Pre-Tutorial Instruction

Good afternoon everyone, hope you did well for you midterms.
For the discussion of this tutorial, here are just some simple steps for you to participate

1. Have your pollev ready. Visit the link: **pollev.com/weichineyo617**
2. Use a nickname you are comfortable with and you will see a survey on midterm currently available to get you started.

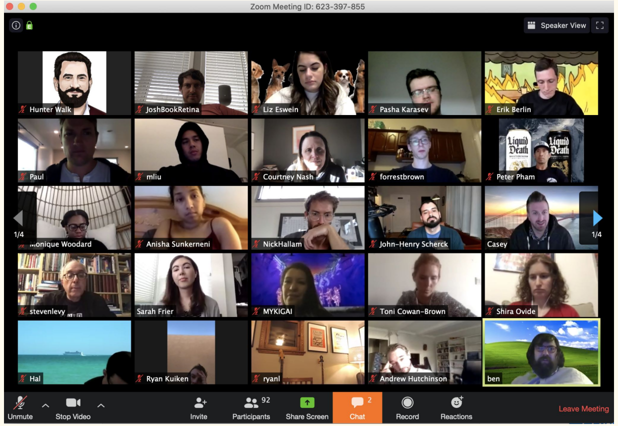
Tutorial 5: InfoSec Program at Zoom Video Communication

Group 2

Chan Jian Hao, Eyo Wei Chin, Ong De Zhi, Ong Xin Bin

Zoom University

- Zoom background



Federal Trade Commission

- **Federal Trade Commission** is an independent agency of the United States government whose principal mission is the enforcement of civil law that prevent fraud, deception and unfair business practices
- **Case background**
  - With reason to believe that Zoom has violated the Federal Trade Commission Act
  - The Commission issues its Complaint, with its findings, and issues the FTC final Order
- Refusal to comply with a court enforcement order is subject to penalties for contempt of court.

Warm-Up Question 1

Considering the misleading and misrepresented information Zoom claimed on its offered videoconferencing services, the FTC commission had reason to believe that Zoom has violated the Federal Trade Commission Act. In Singapore, it would be more likely to be charged under what law?

a) PDPA
b) Cybersecurity Act
c) Consumer Protection Act
d) Competition Act

Warm-Up Question 1

Considering the misleading and misrepresented information Zoom claimed on its offered videoconferencing services, the FTC commission had reason to believe that Zoom has violated the Federal Trade Commission Act. In Singapore, it would be more likely to be charged under what law?

a) PDPA
b) Cybersecurity Act
c) Consumer Protection Act
d) Competition Act

Warm-Up Question 1

Consumer Protection Act

- The Consumer Protection (Fair Trading) Act (Cap. 52A) or CPFTA was enacted to protect consumers against unfair practices and to give consumers additional rights in respect of goods that do not conform to contract, and for matters connected therewith.
- https://www.case.org.sg/consumer_guides_cpfta.aspx

Warm-Up Question 2

Based on the Final Order from the FTC, what information is not considered as "Covered Information"?

a) Screen name
b) Chat transcripts
c) Processor serial number
d) None of the above.

Warm-Up Question 2

Based on the Final Order from the FTC, what information is not considered as “Covered Information”?

a) Screen name
b) Chat transcripts
c) Processor serial number
d) **None of the above.**

Warm-Up Question 2

Covered Information:

(c) an email address or other online contact information, such as an instant messaging user identifier or **a screen name**;

(i) recorded or livestream video or audio content, **chat transcripts**, documents, or any other multimedia content shared by Users during a Meeting

(j) a persistent identifier, such as a customer number held in a "cookie," a mobile device ID, or **processor serial number**;

Warm-Up Question 3

In the FTC’s Final Order, the design and implementation of security measures (i.e., policies, procedures, and technical) follows what kind of approach?

a) User based
b) Cost based
c) Risk based
d) Volume based

Warm-Up Question 3

- **User based**

  The user-based approach **focuses exclusively on the customer in the determination of quality**. The strength of this approach is that it allows the customer the say in defining quality.

- **Cost based**

  The cost-based approach is a valuation method used by organizations to **consider all expenses associated** with a particular activity when determining the appropriateness of executing said activity.

Warm-Up Question 3

- **Risk based**
  The Risk-Based approach is a systematic method that **identifies, evaluates, and prioritizes threats facing the organization**.

- **Volume based**
  Volume-based alerting creates a baseline what is normal and expected behavior for various functions and then look for anomalies outside of that norm.
  - Malware detection
  - Data exfiltration

Warm-Up Question 3

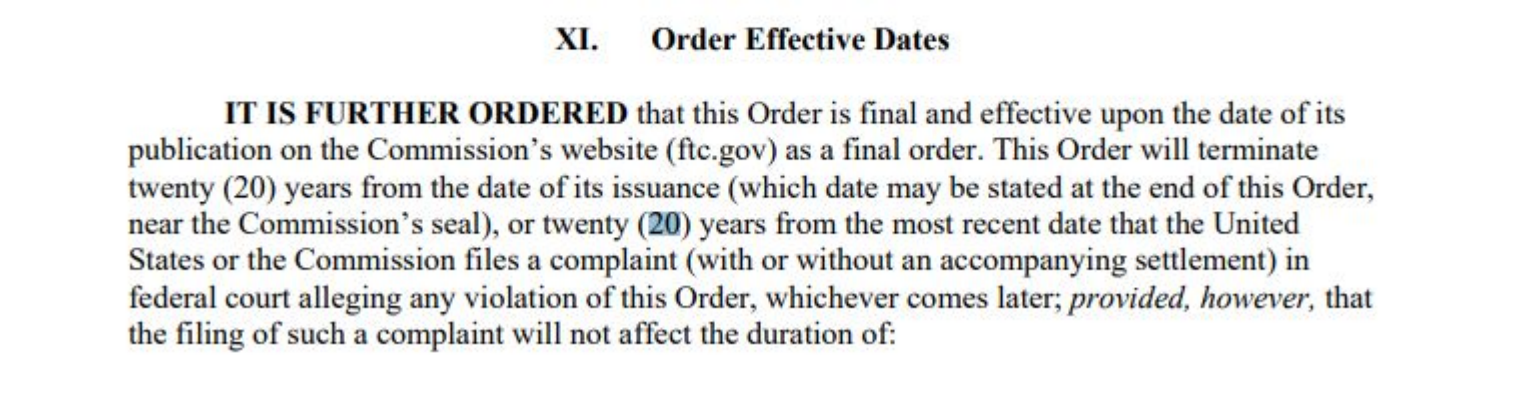
In the FTC's Final Order, the design and implementation of security measures (i.e., policies, procedures, and technical) follows what kind of approach?

