SUMMARY OF PRIVATE SECTOR CONSULTATION AND FEEDBACK STATEMENT
Rule and Statement of Guidance – Cybersecurity for Regulated Entities

Section of Proposed Measure	Comments from the Private Sector	Authority's Response	Consequent Amendments to the Proposed Measure
RULE			
2.2(a)	Should include the long form of the new guidance on "Cyber Security For regulated entities".	The recommendation is noted.	The document will be updated to include the full name of the corresponding guidance in all instances.
2.3	Which investments specifically?	The regulatory instruments to which the document refers are regulatory measures issued by the Authority.	No amendment required.
3.2	Is all data treated the same - regardless of value. Consider using classifying data and only driving action on information which has value.	It is the Authority's expectation that regulated entities carryout due care with regard to data of all their clients.	No amendment required.
	"Services offered to clients are not carried out in such way which may compromise the confidentiality, …. The Rule on Cybersecurity along with the corresponding Guidance on Cyber security " Suggest that references to documents should be spelled out as the documents are titled to avoid any ambiguity.	Noted.	The document will be updated to include the full name of the corresponding guidance in all instances.
	Suggest rewording the last section. … "where applicable to ensure that there is a <u>suitable and</u> robust cybersecurity framework in place.	The Authority notes and agrees with this suggestion. The proposed measure has been amended as recommended.	Amended.

Section of Proposed Measure	Comments from the Private Sector	Authority's Response	Consequent Amendments to the Proposed Measure
4	In relation to the definition of "Cybersecurity Framework", whilst it may be possible to mitigate "Cyber-risks" or a "Cybersecurity breach", it is unlikely that the regulated entity will be able to mitigate a "Cyber-attack" which would be entirely outside the regulated entity's control.	It is the expectation of the Authority that regulated entities have controls in place to respond to and recover from cyber attacks. The measure will be updated to reflect this.	The definition of the term "cybersecurity framework" has been updated to read as follows: *"A complete set of organizational resources including policies, staff, processes, practices and technologies used to assess and mitigate cyber risks;* ***and respond to and recover from cyber attacks****."*
4.1	Many of the definition differ from the Internationally accepted ones - suggest that CIMA doesn't create its own definitions but re-uses those of an organization like NIST or ISO	The definitions contained in the measure are adopted from the Glossary of Key Information Security Terms published by the National Institute of Standards and Technology in the U.S. Department of Commerce ("NIST").	No amendment required.
	Often within the document Cyber-risk, Cyber-attack, cyber-space, is not hyphenated - if the author wishes to use hyphens for these areas suggest making changes throughout.	The Authority notes this suggestion and accepts this recommendation. The document has been revised to ensure the consistency of terms used throughout.	The document has been updated to remove the hyphenations throughout.
	Suggest re-ordering with e) at the top then d) then c) then g) then b) all others can maintain order.	The list has been prepared alphabetically for ease of reference.	No amendment required.
	4.1.a) should be a successful breach with material impact. The current definition would mean even a detected and cleaned piece of malware would be a breach.	The Authority considers any unauthorised penetration of an entity's cybersecurity system as a breach. The definition has been revised to reflect this consideration.	The definition for the term "cybersecurity breach" has been updated to read as follows: *"****Any unauthorised*** *penetration of the defences established to protect against cyber risk."*

Section of Proposed Measure	Comments from the Private Sector	Authority's Response	Consequent Amendments to the Proposed Measure
	Cybersecurity breach, definition is too narrow. Suggest expanding to include internal intentional acts.	"Defences" in the definition refers to both internal and external protection mechanisms. The document has been updated to include a footer to indicate this.	Amended.
	Cyber- Resilience definition only covers some of the aspects of resilience - suggest using the NIST definition.	While there is no specific definition for "cyber resilience", NIST defines the term "information systems resilience" as follows: *The ability of an information system to continue to: (i) operate under adverse conditions or stress, even if in a degraded or debilitated state, while maintaining essential operational capabilities; and (ii) recover to an effective operational posture in a time frame consistent with mission needs.* The definition proposed in this measure captures the elements outlined here.	No amendment required.
	Re damage, suggest specifying financial or reputational.	The suggested amendment is noted however, the Authority concludes that the amendment will not change the substance of the requirement.	No amendment required.
5.1(a)	Suggest to reword: Regulated entities must establish, implement and maintain a documented cyber security framework that is designed to promptly identify, measure, assess, report, monitor and control or minimize cyber security risks as well as respond to and recover from cybersecurity breaches which could have a material impact on their operations.	The Authority agrees with the proposed revision. The proposed measure has been updated as recommended.	Amended.
5.1(b)(ii)	Suggest including respond to and recover from breach	The Authority agrees with the suggested revision.	Section 5(b)(iv) has been updated to read as follows: *"clear, **documented** and effective processes for*

