INFORMATION AND NETWORK SECURITY - REQUIREMENTS (FIRST REVISION)

MCMC MTSFB TC G009:2019

Rafeah Omar
Expert member, Information and Network Security Sub Working Group (INS SWG), MTSFB
12 August 2021

Outline

1. Background and Introduction
2. Benefit
3. Objective
4. Technical Codes Requirement
5. Challenges & Conclusion

Background and Introduction

- This technical code for Information and Network Security - Requirements was developed pursuant to section 185 of the Act 588 by the Malaysian Technical Standards Forum Bhd (MTSFB) via its Security, Trust and Privacy Working Group.

- Major modifications in this revision are as follows:

  a) **update on the risk management process**; and

  b) **update of security controls** with additional control based on Critical Security Controls CIS 20 V7.0.

- Technical Code shall replace the following Technical Codes:

2016

- Requirement for Information & Network Security; MCMC MTSFB TC G009:2016
- Status: Obsolete

2019

- Information & Network Security - Requirements (First Revision); MCMC MTSFB TC G009:2019
- Status: Current

The Technical Code

Title	Technical Code number	Registration date
Information and Network Security – Requirements (First Revision)	MCMC MTSFB TC G009:2019	4 Oct 2019

Contributors

- Celcom Axiata Berhad
- CyberSecurity Malaysia
- Digi Telecommunications Sdn Bhd
- Huawei Technologies (M) Sdn Bhd
- Jabatan Penyiaran Malaysia
- Maxis Communications Berhad
- Orbitage Sdn Bhd
- Telekom Malaysia Berhad
- TIME dotCom Berhad
- Universiti Kuala Lumpur
- Universiti Sains Malaysia
- webe digital sdn bhd

3 Objective

Objectives of the Technical Code

To provide requirement for establishing, implementing, maintaining and continuously improving an INS management system.

To establish requirements for the assessment and treatment of Information Security Risks, tailored to the needs of the organization.

The requirement set out in this Technical Code are generic and intended to be applicable to all organizations, regardless of size, type or nature.

4 Technical Code Requirements

Technical Code Requirements

Part 1
INS Mandatory Requirement

INS Management System mandatory clause are mapped to ISO 27001:2013.

Item 5 to 10 ~ Page 1 to 12

Part 2
INS Risk Management

Requirement for INS Risk Management are based on *ISO 31000:2018 Guidelines for Risk Management.*

Item 5.2 ~ Page 2 to 5

Part 3
Security Controls

Revise the controls in Annexe A with additional control based on Critical Security Controls CIS 20 ver7.0.

Annexe A ~ Page 13 to 23

Part 1

INS Mandatory Requirement

INS Management System mandatory requirement are mapped to **ISO 27001:2013** clauses.

CLAUSE

- 5 Requirements
- 6 Roles and Responsibilities
- 7 Support
- 8 Operations
- 9 Performance Evaluation
- 10 Improvements

