A Spotlight On... Operational Resilience

Background

Operational Resilience describes an organisation's ability to protect or sustain its critical functions in the face of operational disruptions by anticipating, preventing, recovering from, and adapting to such disruptions.

Cyber security is one of several key pillars organisations must focus on to improve this ability.

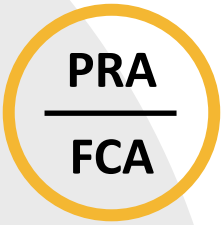
Business services that can impact customers or financial stability should be prioritised, the critical business processes supporting them identified, and the impact tolerance established.

Everyone is talking about it — why now?

There has been a strong regulatory focus on Operational Resilience in recent years. The Prudential Regulation Authority (PRA) in particular has committed to strengthening its supervision in this area.

The threat of a cyber attack is often cited as the most urgent concern among senior executives. This reflects the number of incidents and their potential financial and reputational impacts.

Organisations require both new and enhanced frameworks, as well as the governance to manage increasingly strict requirements.



These are testing times for many...

At the heart of Operational Resilience for cyber security is understanding the level of protection applied to your critical assets through an effective control testing approach.

Many organisations struggle, however, to ensure their cyber control testing is rigorous enough to meet increasing regulatory demands.

They often rely on information captured from only a small proportion of the IT assets supporting their critical business processes (CBPs).

i-confidential has the answers

We help clients address their Operational Resilience challenges with **Security Metrics**, a comprehensive library of metrics aligned to controls that enable organisations to effectively manage security.

- **Security Metrics** uses i-confidential's Control Framework, which is based on best practice and industry standards, such as ISO and NIST. It covers all the typical controls organisations require.
- **Security Metrics** can measure cyber controls used to secure CBPs against the stringent tolerances required for Operational Resilience.
- **Security Metrics** enables organisations to ensure control measurement is both comprehensive and meaningful. It provides the key dimensions for most security metrics — coverage, results, and remediation.

By overlaying agreed tolerance levels with **Security Metrics**, an overall Cyber Resilience Score can be established.

The responsible executive can use the Cyber Resilience Score and supporting data to focus remediation tasks and report to the wider organisation and regulator, instilling confidence that security is understood and managed.

For more information about how we can help your business, please contact us

i-confidential
Cyber Security & Information Risk Specialists®

www.i-confidential.com
info@i-confidential.com
0131 445 1458