Section of Proposed Measure	Comments from the Private Sector	Authority's Response	Consequent Amendments to the Proposed Measure
			***responding to**, containing and **recovering from cyber attacks, breaches** and incidents as quickly as possible or within regulated entities' Governing body approved Recover Point Objective or Recovery Time Objective depending on the type of attack or incident."*
5.1(b)(iv)	Suggest adding that the processes should be tested on a periodic basis.	The Authority notes that while this suggestion promotes best practices, is suggestion, however the measure is not intended to be prescriptive.	No amendment required.
5.1(b)(iv)	RTO & RPO - are done by business service there are never a separate measurement for Cyber Security. Does the regulator not have instruments that define DR and BCP requirements? it would seem more appropriate to be in there.	The explicit inclusion of the 'recovery point objective' and the 'recovery time objective' processes is at the discretion of each regulated entity. It is not the Authority's intention to prescribe the methodology to be employed by regulated entities.	No amendment required.
5.1(c)	Suggest rewording - Regulated entities must regularly review the <u>emerging (or evolving) cybersecurity threats and information technology landscape.</u>	The Authority agrees with the proposed revision. The proposed measure has been updated to reflect the recommendation.	Section 5.2(c) has been updated to read as follows: *"Regulated entities must regularly review the **emerging (or evolving) cybersecurity threats and information technology landscape** and assess their cybersecurity framework"*
5.2(a)(i)	No definition provided of the contents of these documents - definition is required - I'd also suggest a Current Operating Model and Target Operating Model.	The Rule is not intended to be prescriptive on any particular methodology. The requirement for risk management strategies are set out in the Statements of Guidance on Corporate	Amended.

Section of Proposed Measure	Comments from the Private Sector	Authority's Response	Consequent Amendments to the Proposed Measure
		Governance, Internal Controls and Business Continuity. The *Statement of Guidance – Cybersecurity for Regulated Entities* has been updated to include a definition for risk tolerance, guided by the definition published by NIST. The process of selection for risk management strategies is done at the sole discretion of each regulated entity.	
5.3(b)	Reference to the Group Security - Does this refer to the entity under the parent company or the collective parent group? Suggest to clarify Group Security.	The group cybersecurity framework is intended to be applied to the entity, its parent company and its subsidiaries, if applicable. The document will be updated to clarify this point.	5.3(b) amended to read: ***"The cybersecurity framework should be implemented on a consolidated basis and must at a minimum cover the requirements noted in this Rule."***
5.4	Suggest to include the importance of contract and vendor management agreements which align to the parent company's Vendor Management Agreement practices.	This is covered in the *Statement of Guidance: Outsourcing – Regulated Entities*.	No amendment required.
	Suggest including the need for entities need to develop a bespoke risk assessment process that is tailored specifically to the threats posed by service providers to ensure your organisation's cybersecurity preparedness and the protection of its critical assets.	The proposed rule is not intended to be prescriptive on what method an entity employs to manage its cybersecurity framework. However, if regulated entities choose to utilise a risk assessment, then guidance is provided under section 7 of the *Statement of Guidance – Cybersecurity for Regulated Entities*.	No amendment required.
5.5	Title: Awareness is duplicated - Suggest removing the second Awareness	Noted.	The title for section 5.5 has been updated to read:

