

Standardy (normy) informační bezpečnosti

Řízení informační bezpečnosti PV017

Kamil Malinka

(využity materiály Doc. Staudka a konzultace Prof. Matyáše)

Verze: podzim 2024

Osnova

- Standardy (normy) informační bezpečnosti
 - Terminologie
 - Rodina standardů ISO/IEC 27000
 - Standard NIST, rodina SP 800
 - Certifikace

Standardy (normy) a legislativa

- Cíl přednášky o standardech a standardizaci - umět odpovědět na otázky:
 - Co to jsou standardy, normy, doporučení?
 - Jak vznikají standardy a doporučení?
 - Kdo je kdo ve světě standardů a doporučení ?
 - Které standardy informační bezpečnosti jsou reprezentativní ?
- Standardizační organizace a principy jejich činnosti a působení
- Upozornění na hlavní de iure standardy InfoSec

Standard, norma, doporučení = dokumentovaná úmluva 1/3

- Úmluva
 - O technické specifikaci nebo
 - O jiném podobném přesně stanoveném kritériu
- Cíl úmluvy
 - Pravidlo/směrnice definující charakteristické vlastnosti materiálů, výrobků, procesů, služeb, ...
 - Standardy lze použít jako měřítko pro porovnávání nebo dokonce hodnocení
 - Umožňuje, aby materiály, výrobky, procesy, služby, ... byly takové, jaké se zamýšlí, že mají být
 - Formát platební karty,
 - Protokol komunikace,
 - Politika poskytování služby,
 - ...

Standard, norma, doporučení = dokumentovaná úmluva 2/3

- Standard nebo norma?
- V Česku (mimo oblast IT) se tradičně používá pojem „**norma**“, v oblasti IT celosvětově převládá „**standard**“
- **Doporučení** (*recommendation*) - termín používaný některými organizacemi vydávající standardy místo termínu „standard“ (ITU - telekomunikace, ...)
- **De facto standard** - standard vyvinutý na bázi konsensu jisté komunity,
 - Standard vypracovaný v rámci jisté komunity, která si před jeho vydáním odsouhlasí, že standard odpovídá jí stanoveným cílům
- **De iure standard**- standard „podle práva“ ,
 - Úmluva schválená uznávanou institucí pověřenou tímto posláním, legislativou, rozhodnutím státních autorit, ...

