Management of Cybersecurity - ISO/IEC 27001 Certification

Mr. Steve Fok

Head of ICT, BSI Hong Kong

28-July-2021

Get latest updates from

LinkedIn

Facebook

By Royal Charter

Agenda

- Introduction of ISO/IEC 27001 Standard – Information Security Management System
- How ISO/IEC 27001 Helps for Management of Cybersecurity
- ISO/IEC 27001 Implementation and Certification

Introduction of ISO/IEC 27001 Standard – Information Security Management System

What is information security?

Preservation of confidentiality, integrity and availability of information

What is information security?

What is information security management?

Information security management is about preserving the **'Confidentiality, Integrity and Availability'** of information and associated information processing facilities, whether that's systems, services, infrastructure or the physical locations. It ensures business continuity by minimizing business damage by preventing and reducing the impact of security incidents.

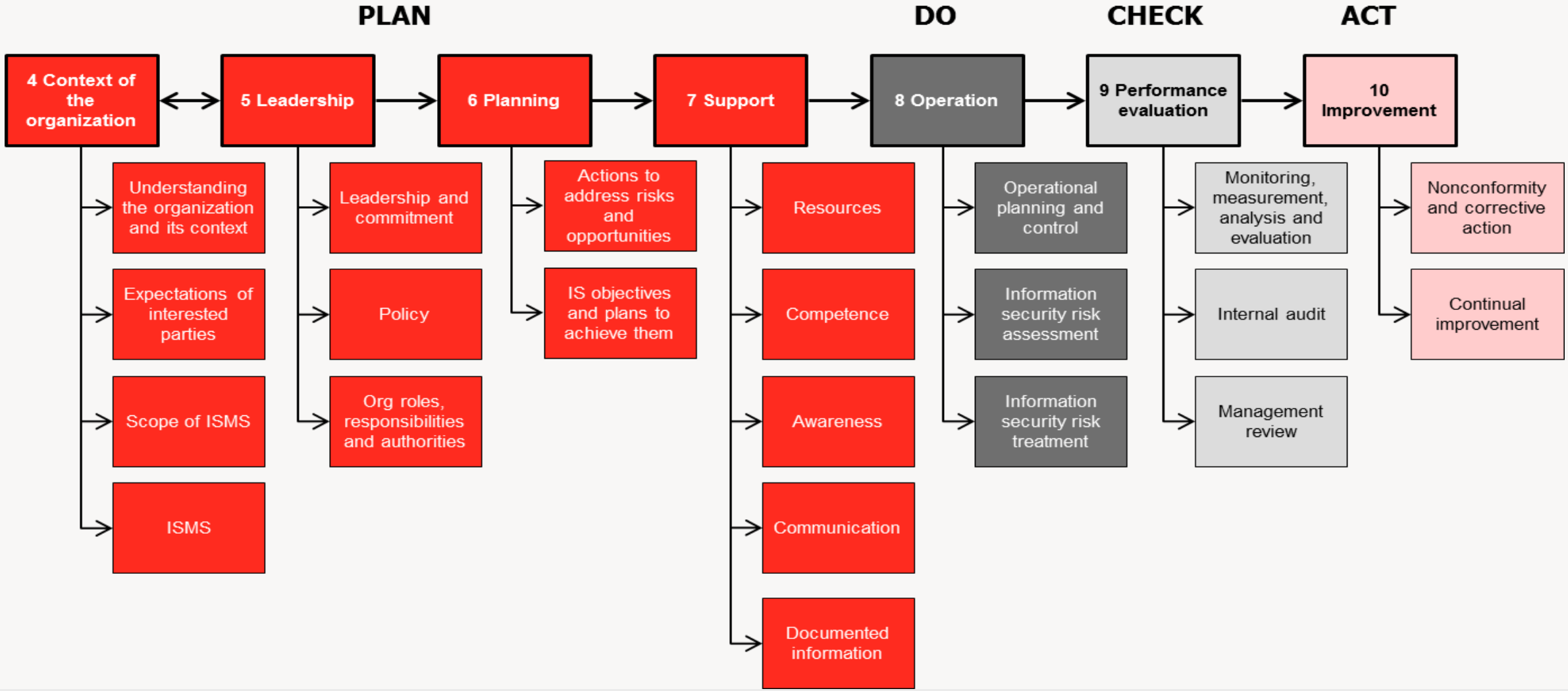
What is ISO/IEC 27001 standard?