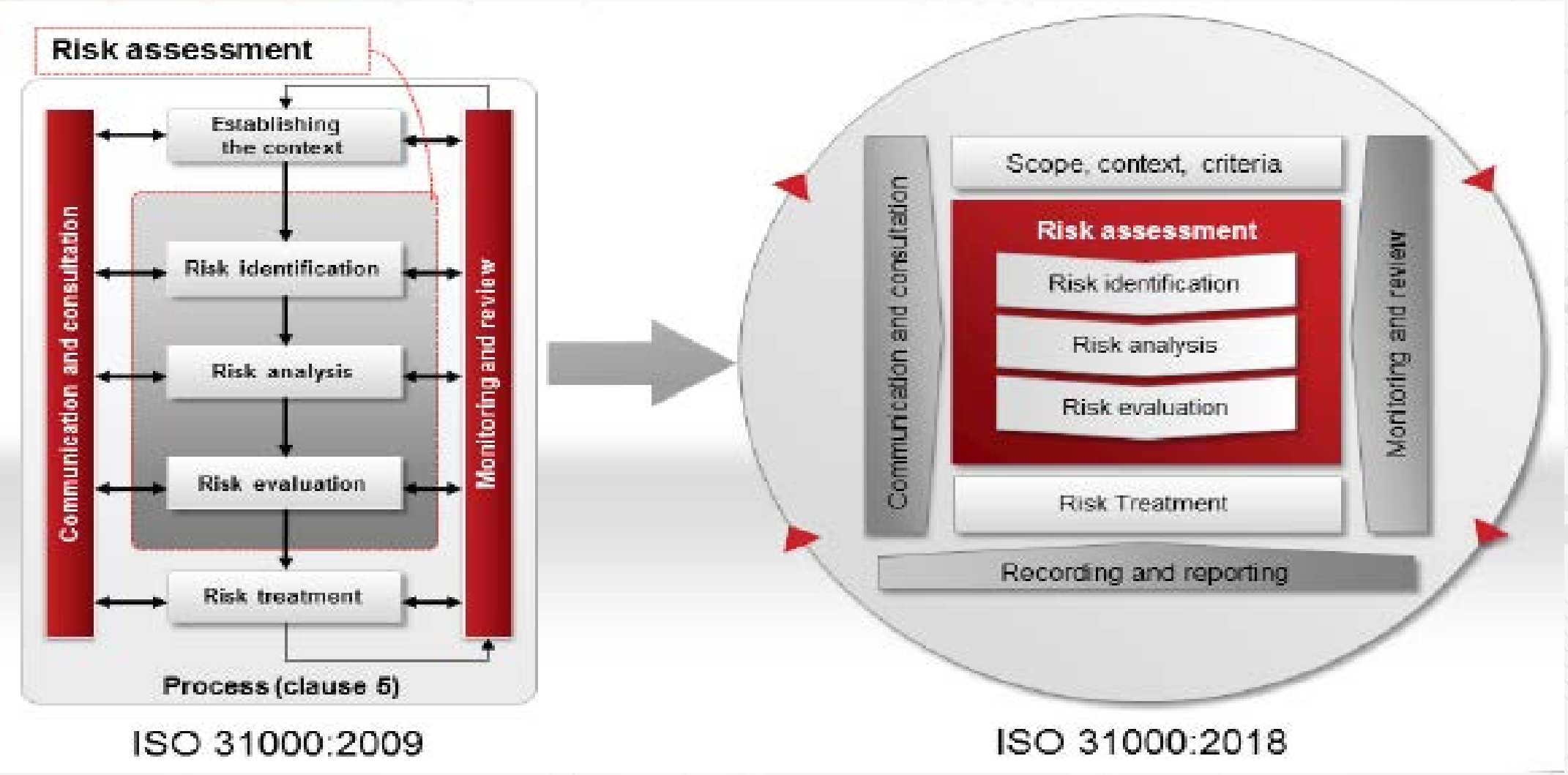
Part 1

INS Mandatory Requirement

Clause	INS – Requirement	ISO 27001:2013
5	Requirement	Clause 4 : Context of the organization Part of clause 6 ISO 31000:2018 Risk Management - Guidelines
6	Roles and responsibilities	Part of clause 5
7	Support	Clause 7 : Support
8	Operations	Part of clause 6 Clause 8: Operations
9	Performance Evaluation	Clause 9: Performance Evaluation
10	Improvement	Clause 10: Improvement