Section of Proposed Measure	Comments from the Private Sector	Authority's Response	Consequent Amendments to the Proposed Measure
			"Cybersecurity Awareness, Training and Resources"
5.5(a)	No mention of the availability of resources as suggested in the title. Suggest adding sufficient internal or external resources to execute the training and awareness program.	Noted. The measure has been updated to address the availability of resources.	Section 5.5 has been inserted as follows: ***"Regulated entities must ensure that they have sufficient and suitable personnel to maintain their cybersecurity framework, taking into consider the size, nature and complexity of the business."***
6.1	Suggest referencing the guidance material provided in the ombudsman's website to include within the Cyber security framework and that all aspects of the data Protection Law are complied with. This is an extensive topic which is not emphasized.	The measure has been amended to take into account the requirements of the Data Protection Law and the guidance of the Ombudsman.	Section 6.1 has been updated to read as follows: "Regulated entities must demonstrate that data protection is part of their strategy and cybersecurity framework ***taking into consideration the provisions of the Data Protection Law and the guidance issued by the Ombudsman on data protection.***"
7	Generally, the Rule should set out CIMA's proposed or intended response to a reported Cybersecurity Incident, if possible. It should perhaps be recognised that it may be neither helpful nor appropriate for CIMA to take the usual enforcement actions set out in CIMA's Enforcement Manual, such as warnings,	A breach of a regulated entity's cybersecurity system is not an indicator of a breach of these Rules and corresponding Statement of Guidance. The Authority's enforcement actions will be guided by the Enforcement Manual and the content of this Rule and	Not applicable

Section of Proposed Measure	Comments from the Private Sector	Authority's Response	Consequent Amendments to the Proposed Measure
	suspension of licenses, appointment of controllers, etc. where the regulated entity is fully compliant with the SoG and Rule but nevertheless subject to a sophisticated Cyber-attack. Alternatively, depending on the nature of the Cybersecurity incident, it may be more beneficial for a CIMA-analyst to be assigned to the regulated entity to ensure that it receives appropriate assistance where needed including acting as a liaison with other relevant CIMA divisions, where the regulated entity is subject to time-sensitive obligations or reporting requirements. It should also be clear whether CIMA will be implementing a 24 hour monitoring system given the immediate reporting obligations in certain situations. Furthermore, there should perhaps be clear guidance that CIMA will work with the regulated entity's cyber-response team in assessing the appropriateness of publication of cybersecurity incidents (if considered), where such publication could negatively impact forensic investigation, response or recovery, including where internal or external law enforcement may be involved due to the commission of criminal offences pursuant to the Computer Misuse Law (2015 Revision) and/or other applicable statutes.	corresponding guidance on Cybersecurity for Regulated Entities. The Authority notes the suggestions presented regarding the occurrence and containment of a cybersecurity incident.	
7.1	Does the guidance provide a reference to an email address or physical address where this should be mailed to in writing? Is there any fines levied if the entity does not comply with the 72 hour notice?	Reports may be submitted to the regulated entity's primary contact within the respective regulatory divisions.	No amendment required.

Section of Proposed Measure	Comments from the Private Sector	Authority's Response	Consequent Amendments to the Proposed Measure
		Fines are levied to regulated entities as prescribed in the Monetary Authority (Administrative Fines) Regulations.	
	the Rule should perhaps define the scope of a "material impact" of a Cybersecurity Incident, which may be subjective to the type of regulated entity.	Since the material impact is subjective, the Rule cannot be prescriptive in defining a scope as it varies per regulated entity.	No amendment required.
7.2	Suggest add "entity, parent or group".	The suggestion does not indicate the intended placement of the recommendation, therefore the addition will not be accepted.	No amendment required.
STATEMENT OF GUIDANCE			
General	use definitions consistently across SOG, e.g. use "Cybersecurity event" rather than "risk event" at section 7.2 c) iv, use "Cyber –attack" rather than "attack" in 9.2 a) i., use "cyber-resilience" rather than "cyber resilience" at 10.2 h).	The *Statement of Guidance on Cybersecurity for Regulated Entities* for has been updated to maintain consistency throughout.	The *Statement of Guidance - Cybersecurity for Regulated Entities* has been updated to address the inconsistencies highlighted.
	Will CIMA consider the facilitation of a CIMA-based centralised information sharing system for the sharing of non-public information and updates relating to Cybersecurity incidents amongst licensees on an anonymised basis, to promote industry awareness and for the minimisation of systemic Cyber-risk?	This request is outside the scope of this consultation. However, regulated entities may direct such a query to their contact person within the respective regulatory divisions.	No amendment required.
4	References Definition for Cyber Threat but not for Cyber Risk. Suggest including a Definition of a Cyber Security Risk and Cyber Security Incident Examples: Cyber Security Risk is any exposure to harm or loss resulting from breaches of or attacks on information systems. Cyber Security Incident is defined as a breach of systems security policy in order to affect its	The Authority has adopted the definitions of "cyber risk" and "cybersecurity incident" from the NIST standards. The proposed measure has been updated to include the definitions for these terms as outlined in the *Rule - Cybersecurity for Regulated Entities* to maintain consistency across the documents.	Section 4 has been amended to include the definitions of cyber risk and cybersecurity incident as set out in the Rule – Cybersecurity for Regulated Entities.

