Cayman Islands Monetary Authority Rule and Statement of Guidance – Cybersecurity for Regulated Entities

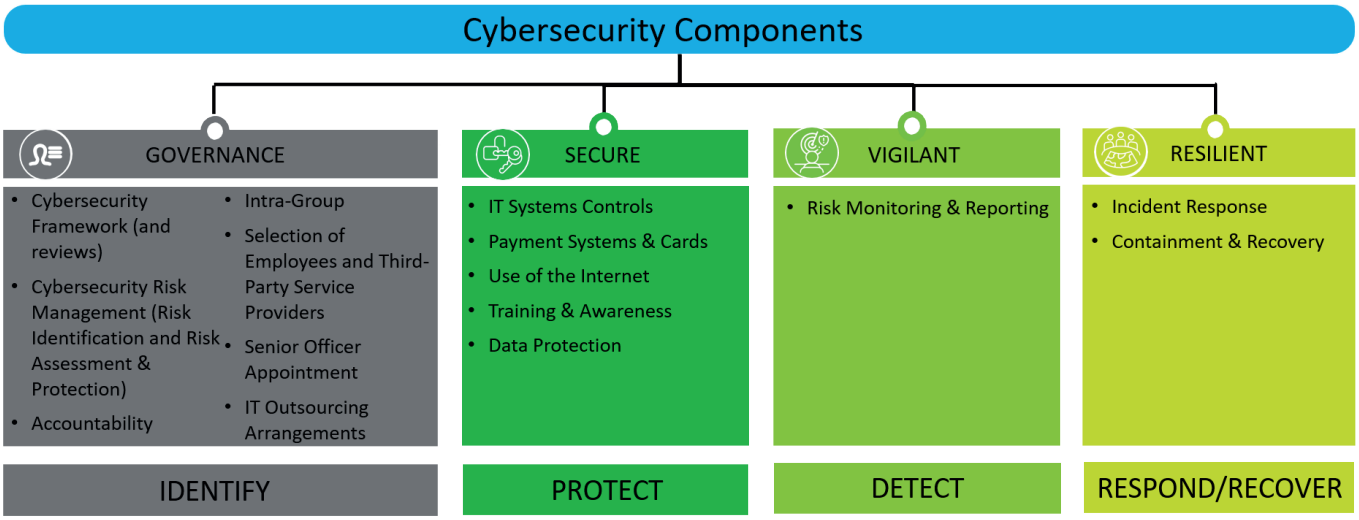
Is your organisation ready?
Across the globe, and in the Cayman Islands, cyber-attacks are increasing in frequency and sophistication. The Financial Services sector is a key target, and there are many well-publicized cybercrime cases involving Financial Institutions. Cybercriminals are becoming more sophisticated, and the cost of cybercrime is becoming increasingly intolerable. The stakeholders – including boards, regulators, investors, analysts, business partners, and customers – expect greater visibility into an organisation's cybersecurity risk management programmes.

In light of the growing cyber threats to financial industry, the Cayman Islands Monetary Authority (CIMA) published Rule and State of Guidance – Cybersecurity for Regulated Entities on May 27, 2020. The Guidance will come into effect on November 27, 2020. The Guidance would require all CIMA–regulated entities to establish a cybersecurity program, develop cybersecurity policies and procedures, and designate a Senior Officer, who must oversee the cybersecurity framework with access to the governing body.

The ultimate goal of the Guidance is to ensure that entities regulated by CIMA establish a robust cybersecurity program and comply with related requirements. The Guidance prescribes specific requirements to ensure appropriate cybersecurity programs are in place. Regulated entities should implement the Guidance in proportion to their cyber risk profile (size, nature and complexity of their business), following an appropriate assessment of their cyber risks. Each entity is required to assess its particular risk profile and design a program that robustly addresses such risks.

