Tutorial 2: InfoSec Compliance

Part 1: CII Code of Practice

Please read the **Cybersecurity Code of Practice for CII Dec 2019** and answer the following questions.

- True or False questions

1) This Code of Practice specifies the maximum protection policies that a CIIO shall implement to ensure the cybersecurity of its CII.

False - 1.3.1 The Code is specifying the minimum protection policies that CIIO must implement

2) An independent cybersecurity audit of CII should be carried out by the CIIO at least once every 12 months.

False - 2.1.1 requires the CIIO to carry out the independent audit once every 2 years

3) The policies, standards and guidelines for managing cybersecurity risks of CII should be reviewed at least once every 2 years.

False - 3.3.2 requires CIIO to review the policies, standards and guidelines against current CII cyber operating environment and cybersecurity threat landscape every 1 year

4) The penetration test on a CII should be conducted by the CIIO at least once every 12 months from the time of previous penetration test.

False - 5.5.1.b states that OT systems can have up to 24 months (2 years) between each penetration test

5) For a CII which is an IT system, vulnerability assessment should be conducted at least once every 12 months from the time of previous vulnerability assessment.

True - 5.5.1.a 12 months between penetration tests for IT systems

6) For a CII which is an OT system, vulnerability assessment should be conducted at least once every 12 months from the time of previous vulnerability assessment.

False - 5.5.1.b requires for OT systems to conduct penetration testing every 24 months (2 years)

7) CIIO should adopt least-privilege principle for CII access control.

True - 5.2.2.a Security baseline confguration are for least access privilege and separation of duties

8) The CIIO only need to establish cybersecurity awareness program for its own employees.

False - 8.1.1 CIIO must establish a cybersecurity awareness program for employees, contractors, and 3rd party vendors who have access

9) The CIIO should establish process for validating vendor's compliance with cybersecurity requirements in the terms of contract.

True - 11.1.2

10) The CIIO should apply a white-list approach on application security management on CII.

True? - 5.2.2.d removing of unnecessary services

4.1 CIIO must identify all assets and maintain inventory of CII assets identified

Part 2: MAS Technology Risk Management Guideline for Financial Institutions

Please read the **MAS Technology Risk Management Guidelines Jan 2021** and answer the following questions.

- True or False questions

1) It is compulsory for an FI to appoint a Chief Information Security Officer (CISO) or Head of Information Security, with the requisite expertise and experience, to be responsible for the FI's IT security strategy and program.

True - 3.1.3 Requires specific roles to be in

2) For FIs, system security patches should be applied within 7 days.

False - 7.4.1 based on the criticality of the new patch instead of a fixed

3) Strong authentication, such as multiple-factor authentication, should be implemented for users remotely accessing the FI's IT environment.

True - 9.3.1 Remote access is required for access into internal network from

4) Considering the business operation efficiency and flexibility, for application installation on the FI's system, a black-listing approach should be implemented.

False - 11.3.6 recommends application white-listing

5) A unique cryptographic key should be used to generate each type of authentication factors (e.g., key for OTP login, key for transaction-signing code)

True - 10.2.6 requires the diversification of keys so that they can only be used and generated for a single purpose