Szabványok, ajánlások

- ISO 27000 szabványcsalád
- COBIT (Control Objectives for Information and Related Technology)
- Common Criteria (ISO/IEC 15408)
- ITIL és ISO/IEC 20000 (IT Infrastructure Library)
- KIB 25. ajánlás (Közigazgatási Informatikai Bizottság)
- NIST Special Publication 800-53
- PCI DSS (Payment Card Industry (PCI) Data Security Standard)

ISO 27000 szabványcsalád

- BS 7799 informatikai biztonsági követelmények
- ISO/IEC 27000:2012 Information security management systems – Overview and vocabulary
- ISO/IEC 27001:2013 Information security management systems
- ISO/IEC 27002:2013 Code of practice for information security controls
- ISO/IEC 27005:2011 Information security risk management

  ISO/IEC 27007:2011 Guidelines for information security management systems auditing

COBIT (Control Objectives for Information and Related Technology)

- Information Systems Audit and Control Association (ISACA) és az IT Governance Institute (ITGI) 1992-ben
- COBIT 4.1 verziója 34 magas szintű folyamatot,
- 210 kontroll célkitűzést tartalmaz, amelyek négy szakterület köré csoportosulnak:
  - Tervezés és szervezés (Planning and Organization)
  - Beszerzés és megvalósítás (Acquisition and Implementation)
  - Szolgáltatás és támogatás (Delivery and Support)
  - Figyelemmel kísérés és értékelés (Monitoring and Evaluation)

Common Criteria

- 1996-ban elkészítették a Common Criteria for Information Technology Security Evaluation
- Informatikai biztonsági termékszabvány, amely ma az informatikai biztonság területén etalonnak tekinthető
- 2.0-ás változatát az Informatikai Tárcaközi Bizottság 16. számú ajánlásaként magyar nyelven közreadta, majd az MSZ ISO/IEC 15408 jelzetű szabvány is lefordításra került.
- A szabványban a funkcionális követelmények, bizonyossági követelmények és értékelési bizonyossági szintek (EAL) mátrixaként határozhatóak meg az alkalmazandó biztonsági követelmények.

ITIL és ISO/IEC 20000

- Elsősorban informatikai üzemeltetésére és fejlesztésére szolgáló módszertani gyűjtemény, folyamatszabvány
- Előírásaiban érinti a biztonsági területet.
- Nemzetközi legjobb gyakorlatként az IT szolgáltatások területén szolgál követelményhalmazként.
- Célja a jó minőségű, költséghatékony IT szolgáltatások támogatása, a minőségügyben ismert Plan-Do-Check-Act (PDCA) elv alkalmazásával.
- Öt kötete:
  - Szolgáltatás-stratégia (Service Strategy)
  - Szolgáltatás-tervezés (Service Design)
  - Szolgáltatás-létesítés és változtatás (Service Transition)
  - Szolgáltatás-üzemeltetés (Service Operation)
  - Állandó szolgáltatás-fejlesztés (Continual Service Improvement)

KIB 25. ajánlás (Magyar Informatikai Biztonsági Ajánlások)

- 25/1. Magyar Informatikai Biztonsági Keretrendszer (MIBIK)
- 25/1-1. kötet: Informatikai Biztonsági Irányítási Rendszer (IBIR)
- 25/1-2. kötet: Informatikai Biztonság Irányítási Követelmények (IBIK)
- 25/1-3. kötet: Az Informatikai Biztonság Irányításának Vizsgálata (IBIV)
- 25/2. kötet: Magyar Informatikai Biztonsági Értékelési és Tanúsítási Séma (MIBÉTS)
- 25/2-1. segédlet: MIBÉTS - Modell és Folyamatok
- 25/2-2. segédlet: MIBÉTS – Útmutató a Megbízók számára
- 25/2-3. segédlet: MIBÉTS – Útmutató a Fejlesztők számára
- 25/2-4. segédlet: MIBÉTS – Útmutató Értékelőknek
- 25/2-5. segédlet: MIBÉTS – Értékelési módszertan
- 25/3. kötet: Informatikai Biztonsági Iránymutató Kis Szervezeteknek (IBIX)

NIST Special Publication 800-53

- Security and Privacy Controls for Federal Information Systems and Organizations

ID	FAMILY	ID	FAMILY
AC	Access Control	MP	Media Protection
AT	Awareness and Training	PE	Physical and Environmental Protection
AU	Audit and Accountability	PL	Planning
CA	Security Assessment and Authorization	PS	Personnel Security
CM	Configuration Management	RA	Risk Assessment
CP	Contingency Planning	SA	System and Services Acquisition
IA	Identification and Authentication	SC	System and Communications Protection
IR	Incident Response	SI	System and Information Integrity
MA	Maintenance	PM	Program Management

PCI DSS (Payment Card Industry (PCI) Data Security Standard)

Control Objectives	PCI DSS Requirements
Build and Maintain a Secure Network	1. Install and maintain a firewall configuration to protect cardholder data
	2. Do not use vendor-supplied defaults for system passwords and other security parameters
Protect Cardholder Data	3. Protect stored cardholder data
	4. Encrypt transmission of cardholder data across open, public networks
Maintain a Vulnerability Management Program	5. Use and regularly update anti-virus software on all systems commonly affected by malware
	6. Develop and maintain secure systems and applications
Implement Strong Access Control Measures	7. Restrict access to cardholder data by business need-to-know
	8. Assign a unique ID to each person with computer access
	9. Restrict physical access to cardholder data
Regularly Monitor and Test Networks	10. Track and monitor all access to network resources and cardholder data
	11. Regularly test security systems and processes
Maintain an Information Security Policy	12. Maintain a policy that addresses information security

Minősítések

- CISA (Certified Information Systems Auditor)
- CISM (Certified Information Security Manager)
- CRISC (Certified in Risk and Information Systems Control)
- CISSP (Certified Information Systems Security Professional)
- CEH (Certified Ethical Hacker)
- OSCP (Offensive Security Certified Professional)

Hazai jogszabályok

- 2011. évi CXII. törvény az információs jogról és az információszabadságról
- 1139/2013. (III. 21.) Korm. határozat Magyarország Nemzeti Kiberbiztonsági Stratégiájáról
- 2013. évi L. törvény az állami és önkormányzati szervek elektronikus információbiztonságáról (Ibtv)
- 77/2013. (XII. 19.) NFM rendelet az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvényben meghatározott technológiai biztonsági, valamint biztonságos információs eszközökre, termékekre vonatkozó, valamint a biztonsági osztályba és biztonsági szintbe sorolási követelményeiről
- 2012. évi CLXVI. törvény a létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről (Lrtv)