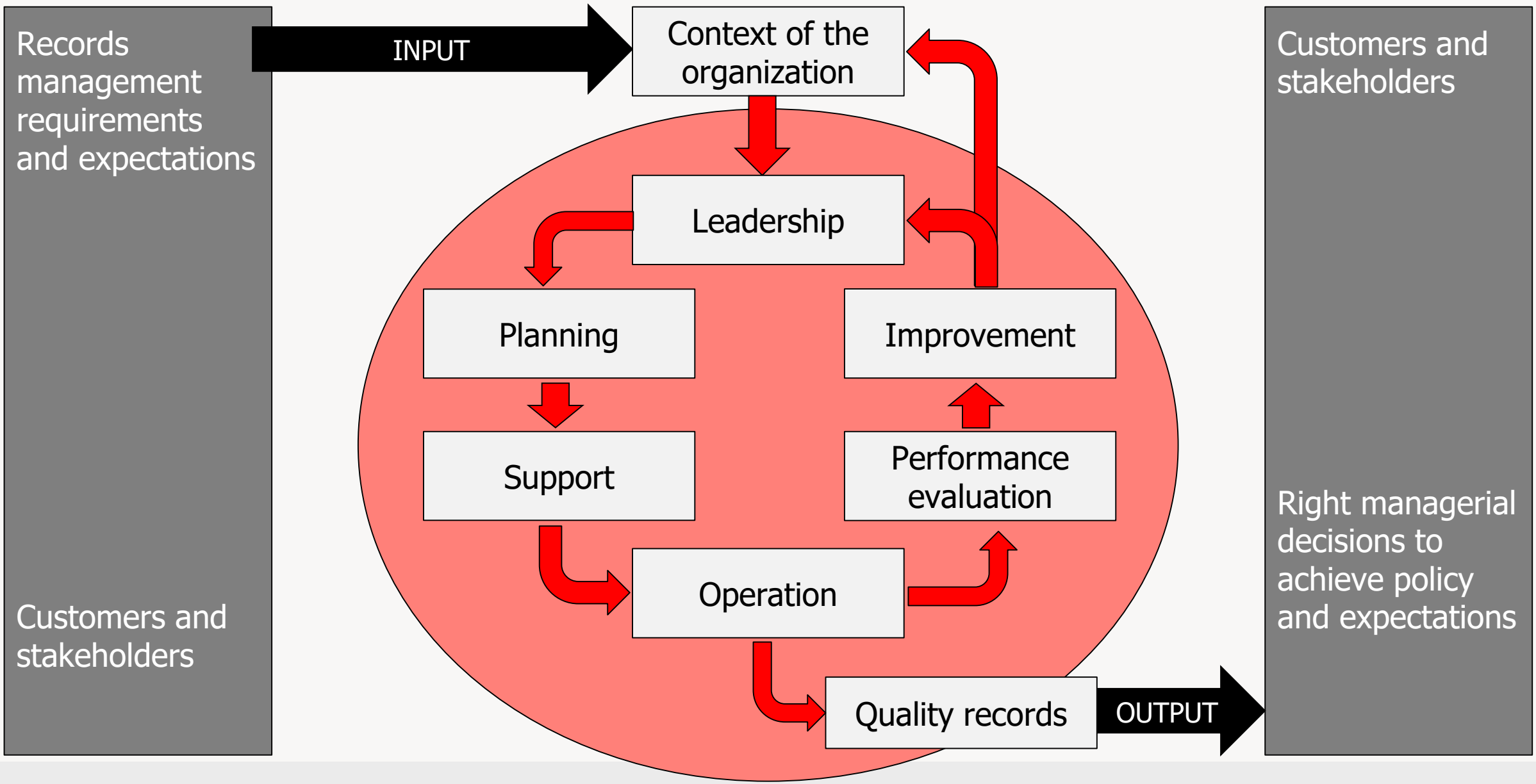
- ISO/IEC 27001 standard specifies the requirements for an information security management system (ISMS)
- Provides a common framework to manage information security
- Takes a risk-based approach to help plan and implement an ISMS
- Ensures the right people, processes, procedures and technologies are in place to protect information assets
- Protects information in terms of confidentiality, integrity and availability
- applicable to all organizations, regardless of type, size or nature

Structure of ISO/IEC 27001

- Annex SL (High Level Structure)
- Annex A (114 Security Controls)

