Ember Lake

CIMA Statement of Guidance & Rule for Cybersecurity Checklist

What is it?

1. "...intended to ***provide guidance to regulated entities*** on cybersecurity..." *(SOG:R 1.1)*
2. "... sets out the Cayman Islands Monetary Authority's ("the Authority") ***minimum expectations*** in relation to the management of cybersecurity risks." *(SOG:R 1.2)*

Who is affected?

1. "This Guidance ***applies to all entities regulated by the Authority*** including controlled subsidiaries as defined in the Banks and Trust Companies Law." *(SOG:R 3.1)*
2. "***Regulated entities are ultimately responsible for ... assessing the service provider(s)' compliance with this Rule*** and the related SOG on Cybersecurity for Regulated Entities;" *(SOG:R 5.4a)*

What are the requirements?

1. "Regulated entities ***must establish, implement, and maintain a documented cybersecurity framework***" *(SOG:C 5.1a)*
2. "A ***well-documented cybersecurity risk management strategy***, (including):" *(SOG:C 5.1b)*
    i. Cybersecurity and IT security policies and procedures
    ii. Clearly identified managerial responsibilities and controls
    iii. Processes for responding to, containing and recovering from cyber attacks, breaches and incidents
3. "***Regularly review the emerging (or evolving) cybersecurity threats and IT landscape and assess their cybersecurity framework*** to ensure that the framework continues to be appropriate" *(SOG:C 5.1c)*

Requirement 1 | *Cybersecurity Framework*

1. Any "***reputable international standards or frameworks on cybersecurity***" can be used. Frameworks referenced and listed include:
    i. National Institute of Standards and Technology (NIST)
    ii. Control Objective for Information and Related Technologies (COBIT)
    iii. Information Technology Infrastructure Library (ITIL) **ITIL based on the ISO 27001 standard*
    iv. International Organization for Standardization (ISO)
2. Implementation of a CSF will help satisfy the rest of the requirements as part of the process
    i. Requires IT Policies & Procedures, parties responsible for the CSF, and constant improvement processes

Requirement 2 | *Cybersecurity Risk Management Strategy*

1. Key Policies and Procedures include:
    - IT Security Program Policy
    - Acceptable Use Policy
    - Business Continuity Policy
    - Cybersecurity Risk & Vulnerability Management Policy
    - Data Breach Policy
    - Data Classification Policy
    - Data Encryption Policy
    - Disaster Recovery Policy
    - Incident Response Policy
    - Remote Access Policy
    - Vendor Management Policy
2. Organizations should ***practice "Defense in Depth" and test, deploy, and inventory technical and procedural controls*** that satisfy the requirements outlined in each of these policies.

Requirement 3 | *Regular Review of Cybersecurity Framework*

1. Perform third-party assessments ***at least annually or whenever major changes have been made to infrastructure***. These assessments include:
    i. Penetration Testing (technical simulation of cyber-attacks to identify vulnerabilities)
    ii. CSF Audit (attestation reports to determine successful and failures of a CSF)
    iii. Cyber Risk Assessment (assessment to check readiness and reaction capabilities of an organization regarding cyber events)
2. Any CSF will require specific third-party assessments performed as part of the implementation process.

Questions? Reach us at **info@emberlake.ky**