Cybersecurity: CIMA releases updated Rule and Statement of Guidance

Insights - 01/01/2022

The Cayman Islands Monetary Authority (**CIMA**) has updated its Rule and Statement of Guidance – Cybersecurity for Regulated Entities following feedback received during a private sector consultation. The Rule (**Rule**), which sets out CIMA's requirements in relation to the management of cybersecurity risks, is a clear and precise directive that creates binding obligations and breach of which may lead to a fine or regulatory action being taken by CIMA. The Statement of Guidance (**SOG**) is intended to assist relevant entities in their compliance with the Rule and represents a measure against which CIMA will assess such compliance and implementation. The Rule and SOG came into effect on 27 November 2020.

Scope

The Rule applies to entities regulated by CIMA (including controlled subsidiaries) under the following acts: Banks and Trust Companies Act (Revised), Insurance Act (Revised), Mutual Funds Act (Revised) (with the exception of regulated mutual funds), Securities Investment Business Act (Revised), Building Societies Act (Revised), Cooperative Societies Act (Revised), Development Bank Act (Revised), Money Services Act (Revised), Companies Management Act (Revised), Directors Registration and Licensing Act (Revised) and Private Trust Companies Regulations (Revised). **Investment funds are not within the scope of the Rule or the SOG.**

Key Features

The Rule requires regulated entities to *"establish, implement and maintain a documented cybersecurity framework that is designed to promptly identify, measure, assess, report, monitor and control or minimize cybersecurity risks as well as responding to and recovering from cybersecurity breaches that could have a material impact on their operations"*.

A cybersecurity framework is defined as *"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".

CIMA's feedback statement, published following the private sector consultation, emphasises that the Rule and SOG are not intended to be prescriptive regarding the methods a regulated entity uses to establish, implement and maintain its cybersecurity framework but rather that regulated entities are expected to develop a cybersecurity framework that takes into consideration the size and complexity of their business and the nature of their cyber risk exposures.

In addition, CIMA has clarified that it expects regulated entities to have in place measures that not only mitigate cyber risks and cybersecurity breaches, but also that allow regulated entities to respond to and recover from cyber attacks effectively.

Cybersecurity Framework

The Rule sets out a non-exhaustive list of factors that should be included in a regulated entity's cybersecurity framework. These include:

> (a) a well-documented cybersecurity risk management strategy which addresses all material cybersecurity risks relevant to the regulated entity;
>
> (b) cybersecurity and IT security policies and procedures adequate to identify, assess, mitigate, control, monitor and report on such risks;
>
> (c) clearly identified managerial responsibilities and controls; and
>
> (d) clear, documented and effective processes for responding to, containing and recovering from cyber attacks, breaches and incidents.

A cybersecurity framework can be implemented on a consolidated basis across a corporate group and in such instances the framework can be applied to the regulated entity, its parent company and its subsidiaries (as applicable) so long as it covers, at a minimum, the requirements set out in the Rule.

As part of its overall cybersecurity risk management strategy, a regulated entity should ensure that the following key components are taken into consideration: risk identification, risk assessment and protection, risk monitoring and reporting and policies and procedures for incident responses and containment and recovery. Regular self-assessments should be conducted by the relevant entity, at least annually, taking into account the requirements of the Rule and the SOG, as well as any other relevant frameworks and emerging trends in cybersecurity.

Responsibility

The governing body of the regulated entity has ultimate responsibility for its cybersecurity. Their duties include:

(a) the approval of written cybersecurity risk management strategy and a comprehensive cybersecurity framework;

(b) appropriate oversight of the risk management framework and periodic reviews of such framework;

(c) the approval of a cybersecurity audit plan (which is to be driven by the regulated entity's existing internal audit policies and procedures); and

(d) 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.

The SOG indicates that a suitable senior officer such as a Chief Information Officer (CIO) or Chief Information Security Officer (CISO) should also be appointed by a regulated entity to oversee the cybersecurity framework, liaise with the governing body and create a feedback loop to ensure that decisions made by the governing body and senior management are monitored and remain appropriate and up-to-date.

Senior management is also responsible for developing, implementing and monitoring the cybersecurity framework and ensuring that the appointed senior officer (CIO or CISO) has access to the governing body.

Management of Outsourcing Risks

If a regulated entity outsources its IT functions, either externally to a third party or internally to an affiliated entity, they still remain ultimately responsible for such outsourced functions and their cybersecurity. It is the responsibility of the regulated entity to assess the relevant service provider's compliance with the Rule and related SOG (in particular, SOG – Cybersecurity for Regulated Entities and SOG – Outsourcing: Regulated Entities).

Other ongoing obligations

Regulated entities should establish a comprehensive cybersecurity training and awareness programme that is reviewed and maintained on an ongoing basis. Internal IT systems and controls should be established and documented. Where financial services are provided online and/or clients transact online (including by mobile platforms and other emerging technologies), policies and controls should be established around internet usage. The SOG also recommends that regulated entities maintain inventories of all relevant cybersecurity risks and applicable controls.

Data protection

The Rule requires regulated entities to demonstrate that data protection is taken into account in its risk strategy and cybersecurity framework. More specifically, the Rule states that the cybersecurity

framework must take into consideration the provisions of the Data Protection Act (Revised) and guidance issued by the Ombudsman on data protection.

Notification Requirements

If a regulated entity becomes aware of a cybersecurity incident which is deemed to have a material impact or has the potential to become a material incident, they must immediately notify CIMA in writing and no later than 72 hours following the discovery of the incident. If such incident results in the breach of non-public information or disrupts services then the regulated entity must notify the affected persons.

Next Steps

Cybersecurity risks are constantly changing and there may be further developments in this area. CIMA regulated entities should take the opportunity to review all information technology associated risks as part of their broader risk management processes and consider any potential gaps in existing policies and procedures.

For further information, or to discuss specific requirements, please contact your usual Ogier contact or one of our team listed.

About Ogier

Ogier is a professional services firm with the knowledge and expertise to handle the most demanding and complex transactions and provide expert, efficient and cost-effective services to all our clients. We regularly win awards for the quality of our client service, our work and our people.

Disclaimer

Meet the Author

Bradley Kruger

Partner

Cayman Islands

E: bradley.kruger@ogier.com

T: +1 345 815 1877

Key Contacts

James Heinicke

Partner

Cayman Islands

E: James.Heinicke@ogier.com

T: +1 345 815 1768

Joanne Huckle

Partner

Cayman Islands

E: joanne.huckle@ogier.com

T: +1 345 815 1895

Nathan Powell

Partner 合伙人

Hong Kong

E: nathan.powell@ogier.com

T: +852 3656 6054

Related Services

Banking and Finance

Corporate

Regulatory

Legal

Related Sectors

Technology and Web3