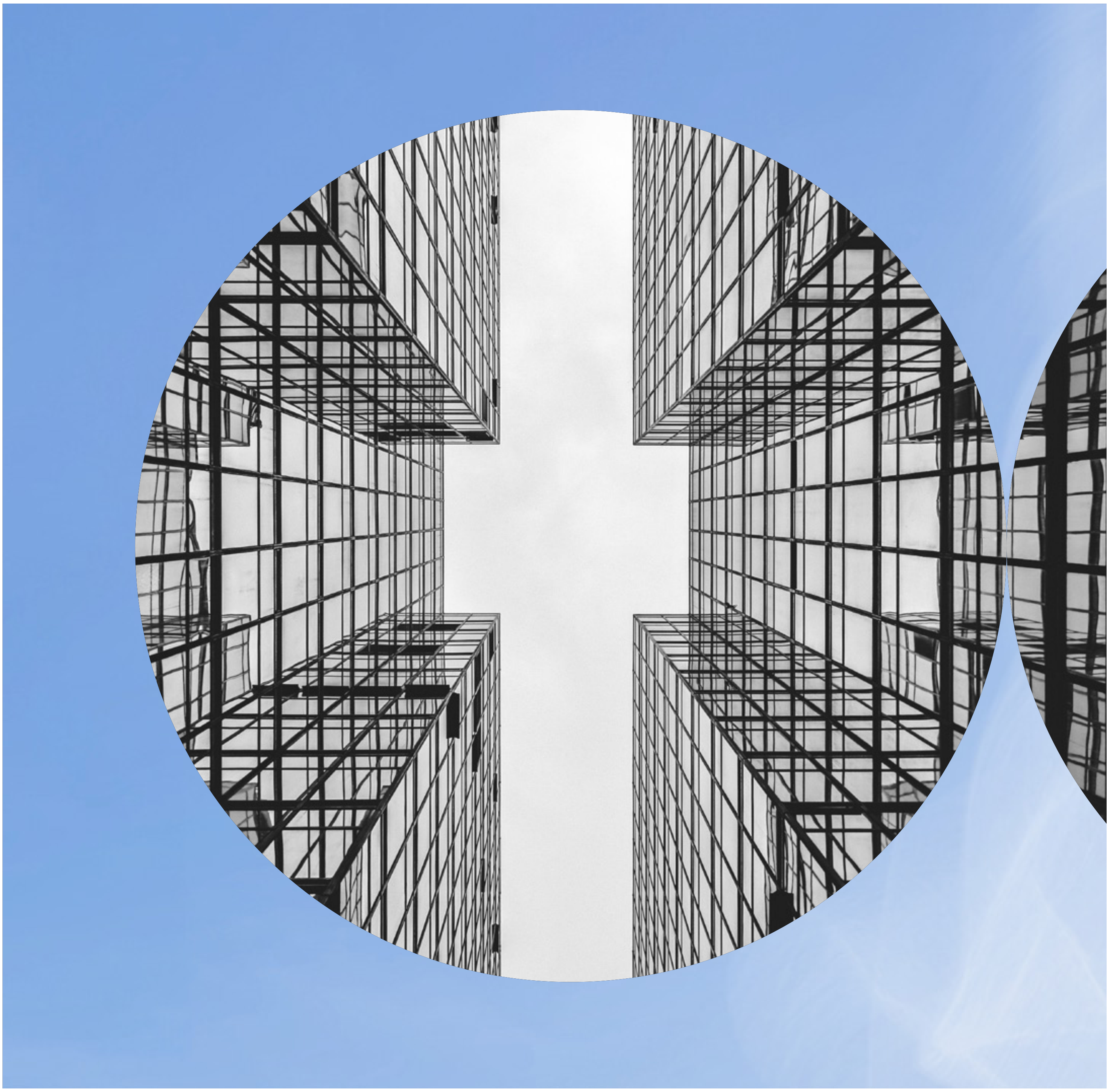
DORA compliance

Digital Operational Resilience Act

Visit: www.pgitl.com
Email: findoutmore@pgitl.com

Phone: +44 (0) 20 4566 6600
Address: 13-14 Angel Gate, London, EC1V 2PT, UK

PGI - Protection Group International Ltd.
Registered in England & Wales. 07967865



What is DORA?

The Digital Operational Resilience Act (DORA) is a regulation introduced by the European Union to strengthen the resilience of the financial sector in the face of increasing cyber attacks and other digital risks.

It aims to ensure that financial institutions including banks, insurance companies, and investment firms, are resilient against, and can recover from, cyber incidents, operational disruptions, and other technological challenges.

DORA sets out a comprehensive framework for managing your digital operational risks and lays down specific requirements for risk management, testing, incident reporting, and third-party service provider oversight.

Benefits of DORA

DORA has the potential to create a virtuous cycle by strengthening risk management, business alignment, and operational resilience within the sector. It encourages entities to go beyond compliance and integrate these priorities into their overall strategy.

This connection between operational teams and leadership aligns strategic and operational priorities, fostering a culture of continuous improvement. It also empowers IT risk teams and supports the transformation of organisations toward greater digital resilience.