a) User based
b) Cost based
c) Risk based
d) Volume based

Design, implement, maintain, and document safeguards that control for the **internal and external risks** Respondent identifies to the security, confidentiality, and integrity of Covered Information...

Bonus Discussion

Is this order permanent till the end of time? Or will it last a fixed amount of years? (Give your answers in years)



XI. Order Effective Dates

IT IS FURTHER ORDERED that this Order is final and effective upon the date of its publication on the Commission's website (ftc.gov) as a final order. This Order will terminate twenty (20) years from the date of its issuance (which date may be stated at the end of this Order, near the Commission's seal), or twenty (20) years from the most recent date that the United States or the Commission files a complaint (with or without an accompanying settlement) in federal court alleging any violation of this Order, whichever comes later; *provided, however,* that the filing of such a complaint will not affect the duration of:

Deceptive & Unfair Practices by Zoom

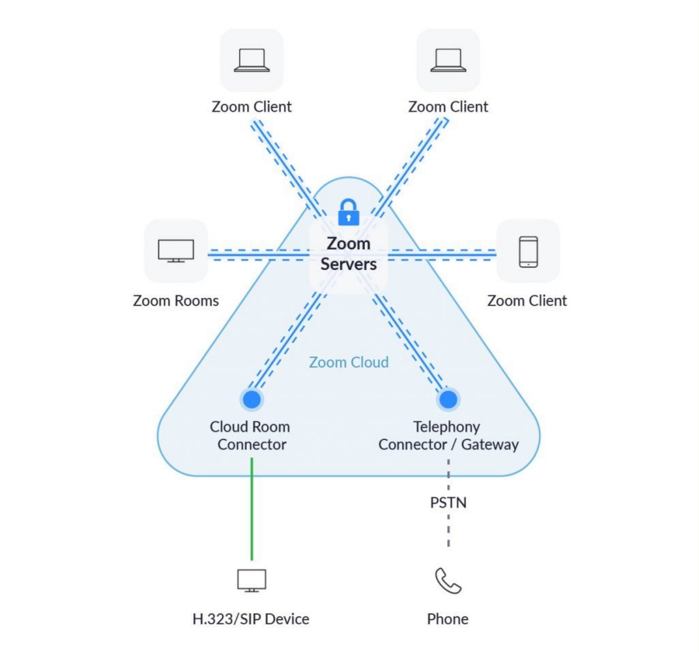
Our Answer

- Claimed to offer “**end-to-end, 256-bit encryption**”.
- Claimed that all recorded meetings kept on cloud are **encrypted immediately**.
- **Secretly** installed ZoomOpener on Mac users **without consent**.
    - **Hidden** from release notes → **Violates** FTC Act.
- **Increased** the user’s risk of remote video surveillance by strangers **without offset measures** taken.
- ZoomOpener remained even after Zoom’s uninstallation, and may be used to reinstall itself.

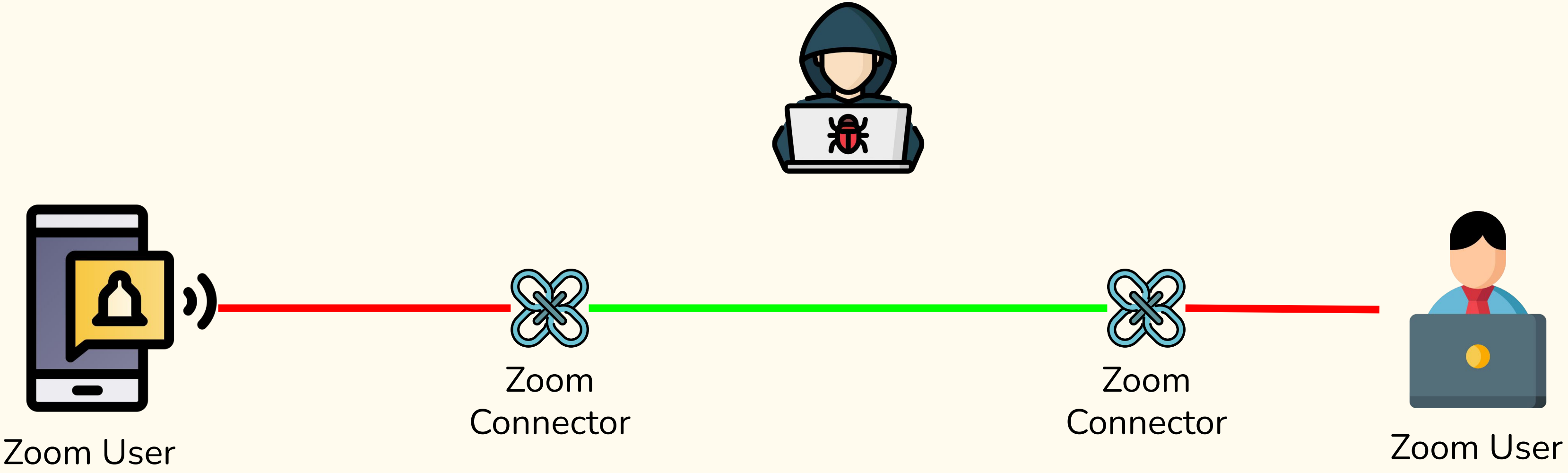
Bonus Discussion

However, Zoom clarified about E2E encryption:

- Connection between clients are encrypted
- **Connector** technology to support diverse clients (e.g. phones, skype)
  - Encrypted once connection with **connector** is established
- Does this mean Zoom is E2E encrypted?

