OneStopNetworks – Bermuda
in Collaboration with
Nangia Andersen LLP

Our Offerings

Bermuda Monetary Authority

Operational Cyber Risk Management Code of Conduct

ONESTOPNETWORKS
web development - cloud services

A member firm of ANDERSENGLOBAL

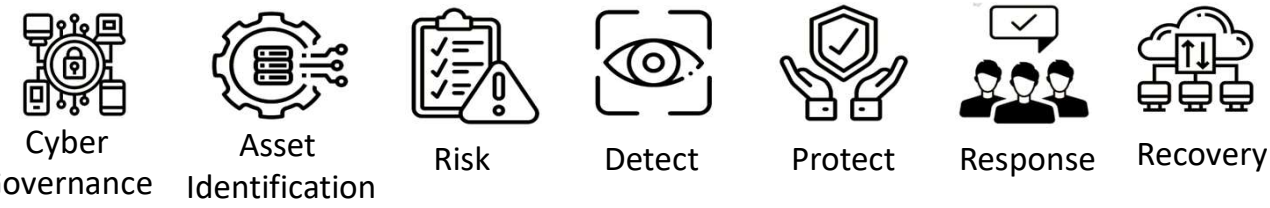
Introduction
BMA Operational Cyber Risk Management Code of Conduct 2022

The Bermuda Monetary Authority ('BMA') published its Operational Cyber Risk Management Code of Conduct ('Code') for CSPs, Trust Companies, Money Service Business, Investment Business and Fund Administration Providers (Relevant Licensed Entities or 'RLE') on 15 March 2022 and RLE are required to comply by 15 February 2023.

The goals of the Code are to ensure that RLE establish a robust cybersecurity program and comply with related requirements. The Code prescribes specific requirements to ensure appropriate cybersecurity programs are in place. RLE should implement the Code in proportion to their cyber risk profile (nature, scale 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.

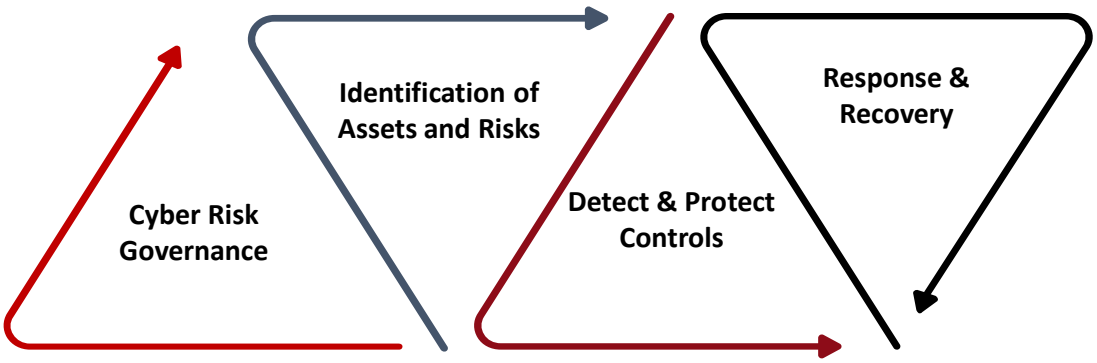
The Code emphasizes the importance for RLE to ensure that robust cybersecurity measures are in place:

- Cyber risk governance;
- Identification of assets and risks;
- Detect and protect controls; and
- Response and recovery controls.



What You Need To Know

RLE are required to identify and manage cyber risks to organizational systems, assets, data, and capabilities. They also need to ensure senior management and Board 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.



Below are the key responsibilities and minimum standard requirements:

- Board of Directors & management must have oversight of risks.
- Create an asset inventory listing.
- Appoint a CISO (Chief Information Security Officer) or outsource the role.
- Consider a cyber insurance policy and review coverage at least annually.
- Identify and understand the cyber risk posture.
- Measure the potential impact and consequences of risk.
- Monitor & report – maintain a risk register.
- Compliance and audit: The control environment should be continuously monitored and evaluated.
- IT Service Management, IT Incident Management & Security Incident Management.
- Business Continuity Planning (BCP) & Disaster Recovery (DR).

What's Next?

Assessing Your Compliance

The Code is not a "one size fits all" approach for all RLE. The BMA developed the Code as a flexible reference point and encourages RLE to align their cyber risk profile to the nature, scale, and complexity of the business.

We recommend that RLE undertake evaluative processes to assess their individual cyber security risks and compliance with BMA requirements, considering other new regulatory requirements.

How Can We Help?

Our team of cyber security experts will work with your company to:

- Identify and assess cyber security risks and current compliance with the Code.
- Develop a cyber security document tailored to your organization, in line with BMA requirements.
- Develop document response and recovery processes.
- Oversee design, implementation and monitoring (audit) of controls.
- Provide ongoing support to maintain and grow a cyber security program.

Andersen Global

Nangia Andersen is a full member firm of Andersen Global. Andersen Global is an international association of legally separate, independent member firms with more than 1000+ global partners.

As part of Andersen Global we have reached more than 220 offices globally, having presence in more than 120 countries. Our core values are:

Best-In-Class

We aim to be the benchmark for quality in our industry and the standard by which other firms are measured.

Stewardship

We hire the best and the brightest and we invest in our people to ensure that legacy.

Seamless

Our firm is constructed as a global firm. We share an interest in providing the highest level of client services regardless of location.

Independence

Our platform allows us to objectively serve as our client's advocate; the only advice and solutions we offer are those that are in the best interest of our client.

Transparency

We value open communication, information sharing and inclusive decision making.

OneStopNetworks in collaboration with Nangia Andersen LLP

- Service delivery will be managed and executed in Bermuda by OneStopNetworks. Rene Ambrusch of OneStopNetworks will be your main point of contact in Bermuda.
- Nangia Andersen LLP's cyber security expert team will provide technical support remotely.
- Nangia Andersen's Cyber Security team comprises professionals having unique skills in technology and business from a diverse range of backgrounds, industry & sector experience.
- Nangia Andersen's Cyber Security practice has executed and delivered numerous engagements in multiple geographies across the globe, viz. Africa, the Middle East, Asia Pacific, etc. We collaborate with OneStopNetworks on various client projects Bermuda.

ONESTOPNETWORKS
web development - cloud services

A member firm of ANDERSENGLOBAL

NEXT STEP

To find out more about what the new Cyber Risk Management Code of Conduct means for your business, and for help assessing and managing your cybersecurity program(s), contact our leaders:

OneStopNetworks Bermuda

www.OneStopNetworks.bm

support@onestopnetworks.bm

Tel (441) 296 2836