

Hong Kong

Boosting Information Security: Insights on ISO/IEC 27001 Adoption and Best Practices

PECB REGIONAL WEBINARS

Agenda

1. Information Security Objectives
2. Confidentiality, Integrity & Availability (CIA)
3. Benefits Beyond Improved Information Security
4. Clauses of ISMS
5. Best Practice
6. Security Tips

Information Security Objectives

Protecting the interests of those relying on information, and the systems and communications that deliver the information, from harm resulting from failures of :

Confidentiality	Integrity	Availability
▪ Ensuring that information is accessible only to authorized individuals or entities. ▪ Preventing the disclosure of sensitive or private data to unauthorized parties.	▪ Maintaining the accuracy, completeness, and trustworthiness of information. ▪ Ensuring that data is not altered or tampered with by unauthorized individuals.	▪ Ensuring that authorized users have reliable and timely access to information and resources when needed. ▪ Protecting against disruptions or attacks that could make information or systems unavailable.



Confidentiality & Integrity

IT security incident detected

May 6, 2024 Like 0

The Fire Services Department said today that it has discovered a potential personal data leakage incident on one of its IT systems. It added that there is no evidence of data having been released.

The contractor responsible for the system was asked to immediately suspend it and had its access rights to the system withdrawn.

A preliminary investigation discovered that the incident occurred when the contractor handled a data migration procedure. The access rights to the data were found to have been altered without authorisation, posing a potential risk of data leakage.

The data includes the surnames and telephone numbers of approximately 480 members of the public who reported tree collapse incidents during Super Typhoon Saola on September 2, 2023.

It also includes personal information relating to about 5,000 department staff, including their names, telephone numbers, ranks, numbers, and postings. The incomplete identity card numbers of 960 of these individuals are also involved.

On discovering the incident the department liaised with the abovementioned contractor, requesting immediate suspension of the system and all of its contract jobs.

The department, together with the contractor, is conducting a comprehensive review and stepping up protective measures to prevent similar incidents. It has also reported the incident to Police, the Security Bureau, the Office of the Privacy Commissioner for Personal Data and the Office of the Government Chief Information Officer.

The Fire Services Department expressed its sincere apologies over the incident. It has notified the affected members of the public through SMS and phone calls. They should report any suspicious circumstances to Police as soon as possible,

For enquiries, call 2723 8787 or email hkfsdenq@hkfsd.gov.hk.

Source: https://www.news.gov.hk/eng/2024/05/20240506/20240506_200522_340.html?type=ticker

【本報訊】內地個人資料外洩問題嚴重，淘寶出事更非首次。流動應用程式「淘寶全球」2016年被揭會取得權限，讀取用戶電話號碼、通話狀態、通話雙方電話號碼等敏感資料。近日，內地網絡安全和信息化委員會辦公室（網信辦）亦公開點名批評105款應用程式過度索取及侵害用戶個人資料。

相關新聞：「爬蟲」襲淘寶　盜12億條用戶數據

百度地圖擅自下載改密碼

網信辦根據內地「網絡安全法」中的相關規定，檢查出逾百款違規應用程式。其中下載量以億計的抖音和快手，均被發現違反「必要原則」，收集與其提供服務無關的個人資料。此次被通報批評的亦包括一些工具程式，如QQ輸入法、百度地圖，同涉收集不必要個人資料，其中後者更會擅自為用戶下載文件、創建賬戶並修改密碼。

淘寶2016年曾被揭其「淘寶全球」要求「讀取手機狀態及識別碼」的權限，該權限允許存取用戶通話資料，包括通話雙方電話號碼等，程式更會將部份資料，傳回杭州阿里巴巴廣告有限公司。

官方程式亦不安全。名為「北京健康寶」的北京版「安心出行」去年被踢爆外洩大量用戶的照片、核酸檢測資訊、身份證號碼。藝人包括楊冪等的資料，不足數元就可買到。今年3月，公安部推出的「國家反詐中心App」，被投訴過度收集個人資料，程式要求的私隱權限多達29項，甚至可刪除資料及要上傳人臉。

Source: Apple Dairy 17 Jun 2021

Availability

Tech

Microsoft down: Online services hit by outage again days after global IT meltdown

Andrew Griffin • 17 hours ago • 1 Comment



(REUTERS)

Microsoft's online service have been hit by another outage, days after an IT meltdown that brought much of the world to a halt.

The company said it was investigating reports of user problems accessing its services, with some reporting being unable to access email and other functions.

An alert on the technology giant's service status website said it was looking into a "network infrastructure" issue that was impacting access to Microsoft services.

The incident comes less than two weeks after a major global IT outage knocked global infrastructure including transportation and healthcare services offline because of a flawed software update from cybersecurity firm CrowdStrike affected Microsoft devices.

On its service status website, Microsoft said: "We are investigating reports of issues connecting to Microsoft services globally.

