www.isea.gov.in

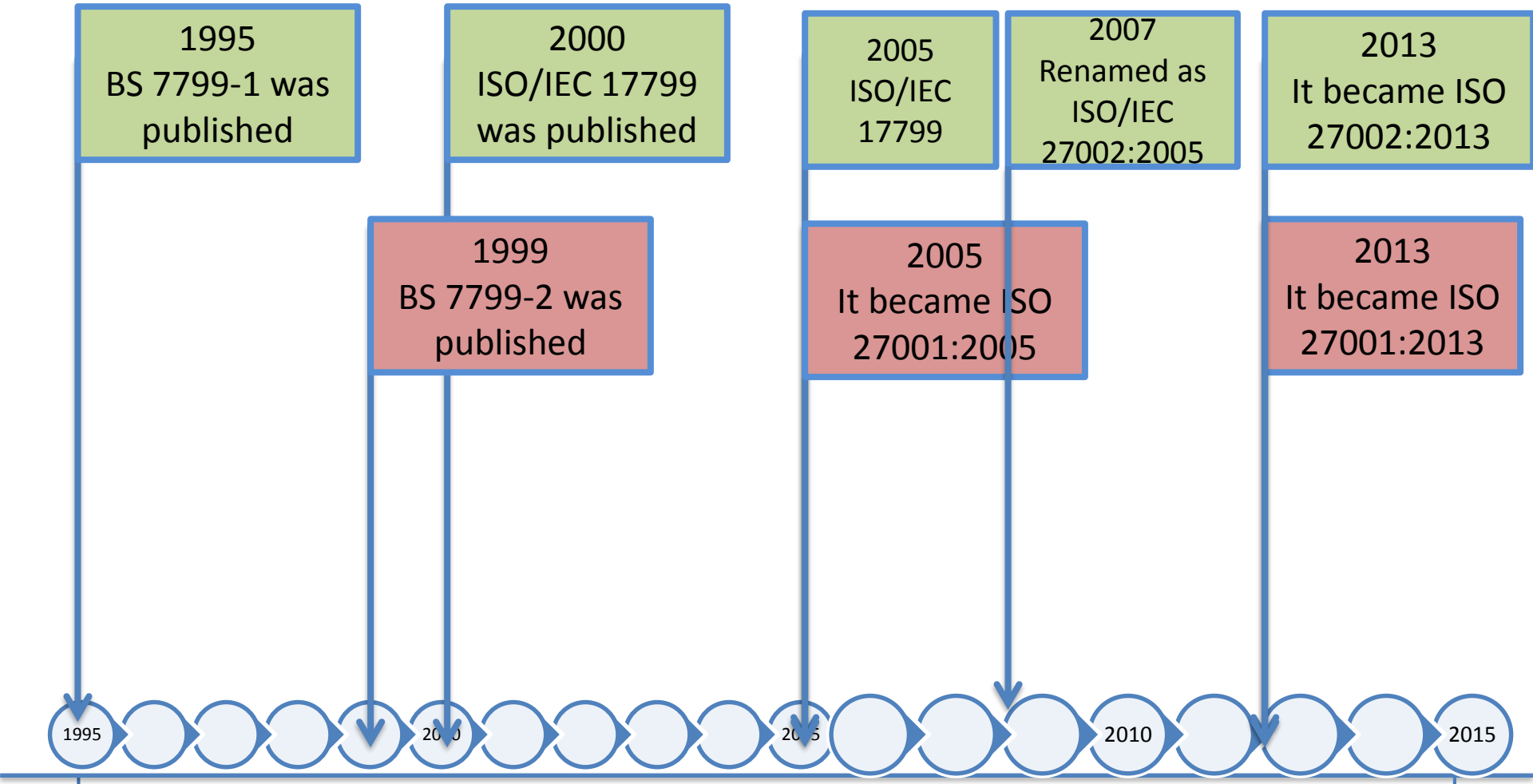
ISMS requirements and ISO/IEC 27000 family