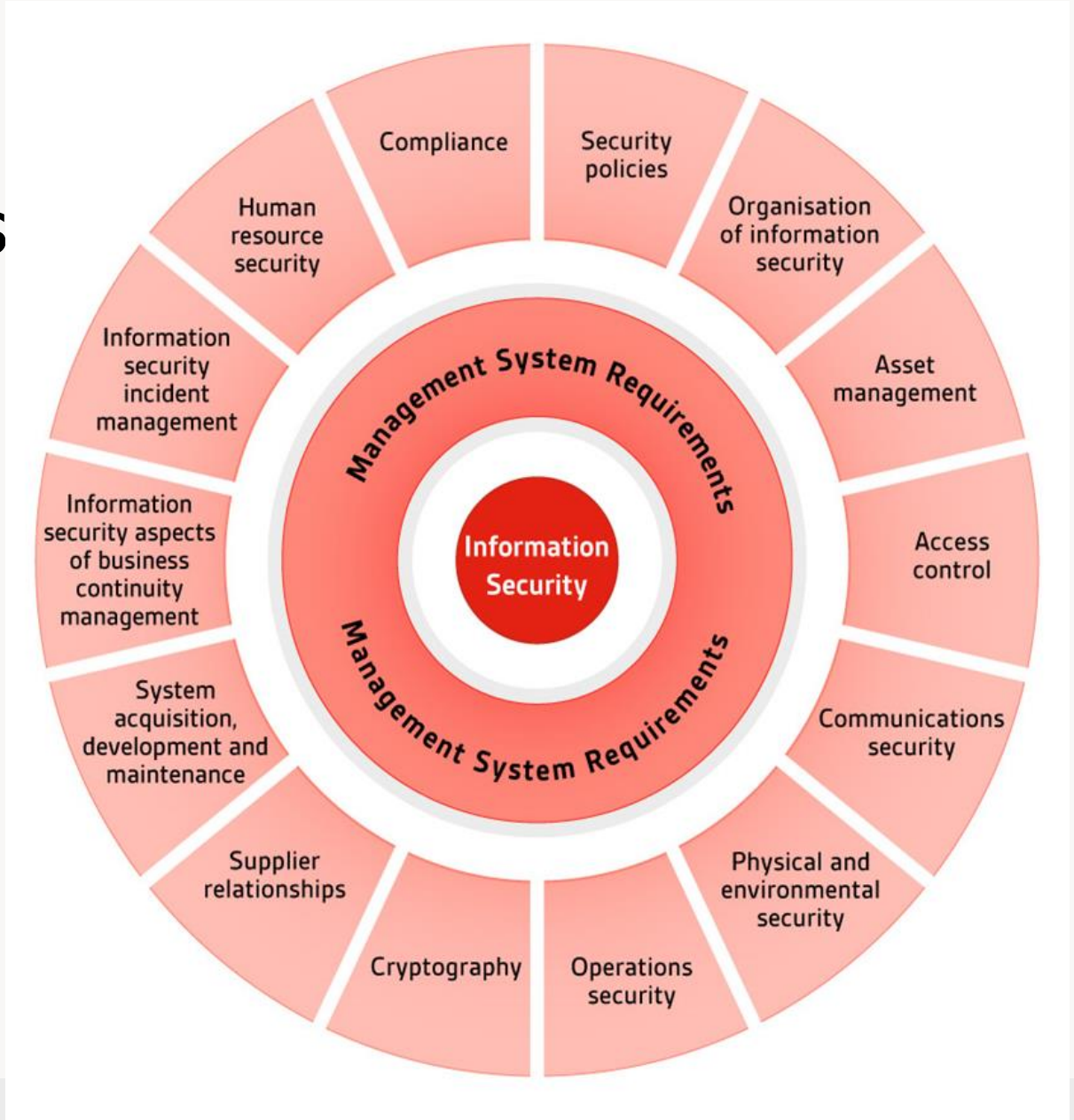
High Level Structure of ISO/IEC 27001





Annex A

- 14 security clause headings
- 35 security categories
- 114 controls



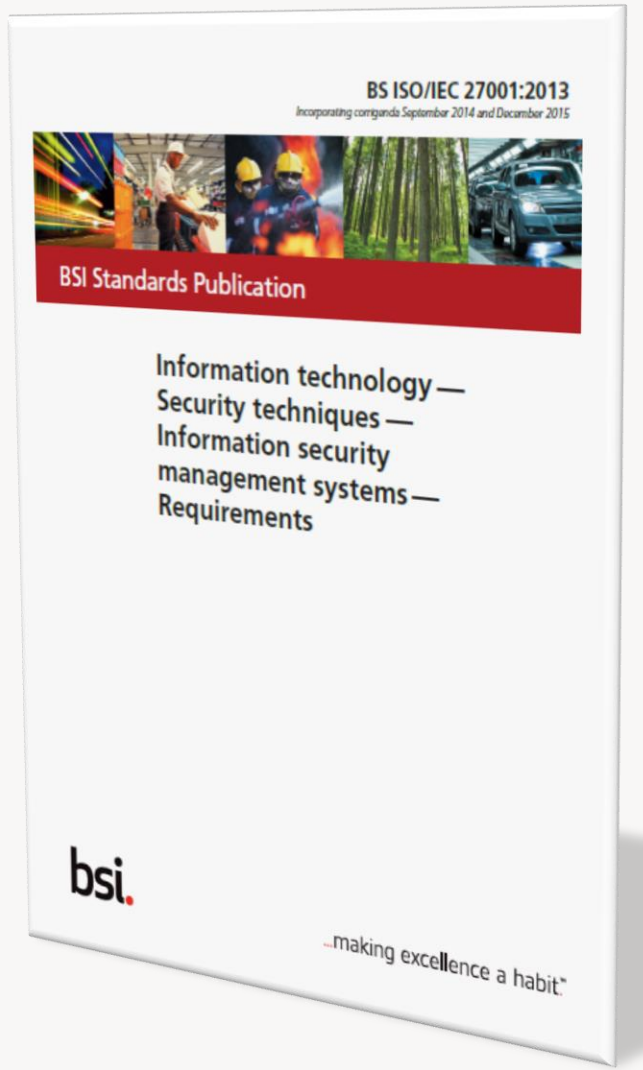
Annex A

- A.5 Information security policies
- A.6 Organization of Information security
- A.7 Human resource security
- A.8 Asset management
- A.9 Access Control
- A.10 Cryptography
- A.11 Physical and environment security

bsi.

Annex A

- A.12 Operations security
- A.13 Communication security
- A.14 System acquisition, development and maintenance
- A.15 Supplier relationships
- A.16 Information security incident management
- A.17 Information security aspects of business continuity management
- A.18 Compliance



Benefits of Implementing Information Security Management System

Benefits?

- Improved security for the organization and its clients.
- Increase in the quality of information security processes and procedures.
- Greater security awareness across all levels of the organization.
- Enhanced customer confidence and perception of the organization.
- Clear individual roles and responsibilities of the organization.

How ISO/IEC 27001 Helps for Management of Cybersecurity?

Common Cyber Attacks

- Malware attack (e.g., Ransomware)
- Password attack (e.g., Brutal force)
- Network attack (e.g., network intrusion)
- Application Attack (e.g., SQL injection)
- Phishing attack (e.g., Phishing email)

ISO/IEC 27001 Controls for Cyber Attacks

A.12.2 Protection from malware

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

A.12.2.1 Controls against malware

- Detection, prevention and recovery controls to protect against malware shall be implemented, combined with appropriate user awareness.

ISO/IEC 27001 Controls for Cyber Attacks

A.9.4.2 Secure log-on procedures

- Where required by the access control policy access to systems and applications shall be controlled by a secure log-on procedures.

A.9.4.3 Password management system

- Password management systems shall be interactive and shall ensure quality passwords.

ISO/IEC 27001 Controls for Cyber Attacks

A.13.1.1 Network controls

- Networks shall be managed and controlled to protect information in systems and applications.

A.13.1.2 Security of network services

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

ISO/IEC 27001 Controls for Cyber Attacks

A.14.1.1 Information security requirements analysis & specification

- The information security related requirements shall be across in the requirements for new information systems or enhancements to existing information systems.

A.14.2.1 Secure development policy

- Rules for the development of software and systems shall be established and applied to development within the organization.

ISO/IEC 27001 Controls for Cyber Attacks

A.12.6.1 Management of technical vulnerabilities

- Information about technical vulnerabilities of information systems being used shall be obtained in a timely fashions, the organization's exposure to such vulnerabilities evaluated and appropriate measures taken to address the associated risks.