Section of Proposed Measure	Comments from the Private Sector	Authority's Response	Consequent Amendments to the Proposed Measure
	integrity or availability and or the unauthorized access or attempt to access systems.		
	Not clear why the definition of "Cybersecurity threat" is not consistent between SOG and Rule	The corresponding *Rule - Cybersecurity for Regulated Entities* has been amended to reflect consistency in the defined terms.	Corresponding *Rule - Cybersecurity for Regulated Entities* has been amended to include the definition of "cybersecurity threat" as follows: ***"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."***
6	There is no mention the accountability of CIMA when requesting the information that it is held and managed in a manner which protects the entity reviewed.	This measure is intended to provide guidance on the expected practices of regulated entities with regard to cybersecurity. Under section 34(8) of the MAL, the Authority may require a regulated person to produce or provide specified information or information of a specified description as it may reasonably require in connection with the exercise by the Authority of its regulatory functions.	No amendment required.
	Suggest to move up 6.6 under 6.2 The business and cyber security strategies typically are among the top criteria in the identification of framework	The suggested amendment is noted however, the Authority concludes that the amendment	No amendment required.

Section of Proposed Measure	Comments from the Private Sector	Authority's Response	Consequent Amendments to the Proposed Measure
	NIST CSF (under identify) and ISO both identify security strategies as the first step identifying risk tolerance and developing the organizational understanding to manage cybersecurity.	will not change the substance of the requirement.	
6.1	The scope of the required framework is vague - perhaps deliberately however a minimum scope would be useful given the requirements for documentation and testing.	The SoG is not intended to be prescriptive. Regulated entities are expected develop a cybersecurity framework taking into consideration the size and complexity of their business and the nature of their cyber risk exposures.	No amendment required.
6.5	References Risk Tolerance, suggest adding to the definition section.	The Authority agrees with this suggestion.	The definition of "risk tolerance" was moved to section 4 and reads as follows: *"The degree of risk of a negative event relating to cybersecurity that a regulated entity is willing to accept."*
	Is there a defined taxonomy e.g. limit breach, ALARp etc.	The measure is not intended to be prescriptive and regulated entities are expected to document their risk appetite based on the extent of their cybersecurity risk exposure.	No amendment required.
6.7	What is the level of resources mean? Does this apply to the amount or the skillset capabilities if so suggest to this should be clearly articulated.	The level of resources refers to the amount of resources assigned to the cybersecurity framework.	No amendment required.
	Assume audits will be risk based and driven by the Banks Audit policy.	The Authority confirms that the audits carried out for the cybersecurity framework for will be driven by the internal policies of regulated entities. The proposed measure has been amended to provide clarity on the matter of audits.	Section 6.7 amended to read as follows: *"Regulated entities should ensure that there is an internal audit function or some alternative objective assessment option in place*

Section of Proposed Measure	Comments from the Private Sector	Authority's Response	Consequent Amendments to the Proposed Measure
			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.****"*
6.9	Similar to Policy and Procedures in 6.2, suggest combine.	The point set out in sections 6.2 and 6.9 are connected, but not the same. Section 6.2 sets out that the framework should include policies, procedures and strategies, while 6.9 outlines that these policies and policies should include enforcement and disciplinary actions for non-compliance. However, the Authority agrees that they can be combined.	Section 6.9 has been delated and incorporated into to section 6.2, which now reads as follows: *"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 make reference to enforcement and disciplinary actions for non-compliance."***