for

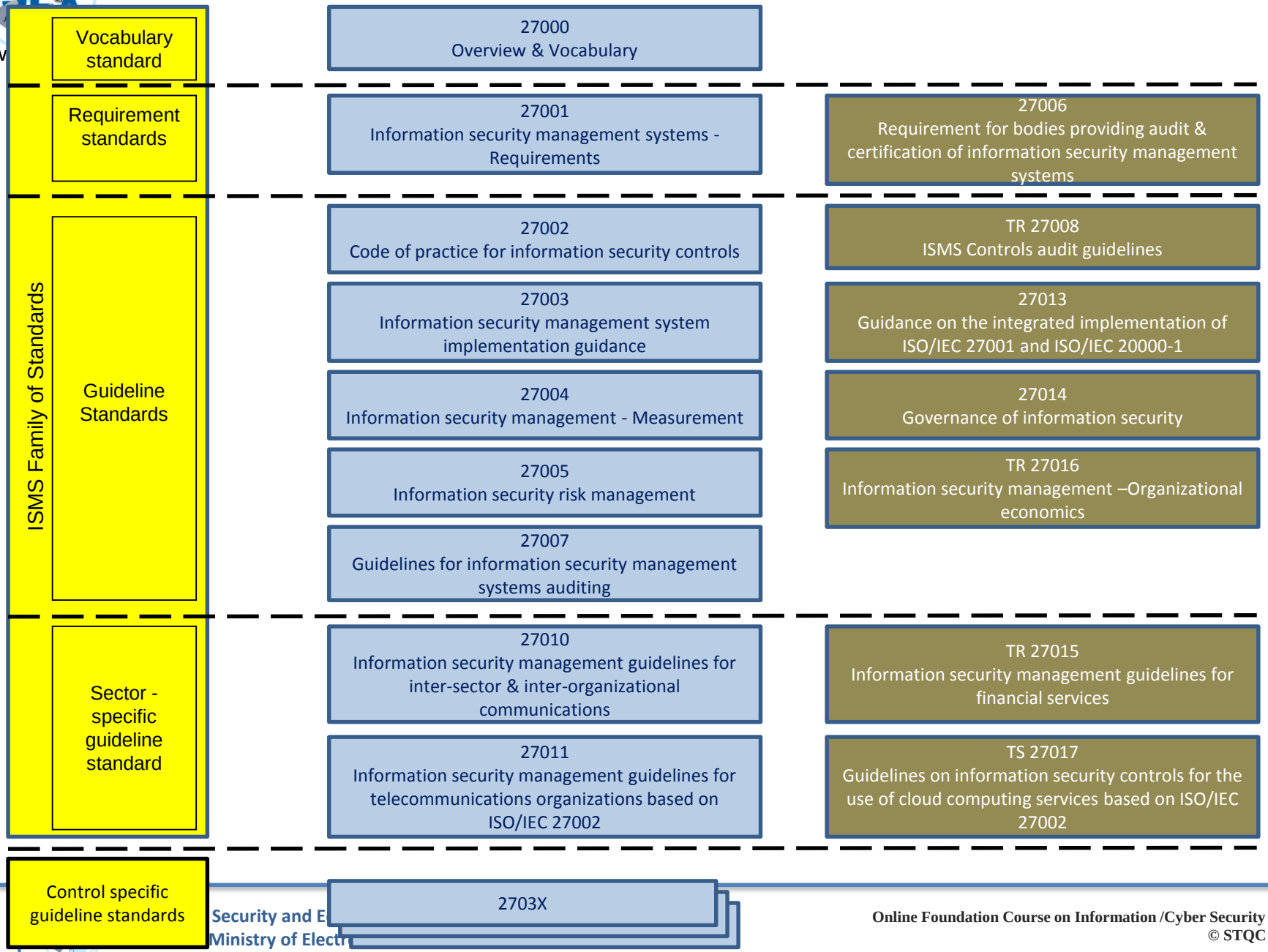
CS&DPL at NALSAR, Hyderbad

Sh. Tapas Bandyopadhyay, Scientist F
Sh. M Vellaipandi , Scientist F
STQC ,MeitY, Govt. of India

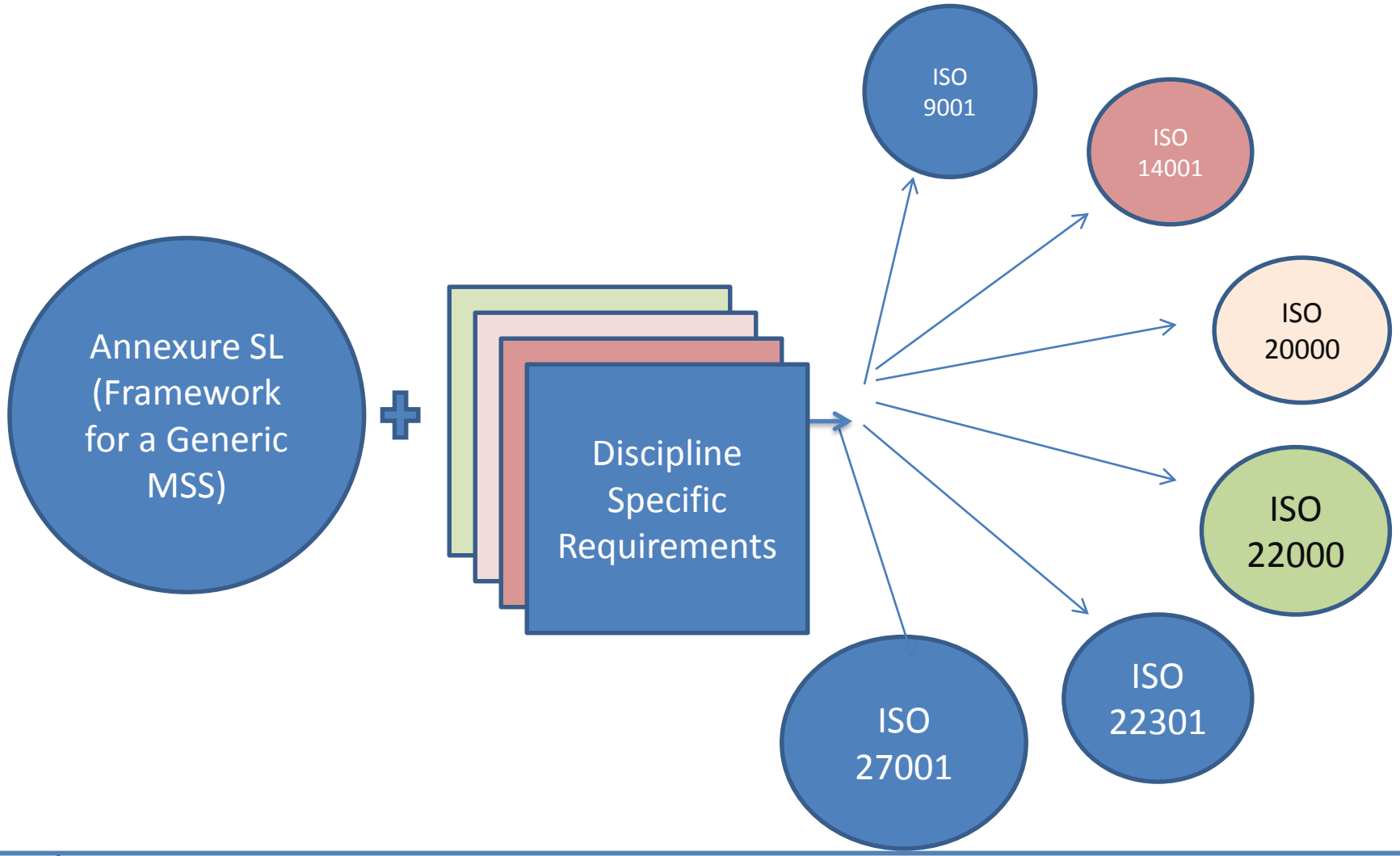
ISO/IEC 27001 – Journey so far



ISMS Family of Standards and the Relationships



Management System Standards



www.isea.gov.in

High Level Structure of ISO/IEC 27001

(as provided by Annex SL - Appendix 2)

