# STATEMENT OF GUIDANCE
# Cybersecurity for Regulated Entities

MAY 2020

## List of Acronyms

| | |
|---|---|
| CIMA | Cayman Islands Monetary Authority |
| CIO | Chief Information Officer |
| CISO | Chief Information Security Officer |
| IT | Information Technology |
| DDoS | distributed denial-of-service |
| DoS | denial-of-service |
| MAL | Monetary Authority Law |
| MITMA | man-in-the-middle attack |
| SaSS | Security as a Service |
| SOG | Statement of Guidance |
| WAFs | web application firewalls |

## 1. Statement of Objectives

1.1. This Statement of Guidance ("Guidance") is intended to provide guidance to regulated entities on cybersecurity and to supplement the *Rule - Cybersecurity for Regulated Entities*.

1.2. This Guidance is not intended to be prescriptive, exhaustive or a comprehensive approach to managing cybersecurity related risks; rather this Guidance sets out the Cayman Islands Monetary Authority's ("the Authority") minimum expectations in relation to the management of cybersecurity risks.

## 2. Statutory Authority

2.1. Section 34(1)(a) of the MAL provides that the Authority:

> *After private sector consultation and consultation with the Minister charged with responsibility for Financial Services, the Authority may -*
>
> *issue or amend rules or statements of principle or guidance concerning the conduct of licensees and their officers and employees, and any other persons to whom and to the extent that the regulatory laws may apply;*

2.2. This Guidance should be read in conjunction, where applicable, with the:

(a) Rule - Cybersecurity for Regulated Entities
(b) Rule on Internal Controls – General for all Licensees
(c) Statement of Guidance – Internal Controls in Banks
(d) Statement of Guidance – Internal Controls - Insurance
(e) Statement of Guidance – Internal Controls for Trust Companies, Company Managers and Corporate Service Providers
(f) Statement of Guidance - Internal Controls - Securities Investment Business
(g) Rule - Risk Management for Insurers
(h) Rule on Corporate Governance for Insurers (Insurance)
(i) Statement of Guidance - Corporate Governance
(j) Rule on Operational Risk Management for Banks
(k) Statement of Guidance - Internal Audit – Banks
(l) Statement of Guidance - Internal Audit – Unrestricted Trust Companies
(m) Statement of Guidance - Operational Risk Management for Banks
(n) Statement of Guidance - Business Continuity Management: All Licensees
(o) Statement of Guidance – Outsourcing: Regulated Entities
(p) Statement of Guidance - Nature, Accessibility and Retention of Records

2.3. This document should also be read in conjunction with other regulatory instruments issued by the Authority from time to time.

## 3. Scope of Application

3.1. This Guidance applies to all entities regulated by the Authority[1] including controlled subsidiaries as defined in the Banks and Trust Companies Law. For the purpose of this Guidance, a regulated entity is an entity that is regulated under the:

(a) Banks and Trust Companies Law

[1] Exceptions: regulated mutual funds.

(b) Insurance Law
(c) Mutual Funds Law
(d) Securities Investment Business Law
(e) Building Societies Law
(f) Cooperative Societies Law
(g) Development Bank Law
(h) Money Services Law
(i) Companies Management Law
(j) Directors Registration and Licensing Law
(k) Private Trust Companies Regulations

## 4. Definitions

4.1. For the purpose of this Guidance, any definition used is the same as assigned within the Rule - Cybersecurity for Regulated Entities ("Rule"), unless otherwise specified below.

a) **CIO:** Chief Information Officer

b) **CISO:** Chief Information Security Officer

c) **Cloud computing:** A model for enabling on-demand network access to a shared pool of configurable IT capabilities/ resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.

d) **Criticality classification:** Method for identifying and prioritizing information systems and components.

e) **Cyber risk:** The risk of financial loss, operational disruption, or damage, from the failure of the digital technologies employed for informational and/or operational functions introduced to a manufacturing system via electronic means from the unauthorized access, use, disclosure, disruption, modification, or destruction of the manufacturing system.

f) **Cybersecurity event:** A cybersecurity change that may have an impact on organisational operations (including mission, capabilities, or reputation).

g) **Cybersecurity incident:** A cybersecurity event that has been determined to have an impact on the organization prompting the need for response and recovery.

h) **Cybersecurity threat:** Any circumstance or event with the potential to adversely impact organizational operations, organizational assets, individuals, other organizations, or the Country through a system via unauthorized access, destruction, disclosure, modification of information, and/or denial of service.

i) **Information system assets:** refer to data, systems, network devices and other IT equipment.

j) **Risk tolerance:** The degree of risk of a negative event relating to cybersecurity that a regulated entity is willing to accept.

