Agenda

- What is Compliance?
- Risk and Compliance Management
- What is a Framework?
- ISO 27001/27002 Overview
- Audit and Remediate
- Improve and Automate

What was Compliance?

What is a Control?

Control is defined as the **policies**, **procedures**, **practices** and **organizational structures** designed to provide reasonable assurance that business objectives will be achieved and undesired events will be prevented or detected and corrected.

*Source: ITGI, COBIT 4.1

Why use a framework?

- Enable effective governance
- Align with business goals
- Standardize process and approach
- Enable structured audit and/or assessment
- Control cost
- Comply with external requirements

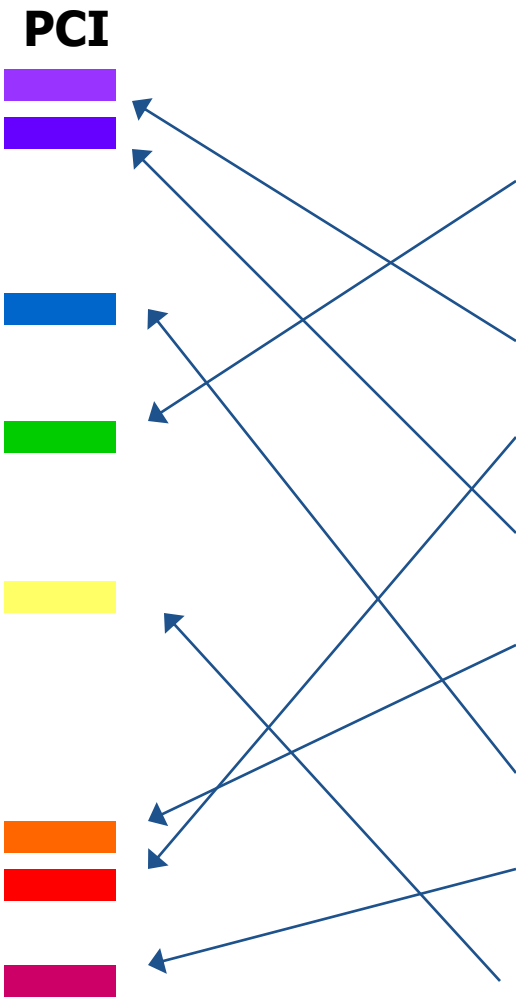
Frameworks and Control Sets

- ISO 27001/27002
- COBIT
- ITIL
- NIST
- Industry-specific – i.e. PCI
- Custom

Frameworks Comparison

Framework	Strengths	Focus
COBIT	Strong mappings Support of ISACA Availability	IT Governance Audit
ISO 27001/27002	Global Acceptance Certification	Information Security Management System
ITIL	IT Service Management Certification	IT Service Management
NIST 800-53	Detailed, granular Tiered controls Free	Information Systems FISMA

Controls Mapping



PCI Data Security Standard

1. Install and maintain a firewall configuration to protect data
2. Do not use vendor-supplied defaults for system passwords and other security parameters
3. Protect stored data
4. Encrypt transmission of cardholder data and sensitive information across public networks
5. Use and regularly update anti-virus software
6. Develop and maintain secure systems and applications
7. Restrict access to data by business need to know
8. Assign a unique ID to each person with computer access…

Logging and Monitoring

PCI – Requirement 10

Requirement 10: Track and monitor all access to network resources and cardholder data.

Logging mechanisms and the ability to track user activities are critical. The presence of logs in all environments allows thorough tracking and analysis when something does go wrong. Determining the cause of a compromise is very difficult without system activity logs.

- **10.2.1** All individual user accesses to cardholder data
- **10.2.2** All actions taken by any individual with root or administrative privileges
- **10.2.3** Access to all audit trails
- **10.2.4** Invalid logical access attempts
- **10.2 5** Use of identification and authentication mechanisms
- **10.2.6** Initialization of the audit logs
- **10.2.7** Creation and deletion of system-level objects.

ISO 17799 – Section 10.10

10.10 Monitoring

Objective: To detect unauthorized information processing activities.

Systems should be monitored and information security events should be recorded. Operator logs and fault log

An orga logging

System conform

Implementation guidance

Audit logs should include, when relevant:

a) user IDs;

b) dates, times, and details of key events, e.g. log-on and log-off;

Organization Example

IT Service Desk

ITIL

Information Security

ISO 27001/27002

Software Delivery

CMMi

Internal Audit

COBIT

Practical Uses for Certification

Regulatory Compliance	**“Best Practice” approach to handling sensitive data and overall security program**
Internal Compliance	**Implement security as an integrated part of the business and as a process**
Third Party Compliance	**Provide proof to partners of good practices around data protection. Strengthen SAS 70 approach.**

ISO 27001/27002

- Information Security Framework

From BS7799

- Requirements and guidelines for development of an ISMS (Information Security Management System)
- Risk Management a key component of ISMS
- Part of ISO 27000 Series of security standards

A Brief History of ISO 27001

BS 7799-1

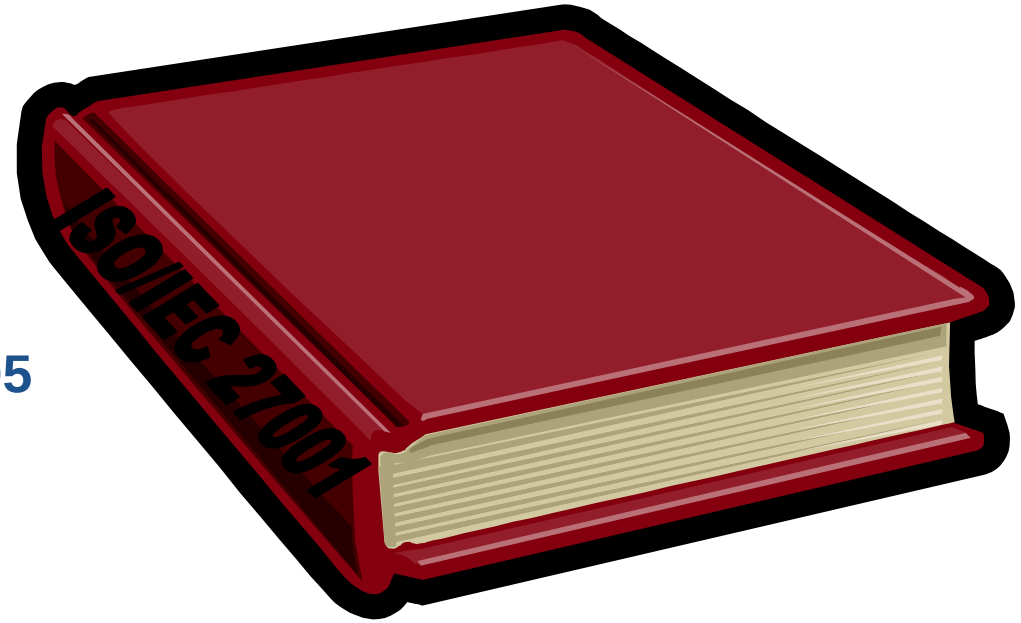
Code of Practice

BS 7799-2

Specification

Revised in 2002

Adopted as international standard in 2005



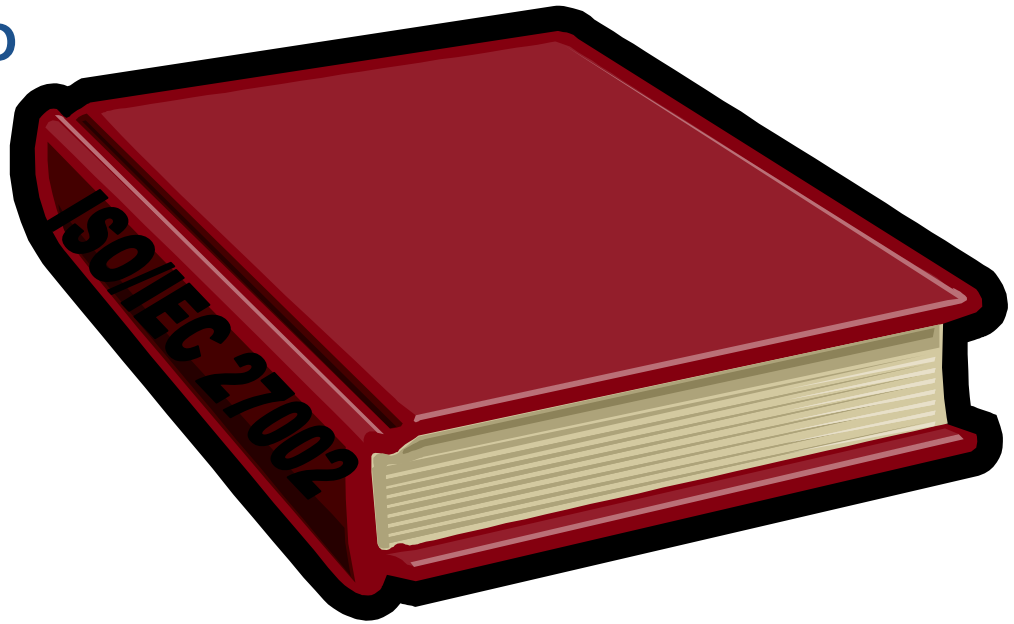
A Brief History of ISO 27002

BS 7799-1

Code of Practice

Adopted as international standard as ISO 17799 in 2000

Revised in 2005
Renumbered to 27002 in 2007



Information Technology

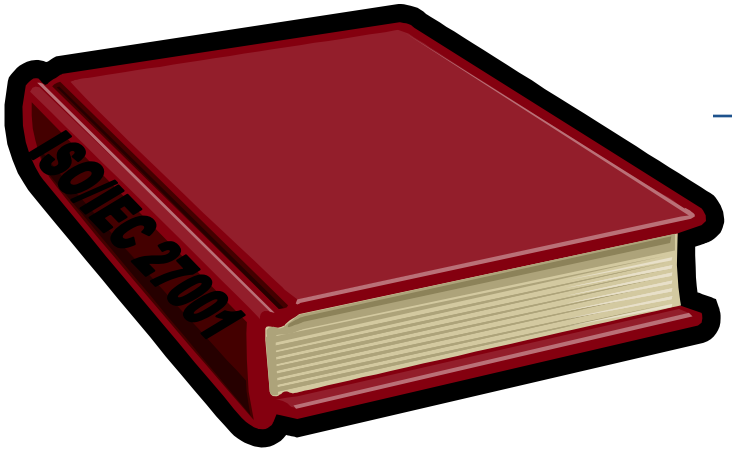
Code of Practice for Information Security Management

BS 7799-2

Specification

Revised in 2002

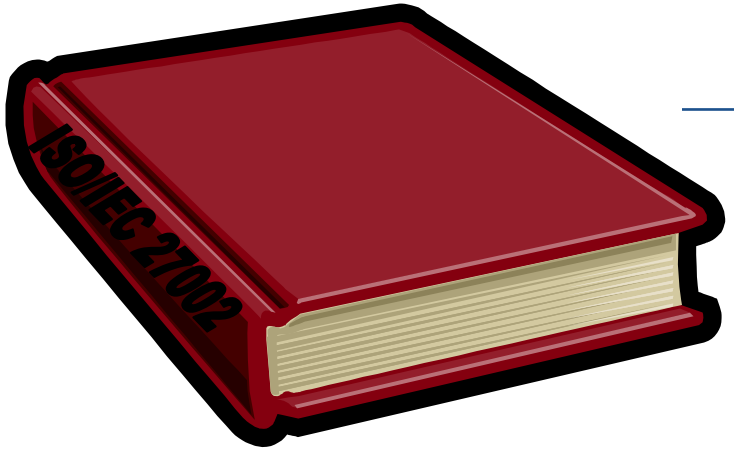
ISO 27001 and 27002



ISO 27001

- Requirements
- Auditable
- Certification

Shared Control Objectives



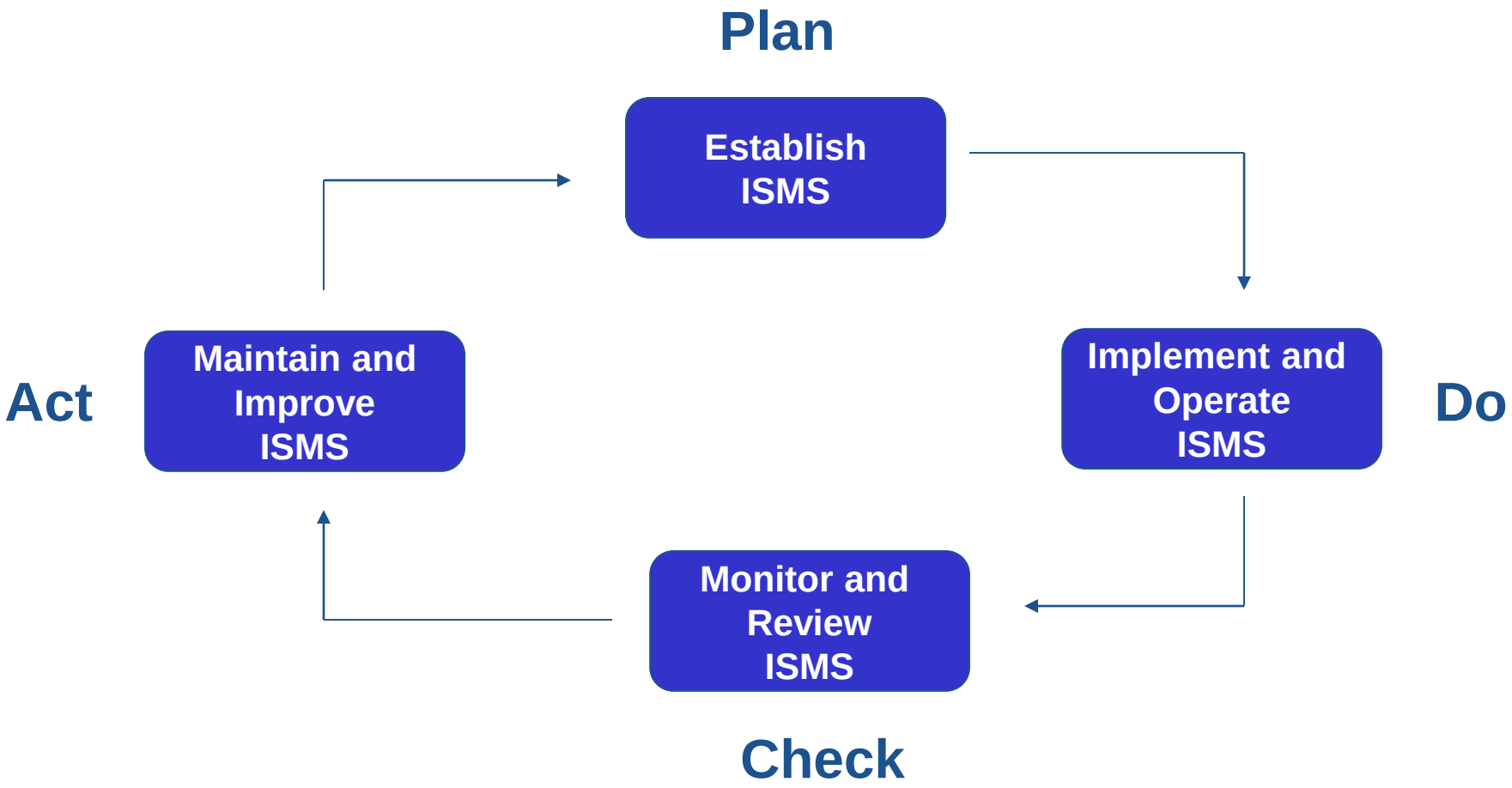
ISO 27002

- Best Practices
- More depth in controls guidance

ISO 27001 – Mgmt Framework

- Information Security Management Systems – Requirements (ISMS)
  - Process approach
    - Understand organization's information security requirements and the need to establish policy
    - Implement and operate controls to manage risk, in context of business risk
    - Monitor and review
    - Continuous improvement