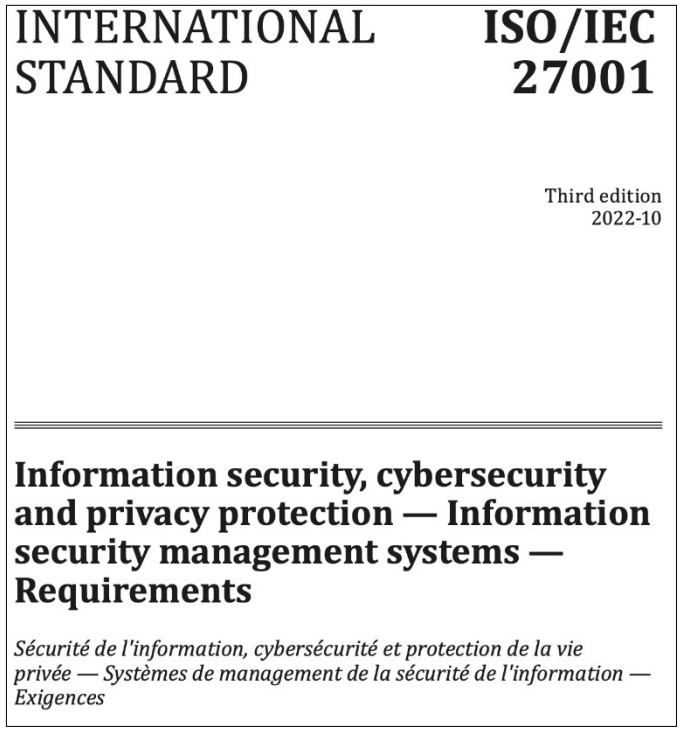
Source: https://www.independent.co.uk/tech/microsoft-down-not-working-online-email-services-b2588262.html

Benefits Beyond Improved Information Security

By implementing and adopting an Information Security Management System (ISMS), organizations can obtain benefits beyond just improved information security:

Improved Reputation and Trust	Operational Efficiency	Regulatory Compliance
Organizational Resilience	Employee Awareness and Culture	Competitive Advantage

Overview


INTERNATIONAL STANDARD

ISO/IEC 27001

Third edition
2022-10

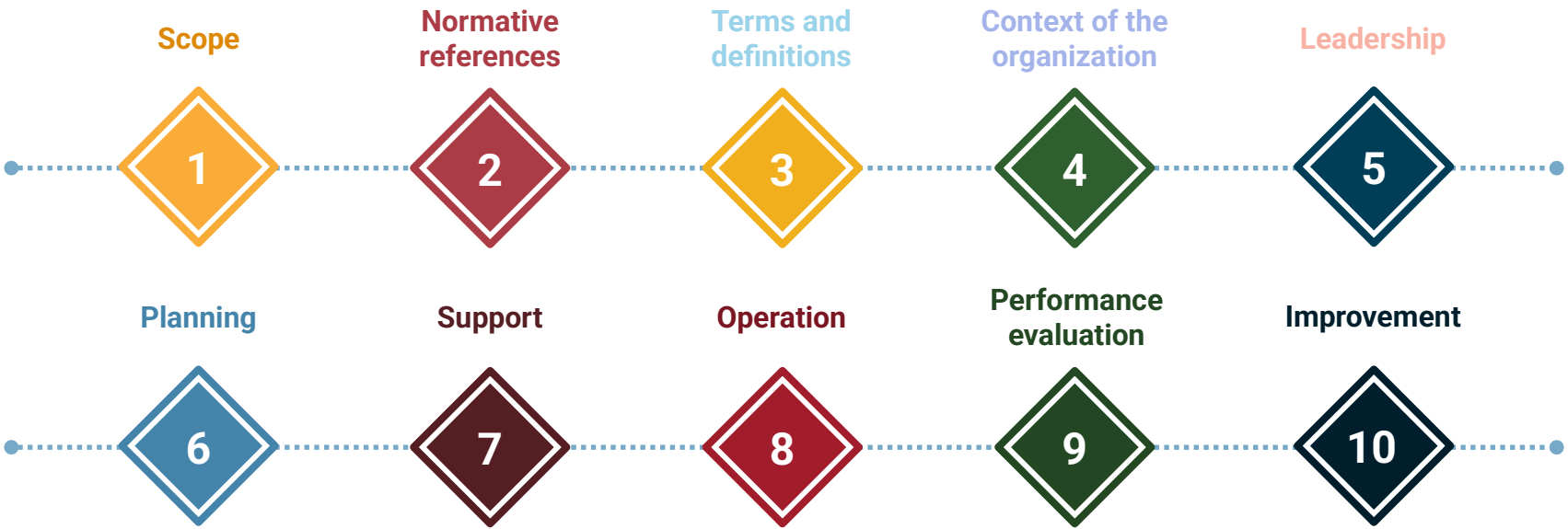
Information security, cybersecurity and privacy protection — Information security management systems — Requirements

Sécurité de l'information, cybersécurité et protection de la vie privée — Systèmes de management de la sécurité de l'information — Exigences

- ISO/IEC 27001:2022 was published on Q4 2022
- Follows the ISO standard High-level Structure (HLS)
- Contains 93 information security controls divided into 4 themes:
  - Organizational
  - People
  - Physical
  - Technological

***Previously contains 114 security controls in 14 areas

Clauses at a Glance



No exclusion for clauses 4 to 10



Understanding the Organization and its Context



Understanding the Organization and its Context



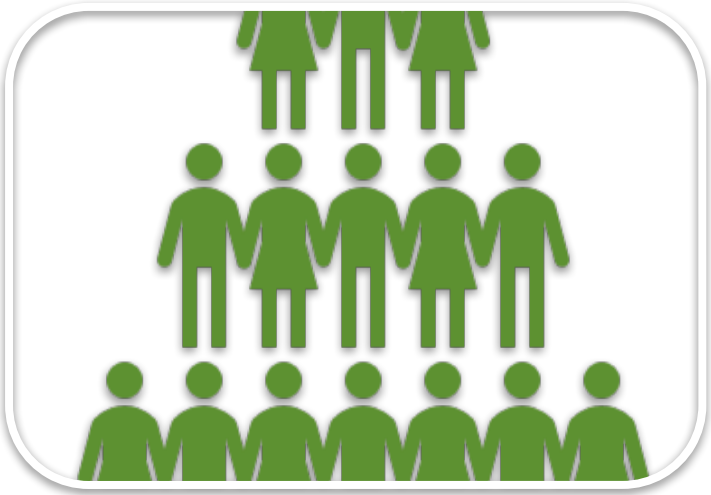
Understanding the Needs and Expectations of Interested Parties