0. Introduction

1. Scope

2. Normative references

3. Terms and definition

4. Context of the organization

4.1. Understanding the organisation and its context.

4.2. Understand the needs and expectations of interested parties.

4.3. Determining the scope of the information security management system.

4.4 Information Security management system

5. Leadership

5.1 Leadership and commitment

5.2 Policy

5.3 Organization roles, responsibilities and authorities

6. Planning

6.1 Actions to address risks and opportunities

6.2 Information security objectives and planning to achieve them

7. Support

7.1 Resources

7.2 Competence

7.3 Awareness

7.4 Communication

7.5 Documented Information

7.5.1 General

7.5.2 Creating & Updating

7.5.3 Control of documented information

8. Operation

8.1 Operational planning and control

8.2 Information security risk assessment

8.3 Information security risk treatment

9. Performance evaluation

9.1 Monitoring, measurement, analysis and evaluation

9.2 Internal Audit

9.3 Management Review

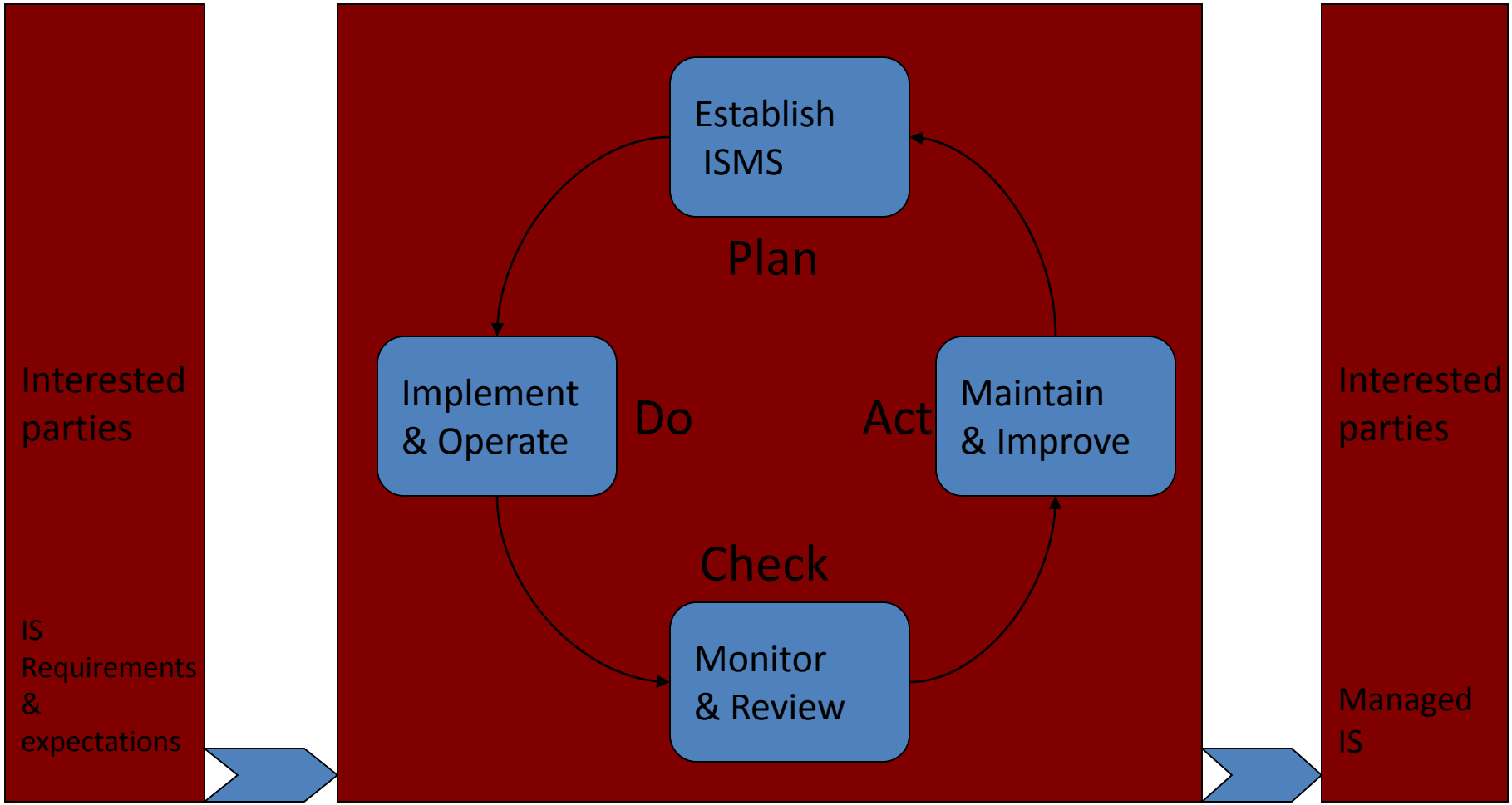
10. Improvement