Section of Proposed Measure	Comments from the Private Sector	Authority's Response	Consequent Amendments to the Proposed Measure
	Cyber policies should NOT define consequences but they may point to the appropriate Human Resource policy which defines consequence management,	The aim is to ensure that disciplinary actions are considered for breaches of the cybersecurity policies and procedures. It is the expectation of the Authority that the matter is either addressed or referenced in policies and procedures regarding cybersecurity.	Section 6.9 has been incorporated into section 6.2. See note above.
7.1	Section 7.1 should clarify that a regulated entity's cybersecurity framework should incorporate a risk management strategy.	The requirement for a documented cybersecurity risk management strategy is set out under section 5.1(b)(i) of the corresponding *Rule - Cybersecurity for Regulated Entities.*	No amendment required.
7.2(a)(iii)	These are two separate things key controls and a Risk Register, Not a single deliverable.	The guidance is recommending that regulated entities maintain inventories of cybersecurity risks and applicable controls. The method for maintaining these inventories are at the sole discretion of each regulated entity.	No amendment required.
7.2(b)(i)	Reference to process and data are identified in the appropriate policies and processes but not in the identification and classification of data elements as suggested in 7.2	The data elements outlined in section 7.2(b)(i) are intended to be listed in section 7.2(a)(ii). Section 7.2(a)(ii) has been updated to include data and processes.	Section 7.2(a)(ii) has been updated to read as follows: *"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, systems interfaces,* ***data, processes,*** *operations and human elements."*

Section of Proposed Measure	Comments from the Private Sector	Authority's Response	Consequent Amendments to the Proposed Measure
7.2(b)(ii)	Suggest replacing " Analysis and measurement of the probability" to "Analysis and evaluation of the Impact to Cyber Threats"	The Authority notes and accepts this revision.	Section 7.2(b)(ii) has been revised to read as follows: *"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"*
7.2(b)(iv)	This section reads very similar to i) suggest merging the two. Ie a comprehensive policy should be in place that identifies that protection of assets should commensurate with the criticality of said assets.	Risk mitigation and control strategies form part of the framework and aid in influencing the development of policies and procedures. As the guidance provided differs, these will remain as separate paragraphs.	No amendment required.
7.2(c)	General comment: This section does not have a reference to Limiting Administrative Privileges – allowing only trusted personnel to configure, manage, and monitor computer systems	The measure is not intended to be prescriptive and therefore the assignment of trusted personnel is at the sole discretion of regulated entities and must be in line with their internal policies and procedures.	No amendment required.
7.2(c)(i)	Reference to a Detection Policy - Does this mean intrusion detection policy? - There is no reference to a detection policy in NIST or ISO standards. Suggest referencing firewalls once and including intrusion detection (host intrusion detection, Network intrusion detection).	NIST highlights detection as one of the five functions in the core framework for cybersecurity.[1] The Detect Function defines the appropriate activities to identify the occurrence of a cybersecurity event and enables timely discovery of cybersecurity events.	No amendment required.

[1] https://www.nist.gov/cyberframework/online-learning/components-framework

Section of Proposed Measure	Comments from the Private Sector	Authority's Response	Consequent Amendments to the Proposed Measure
		One example of outcome categories within this function includes maintaining Detection Processes to provide awareness of anomalous events.	
7.2(c)(ii)	Suggest to add include phishing (as this is growing as the number 1 method to attack).	The Authority notes this comment and will update the measure instead to include "cyber attacks" in the alerts, as it covers a broader range of vulnerabilities, which includes phishing.	Section 7.2(c)(ii) has been updated to read as follows: "*The monitoring/ surveillance system should alert the regulated entity to any abnormal IT system activities, transmission errors,* ***cyber attacks*** *or unusual online transactions."*
	Suggests either IT BAU monitoring or Fraud monitoring neither of which are pure play cyber.	These are examples of the components of monitoring systems that may be included in a regulated entity's monitoring/surveillance system. Furthermore, the guidance is not intended to be prescriptive.	No amendment required.
7.2(c)(iii)	Suggest to add the monitoring of the Intrusion attempts.	The Authority notes this suggestion and accepts this recommendation.	Amended to include "intrusion attempts" as follows: *"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."*

