IS4231_T1_G2

Tutorial 5
InfoSec Program

Tze Xern | Fei Dong | Andy | Alicia

Part I: 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?

Answer: A. PDPA.

Part I: Question 1

A. PDPA

Definition: An Act to govern the collection, use and disclosure of personal data by organisations, and to establish the Do Not Call Register and to provide for its administration, and for matters connected therewith, and to make related and consequential amendments to various other Acts.

Under the Data Protection Obligations in PDPA, the protection obligations enforce that there must be **reasonable security arrangements** have to be made to**protect** the personal data in your organisation’s possession to prevent unauthorised access, collection, use, disclosure or similar risks.

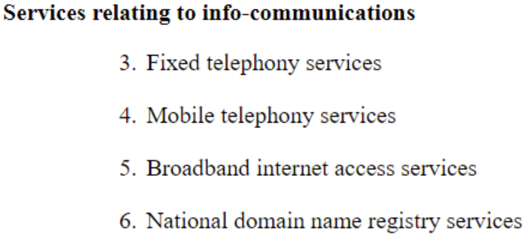
https://www.pdpc.gov.sg/Overview -of-PDPA/The-Legislation/Personal-Data-Protection -Act/Data -Protection -Obligations

Part I: Question 1

B. Cybersecurity Act

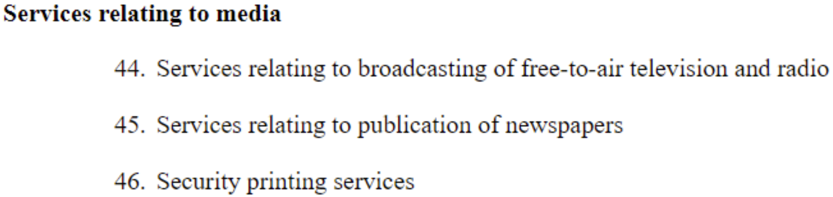
Definition: An Act to require or authorise the taking of measures to prevent, manage and respond to cybersecurity threats and incidents, to regulate owners of critical information infrastructure, to regulate cybersecurity service providers, and for matters related thereto, and to make consequential or related amendments to certain other written laws.

Zoom is not considered a CII in Singapore.



Services relating to info-communications

3. Fixed telephony services
4. Mobile telephony services
5. Broadband internet access services
6. National domain name registry services



Services relating to media

44. Services relating to broadcasting of free-to-air television and radio
45. Services relating to publication of newspapers
46. Security printing services

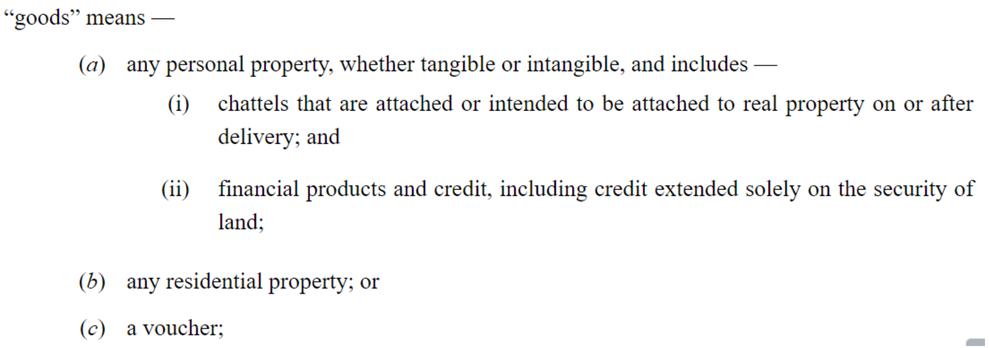
https://sso.agc.gov.sg/Acts-Supp/9-2018/#Sc1-

Part I: Question 1

C. Consumer Protection Act

Definition: An Act 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.

Zoom users’ data (“Covered Information”) is not considered a “good” under this Act.



“goods” means —

(*a*) any personal property, whether tangible or intangible, and includes —

(i) chattels that are attached or intended to be attached to real property on or after delivery; and

(ii) financial products and credit, including credit extended solely on the security of land;

(*b*) any residential property; or

(*c*) a voucher;

https://sso.agc.gov.sg/Act/CPFTA2003#pr2-

Part I: Question 1

D. Competition Act

Definition: An Act to make provision about competition and the abuse of a dominant position in the market; and to establish the Competition and Consumer Commission of Singapore, to provide for its functions and powers and for matters connected therewith.

In this case study, Zoom did not "abuse a dominant position" in the market. The main issue here is that Zoom was not responsible in handling user data and ensuring their security.

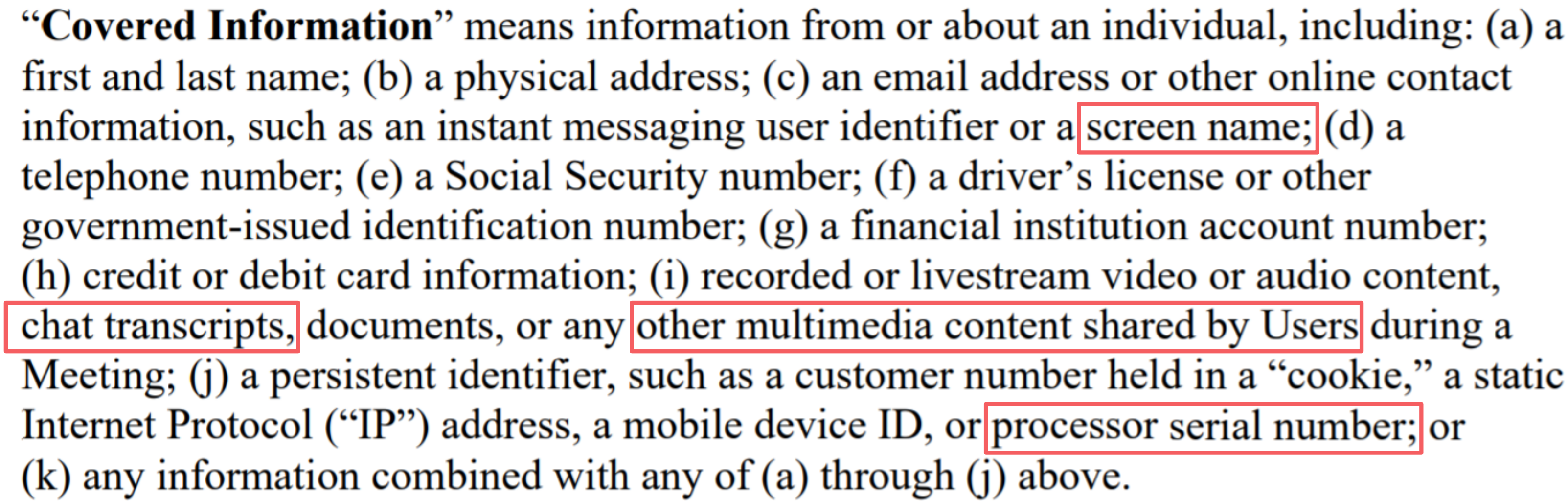
Part I: Question 2

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

Answer: D. none of the above.

