

**BriefBuilder B.V. - Statement of Applicability**

24/09/2025 Version: 2.1

| Information security controls<br>ISO/IEC 27001:2022/Amd. 1:2024 |         |  |  |  | Risk Analysis | Justification for inclusion |                    |            |  | Justification for exclusion |  |
|---|---------|--|--|--|---------------|-----------------------------|--------------------|------------|--|-----------------------------|--|
| Clause  | Chapter | Paragraph  | Control  | Goal   | Applicable    | Control implemented?        | Laws & Regulations | Agreements | Business Requirements / Best Practices | Risk analysis               |  |
|   | 5       | Organizational controls  |  |  |               |                             |                    |            |  |                             |  |
|   | 5.1     | Policies for information security  | Information security policy and topic-specific policies shall be defined, approved by management, published, communicated to and acknowledged by relevant personnel and relevant interested parties, and reviewed at planned intervals and if significant changes occur. | Ensure ongoing appropriateness, adequacy and effectiveness of management guidance and support according to business, legal and contractual requirements.   | Yes           | Yes                         | X                  |            | X                                      | X                           |  |
|   | 5.2     | Information security roles and responsibilities  | Information security roles and responsibilities shall be defined and allocated according to the organization needs.  | A defined, approved and clearly understandable structure for implementation, execution and management of information security within the organization.   | Yes           | Yes                         |                    |            | X                                      | X                           |  |
|   | 5.3     | Segregation of duties  | Conflicting duties and conflicting areas of responsibility shall be segregated.  | Reduce the risk of fraud, errors and circumvention of information security controls.   | Yes           | Yes                         |                    |            | X                                      | X                           |  |
|   | 5.4     | Management responsibilities  | Management shall require all personnel to apply information security in accordance with the established information security policy, topic-specific policies and procedures of the organization.   | Ensure that management understands its role in information security and takes action to ensure that all staff are aware of their responsibilities in the field of information security and compliance with it. | Yes           | Yes                         | X                  |            | X                                      | X                           |  |
|   | 5.5     | Contact with authorities   | The organization shall establish and maintain contact with relevant authorities.   | An appropriate flow of information related to information security between the organization and relevant legal, regulatory and supervisory authorities.  | Yes           | Yes                         | X                  |            | X                                      | X                           |  |
|   | 5.6     | Contact with special interest groups   | The organization shall establish and maintain contact with special interest groups or other specialist security forums and professional associations.  | To ensure an appropriate flow of information related to information security.  | Yes           | Yes                         |                    |            | X                                      | X                           |  |
|   | 5.7     | Threat intelligence  | Information relating to information security threats shall be collected and analysed to produce threat intelligence.   | To provide awareness of the possible threats to the organization so that the appropriate mitigation measures can be taken.   | Yes           | Yes                         |                    |            | X                                      | X                           |  |
|   | 5.8     | Information security in project management   | Information security shall be integrated into project management.  | Ensuring that information security risks within projects, deliverables and services throughout the life cycle of the project in an effective manner within the project management.                             | Yes           | Yes                         |                    |            | X                                      | X                           |  |
|   | 5.9     | Inventory of information and other associated assets   | An inventory of information and other associated assets, including owners, shall be developed and maintained.  | Identify the organization's information and other related assets to maintain its information security and assign appropriate ownership.  | Yes           | Yes                         |                    |            | X                                      | X                           |  |
|   | 5.10    | Acceptable use of information and other associated assets  | Rules for the acceptable use and procedures for handling information and other associated assets shall be identified, documented and implemented.  | Ensure that information and other related assets are adequately protected, used and treated.   | Yes           | Yes                         |                    |            | X                                      | X                           |  |