10.1 Non Compliance & Corrective action

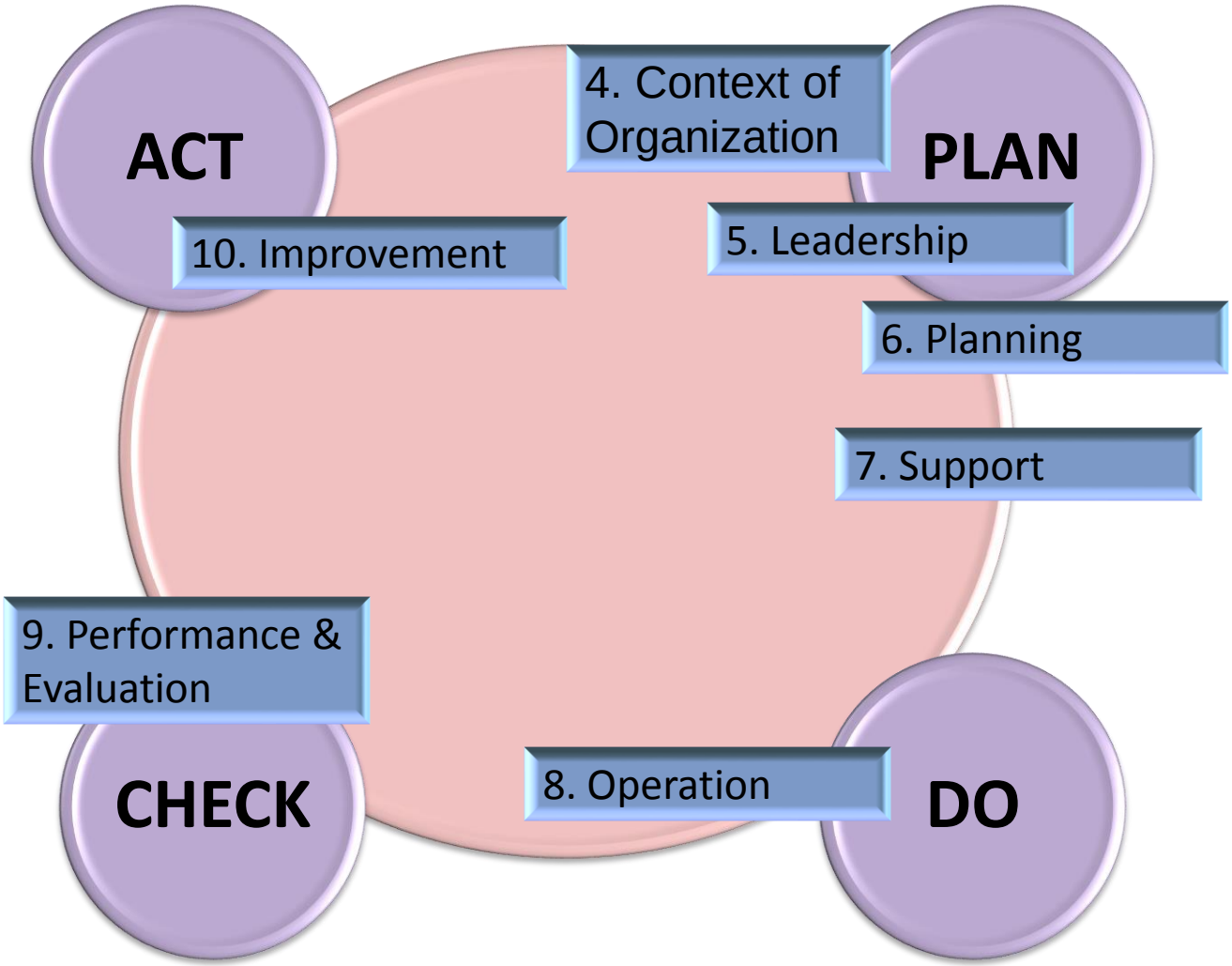
10.2 Continual improvement

All new or revised ISO MSS will have this structure except discipline-specific requirements

PDCA Model of ISMS



Model Solution



4. Context of the organisation

4.1 Understanding the organisation and its context. (Note also the reference to internal and external issues)

- The organization shall determine external and internal issues that are relevant to its purpose and that affect its ability to achieve the intended outcome(s) of its Information Security management system.

4.2 Understand the needs and expectations of interested parties.

4.3 Determining the scope of the information security management system.

4.4 Information security management system

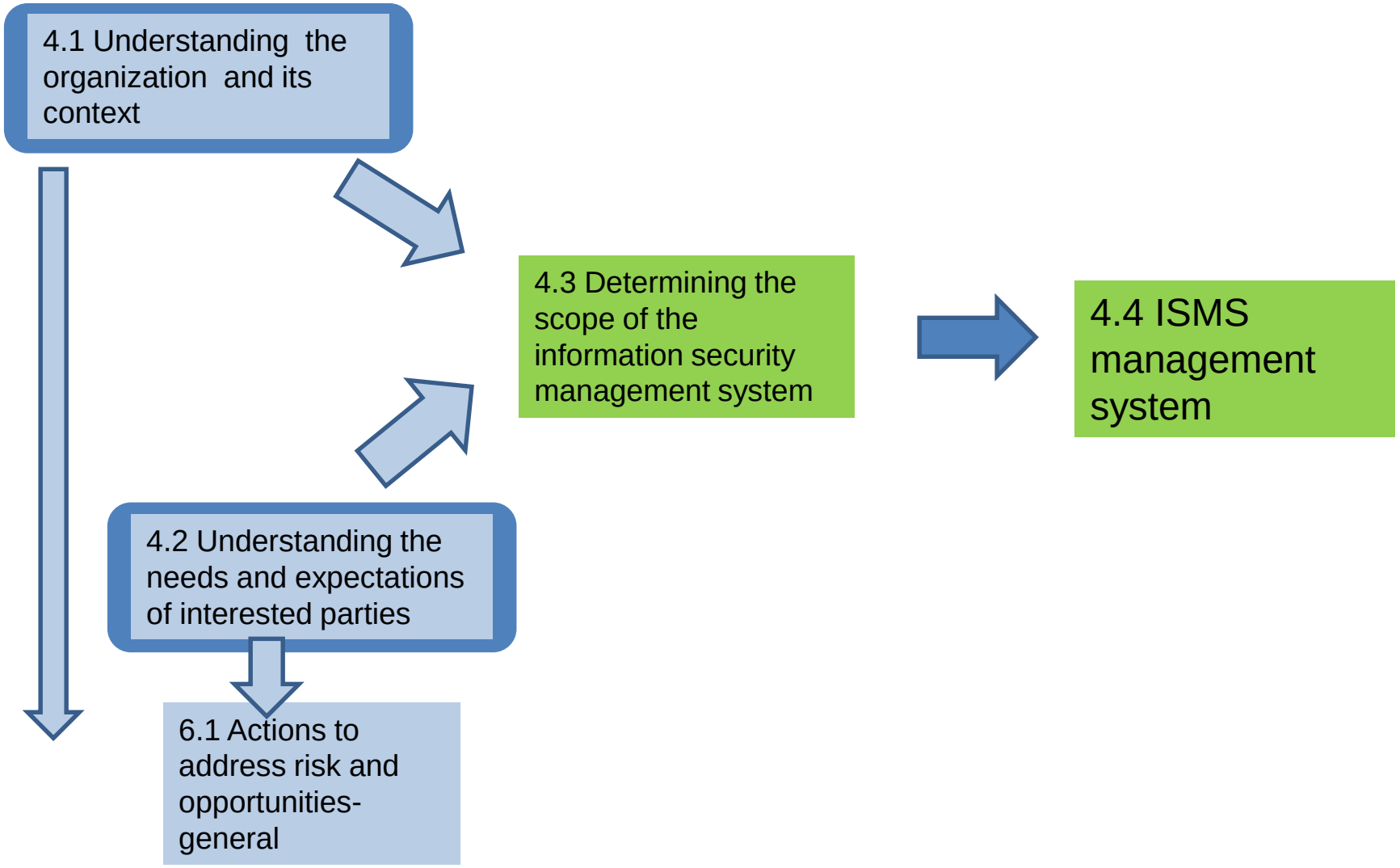
Establish ISMS

- Define the scope of ISMS
- Define an ISMS policy
- Undertake appropriate risk assessment
- Identify the areas of risk to be managed
- Select control objectives and controls to be implemented, justifying the selection
- Prepare a Statement of Applicability