ISO 27001


Plan
Establish ISMS
Implement and Operate ISMS
Do
Monitor and Review ISMS
Check
Maintain and Improve ISMS
Act

ISO 27002 – Controls Framework

ISO 27002 Security Control Domains in ISO27002:2005

- Risk Assessment and Treatment
- Security Policy
- Organizing Information Security
- Asset Management
- Human Resources Security
- Physical and Environmental Security
- Communications and Operations Management
- Access Control
- Information Systems Acquisition, Development and Maintenance
- Information Security Incident Management
- Business Continuity Management
- Compliance

Building a Framework ISO 27002

ISO 27002: Code of Practice for Information Security Management

ISO 27000 Series of Standards

- ISO/IEC 27000:2009 - Overview and vocabulary
- ISO/IEC 27001:2005 **(:2013)**- Requirements
- ISO/IEC 27002:2005 **(:2013)** - Code of Practice
- ISO/IEC 27003 - ISMS Implementation Guidance*
- ISO/IEC 27004 - Measurement*
- ISO/IEC 27005:2008 - Risk Management
- ISO/IEC 27006:2007 - Auditor Requirements
- ISO/IEC 27007 - ISMS Audit Guidelines*

*In Development

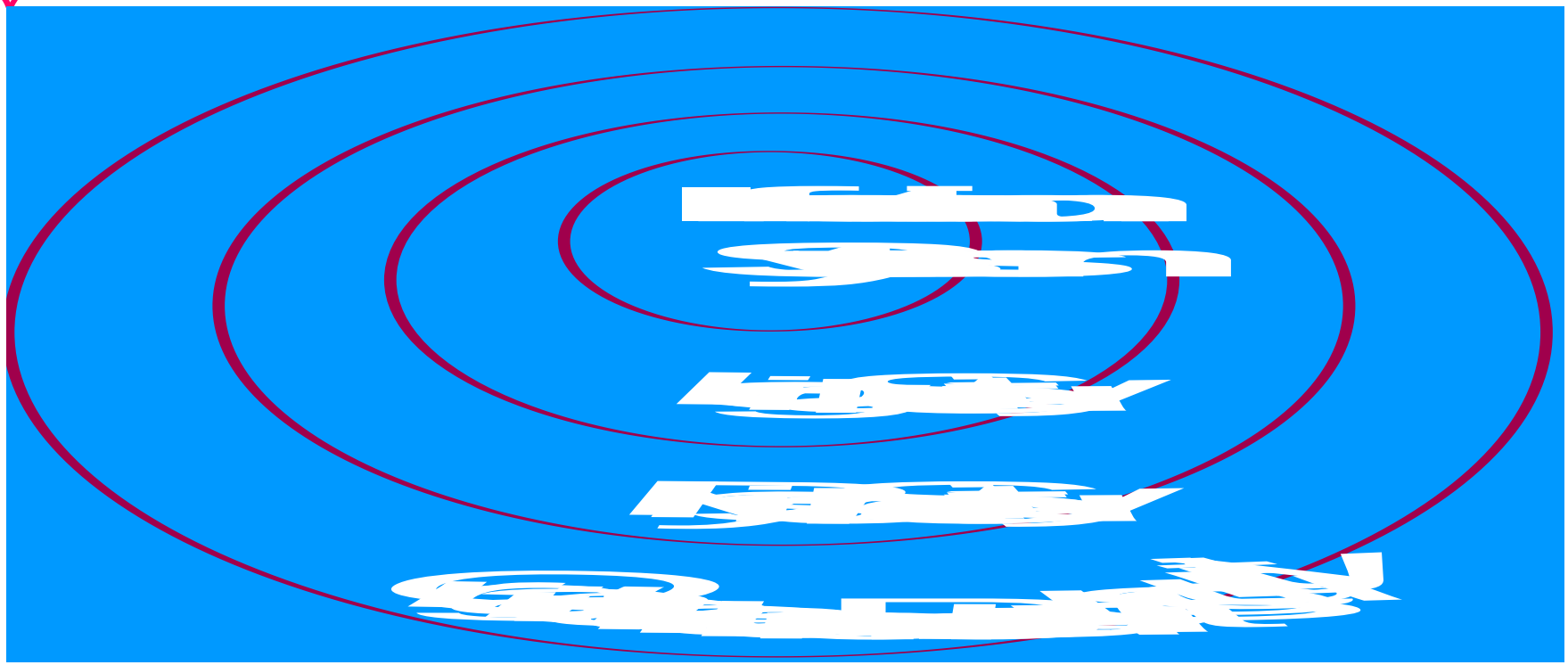
ISMS Standards

- ISO/ IEC 27001 : 2005
  - A specification (specifies requirements for implementing, operating, monitoring, reviewing, maintaining & improving a documented ISMS)
  - Specifies the requirements of implementing of Security control, customised to the needs of individual organisation or part thereof.
  - Used as a basis for certification
- ISO/IEC 27002 : 2005 (Originally ISO/IEC 17799:2005)
  - A code of practice for Information Security management
  - Provides best practice guidance
  - Use as required within your business
  - Not for certification

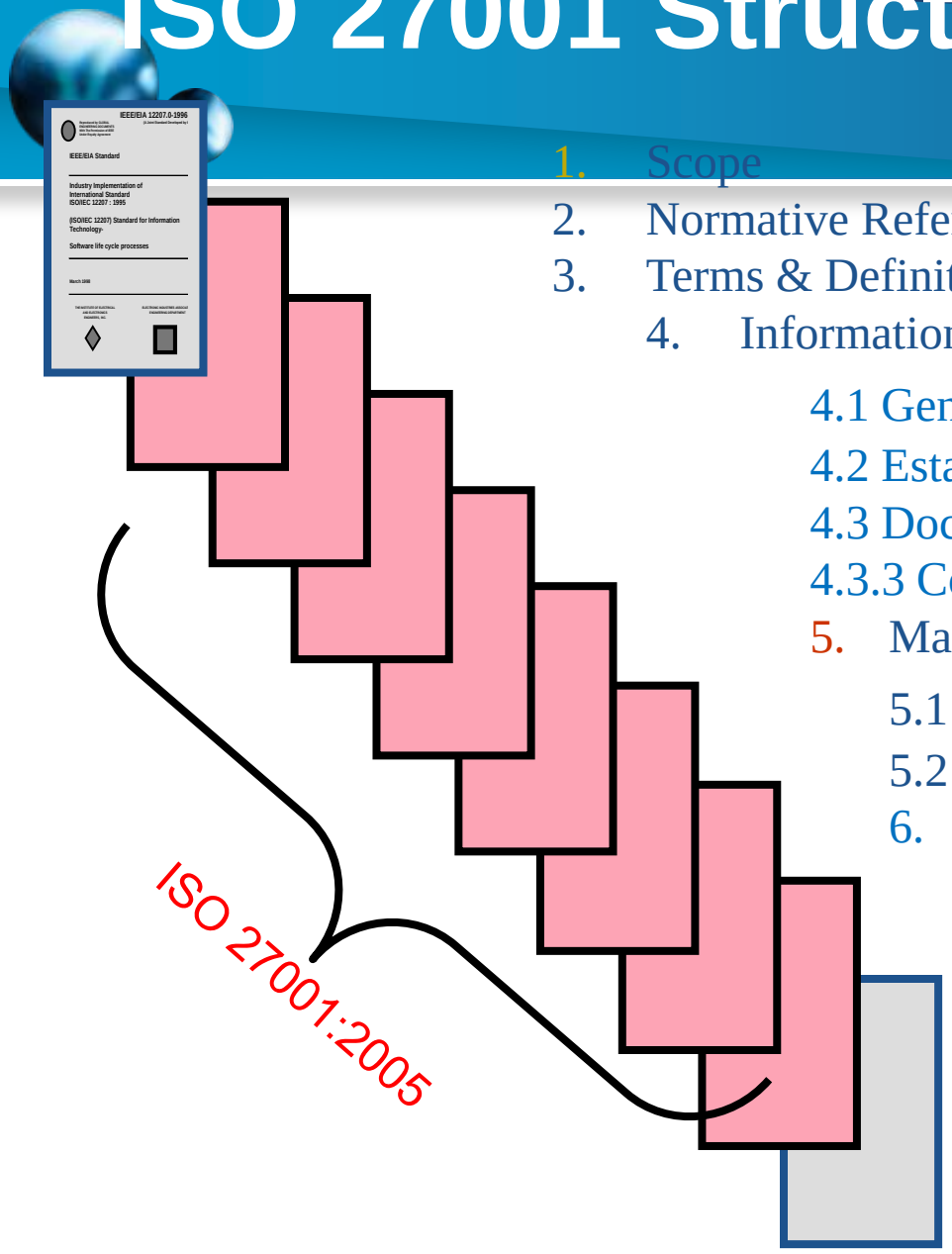
Both ISO 27001 and ISO 27002 security control clauses are fully harmonized

IN PRACTICE….

