Dr Ryszard Kossowski

Standardy w zarządzaniu bezpieczeństwem IT

Przedsięwzięcie, w którym MUSIMY uwzględnić aspekt bezpieczeństwa. Jakie kroki powinniśmy podjąć?
1. Polityka bezpieczeństwa
2. Rozpoznanie zagrożeń (najlepiej wszystkich)
3. Analiza ryzyka
4. Zaprojektowanie zabezpieczeń.

Jak możemy podejść do projektu zabezpieczeń?
1. Projektować samemu
2. Kupić gotowe rozwiązania (lepiej ogłosić przetarg)
3. Przy kupowaniu wymagać certyfikatów

Skąd się biorą certyfikaty?
1. Producent (hardware'owego lub software'owego) urządzenia korzysta ze znormalizowanych rozwiązań. Takie rozwiązania mogą być tańsze i spełniające wyższe wymagania aniżeli rozwiązania własne
2. Producent zgłasza urządzenie do laboratorium uprawnionego do analizy i wydania certyfikatu uznawanego możliwie jak najszerzej
3. Laboratorium, w oparciu o sugestie producenta i znormalizowane kryteria, przeprowadza badania i ewentualnie wydaje certyfikat

Godnym podkreślenia są następujące zalety takiego podejścia
1. Obniżenie kosztów
2. Gwarancja najwyższej jakości według aktualnie znanej wiedzy
3. Kompatybilność i zamienność
4. Delegowanie odpowiedzialności na laboratorium wydające certyfikat

Wymagania rynku
e-Commerce = Internet + Electronic Business + Security Techniques
m-Commerce = Internet + Mobility + Electronic Business + Security Techniques
Standaryzowane techniki bezpieczeństwa zaczynają być obowiązkowymi wymaganiami w elektronicznym handlu, opiece zdrowotnej, i wielu innych obszarach zastosowań.

Cztery globalne instytucje
The International Electrotechnical Commission (IEC)
– http://www.iec.ch
The International Organization for Standardization (ISO)
– http://www.iso.org
The International Telecommunication Union (ITU)
– http://www.itu.int
The United Nations Economic Commission for Europe (UN/ECE)
– http://www.unece.org/cefact

Instytucje standaryzacyjne działają w ramach międzynarodowego porozumienia
• IEC i ISO są "rodzicami" JTC1 w standardach IT

• ISO, IEC i ITU każda ma grupy techniczne opracowujące standardy dla e-business
• UN/ECE obejmuje również kraje z poza Europy, takie jak Kanada i USA
• UN/ECE jest “rodzicem” UN/CEFACT – UN’s Centre for Trade Facilitation and Electronic Business

Zestawienie standardów

INTERNATIONAL STANDARD ISO/IEC 17799-1 Information security management — Part 1: Code of practice for information security management

BS 7799-2:2002 Information security management systems - Specification with guidance for use

BS 7799-3:2006 Information security management systems – Part 3: Guidelines for information security risk management

ISO/IEC 13335-1 Information technology — Security techniques — Management of information and communications technology security —
Part 1: Concepts and models for information and communications technology security management

ISO/IEC 1st CD 13335-2 Information technology – Security techniques – Management of information and communications technology security –
Part 2: Information security risk management

ISO/IEC TR 13335-3, Information technology - Guidelines for the management of IT Security (GMITS) –
Part 3: Techniques for the management of IT Security

ISO/IEC WD 13335-4, Information technology - Security techniques - Guidelines for the management of IT Security (GMITS) –
Part 4: Selection of safeguards

ISO/IEC PDTR 13335-5 Information technology – Security techniques – Guidelines for the management of IT security –
Part 5: Management guidance on network security

INFORMATION SECURITY MANAGEMENT SYSTEMS

The ISO/IEC 27000 information security management systems (ISMS) family of standards listed below has been developed to assist organizations, of all types and sizes, to implement and operate effective ISMS.
— ISO/IEC 27000 provides an overview and specifies the terminology for the ISO/IEC 27000 ISMS family of standards.