## 5. General Guidance

5.1. Regulated entities face many varied risks relating to their use of information technology. This Guidance seeks to provide information to regulated entities on the Authority's expectations specifically related to cybersecurity risks. However, the Authority encourages regulated entities to consider all information technology ("IT") associated risks as part of their broader risk management efforts.

5.2. Regulated entities should implement this Guidance in proportion to the risks, size, nature and complexity of their business, following an appropriate assessment of their IT risks including cybersecurity.

5.3. As part of their cybersecurity risk management efforts, regulated entities should conduct regular self-assessments of their cybersecurity framework against this Guidance, the related Rule, any other reputable standard used to develop their framework and any emerging trends in cybersecurity, at a minimum, annually.

5.4. Regulated entities can consider reputable international standards or frameworks on cybersecurity, IT Security and Technology Risk Management (TRM) in developing an appropriate cybersecurity risk management framework or their risk profile and risk tolerance. The National Institute of Standards and Technology (NIST), Control Objective for Information and Related Technologies (COBIT), Information Technology Infrastructure Library (ITIL) and International Organization for Standardization (ISO) are some examples of recognised standards in these areas but the reference made to them in this Guidance should not be deemed as an endorsement by the Authority of any one standard or framework. Future standards/frameworks may emerge that are reputable and regulated entities should consider any and all standards/frameworks that help them develop the most robust and prudent cybersecurity framework to meet their needs and those of their clients.

5.5. Regulated entities that are natural persons should ensure that services offered to clients are not carried out in such a way that compromises the confidentiality, integrity and availability of clients' data or the regulated entities' systems, where applicable, and the Rule along with this Guidance should be considered and applied, where applicable.

## 6. Cybersecurity Framework

6.1. Regulated entities' cybersecurity frameworks should, at a minimum, consider the elements contained within this Guidance and comply with the related Rule, if applicable.

6.2. Regulated entities' cybersecurity frameworks should include appropriate documented strategies, policies and procedures. Regulated entities should ensure that these cybersecurity-related policies and procedures include or refer to enforcement and disciplinary actions for non-compliance.

6.3. The cybersecurity framework should be appropriate, having regard to the size and complexity of regulated entities' and the nature of their cyber risk exposures.

6.4. The cybersecurity framework of a regulated entity should contain mechanisms to ensure that the regulated entity has appropriate and sufficient resources in place to oversee and manage its cybersecurity and information systems.

6.5. The cybersecurity framework should set out the regulated entity's tolerance level or risk limit relating to cybersecurity risk. This risk tolerance should be approved by the governing body.

6.6. The business objectives and cybersecurity strategies developed by regulated entities should coincide with their governing body's approved risk appetite and tolerance levels and consumer/client protection responsibilities.

6.7. Regulated entities should ensure that there is an internal audit function or some alternative objective assessment option in place that can provide independent assurance to their governing body and senior management in respect of their cybersecurity framework, regularly and in a timely manner, including key cyber-vulnerabilities, plans to remedy vulnerabilities and the level of resources applied to cybersecurity. The internal audit process should be driven by the regulated entities' internal audit policies and procedures.

6.8. Regulated entities should make every effort to improve their level of resilience to cyber attacks as well as their ability to respond and recover from any actual cyber incidents by protecting interconnections and other means of access to insider and outsider threats to their business.

## 7. Cybersecurity Risk Management

7.1. A regulated entity's cybersecurity risk management strategy should involve putting measures in place to ensure the confidentiality, integrity and availability of its data and systems.

7.2. The following key components should, at a minimum, be considered by regulated entities in their cybersecurity risk management efforts:

a) **Risk Identification:**

i. Identification and criticality classification of information systems. Identify and maintain an up-to-date physical inventory of all assets including computers, servers, routers and switches, as applicable.

ii. Identification and assessment of current and emerging threats, risks and vulnerabilities as well as the impact and likely impact to its IT environment which comprises internal and external networks, hardware, software, applications, data, processes, systems interfaces, operations and human elements.

iii. Maintenance of an inventory of cybersecurity risks and applicable controls.

b) **Risk Assessment and Protection:**

i. Establishment of an appropriate policy and processes to conduct regular and comprehensive cybersecurity risk assessments that consider people (i.e. employees, customers and other external parties), processes, data, and technology across all its business lines and geographies, as applicable.

ii. Analysis and evaluation of the probability of and potential impact and consequences of the identified cybersecurity risk exposure on regulated entities' overall business and operations should an adverse event occur.

