiation - Part 1: General.

CSN ISO/IEC 13888-2:2001

Information technology- Security techniques - Non repudiation - Part 2: Mechanisms using symmetric techniques.

CSN ISO/IEC 13888-3:2001

Information technology- Security techniques - Non repudiation - Part 3: Mechanisms using asymmetric techniques.

CSN EN ISO 19011:2003

Guidelines for quality and/or environmental management systems auditing.

General Principles

Security aims, security policies and all activities involved with information security must support the strategic aims of an organisation.

Security resolution must be supported by an organisation's top management.

Security is a comprehensive and dynamic issue. It is a single concept which cannot be broken down into parts.

Information security processes are implemented using the PDCA model Plan - Do - Check - Act.

Security is a continuous process due to constantly changing environments.

Security cannot be limited only to information systems (IS) or information and communication technology (ICT). It must cover all aspects, including organisational procedures and the behaviour of individuals.

Security must cover all its parts, which must all be paid the same attention. One element cannot be left as being the weakest point which would then be the most vulnerable to attack.

Security cannot be 100% assured (there will always be residual risk)

Cost spent on security must be proportional to the value of the protected assets (or the level of risk).

Information security solutions are always unique and cannot be transferred on a 1:1 basis from an (albeit very similar) organisation, as two identical organisations which would have identical security environments do not exist (e.g. there are different locations, employees, information systems, processes, technology used etc.).

Each organisation will have different information security solutions with varying degrees of security, including required documentation (there is a different scope for an organisation with 3 employees with its accounts on a PC which is not connected to the internet and another company with 3,000 employees and a number of regional offices and an extensive information system).

Information Security Management Recommendations

In order to achieve sufficiently effective information security it must be seen as being a managed process which is balanced in all areas, which has the support of the management and which respects the organisation's culture.

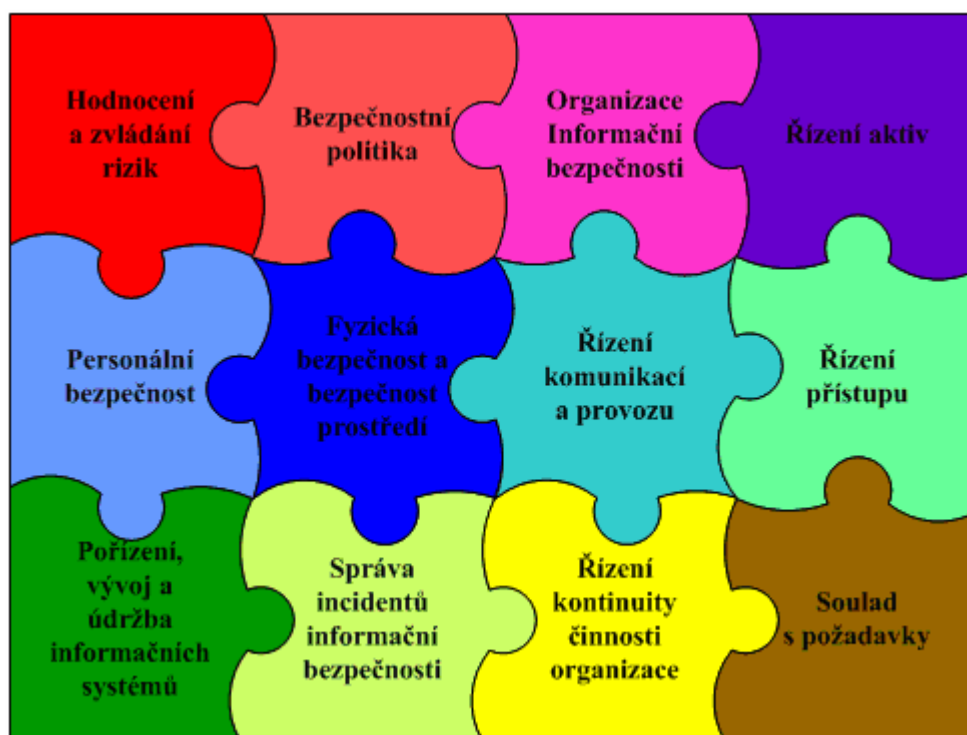
Each information and communication system user must be acquainted with information security organisation structures and rules (via guidelines). There must be a system of education and training in the field so that each employee can understand the purpose of the various security measures.