Part I: Question 2

Reasoning:



"**Covered Information**" means information from or about an individual, including: (a) a first and last name; (b) a physical address; (c) an email address or other online contact information, such as an instant messaging user identifier or a screen name; (d) a telephone number; (e) a Social Security number; (f) a driver's license or other government-issued identification number; (g) a financial institution account number; (h) credit or debit card information; (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 static Internet Protocol ("IP") address, a mobile device ID, or processor serial number; or (k) any information combined with any of (a) through (j) above.

Part I: Question 3

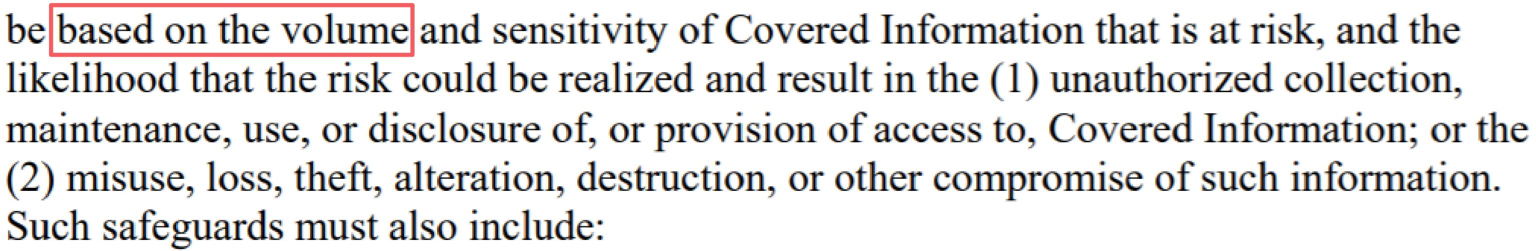
In the FTC’s Final Order, the design and implementation of security measures (i.e., policies, procedures, and technical) follows what kind of approach?

Answer: D. Volume based (II.E).

Part I: Question 3

Reasoning for volume-based:

It is stated in the document that a Covered Information will be based on it’s volume and sensitivity to determine whether or not it is at risk - II. Mandated Information Security Program - Section D



be based on the volume and sensitivity of Covered Information that is at risk, and the likelihood that the risk could be realized and result in the (1) unauthorized collection, maintenance, use, or disclosure of, or provision of access to, Covered Information; or the (2) misuse, loss, theft, alteration, destruction, or other compromise of such information. Such safeguards must also include:

Part II: Question 1

According to the FTC's investigation result, what were the deceptive and unfair practices of Zoom that undermined the security of its users?

Part II: Question 1

- “**end-to-end, 256-bit encryption**” to secure users’ communications, when in fact it provided a lower level of security;
  - End-to-end encryption is a method of securing communications so that only the sender and recipient(s)—and no other person, not even the platform provider—can read the content.
- Zoom **maintained the cryptographic keys** that could allow Zoom to access the content of its customers’ meetings, and secured its Zoom Meetings
- some recordings allegedly were **stored unencrypted** for up to 60 days on Zoom’s servers before being transferred to its secure cloud storage.
- **secretly installed software**, called a ZoomOpener web server
- The software remained on users’ computers even after they deleted the Zoom app, and would automatically reinstall the Zoom app
- Zoom’s **release notes** for the July 2018 update were **deceptive**

Part II: Question 2

Based on the FTC’s Final Order, what is the mandated comprehensive security program for Zoom to establish, implement, and maintain?

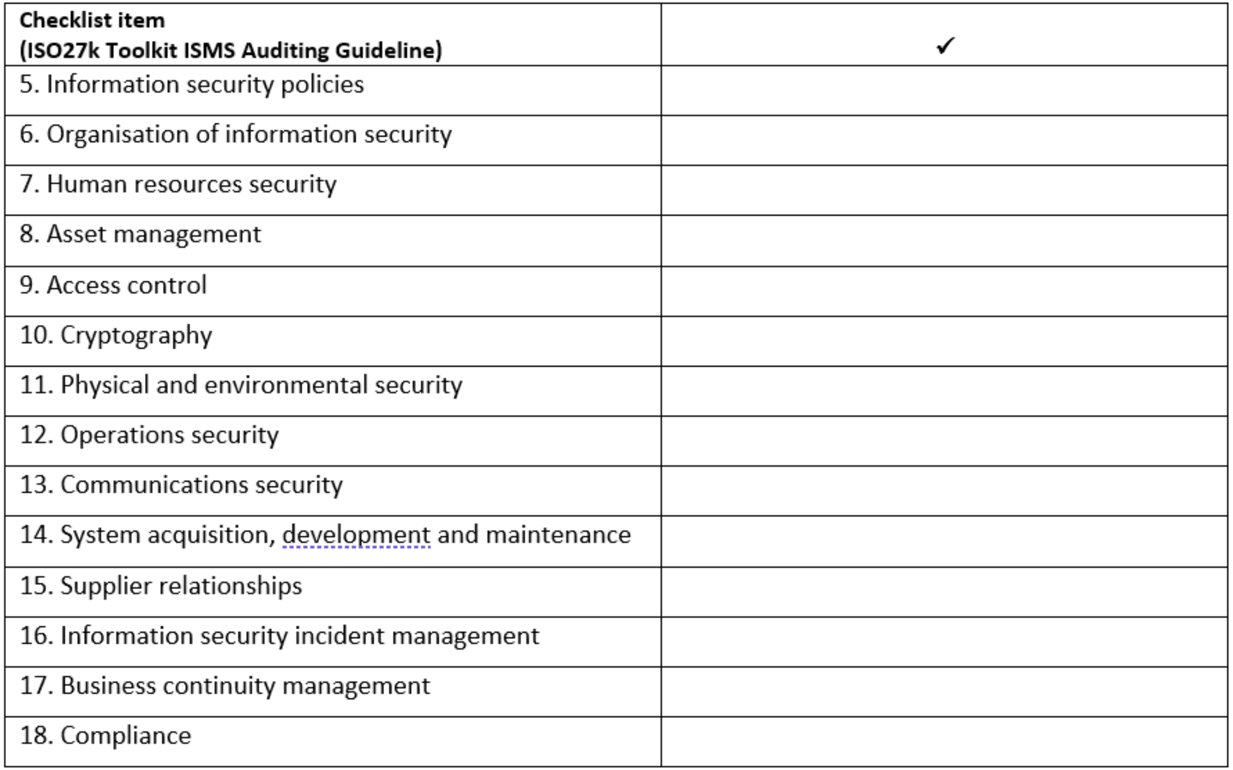
Part II: Question 2

Answer: Section A to Section J of Part II. Mandated Information Security Program

Each section will be covered in detail in question 3.

Part II: Question 3

Read ISO27k Toolkit ISMS Auditing Guideline Appendix A- Generic Information Security Audit Checklist. Map the detailed requirements from the mandated security program to this checklist.