|   | 5.11    | Return of assets   | Personnel and other interested parties as appropriate shall return all the organization's assets in their possession upon change or termination of their employment, contract or agreement.  | Protecting the organization's assets as part of the change or termination of employment, contract or agreement.  | Yes           | Yes                         |                    |            | X                                      | X                           |  |
|   | 5.12    | Classification of information  | Information shall be classified according to the information security needs of the organization based on confidentiality, integrity, availability and relevant interested party requirements.  | Ensure that the identification and understanding of the protection needs for information are commensurate with its importance to the organization.   | Yes           | Yes                         |                    |            | X                                      | X                           |  |
|   | 5.13    | Labelling of information   | An appropriate set of procedures for information labelling shall be developed and implemented in accordance with the information classification scheme adopted by the organization.  | Enable the communication of the classification of information and support the automation of information processing and management.   | Yes           | Yes                         |                    |            | X                                      | X                           |  |
|   | 5.14    | Information transfer   | Information transfer rules, procedures, or agreements shall be in place for all types of transfer facilities within the organization and between the organization and other parties.   | Maintaining the security of information exchanged within an organization and with external stakeholders.   | Yes           | Yes                         |                    |            | X                                      | X                           |  |
|   | 5.15    | Access control   | Rules to control physical and logical access to information and other associated assets shall be established and implemented based on business and information security requirements.  | Establish authorized access and prevent unauthorized access to information and other related assets.   | Yes           | Yes                         |                    |            | X                                      | X                           |  |
|   | 5.16    | Identity management  | The full life cycle of identities shall be managed.  | The unique identification of individuals and systems that have access to the organization's information and other related assets, and enable proper assignment of access rights.                               | Yes           | Yes                         |                    |            | X                                      | X                           |  |
|   | 5.17    | Authentication information   | Allocation and management of authentication information shall be controlled by a management process, including advising personnel on appropriate handling of authentication information.   | Achieve proper authentication and prevent errors in authentication processes.  | Yes           | Yes                         |                    |            | X                                      | X                           |  |
|   | 5.18    | Access rights  | Access rights to information and other associated assets shall be provisioned, reviewed, modified and removed in accordance with the organization's topic-specific policy on and rules for access control.   | Ensure that access to information and other related assets is established and approved in accordance with business requirements.   | Yes           | Yes                         |                    |            | X                                      | X                           |  |
|   | 5.19    | Information security in supplier relationships   | Processes and procedures shall be defined and implemented to manage the information security risks associated with the use of supplier's products or services.   | Maintain an agreed level of information security in supplier relationships.  | Yes           | Yes                         |                    | X          | X                                      | X                           |  |
|   | 5.20    | Addressing information security within supplier agreements                                       | Relevant information security requirements shall be established and agreed with each supplier based on the type of supplier relationship.  | Maintain an agreed level of information security in supplier relationships.  | Yes           | Yes                         |                    | X          | X                                      | X                           |  |
|   | 5.21    | Managing information security in the information and communication technology (ICT) supply chain | Processes and procedures shall be defined and implemented to manage the information security risks associated with the ICT products and services supply chain.   | Maintain an agreed level of information security in supplier relationships.  | Yes           | Yes                         |                    | X          | X                                      | X                           |  |

Organizational controls

|      |  |   |  |     |     |   |   |   |   |  |
|------|--|---|--|-----|-----|---|---|---|---|--|
