Compliance Can Be Complicated and Expensive

As cyberattacks become more frequent and damaging, we are compelled to rethink our risk strategies – to protect ourselves and our customers from the magnitude of cyber-related financial losses. The practice of recognising risks and guarding against them is imperative to running a successful business, especially now with the threat landscape evolving at a blistering pace in this era, *4th Industrial Revolution* (*4IR*).

One of the biggest and fastest-growing risks that businesses face are cyber-related incidents. The WEF Global Risks Report 2019 highlights a significant increase in the risk of cyberattacks leading to theft of money, data, and the disruption of operations.

Small- to medium-sized businesses are not safe from cyberattacks. Attackers target networks of small companies as they tend to be less secure than larger corporations. As a smaller organisation, you don't have the time, resources, or budget to implement expensive, time-consuming security practices.

The challenge for smaller organisations is to be secure and compliant without having to purchase expensive cybersecurity tests and tools.

Working with Cerebus

To mitigate against these barriers, Cerebus has developed an approach that is designed to meet the regulatory requirements while remaining within budget constraints. Every organisation – big or small – deserves the opportunity to be secure and safe; we believe that our services can achieve this for you. Our cybersecurity audits include a *comprehensive report* with *actionable intelligence* ™ to further your cybersecurity program and *prove compliance*.

Cybersecurity Audit

Although your firm may have IT security controls, do you verify that these controls are in place and working to protect your organisation? Our cybersecurity auditors are tasked to review your IT environment and report – with physical proof – on the implementation of controls.

Our *cybersecurity audit is scalable* to the size of the organisation and its risk posture. Audits are optimised to suit the organisation's context while still *adhering to the standard Information Security requirements* from examiners.

Our Cybersecurity Audit Is Designed To:

- ✓ Adopt a risk-based approach by giving priority to the most exploited weaknesses
- ✓ Deter attackers from seeing you as an easy target
- ✓ Align to budget constraints
- ✓ Create a cybersecurity roadmap
- ✓ Provide real-time actionable intelligence to strengthen your cybersecurity program.

Risk Assessment

Risk assessments identify threats to your assets, as well as the impact and probability of those threats occurring within your IT environment. Cerebus *evaluates both the existence of security controls*, and the *effectiveness of controls* used to mitigate threats to your IT security program. Cerebus will enable you to *better understand your security posture and risk level* as viewed by the regulatory bodies. In addition, Cerebus will provide you with a remediation action plan: a foundation for reducing the identified risks.

Network Assessment

Together with the cybersecurity audit, clients receive a network assessment bundle – an *internal and external network vulnerability assessment* and an *external penetration test of critical systems*.

A *vulnerability assessment* involves a comprehensive scan of your firm's internal and external networks to identify any vulnerabilities on the systems.

During the *external penetration test*, an attempt is made to manually exploit any of the vulnerabilities identified to determine what an attacker could potentially access.

From these tests, which reveal the most exploited weaknesses in your firm's network, Cerebus provides recommendations on how to *secure vulnerabilities* to *reduce your risk exposure* to easy target attacks.