Checklist item **(ISO27k Toolkit ISMS Auditing Guideline)**	✓
5. Information security policies	
6. Organisation of information security	
7. Human resources security	
8. Asset management	
9. Access control	
10. Cryptography	
11. Physical and environmental security	
12. Operations security	
13. Communications security	
14. System acquisition, development and maintenance	
15. Supplier relationships	
16. Information security incident management	
17. Business continuity management	
18. Compliance	

Part II: Question 3

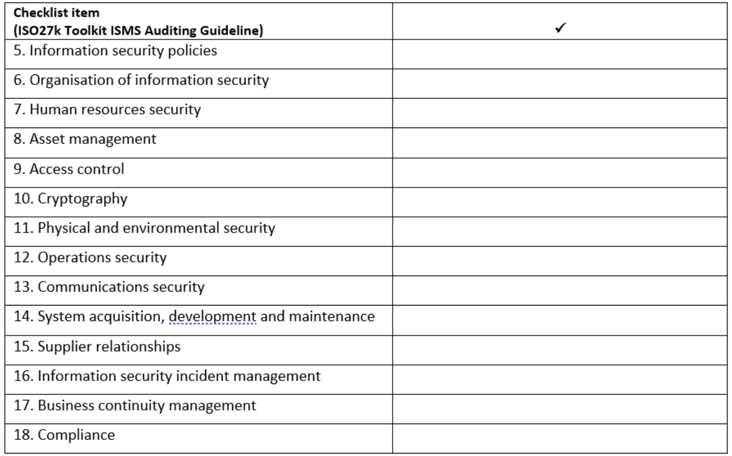
(12)

A. Document in writing the content, implementation, and maintenance of the Program, including all processesand procedures that will be used to implement all Program policies and safeguards;

(5)

5. Information Security Policies
- is there clear evidence of a sensibly designed and managed overall framework/ structure/ hierarchy?
- How are the policies authorized, communicated, understood, and accepted?

12. Operations security
- Documented operating procedures



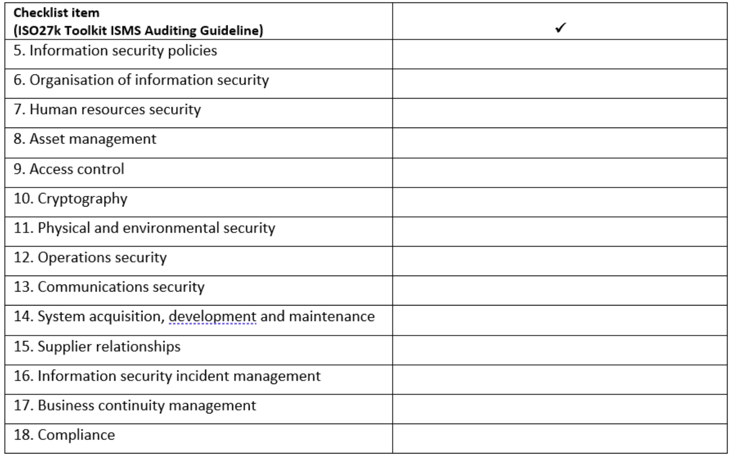
Checklist item (ISO27k Toolkit ISMS Auditing Guideline)	✓
5. Information security policies	
6. Organisation of information security	
7. Human resources security	
8. Asset management	
9. Access control	
10. Cryptography	
11. Physical and environmental security	
12. Operations security	
13. Communications security	
14. System acquisition, development and maintenance	
15. Supplier relationships	
16. Information security incident management	
17. Business continuity management	
18. Compliance	

Part II: Question 3

B. Provide the written Program and any material evaluations thereof or material updates thereto to Respondent's board of directors or governing body or, if no such board or equivalent governing body exists, to a senior officer of Respondent responsible for Respondent's Program at least once every twelve (12) months and promptly (not to exceed thirty (30) days) after a Covered Incident;

Rationale: key focus is on the governing body, and who should manage security incidents.

6. Organization of Information security



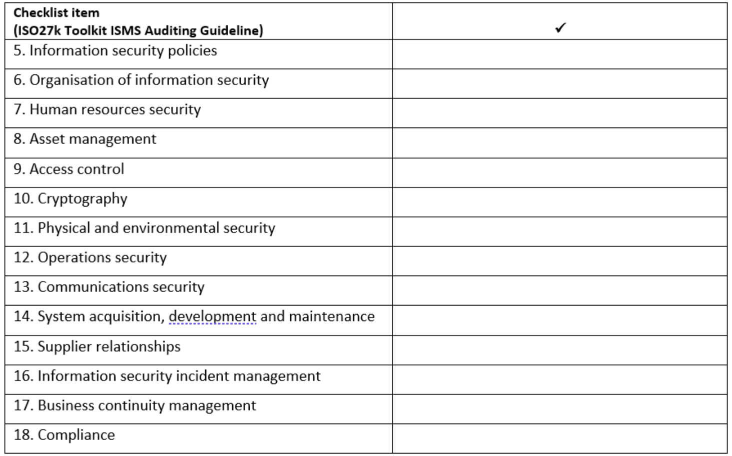
Checklist item **(ISO27k Toolkit ISMS Auditing Guideline)**	✓
5. Information security policies	
6. Organisation of information security	
7. Human resources security	
8. Asset management	
9. Access control	
10. Cryptography	
11. Physical and environmental security	
12. Operations security	
13. Communications security	
14. System acquisition, development and maintenance	
15. Supplier relationships	
16. Information security incident management	
17. Business continuity management	
18. Compliance	

Part II: Question 3

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

Referring to Security Program

6. Organization of Information security



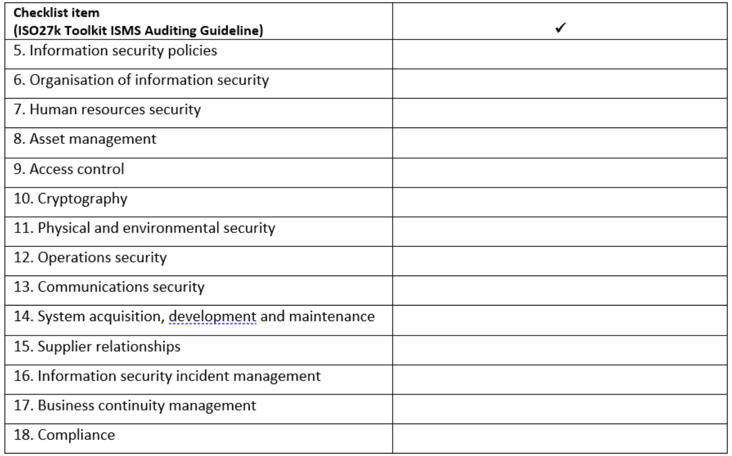
Checklist item (ISO27k Toolkit ISMS Auditing Guideline)	✓
5. Information security policies	
6. Organisation of information security	
7. Human resources security	
8. Asset management	
9. Access control	
10. Cryptography	
11. Physical and environmental security	
12. Operations security	
13. Communications security	
14. System acquisition, development and maintenance	
15. Supplier relationships	
16. Information security incident management	
17. Business continuity management	
18. Compliance	

Part II: Question 3

D. Assessand document, at least once every twelve (12) months and promptly (not to exceed thirty (30) days) following a Covered Incident, internal and external risks to the security, confidentiality, or integrity of Covered Information that could result in the (1) unauthorized collection, maintenance, use, or disclosure of, or provision of accessto, Covered Information ; or the (2) misuse, loss, theft, alteration, destruction, or other compromise of such information ;

Rationale: Explains what should be done in the event of a security incident.