| 5.22 | Monitoring, review and change management of supplier services          | The organization shall regularly monitor, review, evaluate and manage change in supplier information security practices and service delivery.   | Maintain an agreed level of information security and service provision in accordance with the Supplier Agreements.   | Yes | Yes |   | X | X | X |  |
| 5.23 | Information security for use of cloud services                         | Processes for acquisition, use, management and exit from cloud services shall be established in accordance with the organization's information security requirements.   | Specify and manage information security for the use of cloud services.   | Yes | Yes |   | X | X | X |  |
| 5.24 | Information security incident management planning and preparation      | The organization shall plan and prepare for managing information security incidents by defining, establishing and communicating information security incident management processes, roles and responsibilities.           | To ensure a rapid, effective, consistent and orderly response to information security incidents, including communication of information security events.   | Yes | Yes | X |   | X | X |  |
| 5.25 | Assessment and decision on information security events                 | The organization shall assess information security events and decide if they are to be categorized as information security incidents.   | Achieve effective categorization and prioritization of information security events.  | Yes | Yes | X |   | X | X |  |
| 5.26 | Response to information security incidents                             | Information security incidents shall be responded to in accordance with the documented procedures.  | To ensure an efficient and effective response to information security incidents.   | Yes | Yes | X |   | X | X |  |
| 5.27 | Learning from information security incidents                           | Knowledge gained from information security incidents shall be used to strengthen and improve the information security controls.   | Reduce the likelihood or impact of future incidents.   | Yes | Yes | X |   | X | X |  |
| 5.28 | Collection of evidence   | The organization shall establish and implement procedures for the identification, collection, acquisition and preservation of evidence related to information security events.  | Establish consistent and effective management of evidence related to information security incidents in the context of disciplinary and judicial action.  | Yes | Yes | X |   | X | X |  |
| 5.29 | Information security during disruption                                 | The organization shall plan how to maintain information security at an appropriate level during disruption.   | Protect information and other related assets during a disruption.  | Yes | Yes | X |   | X | X |  |
| 5.30 | ICT readiness for business continuity                                  | ICT readiness shall be planned, implemented, maintained and tested based on business continuity objectives and ICT continuity requirements.   | Ensure the availability of the organization's information and other related assets during a disruption.  | Yes | Yes |   | X |   | X |  |
| 5.31 | Legal, statutory, regulatory and contractual requirements              | Legal, statutory, regulatory and contractual requirements relevant to information security and the organization's approach to meet these requirements shall be identified, documented and kept up to date.                | Achieve compliance with legal, statutory, regulatory, and contractual requirements related to information security.  | Yes | Yes |   | X |   | X |  |
| 5.32 | Intellectual property rights   | The organization shall implement appropriate procedures to protect intellectual property rights.  | To ensure compliance with legal, regulatory, statutory and contractual requirements related to intellectual property rights and the use of patented products.                                    | Yes | Yes | X | X |   | X |  |
| 5.33 | Protection of records  | Records shall be protected from loss, destruction, falsification, unauthorized access and unauthorized release.   | To achieve compliance with laws, regulations, statutory and contractual requirements, as well as community or societal expectations, regarding the protection and availability of registrations. | Yes | Yes | X |   |   | X |  |
| 5.34 | Privacy and protection of personal identifiable information (PII)      | The organization shall identify and meet the requirements regarding the preservation of privacy and protection of PII according to applicable laws and regulations and contractual requirements.                          | To ensure compliance with laws, regulations, statutory and contractual requirements relating to the information security aspects for the protection of personal data.                            | Yes | Yes | X |   |   | X |  |
| 5.35 | Independent review of information security                             | The organization's approach to managing information security and its implementation including people, processes and technologies shall be reviewed independently at planned intervals, or when significant changes occur. | Ensure that the organization continuously adopts an appropriate, adequate, and effective approach to information security management.  | Yes | Yes |   |   | X | X |  |
| 5.36 | Compliance with policies, rules and standards for information security | Compliance with the organization's information security policy, topic-specific policies, rules and standards shall be regularly reviewed.   | Ensure that information security is implemented and executed in accordance with the organization's information security policy, subject-specific policies, rules, and standards.                 | Yes | Yes |   |   | X | X |  |
