

ISO/IEC 27000 szabványcsalád (2023. 01. 27)

<u>ISO/IEC 27000:2018</u> Information technology — Security techniques — Information security management systems — Overview and vocabulary	<u>90.20</u>	<u>35.030</u> <u>01.040.35</u>
<u>ISO/IEC 27001:2022</u> Information security, cybersecurity and privacy protection — Information security management systems — Requirements	<u>60.60</u>	<u>35.030</u> <u>03.100.70</u>
<u>ISO/IEC 27002:2022</u> Information security, cybersecurity and privacy protection — Information security controls	<u>60.60</u>	<u>35.030</u>
<u>ISO/IEC 27003:2017</u> Information technology — Security techniques — Information security management systems — Guidance	<u>90.20</u>	<u>35.030</u> <u>03.100.70</u>
<u>ISO/IEC 27004:2016</u> Information technology — Security techniques — Information security management — Monitoring, measurement, analysis and evaluation	<u>90.60</u>	<u>35.030</u>
<u>ISO/IEC 27005:2022</u> Information security, cybersecurity and privacy protection — Guidance on managing information security risks	<u>60.60</u>	<u>35.030</u>
<u>ISO/IEC 27006:2015</u> Information technology — Security techniques — Requirements for bodies providing audit and certification of information security management systems	<u>90.92</u>	<u>35.030</u> <u>03.120.20</u>
<u>ISO/IEC 27006:2015/AMD 1:2020</u> Information technology — Security techniques — Requirements for bodies providing audit and certification of information security management systems — Amendment 1	<u>60.60</u>	<u>35.030</u>
<u>ISO/IEC DIS 27006-1</u> Requirements for bodies providing audit and certification of information security management systems – Part 1: General	<u>40.60</u>	<u>35.030</u> <u>03.120.20</u>
<u>ISO/IEC CD 27006-2.2</u> Requirements for bodies providing audit and certification of information security management systems – Part 2: Privacy information security management systems	<u>30.60</u>	<u>35.030</u> <u>03.120.20</u>
<u>ISO/IEC TS 27006-2:2021</u> Requirements for bodies providing audit and certification of information security management systems – Part 2: Privacy information security management systems	<u>90.92</u>	<u>35.030</u> <u>03.120.20</u>
<u>ISO/IEC 27007:2020</u> Information security, cybersecurity and privacy protection — Guidelines for information security management systems auditing	<u>60.60</u>	<u>35.030</u> <u>03.120.20</u>

ISO/IEC 27000 szabványcsalád (2023. 01. 27)

<u>ISO/IEC TS 27008:2019</u> Information technology — Security techniques — Guidelines for the assessment of information security controls	90.20	35.030
<u>ISO/IEC 27009:2020</u> Information security, cybersecurity and privacy protection — Sector-specific application of ISO/IEC 27001 — Requirements	60.60	35.030
<u>ISO/IEC 27010:2015</u> Information technology — Security techniques — Information security management for inter-sector and inter-organizational communications	90.93	35.030 03.100.70
<u>ISO/IEC 27011:2016</u> Information technology — Security techniques — Code of practice for Information security controls based on ISO/IEC 27002 for telecommunications organizations	90.92	35.030
<u>ISO/IEC 27011:2016/Cor 1:2018</u> Information technology — Security techniques — Code of practice for Information security controls based on ISO/IEC 27002 for telecommunications organizations — Technical Corrigendum 1	60.60	35.030
<u>ISO/IEC DIS 27011</u> Information security, cybersecurity and privacy protection — Information security controls based on ISO/IEC 27002 for telecommunications organizations	40.60	35.030
<u>ISO/IEC 27013:2021</u> Information security, cybersecurity and privacy protection — Guidance on the integrated implementation of ISO/IEC 27001 and ISO/IEC 20000-1	60.60	35.020 35.030 03.080.99 03.100.70
<u>ISO/IEC 27013:2021/CD Amd 1</u> Information security, cybersecurity and privacy protection — Guidance on the integrated implementation of ISO/IEC 27001 and ISO/IEC 20000-1 Amendment 1	30.00	35.020 35.030 03.080.99 03.100.70
<u>ISO/IEC 27014:2020</u> Information security, cybersecurity and privacy protection — Governance of information security	60.60	35.030
<u>ISO/IEC TR 27016:2014</u> Information technology — Security techniques — Information security management — Organizational economics	60.60	35.030
<u>ISO/IEC 27017:2015</u> Information technology — Security techniques — Code of practice for information security controls based on ISO/IEC 27002 for cloud services	90.92	35.030
<u>ISO/IEC WD 27017</u> Information technology — Security techniques — Code of practice for information security controls based on ISO/IEC 27002 for cloud services	20.20	35.030