— ISO/IEC 27001 specifies requirements for an information security management system where an organization needs to demonstrate its ability to protect information security assets and give confidence to interested parties.
— ISO/IEC 27002 provides implementation guidance that can be used when designing controls for achieving information security.
— ISO/IEC 27003 provides practical guidance for implementing an information security management system based on ISO/IEC 27001.
— ISO/IEC 27004 provides guidance and advice on the development and use of measurements in order to assess the effectiveness of ISMS, control objectives, and controls used to implement and manage information security, as specified in ISO/IEC 27001.
— ISO/IEC 27005 provides guidelines for an organization to define their approach to risk management to address the requirements in ISO/IEC 27001.
— ISO/IEC 27006 provides requirements for bodies providing audit and certification of information security management systems.
— ISO/IEC 27007 provides guidance on the principles of auditing, managing audit programmes, conducting quality management system audits and environmental management system audits, as well as guidance on the competence of quality and environmental management system auditors.
— ISO/IEC 27010 Information security management for intersector and inter-organisational communications
This International Standard is a specialist supplement to ISO/IEC 27001 and ISO/IEC 27002 for use by information sharing communities. The guidelines contained within this International Standard are in addition to and complement the implementation guidance given in the ISO/IEC 27000 family of standards.
— ISO/IEC 27011 provides an implementation baseline of ISM within telecommunications organizations to ensure the confidentiality, integrity and availability of telecommunications facilities and services.
— ISO/IEC 27013 Guidelines on the integrated implementation of ISO/IEC 27001 and ISO/IEC 20000-1
The relationship between information security and service management is so close that many organizations already recognize the benefits of adopting both sets of standards. It is common for an organization to adopt one standard, improve the way it operates to comply with the requirements of that standard, and then make further improvements to conform to the requirements of the other.
There are a number of advantages in implementing an integrated management system which takes into account both the services provided, and the protection of information assets. These benefits can be experienced whether one standard is implemented before the other, or both standards are implemented simultaneously. Management and organizational processes, in particular, can derive benefit from the similarities between the standards and their common objectives.
— ISO/IEC 27014 Governance of information security
This International Standard provides guidance on the governance of information security. The governing body, as part of its governance responsibilities, is increasingly required to oversee information security to ensure the objectives of the organization are achieved.
— ISO/IEC 27015 Information security management guidelines for financial services
Continuous developments in information technology have led to an increased reliance by organizations providing financial services on their information processing assets. Consequently, management, customers and regulators have heightened expectations regarding effective information security protection of these assets and information.

— ISO/IEC 27016 Information security management – Organizational economics
A successful information security management (ISM) requires a strongly integrated understanding of both the technical (i.e. balance of risk and security) and economic (i.e. balance of benefit and cost) approaches in all aspects of its inception, design, implementation, management, improvement, and retirement. Relying only on a technical approach through the use of controls (i.e. encryption, access and privilege management, firewalls and, intrusion and malicious code eradication) without the incorporation of an understanding as to the economic value supporting the technical approach will not always provide an appropriate level of protection to the information assets of an organization. Information security management needs to adopt a risk management approach whereby by both the technical and economic aspects are considered in unison.
— ISO/IEC 27031 provides business continuity management as an integral part of a holistic risk management process that safeguards the interests of an organization's key stakeholders, reputation, brand and value creating activities through:

a) identifying potential threats that may cause adverse impacts on an organization's business operations, and associated risks;
b) providing a framework for building resilience for business operations;
c) providing capabilities, facilities, processes, action task lists, etc., for effective responses to disasters and failures.

— ISO/IEC 27032 Cybersecurity is the collection of tools, policies, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect organization and user's assets on the cyber environment. Organization and user's assets include connected computing devices, computing users, applications/services, communications systems, multimedia communication, and the totality of transmitted and/or stored information in the cyber environment.
— ISO/IEC 27033 consists of the following parts, under the general title *Information technology — Security techniques — Network Security*:
— *Part 1: Overview and concepts,*
— *Part 2: Guidelines for the design and implementation of network security,*
— *Part 3: Reference networking scenarios – Risks, design techniques and control issues,*
— *Part 4: Securing Communications between networks using security gateways - Risks, design techniques and control issues,*
— *Part 5: Securing communications across networks using Virtual Private Networks (VPNs) - Risks, design techniques and control issues,*
— *Part 6: IP convergence*
— *Part 7: Wireless*
— ISO/IEC 27032 Security techniques – Guidelines for cybersecurity
This International Standard gives guidelines for stakeholders to establish baseline security practices for Cyberspace and provides a framework for information sharing, coordination and incident handling.
— ISO/IEC 27034 provides guidelines for application security - specify an application security life cycle, incorporating the security activities and controls for use as part of an application life cycle, covering applications developed through internal development, external acquisition, outsourcing/offshoring[1], or a hybrid of these approaches.

