Cybersecurity regulation on the horizon

The Cyber landscape is constantly evolving and so is the regulatory environment. The Cayman Islands Monetary Authority ("CIMA") released its consultation paper on Proposed Rule & Statement of Guidance ("SOG") – Cybersecurity, comments for which were closed on November 28th 2019. While the final versions are still pending, below are some highlights as you plan your priority focus areas for 2020.

Who should care?

If your organisation is regulated by CIMA – then this applies to you. For clarity this covers entities (including controlled subsidiaries) regulated under the: Insurance Law, Mutual Funds Law (Exceptions: Regulated mutual funds), Securities Investment Business Law, Building Societies Law, Cooperative Societies Law, Development Bank Law, Money Services Law, Companies Management Law, Directors Registration and Licensing Law and Private Trust Companies Regulations.

5 key considerations

- **Formal framework and strategy**
- **Regular self assessments**
- **Increased accountability**
- **Formal intra-group arrangements**
- **Increased regulatory focus**

pwc

Cybersecurity framework and risk management strategy:

If your organization does not currently have a documented cyber strategy, policies and procedures supported by a formalised governance structure then now is a good time to start working on this. While CIMA's proposed Rules and Statement of Guidance is not prescriptive, it does encourage entities to consider leading industry IT frameworks or a combination of industry standards (e.g. NIST, ITIL, COBIT, ISO etc.) in developing its cybersecurity risk management framework and the appointment of one Senior Officer accountable for reporting on the organisation's capability to manage the implementation of the cyber framework and overall cyber-resilience program.

Self assessments:

Aside from the regular penetration testing and vulnerability assessments at least once a year (or more), there is a proposed requirement for regular assessments of cyber strategies and overall framework against the (draft) SOG, Rule, industry frameworks and any emerging trends in cybersecurity, at a minimum, annually. With the growing risks associated with cyber- attacks, it's not surprising to see risk assessments for fraud scenarios and IT General Controls also being included in the scope of testing. Internal Audit (or other independent party) is also expected to play a key role in providing independent reporting to the governing body in respect of the entity's framework including key vulnerabilities identified and potential remediation.

Increased accountability for Governance body:

With responsibility for overseeing cybersecurity and cyber-resilience, the regulated Governance body would now be expected to ensure management supports the Senior Officer accountable for cyber-resilience by the creation, implementation, testing and ongoing improvement of cyber-resilience plans. The Governance body will also be expected to receive regular training and carry 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, if necessary.

More formalised intra-group arrangements:

For organisations relying on parent or Group entities for their cybersecurity posture (e.g. via shared infrastructure, policies and procedures etc.), the draft Rule and SOGs requires these to be more formalised through written agreements. The contents of intra-group agreements are proposed to include details of any outsourced IT or cyber-related matters that may directly impact your business and cyber risks; and the end-of-support dates or replacement of any technology that may impact the regulated entity's cybersecurity.

More regulatory oversight:

The proposed Rule, if approved, requires a 72-hour reporting period to CIMA for material incidents. To avoid ambiguity, guidance on reportable incidents has been provided while still allowing organisations to define incident criticality within their own incident management framework. Cybersecurity and IT system reviews will also be included in the scope of inspections performed by CIMA reinforcing the need to formalise and evidence the cyber strategy and supporting procedures as well as evidence of control implementation.

If the proposed Rule and SOG are finalised and come into effect, organisations may have only 6 months to get ready. We encourage you to read the proposed rules and SOGs in full and consider the potential gaps and next steps, whilst continuing to monitor further developments in this space.

Continue the conversation with us

Marlon Bispath
Partner
Risk Assurance and Advisory
Office: 1 (345) 938 8674
Email: marlon.bispath@pwc.com

Isabel Gumeyi
Senior Manager
Risk Assurance and Advisory
Office: 1 (345) 914 8643
Email: isabel.y.gumeyi@pwc.com