Cybersecurity components

The CIMA Guidance emphasizes the importance for the regulated entities to ensure that robust cybersecurity measures are in place and that they can appropriately identify, protect, detect, respond to and recover from such cybersecurity-related threats, incidents and breaches. Broadly speaking, the requirements in the Guidance fall under the four main pillars - Governance. secure. Vigilant. Resilient.(tm)



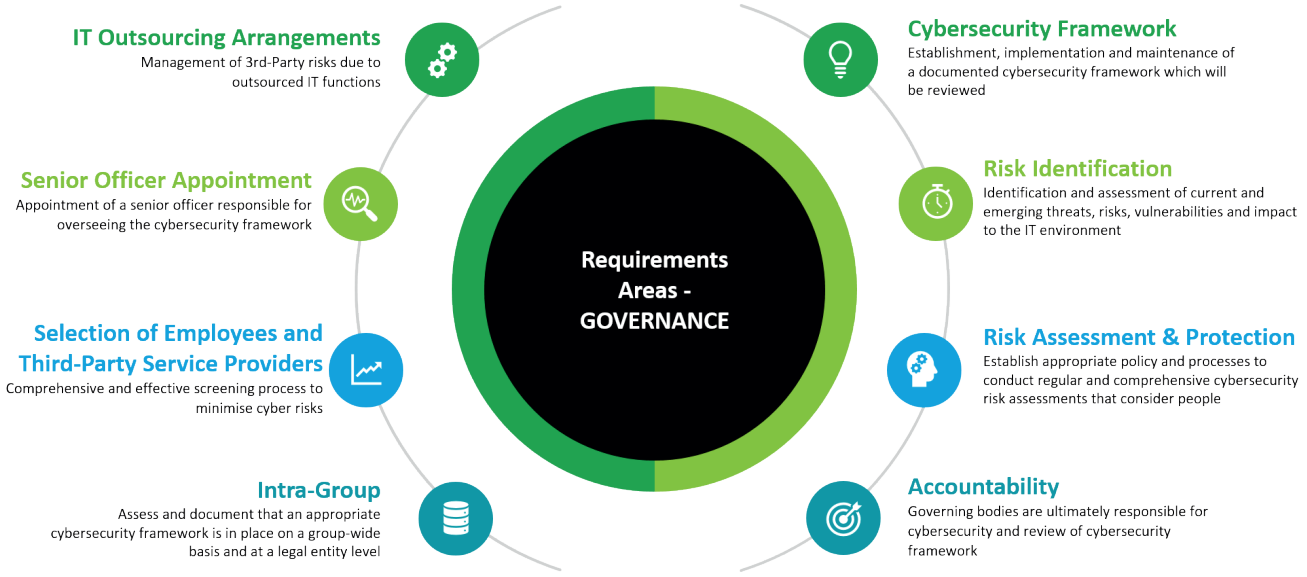
Identify, Protect, Detect, Respond to and Recover are the function areas of the National Institute of Standards and Technology Cybersecurity Framework (NIST CSF).

Governance

Regulated entities are required to identify and manage cyber risks to organisational systems, assets, data, and capabilities. They also need to ensure management involvement and sponsorship of a business-aligned cybersecurity program. A cybersecurity program that is designed with security, vigilance, and resilience in mind, guided by a clear strategy and supported by strong governance measures will be well placed to meet the regulatory requirements.

The Guidance highlights the importance of the Governing Body in overseeing cybersecurity and cyber–resilience and also carrying out periodic reviews of the effectiveness of the cybersecurity framework and cyber–resilience.