16. Information security incident management



Checklist item **(ISO27k Toolkit ISMS Auditing Guideline)**	✓
5. Information security policies	
6. Organisation of information security	
7. Human resources security	
8. Asset management	
9. Access control	
10. Cryptography	
11. Physical and environmental security	
12. Operations security	
13. Communications security	
14. System acquisition, development and maintenance	
15. Supplier relationships	
16. Information security incident management	
17. Business continuity management	
18. Compliance	

Part II: Question 3

E. 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 identified in response to sub-Provision II.D. Each safeguard must 5 be based on the volume and sensitivity of Covered Information that is at risk, and the likelihood that the risk could be realized and result in the (1) unauthorized collection, maintenance, use, or disclosure of, or provision of access to, Covered Information; or the (2) misuse, loss, theft, alteration, destruction, or other compromise of such information. Such safeguards must also include:

Part II: Question 3

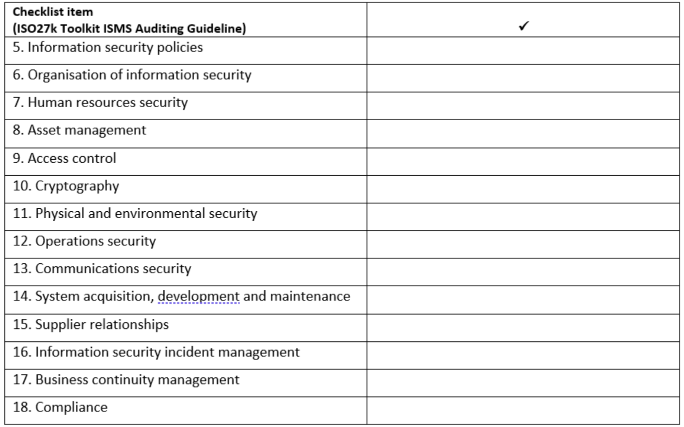
E.1. Implementing a security review by Zoom Security Personnel designated by Respondent of all new Meeting Servicessoftware or software updates, prior to release that, at a minimum, includes:

E.1.a. Policies, procedures, and any applicable technical measuresfor reviewing all new Meeting Service software or software updates for commonly known vulnerabilities, including those identified by the Open Web Application Security Project (OWASP) and critical or high severity vulnerabilities in the National Vulnerability Database (NVD), and remediating or otherwise mitigating any such vulnerabilities ;

Rationale: Discusses the implementation of technical and organizational measures that **bring down security risks of Zoom to common vulnerabilities, such as those found in OWASP and NVD**. These are covered in the “Operational security” and “System maintenance” sections by definition.

12. Operational security

14. System acquisition, development, maintenance



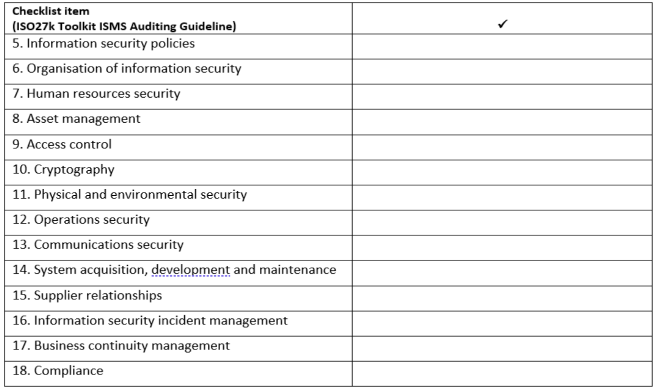
Checklist item **(ISO27k Toolkit ISMS Auditing Guideline)**	✓
5. Information security policies	
6. Organisation of information security	
7. Human resources security	
8. Asset management	
9. Access control	
10. Cryptography	
11. Physical and environmental security	
12. Operations security	
13. Communications security	
14. System acquisition, development and maintenance	
15. Supplier relationships	
16. Information security incident management	
17. Business continuity management	
18. Compliance	

Part II: Question 3

E.1.b. Policies, procedures, and any applicable technical measures to: (i) determine whether any new Meeting Services software or software update is designed to circumvent or bypass, in whole or in part, any Third-Party Security Feature such that the Third-Party Security Feature no longer provides the same protection(s) for Users against the risk of unauthorized access,collection, disclosure, use, misuse, loss, theft, alteration, destruction, or other compromise of Users' Covered Information ; and (ii) assess the risk of unauthorized access,collection, disclosure, use, misuse, loss, theft, alteration, destruction, or other compromise of the User's Covered Information that will result from such circumvention or bypass, based on the volume and sensitivity of Covered Information that is at risk, and the likelihood that the risk could be realized; and

Rationale: Discusses access control policies

9. Access Control



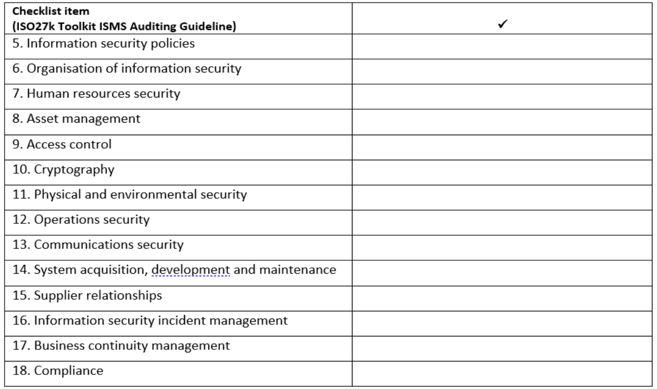
Checklist item **(ISO27k Toolkit ISMS Auditing Guideline)**	✓
5. Information security policies	
6. Organisation of information security	
7. Human resources security	
8. Asset management	
9. Access control	
10. Cryptography	
11. Physical and environmental security	
12. Operations security	
13. Communications security	
14. System acquisition, development and maintenance	
15. Supplier relationships	
16. Information security incident management	
17. Business continuity management	
18. Compliance	

Part II: Question 3

E.1.c. Policies, procedures, and any applicable technical measures so that Respondent will not implement any new Meeting Services software or software update that has been identified under Part II.E.1.b(i) of this Order as designed to circumvent or bypass a Third-Party Security Feature, unless: (i) Zoom Security Personnel determine that the bypass or circumvention does not create a material risk of unauthorized access, collection, disclosure, use, misuse, loss, theft, alteration, destruction, or other compromise of Users' Covered Information ; or (ii) Respondent implements security measure(s) that offset or otherwise mitigate the risk(s) of unauthorized access, collection, disclosure, use, misuse, loss, theft, alteration, destruction, or other compromise of Users' Covered Information that were identified under Part II.E.1.b(ii) of this Order ;

Rationale: Discusses access control policies

9. Access Control



Checklist item **(ISO27k Toolkit ISMS Auditing Guideline)**	✓
5. Information security policies	
6. Organisation of information security	
7. Human resources security	
8. Asset management	
9. Access control	
10. Cryptography	
11. Physical and environmental security	
12. Operations security	
13. Communications security	
14. System acquisition, development and maintenance	
15. Supplier relationships	
16. Information security incident management	
17. Business continuity management	
18. Compliance	

Part II: Question 3

E.2. Implementing a vulnerability management program that includes:

E.2.a. Conducting vulnerability scans of Respondent's networks and systems on at least a quarterly basis; and