ISO/IEC 27000 szabványcsalád (2023. 01. 27)

<u>ISO/IEC 27018:2019</u> Information technology — Security techniques — Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors	<u>60.60</u>	<u>35.030</u>
<u>ISO/IEC 27019:2017</u> Information technology — Security techniques — Information security controls for the energy utility industry	<u>90.92</u>	<u>35.030</u>
<u>ISO/IEC CD 27019</u> Information technology — Security techniques — Information security controls for the energy utility industry	<u>30.20</u>	<u>35.030</u>
<u>ISO/IEC 27021:2017</u> Information technology — Security techniques — Competence requirements for information security management systems professionals	<u>90.20</u>	<u>35.030</u>
<u>ISO/IEC 27021:2017/AMD 1:2021</u> Information technology — Security techniques — Competence requirements for information security management systems professionals — Amendment 1: Addition of ISO/IEC 27001: 2013 clauses or subclauses to competence requirements	<u>60.60</u>	<u>35.030</u>
<u>ISO/IEC TS 27022:2021</u> Information technology — Guidance on information security management system processes	<u>60.60</u>	<u>35.030</u> <u>03.100.70</u>
<u>ISO/IEC AWI TR 27024</u> ISO/IEC 27001 family of standards references list – Use of ISO/IEC 27001 family of standards in Governmental / Regulatory requirements	<u>20.00</u>	<u>35.030</u>
<u>ISO/IEC 27031:2011</u> Information technology — Security techniques — Guidelines for information and communication technology readiness for business continuity	<u>90.92</u>	<u>35.030</u>
<u>ISO/IEC CD 27031</u> Information technology — Cybersecurity — Information and communication technology readiness for business continuity	<u>30.60</u>	<u>35.030</u> <u>35.030</u>
<u>ISO/IEC 27032:2012</u> Information technology — Security techniques — Guidelines for cybersecurity	<u>90.92</u>	<u>35.030</u>
<u>ISO/IEC DIS 27032</u> Cybersecurity — Guidelines for Internet Security	<u>40.60</u>	<u>35.030</u>
<u>ISO/IEC 27033-1:2015</u> Information technology — Security techniques — Network security — Part 1: Overview and concepts	<u>90.93</u>	<u>35.030</u>

ISO/IEC 27000 szabványcsalád (2023. 01. 27)