iii. The approach and key assumptions made when measuring cybersecurity risks should be clearly documented.

iv. Establishment of cybersecurity risk mitigation and control strategies that align with regulated entities' business strategy, value of their information assets, risk tolerance and client interests.

v. Assessment of cyber threats to the continuity or operations of regulated entities resulting from internally managed functions, and outsourced arrangements and critical IT service providers.

vi. Consideration for securing insurance against various cybersecurity risks including recovery costs and compensation.

vii. A clear policy should be in place to detail the level of protection required based on the risk and criticality rating of the information system. The policy should consider appropriate safeguards to ensure critical products and services are available as well as the regulated entity's ability to prevent, mitigate or contain the impact of a potential cybersecurity event. Evidence of protection should be supported by risk or business impact assessments.

c) **Risk Monitoring and Reporting:**

i. Implementation of documented monitoring/surveillance and detection policies, techniques and systems that allow real-time monitoring and detection of threats (examples include, but are not limited to, firewalls, web application firewalls (WAFs), network behaviour analysis, anti-virus, and third-party monitoring tools).

ii. The monitoring/surveillance system should alert the regulated entity to any abnormal IT system activities, transmission errors, cyber attacks or unusual online transactions.

iii. Continuous monitoring of emerging cybersecurity threats such as denial of service attacks, internal sabotage and malware infestations to facilitate prompt detection of intrusion attempts, unauthorised or malicious activities by internal and external parties.

iv. Monitoring and development of cybersecurity metrics, considering such things as risk events, regulatory requirements and audit findings, to highlight systems, processes or infrastructure that have the highest risk exposure.

v. On-going reporting to the governing body of significant risks, associated status of containment and recovery actions and plans including recommendations on how to mitigate for similar events in the future.

vi. Completing periodic reviews and updates of regulated entities' cybersecurity risk management processes, re-evaluating past risk-control methods with improved testing as well as assessing the adequacy and effectiveness of their cybersecurity risk management processes.

d) **Incident Response:**

i. Documented policies and procedures for responding to cybersecurity incidents. In developing these policies and procedures, regulated entities should consider the four major phases of the incident response process: preparation; detection and analysis; containment, eradication and recovery; and, post-incident activity.

ii. Incident response management should be designed to allow for rapid response to all levels of cybersecurity incidents, highlighting material cyber incidents and it should include escalation criteria that align with its cybersecurity criticality classification. Appropriate response plans should be established for various cyber and data loss events ranging from minor cyber incidents to major incidents that result in breach, data loss, compromised data or destroyed data.

iii. Appropriate response plans for incidents such as denial of service attacks that prevent end-users from accessing the system.

iv. Incident management processes should ensure that the following tasks are fully completed before an incident is considered closed formally (1) recovery from disruption of series from cybersecurity incident, (2) assurance of the IT system's integrity following the cybersecurity incident, and (3) recovery of lost or corrupted data due to the cybersecurity incident.

v. Clear roles and responsibilities of staff involved in the incident management process which includes recording, analysing, remediating, and monitoring incidents.

vi. An appropriate log should be maintained (or audit trail system implemented) that would allow for effective and efficient investigations relating to cybersecurity events.

vii. Establish a post-incident response review process for material cybersecurity incidents which should include:
   (a) conducting appropriate cyber forensic investigations;
   (b) chronicling the events leading up to, during and following the cybersecurity incident;
   (c) identifying the root cause and control deficiencies;
   (d) assessing any breakdown in the incident management process; and
   (e) establishing of a plan of action to address the identified deficiencies.

viii. Document, implement and communicate to relevant staff an escalation process for reporting on IT and cybersecurity issues within established timeframes. These timeframes should be driven by the severity and urgency of the identified issue.

e) **Containment and Recovery:**

i. Establish appropriate containment and recovery policies and procedures to deal with cybersecurity events that may prevent access to data, disrupt the availability of the IT system or results in data loss.

ii. Ensure that the containment and recovery plan allow regulated entities to resume operations responsibly, while continuing their remediation efforts, including the:
   (a) elimination of harmful remnants of the incident or event;
   (b) restoration of systems and data to normal and confirming normal state;
   (c) identification and mitigation of all vulnerabilities that were exploited;
   (d) remediation of vulnerabilities to prevent similar incidents; and
   (e) appropriate internal and external communication.

## 8. Review of the Information Systems and Cybersecurity Framework

8.1. Regulated entities should regularly review the cybersecurity and IT risks and assess their cybersecurity framework to ensure they continue to be appropriate to manage adverse impacts of the cyber risks and IT risks on the regulated entities' business.

