open gi

Operational Resilience

Strengthening Security Postures

In response to the growing sophistication and frequency of cyber threats, plus perceived weaknesses of general operational resilience in the financial services sector, regulatory oversight has intensified, emphasising the need for organisations to strengthen their operational resilience and security postures.

Notably, the recently implemented EU Digital and Operational Resilience Act (DORA), plus the UK's Bank of England PRA SS1/21, and other FCA or FCA/PRA joint statements, have substantially raised the bar of operational resilience. What were previously "best-practices" have become regulatory requirements for our customers.

ogi

The Five Pillars of DORA

Although DORA is an EU regulatory framework and may not be directly or indirectly applicable to some UK entities, it is viewed as being more prescriptive than its English counterparts and is helpful in setting the bar for operational resilience controls.

DORA, specifically, is underpinned by Five Pillars. These are:

- **ICT[1] risk management**
- **Incident reporting**
- **Digital operational resilience testing**
- **Information sharing**
- **Third-party risk management**

As an organisation, Open GI has adopted and built upon these Five Pillars as part of our operational resilience strategy.

Our Commitment

Open GI recognises the key role we, and our solutions, play in our customer's daily operations, and the necessity for consistently reliable services. We are fully committed to upholding the highest standards of operational resilience and to aiding our customers to satisfy their regulatory compliance requirements.

[1] *Information and Communication Technology – A broad term used to capture IT (Information Technology) including all associated technologies, such as networking, software, end user devices, internet cloud services, etc.*

Our Approach

In this document, we will demonstrate our approach to operational resilience and how this is implemented across our organisation against the five pillars outlined above.

ICT risk management

A core component is a risk management framework that focuses on identification and management of risks; protection, prevention, detection, and response to risks or threats; recoverability of systems and processes; secure and frequent backups; lessons learned; and continually strengthening technical and organisational controls to minimise risks.

- Open GI's ICT Risk Management Framework includes an operational risk register, plus more focused risk registers such as cyber, and cover all aspects of the business, including:
  - Cyber
  - Data protection
  - Operational risk
  - People related risk
  - Environment risk
  - Financial risk
- Through the ICT Risk Management Framework and associated risk registers, we aim to proactively identify potential risks and mitigate them before they become material issues.
- Our risk management process and risks registers, as well as our risk appetite and tolerances, are regularly reviewed by our Executive Team.

Incident reporting

Mitigating the impact of ICT related incidents through preparation testing and having robust mechanisms in place to report incidents in a timely manner, with accurate and frequent updates.

Open GI has a comprehensive Incident Reporting and Management process in place that includes the following:

- Incident Notification: Notify affected customers of significant ICT related incidents within 24 hours of detection.
- Incident Response Plan Testing: Test incident response plans (which include our Business Continuity Plan and Disaster Recovery Plan) at least annually to ensure effectiveness and readiness.
- Maintain logging records to facilitate detailed post-incident analysis and compliance audits.
- A documented process to ensure quick classification of an incident and the allocation of an appropriate severity level to ensure a consistent and clear response.
- Detailed internal and external reporting and record keeping, including root cause analysis and lessons learned.

Digital operational resilience testing

Establishing a comprehensive testing program, which includes system and data recovery testing, vulnerability assessments, open-source code analysis, network security assessments, process audits and subsequent gap analysis, scenario-based resilience and recoverability tests, including desktop-based assessments.

To ensure business continuity in unforeseen circumstances, Open GI implements various measures to assess and enhance its recovery capabilities, minimising disruptions. Measures include:

- Business Continuity and IT Disaster Recovery Plans.
- Scenario planning and desktop based “what if” exercises.
- External penetration testing.
- Internal vulnerability testing.
- Software development pipeline code scanning for vulnerabilities.
- Monitoring of open-source libraries.
- Supporting resilient infrastructure such as dual active-active (mirrored) data centres.
- Strengthening of internal audits and testing against policies and applicable regulations.

Information sharing

Encouraging and enabling information sharing of threat and vulnerability intelligence between entities, including between Open GI departments, its customers, its own partners, and other appropriate interested parties.

While not all incidents are preventable, the impact and frequency of them can be mitigated through proactive information collection and dissemination.

- Open GI employs a system of continuous system monitoring to notify our specialised systems engineers of any irregularities.
- Monitoring capabilities are subject to continuous enhancement, reflecting the ongoing development of systems and software.
- We consistently seek to enhance our intelligence-gathering methodologies in response to developing threats or regulatory frameworks.
- Log files, alerts, and threat indicators undergo analysis and remediation to proactively mitigate incidents.
- To minimise threats and the impact of incidents, information is disseminated amongst internal teams and, when appropriate, external partners, suppliers, and customers to foster collaboration.
- Proactive monitoring of external security bulletins/advisories to ensure the prompt deployment of any required patches or mitigations.

Third-party risk management

Effective management of ICT third-party risk is required, encompassing ICT risks and vulnerabilities and upstream operational resilience.

We maintain control over our supply chain through risk management processes, including:

- Assessment and scoring of all suppliers based on criticality and risk exposure.
- Contract and documentation reviews before onboarding new vendors.
- Monitoring of supplier compliance through periodic audits, with further enhancements planned.
- Appropriate contractual terms with third parties addressing risk, cyber, and data protection.
- Dedicated partner managers for key suppliers or business partners.
- Responding to our customers' needs for compliance alignment through targeted due diligence questionnaires, or other assessments or workshops.

More information

For more information about our operational resilience measures, please contact your OGI Account Manager in the first instance.