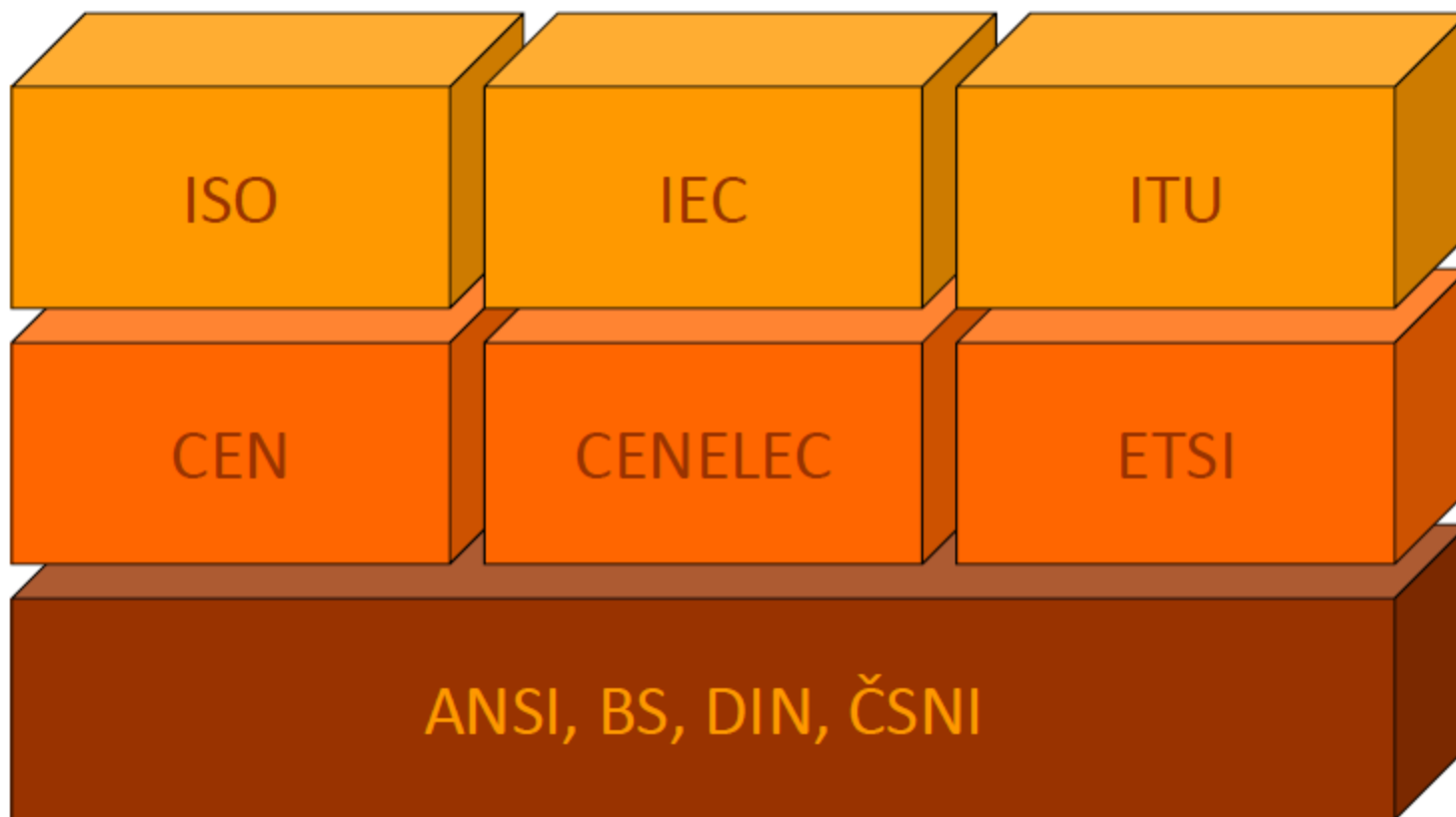
Standard, norma, doporučení = dokumentovaná úmluva 3/3

- Závaznost standardů
 - Žádný standard sám o sobě nemá charakter právního předpisu
 - Právní předpis může stanovit povinné vyhovění standardu
 - V tom případě se obvykle dává přednost de iure standardům
- Mezinárodní charakter standardů
 - Výrobci standardizovaných produktů/procesů v globálním prostředí musí zvolit standard, kterému proces/produkt vyhovuje
 - Tudíž je nutné zabránit přílišné diverzifikaci prosazování „správných“ technik,
...
 - **Mnoho standardů pokroku v technologiích smrt**

Vyhovění standardu vs. certifikace

- **Compliance** (vyhovění) vs. **Certification** (certifikace)
- Produkt, služba, proces, ... může být prohlášena za **vyhovující standardu**
 - Prohlášení, že produkt, služba, proces, splňuje podmínky definované standardem
 - Požadavek vyhovění může být předepsaný zákonem, smlouvou, ...
- Produkt, služba, proces, ... může být **certifikovaný**, tj. existuje certifikát potvrzující, že je vyhovující standardu
 - Certifikace - neutrální důvěryhodná třetí strana prověří validitu prohlášení o vyhovění standard a vydá o tom relevantní certifikát
 - Standardy definující např. algoritmus, jsou snadno certifikovatelné
 - Standardy návodů jak budovat systém/službu jsou spíše radou a certifikace se obvykle nepožaduje

Standardizační organizace



- Mezinárodní

- Evropské

- Národní

Příklady oblasti de facto standardů

- **OWASP** , *The Open Web Application Security Project*
 - A worldwide free and open community focused on improving the security of application software
 - <http://www.owasp.org/>
 - Standard vývoje bezpečné webovské aplikace
 - Standard testování bezpečné webovské aplikace
 - Standard hodnocení a kritéria záruk za bezpečnost bezpečné webovské aplikace
- **RFC** (Request for Comment)
 - Název internetových standardů, dáno historickou souvislostí
 - V pozadí působí - Internet Society, ISOC, <http://www.isoc.org/>
 - 150 institucionálních, 6000 individuálních členů z cca 100 zemí
 - Internet reprezentuje - Internet Activities Board, **IAB**
 - Rada pro internetovské činnosti, manažersky spravuje a řídí provoz Internetu
 - Hlavní odpovědnost za vývoj a posuzování RFC IAB delegovala na technickou poradní komisi - IETF, Internet Engineering Task Force
 - Konečné rozhodnutí o vydání (přijetí) RFC dělá IAB