Customer

- Examples:
- Fulfill customer SLA requirements.
- (T&RH – T : 22 ± 3°C , RH : 50 ± 20%)
- No power interruption
- Low probability of service interruption
- Maintain the ISO Certification (e.g., ISMS)

Understanding the Needs and Expectations of Interested Parties



Supplier

Examples:

- Fulfill PR and PO can be ready before starting work
- Issue or change communicated promptly
- Storeroom for storing PM tools and materials

Understanding the Needs and Expectations of Interested Parties



Legal and Regulatory Requirement

Examples:

- Cap. 486 Personal Data (Privacy) Ordinance
- Certificate of Fire Service Installations and Equipment – (FS251)
- Cap. 406 Electricity Ordinance (WR2)

Understanding the Needs and Expectations of Interested Parties



Contractual Obligations

- Examples:
- Fulfill Compliance with Policies (e.g., Information Classification and Labelling Policy) outlined in the ISMS framework.
- Data Security - Maintain the CIA of all information assets shared or accessed.
- Promptly report any security breaches or incidents

Climate Action Amendments to Management Systems Standards - Climate Change

4.1 Understanding the organization and its context.

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

Added: The organization shall determine whether climate change is a relevant issue.

4.2 Understanding the needs and expectations of interested parties.

The organization shall determine:

- the interested parties that are relevant to the XXX management system.
- the relevant requirements of these interested parties.
- which of these requirements will be addressed through the XXX management system.

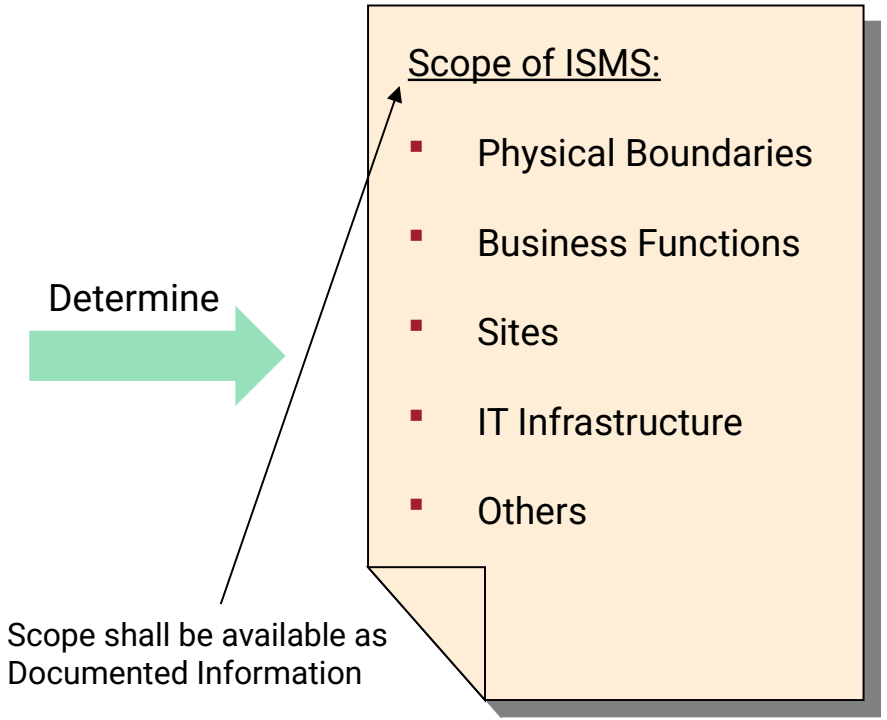
Added: NOTE: Relevant interested parties can have requirements related to climate change.

Source: https://iaf.nu/iaf_system/uploads/documents/Joint_ISO-IAF_Communique_re_Climate_Change_Amds_to_ISO_MSS_Feb_2024_Final.pdf

Determining the Scope of ISMS

Consider :

- External and Internal issues
- Requirements from interested parties
- Activities performed by the organization and by other external parties



Leadership and Commitment

Top Management shall :

01 Ensure that information security policy and objectives are established

02 Ensure that required resources are available

03 Ensure the integration of ISMS requirements into organization's processes

04 Communicate the importance of an effective information security management

Leadership and Commitment

Top Management shall :