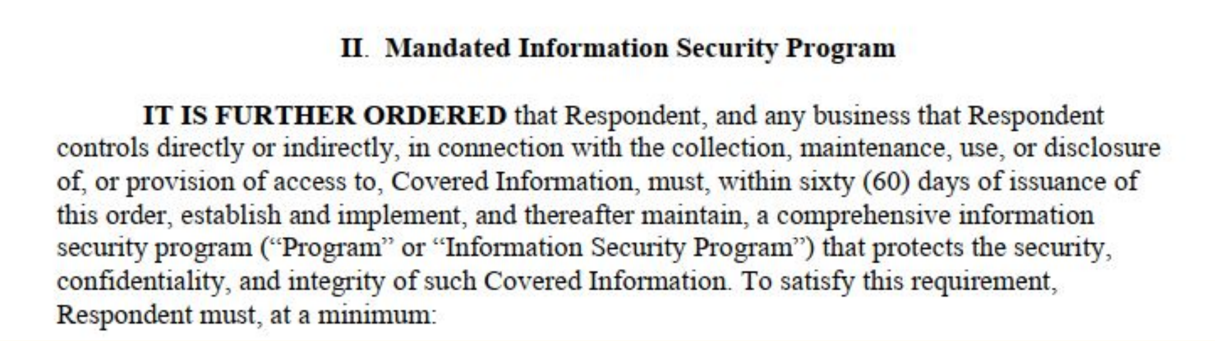


Bonus Discussion



Mandated security program

Where is it located in FTC's Final Order on Zoom?



II. Mandated Information Security Program

IT IS FURTHER ORDERED that Respondent, and any business that Respondent controls directly or indirectly, in connection with the collection, maintenance, use, or disclosure of, or provision of access to, Covered Information, must, within sixty (60) days of issuance of this order, establish and implement, and thereafter maintain, a comprehensive information security program ("Program" or "Information Security Program") that protects the security, confidentiality, and integrity of such Covered Information. To satisfy this requirement, Respondent must, at a minimum:

Any similarities to Singapore's regulations? MAS TRM Guidelines?

MAS TRM Guidelines

- Requirement to have policies, standards to manage IT risks.
- Management of third party services & vendor
- Cryptography requirements, ... many more

Poll Everywhere

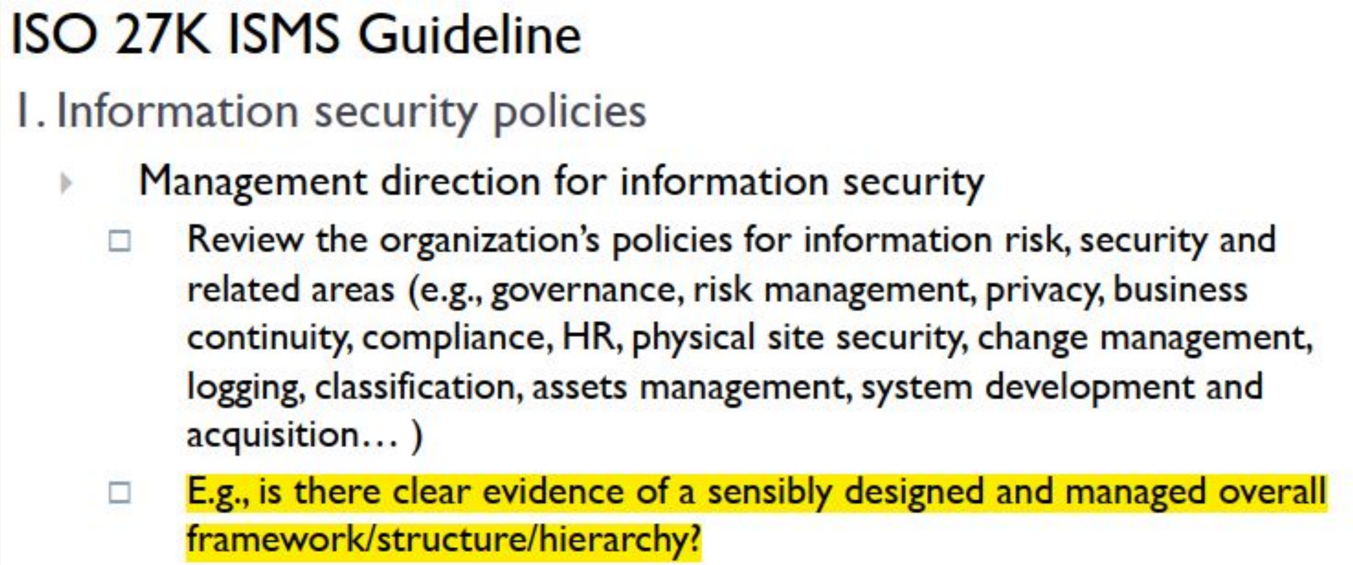
A. Document in writing the content, implementation, and maintenance of the Program

A.5 Information Security Policies [Answer]