Firemní, proprietární standardy

- Kategorie de facto standardů
- Obvykle standardy patentovaných technik
- Významný nástroj pro „udržení trhu“ silnou společností
 - Pokud silný výrobce nahradí nezávislé standardy svými proprietárními standardy, váže zákazníky na svoji proprietární funkcionalitu
- Mnohdy hrají velmi silnou roli
 - Např. **PKCS** (Public-Key Cryptography Standards) publikovaný RSA Labs

Hlavní standardy vydané ISO/IEC

- ISO (International Organization for Standardization)
 - Obvykle pětiletá perioda hodnocení mezinárodního standardu
 - Když se odhalí vada standardu (např. byla podceněna rychlost rozvoje technologie), jsou přijímána opatření, aby standardy byly revidovány i dříve než v pětiletém hodnotícím cyklu
- V současnosti především **rodina standardů ISO/IEC 27000**
 - Více viz <http://www.iso27001security.com/html/iso27000.html>
 - Doporučení jak řídit informační bezpečnost, řešit zvládání rizik a jak implementovat opatření v kontextu celého systému systému řízení informační bezpečnosti
 - **V současnosti celosvětově uznávaný základní standard zajišťování informační bezpečnosti**

Osnova

- Standardy (normy) informační bezpečnosti
 - Terminologie
 - **Rodina standardů ISO/IEC 27000**
 - Standard NIST, rodina SP 800
 - Certifikace

Rodina standardů ISO/IEC 27000, ISO/IEC 27001:2022

- **Information Security Management System - Requirements**
- Definuje požadavky na funkcionalitu a vlastnosti systému správy (řízení) informační bezpečnosti
- **Požadavky na možná bezpečnostní opatření vymezuje standard ISO/IEC 27002**
- ISO/IEC 27001 je původně britský standard BS 7779-2
- Standard je detailním popisem požadavků, které **musí** ISMS splnit (v originále se používá *must* a *shall*), pokud ISMS chce standardu vyhovět
- Je nezávislý na technologii, určený pro organizace všech typů, velikostí a podstat, působících v jakémkoli sektoru (komerce, státní správa, neziskovky), kdekoli ve světě

Rodina standardů ISO/IEC 27000, ISO/IEC 27001:2022

- V dodatku standard 27001 uvádí seznam cílů opatření definovaných v ISO/IEC 27002
- ISO/IEC 27002 obsahuje návody, jak je implementovat
- Povinným požadavkem 27001 je porovnat opatření zvolená při zvládnání rizik proti dodatku 27001, aby byla jistota, že se na nic nezapomnělo
- 27001 nařizuje použít 27002 jak zdroj návodů pro volbu a implementaci opatření, nezakazuje použití i dalších zdrojů
- Seznam cílů a opatření v dodatku 27001 není chápán jako úplný, vyčerpávající, podle potřeby lze doplňovat další cíle a opatření
- ISMS organizace lze certifikovat na vyhovění ISO/IEC 27001

Rodina standardů ISO/IEC 27000, ISO/IEC 27002:2022

- **Code of practice for information security management**
- Doporučení jak navrhovat, implementovat, udržovat a vylepšovat opatření prosazující informační bezpečnost, používá slova *may*, *should* (může, měl by)
- Původně britský standard BS 7779, poté standard ISO/IEC 17779, nyní standard ISO/IEC 27002:2013
- Jde o mezinárodně uznávané nejlepší praktiky řízení informační bezpečnosti
- Je návodem, jak implementovat certifikovatelný ISMS, externí auditor se může na 27002 odkazovat
- Standard ISO/IEC 27002 je kodexem, radami pro budování bezpečného systému, obvyklé je deklarovat vyhovění standardu, certifikace vyhovění ISO/IEC 27002 se nedělá