A.12.4.1 Event logging

Event logs recording user activities, exceptions, faults, and information security events shall be produced, kept and regularly reviewed.

ISO/IEC 27001 Controls for Cyber Attacks

A.15.1.1 Information security policy for supplier relationships

- Information security requirements for mitigating the risks associated with supplier's access to the organization's assets shall be agreed with the supplier and documented.

A.16.1.1 Information security incident management responsibilities and procedures

- Management responsibilities and procedures shall be established to ensure a quick effective and orderly response to information security incidents.

ISO/IEC 27001 Controls for Cyber Attacks

A.17.1.2 Implementing information security continuity

- The organization shall establish, document, implement and maintain process, procedures and controls to ensure the required level of continuity for information security during as adverse situation.

A.7.2.2 Information Security awareness, education and training

- All employees of the organization and, where relevant contractors shall receive appropriate awareness, education and training and regular updates in organizational policies and procedures, as relevant for their job function.

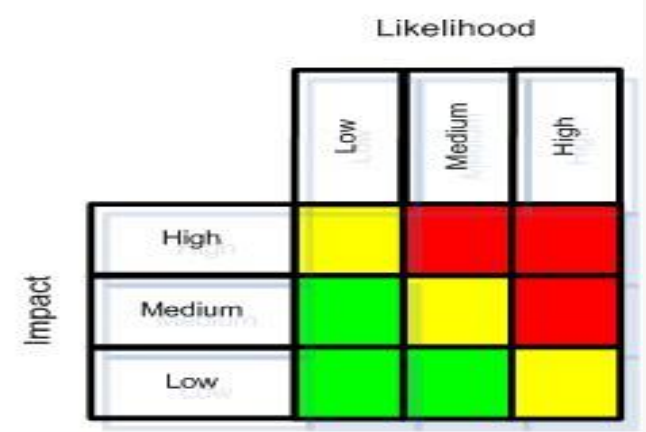
Information Security Risk Assessment

Define and apply information security risk assessment process

- Risk acceptance criteria
- Criteria for performing information security risk assessment
- Repeated Information security risk assessments produce consistent, valid and comparable results
- Identify the information security risks
  - Loss of CIA
- Analysis the information security risks
  - Consequence, Likelihood, Risk Level
- Evaluates the Information security risks
  - Compare with the risk criteria Risk acceptance criteria
  - Prioritize the risk treatment

Information Security Risk Assessment

- Define and apply Information security risk treatment process to
  - Select appropriate information security risk treatment option
  - Determine all necessary controls
  - Compare it with the Annex A and no necessary control is omitted
  - Organizations can design controls as required or identify them from any source



How ISO/IEC 27001 Helps for Management of Cybersecurity?

How ISO/IEC 27001 helps	Benefits
• It provides a framework for the management of information security risks, which ensures you take into account your legal, regulatory, business, and internal requirements. • It is based around continual improvement, and requires you to regularly review the effectiveness of your information security management system (ISMS) and take action to address new and emerging security risks.	• Supports compliance with relevant laws and regulations • Reduces likelihood of facing prosecution and fines • Can help you gain status as a preferred supplier • Get a competitive advantage

How ISO/IEC 27001 Helps for Management of Cybersecurity?

How ISO/IEC 27001 helps	Benefits
• Gives you a framework for identifying risks to information security and implementing appropriate management and technical controls. • Is risk based – delivering an appropriate and affordable level of information security. • It provides a way of ensuring that a common set of policies, procedures and controls are in place to manage risks to information security.	• Confidence in your information security arrangements • Improved internal organization • Better visibility of risks amongst interested stakeholders

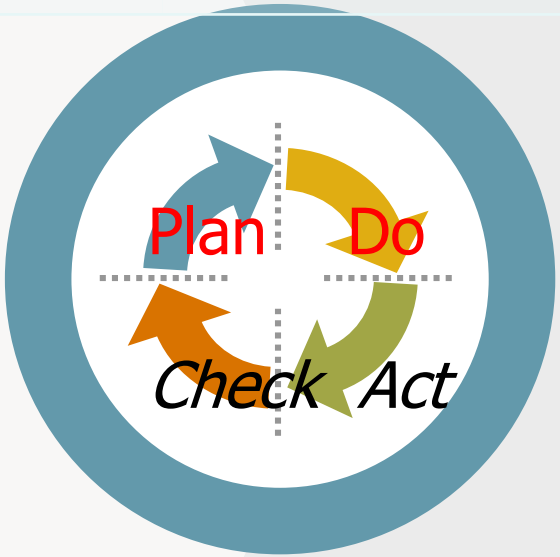
How ISO/IEC 27001 Helps for Management of Cybersecurity?