Define the Scope of ISMS

- A document should be prepared that describe the scope of ISMS in terms of Organization, Location, Assets and Technology
- The scope will demonstrate to the management, their security responsibilities and encourage them to pay appropriate attention to the subject

Defining Scope



Example: Scope

- The personnel information about the staff and all other information related to their business processes
- All information processing facilities including computers, printers, LAN and internet connection
- All software used to process information
- Storage media such as disc, CDs, tapes etc

Define Information Security Policy

- A written policy document should be available to all employees responsible for information security
- It should contain a statement of intent by the senior management
- The policies should be simple and to the point
- The top level policy, the ***Security Policy Statement***, should be distributed to all staff
- The appropriate lower level policies - ***Security Policy Manual*** - should be available to the staffs

5. Leadership

5.1 Leadership and commitment
5.2 Policy
5.3 Organization roles, responsibilities and authorities

There is a change in term, as it was previously 'Management responsibility'.

Note:

ensuring that the ISMS policy and ISMS objectives are established and are compatible with the strategic direction of the organization directing and supporting persons to contribute to the effectiveness of the ISMS management system

6. Planning

6.1 Actions to address risks and opportunities

- When planning for the ISMS management system, the organization shall consider the issues referred to in 4.1 and the requirements referred to in 4.2 and determine the risks and opportunities that need to be addressed to
  - assure the management system can achieve its intended outcome(s)
  - prevent, or reduce, undesired effects
  - achieve continual ISMS improvement.
- The organization shall plan:
  - a) actions to address these risks and opportunities, and
  - b) how to
    - integrate and implement the actions into its ISMS management system processes
    - evaluate the effectiveness of these actions.

6.2 ISMS objectives and planning to achieve them

Risk Assessment & Management

- Perform a risk assessment to identify the high security risk areas
- Depending on the degree of assurance required, manage the risk, by reducing / avoiding / transferring it, employing suitable controls
- Monitor risk with regular reviews of threats, controls in place and their effectiveness, and audits

Information security objectives

- Sub clause 6.2 requires the organization to establish ISMS objectives at relevant functions and levels.
- The term ‘function’ refers to the functions of the organization. The term ‘level’ refers to the level of management of which top management is the highest.

Examples of Security Objectives

- **Resource protection –**
  - The ability to secure all types of system resources.
  - Define the different categories of users that can access your system.
  - Define what access authorization you want to give these groups of users as part of creating your security policy.
- **Authentication –**
  - The assurance or verification that the resource (human or machine) is really what it claims to be
- **Authorization –**
  - Determining who can access system resources or perform certain activities on a system

Selection of Control Objectives and Controls

- Review the risks and identify control options
- The selection of controls should be made to bring down the risk to acceptable level
- The selection of controls should be cost effective

Statement of Applicability

- Having selected relevant control objectives and controls for each risk, it is necessary to record the selection in a Statement of Applicability(SoA)
- The Statement should also record the exclusion, with justification, of any controls listed in the ISMS Standard (ISO/IEC 27001:2013)

Example: SoA

Control	Selected	Justification
Controls against malicious software	Yes	Highlighted by risk assessment. High risk of damage to network
Authentication for external connections	Yes	High risk of unauthorized access through dial-up lines. Security policy specifies authentication to be mandatory
Duress alarm to safeguard users	No	Not relevant in this organization.

7.Support

7.1 resources

7.2 Competence

7.3 Awareness

7.4 Communication

7.5 Documented Information

- 7.5.1 General
- 7.5.2 Creating & Updating
- 7.5.3 Control of documented information

8. Operation

8.1 Operational planning and control

8.2 Information security risk assessment

8.3 Information security risk treatment

Implement and Operate ISMS

- Implement the risk management plan
  - Allocate resources, roles and responsibilities
- Implement controls to meet control objectives
- Implement training and awareness
- Manage operations
- Manage resources
- Implement procedures

9. Performance evaluation

9.1 Monitoring, measurement, analysis and evaluation

9.2 Internal Audit

9.3 Management Review

10. Improvement

10.1 Non Compliance & Corrective action

10.2 Continual improvement

Monitor and Review the ISMS

- Execute monitoring controls to
  - detect errors in processing
  - detect security incidents
- Review effectiveness of the ISMS
- Review risk taking account of changes to
  - Organization
  - Technology
  - Business objectives and processes
  - Identified threats
  - External events like legal requirements, social climate etc.

Maintain and Improve the ISMS

- Implement the identified improvements
- Take appropriate corrective and preventive actions
- Communicate the results and actions and agree with all interested parties
- Ensure that the improvements achieve their intended objectives

ISMS Documentation

- Documented statements of security policy and control objectives
- The scope of the ISMS and procedures and controls in support of the ISMS
- Risk assessment and management reports
- Documented procedures needed by the organization to ensure planning, operation and control of its IS processes
- Records required by the ISMS standard
- Statement of Applicability