05 Ensure ISMS can achieve its Intended outcome

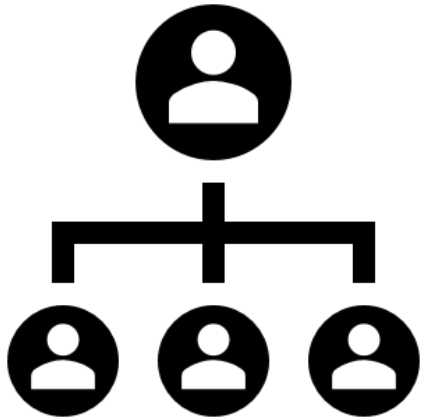
06 Promote continual improvement

07 Direct and support staff to contribute to the effectiveness of the ISMS

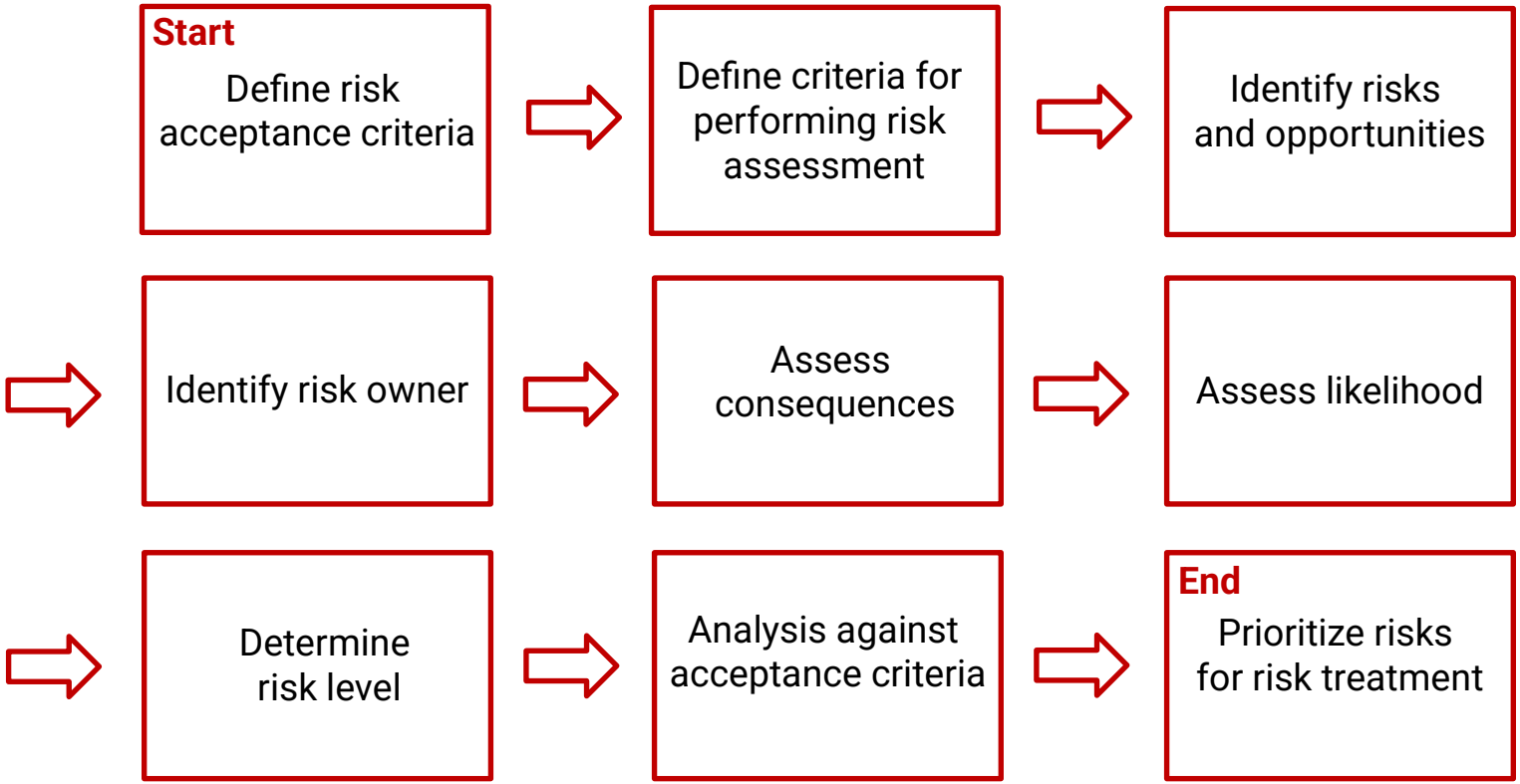
08 Support relevant management roles to demonstrate their leadership

Organization Roles, Responsibilities and Authorities

- Top management to assign and communicate responsibilities and authorities for information security roles
- Assign responsibility and authority for ensuring the conformance of the ISMS to ISO/IEC 27001:2022
- Assign responsibility and authority for reporting the performance of the ISMS to top management



Information Security Risk Assessment



Example of Risk Criteria

Classification	Description
High Impact	Most significant: Major loss and seriously damaging the organization, or serious long-term damage/disruption like denial of service or unauthorized access to system.
Medium Impact	Significant: Medium loss which can be detrimental to the organization, serious short-term, or limited long-term damage/disruption like intruder may gather system critical information to gain unauthorized access or launch further attacks.
Low Impact	Least significant: Low loss which would cause little or no damaging to the organization, limited and short-term damage/disruption like intruder may gain non-critical information for processing.