8.2. The cybersecurity framework should include a "feedback loop" which ensures transparency and allows the governing body and senior management to take necessary action in response to changes in the IT and cybersecurity risk profile of regulated entities, particularly between the governing body and the designated Chief Information Officer (CIO) or Chief Information Security Officer (CISO) where such positions exist in regulated entities or some other similar position that would be responsible for liaising with the governing body. The feedback loop will also ensure that decisions made by the governing body and Senior Management are implemented and their effects monitored to determine whether they are in fact appropriate.

8.3. The cybersecurity framework should be tested on a periodic basis for effectiveness and updated or amended as needed

## 9. IT System Controls and Use of the Internet

9.1. **IT System Controls:**

a) Regulated entities should establish documented policies and baseline standards to facilitate consistent application of security configurations to operating systems, databases, network devices and enterprise mobile devices within the IT environment.

b) Regulated entities should implement:

i. physical and logical access security to allow only authorised staff to access their internet operations and IT systems.

ii. appropriate processing and transmission controls to protect the integrity of their systems and data.

c) Regulated entities should ensure that their personnel, responsible for supporting internet operations, IT systems and cybersecurity, have their duties and access to IT systems, databases and applications resources scrutinized with clear segregation of duties in place.

d) Regulated entities should establish a control framework around the management of their IT system that should comprise of the governance structure, processes and procedures for change management, software

release management, incident and problem management as well as capacity management.

e) Regulated entities should ensure that clear audit trails exist for all internet transactions. Effective internal controls should be in place in highly automated environments and these controls should be independently audited, particularly for all critical internet events and applications.

f) Regulated entities should develop a technology refresh plan[2] to ensure that IT infrastructure is properly supported, up-to-date and replaced in a timely manner, as needed.

g) Regulated entities should ensure that maintenance and repairs relating to IT infrastructure are performed in accordance with entities' policies and procedures. Maintenance and repairs should be appropriately approved and logged and performed in a manner to prevent unauthorised access.

h) Regulated entities should carry out vulnerability assessments and realistic penetration tests that replicate sophisticated, current attacks based on current and targeted threat intelligence, having regard to the size and complexity of their business, and the nature of regulated entities risk exposures. Such assessments and testing should, at a minimum, be carried out annually or more frequently depending on if major changes to defences are made or threats perceived. The assessments and testing should also include, but not be limited to (as applicable):

   i. Regular vulnerability hardware and software scans and testing of client servers and network infrastructure to identify security control gaps.

   ii. Regular penetration testing of the network boundary (e.g. open network entry and exit points) to identify security control gaps.

   iii. Regular testing with third party cyber-mitigating services.

   iv. Regular cyber attack (including distributed denial-of-service [DDoS] and phishing attacks) and recovery simulation exercises.

   v. Consideration of the impact of an internet outage across the Cayman Islands for an extended period of time on their assessment, testing and risk assessment generally.

i) Regulated entities should establish baseline standards to facilitate consistent application of security configurations to operating systems, databases, network devices and enterprise mobile devices within the IT environment.

j) Regulated entities should install network security devices, such as firewalls as well as intrusion detection and prevention systems, at critical junctures of their IT infrastructure to protect their network perimeters. Regulated entities should deploy firewalls, or other similar measures, within internal networks to minimise the impact of security exposures originating from

[2] Technology refresh is the cycle of regularly updating key elements of an IT infrastructure to maximise system performance.

third party or overseas systems (i.e. running codes that are developed by an overseas firm), as well as from the internal trusted network.

k) Payment systems and Card Payment Cards

i. Regulated entities, that accept, store, process, and/or transmit cardholder data should maintain a secure environment and ensure that they are *Payment Card Industry Data Security Standard* compliant.

ii. Regulated entities should implement IT security measures that apply to their participation in payment systems including point of sale terminals; online services and payments (inclusive of mobile platforms); and other emerging technologies, as applicable.

iii. Regulated entities should conduct a risk assessment to identify possible fraud scenarios with respect to the issuance of payment cards and put in place appropriate measures to counteract payment card fraud via mobile devices.