Information Security ……



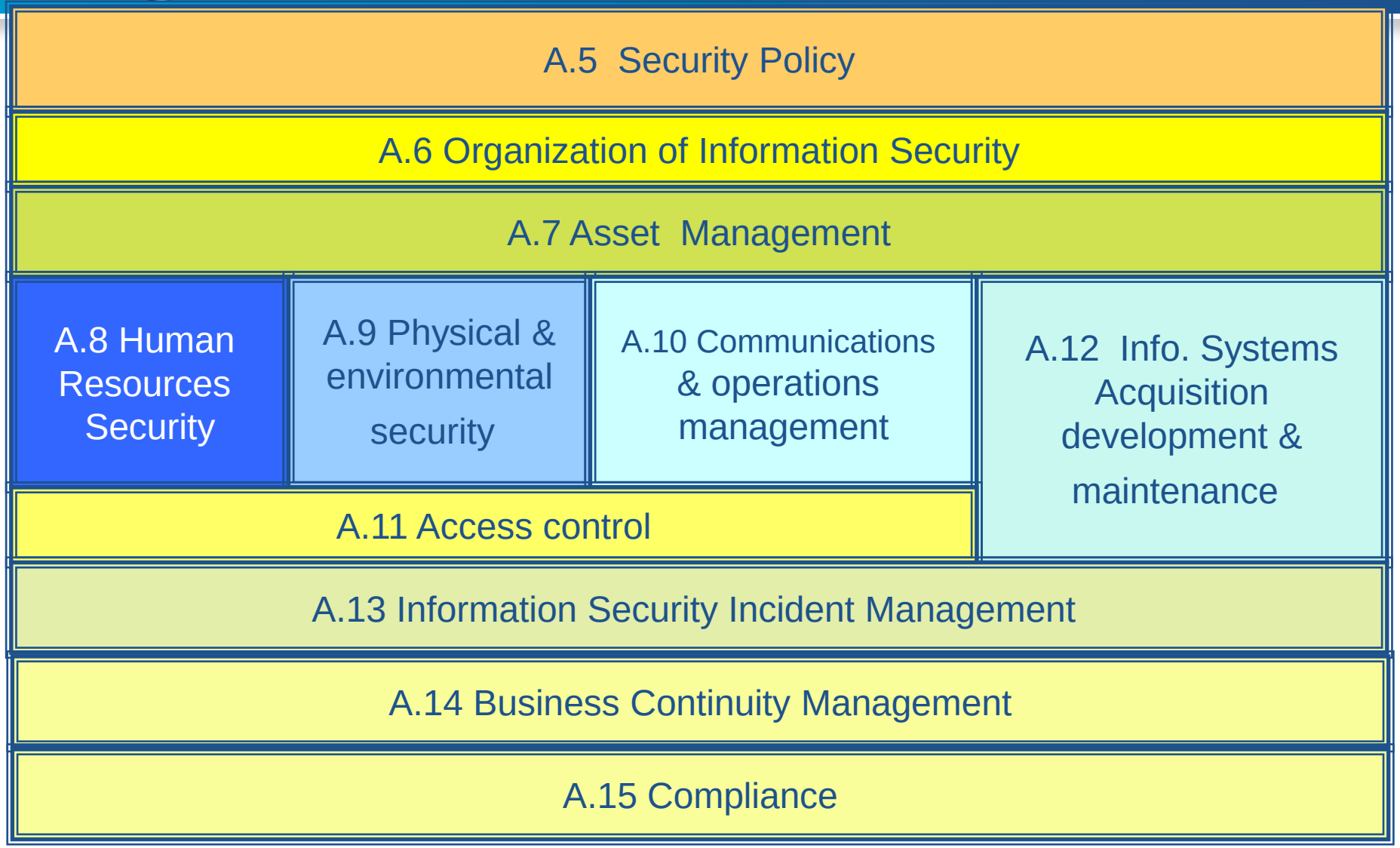
ISO 27001 Structure



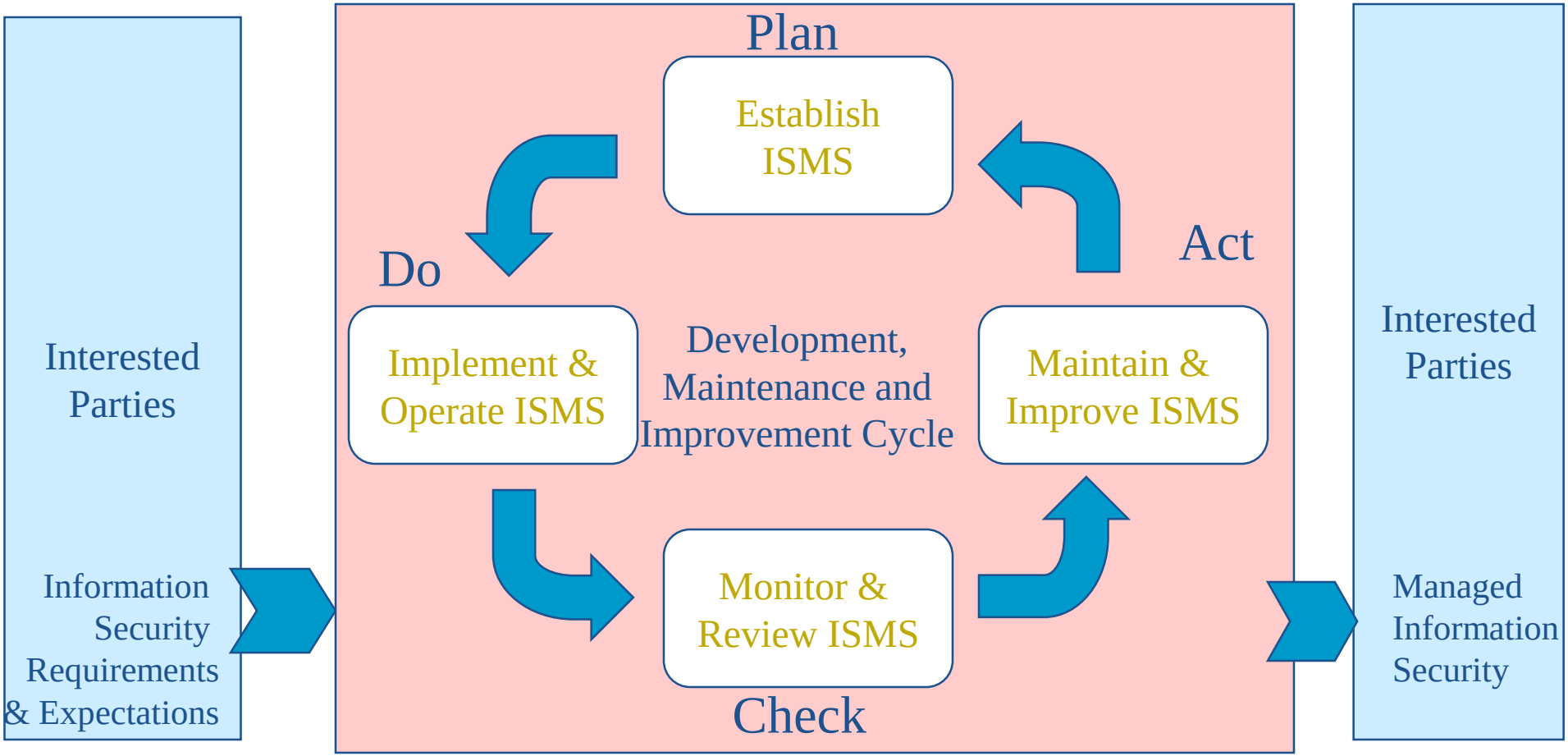
1. Scope
2. Normative References
3. Terms & Definitions
4. Information Security Management System
   - 4.1 General
   - 4.2 Establish and manage ISMS
   - 4.3 Documentation
   - 4.3.3 Control of Records
5. Management Responsibility
   - 5.1 Management Commitment
   - 5.2 Resource Management
6. Internal ISMS Audits
7. Management Review of the ISMS
8. ISMS Improvement
   - 8.1 Continual Improvement
   - 8.2 Corrective Actions
   - 8.3 Preventive Actions

Annexure A,B & C

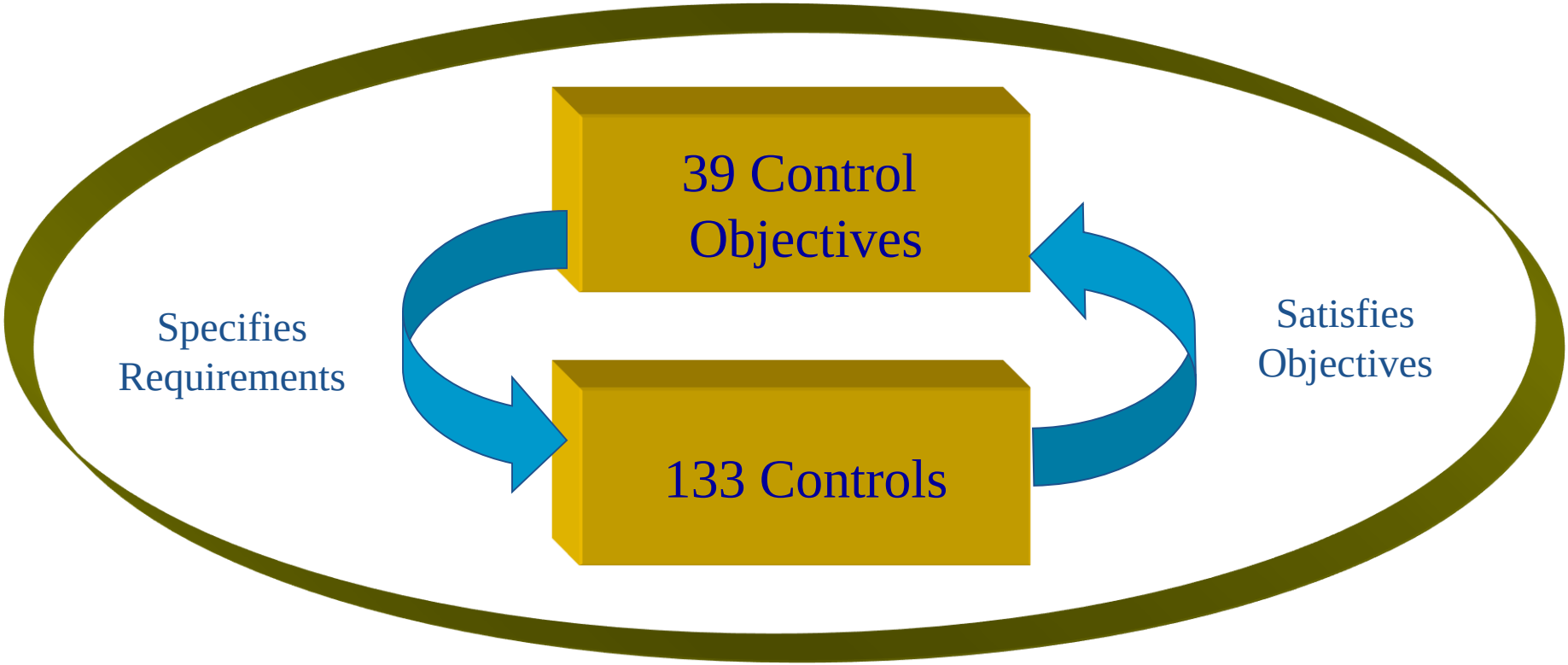
Structure of Annexure-A



PDCA Model applied to ISMS Processes



ISO 27001: Control Objectives and Controls

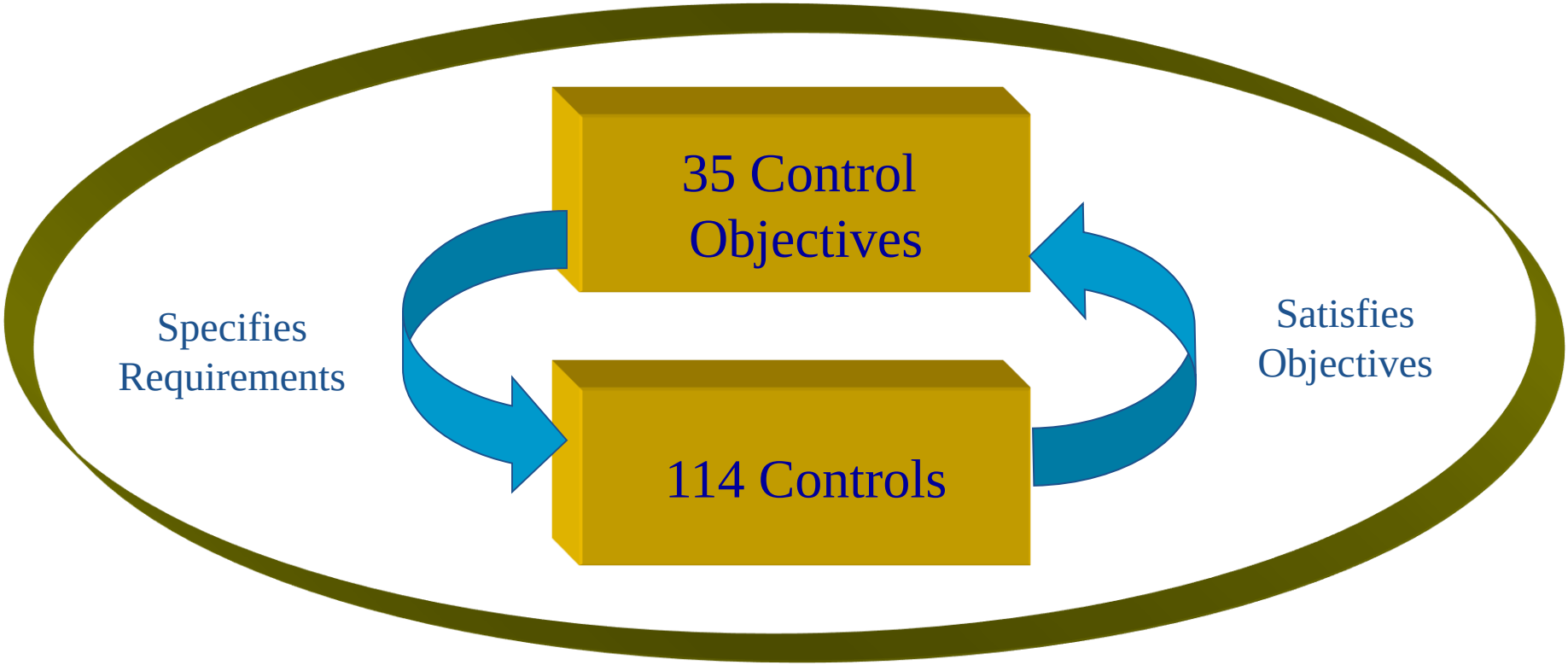


11 Domains
Clauses

ISO 27002:2005 Structure

- 1 introductory clause on Risk assessment and Treatment.
- 11 security Control Clauses (fully harmonised with ISO 27001)
- 39 main Security categories each containing
  - Control Objective and
  - One or more control to support achievement of control objective
- Control descriptions each containing
  - Control statement
  - Implementation Guidance
  - Other Information

ISO 27001:2013 Control Objectives and Controls



14 Domains
Clauses

ISO 27002:2013 Structure

- 14 security Control Clauses
- 35 main Security categories each containing
  - Control Objective and
  - One or more control to support achievement of control objective
- Control descriptions each containing
  - Control statement
  - Implementation Guidance
  - Other Information

  114 Controls in total

ISO/IEC 2013: Clauses

ISO27002:2013
5 Information security policies
6 Organization of information security
7 Human resource security
8 Asset management
9 Access control
10 Cryptography
11 Physical and environmental security
12 Operations security
13 Communications security
14 System acquisition, development and maintenance
15 Supplier relationships
16 Information security incident management
17 Information security aspects of business continuity management

ISO27002:2005 vs ISO 27002:2013

5 Security Policy *5 Security Policy*

6 Organization of information security
6 Organization of Information Security

8 Asset management *7 Asset Management*

7 Human Resources Security (*8*)

11 Physical & Environmental security (*9*)

12 Operations security
13 Communications security
10 Communications & operations management

14 System acquisition, development and maintenance
15 Supplier relationships
12 Info. Systems Acquisition development & maintenance

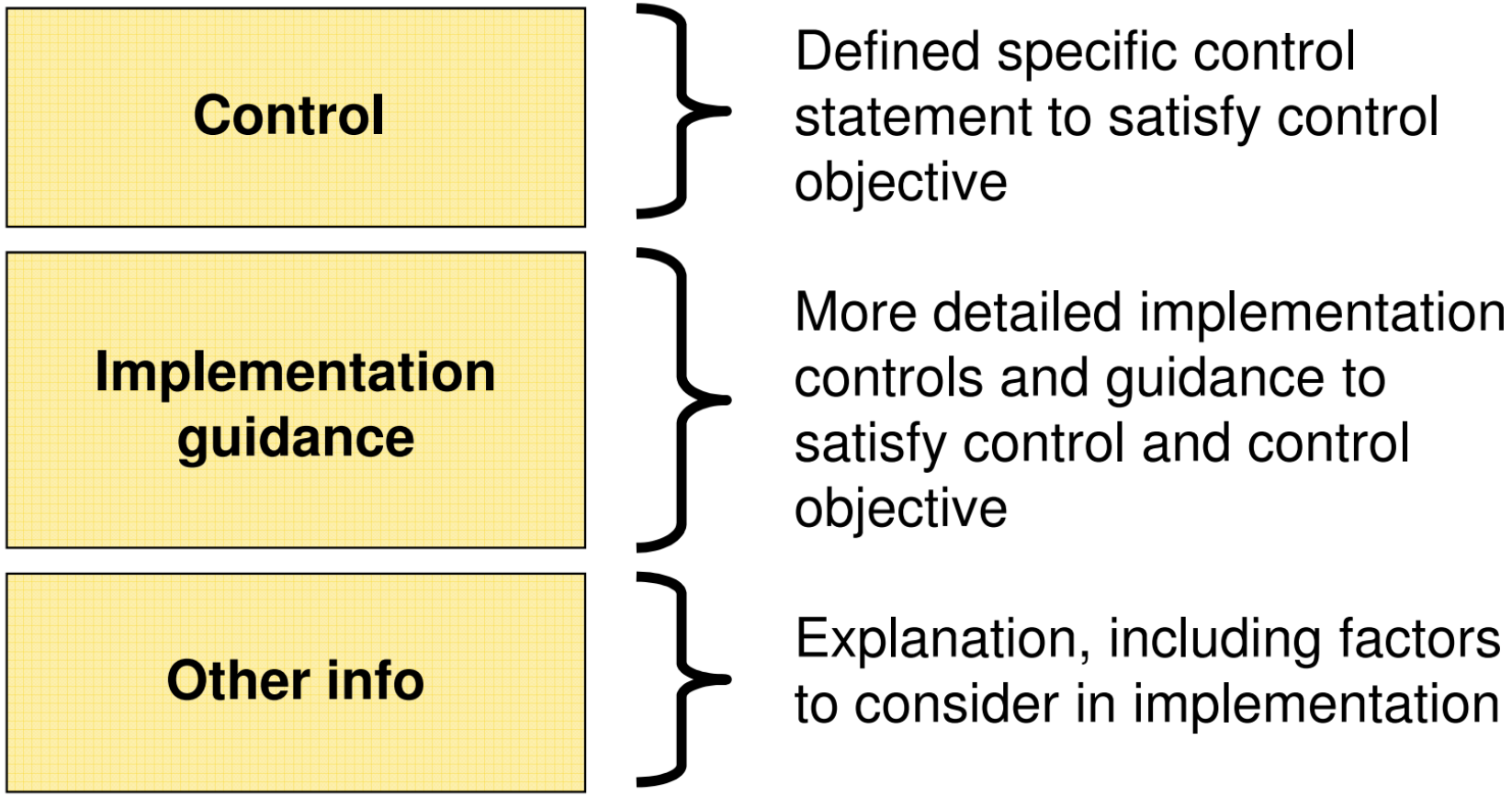
9 Access control *11 Access control*
10 Cryptography

16 Information Security Incident Mngmnt *13 Information Security Incident Mngnt*

17 business continuity management *14 Business Continuity Management*

18 Compliance *15 Compliance*

ISO 27002 Control Descripions



A 5 Security Policy

A 5.1 Information security policy

Objective:

To provide management direction and support for information security in accordance with business requirements and relevant laws regulations.

