

Risk treatment options

1. Avoidance of activity
2. Transfer of risk to third party
3. Retention
4. Mitigation

Controls according to Annex A of the ISO/IEC 27001 standard

A.5.1 Policies for information security

A.5.2 Information security roles and responsibilities

A.5.3 Segregation of duties

ISO/IEC 27001:2017
Annex A
A.5.1 Policies for information security
A.5.2 Information security roles and responsibilities
A.5.3 Segregation of duties
A.5.4 Information security incident management
A.5.5 Information security breach management
A.5.6 Information security continuity management
A.5.7 Information security assessment
A.5.8 Information security monitoring, measurement, reporting, analysis and improvement
A.5.9 Information security awareness, education and training
A.5.10 Information security risk management
A.5.11 Information security policies
A.5.12 Information security objectives
A.5.13 Information security management system
A.5.14 Information security management system improvement
A.5.15 Information security management system documentation

A.5.16 Identity management

A.5.17 Authentication information

A.5.18 Access rights

ISO/IEC 27001:2017
Annex A
A.5.16 Identity management
A.5.17 Authentication information
A.5.18 Access rights
A.5.19 Information security incident management
A.5.20 Information security breach management
A.5.21 Information security continuity management
A.5.22 Information security assessment
A.5.23 Information security monitoring, measurement, reporting, analysis and improvement
A.5.24 Information security awareness, education and training
A.5.25 Information security risk management
A.5.26 Information security policies
A.5.27 Information security objectives
A.5.28 Information security management system
A.5.29 Information security management system improvement
A.5.30 Information security management system documentation

A.5.32 Intellectual property rights

A.5.33 Protection of records

ISO/IEC 27001:2017
Annex A
A.5.32 Intellectual property rights
A.5.33 Protection of records
A.5.34 Information security incident management
A.5.35 Information security breach management
A.5.36 Information security continuity management
A.5.37 Information security assessment
A.5.38 Information security monitoring, measurement, reporting, analysis and improvement
A.5.39 Information security awareness, education and training
A.5.40 Information security risk management
A.5.41 Information security policies
A.5.42 Information security objectives
A.5.43 Information security management system
A.5.44 Information security management system improvement
A.5.45 Information security management system documentation

A.6.2 Terms and conditions of employment

A.6.3 Information security awareness, education and training

A.6.4 Disciplinary process

ISO/IEC 27001:2017
Annex A
A.6.2 Terms and conditions of employment
A.6.3 Information security awareness, education and training
A.6.4 Disciplinary process
A.6.5 Information security incident management
A.6.6 Information security breach management
A.6.7 Information security continuity management
A.6.8 Information security assessment
A.6.9 Information security monitoring, measurement, reporting, analysis and improvement
A.6.10 Information security awareness, education and training
A.6.11 Information security risk management
A.6.12 Information security policies
A.6.13 Information security objectives
A.6.14 Information security management system
A.6.15 Information security management system improvement
A.6.16 Information security management system documentation

A.7.4 Physical security monitoring

A.7.5 Protecting against physical and environmental threats

ver [version] from [date]