Section of Proposed Measure	Comments from the Private Sector	Authority's Response	Consequent Amendments to the Proposed Measure
	Does this mean Cyber Intelligence or something else?	This section of the proposed measure has outlined the expectations for the monitoring of emerging cybersecurity risks. The queried term will not be utilised in the proposed measure.	No amendment required.
7.2(c)(iv)	Suggest adding Mean Time to Detect (MTTD) and Mean Time to Resolve (MTTR): How long do security threats fly under the radar at your organization? MTTD measures how long it takes for your team to become aware of a potential security incident. Mean Time to Resolve (MTTR): How long does it take your team to respond to a threat once your team is aware of it?	Regulated entities should consider this and may find it prudent to include in their own policies, procedures and processes, however, based on the diversity of CIMA-regulated with regard to complexity and nature of business, the guidance will not be prescriptive for these concepts.	No amendment required.
7.2(c)(vi)	Suggest its made clear what part of an organization should do this.	Regulated entities are responsible for appointing appropriate personnel, or third-party service provider, who is responsible for managing the cybersecurity framework.	No amendment required.
7.2(d)(i)	Suggest adding a checklist in place to ensure that there is a consistent method in place,	The Authority notes the proposed recommendation; however the guidance is not intended to be prescriptive by specifying a methodology for handling incident response mechanisms.	No amendment required.
7.2(d)(ii)-(iii)	These clauses should be combined - also not clear why there is such a focus on DDOS & DOS - given there are much higher and likely risks?	DDOS and DOS are among the most common cyber attacks and tend to be one of the most difficult to prevent. The Authority however notes the recommendation to combine the paragraphs and has updated the measure to reflect this.	Section 7.2(d)(ii) has been updated to read as follows: *"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*

Section of Proposed Measure	Comments from the Private Sector	Authority's Response	Consequent Amendments to the Proposed Measure
			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."*
7.2(d)(v)	Suggest to include the 5 phases of cyber security incident management plan and prepare, Detect and report, assess and decide, respond , Post incident activity.	Noted. The measure has been updated to consider the phases in the incident response process as set out in the NIST recommendations for incident handling.	Section 7.2(d)(i) will include the following addition: ***"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."***
7.2(d)(vi)	Suggest adding among clear responsibilities and roles that we also include appropriate skill and trusted members of the organizations. Incident response activities should include: • Alert and activate everyone on the response team to begin executing the preparedness plan. • Secure the premises around the area where the data breach occurred to help preserve evidence.	The guidance is not intended to be prescriptive, but we expect that that regulated entities develop through procedures for the management of cybersecurity incidents. .	No amendment required.

Section of Proposed Measure	Comments from the Private Sector	Authority's Response	Consequent Amendments to the Proposed Measure
	• Stop additional data loss. Take affected computer systems offline. • Document everything known about the breach. • Interview those involved in discovering the breach and anyone else who may know about it. • Review protocols regarding disseminating information about the breach for everyone involved in this early stage. • Assess priorities and risks based on what you know about the breach. • Inform the proper authorities, including your regulator. • Notify law enforcement, if needed, to begin an in-depth investigation		
	"Monitoring incidents": Vague - Does this mean detecting or oversight of an incident ?	The term monitoring is broad and may include detection and general oversight of incidents as indicated, however the Authority intends for the broad application of the term to be applied in this measure.	No amendment required.
7.2(d)(vii)	Vague - suggest this is driven by risk - do you need every log ? Also focus seems to be post event analysis rather than detection and response.	The guidance is not intended to be prescriptive in this regard and regulated entities are encouraged to apply a risk-focused approach in regard to their operations. Regulated entities must determine whether the magnitude of the incident is significant enough to be recorded.	No amendment required.
7.2(d)(viii)	Suggest adding the below to the review process, "record the date and time when the breach was discovered".	The Authority agrees that this suggestion would enhance the content of the paragraph.	Amended per recommendation.