A.8 Asset Management

A.18 Compliance

A.13 Communication Security



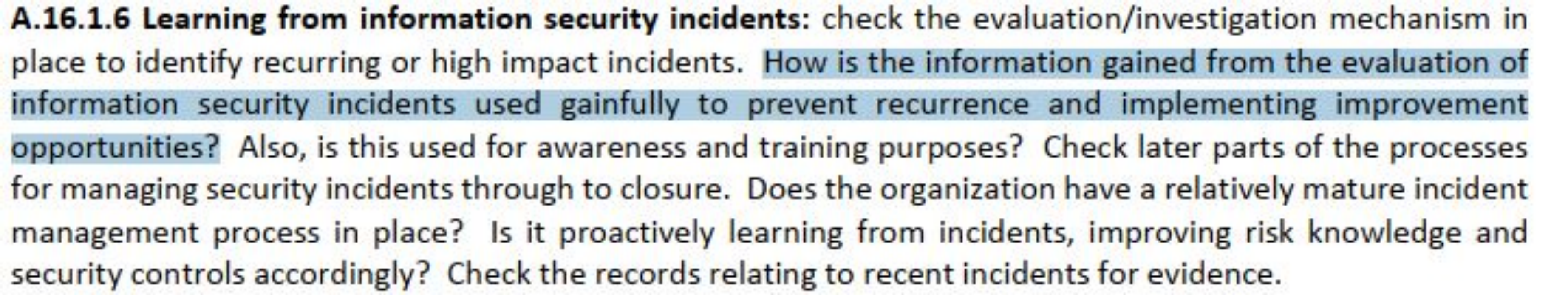
ISO 27K ISMS Guideline

1. Information security policies

- Management direction for information security
  - □ Review the organization’s policies for information risk, security and related areas (e.g., governance, risk management, privacy, business continuity, compliance, HR, physical site security, change management, logging, classification, assets management, system development and acquisition…)
  - □ E.g., is there clear evidence of a sensibly designed and managed overall framework/structure/hierarchy?

B. In the event of a **covered incident**, provide material evaluation and updates to respondent’s board

A.5 Information Security Policies
A.11 Communication Security
A.17 Business Continuity Management
A.16 Information Security Incident Management [Answer]



A.16.1.6 Learning from information security incidents: check the evaluation/investigation mechanism in place to identify recurring or high impact incidents. How is the information gained from the evaluation of information security incidents used gainfully to prevent recurrence and implementing improvement opportunities? Also, is this used for awareness and training purposes? Check later parts of the processes for managing security incidents through to closure. Does the organization have a relatively mature incident management process in place? Is it proactively learning from incidents, improving risk knowledge and security controls accordingly? Check the records relating to recent incidents for evidence.

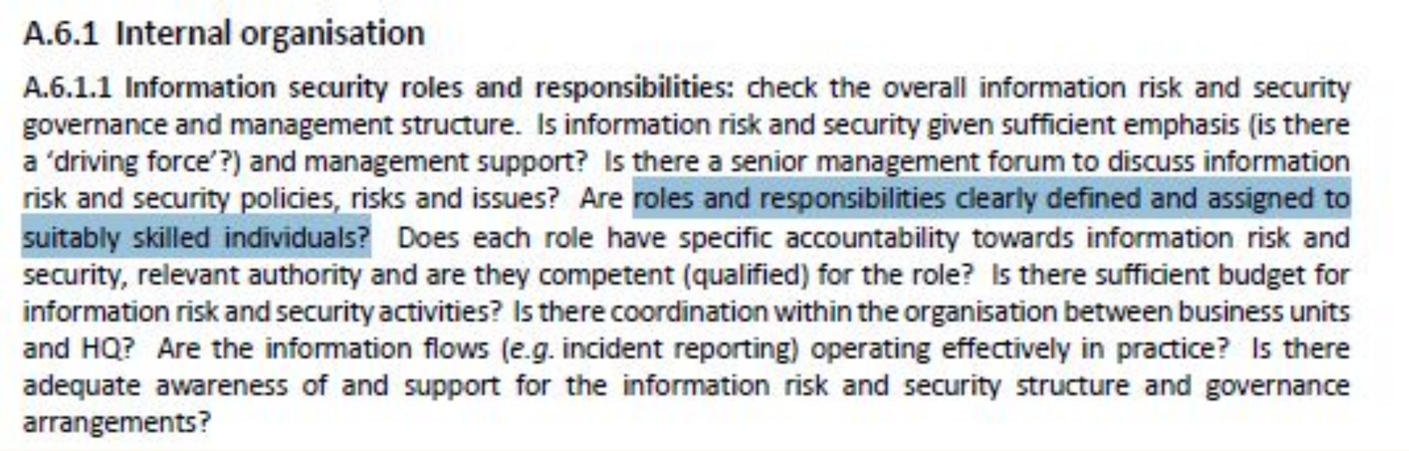
C. Designate a qualified employee or employees to coordinate and be responsible for the Program

A.6 Organizations of Information security [Answer]