Critical Success Factors

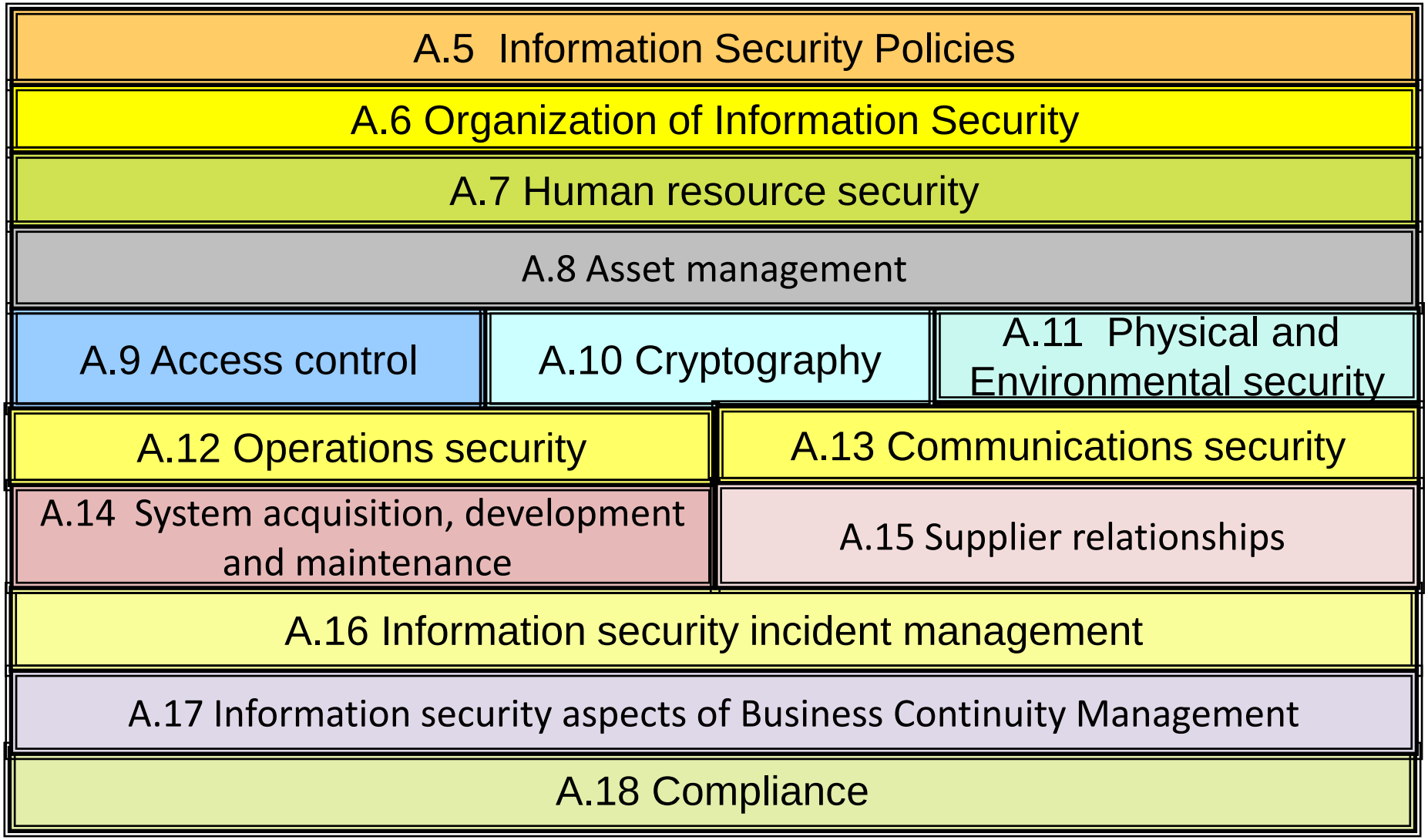
- Security policy, objectives and activities should reflect business objectives
- Visible support and commitment from management
- Good understanding of security requirements, risk assessment and risk management
- Effective marketing of security to all (management and users)
- Distribution of comprehensive guidance, education & training
- Comprehensive and balanced system of measurement

But the Problem is....

"To determine how much is too much, so that we can implement appropriate security measures to build adequate confidence and trust"

Therefore Information Security needs to be managed!

Control Clauses of ISO/IEC 27001:2013



Why Security Policy ?

"The best security technology with a bad policy like a grass hut with a steel gate."

"The policy on security is the organization's statement of intent that provides the foundation for management and staff alike."

Organization of Information Security

Internal organization (A 6.1)

Objective : To establish a management framework to initiate and control the implementation and operation of information security within the organization

Mobile devices and Teleworking (A6.2)

Objective : To ensure the security of teleworking and use of mobile devices.

Human resources Security

The organization will be vulnerable to widespread insecurity, if the employee are not aware of Security Policy and Expectations.

Prior to employment(A7.1)

Objective : To ensure that employees and contractors understand their responsibilities and are suitable for the roles for which they are considered..

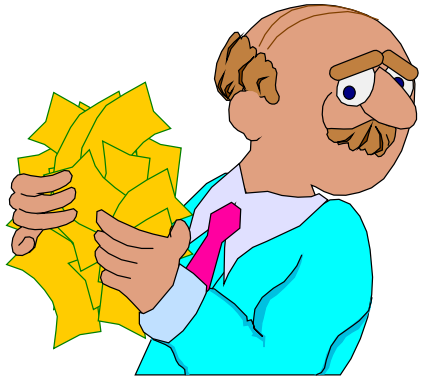
During employment(A7.2)

Objective : To ensure that employees and contractors are aware of and fulfil their information security responsibilities.

Asset Management

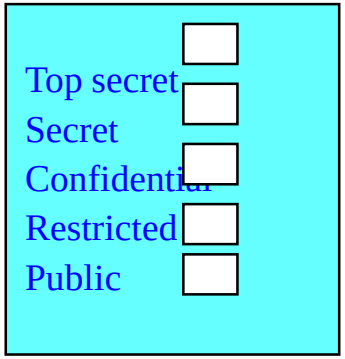
www.isea.gov.in

An asset is something to which an organization assigns value and hence requires protection.



Responsibility of Asset (A8.1)

Objective :To identify organizational assets and define appropriate protection responsibilities.



Information Classification (A8.2)

Objective :To ensure that Information Assets receive appropriate level of protection.

Media Handling (A8.3)

Objective : **To prevent unauthorized disclosure, modification, removal or destruction of information stored on media.**

Responsibility of Asset (A 8.1)

Controls :

A 8.1.1 Inventory of assets

A 8.1.2 Ownership of assets

A 8.1.3 Acceptable use of assets

A 8.1.4 Return of assets

Media handling(A 8.3)

Controls :

A 8.3.1 Management of removable media

A 8.3.2 Disposal of media

A 8.3.3 Physical media transfer

Access control

Business requirement for access control (A 9.1)

Objective : To limit access to information and information processing facilities.

User access management (A 9.2)

Objective : To ensure authorized user access and to prevent unauthorized access to systems and services.