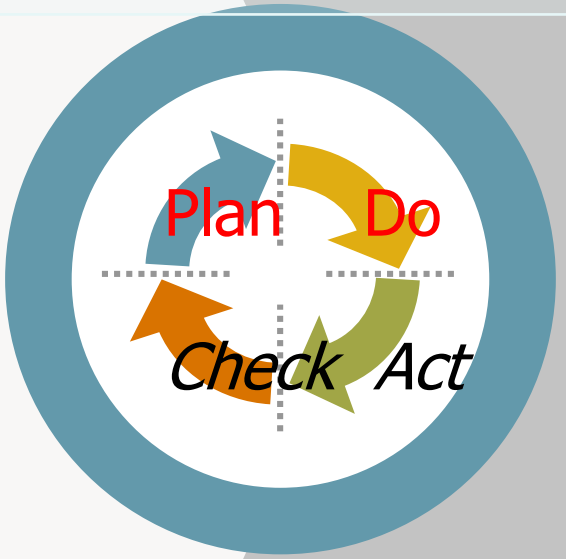
How ISO/IEC 27001 helps	Benefits
• It ensures senior management recognize information security as a priority and that there is clear tone from the top. • It requires you to implement a training and awareness programme throughout your organization. • It requires management to define ISMS roles and responsibilities and ensure individuals are competent to perform their roles.	• Improved information security awareness • Shows commitment to information security at all levels throughout your organization • Reduces staff-related security breaches

ISO/IEC 27001 Implementation and Certification

Implementing Information Security Management System (ISMS)