Rodina standardů ISO/IEC 27000 v 05.2019

By Gary Hinson, standardy, které úzce souvisí s obsahem předmětu PV017, jsou v tabulce v červeném rámci

#	Standard	Published	Title	Notes
1	ISO/IEC 27000	2018	Information security management systems — Overview and vocabulary	Overview/introduction to the ISO27k standards as a whole plus a glossary of terms; FREE!
2	ISO/IEC 27001	2013	Information security management systems — Requirements	Formally specifies an ISMS against which thousands of organizations have been certified compliant
3	ISO/IEC 27002	2013	Code of practice for information security controls	A reasonably comprehensive suite of information security control objectives and generally-accepted good practice security controls
4	ISO/IEC 27003	2017	Information security management system implementation guidance	Sound advice on implementing ISO27k, expanding section-by-section on the main body of ISO/IEC 27001
5	ISO/IEC 27004	2016	Information security management — Measurement	Much improved second version, with useful advice on security metrics
6	ISO/IEC 27005	2018	Information security risk management	Discusses information risk management principles in general terms without specifying or mandating particular methods. Major revision in progress

#	Standard	Published	Title	Notes
7	ISO/IEC 27006	2015	Requirements for bodies providing audit and certification of information security management systems	Formal guidance for the certification bodies, with several grammatical errors – needs revision
8	ISO/IEC 27007	2017	Guidelines for information security management systems auditing	Auditing the management system elements of the ISMS
9	ISO/IEC TR 27008	2011	Guidelines for auditors on information security controls	Auditing the information security elements of the ISMS
10	ISO/IEC 27009	2016	Sector-specific application of ISO/IEC 27001 – requirements	Guidance for those developing new ISO27k standards (i.e. ISO/IEC JTC1/SC27 – an internal committee standing document really)
11	ISO/IEC 27010	2015	Information security management for inter-sector and inter-organisational communications	Sharing information on information security between industry sectors and/or nations, particularly those affecting “critical infrastructure”
12	ISO/IEC 27011	2016	Information security management guidelines for telecommunications organizations based on ISO/IEC 27002	Information security controls for the telecoms industry; also called “ITU-T Recommendation x.1051”
13	ISO/IEC 27013	2015	Guidance on the integrated implementation of ISO/IEC 27001 and ISO/IEC 20000-1	Combining ISO27k/ISMS with IT Service Management/ITIL
14	ISO/IEC 27014	2013	Governance of information security	Governance in the context of information security; will also be called “ITU-T Recommendation X.1054”
16	ISO/IEC TR 27016	2014	Information security management – Organizational economics	Economic theory applied to information security

#	Standard	Published	Title	Notes
17	ISO/IEC 27017	2015	Code of practice for information security controls for cloud computing services based on ISO/IEC 27002	Information security controls for cloud computing
18	ISO/IEC 27018	2014	Code of practice for controls to protect personally identifiable information processed in public cloud computing services	Privacy controls for cloud computing
19	ISO/IEC TR 27019	2017	Information security management guidelines based on ISO/IEC 27002 for process control systems specific to the energy industry	Information security for ICS/SCADA/embedded systems (not just used in the energy industry!), excluding the nuclear industry
20	ISO/IEC 27021	2017	Competence requirements for information security management professionals	Guidance on the skills and knowledge necessary to work in this field
21	ISO/IEC 27023	2015	Mapping the revised editions of ISO/IEC 27001 and ISO/IEC 27002	Belated advice for those updating their ISMSs from the 2005 to 2013 versions
22	ISO/IEC 27030	DRAFT	Guidelines for security and privacy in Internet of Things (IoT)	A standard about the information risk, security and privacy aspects of IoT
23	ISO/IEC 27031	2011	Guidelines for information and communications technology readiness for business continuity	Continuity (i.e. resilience, incident management and disaster recovery) for ICT, supporting general business continuity
24	ISO/IEC 27032	2012	Guidelines for cybersecurity	Ignore the vague title: this standard actually concerns Internet security
25	ISO/IEC 27033	-1 2015	Network security overview and concepts	Various aspects of network security, updating and replacing ISO/IEC 18028