The scope and structure of information security management depends on a number of objective elements (an organisation's size, geographic location, the scope and significance of the information and communication systems and the information and communications technology used etc.) This is the main reason why best practice (standards and recommendations) are applied when implementing information security and why a universal solution cannot be used. Generally speaking, when an information security system is being built, it must be based on analyses of the actual status and the actual risks.

Information security management recommendations are based on the CSN ISO/IEC 17799:2005 and CSN BS 7799-2:2004 standards which are set out in the 12 areas of information security below. The implementation processes for information security systems management is described in the following section of this annex.

Figure:

*Risk assessment and management Security policy Information security organisation Asset management
Personnel security Physical and environmental security Communications and operations management Access control
Procurement, development and maintenance of information systems Information security incident management Business continuity management
Compliance*



1) Introduce Risk Management as a Part of Information Security Management

Risk management is made up of a process which includes the systematic process of risk assessment and its subsequent management. Part of the process is to identify the various threats and the ensuing risks. Risk management must be an inseparable part of the overall information security management. This means that risks are monitored and assessed, risk minimisation counter-measures are proposed and residual risk is accepted.

2) Have a Security Policy

A security policy contains an information security goal and a method for achieving this goal. The policy also briefly sets out the connection the information security management system has to the organisations' aims and the regulatory requirements arising from standards and the relevant legislation. Defining basic responsibilities for creating the information security management system and setting the criteria for risk assessment are also important parts of a security policy.

A security policy covers the following areas of information security:

- a) Security organisation and management;
- b) Asset management;
- c) Personnel security;
- d) Physical and environmental security;
- e) Communications and operations management;
- f) Access control;
- g) Information system procurement, development and maintenance;
- h) Information security incident management;
- i) Business continuity management;
- j) Compliance.

3) Managing Information Security

The task of information security management is to set out rules and measures for managing an organisation's information security. The organisation's management structure and the responsibilities of managers at all levels must be clearly set out. The management organisation, information security responsibilities of managers at all levels and technical bodies must be described clearly along with the roles in the information security system.

Some possible special roles:

Information systems guarantor – mainly managers responsible for specific information systems or subsystems.

Asset (information) owners – the person who administers specific information and communication assets.

Information security manager – a manager for information security whose main task is to organise, manage and supply technical information security tasks.

Information system security administrator – a technical employee for information security whose main task is to perform technical tasks connected to information security.

Security coordinator – a chosen information system user or administrator who works with the security manager and the security administrator in implementing the security policy and security measures (e.g. for geographically extensive information systems).

Information and communications technology systems administrator – an appointed employee whose task is the administration, service and maintenance of information and communication technology systems.

Information system users – a person who has the right to use an information and communication system of an organisation under defined conditions, and in particular who may use and request information from these systems.

Information systems auditor – an expert for performing inspections of information and communication systems, whose main tasks is to perform activities related to the independent auditing of information and communication systems administration, the security of these systems and checks that security is being upheld by users.

The following roles can be defined in documentation:

Approver - an employee authorised to approve and issue documents.

Coordinator – an employee responsible for drafting, maintaining documents, and making sure the content is correct – *the document owner*.

Compiler – an employee responsible for drafting proposals and performing the corrections and comments process.

Opposer – employee appointed to participate in the corrections and comments process.

Recipient – employee for whom the document is intended and who is obliged to respect its content.

Administrator – employee responsible for filing and distributing documents in both written and electronic form.

4) Managing Assets

Asset management involves defining a method of identifying an organisation's assets, and then identifying and assessing these assets. A register of the assets contained in information and communication systems should be maintained in order to provide thorough asset protection. This register is also important from a risk management perspective.

Each important asset should have an assigned owner who is responsible for setting reasonable measures for protecting it in accordance with the regulations issued within the organisation.

5) Paying Sufficient Attention to Personnel Security

Personnel security involves setting and implementing security rules and procedures for human resources management. Individuals and their actions present a significant threat to information security, either through basic human errors or malicious intent. Resolving personnel security will reduce the risks involved with human manipulation and should be included in the overall human resources management process, from the moment of recruitment, throughout the employment period and until after this has been completed.

6) Resolving Physical Security

The purpose here is the physical protection of assets.

Security zones (perimeters) should be set up, with rules for the procedures and behaviour allowed in these defined (so-called regime guidelines). The security of each separate piece of equipment and environment should also be dealt with for their entire life-cycles (from procurement to liquidation) both in terms of the relevant building and outside it (e.g. for portable computers and media).