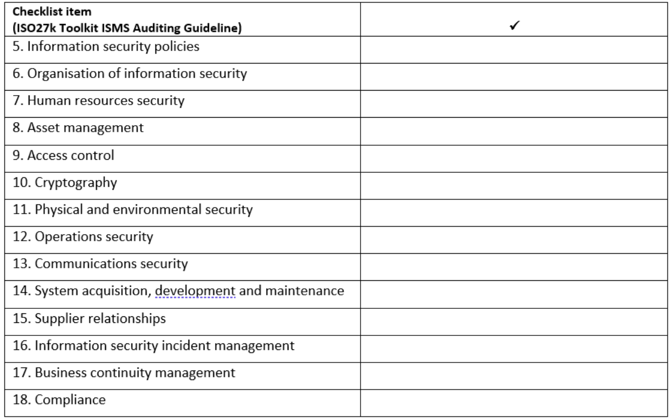
E.2.b. Policies, procedures, and any applicable technical measures for remediating or otherwise mitigating any critical or high severity vulnerabilities promptly (but in no event later than thirty (30) days after the vulnerability is detected), unless Respondent documents its rationale for not doing so;

14. System acquisition, development, maintenance

- **System security testing**

16. Information security incident management

- **Responsibility and procedures**



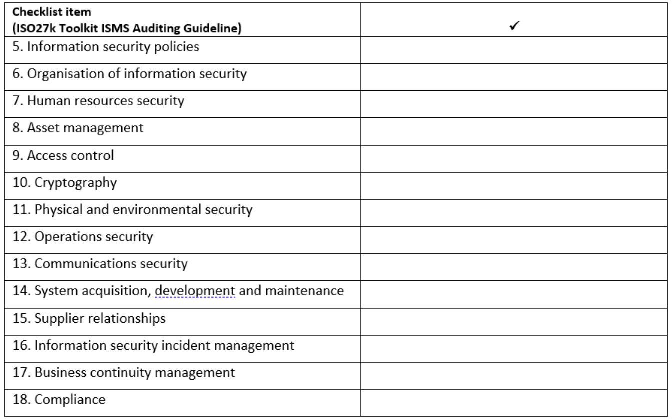
Checklist item **(ISO27k Toolkit ISMS Auditing Guideline)**	✓
5. Information security policies	
6. Organisation of information security	
7. Human resources security	
8. Asset management	
9. Access control	
10. Cryptography	
11. Physical and environmental security	
12. Operations security	
13. Communications security	
14. System acquisition, development and maintenance	
15. Supplier relationships	
16. Information security incident management	
17. Business continuity management	
18. Compliance	

Part II: Question 3

E.3. Implementing a default, randomized naming convention for recorded Meetings that are to be stored on Users’ local devices, and instructing Users to employ a unique file name when saving such recorded Meetings;

8. Asset management

- Labelling of information

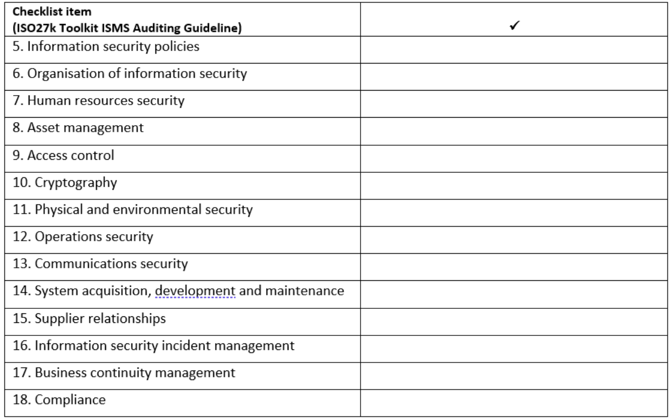


Checklist item **(ISO27k Toolkit ISMS Auditing Guideline)**	✓
5. Information security policies	
6. Organisation of information security	
7. Human resources security	
8. Asset management	
9. Access control	
10. Cryptography	
11. Physical and environmental security	
12. Operations security	
13. Communications security	
14. System acquisition, development and maintenance	
15. Supplier relationships	
16. Information security incident management	
17. Business continuity management	
18. Compliance	

Part II: Question 3

E.4. Policies, procedures, and any applicable technical measures to: (a) systematically classify and inventory Covered Information in Respondent's control; (b) log and monitor access to repositories of Covered Information in Respondent's control; and (c) limit access to Covered Information by, at a minimum, limiting employee and service provider access to Covered Information to what is needed to perform that employee or service provider's job function;

8. Asset management (a)
   - Classification of Information
12. Operational security (b)
   - Logging and monitoring
9. Access control (c)
   - Access control policy

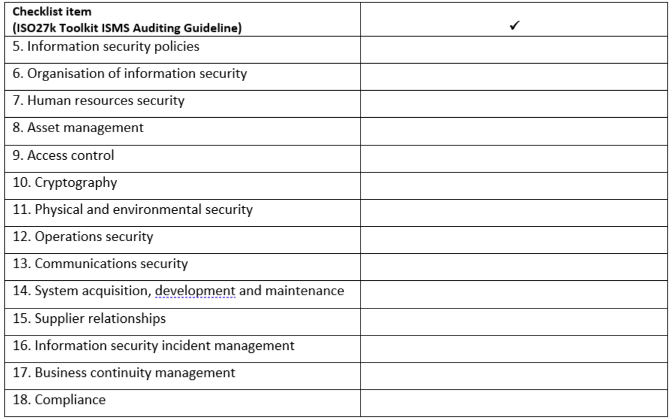


Checklist item **(ISO27k Toolkit ISMS Auditing Guideline)**	✓
5. Information security policies	
6. Organisation of information security	
7. Human resources security	
8. Asset management	
9. Access control	
10. Cryptography	
11. Physical and environmental security	
12. Operations security	
13. Communications security	
14. System acquisition, development and maintenance	
15. Supplier relationships	
16. Information security incident management	
17. Business continuity management	
18. Compliance	

Part II: Question 3

E.5. Data deletion policies, procedures, and any applicable technical measures,including validating that all copies of Covered Information identified for deletion are deleted within thirty -one (31) days;

8. Asset management
    - Media handling
        - Disposal of media



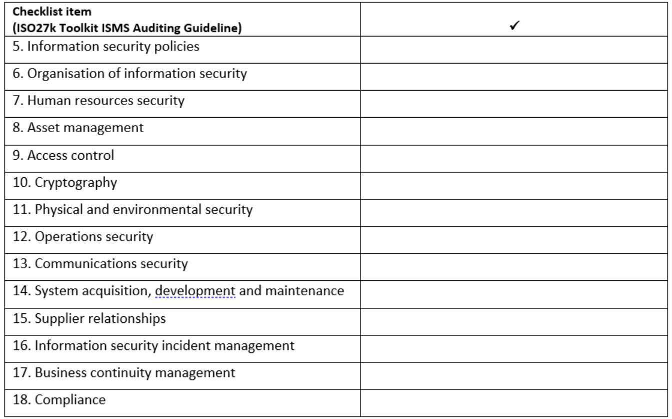
Checklist item **(ISO27k Toolkit ISMS Auditing Guideline)**	✓
5. Information security policies	
6. Organisation of information security	
7. Human resources security	
8. Asset management	
9. Access control	
10. Cryptography	
11. Physical and environmental security	
12. Operations security	
13. Communications security	
14. System acquisition, development and maintenance	
15. Supplier relationships	
16. Information security incident management	
17. Business continuity management	
18. Compliance	