<u>ISO/IEC 27033-2:2012</u> Information technology — Security techniques — Network security — Part 2: Guidelines for the design and implementation of network security	<u>90.93</u>	<u>35.030</u>
<u>ISO/IEC 27033-3:2010</u> Information technology — Security techniques — Network security — Part 3: Reference networking scenarios — Threats, design techniques and control issues	<u>90.93</u>	<u>35.030</u>
<u>ISO/IEC 27033-4:2014</u> Information technology — Security techniques — Network security — Part 4: Securing communications between networks using security gateways	<u>90.93</u>	<u>35.030</u>
<u>ISO/IEC 27033-5:2013</u> Information technology — Security techniques — Network security — Part 5: Securing communications across networks using Virtual Private Networks (VPNs)	<u>90.93</u>	<u>35.030</u>
<u>ISO/IEC 27033-6:2016</u> Information technology — Security techniques — Network security — Part 6: Securing wireless IP network access	<u>90.93</u>	<u>35.030</u>
<u>ISO/IEC DIS 27033-7</u> Information technology – Network security — Part 7: Guidelines for network virtualization security	<u>40.60</u>	
<u>ISO/IEC 27034-1:2011</u> Information technology — Security techniques — Application security — Part 1: Overview and concepts	<u>90.93</u>	<u>35.030</u>
<u>ISO/IEC 27034-1:2011/Cor 1:2014</u> Information technology — Security techniques — Application security — Part 1: Overview and concepts — Technical Corrigendum 1	<u>60.60</u>	<u>35.030</u>
<u>ISO/IEC 27034-2:2015</u> Information technology — Security techniques — Application security — Part 2: Organization normative framework	<u>90.93</u>	<u>35.030</u>
<u>ISO/IEC 27034-3:2018</u> Information technology — Application security — Part 3: Application security management process	<u>60.60</u>	<u>35.030</u>
<u>ISO/IEC 27034-5:2017</u> Information technology — Security techniques — Application security — Part 5: Protocols and application security controls data structure	<u>90.20</u>	<u>35.030</u>
<u>ISO/IEC 27034-6:2016</u> Information technology — Security techniques — Application security — Part 6: Case studies	<u>90.93</u>	<u>35.030</u>
<u>ISO/IEC 27034-7:2018</u> Information technology — Application security — Part 7: Assurance prediction framework	<u>60.60</u>	<u>35.030</u>

ISO/IEC 27000 szabványcsalád (2023. 01. 27)

<u>ISO/IEC TS 27034-5-1:2018</u> Information technology — Application security — Part 5-1: Protocols and application security controls data structure, XML schemas	<u>90.93</u>	<u>35.030</u>
<u>ISO/IEC 27035-1:2016</u> Information technology — Security techniques — Information security incident management — Part 1: Principles of incident management	<u>90.92</u>	<u>35.030</u>
<u>ISO/IEC 27035-1</u> Information technology – Information security incident management — Part 1: Principles and process	<u>60.00</u>	<u>35.030</u>
<u>ISO/IEC 27035-2:2016</u> Information technology — Security techniques — Information security incident management — Part 2: Guidelines to plan and prepare for incident response	<u>90.92</u>	<u>35.030</u>
<u>ISO/IEC 27035-2</u> Information technology — Information security incident management — Part 2: Guidelines to plan and prepare for incident management	<u>60.00</u>	<u>35.030</u>
<u>ISO/IEC 27035-3:2020</u> Information technology — Information security incident management — Part 3: Guidelines for ICT incident response operations	<u>60.60</u>	<u>35.030</u>
<u>ISO/IEC CD 27035-4</u> Information technology — Information security incident management — Part 4: Coordination	<u>30.60</u>	
<u>ISO/IEC 27036-1:2021</u> Cybersecurity — Supplier relationships — Part 1: Overview and concepts	<u>60.60</u>	<u>35.030</u>
<u>ISO/IEC 27036-2:2022</u> Cybersecurity — Supplier relationships — Part 2: Requirements	<u>60.60</u>	<u>35.030</u>
<u>ISO/IEC 27036-3:2013</u> Information technology — Security techniques — Information security for supplier relationships — Part 3: Guidelines for information and communication technology supply chain security	<u>90.92</u>	<u>35.030</u>
<u>ISO/IEC FDIS 27036-3</u> Cybersecurity — Supplier relationships — Part 3: Guidelines for information and communication technology supply chain security	<u>50.00</u>	<u>35.030</u>
<u>ISO/IEC 27036-4:2016</u> Information technology — Security techniques — Information security for supplier relationships — Part 4: Guidelines for security of cloud services	<u>90.93</u>	<u>35.030</u>
<u>ISO/IEC 27037:2012</u> Information technology — Security techniques — Guidelines for identification, collection, acquisition and preservation of digital evidence	<u>90.93</u>	<u>35.030</u>

ISO/IEC 27000 szabványcsalád (2023. 01. 27)