7) Managing Communications and Operations

Communications and operations management involves defining the basic framework for secure communications and operations management. The secure operation and communication of information and communication technology should be described in operational and operative documentation:

- Operational procedures;
- Security incident resolution procedures;
- Operations and technical logbooks;
- Equipment cards;
- Security incidents and insufficiencies logbook.

Any changes performed to equipment used to process information must be subject to managed processes. The principles of separate obligations and separating development from operation should be respected.

A suitable method for using operational and technical logbooks will serve as the basis for planning updating and capacity issues for new information and communication systems.

Protection from malicious software, integrity administration, accessibility, communications network administration, information carrier handling (media) and information exchange (transfer) also belongs under operational security.

8) Managing Access to Systems

This process, which includes all phases of the user access life-cycle (registration – changes – cancellation) involves preventing unauthorised access to information and communication systems.

Access to information must be clearly set out for each user based on their work duties (based on the role they have in the information system) according to rules and operational requirements (the “need to know” principle). Closer attention needs to be paid to privileged users, who administer passwords and control access rights, access to network equipment, operational and application systems and portable computer equipment, and to the systematic monitoring of the entire system.

Each user must know their obligations and responsibilities in relation to access to information and communication systems.

9) Paying Sufficient Attention to Procurement, Development and Maintenance

Procuring, developing and maintaining information systems involves managing the life-cycle of equipment and systems used for processing an organisation's information in accordance with their security requirements and needs. Security issues must be considered at the phase when requirements are specified when infrastructure and application equipment is being developed and maintained. Attention must be paid to cryptographic measures, system files and development and maintenance processes.

10) Resolving Security Incidents and Insufficiencies

Information security incident administration involves ensuring that such events and the weaknesses in information systems are communicated in way that enables faults to be corrected in time. Any incidents or insufficiencies must be recorded and investigated taking into account the causes so that the faults can be corrected.

11) Managing Continuity Administration

Managing the continuity of an organisation's activities involves preventing a stoppage in these activities and protecting against or minimising the consequences of serious errors or disasters. It is made up of a system of measures aimed at preparing adequate reactions in the event an organisation's core activities are threatened. Continuity management includes a system of documentation, testing, reviews and the distribution of proposed measures together with the assignment of the corresponding authority. A management process should be implemented which is made up of plans of procedures and the maintenance of these plans. They should be regularly tested and updated (reassessed) on the basis of these tests.

12) Ensuring Compliance with Standards and Legislation

Ensuring compliance with legislation and regulatory standards serves to warn against any breaches of the criminal, commercial or civil codes, legal or contractual obligations and security requirements when implementing security and technological measures within an organisation. Compliance with the law (legal and sub-legal standards) and other binding documents must be ensured by recording the various obligations and performing analyses on their ensuing requirements.

Implementing Information Security Management Systems

An information security management system is created and managed in accordance with the CSN BS 7799-2:2004 standard – Management Systems for Information Security – specifications with instructions for use.

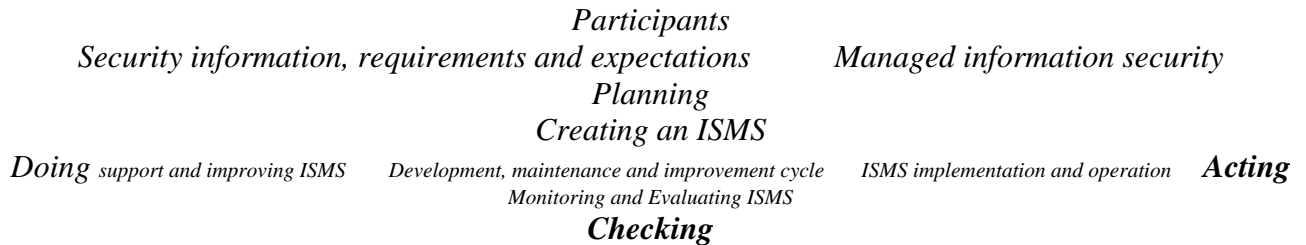
It makes up a part of an organisation’s management activities with its main objective being to eliminate or reduce the risks related to possible breaches to the integrity, accessibility and credibility of an organisation’s information.