A.8 Asset Management

A.18 Compliance

A.13 Communication Security

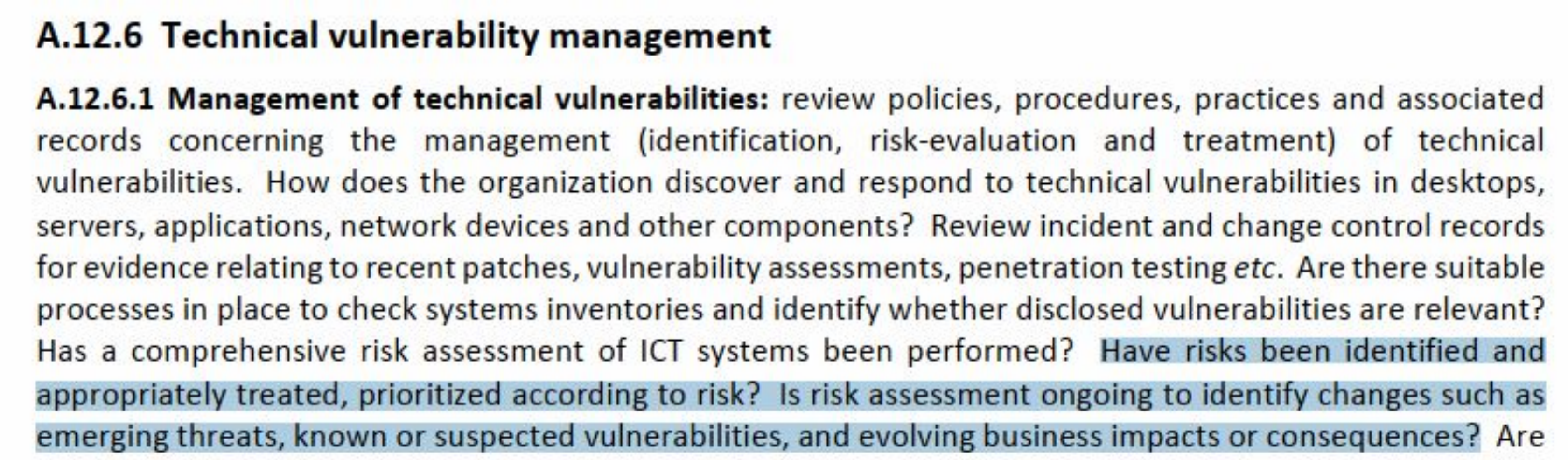


A.6.1 Internal organisation

A.6.1.1 Information security roles and responsibilities: check the overall information risk and security governance and management structure. Is information risk and security given sufficient emphasis (is there a 'driving force'?) and management support? Is there a senior management forum to discuss information risk and security policies, risks and issues? Are roles and responsibilities clearly defined and assigned to suitably skilled individuals? Does each role have specific accountability towards information risk and security, relevant authority and are they competent (qualified) for the role? Is there sufficient budget for information risk and security activities? Is there coordination within the organisation between business units and HQ? Are the information flows (*e.g.* incident reporting) operating effectively in practice? Is there adequate awareness of and support for the information risk and security structure and governance arrangements?

D. Assess and document, internal and external risks to the security, confidentiality, or integrity of Covered Information

A.5 Information Security Policies
A.11 Communication Security
A.17 Business Continuity Management
A.12 Operation Security [Answer]

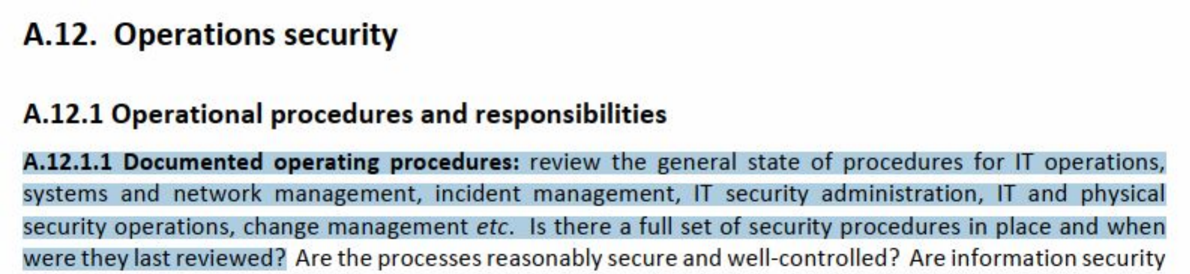


A.12.6 Technical vulnerability management

A.12.6.1 Management of technical vulnerabilities: review policies, procedures, practices and associated records concerning the management (identification, risk-evaluation and treatment) of technical vulnerabilities. How does the organization discover and respond to technical vulnerabilities in desktops, servers, applications, network devices and other components? Review incident and change control records for evidence relating to recent patches, vulnerability assessments, penetration testing *etc*. Are there suitable processes in place to check systems inventories and identify whether disclosed vulnerabilities are relevant? Has a comprehensive risk assessment of ICT systems been performed? Have risks been identified and appropriately treated, prioritized according to risk? Is risk assessment ongoing to identify changes such as emerging threats, known or suspected vulnerabilities, and evolving business impacts or consequences? Are

E. Design, implement, maintain, and document safeguards that control for the internal and external risks

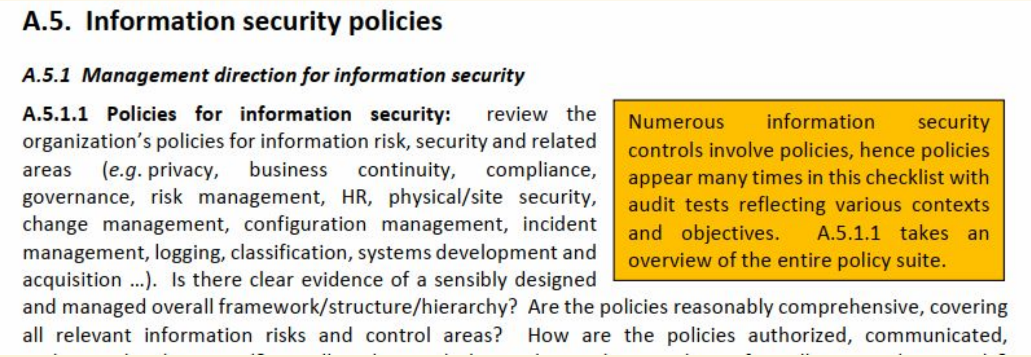
A.5 Information Security Policies [Answer]
A.10 Cryptography [Answer]
A.11 Physical and Environmental Security
A.12 Operation Security [Answer]