- **Information security policy document**

  A **written policy document** should be **approved** by management, be **published** and **communicated** to all employees responsible for information security in a manner that is understandable to the intended reader.

- **Review of the information security policy**

  The owner of the policy must ensure that the policy is reviewed according to a determined schedule, both **time** and **event** based.

5.1.1 Information security policy document

An information security policy document should be approved by management, and published and communicated to all employees and relevant external parties.

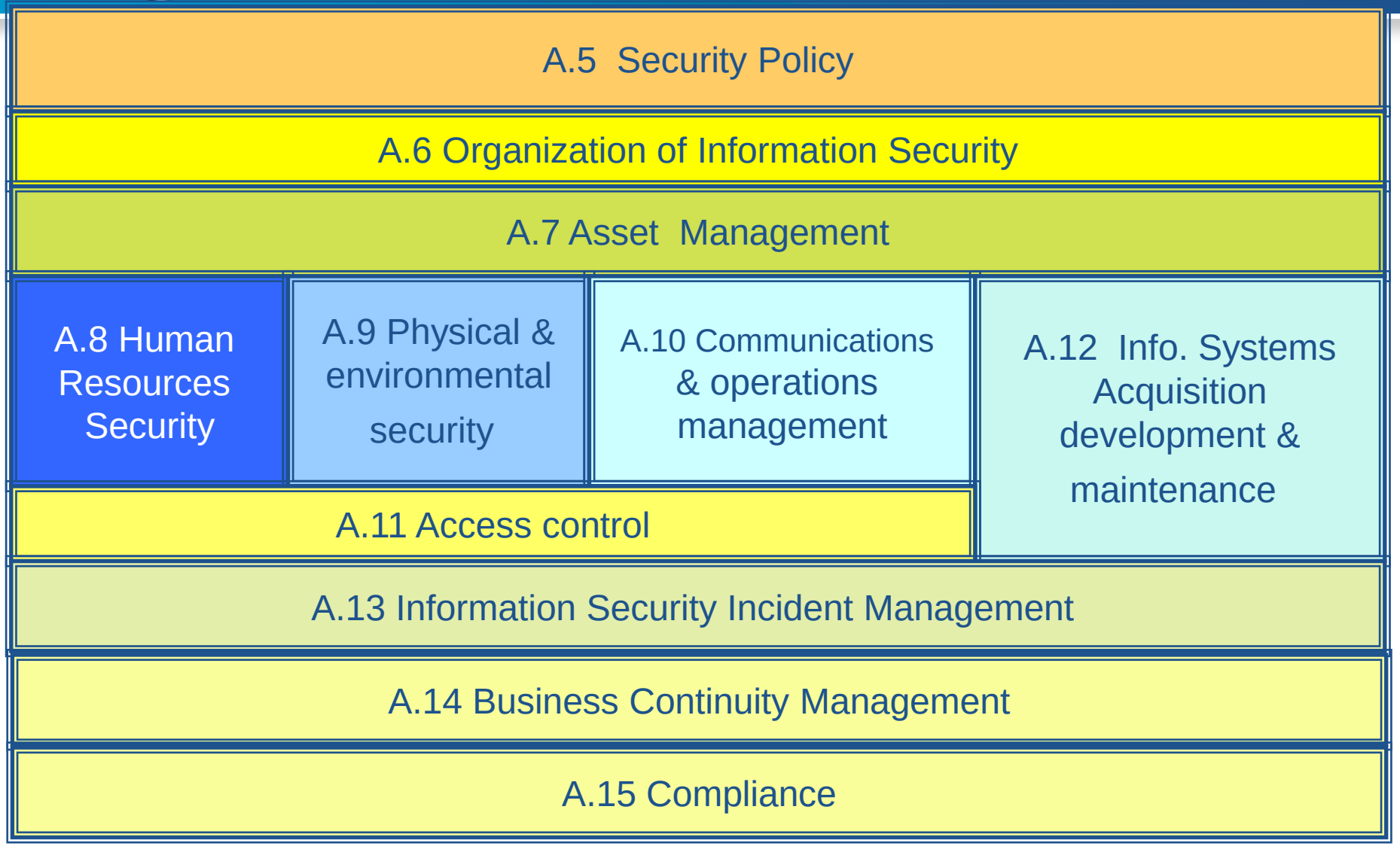
- Define information security in line with business by Management
- Objectives/ Goals for achieving
- Policy of the organization in implementing the Controls.

5.1.2 Review of the information security policy

The information security policy should be reviewed at planned intervals or if significant changes occur to ensure its continuing suitability, adequacy, and effectiveness.

- Periodic Management Reviews can take place

Structure of Annexure-A



A.6 Organization of information security

A.6.1 Internal organization

Objective: To manage information security within the organization

- A 6.1.1 Management commitment to information security
- A 6.1.2 Information security co-ordination
- A.6.1.3 Allocation of information security responsibilities
- A 6.1.4 Authorization process for information processing facilities
- A.6.1.5 Confidentiality agreements
- A 6.1.6 Contact with authorities
- A.6.1.7 Contact with special interest groups
- A 6.1.8 Independent review of information security

A.6.2 External parties

Objective: To maintain the security of the organization's information and information processing facilities that are accessed, processed, communicated to or managed by external parties.

- A.6.2.1 Identification of risks related to external parties
- A.6.2.2 Addressing security when dealing with customers
- A.6.2.3 Addressing security in third party agreements

6 Organization of information security

6.1 Internal organization

Objective:

A management framework should be established to initiate and control the implementation of information security within the organization.

6.1.1 Management commitment to information security

Management should actively support security within the organization through clear direction, demonstrated commitment, explicit assignment, and acknowledgement of information security responsibilities.

6.1.2 Information security co-ordination

Information security activities should be co-ordinated by representative from different parts of the organization with relevant roles and job functions.

6.1.3 Allocation of information security responsibilities

All information security responsibilities should be clearly defined.

6.1.4 Authorization process for information processing facilities

A management authorization process for process for new information processing facilities should be defined and implemented.

6.1.5 Confidentiality agreements

Requirements for confidentiality or non-disclosure agreements reflecting the organization’s needs for the protection of information should be identified nd regularly reviewed.

6.1.6 Contact with authorities

- Appropriate contacts with relevant authorities should be maintained.

6.1.7 Contact with special interest groups

- Appropriate contacts with special interest groups or other specialist security forums and professional associations should be maintained.

6.1.8 Independent review of information security

- The organization’s approach to managing information security and its implementation (i.e. control objectives, controls, policies, processes, and procedures for information security) should be reviewed independently at planned interval, or when significant changes to the security implementation occur.

6.2 External parties

- **Objective:** To maintain the security of the organization's information and information processing facilities that are accessed processed, communicated to, or managed by external parties.

6.2.1 Identification of risks related to external parties

- The risks to the organization's information and information processing facilities from business processes involving external parties should be identified and appropriate controls implemented before granting access.

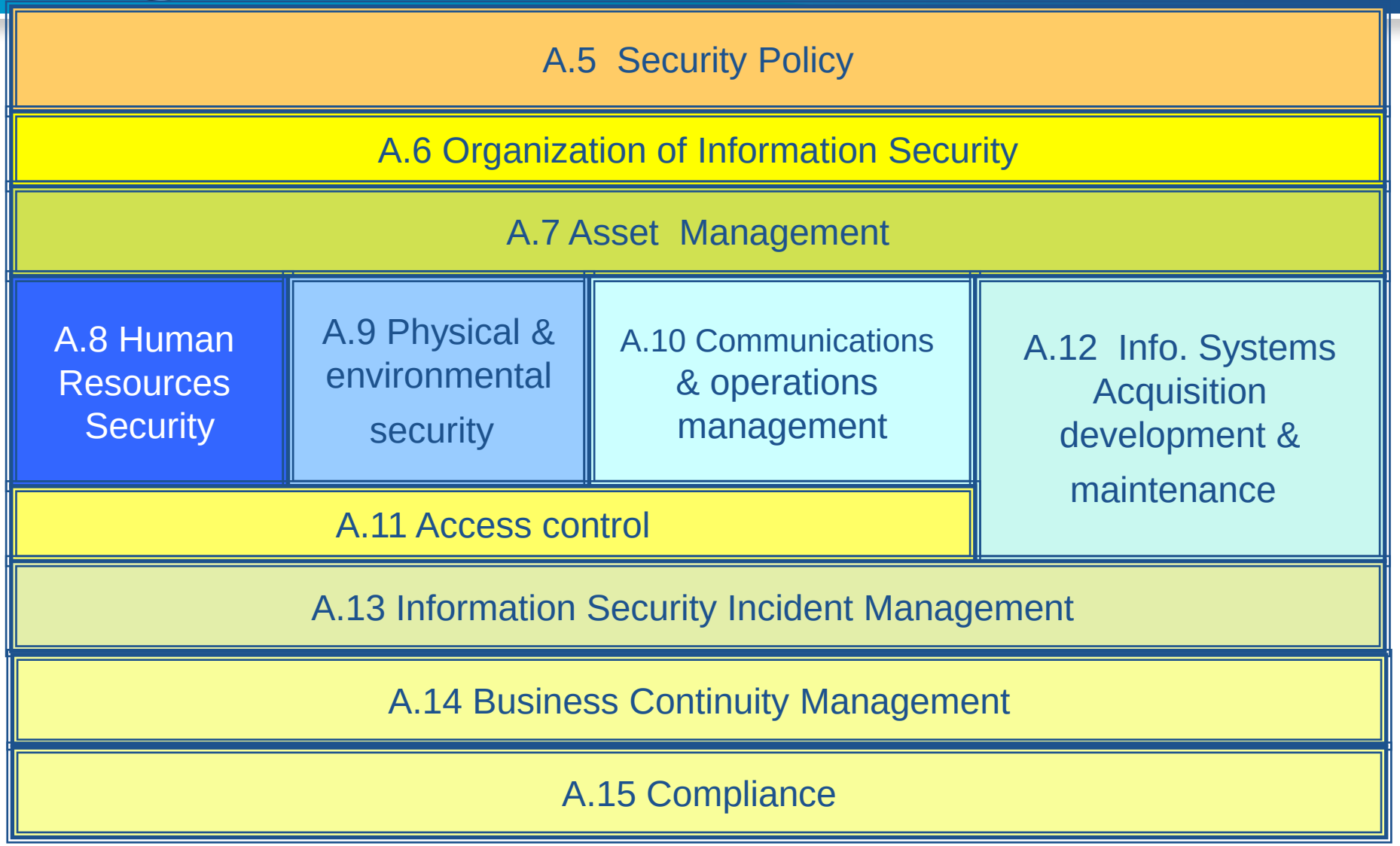
6.2.2 Addressing security when dealing with customers

- All identified security requirements should be addressed before giving customers access to the organization's information or assets.

6.2.3 Addressing security in third party agreements

- Agreements with third parties involving accessing, processing, communicating or managing the organization's information or information processing facilities, or adding products or services to information processing facilities should cover all relevant security requirements.

Structure of Annexure-A



A.7 Asset management

A.7.1 Responsibility for assets

Objective: To achieve and maintain appropriate protection of organizational assets.

- A.7.1.1 Inventory of assets
- A.7.1.2 Ownership of assets
- A.7.1.3 Acceptable use of assets

A.7.2 Information classification

Objective: To ensure that information receives an appropriate level of protection.

- A.7.2.1 Classification guidelines
- A.7.2.2 Information labelling and handling

7 Asset management

7.1 Responsibility for assets

Objective: To achieve and maintain appropriate protection of organizational assets.

7.1.1 Inventory of assets

- All assets should be clearly identified and an inventory of all important assets drawn up and maintained.

7.1.2 Ownership of assets

- All information and assets associated with information processing facilities should be owned2 by a designated part of the organization.

7.1.3 Acceptable use of assets

- Rules for the acceptable use of information and assets associated with information processing facilities should be identified, documented, and implemented.

7.2 Information classification

- **Objective:** To ensure that information receives an appropriate level of protection.