Part II: Question 3

E.6. Policies, procedures, and any applicable technical measures designed to reduce the risk of online attacks resulting from the misuse of valid Credentials by unauthorized third parties, including: (a) requiring Users to secure their accounts with strong, unique passwords; (b) using automated tools to identify non-human login attempts; (c) rate-limiting login attempts to minimize the risk of a brute force attack; and (d) implementing password resets for known compromised Credentials;

9. Access control

- Password management system (a)
- Secure log-on procedures (b & c)
- Removal or adjustment of access rights (d)



Checklist item **(ISO27k Toolkit ISMS Auditing Guideline)**	✓
5. Information security policies	
6. Organisation of information security	
7. Human resources security	
8. Asset management	
9. Access control	
10. Cryptography	
11. Physical and environmental security	
12. Operations security	
13. Communications security	
14. System acquisition, development and maintenance	
15. Supplier relationships	
16. Information security incident management	
17. Business continuity management	
18. Compliance	

Part II: Question 3

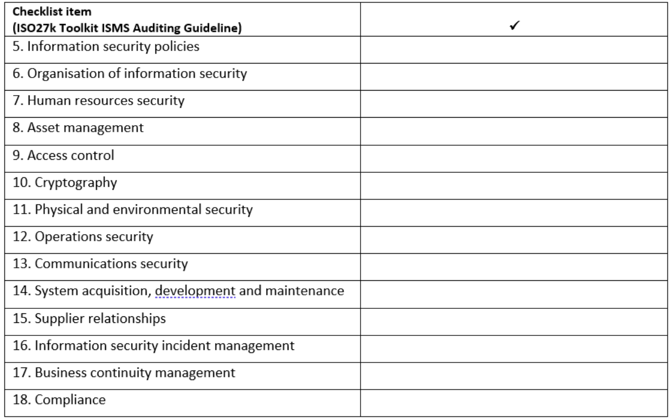
E.7. Regular security training programs, on at least an annual basis, that are updated, as applicable, to address internal or external risks identified by Respondent under subProvision II.D of this Order, and that include, at a minimum:

E.7.a Security awareness training for all employees on Respondent's security policies and procedures, including the requirements of this Order and the process for submitting complaints and concerns; and

E.7.b Training in secure software development principles, including secure engineering and defensive programming concepts, for developers, engineers, and other employees that design Respondent's products or services or that are otherwise responsible for the security of Covered Information ;

7. Human resources security

- During employment
  - Security awareness (a)
  - Security education and training (b)

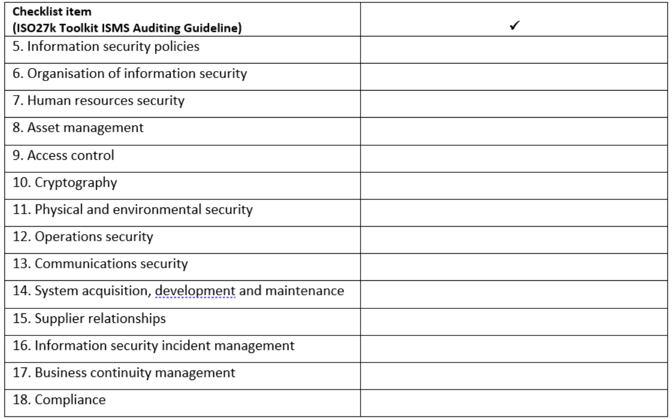


Checklist item (ISO27k Toolkit ISMS Auditing Guideline)	✓
5. Information security policies	
6. Organisation of information security	
7. Human resources security	
8. Asset management	
9. Access control	
10. Cryptography	
11. Physical and environmental security	
12. Operations security	
13. Communications security	
14. System acquisition, development and maintenance	
15. Supplier relationships	
16. Information security incident management	
17. Business continuity management	
18. Compliance	

Part II: Question 3

E.8. Technical measures to monitor all of Respondent’s networks, systems, and assets within those networks to identify anomalousactivity and/or data security events on Respondent’snetwork, including unauthorized attempts to exfiltrate Covered Information from Respondent’snetworks;

9. Access control
   - Access to network and network services
12. Operational security
   - Monitoring
13. Communication security
   - Security of network
16. Information security incident management
   - Monitoring/detecting and reporting information security events
   - Reporting information security weaknesses

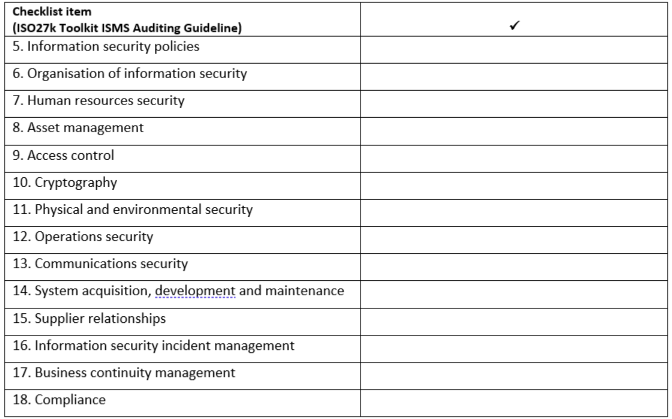


Checklist item **(ISO27k Toolkit ISMS Auditing Guideline)**	✓
5. Information security policies	
6. Organisation of information security	
7. Human resources security	
8. Asset management	
9. Access control	
10. Cryptography	
11. Physical and environmental security	
12. Operations security	
13. Communications security	
14. System acquisition, development and maintenance	
15. Supplier relationships	
16. Information security incident management	
17. Business continuity management	
18. Compliance	

Part II: Question 3

E.9. Incident response policies, procedures, and any applicable technical measures,including centralized log management and documenting remedial security actions;

16. Information Security Incident Management
  - Responsibilities and procedures

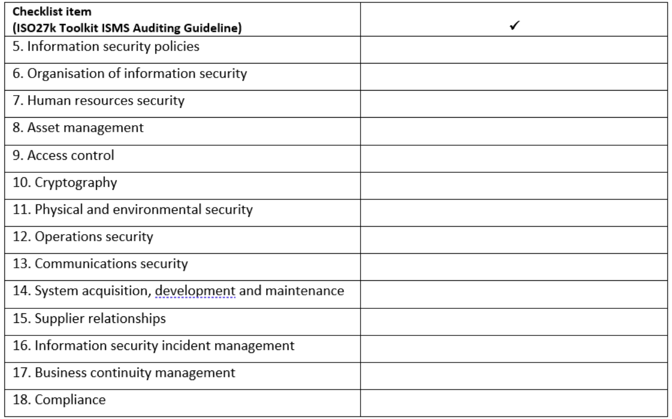


Checklist item **(ISO27k Toolkit ISMS Auditing Guideline)**	✓
5. Information security policies	
6. Organisation of information security	
7. Human resources security	
8. Asset management	
9. Access control	
10. Cryptography	
11. Physical and environmental security	
12. Operations security	
13. Communications security	
14. System acquisition, development and maintenance	
15. Supplier relationships	
16. Information security incident management	
17. Business continuity management	
18. Compliance	

Part II: Question 3

E.10. Technical measures designed to safeguard against unauthorized access to any network or system that stores, collects, maintains, or processes Covered Information, such as properly configured firewalls; properly configured physical or logical segmentation of networks, systems, and databases; and securing of remote access to Respondent's networks through multi-factor authentication or similar technology except for when accessing such networks is for the purpose of using Meeting Services; and