Implementing and ISMS (Information Security Management System) pursuant to the BS 7799-2:2002 standards are performed using the PDCA model (Plan - Do - Check - Act), which divides the whole process into four steps making a closed management cycle:

- Step one – Planning;
- Step two - Doing;
- Step three - Checking;
- Step four – Acting.

Figure:

PDCA Model Applied to ISMS Processes



PDCA model aplikovaný v procesech ISMS

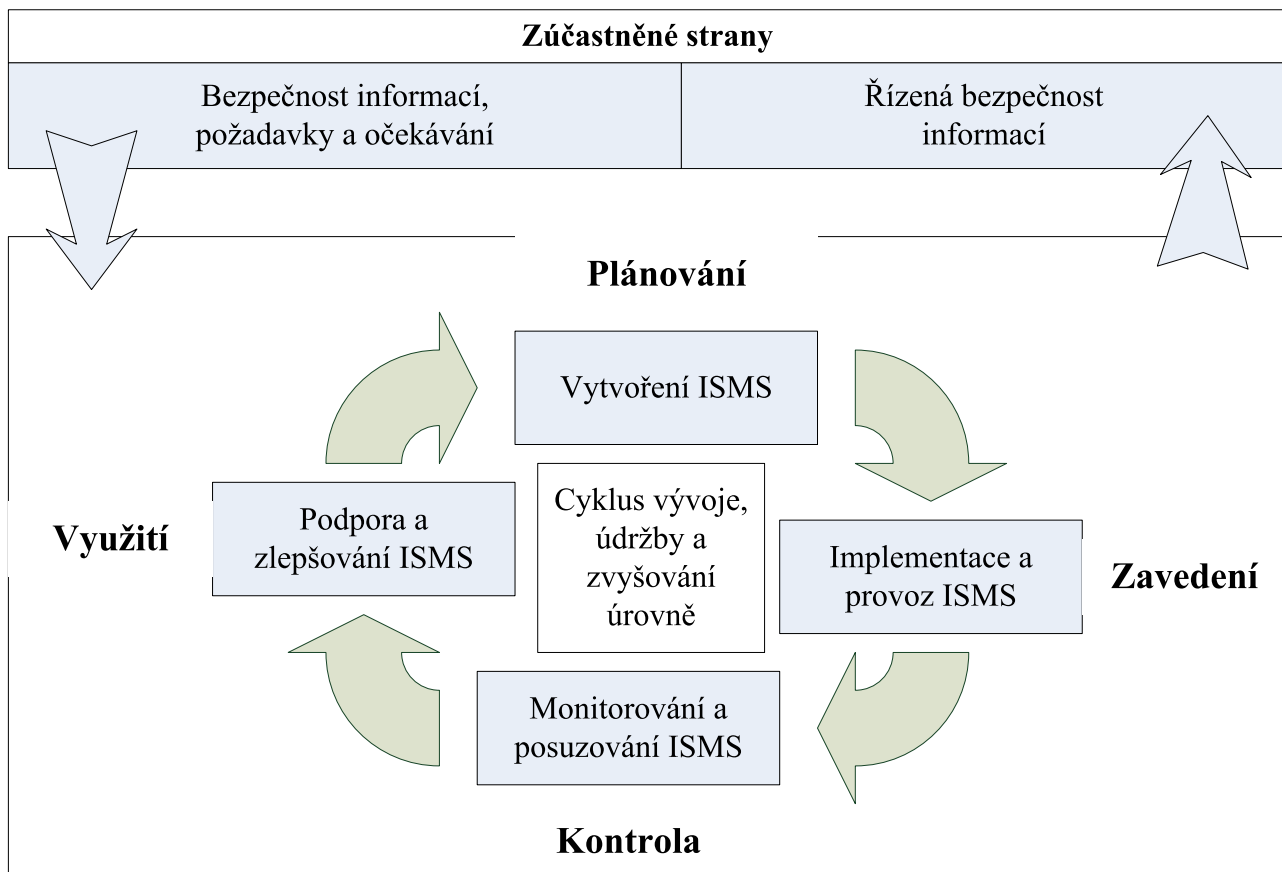


Figure 1

- **Step one - Planning**

Planning is the foundation of creating an information security management system. This step includes setting security policies, plans, objectives and procedures related to risk management and improving information security so that these provide results which correspond to an organisation's objectives. The objective is to set parameters for creating an ISMS to a defined scope which is based on a risk assessment.