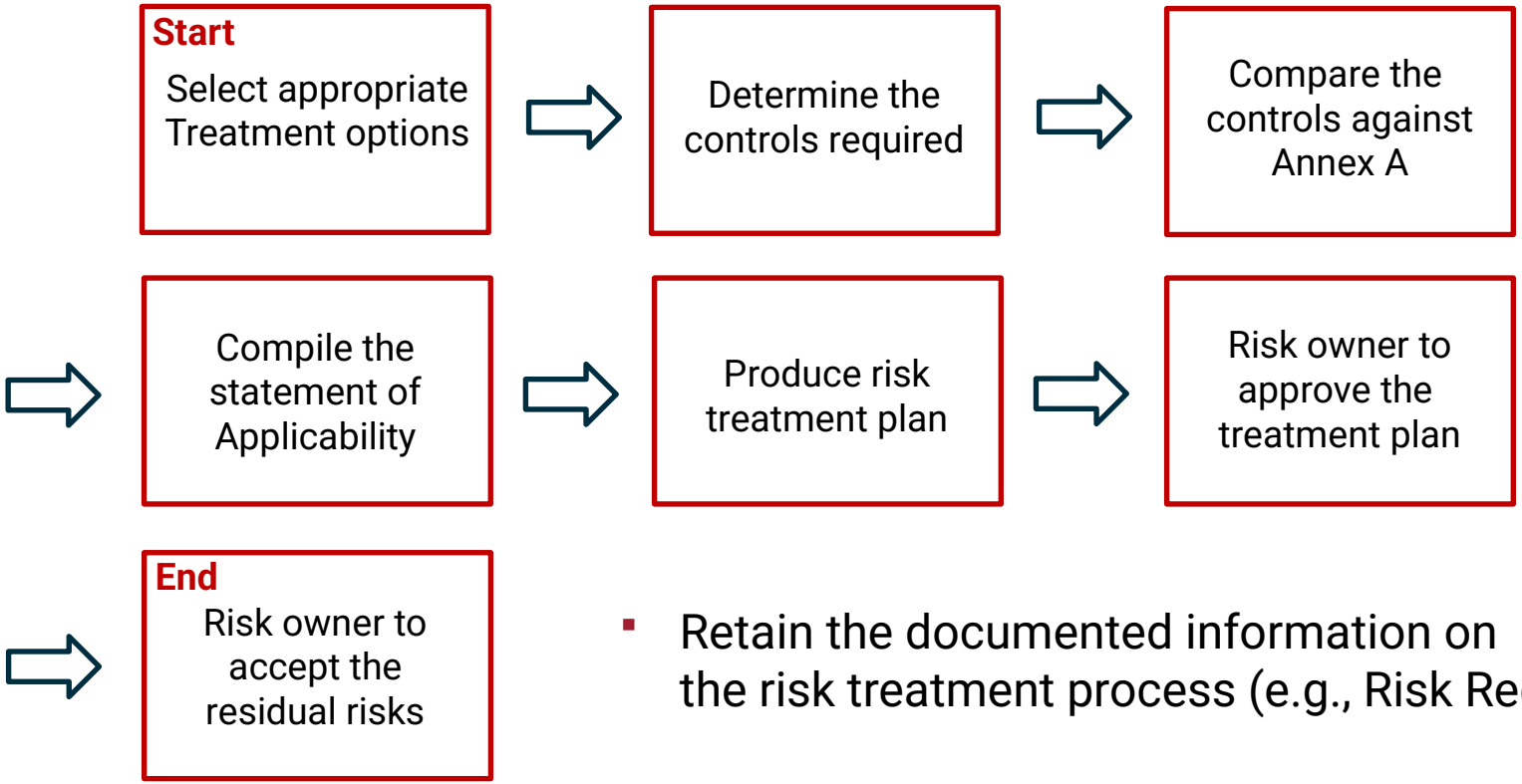
Classification	Description
High Likelihood	Expected to occur in most circumstances.
Medium Likelihood	Should occur occasionally.
Low Likelihood	Could occur at specific time or in exceptional circumstances.

Example of Risk Criteria

Risk Level		Impact		
		High (3)	***Medium (2)***	***Low (1)***
Likelihood	***High (3)***	High (9)	Medium (6)	Low (3)
	Medium (2)	Medium (6)	Medium (4)	Low (2)
	Low (1)	Low (3)	Low (2)	AOI / Informative* (1)

(*Area of Improvement (AOI) / Informative - This is not a high-risk item, and no significant damage or loss would be incurred. However, allocating resources to address such issues could result in improved work and more effective security protection.)

Information Security Risk Treatment



- Retain the documented information on the risk treatment process (e.g., Risk Register)

Example of Risk Register

Asset Group	Asset Details	Threat	Vulnerability
Organization Reputation	Organization Reputation	Loss of Organization Reputation	Inadequate and/or Ineffective Security Mechanism
		Non-Compliance to Contractual, Legal and Regulatory Requirements	Unaware of Contractual, Legal and Regulatory Requirements

Type (CIA)	Risk Owner	Likelihood	Implact	Risk Level	Adopted ISO/IEC 27001:2022 Controls (Treatments)	Residual Risk	Status
C/I/A	Managing Director	3	3	9	A.5.1, A.5.2, A.5.3, A.5.5, A.5.6, A.5.8, A.5.35, A.5.36, A.8.34	6	Accepted (continuous monitoring)
A	Managing Director	3	3	9	A.5.1, A.5.31, A.5.32, A.5.33, A.5.34	6	Accepted (continuous monitoring)

Information Security Objectives and Planning to achieve them

- Establish information security objectives:
  - At relevant functions and levels
  - Consistent with information security policy
  - Measurable (if practicable)
  - Consider information security requirements and results from risk assessment and risk treatment
  - Communicate to relevant parties
  - Update when necessary
  - Retain documented information on the objectives