— ISO/IEC 27035 provides the information and guidance for any organization to implement and maintain a quality approach for information security incident management.
— ISO/IEC 27036

ISO/IEC 27036-1 consists of the following parts, under the general title *Information technology — Security techniques — Information security for supplier relationships.*

- *Part 1: Overview and concepts*
- *Part 2 Generic requirements [Co-editor's note: potential change of title not officially requested.]*
- *Part 3: ICT Supply Chain Security*
- *Part 4: Outsourcing [Co-editor's note: co-editor assignment to be determined.]*
- *Part 5: Cloud Computing [Co-editor's note: co-editor assignment to be determined.]*
- *Part 6: TBD [Co-editor's note: title and co-editor assignment to be determined.]*

This International Standard provides further detailed implementation guidance on the controls dealing with supplier relationships that are described as general recommendations in ISO/IEC 27002.

— ISO/IEC 27037 Security techniques – Guidelines for identification, collection, acquisition and preservation of digital evidence

This International Standard provides guidelines for specific activities in the handling of digital evidence, which are identification, collection, acquisition and preservation of digital data that may be of evidential value (i.e. potential digital evidence). These steps are required in an investigation process which is designed to maintain the integrity of the digital evidence – an acceptable methodology in obtaining digital evidence will ensure its admissibility in meeting its purposes.

— ISO/IEC 27038 Security techniques -- Specification for digital redaction

The redaction of born-digital documents is a relatively new area of document management practices, and raises unique issues and potential risks. Where electronic documents are redacted, removed information must not be recoverable. Hence, care needs to be taken so that redacted information remains hidden within non-displayable portions of bit streams. This international standard specifies methods for digital redaction of digital documents as well as a testing methodology for evaluating the functionality of these functions.

—ISO/IEC 27040 Storage security: provides further detailed implementation guidance on the storage security controls that are described at a basic standardized level in ISO/IEC 27002.

The objectives for this international standard are to:
help draw attention to the risks,
assist organizations in better securing their data when stored,
provide a basis for auditing storage security controls.

—ISO/IEC Security techniques – Vulnerability disclosure

A vulnerability is a weakness of software, hardware, or online service that can be exploited. Vulnerabilities can be caused by software and hardware design flaws, poor administrative processes, lack of awareness and education, and advancements in the state of the art or improvements to current practices. Regardless of cause, an exploitation of such vulnerabilities may result in real threats to mission-critical information systems.

—ISO/IEC 30111 -- Information technology -- Security techniques – Vulnerability handling processes

This International Standard describes processes to handle reports of potential vulnerabilities in products and
online services. The audience for this standard includes consumers, developers, vendors, and evaluators of secure IT
products.

— ISO/IEC 29146 -- Information technology -- Security techniques – A framework for access management

An access management framework needs to establish the following components, which are critical to the success of an organization's access management solution:

Access relationships that may be based on the identity of an entity in a context, or may be based on whether an entity meets other criteria (such as membership of a group of entities).

Access management operations concerns establishment of such relationships and their types, including authenticating and monitoring the access, accountability, suspension (optional) and termination of the relationship itself.

Enforcing organizational access policies *by means of linking* directly the main processes *who users are (identification and authentication) and what users can do (authorization).*

The principles given in the OECD Guidelines for the Security of Information Systems and Networks [1] apply throughout the ISO/IEC 27000 ISMS family of standards. A short overview of these OECD principles is as follows:

(1) Awareness of the need for information security.
Świadomość potrzeby bezpieczeństwa informacji.

(2) Responsibility assignment of information security.
Przypisanie odpowiedzialności za bezpieczeństwo informacji.

(3) Response to and detect information security incidents.
Reagowanie aby zapobiegać i wykrywać incydenty bezpieczeństwa informacji.

(4) Ethics respecting legitimate interests.
Problemy etyczne uwzględniające prawne korzyści.

(5) Democracy to ensure information security is compatible with society values.
Demokracja dla zapewnienia, że bezpieczeństwo informacji daje się pogodzić z wartościami społeczeństwa