The following activities are performed as part of Planning:

- Definition of the scope of the information security management system;
- Definition of the security policy;
- Risk identification and assessment;
- Asset identification and assessment;
- Threats and vulnerability identification and assessment;
- Existing risk assessment;
- Selection of objective measures and individual measures (controls) for risk coverage;
- Preparation of the Applicability Declaration.

• **Step two - Doing**

As part of the implementation of the information security management system, selected information security measures will be put into practice.

These measures will be described and employees will be acquainted with them. An inseparable part of this step is to create a system of detection and reaction to security incidents which could jeopardise information.

The objective is to implement, record and manage selected security measures (controls) and acquaint employees with these measures.

The following activities will be performed as part of implementation:

- Drafting and implementation of risk management;
- Implementation of measures (controls) pursuant to the organisation's requirements;
- Implementation of programmes for increasing security awareness;
- Management of available resources;
- Operations management – implementation of procedures for administering documents and records;
- Implementation of procedures for early detection of security incidents and rapid reaction.

• **Step three - Checking**

Checking the information security management system ensures that errors are detected and that incidents are identified and provides a basis for assessing the effectiveness and efficiency of the system in operation.

For this purpose a system of controls and internal audits of the information security is implemented. The system of controls assesses the coverage of ascertained risks of the security procedures and rules implemented throughout the organisation. The internal audit system is included into the organisation's internal audit system.

The objective is to ensure the validity of the proposed information security management system and the effective coverage of ascertained risks by the measures.

The following activities should be performed as part of implementation:

- Security incident detection and monitoring of the effectiveness of information security measures;
- Regular assessment of the effectiveness of information security measures;
- Regular reviews of residual and acceptable risks;
- Regular internal audits of information security ;
- Regular reassessments of the information security management system at an organisation's management level;
- Recording of events that impact on the effectiveness and efficiency of the information security measures.

• **Step four - Acting**

Acting closes the cycle of implementing, operating and maintaining the ISMS. Remedial and preventive activities are performed on the information security processes as part of this step, based on

the already performed controls and audits. Any identified possibilities to improve the management system should also be implemented.

The objective is to eliminate any inconsistencies in the management system and implement more efficient processes and further improve the system's implementation.

The following activities should be performed as part of implementation:

- Implementation of ascertained possibilities of optimising the information security management system;
- Adoption of suitable remedial and preventative measures;
- Discussion of results with all interested parties;
- Checks to see if the planned objective was achieved by the applied improvements.

Information security management system implementation means that:

- a) Individual areas are described in the security policy,
- b) Individual areas are described as processes,
- c) Processes are implemented,
- d) Processes are tested,
- e) Individual processes make up integral parts of the management process.

Other Recommendations

- Managing information security should be separated from managing information and communication technology due to a conflict of interest. It should be joined to managing physical security, for example.
- The accumulation of incompatible roles should be restricted, for example information system administration and controls.
- Separate development, operations, security and controls of information and communication systems.
- Introduce control rules ("four eyes") for important activities so that they are not performed by a single person.

Main Processes for Managing the Life-Cycle of Security Documentation

A complete set of security documentation must exist which covers the entire life cycle of an organisation's information and communication systems and all their activities.

In order for this set of documents to fulfil the requirements of a manageable system it must:

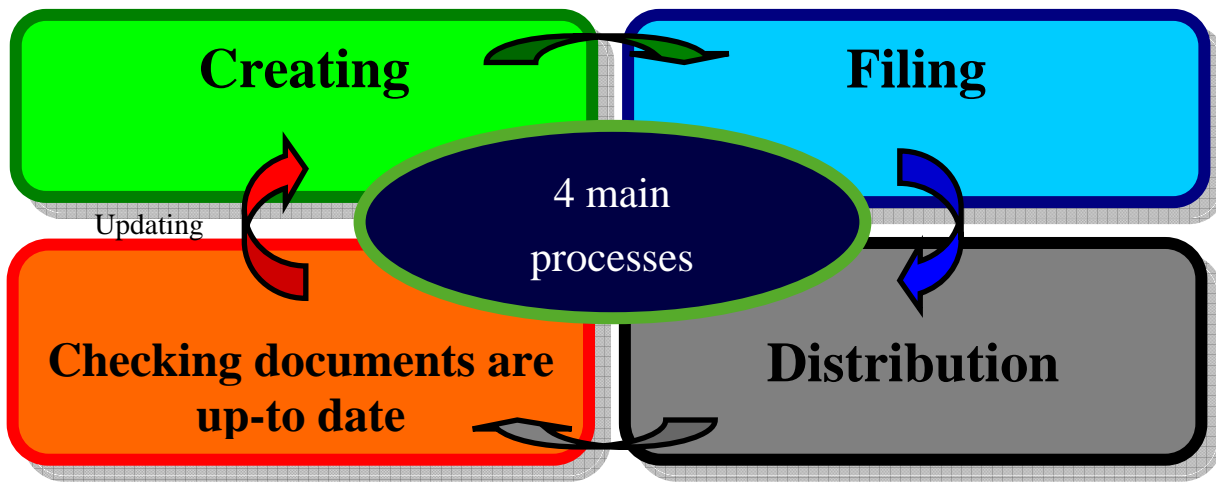
- Have all documents clearly identified,
- A uniform record system for the documentation,
- A defined role in the management system, and its sphere of activity and responsibility,
- A defined process of managing the life-cycle of these documents.