Section of Proposed Measure	Comments from the Private Sector	Authority's Response	Consequent Amendments to the Proposed Measure
7.2(d)(ix)	Suggest to include contacting legal counsel for guidance on the incident or breach	Regulated entities must decide the most suitable approach for an escalation process.	No amendment required.
	Remove IT that should be covered in the normal IT processes.	The suggested amendment is noted however, the Authority concludes that the amendment will not change the substance of the proposed measure.	No amendment required.
	Should be driven by the severity of the incident. Wording is rather awkward.	Noted.	Section 7.2(d)(ix) is now 7.2(d)(viii) and reads as follows: ***"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."***
8	Suggest adding 8.3: The Cybersecurity Framework should be tested on a periodic basis for effectiveness and updated or amended as required.	The Authority agrees with the proposed addition. The document has been amended to reflect the addition.	Section 8.3 has been added to the proposed measure and reads as follows: ***"The cybersecurity framework should be tested on a periodic basis for effectiveness and updated or amended as needed."***
8.2	CISO should take precedence.	The recommendation does not change the substance of the measure.	No amendment required.

Section of Proposed Measure	Comments from the Private Sector	Authority's Response	Consequent Amendments to the Proposed Measure
9.1(b)(ii)	Suggestion to include segregation of critical assets and infrastructures from less sensitive environments this is particularly important in Virtual environments.	The recommendation is considered to be prescriptive and may not hold for all regulated entities.	No amendment required.
9.1(c)	Missing key processes like vulnerability & patch management.	The Authority notes the query however to avoid being prescriptive on the matter as each regulated entity has the discretion to employ various testing mechanisms based on their exposure.	No amendment required.
9.1(h)	Suggest to include phishing attacks in the sample or suggested attack vectors.	Noted.	Section 9.1(h) amended to include phishing attacks.
	"Vulnerability assessment" - should be far more regularly than annually suggest monthly as an absolute minimum.	In some cases, the frequency for the review may be more regular, based on the size, nature and complexity of the regulated entity, however that would be dictated by the approved internal policies of each entity.	No amendment required.
9.1(j)	This taken verbatim will drive a legacy security architecture suggest stripping back.	The Authority is ensuring that regulated entities consider various IT system controls when implementing their cybersecurity framework.	No amendment required.
9.1(k)	Suggest to expand the scope beyond mobile payment and include, Point of Sale Terminals, Online payment gateways and emerging technologies	The Authority agrees with this suggestion.	The measure is revised to reflect this as follows: **"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**

Section of Proposed Measure	Comments from the Private Sector	Authority's Response	Consequent Amendments to the Proposed Measure
			technologies, as applicable."
9.1(k)(i)	"implement IT security" - Inconsistent terms being used in the document.	The use of the term "IT security" here is intended to be applied broadly as entities will be exposed to IT risks associated with each of payment systems outlined.	No amendment required.
9.1(k)(iii)	Suggest moving this section to the top as this is the basis of payment card protection. Reference to the guidance in protecting cardholder data is available through the Payment Card Industry Data Security Standard PCI DSS	Noted.	Paragraph 9.1(k)(iii) has been moved up as suggested to 9.1(k)(i) as suggested,
9.2(a)(ii)	Suggest to move references to 9.1(k) or create a specific subsection on Securing Financial Systems and payment card security	The suggested amendment is noted however, the Authority concludes that the amendment will not change the substance of the proposed measure.	No amendment required.
9.2(d)	is there any reason for the over focus on DOS & DDOS as attack type?	DDOS and DOS are among the most common cyber attacks and tend to be one of the most difficult to prevent.	No amendment required.
9.2(f)	How about driving the use of EV certs?	The SOG is not intended to be prescriptive and therefore will not specify the use of any particular methods.	No amendment required.
10.1(f)	This will drive a massive cost - external review and audit annually will be very costly and time consuming. Consider accreditation like Cyber Essentials.	The Authority has considered the possible financial implications of requiring an annual independent audit. The measure has been updated section, taking this under advisement.	Section 10.1(f) has been updated to read as follows: ***"****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."***