| 5.37 | Documented operating procedures  | Operating procedures for information processing facilities shall be documented and made available to personnel who need them.   | Ensure the correct and safe operation of information processing facilities.  | Yes | Yes |   |   | X | X |  |

|                 |          |  |   |  |     |     |   |   |   |   |  |
|-----------------|----------|--|---|--|-----|-----|---|---|---|---|--|
| People controls | <b>6</b> | <b>People controls</b>                                     |   |  |     |     |   |   |   |   |  |
|                 | 6.1      | Screening  | Background verification checks on all candidates to become personnel shall be carried out prior to joining the organization and on an ongoing basis taking into consideration applicable laws, regulations and ethics and be proportional to the business requirements, the classification of the information to be accessed and the perceived risks. | Ensure that all staff are eligible and suitable for the roles for which they are being considered and that they remain eligible and suitable for them throughout their employment.   | Yes | Yes |   |   | X | X |  |
|                 | 6.2      | Terms and conditions of employment                         | The employment contractual agreements shall state the personnel's and the organization's responsibilities for information security.   | Ensure that staff understand their information security responsibilities for the roles they may be eligible for.   | Yes | Yes |   | X | X | X |  |
|                 | 6.3      | Information security awareness, education and training     | Personnel of the organization and relevant interested parties shall receive appropriate information security awareness, education and training and regular updates of the organization's information security policy, topic-specific policies and procedures, as relevant for their job function.   | Ensure that staff and relevant stakeholders are aware of and fulfil their information security responsibilities.   | Yes | Yes | X |   | X | X |  |
|                 | 6.4      | Disciplinary process                                       | A disciplinary process shall be formalized and communicated to take actions against personnel and other relevant interested parties who have committed an information security policy violation.  | Ensure that staff and other relevant stakeholders understand the consequences of a breach of the information security policy, deter staff and other relevant stakeholders from committing a breach, and appropriately address staff and other relevant stakeholders who have committed a breach. | Yes | Yes |   |   | X | X |  |
|                 | 6.5      | Responsibilities after termination or change of employment | Information security responsibilities and duties that remain valid after termination or change of employment shall be defined, enforced and communicated to relevant personnel and other interested parties.  | Protecting the interests of the organization as part of the employment or contract change or termination process.  | Yes | Yes |   | X | X | X |  |
|                 | 6.6      | Confidentiality or non-disclosure agreements               | Confidentiality or non-disclosure agreements reflecting the organization's needs for the protection of information shall be identified, documented, regularly reviewed and signed by personnel and other relevant interested parties.   | Maintain the confidentiality of information accessed by personnel or external parties.   | Yes | Yes |   |   | X | X |  |
|                 | 6.7      | Remote working   | Security measures shall be implemented when personnel are working remotely to protect information accessed, processed or stored outside the organization's premises.  | Ensure the security of information when staff are working remotely.  | Yes | Yes |   |   | X | X |  |

|                        |                         |   |  |   |     |     |  |   |   |   |   |   |   |
|------------------------|-------------------------|---|--|---|-----|-----|--|---|---|---|---|---|---|
|                        | 6.8                     | Information security event reporting  | The organization shall provide a mechanism for personnel to report observed or suspected information security events through appropriate channels in a timely manner.  | Support timely, consistent, and effective reporting of information security events that can be identified by personnel.   | Yes | Yes |  |   |   | X | X |   |   |
| Physical controls      | 7                       | Physical controls   |  |   |     |     |  |   |   |   |   |   |   |
|                        | 7.1                     | Physical security perimeters  | Security perimeters shall be defined and used to protect areas that contain information and other associated assets.   | Prevent unauthorized physical access to, damage to, and interference with information and other related organizational assets.  | Yes | Yes |  |   |   |   | X | X |   |
|                        | 7.2                     | Physical entry  | Secure areas shall be protected by appropriate entry controls and access points.   | Ensuring that only authorized physical access to the organization's information and other related assets takes place.   | Yes | Yes |  |   |   |   | X | X |   |
|                        | 7.3                     | Securing offices, rooms and facilities  | Physical security for offices, rooms and facilities shall be designed and implemented.   | Prevent unauthorized physical access to, damage to, and interference with information and other related assets of the organization in offices, spaces, and facilities.                        | Yes | Yes |  |   |   |   | X | X |   |