13. Communications Security
    - Network controls e.g. firewall
    - Security of network services
    - Segregation in network services

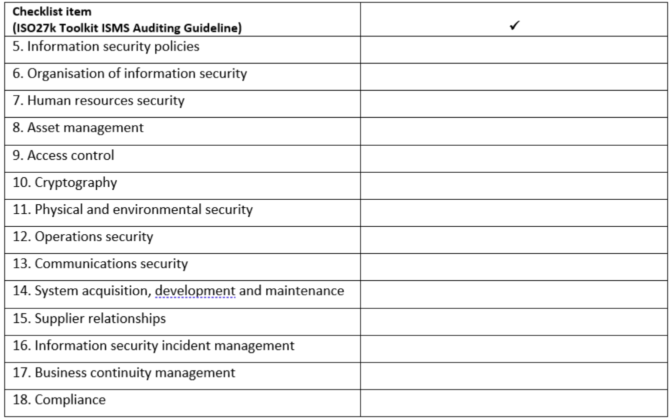


Checklist item **(ISO27k Toolkit ISMS Auditing Guideline)**	✓
5. Information security policies	
6. Organisation of information security	
7. Human resources security	
8. Asset management	
9. Access control	
10. Cryptography	
11. Physical and environmental security	
12. Operations security	
13. Communications security	
14. System acquisition, development and maintenance	
15. Supplier relationships	
16. Information security incident management	
17. Business continuity management	
18. Compliance	

Part II: Question 3

E.11. Protections, such as encryption, tokenization, or other same or greater protections, for Covered Information collected, maintained, processed,or stored by Respondent,including in transit and at rest;

10. Cryptography
    - Cryptographic controls



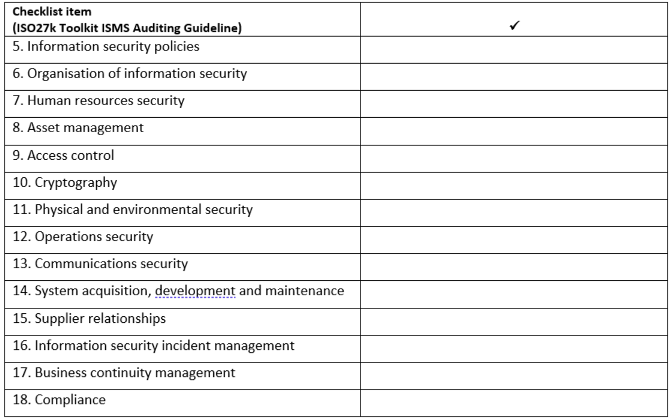
Checklist item (ISO27k Toolkit ISMS Auditing Guideline)	✓
5. Information security policies	
6. Organisation of information security	
7. Human resources security	
8. Asset management	
9. Access control	
10. Cryptography	
11. Physical and environmental security	
12. Operations security	
13. Communications security	
14. System acquisition, development and maintenance	
15. Supplier relationships	
16. Information security incident management	
17. Business continuity management	
18. Compliance	

Part II: Question 3

F. Assess, at least once every twelve (12) months and promptly (not to exceed thirty (30) days) following a Covered Incident, the sufficiency of any safeguards in place to address the internal and external risks to the security, confidentiality, and integrity of Covered Information, and modify the Program based on the results;

16. Information Security Incident Management

- Periodic and/or post-event security review meetings and learning/improvement processes



Checklist item **(ISO27k Toolkit ISMS Auditing Guideline)**	✓
5. Information security policies	
6. Organisation of information security	
7. Human resources security	
8. Asset management	
9. Access control	
10. Cryptography	
11. Physical and environmental security	
12. Operations security	
13. Communications security	
14. System acquisition, development and maintenance	
15. Supplier relationships	
16. Information security incident management	
17. Business continuity management	
18. Compliance	

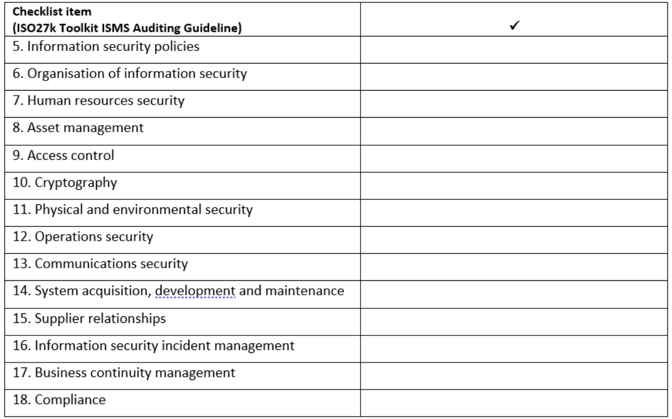
Part II: Question 3

G. Test and monitor the effectiveness of the safeguards at least once every twelve (12) months and promptly (not to exceed thirty (30) days) following a Covered Incident, and modify the Program based on the results. Suchtesting and monitoring must include penetration testing of Respondent’snetwork at least once every twelve (12) months and promptly (not to exceed thirty (30) days) after a Covered Incident;

9. Access control
   - Access to networks and network services

14. System acquisition, development and maintenance
   - Security requirements of information systems e.g. security testing mandatory for all new developments and changes to existing systems

16. Information Security Incident Management
   - Periodic and/or post -event security review meetings and learning/improvement processes



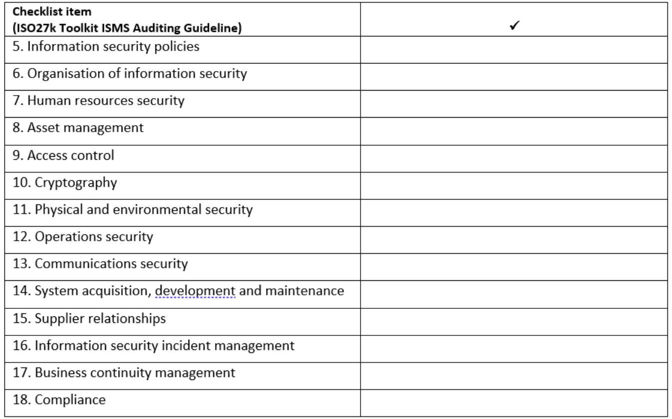
Checklist item **(ISO27k Toolkit ISMS Auditing Guideline)**	✓
5. Information security policies	
6. Organisation of information security	
7. Human resources security	
8. Asset management	
9. Access control	
10. Cryptography	
11. Physical and environmental security	
12. Operations security	
13. Communications security	
14. System acquisition, development and maintenance	
15. Supplier relationships	
16. Information security incident management	
17. Business continuity management	
18. Compliance	

Part II: Question 3

H. Select and retain service providers capable of safeguarding Covered Information they access through or receive from Respondent, and contractually require service providers to implement and maintain safeguards for Covered Information sufficient to address the internal and external risks to the security, confidentiality, or integrity of Covered Information;

15. Supplier relationships

- Information security in supplier relationships
  - Information security policy for supplier relationships
  - Addressing security within supplier agreement
- Supplier service delivery management
  - Monitoring and review supplier services
  - Managing changes to supplier services