A.12. Operations security

A.12.1 Operational procedures and responsibilities

A.12.1.1 Documented operating procedures: review the general state of procedures for IT operations, systems and network management, incident management, IT security administration, IT and physical security operations, change management *etc*. Is there a full set of security procedures in place and when were they last reviewed? Are the processes reasonably secure and well-controlled? Are information security

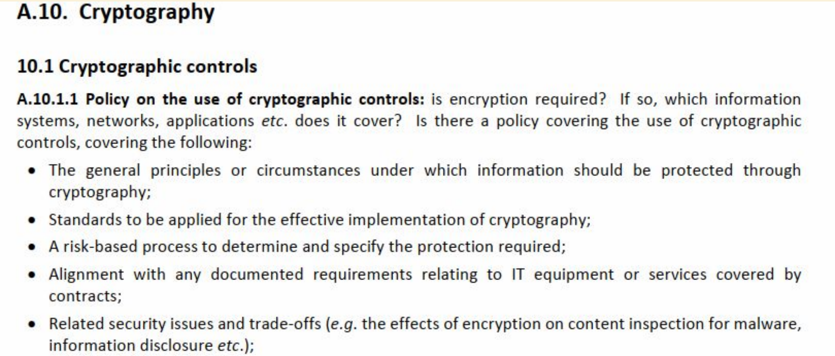


A.5. Information security policies

A.5.1 Management direction for information security

A.5.1.1 Policies for information security: review the organization's policies for information risk, security and related areas (*e.g.* privacy, business continuity, compliance, governance, risk management, HR, physical/site security, change management, configuration management, incident management, logging, classification, systems development and acquisition ...). Is there clear evidence of a sensibly designed and managed overall framework/structure/hierarchy? Are the policies reasonably comprehensive, covering all relevant information risks and control areas? How are the policies authorized, communicated,

Numerous information security controls involve policies, hence policies appear many times in this checklist with audit tests reflecting various contexts and objectives. A.5.1.1 takes an overview of the entire policy suite.



A.10. Cryptography

10.1 Cryptographic controls

A.10.1.1 Policy on the use of cryptographic controls: is encryption required? If so, which information systems, networks, applications *etc*. does it cover? Is there a policy covering the use of cryptographic controls, covering the following:

- The general principles or circumstances under which information should be protected through cryptography;
- Standards to be applied for the effective implementation of cryptography;
- A risk-based process to determine and specify the protection required;
- Alignment with any documented requirements relating to IT equipment or services covered by contracts;
- Related security issues and trade-offs (*e.g.* the effects of encryption on content inspection for malware, information disclosure *etc*.);

F & G. Perform regular vulnerability assessments and pentesting to evaluate the sufficiency of safeguards. Ensure that the Program is modified based on the results.

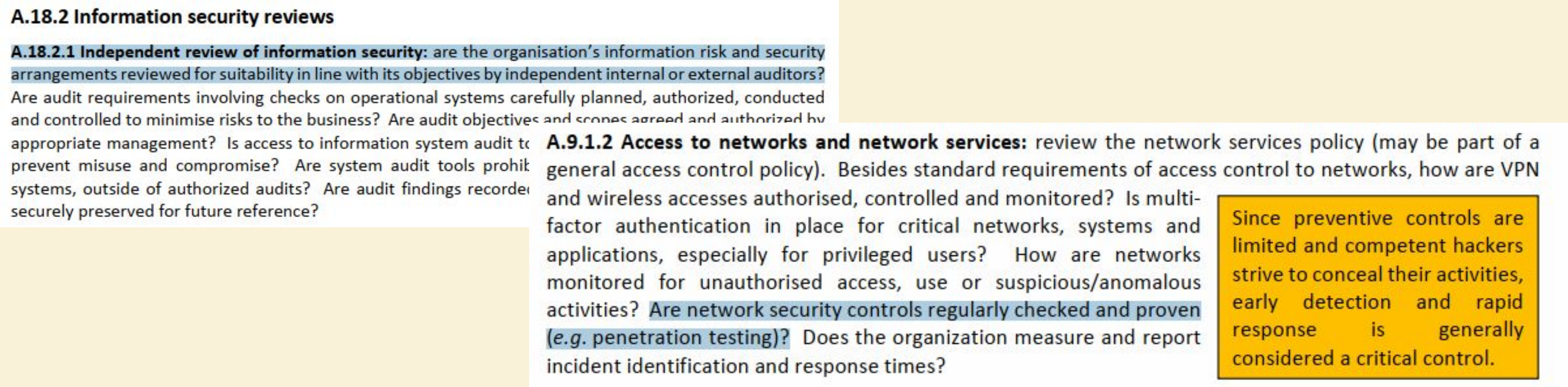
Aside from **Operational Security** what other checklist does this fulfil?

A.5 Information Security Policies

A.9 Access Control [Answer]

A.11 Physical and Environmental Security

A.18 Compliance [Answer]



A.18.2 Information security reviews

A.18.2.1 Independent review of information security: are the organisation's information risk and security arrangements reviewed for suitability in line with its objectives by independent internal or external auditors? Are audit requirements involving checks on operational systems carefully planned, authorized, conducted and controlled to minimise risks to the business? Are audit objectives and scopes agreed and authorized by appropriate management? Is access to information system audit tc prevent misuse and compromise? Are system audit tools prohik systems, outside of authorized audits? Are audit findings recorde securely preserved for future reference?