Examples of Objectives

Objective	Actions	Resources	Responsible
No. of Virus Infected In All Desktops/ Laptops and Servers	- Conducting refreshment training on ISMS regularly; - Ensuring the anti-virus definition file is up-to-date; - Perform regular scanning.	- Manpower - Scanning tools	Head of Operations
No more than 28 hours of downtime due to power failure	- Develop and implement a BCP to respond to the power outage incident to minimize the downtime	- Manpower - Other resources stated in the BCP	Head of Operations
Conduct information security awareness training sessions for all in-scope / new joined employees	- Conducting information security awareness training regularly or as needed basis.	- Manpower - Training Materials	Head of Human Resources

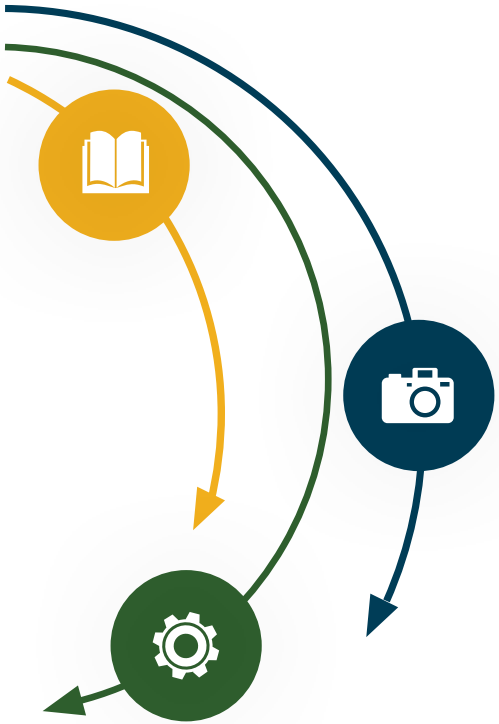
Examples of Objectives

Objective	Responsible	Counting Rules	Review Fequency
No. of Virus Infected In All Desktops/ Laptops and Servers	Head of Operations	No. of virus infected and detected from the anti-virus tool	Annually
No more than 28 hours of downtime due to power failure	Head of Operations	No. of total downtime	Annually
Conduct information security awareness training sessions for all in-scope / new joined employees	Head of Human Resources	All in-scope / new joined employees attended the information security awareness training sessions	Annually

Resources – Tangible & Intangible

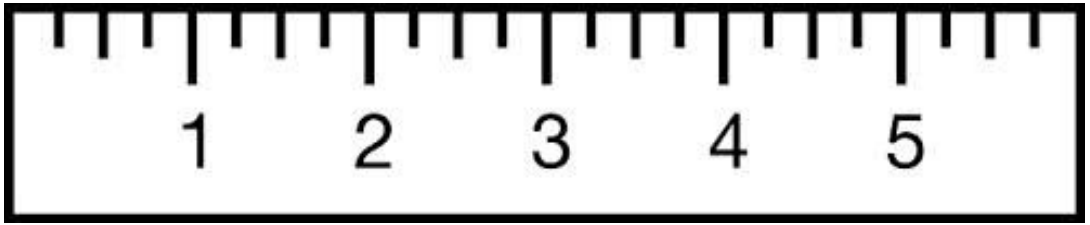
Financial Resources	Hardware and Software	Physical Infrastructure
▪ Budgets for security technologies, tools, and services	▪ Security devices (firewalls, intrusion detection/prevention systems, VPNs) ▪ Endpoint protection (antivirus, anti-malware, encryption)	▪ Access control mechanisms (locks, biometrics, CCTV) ▪ Redundant power and cooling systems ▪ Secure network infrastructure (routers, switches, cables)
Human Resources	**Policies and Procedures**	**Knowledge and Expertise**
▪ Information security professionals (managers, analysts, engineers) ▪ Security awareness and training personnel	▪ Information security policies and standards ▪ Incident response and business continuity plans	▪ Security threat intelligence and vulnerability information ▪ Technical skills and expertise in security technologies

Monitoring, Measurement, Analysis and Evaluation



Information Security Performance

Effectiveness of ISMS



- What needs to be monitored and measured ?
- What are the methods ?
- When to perform the monitoring and measurement ?
- Who is responsible for the monitoring and measurement ?
- When to analyze an evaluate the results ?
- Who is responsible for the analysis and evaluation of the results ?

Internal Audit

- Organization shall conduct Internal Audit at planned interval to see if the ISMS :

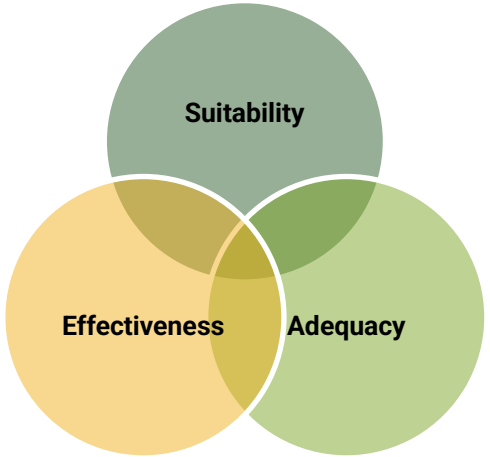


Management Review

- Held at planned intervals
(e.g., Suitability? Adequacy? Effectiveness?)

Review Input

- Status of actions from previous management review
- Changes in external and internal issues
- Changes in needs and expectations of interested parties
- Feedback from interested parties
- Result of risk assessment and status of risk treatment
- Information security performance
  - Nonconformities and corrective actions
  - Result of monitoring and measurement
  - Result of audits
  - Achievement of information security objectives
- Opportunities for improvement



Review Output

- Decisions on continual improvement
- Changes to the ISMS
- Retain documented information on the results of management review

Nonconformity and Corrective Action



Nonconformities found from the result of performance evaluation

Start
Control and Correct

Deal with Consequences

Review

Identify root cause

Identify similar issues

Implement correction and corrective action

Review effectiveness of action

End
Make changes to ISMS

ISO/IEC 27001:2022 – 93 Controls

Annex A

(normative)

Information security controls reference

Best Practices

- Apart from ISMS, there are several other related best practices that organizations can consider beyond the ISMS framework.