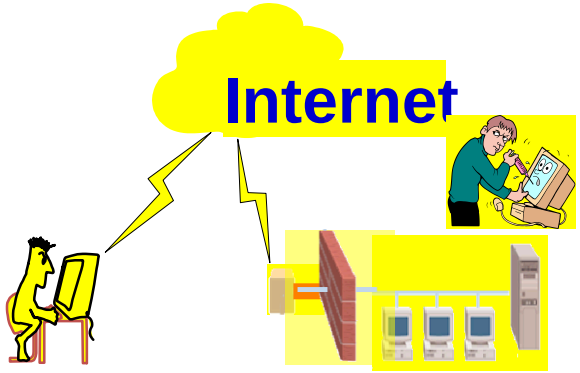
Access control

User responsibilities (A 9.3)

Objective : To make users accountable for safeguarding their authentication information.

System and application access control(A 9.4)

Objective : To prevent unauthorized access to systems and applications..



Cryptography

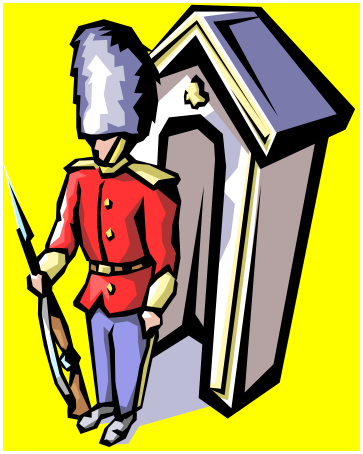
A.10.1 Cryptographic controls

Objective: To ensure proper and effective use of cryptography to protect the confidentiality, authenticity and/or integrity of information.

Physical and environmental security

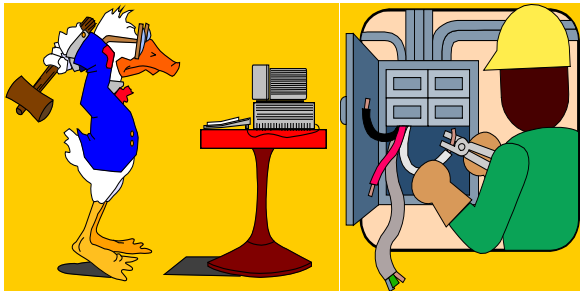
Secure Area (A 11.1)

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



Equipment Security (A 11.2)

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



Operations Security

Operational Procedures and responsibilities (A12.1)

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

Protection from malware(A12.2

Objective : To ensure that information and information processing facilities are protected against malware..

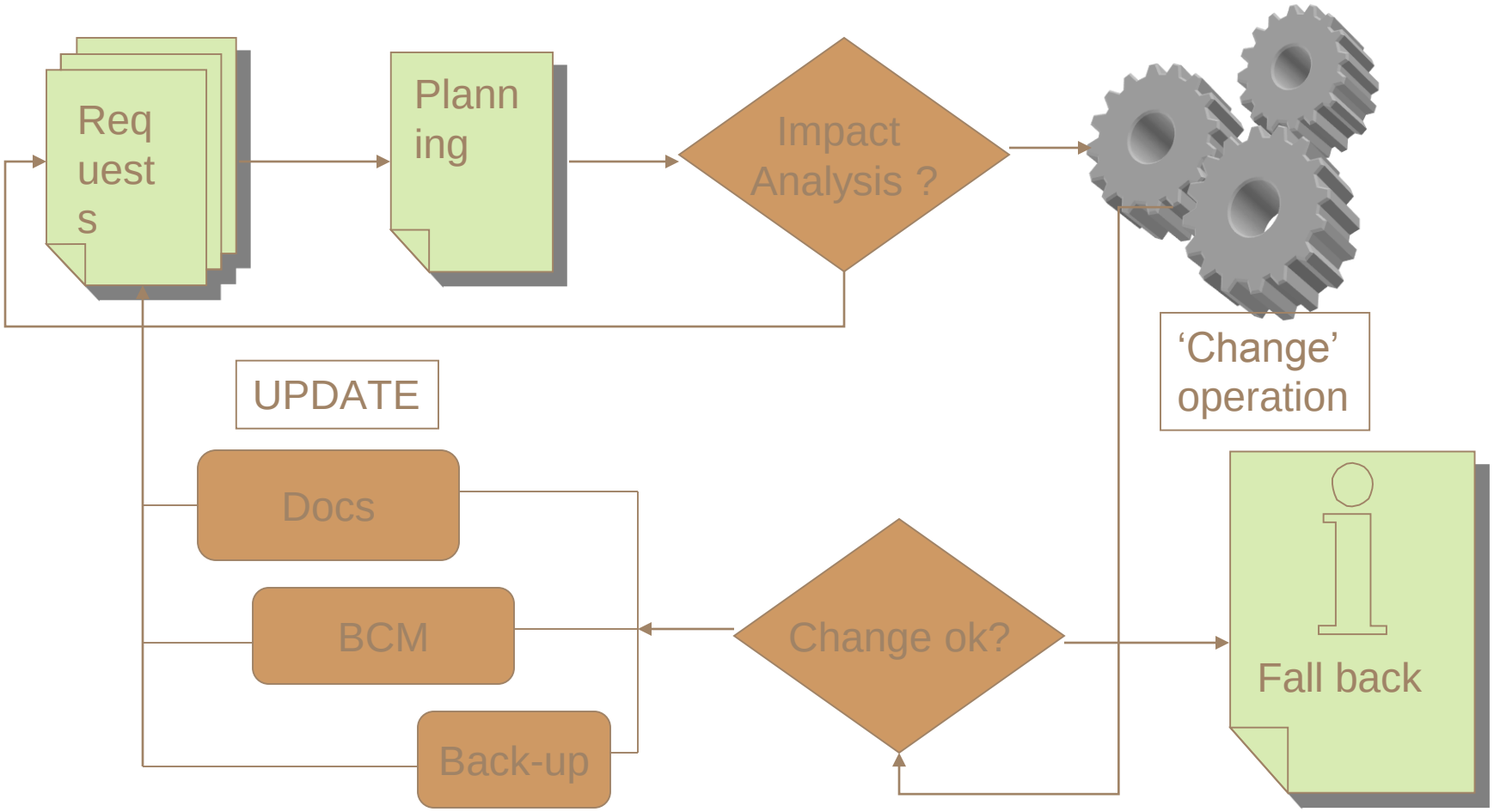
Backup(A12.3)

Objective : To protect against loss of data..

