5. Organizational Controls

- 37 controls
- Structured approach to managing risks
- Align policies with business objectives
- Address legal, regulatory requirements
- Emphasize human factors in security
- Manage physical and digital assets
- Monitor and review supplier services

Organizational Controls (5.1-5.5)

5.1 Policies for Information Security : Define, approve, publish, communicate policies to all.

5.2 Information Security Roles and Responsibilities : Define and allocate the responsibilities for information security.

5.3 Segregation of Duties : Duties and areas of responsibility should be segregated to avoid conflicts.

5.4 Management Responsibilities : Ensure management knows their role in infosec and promotes awareness.

5.5 Contact with Authorities : Encourage proactive security and facilitate timely sharing of critical information.

Organizational Controls (5.6-5.10)

5.6 Contact with Special Interest Groups : Maintain contacts with special interest groups to stay updated regarding information security

5.7 Threat Intelligence : Gathering and analysing information about current and future cyber attacks

5.8 Information Security in Project Management : Addresses information security in project management

5.9 Inventory of Information and Other Associated Assets : Identify Information assets and owners to preserve their security

5.10 Acceptable Use of Information and Other Associated Assets : Define and Document the rules of acceptable use of assets

Organizational Controls (5.11-5.15)

5.11 Return of Assets : Protect assets when changing or terminating employment

5.12 Classification of Information : Identification of protection needs of information in accordance with its importance

5.13 Labeling of Information : To facilitate the communication of information classification

5.14 Information Transfer : Protect information in transfer from interception, copying, modification, mis-routing and destruction

5.15 Access Control : To secure authorized access and prevent unauthorized access to information and assets.

Organizational Controls (5.16-5.20)

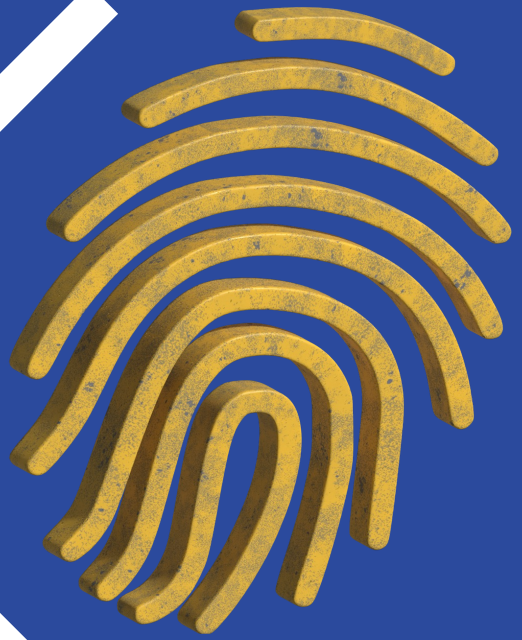
5.16 Identity Management : Uniquely identify individuals and systems accessing an organization's information assets and assign appropriate access rights.

5.17 Authentication Information : To ensure proper entity authentication and prevent failures of authentication processes.

5.18 Access Rights : Define and authorise access according to business requirements

5.19 Information Security in Supplier Relationships : Mitigate the risks on information assets accessible by suppliers.

5.20 Addressing Security Within Supplier Agreements : Establish and agree al relevant information security requirements.



Organizational Controls (5.21-5.25)

5.21 Managing Information Security in the ICT Supply Chain: Address risks of the provided information and communication technology services

5.22 Monitoring, Review & Change Management of Supplier Services: Regularly monitor, review and audit supplier service delivery.

5.23 Information Security for Use of Cloud Services : To specify and manage information security for the use of cloud services.

5.24 Information Security Incident Management Planning and Preparation: Ensure effective response to security incidents.

5.25 Assessment and Decision on Information Security Events: Assess events, categorize as security incidents.

Organizational Controls (5.26-5.30)

5.26 Response to Information Security Incidents: To ensure efficient and effective response to information security incidents

5.27 Learning from Information Security Incidents: Reduce the likelihood or consequences of future incidents

5.28 Collection of Evidence: Ensure effective evidence management for legal purposes

5.29 Information Security During Disruption: Protect information and other associated assets during disruption

5.30 ICT Readiness for Business Continuity: Ensure availability of information during disruption

Organizational Controls (5.31-5.35)

5.31 Statutory, Regulatory and Contractual Requirements: Comply with legal, regulatory, and contract requirements.

5.32 Intellectual Property Rights: Comply with legal requirements for intellectual property rights and proprietary products

5.33 Protection of records: Ensure compliance with legal, regulatory, and contractual requirements

5.34 Privacy and Protection of PII: Compliance with legal requirements for PII protection

5.35 Independent Review of Information Security: Ensure ongoing effective information security management

Organizational Controls (5.36-5.37)

5.36 Compliance with Policies, Rules and Standards for Information Security: To ensure information security compliance with policy.

5.37 Documented operating procedures: Ensure secure and correct operation of information facilities.