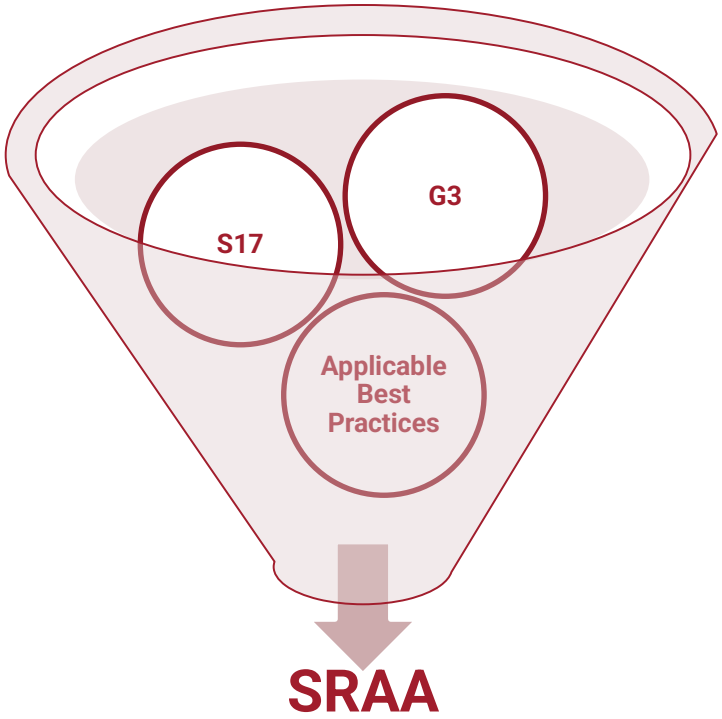
- Below are some examples:
  - Cybersecurity Frameworks
  - Risk Management Frameworks
  - Business Continuity and Disaster Recovery
  - Privacy and Data Protection
  - Industry-Specific Standards and Regulations



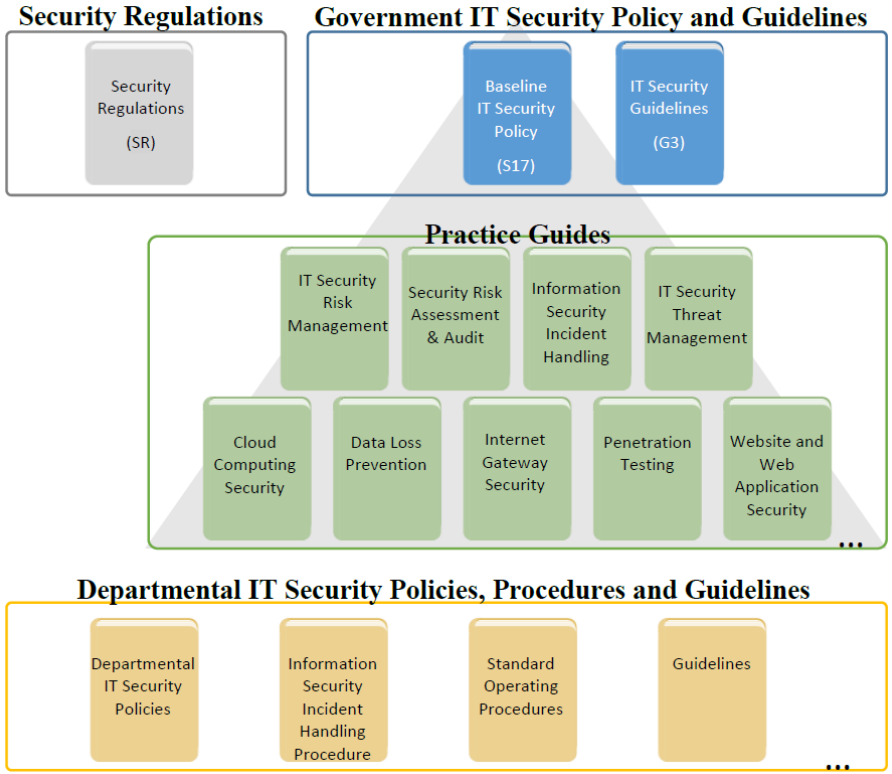


Security Risk Assessment & Audit

In Hong Kong, the primary reason to conduct a Security Risk Assessment and Audit (SRAA) is to identify and mitigate potential security risks and vulnerabilities within an organization's information systems and infrastructure.



