

UK FINANCIAL SERVICES: ARE YOU READY FOR THE FCA'S OPERATIONAL RESILIENCE?

WHAT?

The Operational Resilience regulation has been compiled as a joint venture between the Financial Conduct Authority (FCA), Bank of England and the Prudential Regulation Authority (PRA).

WHEN?

Implemented in full by March 2025.

WHO?

Banks, building societies, Insurers, PRA-designated investment firm and Recognized Investment Exchanges.

WHY?

- 1) Operational disruptions and the unavailability of important business services caused by coronavirus (Covid-19) have shown the potential to cause wide-reaching harm to consumers and businesses, cause risk to market integrity, threaten the viability of firms, and cause instability in the UK financial services system.
- 2) It is vital for organizations to understand the important business services they provide, and to invest in their resilience to protect themselves, consumers, and markets.

Operational Resilience Requirements

- **Identify your important business services (IBS)** that if disrupted, could cause intolerable harm to your customers, risk to market integrity, and threaten your firm's viability.
- **Set impact tolerances** for the maximum tolerable disruption to these services.
- **Carry out mapping and testing** to a level of sophistication necessary to identify the IBS, set impact tolerances and identify any vulnerabilities in your operational resilience.
- **Conduct** lessons learnt exercises to identify, prioritise, and invest in your ability to respond and recover from disruptions as effectively as possible.
- **Develop** internal and external communications plans for when important business services are disrupted.
- **Prepare self-assessment documentation** based on the questionnaire from the FCA.

How Fortinet Is able to help

Our Cyber Threat Assessment Program (CTAP) first provides detailed gap analysis of your current cyber security posture against best practice and we will design a cyber security framework to address your security needs.

Potential security needs addressed:

- **Risk Management:** Fortinet provides unified risk management across environments leading to consolidation of governance, policies, and monitoring.
- **Operational Resilience:** The Fortinet Security Fabric is the industry's most comprehensive cybersecurity platform, with a rich open ecosystem spanning over 500 security and networking integrations. It covers the extended digital attack surface and cycle, enabling self-healing security and networking to secure people, devices, and data.
- **Security monitoring:** Fortinet provides solutions to allow customers to monitor and track risk. FortiManager supports network operations use cases for centralized management, compliance best practices, and workflow automation to protect against advanced threat actors. The threat intelligence provided by FortiGuard Labs helps organizations stay ahead of new and existing threats.
- **Digital resilience testing:** Fortinet customers benefit from a long-standing commitment to meet the requirements of the most security-minded organizations. With a broad portfolio, comprehensive service offering, and a strong network of partners, Fortinet can help customers test their systems and networks to meet regulatory demands.
- **Incident Response Services:** FortiGuard Incident Response Services deliver critical services before/during/after a security incident. Our experts arm your team with fast detection, investigation, containment, and rapidly recover your business to operation in a safe manner.

Get in touch today for your customized

CYBER THREAT ASSESSMENT