A.9.1.2 Access to networks and network services: review the network services policy (may be part of a general access control policy). Besides standard requirements of access control to networks, how are VPN and wireless accesses authorised, controlled and monitored? Is multi-factor authentication in place for critical networks, systems and applications, especially for privileged users? How are networks monitored for unauthorised access, use or suspicious/anomalous activities? Are network security controls regularly checked and proven (*e.g.* penetration testing)? Does the organization measure and report incident identification and response times?

Since preventive controls are limited and competent hackers strive to conceal their activities, early detection and rapid response is generally considered a critical control.

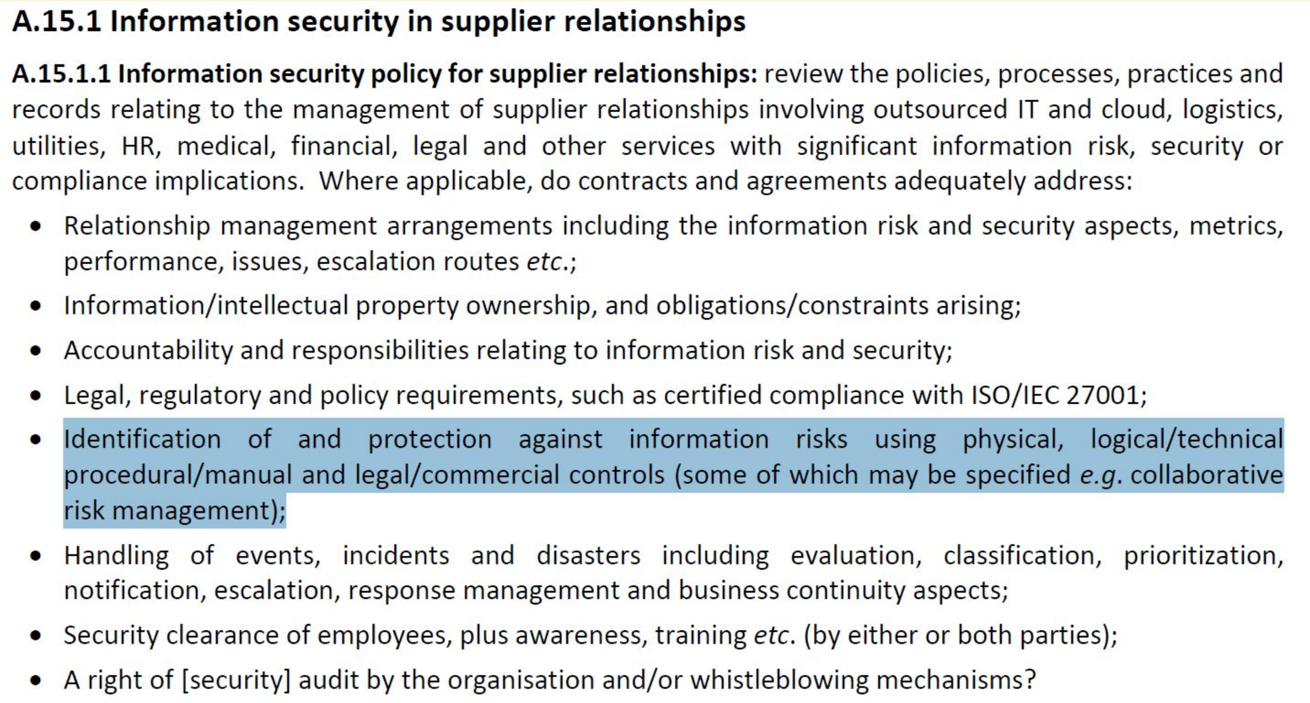
H. Select and retain service providers capable of safeguarding Covered Information they access through or receive from Respondent

A.8 Asset Management

A.9 Access Control

A.15 Supplier Relationships [Answer]

A.17 Business Continuity Management



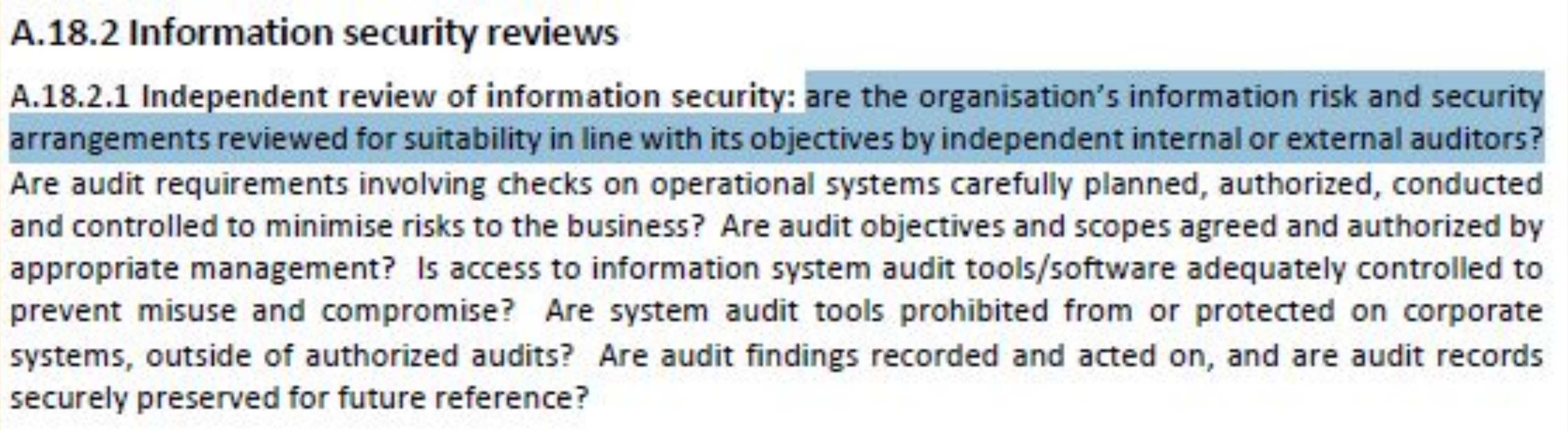
A.15.1 Information security in supplier relationships