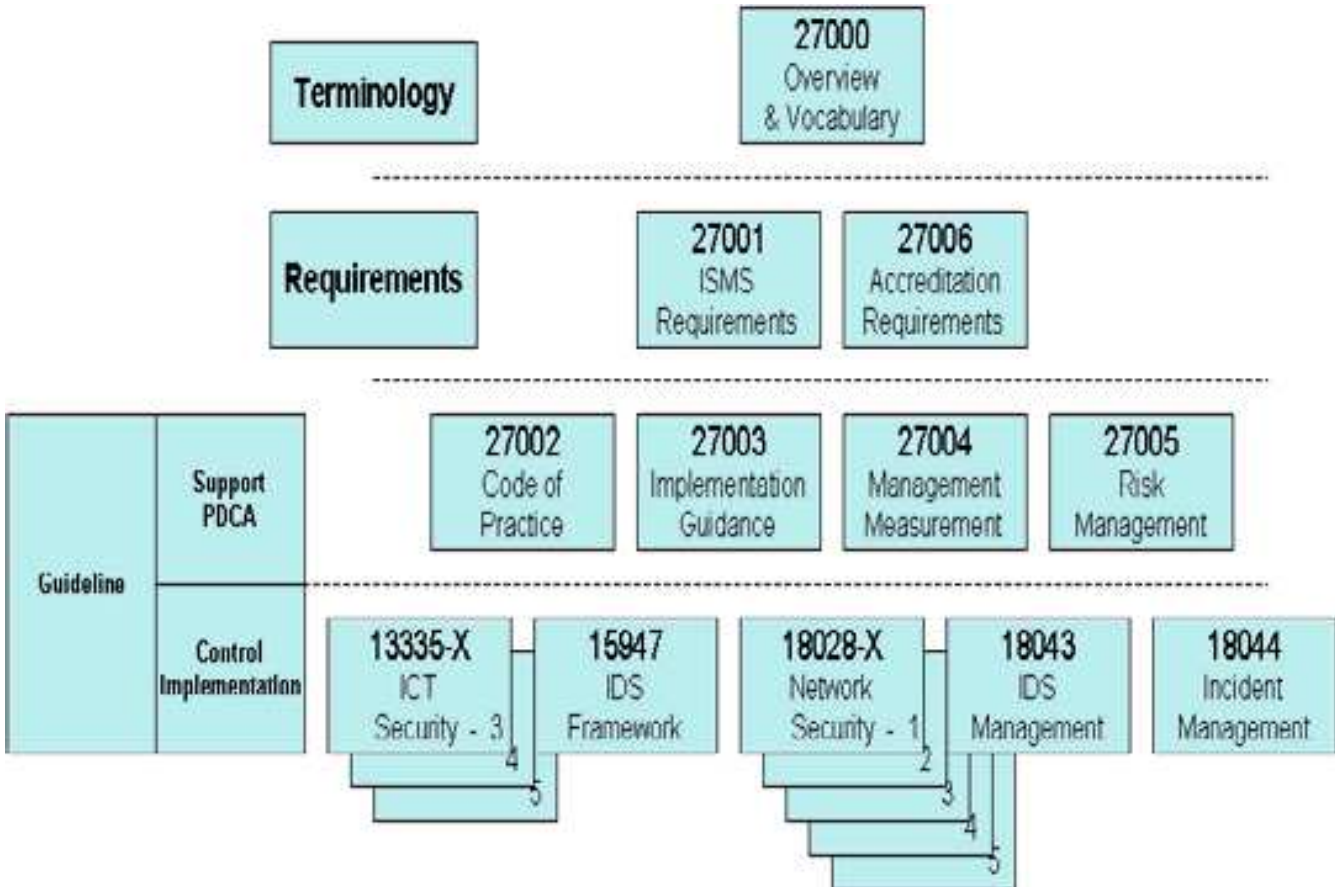
(6) Risk Management providing levels of assurance towards acceptable risks.
Zarządzanie Ryzykiem gwarantujące poziomy pewności względem akceptowalnych ryzyk.

(7) Security design and implementation incorporated as an essential element.
Projekt i implementacja włączone jako element zasadniczy.

(8) Security management ensuring a comprehensive approach.
Zarządzanie bezpieczeństwem zapewniające wszechstronne podejście.

(9) Continuous improvement of information security.
Ciągłe udoskonalanie bezpieczeństwa informacji.

This International Standard is applicable to anyone interested in gaining a better understanding of the ISO/IEC 27000 ISMS family of standards.


Terminology
27000
Overview
& Vocabulary
Requirements
27001
ISMS
Requirements
27006
Accreditation
Requirements
Guideline
Support
PDCA
Control
Implementation
27002
Code of
Practice
27003
Implementation
Guidance
27004
Management
Measurement
27005
Risk
Management
13335-X
ICT
Security - 3
4
5
15947
IDS
Framework
18028-X
Network
Security - 1
2
3
4
5
18043
IDS
Management
18044
Incident
Management