#	Standard	Published	Title	Notes
26	ISO/IEC 27033	-2 2012	Guidelines for the design and implementation of network security	Various aspects of network security, updating and replacing ISO/IEC 18028
27		-3 2010	Reference networking scenarios - threats, design techniques and control issues	
28		-4 2014	Securing communications between networks using security gateways	
29		-5 2013	Securing communications across networks using Virtual Private Networks (VPNs)	
30		-6 2016	Securing wireless IP network access	
31	ISO/IEC 27034	-1 2011	Application security — Overview and concepts	Multi-part application security standard
32		-2 2015	Organization normative framework	
33		-3 2018	Application security management process	
34		-4 DRAFT	Application security validation	
35		-5 2017	Protocols and application security control data structure	Promotes the concept of a reusable library of information security control functions, formally specified, designed and tested
36		-5-1 2018	Protocols and application security control data structure, XML schemas	
37		-6 2016	Case studies	
38		-7 2018	Application security assurance prediction framework	

#	Standard	Published	Title	Notes
39	ISO/IEC 27035	-1 2016	Information security incident management — Principles of incident management	Replaced ISO TR 18044
40		-2 2016	— Guidelines to plan and prepare for incident response	Actually concerns incidents affecting IT systems and networks, specifically
41		-3 DRAFT	— Guidelines for incident response operations??	Part 3 drafting restarted – due out in 2019 or 2020
42	ISO/IEC 27036	-1 2014	Information security for supplier relationships – Overview and concepts (FREE!)	Information security aspects of ICT outsourcing and services
43		-2 2014	— Common requirements	
44		-3 2013	— Guidelines for ICT supply chain security	
45		-4 2016	— Guidelines for security of cloud services	
46	ISO/IEC 27037	2012	Guidelines for identification, collection, acquisition, and preservation of digital evidence	One of several IT forensics standards
47	ISO/IEC 27038	2014	Specification for digital redaction	Redaction of digital documents
48	ISO/IEC 27039	2015	Selection, deployment and operations of intrusion detection and prevention systems (IDPS)	IDS/IPS
49	ISO/IEC 27040	2015	Storage security	IT security for stored data
50	ISO/IEC 27041	2015	Guidelines on assuring suitability and adequacy of incident investigative methods	Assurance of the integrity of forensic evidence is absolutely vital

#	Standard	Published	Title	Notes
51	ISO/IEC 27042	2015	Guidelines for the analysis and interpretation of digital evidence	IT forensics analytical methods
52	ISO/IEC 27043	2015	Incident investigation principles and processes	The basic principles of eForensics
53	ISO/IEC 27050	-1 2016	Electronic discovery – overview and concepts	More eForensics advice
54		-2 2018	Guidance for governance and management of electronic discovery	Advice on treating the risks relating to eForensics
55		-3 2017	Code of practice for electronic discovery	A how-to-do-it guide to eDiscovery
56		-4 DRAFT	ICT readiness for electronic discovery	Guidance on eDiscovery technology (tools, systems and processes)
57	ISO/IEC 27070	DRAFT	Security requirements for establishing virtualized roots of trust	Concerns trusted cloud computing
58	ISO/IEC 27099	DRAFT	Public key infrastructure - practices and policy framework	Infosec management requirements for Certification Authorities
59	ISO/IEC 27100	DRAFT	Cybersecurity – overview and concepts	Perhaps this standard will clarify, once and for all, what ‘cybersecurity’ actually is. Perhaps not.
60	ISO/IEC 27101	DRAFT	Cybersecurity framework development guidelines	Given the above, we can barely guess what this might turn out to be
61	ISO/IEC 27102	DRAFT	Information security management guidelines for cyber insurance	Advice on obtaining insurance to reduce the costs of cyber incidents
62	ISO/IEC TR 27103	2018	Cybersecurity and ISO and IEC standards	Explains how ISO27k and other ISO and IEC standards relate to ‘cybersecurity’ (without actually defining the term!)