|                        | 7.4                     | Physical security monitoring  | Premises shall be continuously monitored for unauthorized physical access.   | Detect and deter unauthorized physical access.  | Yes | Yes |  |   |   |   | X | X |   |
|                        | 7.5                     | Protecting against physical and environmental threats   | Protection against physical and environmental threats, such as natural disasters and other intentional or unintentional physical threats to infrastructure shall be designed and implemented.                                    | Prevent or prevent the consequences of events arising from physical and environmental threats limit.  | Yes | Yes |  |   |   |   | X | X |   |
|                        | 7.6                     | Working in secure areas   | Security measures for working in secure areas shall be designed and implemented.   | Protecting information and other related assets in secure areas from damage and unauthorised disturbance by personnel working in these areas.   | Yes | Yes |  |   | X |   | X | X |   |
|                        | 7.7                     | Clear desk and clear screen   | Clear desk rules for papers and removable storage media and clear screen rules for information processing facilities shall be defined and appropriately enforced.  | Reduce the risks of unauthorized access, loss of, and damage to information on desks, screens, and other accessible places during and outside of normal working hours.                        | Yes | Yes |  |   |   |   | X | X |   |
|                        | 7.8                     | Equipment siting and protection   | Equipment shall be sited securely and protected.   | Reduce the risks of physical and environmental threats and of unauthorized access and damage.   | Yes | Yes |  |   |   |   | X | X |   |
|                        | 7.9                     | Security of assets off-premises   | Off-site assets shall be protected.  | Prevent loss, damage, theft, or compromise of assets outside the building and/or grounds and interruption of the organization's operations.   | Yes | Yes |  |   |   |   | X | X |   |
|                        | 7.10                    | Storage media   | Storage media shall be managed through their life cycle of acquisition, use, transportation and disposal in accordance with the organization's classification scheme and handling requirements.                                  | To effect only the permissible disclosure, modification, deletion or destruction of information on storage media.   | Yes | Yes |  |   |   |   | X | X |   |
|                        | 7.11                    | Supporting utilities  | Information processing facilities shall be protected from power failures and other disruptions caused by failures in supporting utilities.   | Prevent loss, damage, or compromise of information and other related assets or interruption of the organization's operations due to disruption and disruption of supporting utilities.        | Yes | Yes |  |   |   |   | X | X |   |
|                        | 7.12                    | Cabling security  | Cables carrying power, data or supporting information services shall be protected from interception, interference or damage.   | Prevent loss, damage, theft, or compromise of information and other related assets and interruption of the organization's operations related to power and communication cables.               | Yes | Yes |  |   |   |   | X | X |   |
|                        | 7.13                    | Equipment maintenance   | Equipment shall be maintained correctly to ensure availability, integrity and confidentiality of information.  | Prevent loss, damage, theft, or compromise of information and other related assets and interruption of the organization's operations due to inadequate maintenance.                           | Yes | Yes |  |   |   |   | X | X |   |
|                        | 7.14                    | Secure disposal or re-use of equipment  | Items of equipment containing storage media shall be verified to ensure that any sensitive data and licensed software has been removed or securely overwritten prior to disposal or re-use.                                      | Prevent information leakage through equipment to be disposed of or reused.  | Yes | Yes |  |   |   |   | X | X |   |
| Technological controls | 8                       | Technological controls  |  |   |     |     |  |   |   |   |   |   |   |
|                        | 8.1                     | User end point devices  | Information stored on, processed by or accessible via user end point devices shall be protected.   | Protecting information from the risks associated with the use of user endpoint devices.   | Yes | Yes |  |   |   |   | X | X |   |
|                        | 8.2                     | Privileged access rights  | The allocation and use of privileged access rights shall be restricted and managed.  | Ensuring that only authorized users, software components, and services are granted special access rights.   | Yes | Yes |  |   |   |   | X | X |   |
|                        | 8.3                     | Information access restriction  | Access to information and other associated assets shall be restricted in accordance with the established topic-specific policy on access control.  | Establish only authorized access and prevent unauthorized access to information and other related assets.   | Yes | Yes |  |   |   |   | X | X |   |