Logging and monitoring(A12.4)

Objective : To record events and generate evidence..

Change management



Communication security

Network security management (A13.1)

Objective : To ensure the protection of information in networks and its supporting information processing facilities..

Information transfer(A13.2)

Objective : To maintain the security of information transferred within an organization and with any external entity..

Information systems acquisition, development and maintenance

www.isea.gov.in

Security requirements of information systems (A 14.1)

Objective : To ensure that information security is an integral part of information systems across the entire lifecycle. This also includes the requirements for information systems which provide services over public networks.

Security in development and support processes(A 14.2)

Objective : To ensure that information security is designed and implemented within the development lifecycle of information systems.

Test Data(A 14.3)

Objective : To ensure the protection of data used for testing.

Supplier relationships

A.15.1 Information security in supplier relationships

Objective: To ensure protection of the organization's assets that is accessible by suppliers.

A.15.2 Supplier service delivery management

Objective: To maintain an agreed level of information security and service delivery in line with supplier agreements..

Management of information security incidents and improvements (A 16.1)

Issues:

- ***Formal event reporting***
- ***Escalation procedures***
- ***Awareness of all employee and third party member in this regard***
- ***Providing means of reporting***

Controls:

A 16.1.1 Responsibilities and procedures.

A 16.1.2 Reporting information security events

A.16.1.3 Reporting information security weaknesses

A.16.1.4 Assessment of and decision on information security events

A.16.1.5 Response to information security incidents

A.16.1.6 Learning from information security incidents

A.16.1.7 Collection of evidence

Information security aspects of business continuity management

Information security continuity (A 17.1)

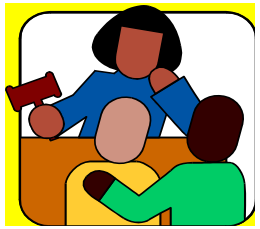
- **Objective :** ***Information security continuity shall be embedded in the organization's business continuity management systems*****.**

Redundancies (A 17.2)

- **Objective :** ***To ensure availability of information processing facilities***

www.isea.gov.in

Compliance with legal and contractual requirements (A 18.1)



Issues:

- ***Operation of ISMS within the legal framework complying with statutory, regulatory and contractual security requirement***
- ***Obtaining proper and reliable legal advice***
- ***Complying with the legal requirements of other country in case of trans broader flow of data.***

Controls:

A.18.1.1 Identification of applicable legislation and contractual requirements

A 18.1.2 Intellectual property rights (IPR)

A 18.1.3 Protection of records

A 18.1.4 Privacy and protection of personally identifiable information

A 18.1.5 Regulation of cryptographic controls

Technical compliance review

Control statement:

Information systems shall be regularly reviewed for compliance with the organization's information security policies and standards.

Details:

- *The information system shall be regularly checked for technical compliance with security to ensure hardware and software controls have correctly been implemented*
- *Technical compliance testing shall be carried out by authorized experts only and under strict supervision.*
- *Extreme caution should be exercised in respect of leakage of the result of such testing.*
- *If penetration tests or vulnerability assessments are used, caution should be exercised as such activities could lead to a compromise of the security of the system. Such tests should be planned, documented and repeatable*

ISO/IEC 27001:2013

Implementation, Auditing and Certification Issues

Documented Requirements from clause 4

Understanding the organization & its context	Understanding the needs & expectations of interested parties	Determining scope of the ISMS
• Mission Statement • Internal & external issues (risk registers, strategy, MOMs) • Context Statement	• Legislation & regulatory compliance register • Contracts	• Scope statement

Mandatory Documentation

- Scope of the ISMS (clause 4.3)
- Information security policy and objectives (clauses 5.2 and 6.2)
- Risk assessment and risk treatment methodology (clause 6.1.2)
- Statement of Applicability (clause 6.1.3 d)
- Risk treatment plan (clauses 6.1.3 e and 6.2)
- Risk assessment report (clause 8.2)
- Definition of security roles and responsibilities (clauses A.7.1.2 and A.13.2.4)
- Inventory of assets (clause A.8.1.1)
- Acceptable use of assets (clause A.8.1.3)
- Access control policy (clause A.9.1.1)
- Operating procedures for IT management (clause A.12.1.1)
- Secure system engineering principles (clause A.14.2.5)
- Supplier security policy (clause A.15.1.1)
- Incident management procedure (clause A.16.1.5)
- Business continuity procedures (clause A.17.1.2)
- Statutory, regulatory, and contractual requirements (clause A.18.1.1)

Mandatory Records

- Records of training, skills, experience and qualifications (clause 7.2)
- Monitoring and measurement results (clause 9.1)
- Internal audit program (clause 9.2)
- Results of internal audits (clause 9.2)
- Results of the management review (clause 9.3)
- Results of corrective actions (clause 10.1)
- Logs of user activities, exceptions, and security events (clauses A.12.4.1 and A.12.4.3)

Non-mandatory documents to be commonly used

- Procedure for document control (clause 7.5)
- Controls for managing records (clause 7.5)
- Procedure for internal audit (clause 9.2)
- Procedure for corrective action (clause 10.1)
- Bring your own device (BYOD) policy (clause A.6.2.1)
- Mobile device and teleworking policy (clause A.6.2.1)
- Information classification policy (clauses A.8.2.1, A.8.2.2, and A.8.2.3)
- Password policy (clauses A.9.2.1, A.9.2.2, A.9.2.4, A.9.3.1, and A.9.4.3)
- Business impact analysis (clause A.17.1.1)
- Exercising and testing plan (clause A.17.1.3)
- Maintenance and review plan (clause A.17.1.3)
- Business continuity strategy (clause A.17.2.1)
- Disposal and destruction policy (clauses A.8.3.2 and A.11.2.7)
- Procedures for working in secure areas (clause A.11.1.5)
- Clear desk and clear screen policy (clause A.11.2.9)
- Change management policy (clauses A.12.1.2 and A.14.2.4)
- Backup policy (clause A.12.3.1)
- Information transfer policy (clauses A.13.2.1, A.13.2.2, and A.13.2.3)

Thank You