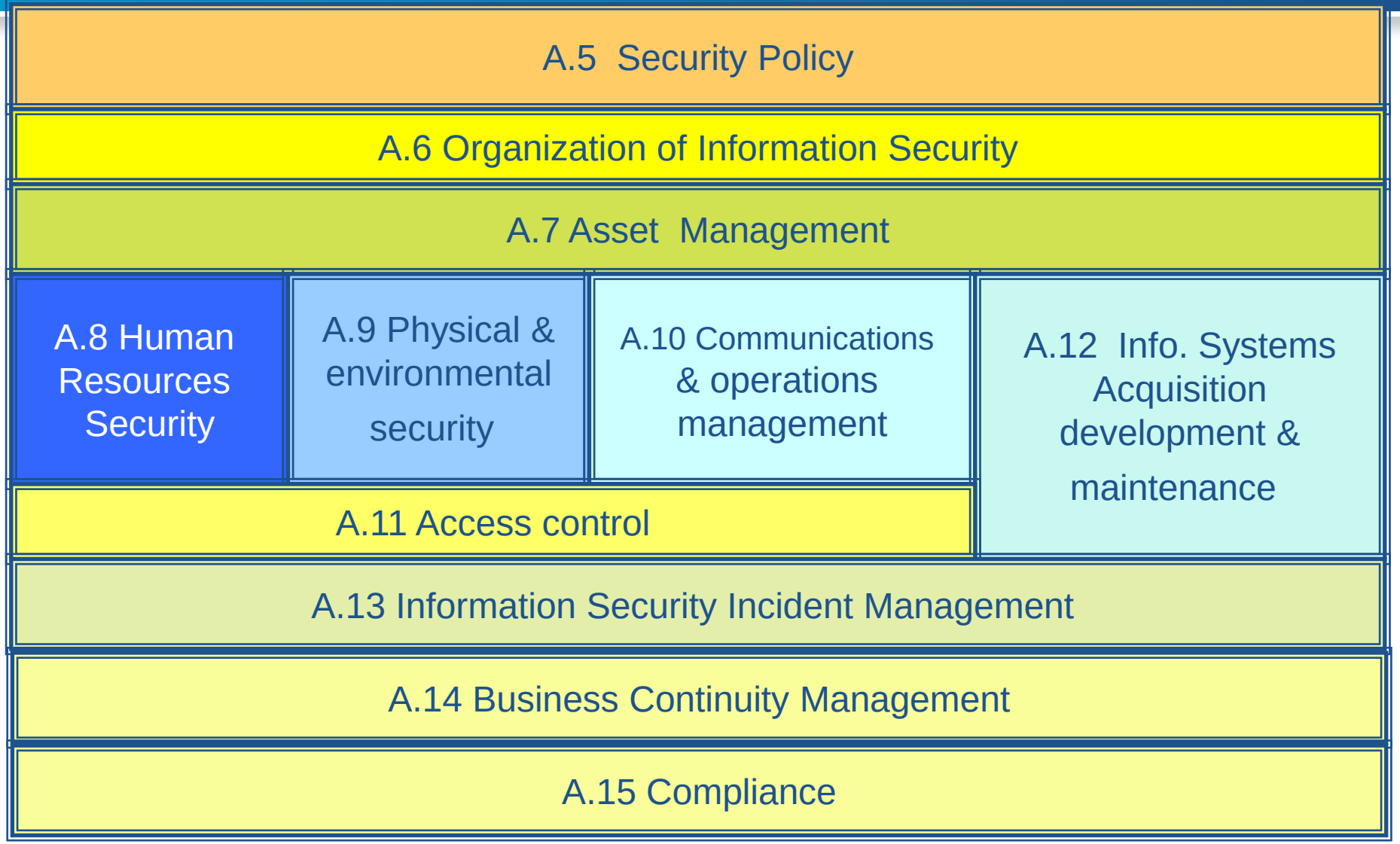
7.2.1 Classification guidelines

- Information should be classified in terms of its value, legal requirements, sensitivity, and criticality to the organization.

7.2.2 Information labeling and handling

- An appropriate set of procedures for information labeling and handling should be developed and implemented in accordance with the classification scheme adopted by the organization.

Structure of Annexure-A



A.8.1 Human resources security

A.8.1 Prior to employment

Objective: To ensure that employees, contractors and third party users understand their responsibilities, and are suitable for the roles they are considered for, and to reduce the risk to theft, fraud or misuse of facilities.

- A.8.1.1 Rotes and responsibilities
- A.8.1.2 Screening
- A.8.1.3 Terms and conditions of employment

A.8.2 During employment

Objective: To ensure that all employees, contractors and third party users are aware of information security threats and concerns, their responsibilities and liabilities, and are equipped to support organizational security policy in the course of their normal work, and to reduce the risk of human error.

- A.8.2.1 Management responsibilities
- A.8.2.2 Information security awareness, education and training
- A.8.2.3 Disciplinary process

A.8.3 Termination or change of employment

Objective: To ensure that employees, contractors and third party users exit an organization or change employment in an orderly manner

- A.8.3.1 Termination responsibilities
- A.8.3.2 Return of assets
- A.8.3.3 Removal of access rights

8 Human resources security

8.1 Prior to employment3

- **Objective:** To ensure that employees, contractors and third party users understand their responsibilities, and are suitable for the roles they are considered for, and to reduce the risk of theft, fraud or misuse of facilities.

8.1.1 Roles and responsibilities

- Security roles and responsibilities of employees, contractors and third party users should be defined and documented in accordance with the organization's information security policy.

8.1.2 Screening

- Background verification checks on all candidates for employment, contractors, and third party users should be carried out in accordance with relevant laws, regulations and ethics, and proportional to the business requirements, the classification of the information to be accessed, and the perceived risks.

8.1.3 Terms and conditions of employment

- As part of their contractual obligation, employees, contractors and their party users should agree and sign the terms and conditions of their employment contact, which should state their and the organization’s responsibilities for information security..

8.2 During employment

- **Objective:** To ensure that employees, contractors and third party users are aware of information security threats and concerns, their responsibilities and liabilities, and are equipped to support organizational security policy in the course of their normal work, and to reduce the risk of human error.

8.2.1 Management responsibilities

- Management should require employees, contractors and third party users to apply security in accordance with established policies and procedures of the organization.

8.2.2 Information security awareness, education, and training

8.2.3 Disciplinary process

8.3 Termination or change of employment

- **Objective:** To ensure that employees, contractors and third party users exit an organization or change employment in an orderly manner.

8.3.1 Termination responsibilities

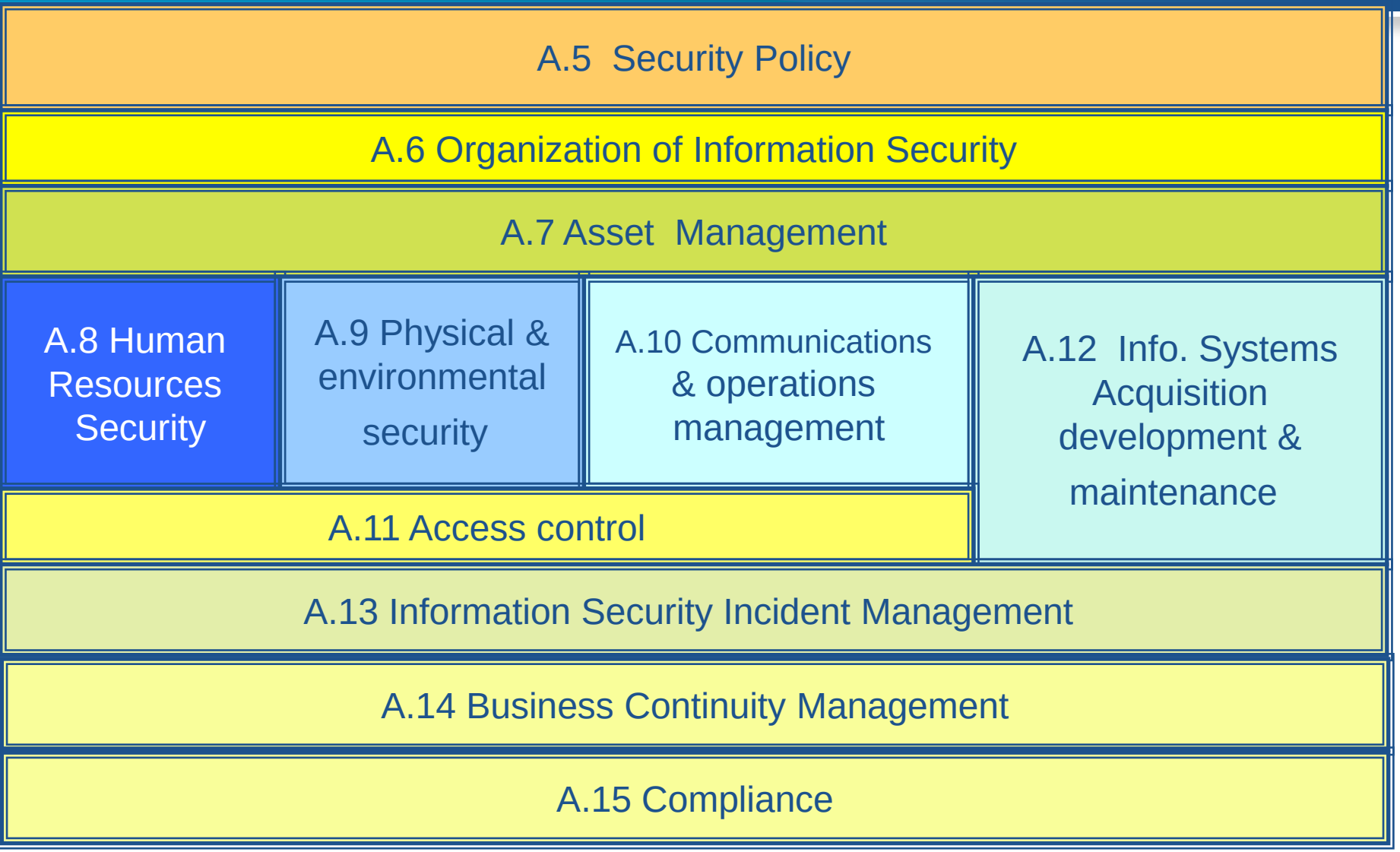
- Responsibilities for performing employment termination or change of employment should be clearly defined and assigned.

8.3.2 Return of assets

- All employees, contractors and third party users should return all of the organization’s assets

8.3.3 Removal of access rights

Structure of Annexure-A



A.9 Physical and environmental security

A.9.1 Secure areas

Objective: To prevent unauthorized physical access, damage and interference to the organization's premises and information.

- A.9.1.1 Physical security perimeter
- A.9.1.2 Physical entry controls
- A.9.1.3 Securing offices, rooms and facilities
- A.9.1.4 Protecting against external and environmental threats
- A.9.1.5 Working in secure areas
- A.9.1.6 Public access, delivery and loading areas

A.9.2 Eqipment security

Objective: To prevent loss, damage, theft or compromise of assets and interruption to the organization's activities.

- A.9.2.1 Equipment siting and protection
- A.9.2.2 Supporting utilities
- A.9.2.3 Cabling security
- A.9.2.4 Equipment maintenance
- A.9.2.5 Security of equipment off-premises
- A.9.2.6 Secure disposal or re-use of equipment
- A.9.2.7 Removal of property

9 Physical and environmental security

9.1 Secure areas

- **Objective:** To prevent unauthorized physical access, damage, and interference to the organization's premises and information.

9.1.1 Physical security perimeter

- Security perimeters (barriers such as walls, card controlled entry gates or manned reception desks) should be used to protect areas that contain information and information processing facilities.

9.1.2 Physical entry controls

- Secure areas should be protected by appropriate entry controls to ensure that only authorized personnel are allowed access.

9.1.3 Securing offices rooms, and facilities

- Physical security for offices, rooms, and facilities should be designed and applied.

9.1.4 Protecting against external and environmental threats

- Physical protection against damage from fire, flood, earthquake, explosion, civil unrest, and other forms of natural or man-made disaster

9.1.5 Working in secure areas

- Physical protection and guidelines for working in secure areas should be designed and applied.

9.1.6 Public access, delivery, and loading areas

- Access points such as delivery and loading areas and other points where unauthorized persons may enter the premises should be controlled and, if possible, isolated from information processing facilities to avoid unauthorized access.

9.2 Equipment security

9.2.1 Equipment siting and protection

- Equipment should be sited or protected to reduce the risks from environmental threats and hazards, and opportunities for unauthorized access.

9.2.2 Supporting utilities

- Equipment should be protected from power failures and other disruptions caused by failures in supporting utilities.

9.2.3 Cabling security

- Power and telecommunications cabling carrying data or supporting information services should be protected from interception or damage.

9.2.4 Equipment maintenance

- Equipment should be correctly maintained to ensure its continued availability and integrity.

9.2.5 Security of equipment off-premises

- Security should be applied to off-site equipment taking into account the different risks of working outside the organization's premises.

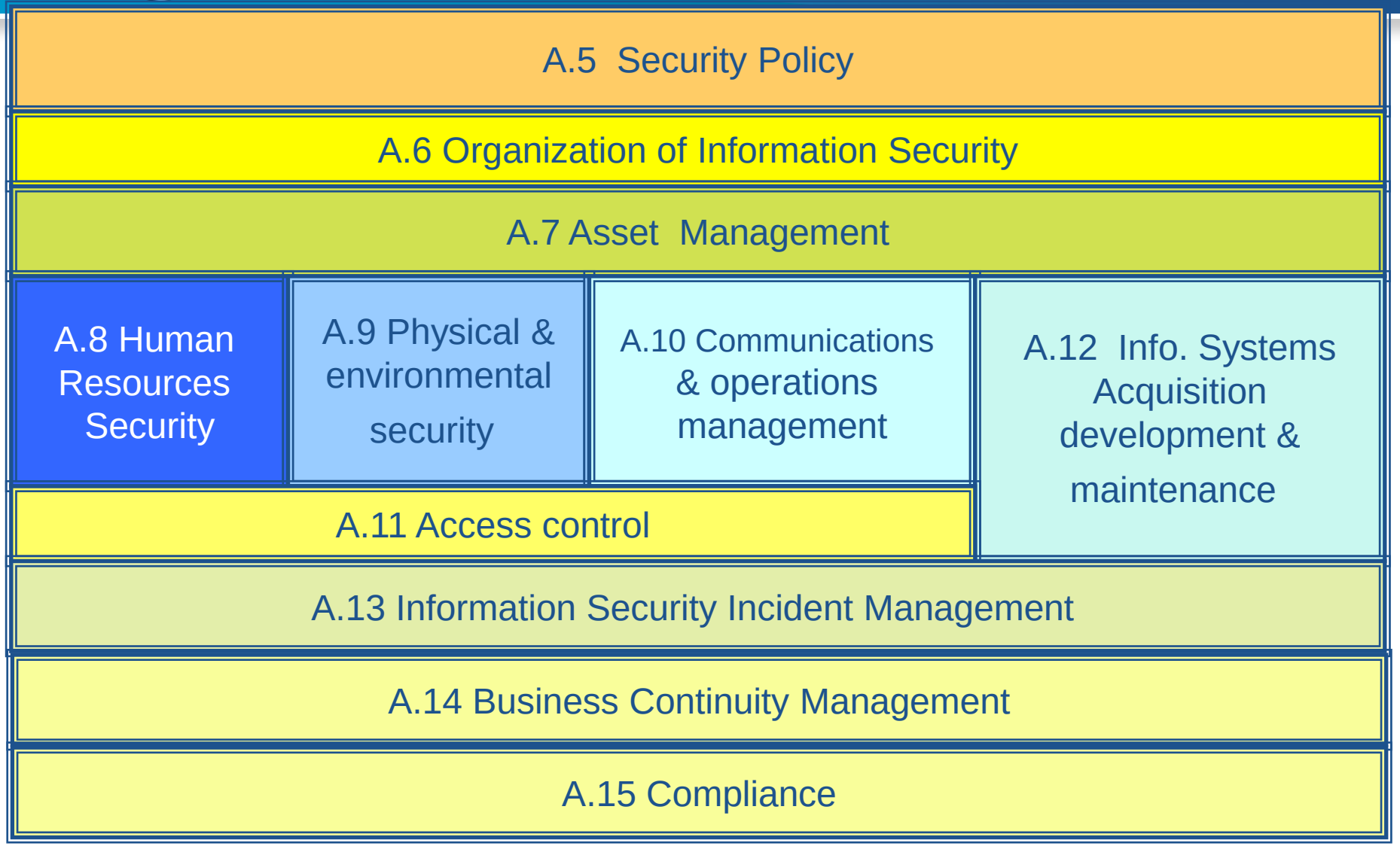
9.2.6 Secure disposal or re-use of equipment

- All items of equipment containing storage media should be checked to ensure that any sensitive data and licensed software has been removed or securely overwritten prior to disposal.