|                        | 8.4                     | Access to source code   | Read and write access to source code, development tools and software libraries shall be appropriately managed.   | Prevent unauthorized functionality from being introduced, prevent accidental or malicious changes, and maintain the confidentiality of valuable intellectual property.                        | Yes | Yes |  |   |   |   | X | X |   |
|                        | 8.5                     | Secure authentication   | Secure authentication technologies and procedures shall be implemented based on information access restrictions and the topic-specific policy on access control.   | Ensure that a user or an entity is securely authenticated when access to systems, applications, and services is granted.  | Yes | Yes |  |   |   |   |   | X |   |
|                        | 8.6                     | Capacity management   | The use of resources shall be monitored and adjusted in line with current and expected capacity requirements.  | Ensure the required capacity of information processing facilities, personnel, offices and other facilities.   | Yes | Yes |  |   |   |   |   | X |   |
|                        | 8.7                     | Protection against malware  | Protection against malware shall be implemented and supported by appropriate user awareness.   | Ensure that information and other related assets are protected from malware.  | Yes | Yes |  |   |   |   |   |   | X |
|                        | 8.8                     | Management of technical vulnerabilities   | Information about technical vulnerabilities of information systems in use shall be obtained, the organization's exposure to such vulnerabilities shall be evaluated and appropriate measures shall be taken.                     | Prevent the exploitation of technical vulnerabilities.  | Yes | Yes |  |   |   |   | X | X |   |
|                        | 8.9                     | Configuration management  | Configurations, including security configurations, of hardware, software, services and networks shall be established, documented, implemented, monitored and reviewed.   | Ensure that hardware, software, services, and networks function correctly with the required security settings and that the configuration is not altered by unauthorized or incorrect changes. | Yes | Yes |  |   |   |   | X | X |   |
|                        | 8.10                    | Information deletion  | Information stored in information systems, devices or in any other storage media shall be deleted when no longer required.   | Prevent unnecessary disclosure of sensitive information and comply with legal, regulatory, statutory and contractual requirements for deletion of information.                                | Yes | Yes |  | X |   |   | X | X |   |
|                        | 8.11                    | Data masking  | Data masking shall be used in accordance with the organization's topic-specific policy on access control and other related topic-specific policies, and business requirements, taking applicable legislation into consideration. | Restrict the disclosure of sensitive information, including personal data, and comply with legal, regulatory, statutory, and contractual requirements.  | Yes | Yes |  | X |   |   | X | X |   |
| 8.12                   | Data leakage prevention | Data leakage prevention measures shall be applied to systems, networks and any other devices that process, store or transmit sensitive information. | To detect and prevent the unauthorized disclosure and extraction of information by persons or systems.   | Yes   | Yes |     |  |   |   | X | X |   |   |

|                        |  |   |   |  |     |     |   |  |   |   |   |  |
|------------------------|--|---|---|--|-----|-----|---|--|---|---|---|--|
| Technological controls | 8.13   | Information backup  | Backup copies of information, software and systems shall be maintained and regularly tested in accordance with the agreed topic-specific policy on backup.        | Enable recovery from data or system loss.  | Yes | Yes |   |  |   | X | X |  |
|                        | 8.14   | Redundancy of information processing facilities   | Information processing facilities shall be implemented with redundancy sufficient to meet availability requirements.  | Ensure the uninterrupted operation of information processing facilities.   | Yes | Yes |   |  |   | X | X |  |
|                        | 8.15   | Logging   | Logs that record activities, exceptions, faults and other relevant events shall be produced, stored, protected and analysed.                                      | Log events, generate evidence, ensure the integrity of information in log files, prevent unauthorized access, identify information security events that could lead to an information security incident, and support investigations.  | Yes | Yes |   |  |   | X | X |  |
|                        | 8.16   | Monitoring activities   | Networks, systems and applications shall be monitored for anomalous behaviour and appropriate actions taken to evaluate potential information security incidents. | Detect anomalous behavior and potential information security incidents.  | Yes | Yes |   |  |   | X | X |  |
|                        | 8.17   | Clock synchronization   | The clocks of information processing systems used by the organization shall be synchronized to approved time sources.   | Enable the correlation and analysis of security-related events and other recorded data and support investigations in the event of information security incidents.  | Yes | Yes |   |  |   | X | X |  |
|                        | 8.18   | Use of privileged utility programs  | The use of utility programs that can be capable of overriding system and application controls shall be restricted and tightly controlled.                         | Ensure that the use of system tools does not harm system and application control measures for information security.  | Yes | Yes |   |  |   | X | X |  |