#	Standard	Published	Title	Notes
63	ISO/IEC 27550	DRAFT	Privacy engineering	How to address privacy throughout the lifecycle of IT systems
64	ISO/IEC 27551	DRAFT	Requirements for attribute-based unlinkable entity authentication	Seems more like an authentication standard than ISO27k ... scope creep?
65	ISO/IEC 27552	DRAFT	Extension to ISO/IEC 27001 and to ISO/IEC 27002 for privacy management — Requirements and guidelines	Explains extensions to an ISO27k ISMS for privacy management
66	ISO/IEC 27553	DRAFT	Security requirements for authentication using biometrics on mobile devices	High-level requirements attempting to standardize the use of biometrics on mobile devices
67	ISO/IEC 27554	DRAFT	Application of ISO 31000 for assessment of identity management-related risk	About applying the ISO 31000 risk management process to identity management
68	ISO/IEC 27555	DRAFT	Establishing a PII deletion concept in organizations	A conceptual framework, of all things, for deleting personal information
69	ISO 27799	2016	Health informatics — Information security management in health using ISO/IEC 27002	Infosec management advice for the health industry

Osnova

- Standardy (normy) informační bezpečnosti
 - Terminologie
 - Rodina standardů ISO/IEC 27000
 - **Standard NIST, rodina SP 800**
 - Certifikace

NIST Special Publications (SP)

- *<http://csrc.nist.gov/publications/PubsSPs.html>*
- SP 800, Computer Security (December 1990-present):
 - NIST's primary mode of publishing computer/cyber/information security guidelines, recommendations and reference materials
- SP 1800, NIST Cybersecurity Practice Guides (2015-present):
 - Complement the SP 800s; targets specific cybersecurity challenges in the public and private sectors; practical, user-friendly guides to facilitate adoption of standards-based approaches to cybersecurity
- SP 500, Computer Systems Technology (January 1977-present):
 - A general IT subseries used more broadly by NIST's Information Technology Laboratory (ITL)

Standard NIST, rodina SP 800, příklady (SP Special Publication)

- SP 800-12: An Introduction to Information Security
- SP 800-30: Guide for Conducting Risk Assessments
- SP 800-45: Guidelines on Electronic Mail Security
- SP 800-50: Building a Cybersecurity and Privacy Learning Program
- SP 800-63: Digital Identity Guidelines
- SP 800-94: Guide to Intrusion Detection and Prevention Systems (IDPS)
- SP 800-95: Guide to Secure Web Services
- SP 800-100: Information Security Handbook: A Guide for Managers
- SP 800-184: Guide for Cybersecurity Event Recovery

Osnova

- Standardy (normy) informační bezpečnosti
 - Terminologie
 - Rodina standardů ISO/IEC 27000
 - Standard NIST, rodina SP 800
 - **Certifikace**

Certifikace ISO/IEC 27001

- ISO/IEC 27001 - standard normálu ISMS, o jehož dosažení **lze získat certifikát**
 - ISMS - prostředí pro návrh, implementaci, řízení, údržby a systematické a konzistentní prosazování procesů a nástrojů zajišťujících informační bezpečnost v celé organizaci
- Standard ISO/IEC 27001 respektuje nástroje definované standardem ISO/IEC 27002
 - ISO/IEC 27001 obsahuje seznam nástrojů dle ISO/IEC 27002 jako menu
 - Organizace přijímající ISO/IEC 27001 si z menu potřebné nástroje vybírá
 - Výběr musí vycházet z výsledků analýzy rizik
 - Škála opatření může být adekvátně rozšířena vůči ISO/IEC 27002

Rámcový průběh certifikace

- Příprava - zvolte si svého šampiona, podpora managementu a gap analýza (může zahrnout i prioritizovaný plán doporučených akcí)
- Ustanovení kontextu, rozsahu a cílů (vč. nákladů a časového rámce, potřeba externího dodavatele atp.)
- Vytvoření rámce řízení (odpovědnosti, harmonogram, audity, ...)
- Analýza rizik – vznik povinných dokumentů (Prohlášení o použitelnosti (SoA) a plán ošetření rizik (RTP))
- Implementace bezpečnostních opatření – akceptace/transfer/mitigace/odstranění rizika
- Školení – zvyšování bezpečnostního povědomí zaměstnanců
- Revize a update relevantní dokumentace – bezpečnostní politika a další (standard vyžaduje určitou minimální množinu dokumentů (15))
- Měření, monitorování, kontrola
- Pravidelný interní audit
- Registrační/certifikační audit