Security Risk Assessment & Audit

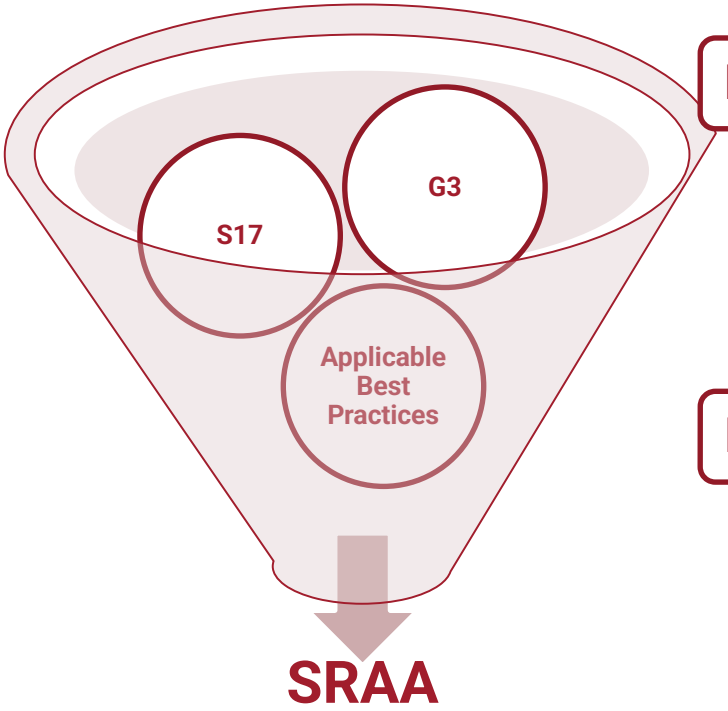


Source: Baseline IT Security Policy [S17], Version 8.1, July 2024

The Hong Kong Government has promulgated a set of security regulations and government IT security policy and guidelines to assist B/Ds in formulating and implementing their IT security policies and control measures to safeguard government information security.

These security documents are indispensable references for information security management.

Security Risk Assessment & Audit



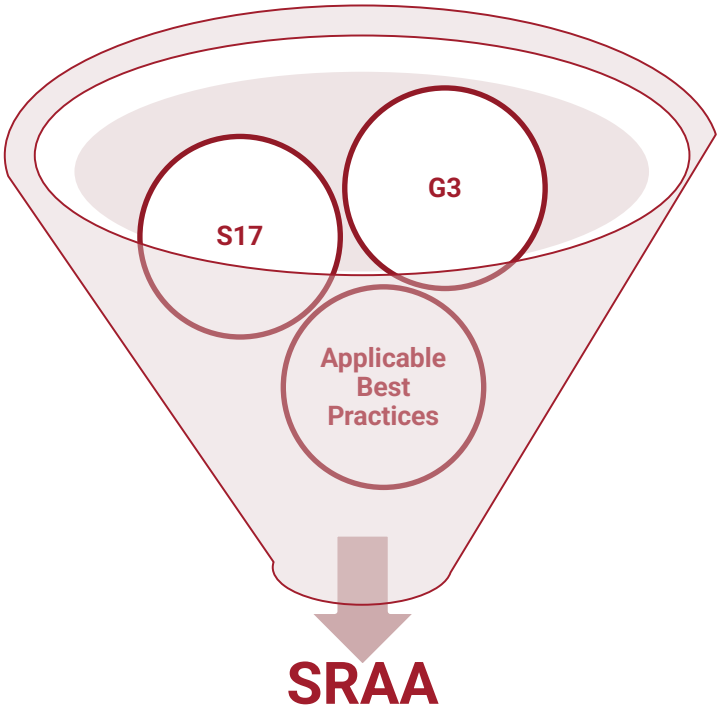
Baseline IT Security Policy (S17)

- A top-level directive statement that sets the minimum standards of a security specification for all B/Ds. It states what aspects are of paramount importance to a B/D.
- Thus, the Baseline IT Security Policy can be treated as basic rules which shall be observed as mandatory while there can still be other desirable measures to enhance security.

IT Security Guidelines (G3)

- Elaborates on the policy requirements and sets the implementation standard on the security requirements specified in the Baseline IT Security Policy.
- B/Ds shall comply with the IT Security Guidelines for effective implementation of the security requirements.

Security Risk Assessment & Audit



Applicable Best Practices / Practice Guide

- Baseline IT Security Policy [S17]
- IT Security Guidelines [G3]
- Practice Guide for Security Risk Assessment & Audit [ISPG-SM01]
- Practice Guide for Information Security Incident Handling [ISPG-SM02]
- Practice Guide for Mobile Security [ISPG-SM03]
- Practice Guide for Cloud Computing Security [ISPG-SM04]

Baseline IT Security Policy (S17)

- Adopts and adapts the security areas and controls specified in the ISO/IEC 27001: 2022 and ISO/IEC 27002: 2022
- Addresses the mandatory security considerations in the following 14 areas:



Some Security Tips

- Keep updating your software and operating system to ensure they are operating in latest version.
- Enable and use the anti-virus software to detect and remove threats.
- Adopt and follow strong password policy.
- Do not open email attachments which are sent from unknown senders.
- Do not click on links in emails from unknown senders or unfamiliar websites.
- Avoid using unsecure Wi-Fi networks in public places.
- Regularly provide security awareness training to employees on topics such as phishing, social engineering, password management, and data protection.

Some Security Tips

- Implement strong authentication mechanisms, such as multi-factor authentication, to control access to critical systems and data
- Regularly review and update user access privileges based on the principle of least privilege.
- Develop and regularly test an incident response plan to ensure effective handling of security incidents.
- Implement firewalls, intrusion detection and prevention systems, and web content filtering to monitor and control network traffic.

Q&A Session



Contact

- Company Website: https://www.evolve-online.com/contact-us
- Phone: +852 6131 6008
- Company Email: aidanc@evolve-asia.com
- Personal Email: aidanonlylivesonce@gmail.com
- LinkedIn: https://www.linkedin.com/in/aidan-chung-b7a8aa199/

PECB REGIONAL WEBINARS

- events@pecb.com