<u>ISO/IEC 27038:2014</u> Information technology — Security techniques — Specification for digital redaction	<u>90.93</u>	<u>35.030</u>
<u>ISO/IEC 27039:2015</u> Information technology — Security techniques — Selection, deployment and operations of intrusion detection and prevention systems (IDPS)	<u>90.93</u>	<u>35.030</u>
<u>ISO/IEC 27040:2015</u> Information technology — Security techniques — Storage security	<u>90.92</u>	<u>35.030</u>
<u>ISO/IEC DIS 27040</u> Information technology — Security techniques — Storage security	<u>40.60</u>	<u>35.030</u>
<u>ISO/IEC 27041:2015</u> Information technology — Security techniques — Guidance on assuring suitability and adequacy of incident investigative method	<u>90.93</u>	<u>35.030</u>
<u>ISO/IEC 27042:2015</u> Information technology — Security techniques — Guidelines for the analysis and interpretation of digital evidence	<u>90.93</u>	<u>35.030</u>
<u>ISO/IEC 27043:2015</u> Information technology — Security techniques — Incident investigation principles and processes	<u>90.93</u>	<u>35.030</u>
<u>ISO/IEC CD 27046</u> Information technology — Big data security and privacy — Implementation guidelines	<u>30.60</u>	
<u>ISO/IEC 27050-1:2019</u> Information technology — Electronic discovery — Part 1: Overview and concepts	<u>60.60</u>	<u>35.030</u>
<u>ISO/IEC 27050-2:2018</u> Information technology — Electronic discovery — Part 2: Guidance for governance and management of electronic discovery	<u>60.60</u>	<u>35.030</u>
<u>ISO/IEC 27050-3:2020</u> Information technology — Electronic discovery — Part 3: Code of practice for electronic discovery	<u>60.60</u>	<u>35.030</u>
<u>ISO/IEC 27050-4:2021</u> Information technology — Electronic discovery — Part 4: Technical readiness	<u>60.60</u>	<u>35.030</u>
<u>ISO/IEC 27070:2021</u> Information technology — Security techniques — Requirements for establishing virtualized roots of trust	<u>60.60</u>	<u>35.030</u>
<u>ISO/IEC DIS 27071</u> Cybersecurity – Security recommendations for establishing trusted connections between devices and services	<u>40.60</u>	<u>35.030</u>

ISO/IEC 27000 szabványcsalád (2023. 01. 27)

<u>ISO/IEC AWI 27090</u> Cybersecurity — Artificial Intelligence — Guidance for addressing security threats and failures in artificial intelligence systems	<u>20.00</u>	<u>35.030</u>
<u>ISO/IEC 27099:2022</u> Information Technology — Public key infrastructure — Practices and policy framework	<u>60.60</u>	<u>35.030</u>
<u>ISO/IEC TS 27100:2020</u> Information technology — Cybersecurity — Overview and concepts	<u>60.60</u>	<u>35.030</u>
<u>ISO/IEC 27102:2019</u> Information security management — Guidelines for cyber-insurance	<u>60.60</u>	<u>35.030</u>
<u>ISO/IEC TR 27103:2018</u> Information technology — Security techniques — Cybersecurity and ISO and IEC Standards	<u>90.93</u>	<u>35.030</u>
<u>ISO/IEC AWI TR 27109</u> Cybersecurity education and training	<u>20.00</u>	
<u>ISO/IEC TS 27110:2021</u> Information technology, cybersecurity and privacy protection — Cybersecurity framework development guidelines	<u>60.60</u>	<u>35.030</u>
<u>ISO/IEC 27400:2022</u> Cybersecurity – IoT security and privacy – Guidelines	<u>60.60</u>	<u>35.030</u>
<u>ISO/IEC DIS 27402</u> Cybersecurity – IoT security and privacy – Device baseline requirements	<u>40.20</u>	<u>35.030</u>
<u>ISO/IEC CD 27403.2</u> Cybersecurity – IoT security and privacy – Guidelines for IoT domotics	<u>30.60</u>	
<u>ISO/IEC TR 27550:2019</u> Information technology — Security techniques — Privacy engineering for system life cycle processes	<u>60.60</u>	<u>35.030</u>
<u>ISO/IEC 27551:2021</u> Information technology, cybersecurity and privacy protection — Requirements for attribute based unlinkable entity authentication	<u>60.60</u>	<u>35.030</u>
<u>ISO/IEC 27553-1:2022</u> Information security, cybersecurity and privacy protection — Security requirements for authentication using biometrics on mobile devices Part 1: Local modes	<u>60.60</u>	<u>35.030</u>

