Outsourced IT service providers – understanding your responsibilities

Insights - 11/09/2023

In today's digitally interconnected world, organisations heavily depend on third parties for various critical functions. Whether it's IT infrastructure, software solutions or staffing resources, these external partners play a vital role in an organisation's success.

Despite being aware of this potential danger, many organisations lack a proper risk mitigation strategy, leaving them unprepared and disconnected in managing the problem. Ogier Regulatory Consulting client director Gavin Baxendale discusses the responsibilities for cybersecurity and the nuances between group and local policy and control frameworks.

The responsibility for cybersecurity in these situations is often unclear, leading to assumptions and potential vulnerabilities. Additionally, the involvement of fourth-party suppliers, connected to the original suppliers, can inadvertently expose sensitive data. The reliance on external partners also exposes organisations to a wide array of risks that must be addressed through a comprehensive Third-Party Risk Management (**TPRM**) program.

TPRM entails the systematic process of identifying, assessing, and mitigating risks associated with third parties, in accordance with company cyber security metrics, local and global regulation. This approach requires an enterprise-wide perspective that goes beyond traditional third-party management practices, including the monitoring of service level agreements.

According to CIMA Rule: Cybersecurity for Regulated Entities (April 2023), licensee's governing bodies are ultimately responsible for cyber security (rule 6.1) and more specifically are required to perform an assessment of any providers (whether third parties or affiliates) to which it has outsourced IT functions to ensure their compliance with the Rule and related Statement of Guidance. Furthermore it must have oversight and clear accountability for all outsourced functions as though they were not outsourced. It is also noted that cybersecurity risks may arise in other outsourcing arrangements, not only IT (rule 6.5).

Thematic Review – the findings

The Cayman Islands Monetary Authority (**CIMA**) being the primary regulator responsible for the regulation of financial services entities operating in and from the Cayman Islands released a Thematic Cybersecurity Review in June 2023. The review involved an analysis of 12 regulated entities from across the banking, insurance and securities sectors over a period from April to December 2022. Insights regarding good practices and areas for improvement are outlined here.

"Where cybersecurity functions are outsourced (whether intra-group or to third parties), entities are to assess and gain a level of assurance that the frameworks implemented by the service providers are adequate and fit for purpose."

Good practices:

- Detailed written agreements with intergroup or third-party service providers.
- Written confirmations of the adequacy of frameworks managed at the group level.

Areas of improvement:

- Entities who rely on group framework should receive written confirmation on the adequacy of the frameworks being managed at the group level.
- The need to conduct regular assessment of the intra-group and third-party cybersecurity frameworks against local requirements to ensure compliance.
- The need to ensure outsourcing agreements comply with local requirements.

Areas of weakness in outsourcing are explained in the graph on page 17 of the review.

How can Ogier Regulatory Consulting help?

Whether you have long-standing third-party relationships or have begun the process of choosing a new partner, it's important to understand where you are on the TPRM roadmap. We can assist with developing, managing, and advising with local experts in AML, Cybersecurity and jurisdictional law.

- Third-party identification
- Evaluation and selection
- Risk assessment

- Risk mitigation and management
- Contracting and procurement
- Reporting and recordkeeping
- Ongoing monitoring
- Vendor offboarding
- Governance documentation

Get in touch with us at regulatoryconsulting@ogier.com or learn more on our service page.

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

Gavin Baxendale

Client Director

Cayman Islands

E: gavin.baxendale@ogier.com

T: +1 345 815 1915

Related Services

Ogier Regulatory Consulting

Cyber security consulting

Related Sectors

Technology and Web3