9.2.7Removal of property

- Equipment, information or software should not be taken off-sie without prior authorization

Structure of Annexure-A



A.10 communications and operations management

A.10.1 Operational procedures and responsibilities
Objective: To ensure the correct and secure operation of information processing facilities.

- A.10.1.1 Documented operating procedures
- Change management
- A.10.1.3 Segregation of duties
- A.10.1.4 Separation of development, test and operational facilities

A.10.2 Third service delivery management
Objective: To implement and maintain the appropriate level of information security and service delivery in line with third party service delivery agreements.

- A.10.2.1 Service delivery
- A.10.2.2 Monitoring and review of third party services
- A.10.2.3 Managing changes to third party services

A.10.3 System planning and acceptance
Objective: To minimize the risk of system failures.

- A.10.3.1 Capacity management
- A.10.3.2 System acceptance

A.10.4 Protection against malicious and mobile code
Objective: To protect the integrity of software and information

- A.10.4.1 Controls against malicious code
- A.10.4.2 Controls against mobile code

A.10.5 Back-up
Objective: To maintain the integrity and availability of information and information processing facilities.

- A.10.5.1 Information back-up

A.10.6 Network security management
Objective: To ensure the protection of information in networks and the protection of the supporting **infrastructure.**

- A.10.6.1 Network controls
- A.10.6.2 Security of network services

A.10.7 Media handling
Objective: To prevent unauthorized disclosure; modification, removal or destruction of assets, and interruption to business activities.

- A.10.7.1 Management of removable media
- A.10.7.2 Disposal of media
- A.10.7.3 Information handling procedures
- A.10.7.4 Security of system documentation

A.10.8 Exchange of information
Objective: To maintain the security of information and software exchanged within an organization and with any external entity

- A.10.8.1 Information exchange policies and procedures
- A.10.8.2 Exchange agreements
- A.10.8.3 Physical media in transit
- A.10.8.4 Electronic messaging
- A.10.8.5 Business information systems

A.10.9 Electronic commerce services
Objective: To ensure the security of electronic commerce services, and their secure use.

- A.10.9.1 Electronic commerce
- A.10.9.2 On-line transactions
- A.10.9.3 Publicly available information

A.10.10 Monitoring
Objective: To detect un authorized information processing activities.

- A.10.10.1 Audit logging
- A.10.10.2 Monitoring system use
- A.10.10.3 Protection of log information
- A.10.10.4 Administrator and operator logs
- A.10.10.5 Fault logging
- A.10.10.6 Clock synchronization

10 Communications and operations management

10.1 Operational procedures and responsibilities

- **Objective:** To ensure the correct and secure operation of information processing facilities.

10.1.1 Documented oprating procedures

- Operating procedures should be documented, maintained, and made available to all users who need them.

10.1.2 Change management

- Changes to information processing facilities and system should be controlled.

10.1.3 Segregation of duties

- Duties and areas of responsibility should be segregated to reduce opportunities for unauthorized or unintentional modification or misuse of the organization’s assets.

10.1.4 Separation of development, test, and operational facilities

10.2 Third party service delivery management

- **Objective:** To implement and maintain the appropriate level of information security and service delivery in line with third party service delivery agreements.

10.2.1 service delivery

- It should be ensured that security controls, services definitions and delivery levels included in the third party service delivery agreements are implemented, operated, and maintained by the third party.

10.2.2 Monitoring and review of third party services

- The services, reports and records provided by the third party should be regularly monitoring and reviewed, and audits should be carried out regularly.

10.2.3 Managing changes to third party services

10.3 System planning and acceptance

- **Objective:** To minimize the risk of systems failures.

10.3.1 Capacity management

- The use of resources should be monitored, tuned, and projections made of future capacity requirements to ensure the required system performance.

10.3.2 System acceptance

- Acceptance criteria for new information system, upgrades, and new versions should be established and suitable tests of the system(s) carried out during development and prior to acceptance.

10.4 Protection against malicious and mobile code

- **Objective:** To protect the integrity of software and information

10.4.1 Controls against malicious code

- Detection, prevention, and recovery controls to protect against malicious code and appropriate user awareness procedures should be implemented.

10.4.2 Controls against mobile code

- Where the use of mobile code is authorized, the configuration should ensure that the authorized mobile code operates according to a clearly defined security policy, and unauthorized mobile code should be prevented from executing.

10.5 Back-up

- **Objective:** To maintain the integrity and availability of information and information processing facilities.

10.5.1 Information back-up

- Back-up copies of information and software should be taken and tested regularly in accordance with the agreed backup policy.

10.6 Network security management

- **Objective:** To ensure the protection of information in networks and the supporting infrastructure.

10.6.1 Network controls

- Networks should be adequately managed and controlled, in order to be protected from threats, and to maintain security for the system and applications using the network, including information in transit.

10.6.2 Security of network services

- Security features, service levels, and management requirements of all network services should be identified and included in any network services agreements, whether these services are provided in house or outsourced.

10.7 Media handling

- **Objective:** To prevent unauthorized disclosure, modification, removal or destruction of assets, and interruption to business activities.

10.7.1 Management of removal media

- There should be procedures in place for the management of removable media.

10.7.2 Disposal of media

- Media should be disposed of securely and safely when no longer required, using formal procedures.

10.7.3 Information handling procedures

- Procedures for the handling and storage of information should be established to protect this information from unauthorized disclosure or misuse.

107.4 Security of system documentation

- System documentation should be protected against unauthorized access.

10.8 Exchange of information

- **Objective:** To maintain the security of information and software exchanged within an organization any external entity.

10.8.1 Information exchange policies and procedures

- Formal exchange policies, procedures, and controls should be in place to protect the exchange of information through the use of all types of communication facilities.

10.8.2 Exchange agreements

- Agreements should be established for the exchange of information and software between the organization and external parties.

10.8.3 Physical media in transit

- Media containing information should be protected against unauthorized access, misuse or corruption during transportation beyond an organization's physical boundaries.

10.8.4 Electronic messaging

- Information involved in electronic messaging should be appropriately protected.

10.8.5 Business information systems

- Policies and procedures should be developed and implemented to protect information associated with the interconnection of business information system.

10.9 Electronic commerce service

- **Objective:** To ensure the security of electronic commerce services, ad their secure use.

10.9.1 Electronic commerce

- Information involved in electronic commerce passing over public networks should be protected from fraudulent activity, contract dispute, and unauthorized disclosure and modification.

10.9.2 On-line Transactions

- Information involved in on-line transactions should be protected to prevent incomplete transmission, mis-routing, unauthorized message alteration, unauthorized disclosure, unauthorized message duplication or replay.

10.9.3 Publicly available information

- The integrity of information being made available on a publicly available system should be protected to prevent unauthorized modification.

10.10 Monitoring

- **Objective:** to detect unauthorized information processing activities.
- System should be monitoring and information security events should be recorded. Operator logs and fault logging should be used to ensure information system problems are identified.

10.10.1 Audit logging

- Audit logs recording user activities, exception, and information security events should be produced and kept for an agreed period to assist in future investigations and access control monitoring.

10.10.2 Monitoring system use

- Procedures for monitoring use of information processing facilities should be established and the results of the monitoring activities reviewed regularly.

10.10.3 Protection of log information

- Logging facilities and log information should be protected against tampering and unauthorized access.

10.10.4 Administrator and operator logs

- System administrator and system operator activities should be logged.

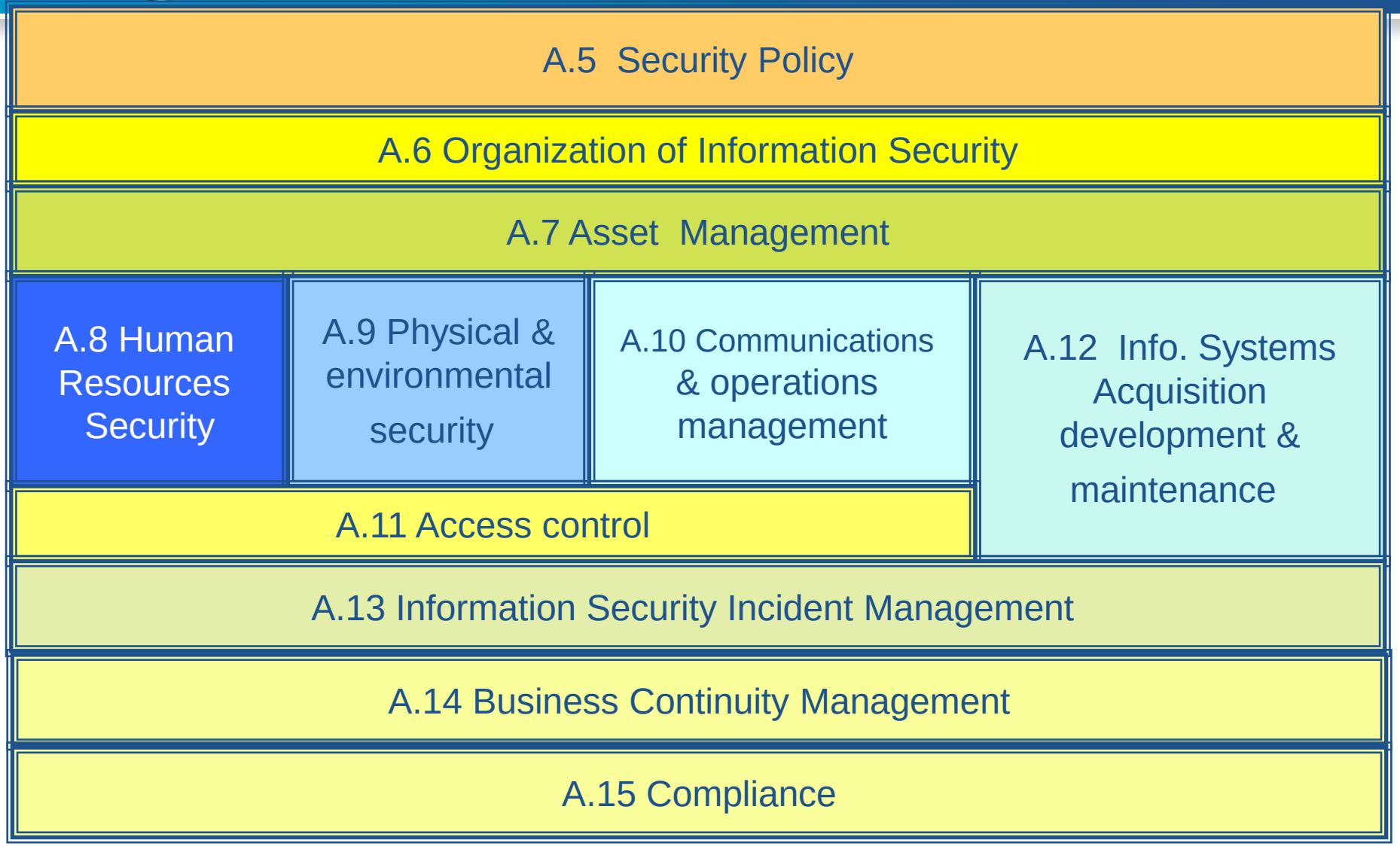
10.10.5 Fault logging

- Faults should be logged, analyzed, and appropriate action taken.

10.10.6 Clock synchronization

- The clocks of all relevant information processing system within an organization or security domain should be synchronized with an agreed accurate time source.

Structure of Annexure-A



A.11 Access control

A.11.1 Business requirement for access control
Objective: To control access to information

- A.11.1.1 Access control policy

A.11.2 User access management
Objective: To ensure authorized user access and to prevent unauthorized access to information system

- A.11.2.1 User registration
- A.11.2.2 Privilege management
- A.11.2.3 User password management
- A.11.2.4 Review of user access rights

A.11.3 User responsibilities
Object: To prevent unauthorized user access, and compromise or theft of information and information processing facilities.

- A.11.3.1 Password use
- A.11.3.2 Unattended user equipment
- A.11.3.3 Clear desk and clear screen policy

A.11.4 Network access control
Objective: To prevent unauthorized access to networked services.

- A.11.4.1 Policy on use of network services
- A.11.4.2 User authentication for external connections
- A.11.4.3 Equipment identification in networks
- A.11.4.4 Remote diagnostic and configuration port protection
- A.11.4.5 Segregation in networks
- A.11.4.6 Network connection control
- A.11.4.7 Network routing control

A.11.5 Operating system access control

Objective: To prevent unauthorized access to operating systems.

- A.11.5.1 Secure log-on procedures
- A.11.5.2 User identification and authentication
- A.11.5.3 Password management system
- A.11.5.4 Use of system utilities
- A.11.5.5 Session time-out
- A.11.5.6 Limitation of connection time

A.11.6 Application and information access control

Objective: To prevent unauthorized access to information held in application system.

- A.11.6.1 Information access restriction
- A.11.6.2 Sensitive system isolation

A.11.7 Mobile computing and teleworking

Objective: To ensure information security when using mobile computing and teleworking facilities.

- A.11.7.1 Mobile computing and communications
- A.11.7.2 Teleworking

11 Access control

11.1 Business requirement for access control

- **Objective:** To control access to information.

11.1.1 Access control policy

- An access control policy should be established, documented, and reviewed based on business and security requirements for access**.**

.

11.2 User access management

- **Objective:** To ensure authorized user access and to prevent unauthorized access to information system.

11.2.1 User registration

- There should be a formal user registration and de-registration procedure in place for granting and revoking access to all information systems and services.

11.2.2 Privilege management

- The allocation and use of privileges should be restricted and controlled.

11.2.3 User password management

- The allocation of passwords should be controlled through a formal management process.

11.2.4 Review of user rights

- Management should review users' access rights at regular intervals using a formal process.

11.3 User responsibilities

- **Objective:** To prevent unauthorized user access, and compromise or theft of information and information processing facilities.

11.3.1 Password use

- Users should be required to follow good security practices and use of passwords.

11.3.2 Unattended user equipment

- Users should ensure that unattended equipment has appropriate protection.