|                        | 8.19   | Installation of software on operational systems   | Procedures and measures shall be implemented to securely manage software installation on operational systems.   | Ensure the integrity of operational systems and prevent the exploitation of technical vulnerabilities.   | Yes | Yes |   |  |   | X | X |  |
|                        | 8.20   | Networks security   | Networks and network devices shall be secured, managed and controlled to protect information in systems and applications.   | Protecting information in networks and the supporting information processing facilities from compromise over the network.  | Yes | Yes |   |  |   | X | X |  |
|                        | 8.21   | Security of network services  | Security mechanisms, service levels and service requirements of network services shall be identified, implemented and monitored.                                  | To ensure security when using network services.  | Yes | Yes |   |  |   | X | X |  |
|                        | 8.22   | Segregation of networks   | Groups of information services, users and information systems shall be segregated in the organization's networks.   | Split the network with security boundaries and control the traffic between them based on the business needs.   | Yes | Yes |   |  |   | X | X |  |
|                        | 8.23   | Web filtering   | Access to external websites shall be managed to reduce exposure to malicious content.   | Protect systems to prevent malware from compromising them and to prevent access to unauthorized Internet resources.  | Yes | Yes |   |  |   | X | X |  |
|                        | 8.24   | Use of cryptography   | Rules for the effective use of cryptography, including cryptographic key management, shall be defined and implemented.  | To ensure the correct and effective use of cryptography to protect the confidentiality, authenticity or integrity of information in accordance with business and information security requirements and in compliance with the requirements of legal, regulatory, statutory and contractual requirements relating to cryptography | Yes | Yes | X |  |   | X | X |  |
|                        | 8.25   | Secure development life cycle   | Rules for the secure development of software and systems shall be established and applied.  | Ensure that information security is designed and implemented within the secure development cycle of software and systems.  | Yes | Yes |   |  |   | X | X |  |
|                        | 8.26   | Application security requirements   | Information security requirements shall be identified, specified and approved when developing or acquiring applications.  | Ensuring that all information security requirements are identified and taken into account when developing or purchasing applications.  | Yes | Yes |   |  |   | X | X |  |
|                        | 8.27   | Secure system architecture and engineering principles   | Principles for engineering secure systems shall be established, documented, maintained and applied to any information system development activities.              | Ensure that information systems are designed, deployed, and managed securely within the development lifecycle.   | Yes | Yes |   |  |   | X | X |  |
|                        | 8.28   | Secure coding   | Secure coding principles shall be applied to software development.  | Ensure that secure software is written that reduces the number of potential information security vulnerabilities in the software.  | Yes | Yes |   |  |   | X | X |  |
|                        | 8.29   | Security testing in development and acceptance  | Security testing processes shall be defined and implemented in the development life cycle.  | Validate that information security requirements are met when deploying applications or code in the production environment.   | Yes | Yes |   |  |   | X | X |  |
|                        | 8.30   | Outsourced development  | The organization shall direct, monitor and review the activities related to outsourced system development.  | Ensure that the information security measures required by the organization are implemented in outsourced system development.   | Yes | Yes |   |  |   | X | X |  |
|                        | 8.31   | Separation of development, test and production environments   | Development, testing and production environments shall be separated and secured.  | Protect the production environment and data from compromise from development and testing activities.   | Yes | Yes |   |  |   | X | X |  |
|                        | 8.32   | Change management   | Changes to information processing facilities and information systems shall be subject to change management procedures.  | Maintain information security while making changes.  | Yes | Yes |   |  |   | X | X |  |
| 8.33                   | Test information                                       | Test information shall be appropriately selected, protected and managed.  | Ensure the relevance of testing and the protection of operational data used for testing.  | Yes  | Yes |     |   |  | X | X |   |  |
| 8.34                   | Protection of information systems during audit testing | Audit tests and other assurance activities involving assessment of operational systems shall be planned and agreed between the tester and appropriate management. | Minimize the impact of audit and other assurance activities on operational systems and business processes.  | Yes  | Yes |     | X |  | X | X |   |  |