A.15.1.1 Information security policy for supplier relationships: review the policies, processes, practices and records relating to the management of supplier relationships involving outsourced IT and cloud, logistics, utilities, HR, medical, financial, legal and other services with significant information risk, security or compliance implications. Where applicable, do contracts and agreements adequately address:

- Relationship management arrangements including the information risk and security aspects, metrics, performance, issues, escalation routes *etc.*;
- Information/intellectual property ownership, and obligations/constraints arising;
- Accountability and responsibilities relating to information risk and security;
- Legal, regulatory and policy requirements, such as certified compliance with ISO/IEC 27001;
- Identification of and protection against information risks using physical, logical/technical procedural/manual and legal/commercial controls (some of which may be specified *e.g.* collaborative risk management);
- Handling of events, incidents and disasters including evaluation, classification, prioritization, notification, escalation, response management and business continuity aspects;
- Security clearance of employees, plus awareness, training *etc.* (by either or both parties);
- A right of [security] audit by the organisation and/or whistleblowing mechanisms?

l. Consult with, and seek appropriate guidance from, independent, third-party experts on data protection in the course of establishing, implementing, maintaining, and updating the Program;

A.5 Information Security Policies
A.6 Organisation of Information Security
A.14 System Acquisition, Development, and Maintenance
A.18 Compliance [Answer]

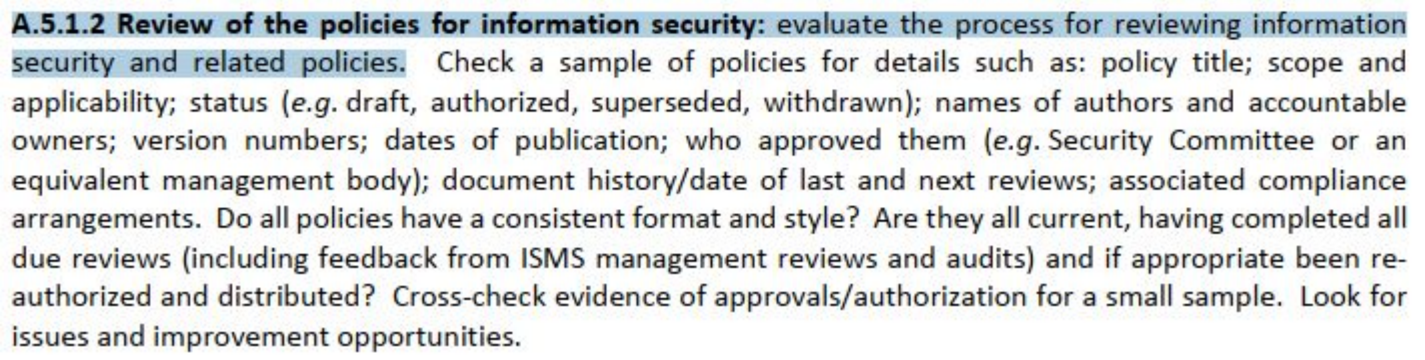


A.18.2 Information security reviews

A.18.2.1 Independent review of information security: are the organisation's information risk and security arrangements reviewed for suitability in line with its objectives by independent internal or external auditors? Are audit requirements involving checks on operational systems carefully planned, authorized, conducted and controlled to minimise risks to the business? Are audit objectives and scopes agreed and authorized by appropriate management? Is access to information system audit tools/software adequately controlled to prevent misuse and compromise? Are system audit tools prohibited from or protected on corporate systems, outside of authorized audits? Are audit findings recorded and acted on, and are audit records securely preserved for future reference?

J. Evaluate and adjust the Program in light of any changes to Respondent’s operations or business arrangements, a Covered Incident, new or more efficient technological or operational methods.

A.5 Information Security Policies [Answer]
A.9 Access Control
A.12 Operation Security
A.18 Compliance



A.5.1.2 Review of the policies for information security: evaluate the process for reviewing information security and related policies. Check a sample of policies for details such as: policy title; scope and applicability; status (*e.g.* draft, authorized, superseded, withdrawn); names of authors and accountable owners; version numbers; dates of publication; who approved them (*e.g.* Security Committee or an equivalent management body); document history/date of last and next reviews; associated compliance arrangements. Do all policies have a consistent format and style? Are they all current, having completed all due reviews (including feedback from ISMS management reviews and audits) and if appropriate been re-authorized and distributed? Cross-check evidence of approvals/authorization for a small sample. Look for issues and improvement opportunities.

What was left out from the checklist?

- A.7. Human Resources Security.
- A.8. Asset Management.
- A.11. Physical and Environmental Security.
- A.13. Communication Security
- A.14. System Acquisition, Development, and Maintenance.
- A.17. Business Continuity Management.

Purpose of Annual Certificate Submission

Our Answer

- For FTC to check that Zoom has continued to comply with the measured outlined in the Consent Agreement.
    - Has met the requirements of the order.
    - Not aware of any "**material noncompliance**" that has not been corrected or disclosed to the FTC.
- Any false certification will subject them to further individual civil and criminal penalties.

Effectiveness of Annual Certificate Submission

Our Answer

- Effective because Zoom must obtain **independent security assessments** every other year during this order's term.
  - Assessors must be those that FTC has approved → Assurance on the effectiveness.
- Assessor must identify evidence to support its conclusions and may not rely "**primarily on assertions or attestations**" by the company.

Thank You!

Q & A