11.3.3 Clear desk and clear screen policy

- A clear desk policy for papers and removable storage media and a clear screen policy for information processing facilities should be adopted.

11.4 Network access control

- **Objective**: To prevent unauthorized access to networked services.
- Access to both internal and external networked services should be controlled.

11.4.1 Policy on use of network services

- Users should only be provided with access to the services that they have been specially authorized to use.

11.4.2 User authentication for external connections

- Appropriate authentication methods should be used to control access by remote users.

11.4.3 Equipment identification in networks

- Automatic equipment identification should be considered as a meant to authenticate connections from specific locations and equipment.

11.4.4 Remote diagnostic and configuration port protection

- Physical and logical access to diagnostic and configuration ports should be controlled.

11.4.5 Segregation in networks

- Groups of information services, users, and information system should be segregated on networks.

11.4.6 Network connection control

- For shared networks, especially those extending across the organization's boundaries, the capacity of users to connect to the network should be restricted, in line with the access control policy and requirements of the business applications (see 11.1).

11.4.7 Network routing control

- Routing controls should be implemented for networks to ensure that computer connection and information flows do not breach the access control policy off the business applications.

11.5 Operating system access control

- **Objective:** To prevent unauthorized access to operating systems.

11.5.1 Secure log-on procedures

- Access to operating system should be controlled by a secure log-on procedure.

11.5.2 User identification and authentication

- All users should have a unique identifier (user ID) for their personal use only, and a suitable authentication technique should be chosen to substantiate the claimed identify of a user.

11.5.3 Password management system

- Systems for managing passwords should be interactive and should ensure quality passwords.

11.5.4 Use of system utilities

- The use of utility programs that might be capable of overriding system and application controls should be restricted and tightly controlled.

11.5.5 Session time-out

- Inactive session should shut down after a defined period of inactivity.

11.5.6 Limitation of connection time

- Restriction on connection times should be used to provide additional security for high-risk applications.

11.6 Application and information access control

- **Objective:** To prevent unauthorized access to information held in application systems.
- Security facilities should be used to restrict access to and within application systems.

11.6.1 Information access restriction

- Access to information and application system functions by users and support personnel should be restricted in accordance with the defined access control policy.

11.6.2 Sensitive system isolation

- Sensitive systems should have a dedicated (isolated) computing environment.

11.7 Mobile computing and teleworking

- **Objective:** To ensure information security when using mobile computing and teleworking facilities.

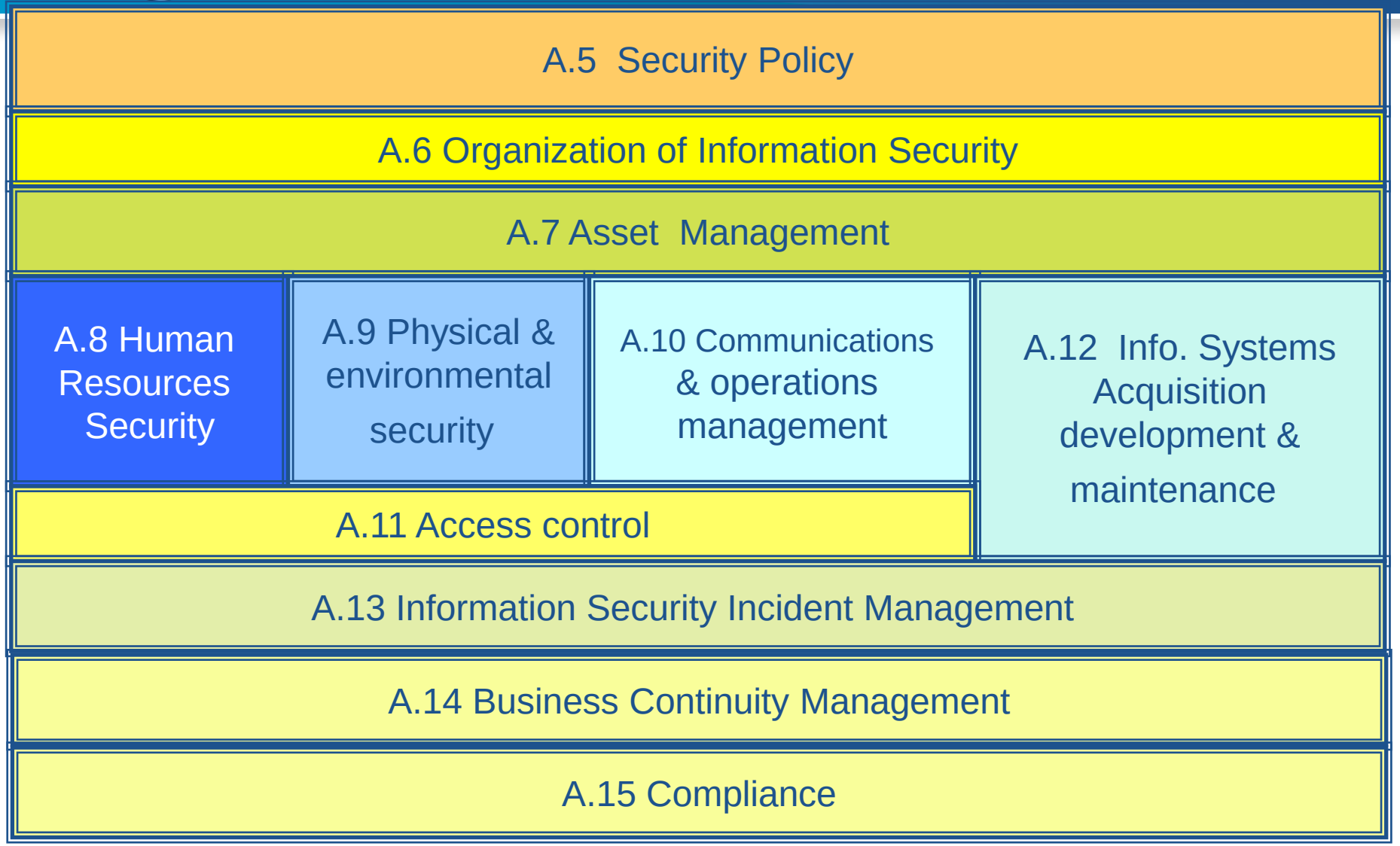
11.7.1 Mobile computing and teleworking

- A formal policy should be in place, and appropriate security measures should be adopted to protect against the risks of using mobile computing and communication facilities.

11.7.2 Teleworking

- A policy, operational plants and procedures should be developed and implemented for teleworking activities.

Structure of Annexure-A



A.12 Information systems acquisition, development and maintatenance

A.12.1 Security requirements of information systems
Objective: To ensure that security is an integral part of information systems.

- A.12.1.1 Security requirements analysis and specifications

A.12.2 Correct processing in applications
Objective: To prevent errors, loss, unauthorized modification or misuse of information in application

- A.12.2.1 Input data validation
- A.12.2.2 Control of internal processing
- A.12.2.3 Message integrity
- A.12.2.4 Output data validation

A.12.3 Cryptographic controls
Objective: To protect the confidentiality, authenticity or integrity of information by cryptographic means.

- A.12.3.1 Policy on the use of cryptographic controls
- A.12.3.2 Key management

A.12.4 Security of system files

Objective: To ensure the security of system files.

- A.12.4.1 Controls of operational software
- A.12.4.2 Protection of system test data
- A.12.4.3 Access control to program source code

A.12.5 Security in development and support processes

Objective: To maintain the security of application system software and information.

- A.12.5.1 Change control procedures
- A.12.5.2 Technical review of applications after operating system changes
- A.12.5.3 Restrictions on changes to software packages
- A.12.5.4 Information leakage
- A.12.5.5 Outsourced software development

A.12.6 Technical vulnerabilities management

Objective: To reduce risks resulting from exploitation of published technical vulnerabilities.

- A.12.6.1 Control of technical vulnerabilities

12 Information systems acquisition, development and maintenance

12.1 Security requirements of information systems

- **Objective:** To ensure that security is an integral part of information systems.

12.1.1 Security requirements analysis and specification

- Statements of business requirements for new information systems, or enhancements to existing information systems should specify the requirements for security controls.

12.2 Correct processing in applications

- **Objective:** To prevent errors, loss, unauthorized modification or misuse of information in applications.
- Appropriate controls should be designed into applications, including user developed applications to ensure correct processing. These controls should include the validation of input data, internal processing and output data.

12.2.1 Input data validation

- Data input to applications should be validated to ensure that this data is correct and appropriate.

12.2.2 Controls of internal processing

- Validation checks should be incorporated into applications to detect any corruption of information through processing errors or deliberate acts.

12.2.3 Message integrity

- Requirements for ensuring authenticity and protecting message integrity in applications should be identified, and appropriate controls identified and implemented.

12.2.4 Output data validation

- Data output from an application should be validated to ensure that the processing of stored information is correct and appropriate to the circumstances.

12.3 Cryptographic controls

- **Objective:** To protect the confidentiality, authenticity or integrity of information by cryptographic means
- A policy should be developed on the use of cryptographic controls. Key management should be in place to support the use of cryptographic techniques

12.3.1 Policy on the use of cryptographic controls

- A policy on the use of cryptographic controls for protection of information should be developed and implemented.

12.3.2 Key management

- Key management should be in place to support the organization's use of cryptographic techniques.

12.4 Security of system files

- **Objective:** To ensure the security of system files
- Access to system files and program source code should be controlled, and IT projects and support activities conducted in a secure manner. Care should be taken to avoid exposure of sensitive data in test environments.

12.4.1 Control of operational software

- There should be procedures in place to control the installation of software on operational systems.

12.4.2 Protection of system test data

- Test data should be selected carefully, and protected and controlled.

12.4.3 Access control to program source code

- Access to program source code should be restricted.

12.5 Security in development and support processes

- **Objective:** To maintain the security of application system software and information.
- Project and support environments should be strictly controlled.

12.5.1 Change control procedures

- The implementation of changes should be controlled by the use of formal change control procedures.

12.5.2 Technical review of applications after operating system changes

- When operating system are changed, business critical applications should be review and tested to ensure there is no adverse impact on organizational operations or security.

•12.5.3 Restrictions on changes to software packages

- Modifications to software packages should be discouraged, limited to necessary changes, and all changes should be strictly controlled.

12.5.4 Information leakage

- Opportunities for information leakage should be prevented.

12.5.5 Outsourced software development

- Outsourced software development should be supervised and monitored by the organization.

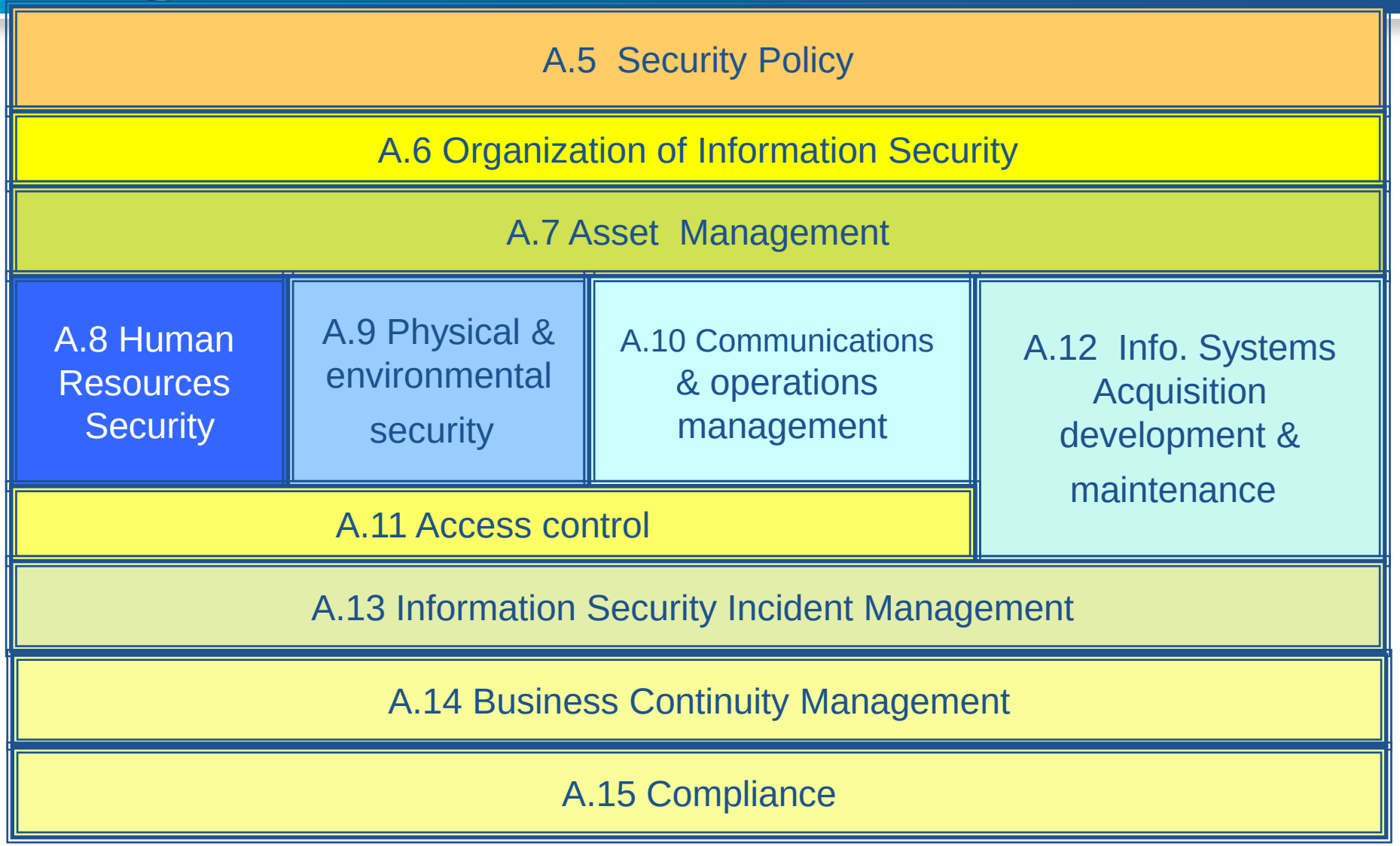
12.6 Technical Vulnerability Management

- **Objective:** To reduce risks resulting from exploitation of published technical vulnerabilities.
- Technical vulnerability management should be implemented in an effective, systematic, and repeatable way with measurements taken to confirm its effectiveness. These considerations should include operating systems, and any other applications in use.

12.6.1 Control of technical vulnerabilities

- Timely information about technical vulnerabilities of information systems being used should be obtained, the organization's exposure to such vulnerabilities evaluated, and appropriate measures taken to address the associated risk.