Stage	1	2	3
	Where we are	Implement & Operate	Manage & Improve



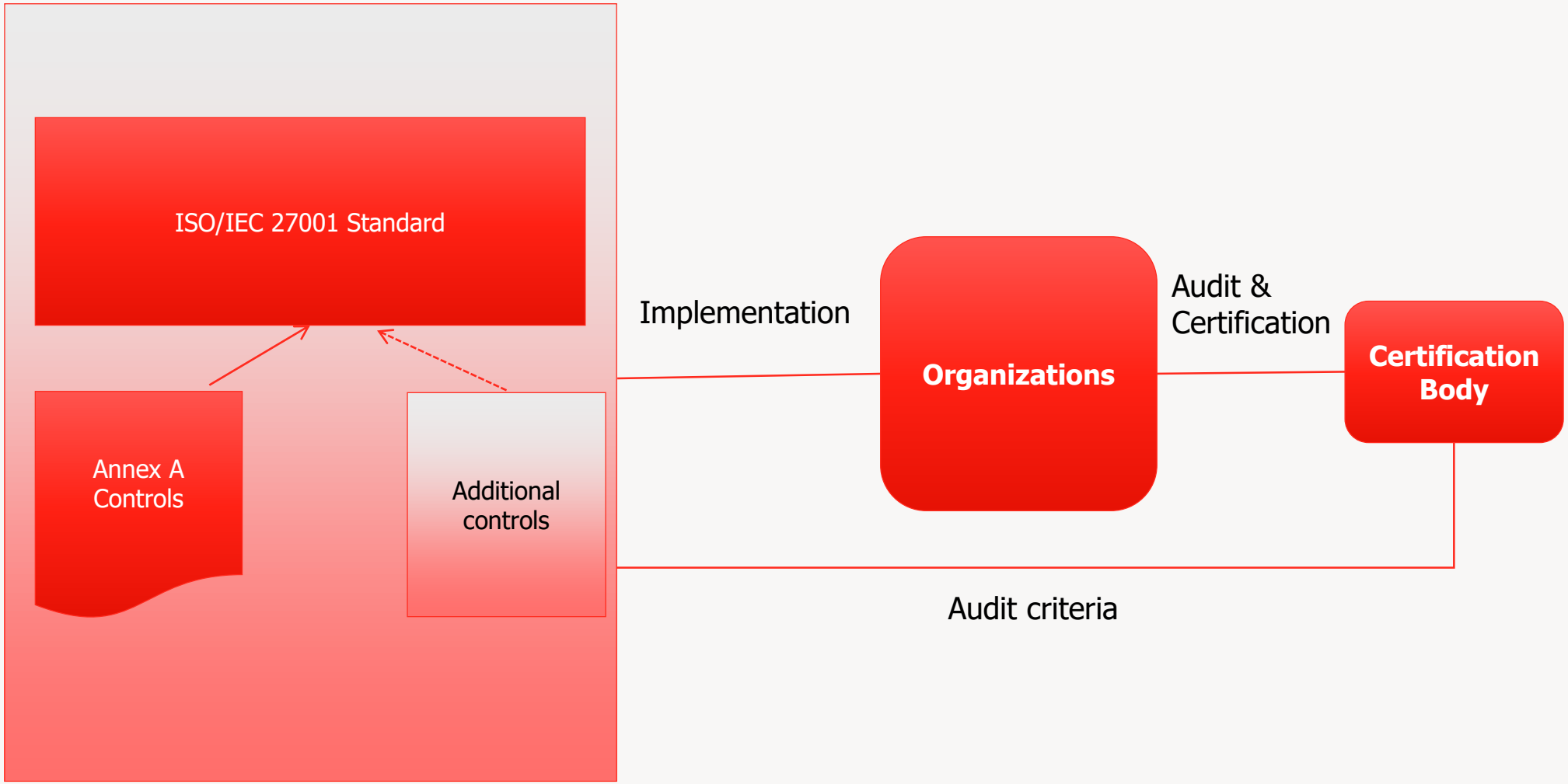


bsi.

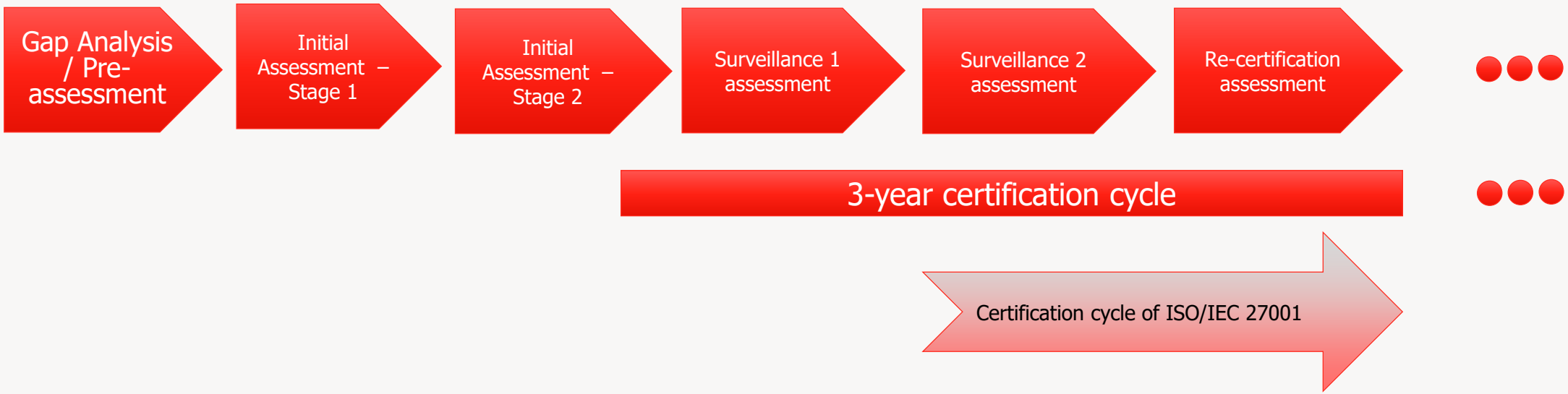
Implementing Information Security Management System (ISMS)

Stage	1	2	3
	Where we are	Implement & Operate	Manage & Improve
	Top Management buy-in	Implement & operate the plan	Monitor, measure, analyze & evaluation
	Understanding requirements including legal, standard, etc.	Project support	Audit and Management review
	Baseline review, Gap Analysis and provide resource	Project monitor	Continual improvement
	Approve and communication		

ISO/IEC 27001 Implementation and Certification



ISO/IEC 27001 Certification



bsi.

Contact us

T: +852 3149 3300
E: hk@bsigroup.com
W: bsigroup.com/en-HK

Get latest updates from

LinkedIn

Facebook

By Royal Charter

bsi.