9.2. **Use of the Internet:**

a) Regulated entities should establish suitable policies and controls to:

i. guard against potential attacks or minimise the impact of such attacks and cybersecurity incidents on their internet systems where they provide financial services online and clients transact online; and

ii. ensure that transactions performed over the internet as well as online login credentials, passwords, personal identification numbers and other sensitive personal or account information are adequately protected and authenticated and secured against exploits such as account takeovers, automated teller machine skimming, card cloning, hacking, phishing and malware.

b) Regulated entities should properly evaluate security requirements associated with their Internet systems and adopt encryption algorithms, which are of well-established international standards and subjected to rigorous scrutiny.

c) Regulated entities should consider the deployment of a two-factor authentication at login for all types of online financial systems and transaction-signing for authorising transactions.

d) Regulated entities should maintain high resiliency and availability of online systems and supporting systems; and should put in place measures to plan and track capacity utilisation as well as guard against online attacks such as denial-of-service attacks (DoS attack) and distributed denial-of-service attacks (DDoS attack).

e) Regulated entities should take appropriate measures to minimise exposure to other forms of cyber attacks such as Business E-mail Compromise schemes also known as middleman attacks, man-in-the-middle attack (MITMA), man-in-the browser attack or man-in-the application attack.

f) Regulated entities should ensure that adequate information is provided on their websites to allow potential customers to make an informed assessment about the institution's identity, in particular, the physical

address of the regulated entity and its head office. As a matter of best practice regulated entities should state that they are regulated by the Authority and the home supervisor, where applicable. There should be a prominent notification of this on the web pages displayed prior to entering into any internet transaction.

## 10. Accountability

10.1. The duties and responsibilities of the governing body and senior management relating to cybersecurity should include, but not be limited to:

a) Ensuring that a sound and robust cybersecurity framework is established and maintained and taking accountability for and ownership of the framework and the financial resources for the framework. They should also be involved in key IT decisions.

b) Approving appropriate programmes, policies and procedures for cybersecurity, cyber resilience and IT management.

c) Ensuring that effective internal controls and cybersecurity risk management practices are implemented to achieve on-going security, reliability, resiliency and recoverability.

d) Properly assessing cost-benefit issues, including factors such as reputation, customer confidence, consequential impact and legal implications, regarding investment in controls and security measures for computer systems, networks, data centres, operations and backup facilities. The costs associated with managing cybersecurity risks should be balanced against resulting benefits while maintaining operational and financial stability.

e) Ensuring that management supports the senior officer accountable for cyber resilience by the creation, implementation, testing and ongoing improvement of cyber-resilience plans, which are appropriately harmonised across the business.

f) Ensuring that a formal, independent cybersecurity and cyber resilience review/audit of the organisation is carried out periodically, taking into consideration the size, nature and complexity of the entity.

10.2. The governing body is responsible for:

a) Establishing a well-documented comprehensive cybersecurity training programme for the Governing body to help ensure it has the requisite knowledge to competently exercise its oversight function and assess the adequacy and effectiveness of the overall cyber resilience programme.

b) Overseeing cybersecurity and cyber-resilience. The Governing body may, as necessary, delegate primary oversight activity to an existing committee (e.g. the risk committee) or a new committee (e.g. a cyber-resilience committee).

c) Having a good command of cyber risks and the cybersecurity environment including regular training in this regard. Governing body members should receive orientation on joining the entity and receive regular updates on recent threats and trends.

d) Holding management accountable for reporting a quantified and

comprehensive assessment of cyber risks, threats and events as a standing agenda item during its meetings.

e) Ensuring that one senior officer is appointed who is accountable for reporting on the regulated entity's capability to manage the implementation of the cybersecurity framework and cyber resilience programme. The governing body should ensure that this officer has regular access to the governing body, sufficient authority, command of the subject matter, experience and resources to fulfil these duties.

f) Ensuring that management integrates cyber resilience and cyber risk assessments into the overall business strategy and enterprise-wide risk management, as well as budgeting and resource allocation.

g) Annually defining and quantifying the business risk tolerance relative to cybersecurity and cyber-resilience and ensuring that this is consistent with the strategy and risk appetite.

h) Carrying out periodic reviews of its own performance in the implementation of the cybersecurity framework and cyber resilience and/or seeking independent advice for continuous improvement.

10.3. Senior management is responsible for:

a) Developing, implementing and monitoring the cybersecurity framework by documenting appropriate policies and procedures and controls relating to cybersecurity, cyber-resilience and IT system controls.

b) Ensuring that the appointed senior officer (e.g. CIO or CISO) has access to the governing body so that there is clear and ready communication to keep the governing body apprised of the regulated entity's potential cyber-risks, current threats, incidents or attacks that are deemed material as well as any necessary changes to the regulated entity's cybersecurity framework and IT systems.