Key Requirement Areas



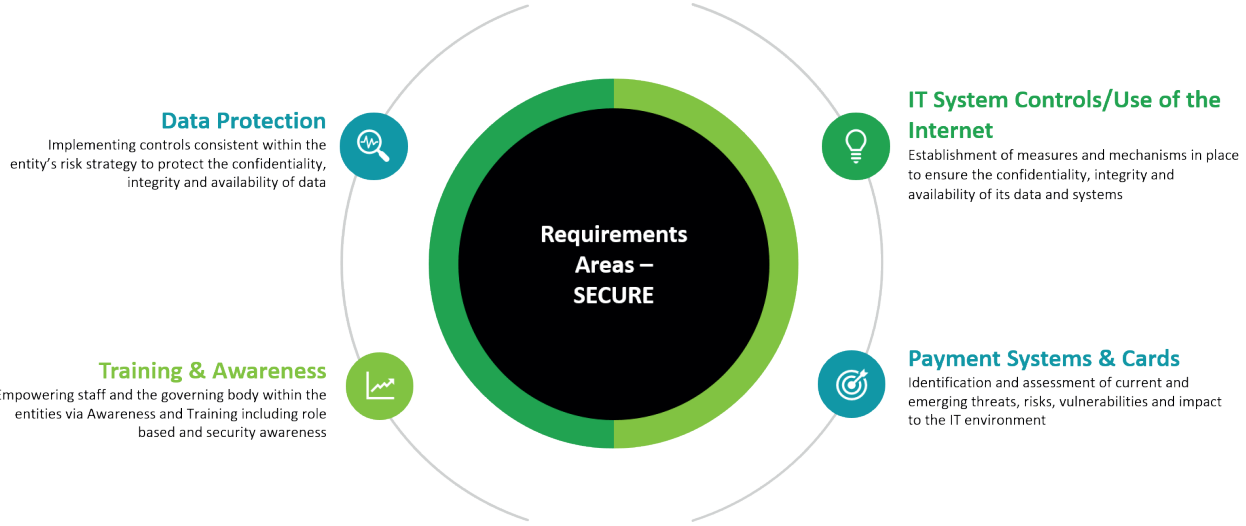
Secure

Regulated entities are required to establish and implement effective mechanisms around information assets, systems, and data and balance the need to reduce cyber risk while enabling productivity, business growth, and cost optimisation objectives.

Regulated entities must demonstrate that data protection is part of their strategy and cybersecurity framework taking into consideration the provisions of the Cayman Islands' Data Protection Law (DPL) and the guidance issued by the Ombudsman on data protection.

A comprehensive cybersecurity training and awareness program must be establish and endorsed by the governing body and/or senior management.

Key Requirement Areas



Vigilant

Regulated entities will need to develop and implement mechanisms and systems to proactively detect and manage cyber threats and respond more effectively to cyber incidents such as Denial of Service (DoS) attacks, Data Leakages, Insider Attacks, etc. from internal and external forces.

Regulated entities must implement monitoring/surveillance and detection techniques and systems that allow real-time monitoring and detection of threats (e.g., Firewalls, Web Application Firewalls (WAFs), Network Behaviour Analysis, etc.).

Key Requirement Areas

Resilient

Cyber threats are continually evolving and increasing in volume, intensity, and complexity. It has become more likely that an attack can penetrate an entity's defenses and controls. When this happens, regulated entities must respond fast, thoroughly, and decisively.

Incident reporting rules under the Regulation and the Cayman Islands' DPL adds further impetus for regulated entities to strengthen their ability to detect security incidents and data breaches rapidly.

Regulated entities must notify CIMA in writing of an incident when it is deemed to have a material impact or has the potential to become a material incident no later than 72 hours following the discovery.

Key Requirement Areas

Incident Response
Development of appropriate cyber incident response plans and procedures for various cyber and data loss incidents

Containment & Recovery
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.

We are here to help!

Every entity is at a different place when it comes to the maturity of its cybersecurity risk management program. Besides, the nature and magnitude of cyber risks are continuously evolving, and so are the practices for staying ahead of these threats. That's why it's essential to understand where you stand today by proactively performing in a compliance readiness assessment and addressing the gaps.

CIMA Sources:
CIMA's Statement of Guidance – Cybersecurity for Regulated Entities
CIMA's Rule – Cybersecurity for Regulated Entities

Alexandra Simonova
Director, Risk Advisory
asimonova@deloitte.com
+1 345 743 6333

Wayne Green
Director, Risk Advisory
wagreen@deloitte.com
+1 345 743 6256

www.deloitte.com/ky/cyber