Structure of Annexure-A



A.13 Information security incident management

A.13.1 Reporting information security events and weakness

Objective: To ensure information security events and weakness associated with information systems are communicated in a manner allowing timely corrective to be

- A.13.1.1 Reporting information security events
- A.13.1.2 Reporting security weaknesses

A.13.2 Management of information security incidents and improvements

Objective: To ensure a consistent and effective approach is applied to the management of information security incidents.

- A.13.2.1 Responsibilities and procedures
- A.13.2.2 Learning from information security incidents
- A.13.2.3 Collection of evidence

13 Information security incident management

13.1 Reporting information security events and weaknesses

- **Objective:** To ensure information security events and weaknesses associated with information systems are communicated in a manner allowing timely corrective active to be taken.

13.1.1 Reporting information security events

- Information security events should be reported trough appropriate management channels as quickly as possible.

13.1.2 Reporting security weaknesses

- All employees, contractors and third party users of information systems and services should be required to note and report any observed or suspended security weaknesses in systems or services.

13.2 Management of information security incidents and improvements

- **Objective:** To ensure a consistent and effective approach is applied to the management of information security incidents.

13.2.1 Responsible and procedures

- Management responsibilities and procedures should be established to ensure a quick, effectiveness, and orderly response to information security incidents.

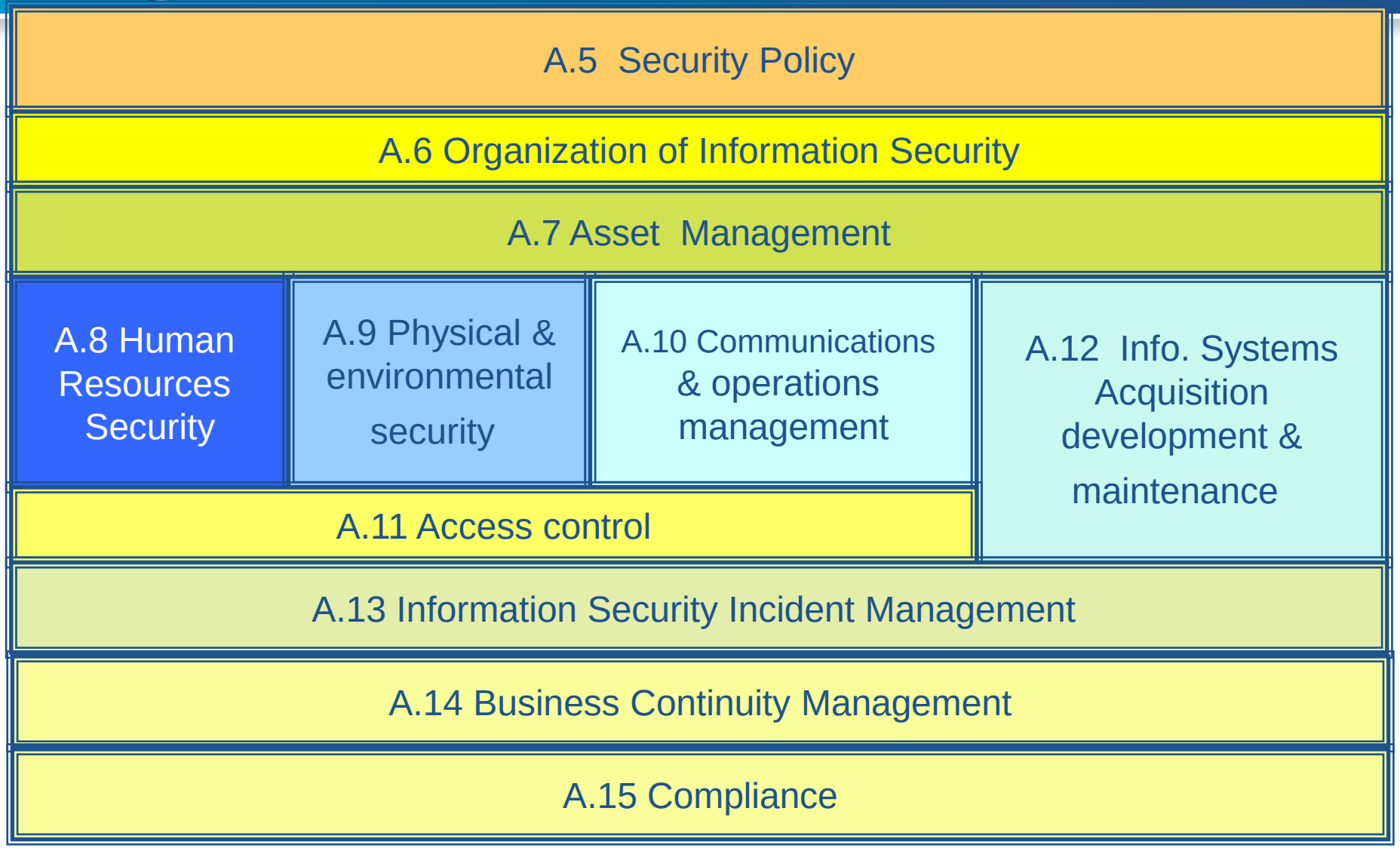
13.2.2 Learning from information security incidents

- There should be mechanisms in place to enable the types, volumes, and costs of information security incidents to be quantified and monitored.

13.2.3 Collection of evidence

- Where a follow-up action against a person or organization after an information security incident involves legal action (either civil or criminal), evidence should be collected, retained, and presented to conform to the rules for evidence laid down in the within the relevant jurisdiction(s).

Structure of Annexure-A



A.14 Business continuity management

A.14.1 Information security aspects of business continuity management

Objective: To counteract interruptions to business activities and to protect critical business processes from the effects of major failures of information systems or disasters and to ensure their timely resumption.

- A.14.1.1 Including information security in the business continuity management process
- A.14.1.2 Business continuity and risk assessment
- A.14.1.3 Developing and implementing continuity plans including information security
- A.14.1.4 Business continuity planning framework
- A.14.1.5 Testing. Maintaining and reassessing business continuity plans

14 Business continuity management

14.1 Information security aspects of business continuity management

- **Objective:** To counteract interruptions to business activities and to protect critical business processes from the effects of major failures of information systems or disasters and to ensure their timely resumption.

14.1.1 including information security in the business continuity management process

- A managed process should be developed and maintained for business continuity throughout the organization that addresses the information security requirements needed for the organization’s business continuity.

14.1.2 Business continuity and risk assessment

- Events that can cause interruptions to business process should be identified, along with the probability and impact o such interruptions and their consequences for information security.

14.1.3 Developing and implementing continuity plans including information security

- Plans should be developed and implemented to maintain or restore operational and ensure availability of information at the required level and in the required time scales following interruption to, or failure of, critical business processes.

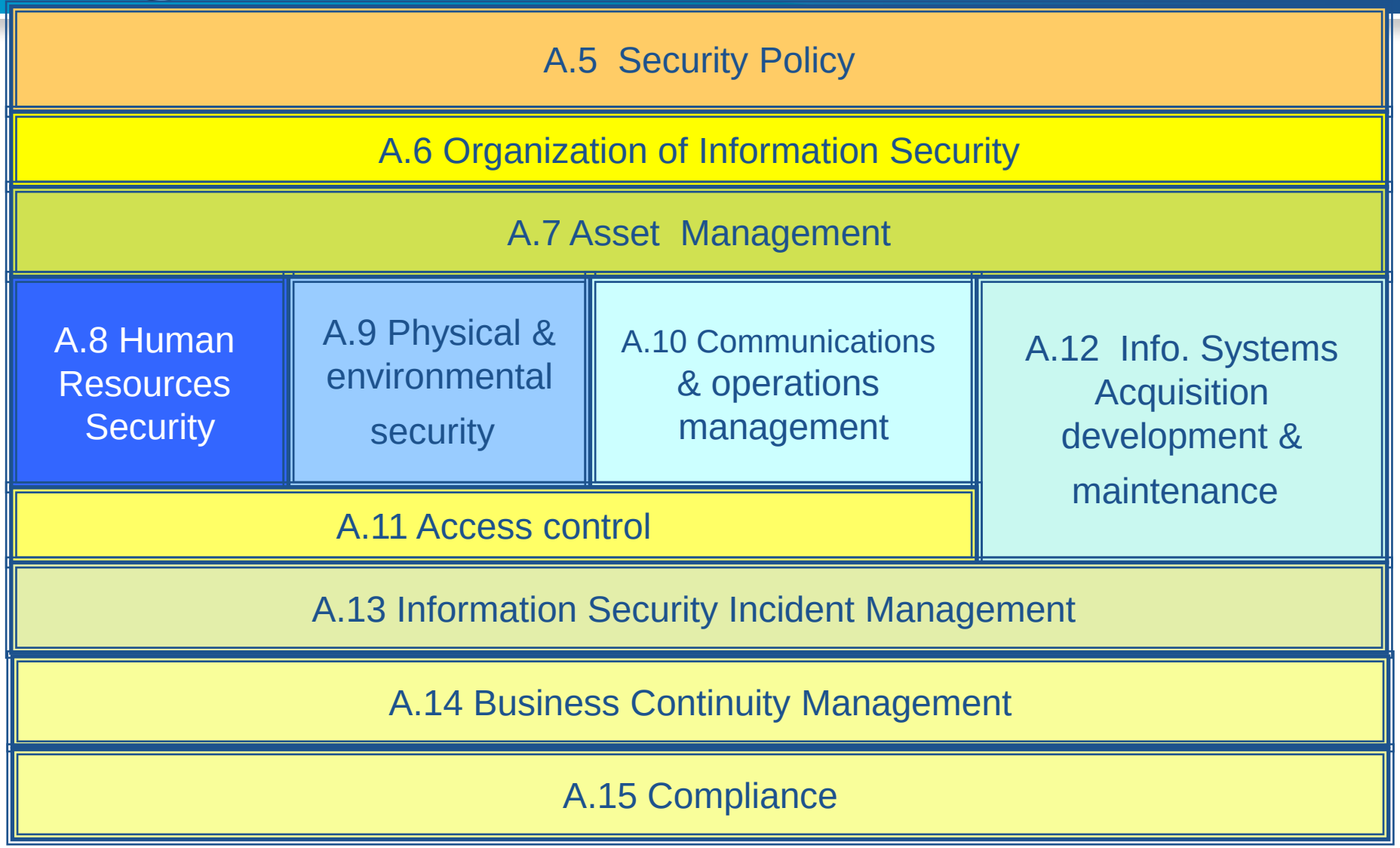
14.1.4 business continuity planning framework

- A single framework of business continuity plans should be maintained to ensure all plans are consistent, to consistently address information security requirements, and to identify priorities for testing and maintenance.

14.1.5 Testing, maintaining and reassessing business continuity plans

- Business continuity plans should be tested and updated regularly to ensure that they are up to data and effective.

Structure of Annexure-A



A.15 Compliance

A.15.1 Compliance with legal requirements
Objective: To avoid breaches of any law, statutory, regulatory or contractual obligations, and of any security requirements.

- A.15.1.1 Identification of applicable legislation
- A.15.1.2 Intellectual property rights (IPR)
- A.15.1.3 Protection of organizational records
- A.15.1.4 Data protection and privacy of personal information
- A.15.1.5 Prevention of misuse of information processing facilities
- A.15.1.6 Regulation of cryptographic controls

A.15.2 Compliance with security policies and standards, and technical compliance
Objective: To ensure compliance of system with organizational security policies and standards.

- A.15.2.1 Compliance with security policies and standards
- A.15.2.2 Technical compliance checking

A.15.3 Information systems audit considerations.
Objective: To maximize the effectiveness of and to minimize interference to/from the information systems audit process.

- A.15.3.1 Information systems audit controls
- A.15.3.2 Protection of information systems audit tools

15 compliance

15.1 Compliance with legal requirements

- **Objective:** To avoid breaches of any law, statutory, regulatory or contractual obligations, and of any security requirements.
- the design, operation, use, and management of information system may be subject to statutory, regulatory, and contractual security requirements.

15.1.1 Identification of applicable legislation

- All relevant statutory, regulatory, and contractual requirements and the organization's approach to meet these requirements should be explicitly defined, documented, and kept up to date for each information system and the organization.

15.1.2 Intellectual property rights (IPR)

- Appropriate procedures should be implemented to ensure compliance with legislative, regulatory, and contractual requirements on the use of material in respect of which there may be intellectual property rights and on the use of proprietary software products.

15.1.3 protection of organizational records

- Important records should be protected from loss, destruction, and falsification, in accordance with statutory, regulatory, contractual, and business requirements.

15.1.4 Data protection and privacy of personal information

- Data protection and privacy should be ensured as required in relevant legislation, regulations, and, if applicable, contractual clauses.

15.1.5 Prevention of misuse of information processing facilities

- Users should be deterred from using information processing facilities for unauthorized purposes.

15.1.6 Regulation of cryptographic controls

- Cryptographic controls should be used in compliance with all relevant agreements, laws, and regulations.

15.2 Compliance with security polices and standards, and technical compliance

- **Objective:** To ensure compliance of systems with organizational security policies and standards.
- The security of information systems should be regularly reviewed.

15.2.1 Compliances with security policies and standards

- Managers should ensure that all security procedures within their area of responsibility are carried out correctly to achieve compliance with security policies and standards.

15.2.2 Technical compliance checking

- Information system should be regularly checked for compliance with security implementation standards.

15.3 Information systems audit considerations

- **Objective:** To maximize the effectiveness of and to minimize interference to/from the information systems audit process.
- There should be controls to safeguard operational systems and audit tools during information systems audits.

15.3.1 Information system audit controls

- Audit requirements and activities involving checks on operational systems should be carefully planned and agreed to minimize the risk of disruptions to business processes.

15.3.2 Protection of information systems audit tools

- Access to information systems audit tools should be protected to prevent any possible misuse or compromise.

Benefits of ISO 27001

- A single reference point for identifying a range of controls needed for most situations where information systems are used
- Facilitation of trading in trusted environment
- An internationally recognized structured methodology
- A defined process to evaluate, implement, maintain and manage information security
- A set of tailored policy, standards, procedures and guidelines
- The standard provides a yardstick against which security can be judged

Advantages of ISO 27001

- Improved effectiveness of Information Security
- Market Differentiation
- Provides confidence to trading partners, stakeholders, and customers (certification demonstrates 'due diligence')
- The only standard with global acceptance
- Potential lower rates on insurance premiums
- Compliance with mandates and laws (e.g., Data Protection Act, Communications Protection Act)
- Reduced liability due to implemented or enforced policies and procedures

Benefits of Certification

- Public demonstration
- Enhanced corporate image
- Accountability/ re-assurance
- Drives forward improvement proc
- Ensures management commitment
- A positive response from potential customers
- Can be part of integrated approach 9001/14001/ISMS
- Staff motivation