## 11. Intra-Group

11.1. With respect to regulated entities that are a part of a group structure, the expectations in this Guidance may be addressed within group-wide processes, policies or plans, provided that any specific cybersecurity risks that the regulated entities are exposed to are properly mitigated, and the Governing Body is able to fulfil its accountabilities under section 8 of this Guidance and to clients.

11.2. Regulated entities that rely on a group cybersecurity framework, should receive written confirmation of certain details regarding the framework including, at a minimum:

a) a declaration that an appropriate cybersecurity framework has been implemented that considers and mitigates any risks to the regulated entities;

b) agreement that the regulated entities can provide input in developing or revising the framework in respect of their needs and the needs of their clients, as necessary;

c) receipt of sufficient information to satisfy themselves that the group's framework aligns with their business strategy, risk tolerance, clients' needs

and that the cyber risks and threats are properly assessed, monitored, managed and mitigated and allow for appropriate containment and recovery;

d) ability to request additional information, as necessary to identify and monitor any group wide risk that may impact the regulated entities as well as their own identified cybersecurity risks;

e) agreement that protective technologies will be made available to assist with monitoring, assessing, detecting, as necessary;

f) details of any outsourced IT- or cyber-related matters that may directly impact the regulated entity's business and cyber risks including pertinent details as outlined in Section 13 of this Guidance;

g) the end-of-support dates or replacement of any technology that may impact the regulated entity's cybersecurity; and

h) appropriate third-party contracts and service level agreements are in place.

11.3. The Authority recognises that the oversight of outsourcing arrangements in relation to regulated entities that are branches, may differ from arrangements in other regulated entities, given the different legal structure of a branch. Branches may be covered by outsourcing arrangements entered into by their head office, however, the regulated entities remain ultimately responsible for their cybersecurity. When that is the case, regulated entities should assess the applicability of the various elements of this Guidance and the corresponding Rule bearing in mind the cybersecurity risks posed to their operations and clients by the outsourcing arrangement and ensure compliance with this Guidance and the corresponding Rule as well as the *Statement of Guidance - Outsourcing*. In particular, regulated entities that are branches should maintain an inventory of their own assets and a log that confirms their cyber-incidents, threats and attacks so that they can properly assess the Group-wide mitigation, containment and recovery efforts to allow them to mitigate their cybersecurity risk and enhance their preventative efforts in the future.

## 12. Employee Selection, Training and Awareness

12.1. **Selection of Employees and Third-Party Service Providers**
Regulated entities should implement a comprehensive and effective screening process, with stringent selection criteria to ensure careful selection of staff, vendors and contractors who support technology functions and minimise cyber risks due to system failure, internal sabotage or fraud.

12.2. **Senior Officer Appointment (Chief Information Security Officer/Chief Information Officer)**

a) A suitable senior officer such as a CISO, CIO or some other similar position should be appointed to oversee the cybersecurity framework of the regulated entity and have responsibility for liaising with the Governing body, following best practices and staying current with all related technologies, and cybersecurity trend.

b) The appointed senior officer (e.g. CIO or CISO) should be suitably qualified, experienced and have a good understanding and knowledge of IT systems and cybersecurity.

c) The appointed Senior person (e.g. CIO or CISO) should be provided with sufficient delegated operational authority to carry out his or her role.

12.3. **Training and Awareness[3]:**

a) Regulated entities should have a formalised plan to provide ongoing technical training to their cybersecurity personnel and IT unit/team (including those involved in developing, maintaining and operating websites and systems) on IT systems and current and emerging cybersecurity subject areas as well as security principles to ensure that they are knowledgeable and aptly trained for their specific IT or cybersecurity roles and functions.

b) Regulated entities should make every effort to ensure that they regularly, disseminate cybersecurity information to their clients or any other action to help increase their clients' level of cybersecurity awareness.

c) Regulated entities should ensure that all staff are trained to understand at a minimum the cyber risks to which the entity is exposed and the mitigating measures employed to reduce the occurrences of cyber incidents. The CIO, CISO or other similarly appointed senior person should ensure that there is enterprise-wide on-going training to new and existing staff on cybersecurity to ensure increased awareness and enterprise-wide efforts to prevent or minimise cyber-attacks and cyber-incidents.

d) Regulated entities' training programmes should ensure that their governing bodies are equipped with the requisite knowledge to competently exercise the oversight function and appraise the adequacy and effectiveness of the regulated entities' overall cyber resilience programmes.

e) Regulated entities should ensure cybersecurity policies and procedures are communicated to senior management and staff at all levels and training is conducted on a regular basis.