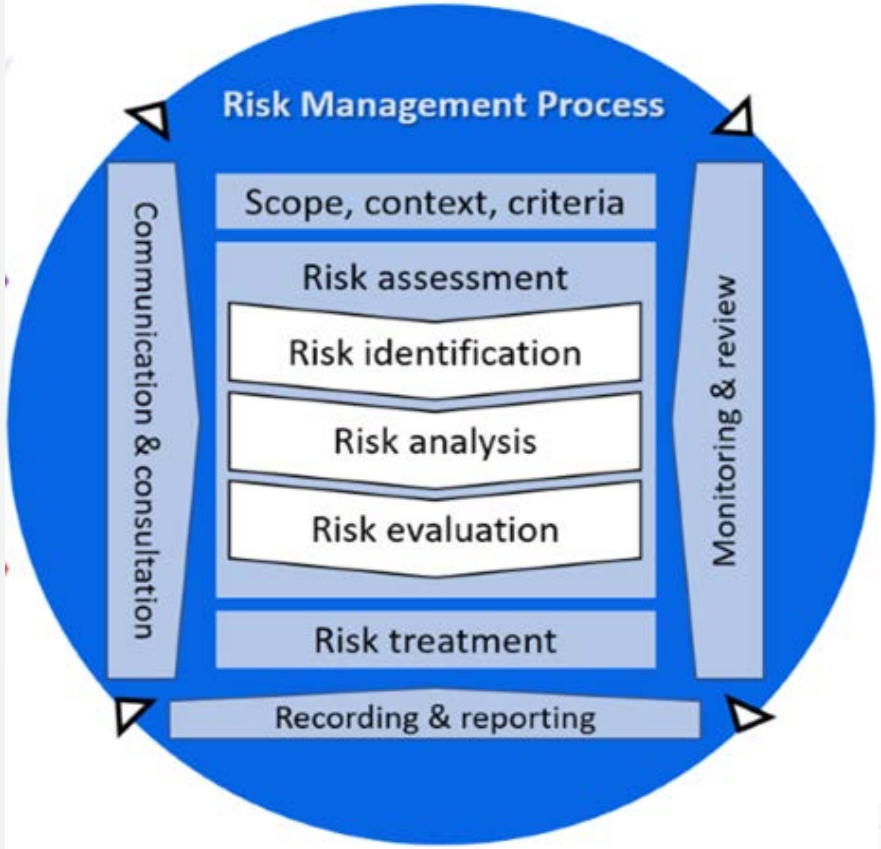
Part 2

INS Risk Management



Part 2

INS Risk Management

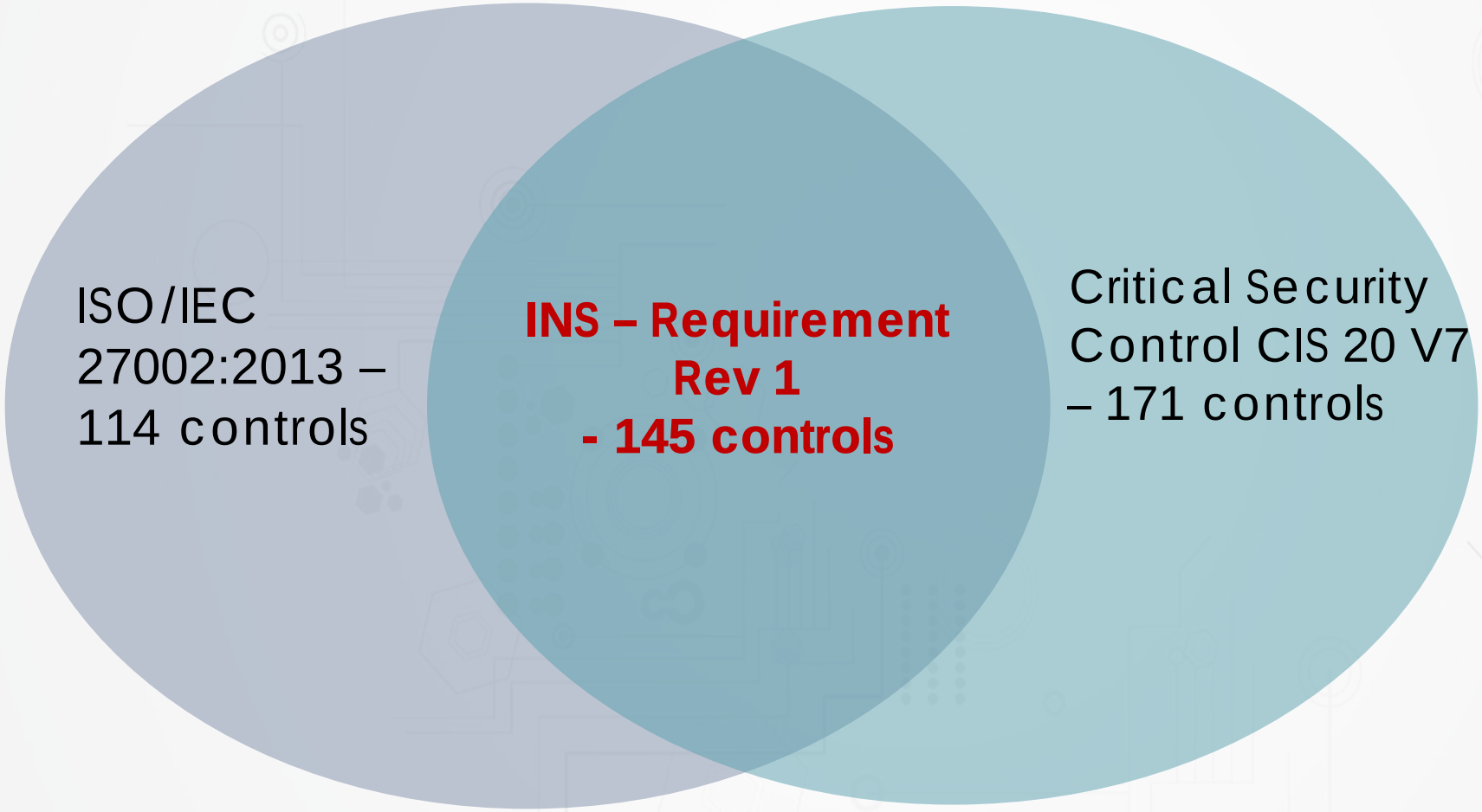


Risk Management Process

- Communication & Consultation
- Scope, Context and Criteria
- Risk Assessment
- Risk treatment
- Monitoring and Review
- Recording & Reporting

Part 3

Security Controls



Part 3

Security Controls

Controls are divided into 4 category:

Part 3

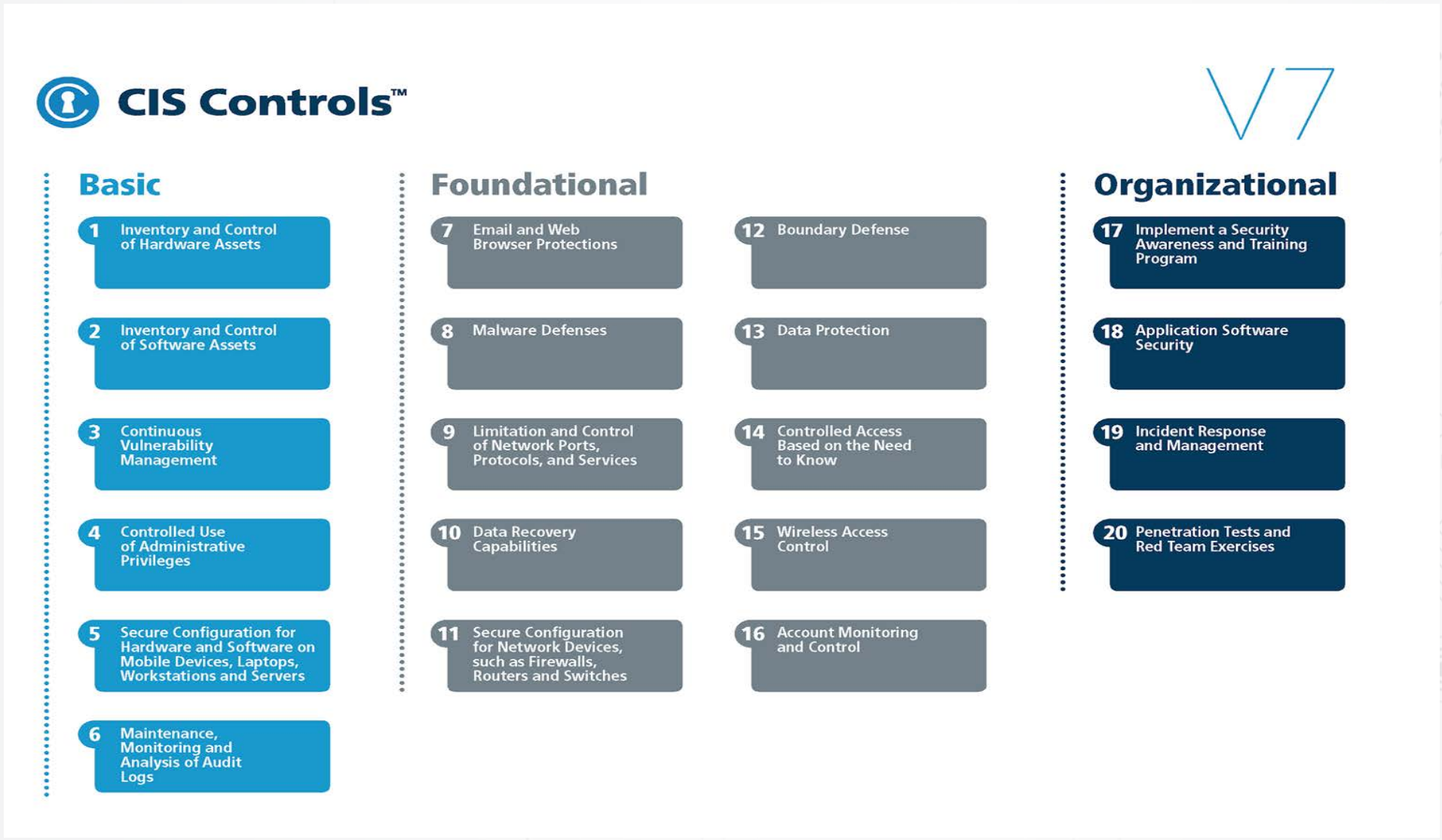
Security Controls

Distribution of controls as per table below:

Category	ISO27001	CSC CIS20
Organization	A.5 IS Policy A.6 Organization of IS A.16 IS incident management A.17 IS aspects of BCM A.18 Compliance	CSC #19
Infrastructure	A.8 Asset Management A.9 Access Control A.10 Cryptography A.12 Operations Security A.13 Communication Security A.14 System acquisition, development and maintenance	CSC#1-16 CSC#18
People	A.7 Human resource security A.15 Supplier relations	CSC #17
Environment	A.11 Physical and Environmental Security	

Part 3

Security Controls



5 Challenges & Conclusion

Challenges

Requirement and Controls for Information and Network Security refers to:

- Different set of standards
- Different kinds of technical experience and background
- Weightage and degree of controls in different industry & organization

Conclusion

It is expected that by the implementation of this technical code, **more organization will comply to the Information and Network Security requirement** as stated in the ISO/IEC 27001: 2013, ISO/IEC 31000:2018 and CIS 20.

The revised Technical Code will benefit:

- Organizations that plan to pursue for Information Security Management System **certification and compliance**.
- **Service providers** as the list of security controls is non-exhaustive and not limited to ISO/IEC 27002:2013

The implementation of this Technical Code is **voluntary basis**.


Q&A

Thank You

Let's Collaborate

Malaysian Technical Standards Forum Bhd

MTSFB

mtsfb_cyberjaya