Section of Proposed Measure	Comments from the Private Sector	Authority's Response	Consequent Amendments to the Proposed Measure
10.2(c)	Duplicative of point 10.2 A)	10.2(a) requires the establishment of training for the governing body while 10.2(c) details the expectations of the Authority regarding the knowledge and responsibilities of the governing body.	No amendment required.
10.2(e)	"and cyber-resilience program" - There is no requirement mentioned up to this point for a separate resilience programme. What does this drive ?	This Guidance should be read in conjunction with the Rule. Rule 5.5 establishes the requirement for a cyber-resilience program. Regulated entities are encouraged to establish appropriate programmes, policies and procedures for cybersecurity, cyber-resilience and IT management. This guidance is in support of the Rule, and provides further emphasis.	No amendment required.
10.3(b)	"(e.g. CIO or CISO)" – switch order	The suggested amendment is noted however, the Authority concludes that the amendment will not change the substance of the proposed measure.	No amendment required.
11.2	Suggest add h) Appropriate third party contract and Service Level Agreements are in place.	The Authority notes and agrees with the recommendation.	Section 11.2 amended to include (h) as recommended.
12.1	Suggest if the objective is to include vendors and contractors that this be added to the title vs just Employees.	The heading	No amendment required.
	Section 12.1 the requirement for a "screening process with stringent selection criteria" concerning the hiring of individuals supporting technology functions will need to be balanced with the realities of the Cayman employment and work permit regime.	This issue is outside the scope of this consultation. CIMA-regulated entities also include those that operate outside of the Cayman Islands.	Not applicable

Section of Proposed Measure	Comments from the Private Sector	Authority's Response	Consequent Amendments to the Proposed Measure
12.2	Section 12.2 b) query whether it would be strictly necessary, where the IT security functions are outsourced, for the Chief Information Security Officer (CISO) or Chief Information Officer (CIO) to be "suitably qualified… of IT systems and cybersecurity" or whether sufficient for such person to simply be delegated with the operational authority to carry out that role.	The proposed measure is not prescriptive with regard to the qualifications of the appointed CISO or CIO, whether internally appointed or outsourced. Regulated entities have the sole discretion to determine the most suitable candidate for the purposes of their business. Additionally, Section 13.3(a) sets out the expectations of regulated entities to consider, prior to the appointment of a service provider, carrying out due diligence to determine its capability, reliability and track record. This is intended to cover any type of outsourcing arrangement. Regulated entities are ultimately responsible and accountable for any outsourcing arrangements.	No amendment required.
14.3	Suggest that Data protection should also include non-digital paper copies and the physical controls necessary to protect personal or sensitive data.	Section 14.3 sets out the requirement for compliance with international and local data protection laws and regulatory requirements. It is the Authority's expectation that regulated entities implement a framework that complies with the proposed measures as well as the guidance set out by the Ombudsman on data protection.	No amendment required.
14.5	This section needs re-written as it excludes the use of pretty much all modern technology. As a business we use things like facebook, Instagram and Twitter to communicate with customers. Cloud based services will be used for information sharing and processing e.g. Office 365, BOX, etc.	The Authority has addressed the categories of internet services, including social media and cloud-based internet storage sites in Section 14.5.	No amendment required.

Section of Proposed Measure	Comments from the Private Sector	Authority's Response	Consequent Amendments to the Proposed Measure
14.7	"Confidential information" - Definition required	The Authority's expectation is that broad definition of the term is applicable here. Otherwise, regulated entities should be guided by the definition of the term as set out in the internal policies.	No amendment required.
14.9	"sensitive" – definition required	The Authority's expectation is that broad definition of the term is applicable here. Otherwise, regulated entities should be guided by the definition of the term as set out in the internal policies.	No amendment required.
14.10	"secure environment" - definition required	The Authority's expectation is that broad definition of the term is applicable here. Otherwise, regulated entities should be guided by the definition of the term as set out in the internal policies.	No amendment required.
14.11	Why just mobile devices? Why just one threat type?	Mobile devices are considered to be very high risks to regulated entities. They have been highlighted for emphasis.	No amendment required.