## 13. IT Outsourcing Arrangements

13.1. The Authority expects that the ultimate responsibility and accountability for outsourcing arrangements and other third-party dependencies, supporting or potentially negatively impacting Internet activities and IT systems, remain with regulated entities; and material outsourcing arrangements, including critical IT service providers, should be approved by their governing body.

13.2. Where regulated entities outsource to a professional security service provider, (e.g. provide 'Security as a Service' ("SasS") firm), mechanisms should be in place to allow the governing body and Senior management to ensure that cybersecurity is being properly monitored in a secure manner at a secure site and deficiencies addressed in a timely manner. This Guidance, the outsourcing requirements noted in the Rule and other relevant measures should be complied with. Regular reports by the third party service provider should be circulated to the governing body and senior management on a regular basis.

[3] Training seeks to teach skills, which allow a person to perform a specific function, while awareness seeks to focus an individual's attention on an issue or set of issues. (Source: NIST Special Publication 800-16)

13.3. Given that outsourcing arrangements could change the cybersecurity risk profile of regulated entities, including critical IT service providers, the following steps should be considered:

a) Prior to the appointment of a service provider, carry out due diligence to determine the viability, capability, reliability, track record and financial position of these service providers. The due diligence process should include any related subcontracting arrangements.

b) Contractual terms and conditions governing the roles, relationships, obligations and responsibilities of all service providers should be set out fully in written agreements. The requirements and conditions covered in the agreements generally include performance targets, service levels, availability, reliability, scalability, compliance, audit, security (including cybersecurity), data protection, reporting requirements (e.g. incidents), contingency planning, disaster recovery capability and backup processing facility.

c) The contractual agreements with the service provider should confirm that the Authority or its authorised agent can perform an assessment of the service provider's IT systems and cybersecurity control environment associated with the outsourced service(s) being carried out on behalf of the regulated entity.

d) Regulated entities should require the service provider to have or implement cybersecurity policies, procedures and controls that are at least as stringent as it would expect for its own operations.

e) Regulated entities should monitor and review the security policies, procedures and controls of the service provider on a regular basis, including commissioning or obtaining periodic independent audits on cybersecurity adequacy and compliance in respect of the operations and services provided.

f) The outsourcing agreement should require the service provider to have or develop and establish a cybersecurity incident recovery contingency framework which defines its roles and responsibilities for documenting, maintaining and testing its contingency plans and recovery procedures.

g) The service provider's disaster recovery plan for regulated entities should be reviewed, updated and tested periodically to reflect changes in technology, cybersecurity and operational requirements. The plan should take into account worse case disruption scenarios, unavailability of existing service provider, and should identify viable alternatives for resuming IT services. Regulated entities should ensure that the plan is shared with relevant stakeholders (e.g. relevant business units, call centres, senior management, Governing body etc.) who are sufficiently trained on the recovery plan execution steps.

h) Regulated entities should ensure that there is an exit strategy in place in the event of termination of the relationship.

13.4. Regulated entities should be able to apply the Rule and this Guidance to any of their material outsourcing arrangements including their critical IT service providers as if it were not an outsourced function or service.

13.5. Regulated entities should implement processes to monitor the levels of cyber risk preparedness for material outsourcing arrangements and critical IT service providers.

13.6. Regulated entities should have processes in place to ensure the timely notification of cyber-incidents from their service providers with which they have one or more material outsourcing arrangements and their critical IT service providers.

13.7. Regulated entities should conduct a risk assessment with respect to the jurisdiction(s) that potential material outsourcing arrangements and critical IT service providers are in, if outside the Cayman Islands, and appropriately mitigate any identified cybersecurity risks, as necessary.

13.8. Regulated entities should regularly assess their aggregate exposures relating to material outsourcing arrangements and critical IT service providers and effectively mitigate and manage any vulnerabilities, threats and cyber risks that may result from the outsourcing arrangement or critical IT service provider(s).

13.9. Regulated entities should maintain a centralised log of all their material outsourcing arrangements and critical IT service providers, which should be updated on an ongoing basis. The Authority should have access to the log at any time upon request.

13.10. Some regulated entities may choose to rely on cloud computing in their IT system architecture. The Authority considers the use of cloud computing to be a form of outsourcing. As such, in performing their due diligence for all forms of outsourcing arrangements, regulated entities should be aware of cloud computing's unique attributes and risks especially in areas of data integrity, sovereignty, commingling, platform multi-tenancy, recoverability and confidentiality, regulatory compliance, auditing and data offshoring.