Reasons for maintaining proper documentation:

- The higher the quality of the documentation, the higher the quality of the materials used for decision-making and managing.
- Quality changes cannot be made without processes being described correctly.
- Activities which are documented (described) will be performed in a shorter time in the future (they are repeated), will be performed better and will not be so demanding of the qualifications of workers.
- Investment protection by enabling substitution (in cases of illness, holidays, termination of employment, etc.)
- Properly maintained documentation is a pre-requisite for a successful audit.

Security documentation contains mostly sensitive information and must therefore be handled, stored and distributed with due attention.

Creation, Filing, Distribution, Checking Documents are up-to-date.



Types of Documentation

Documentation is generally divided into three classes (levels) in order to make management more efficient:

1. **Mandatory regulations** (*external* – generally binding and *internal* – representing the management’s will),
2. **Standards** (these are also external and internal; unlike regulations they are not directly binding, but can become so if they are referred to in binding regulations),
3. **Records** (documenting management system compliance with regulations and standards).

Examples of types of document:

Internal information security standards:

The overall security policy

The security policy for information systems (IS/ICT)

Methodology instructions for users

Methodology instructions for user administration and access management

Methodology instructions for information owners

Methodology instructions for system failure planning

Methodology instructions for applying security aspects in contracts

Principles for managing information and communication systems development and changes

(project documentation)

System Security Policy (*for individual key IS – “subsystems”*)

Security handbook for security administrators

Security handbook for system administrators

Security handbook for users

Operational security documentation:

Regime guidelines for security zones

Guidelines for premises security

Guidelines for handling incidents

System failure plan

Backup and recovery plan

Training and educational textbooks

Operational security documentation (records):

Assigning/changing access rights

Security incident logbook

Registry of information and communication assets

Operations logbook

Equipment card

IS Security Plans

The following plans should be set up for IS security:

- Risk Mitigation Plan

The risk mitigation plan describes procedures for reducing any ascertained risks to the required level. It contains a description of the ways of implementing individual measures and security projects which will achieve the objectives defined in the security policy. Measures are defined for each project with the following minimum criteria: critical value, implementation time, responsibility, expected costs outputs and any potential further steps.

- Continuity Preservation Plan (main activities)

This is a plan which should ensure that main activities will continue to function (e.g. without the support of information and communications technology).

- Backup and Recovery Plan

This plan describes the process of regular operational backing up (data, programmes and settings) including descriptions of recovery using the backup (e.g. recovery procedures after faulty implementation of service repairs to operating systems).

- System Failure plan (for individual IS) + map of all system failure plans

Plans which deal with various types of failure for individual IS. The overall map of these plans is important for setting out which parts of information and communication systems need to be put back into operation first as they affect the other parts (e.g. in order to use e-mail the first thing is to set up a connection to the internet, and then the local network, all the necessary network services and only then can the postal server and end-user programme be dealt with). This map also sets out priorities for IS recovery as a whole.

- Testing Plan for the System Failure Plan

The system failure plan must be regularly tested and the plan then reassessed using the test results.

- Security Education and Training Plan

It is recommended to set up an information security education and training plan (for individual IS roles) so the training is provided systematically.

- IS Audit Plan

Various types of checks should be included in this plan, for example regular operational checks, internal and external audits and penetration tests.