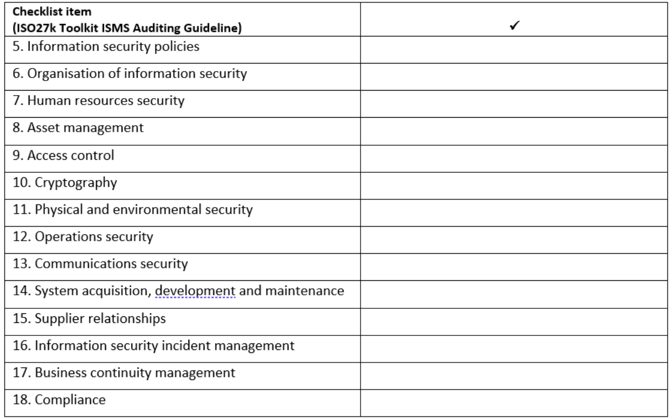
Checklist item **(ISO27k Toolkit ISMS Auditing Guideline)**	✓
5. Information security policies	
6. Organisation of information security	
7. Human resources security	
8. Asset management	
9. Access control	
10. Cryptography	
11. Physical and environmental security	
12. Operations security	
13. Communications security	
14. System acquisition, development and maintenance	
15. Supplier relationships	
16. Information security incident management	
17. Business continuity management	
18. Compliance	

Part II: Question 3

I. 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; and

5. Information Security Policies
- Management direction for information security
  - Review for consistency with good practices e.g. ISO27k, NIST SP800, standards, advisories,

18. Compliance
- Information security reviews
  - Independent review of information security
  - Compliance with security policies, standards



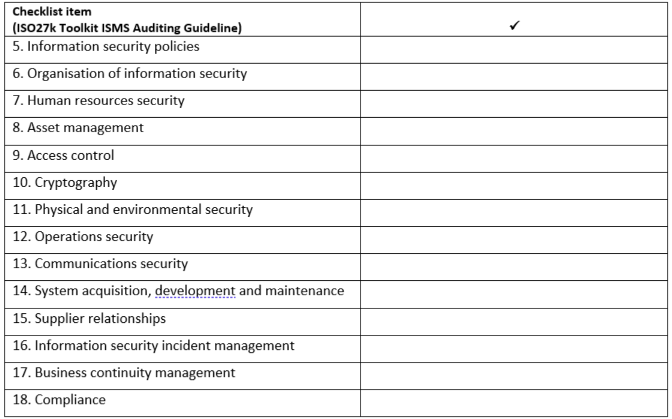
Checklist item **(ISO27k Toolkit ISMS Auditing Guideline)**	✓
5. Information security policies	
6. Organisation of information security	
7. Human resources security	
8. Asset management	
9. Access control	
10. Cryptography	
11. Physical and environmental security	
12. Operations security	
13. Communications security	
14. System acquisition, development and maintenance	
15. Supplier relationships	
16. Information security incident management	
17. Business continuity management	
18. Compliance	

Part II: Question 3

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 to control for the risks identified in sub-Provision II.D of this Order, or any other circumstances that Respondent knows or has reason to know may have a material impact on the effectiveness of the Program or any of its individual safeguards. At a minimum, Respondent must evaluate the Program at least once every twelve (12) months and modify the Program as necessary based on the results.

5. Information Security Policies
- Management direction for information security
    - Review the organization's policies for information risk, security and related areas (e.g., business continuity)
    - Review for consistency with corporate strategies
    - Opportunities for improvement

15. Business Continuity Management



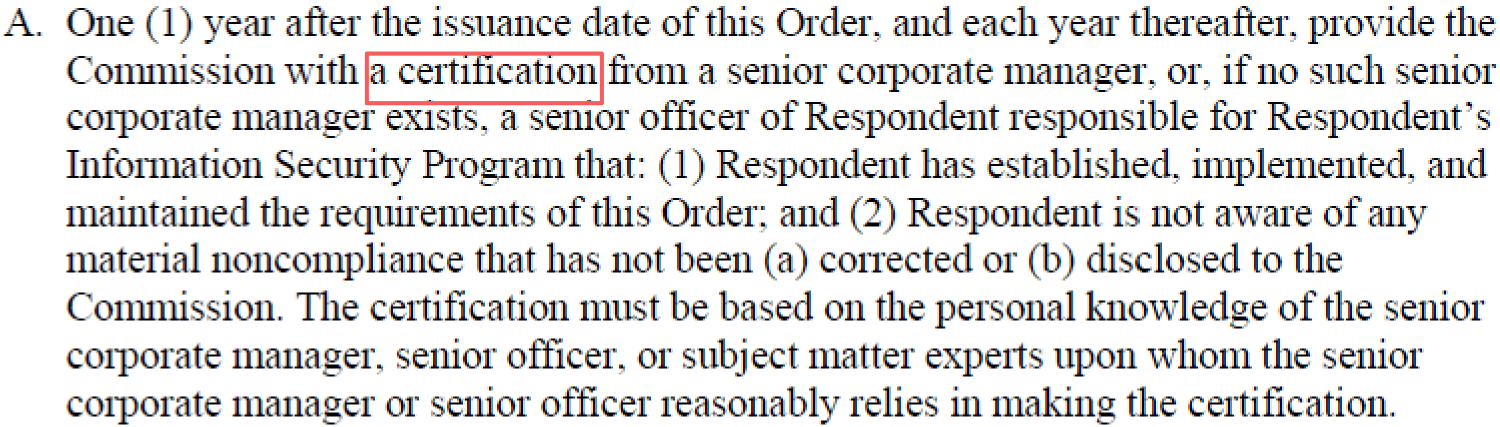
Checklist item **(ISO27k Toolkit ISMS Auditing Guideline)**	✓
5. Information security policies	
6. Organisation of information security	
7. Human resources security	
8. Asset management	
9. Access control	
10. Cryptography	
11. Physical and environmental security	
12. Operations security	
13. Communications security	
14. System acquisition, development and maintenance	
15. Supplier relationships	
16. Information security incident management	
17. Business continuity management	
18. Compliance	

Part II: Question 4

In the Final Order, a senior corporate manager, or if no such senior corporate manager exists, a senior officer of Zoom responsible for Respondent's Information security program is required to submit an annual certification to the Commission. Comments on the purpose and effectiveness of such internal certification arrangement from an information security management perspective.

What do you think?

Section V. A.



A. One (1) year after the issuance date of this Order, and each year thereafter, provide the Commission with a certification from a senior corporate manager, or, if no such senior corporate manager exists, a senior officer of Respondent responsible for Respondent's Information Security Program that: (1) Respondent has established, implemented, and maintained the requirements of this Order; and (2) Respondent is not aware of any material noncompliance that has not been (a) corrected or (b) disclosed to the Commission. The certification must be based on the personal knowledge of the senior corporate manager, senior officer, or subject matter experts upon whom the senior corporate manager or senior officer reasonably relies in making the certification.

Certification of the Program

Purpose: to declare that

- Zoom has established, implemented and maintained the mandated program and other actions required by the FTC Final Order (1)
- There are no known material non-compliance that has not been corrected/ disclosed (2)

Effectiveness: It depends, but generally no.

As the job of senior officer might not fully understand the company’s objective and strategic roles, they might not be a suitable candidate to evaluate the written program.

“The certification must be based on the personal knowledge of the senior corporate manager, senior officer, or subject matter experts upon whom the senior corporate manager or senior officer reasonably relies in making the certification”

- If he is competent, then it may be effective
- However, such internal auditing/compliance can always be subject to bias?

Question?

Thank you!