13.11. Where a cloud computing service provider adopts multi-tenancy and data commingling architectures to process data for multiple customers, regulated entities should consider cloud computing service providers' abilities to isolate and clearly identify their customer data and other information system assets for protection.

13.12. In the event of contract termination with a cloud computing service provider, either on expiry or prematurely, regulated entities should have the contractual power and means to promptly remove or destroy data stored at the service provider's systems and backups.

13.13. Regulated entities should verify the cloud computing service provider's ability to recover the outsourced systems and IT services within the stipulated recovery time objective prior to contracting with the service provider.

13.14. In all cases of outsourcing, a regulated entity should satisfy itself that the service provider is carrying out its functions in compliance with applicable laws, regulations, and relevant regulatory measures, where applicable.

## 14. Data Protection

14.1. Regulated entities should implement policies, procedures, internal control mechanisms and training that:

a) support the protection of privacy of clients' personal information and sensitive

personal information, including preventing or minimising the misuse or inappropriate communication of personal information to third parties; and

b) assess the cyber risks that may result in a failure to protect the privacy of personal information including any exposures relating to the use of third-party providers.

14.2. Regulated entities should establish suitable response measures, where a failure to protect the privacy of personal information occurs, including matters such as timely notification to affected customers and relevant competent authorities.

14.3. Regulated entities should comply with applicable local and international data protection laws and regulatory requirements to ensure protection of sensitive and confidential information at all points along the flow of data. This includes data at endpoint (such as end user devices – mobile, notebooks, personal computers, and removable media), data in transit (data flowing in networks or between sites) and data at rest (data stored in databases, servers, on backup media and in storage platforms).

14.4. Regulated entities should ensure that endpoint devices protect confidential information stored on the devices with strong encryption. There should be appropriate controls to address the risks of data theft, data loss and data leakage from endpoint devices, customer service locations and call centres.

14.5. Regulated entities should, as much as possible, avoid the use of unsafe internet services such as social media sites, cloud-based internet storage sites, and web-based emails to communicate or store confidential information. Appropriate control measures should be in place to prevent and detect the use of such services within regulated entities or to report issues with such services should they be employed.

14.6. Whenever confidential data is exchanged internally or externally, regulated entities should take appropriate measures to send information via encrypted channels (e.g. via encrypted mail protocol) or encrypting the email and the contents using strong encryption with adequate key length. The encryption key should be sent via a separate transmission channel to the intended recipients. Alternatively, regulated entities may choose other secure means to exchange confidential information with their intended recipients.

14.7. Confidential information stored on regulated entities' IT systems, servers and databases should be encrypted and protected through strong access controls, and restricting access on a least privilege basis[4].

14.8. Regulated entities should assess various methods by which data could be securely removed from storage media and implement measures to prevent the loss of confidential information through the disposal of IT systems.

14.9. Regulated entities should ensure that sensitive or confidential information stored on and accessed by mobile devices should be encrypted to ensure the confidentiality and integrity of this information in storage and transmission.

14.10. Regulated entities should ensure that the processing of sensitive or confidential transaction and customer information occurs in a secure environment.

[4] Least privilege is defined as assigned privileges on a "need-to-have" basis.

14.11. Regulated entities should take steps to educate customers on security measures to protect their own mobile devices from viruses and other errant software which could lead to malicious damage and have harmful consequences.

## 15. Cybersecurity Framework Review by the Authority

15.1. The Authority incorporates cybersecurity and IT system reviews in its examination/inspection procedures.

## 16. Notification Requirements

16.1. In the case of loss of financial assets, personally identifiable data, or any other information covered under an applicable data protection law, regulated entities should communicate to affected individuals, the Authority and the Ombudsman, where applicable as quickly as possible or within appropriate time standards established by the regulated entities or applicable data protection laws.

16.2. The Authority requires that regulated entities provide regular updates to the Authority as new information becomes available, and until all material details about the incident have been provided.

16.3. Until the incident is contained or resolved, the Authority expects regulated entities to provide situation updates to the Authority, including any short term and long-term remediation actions and plans.

16.4. Depending on the severity, impact and velocity of the incident, the Authority may require that regulated entities report using a specific method and at a specific frequency.

16.5. Once regulated entities have contained and recovered from the incident, they should complete a post incident review documenting lessons learned and the plan of action to address identified deficiencies and IT controls. This documented review should be made available to the Authority upon request.

16.6. Notification of internal business systems, may, at the discretion of the regulated entities, be withheld providing such lack of notification has no financial or personal impact on the regulated entities' customers.

## 17. Effective Date

17.1. This Guidance will come into effect within six months of the date that it is published in the Gazette.