ISO/IEC 27000 szabványcsalád (2023. 01. 27)

<u>ISO/IEC WD 27553-2</u> Information security, cybersecurity and privacy protection — Security requirements for authentication using biometrics on mobile devices Part 2: Remote modes	<u>20.20</u>	<u>35.030</u>
<u>ISO/IEC CD 27554.2</u> Application of ISO 31000 for assessment of identity related risk	<u>30.60</u>	
<u>ISO/IEC 27555:2021</u> Information security, cybersecurity and privacy protection — Guideline on personally identifiable information deletion	<u>60.60</u>	<u>35.030</u>
<u>ISO/IEC 27556:2022</u> Information security, cybersecurity and privacy protection – User centric privacy preferences management framework	<u>60.60</u>	<u>35.030</u>
<u>ISO/IEC 27557:2022</u> Information technology – Information security, cybersecurity and privacy protection – Organizational privacy risk management	<u>60.60</u>	<u>35.030</u>
<u>ISO/IEC 27559:2022</u> Information security, cybersecurity and privacy protection – Privacy enhancing data de-identification framework	<u>60.60</u>	
<u>ISO/IEC TS 27570:2021</u> Privacy protection — Privacy guidelines for smart cities	<u>60.60</u>	<u>35.030</u>
<u>ISO/IEC 27701:2019</u> Security techniques — Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management — Requirements and guidelines	<u>90.92</u>	<u>35.030</u>
<u>ISO/IEC DIS 27701</u> Security techniques — Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management — Requirements and guidelines	<u>40.20</u>	<u>35.030</u>
<u>ISO/IEC TS 29003:2018</u> Information technology — Security techniques — Identity proofing	<u>90.93</u>	<u>35.030</u>
<u>ISO/IEC 29100:2011</u> Information technology — Security techniques — Privacy framework	<u>90.92</u>	<u>35.030</u>
<u>ISO/IEC 29100:2011/AMD 1:2018</u> Information technology — Security techniques — Privacy framework — Amendment 1: Clarification	<u>60.60</u>	<u>35.030</u>
<u>ISO/IEC FDIS 29100</u> Information technology — Security techniques — Privacy framework	<u>50.00</u>	<u>35.030</u>

ISO/IEC 27000 szabványcsalád (2023. 01. 27)

<u>ISO/IEC 29101:2018</u> Information technology — Security techniques — Privacy architecture framework	<u>60.60</u>	<u>35.030</u>
<u>ISO/IEC 29134:2017</u> Information technology — Security techniques — Guidelines for privacy impact assessment	<u>90.92</u>	<u>35.030</u>
<u>ISO/IEC FDIS 29134</u> Information technology — Security techniques — Guidelines for privacy impact assessment	<u>50.00</u>	<u>35.030</u>
<u>ISO/IEC 29146:2016</u> Information technology — Security techniques — A framework for access management	<u>90.92</u>	<u>35.030</u>
<u>ISO/IEC 29146:2016/Amd 1:2022</u> Information technology — Security techniques — A framework for access management – Amendment 1	<u>90.92</u>	<u>35.030</u>
<u>ISO/IEC FDIS 29146</u> Information technology — Security techniques — A framework for access management	<u>50.00</u>	<u>35.030</u>
<u>ISO/IEC 29147:2018</u> Information technology — Security techniques — Vulnerability disclosure	<u>60.60</u>	<u>35.030</u>
<u>ISO/IEC 29151:2017</u> Information technology — Security techniques — Code of practice for personally identifiable information protection	<u>90.60</u>	<u>35.030</u>
<u>ISO/IEC TS 30104:2015</u> Information technology — Security techniques — Physical Security Attacks, Mitigation Techniques and Security Requirements	<u>90.93</u>	<u>35.030</u>
<u>ISO/IEC 30111:2019</u> Information technology — Security techniques — Vulnerability handling processes	<u>60.60</u>	<u>35.030</u>