Risk Management

By adopting DORA, businesses can better withstand digital disruptions and maintain operational continuity.

Regulatory Confidence

Ensuring compliance with DORA builds trust with regulators and stakeholders.

Improved Cyber Resilience

DORA encourages businesses to adopt advanced cybersecurity practices, reducing the risk of cyberattacks.

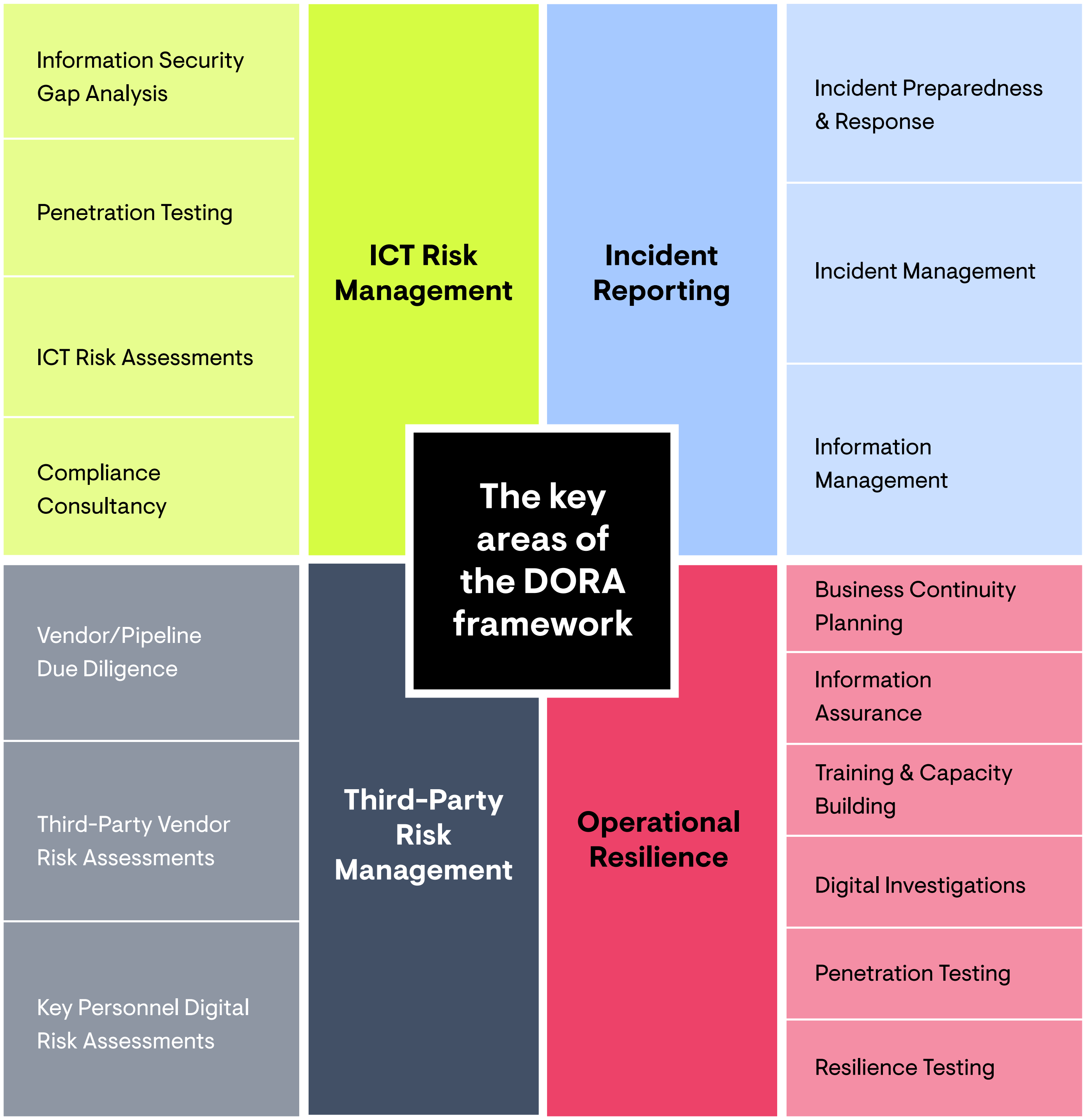
How does DORA work?

DORA works by mandating financial entities to implement robust operational resilience frameworks to reduce risks and strengthen security.

Historically, these areas are often handled in a fragmented, siloed manner. However, DORA demands significant and measurable progress in resilience, which requires a more coherent and integrated business approach.

We know that the weight and scope of these new regulations can be overwhelming, even for more experienced risk managers. That's why PGI are here to manage all areas of the DORA framework to help you successfully achieve and maintain compliance.

DORA can be broken down into the following four key areas:



The key areas of the DORA framework

ICT Risk Management
- Information Security Gap Analysis
- Penetration Testing
- ICT Risk Assessments
- Compliance Consultancy

Incident Reporting
- Incident Preparedness & Response
- Incident Management
- Information Management

Third-Party Risk Management
- Vendor/Pipeline Due Diligence
- Third-Party Vendor Risk Assessments
- Key Personnel Digital Risk Assessments

Operational Resilience
- Business Continuity Planning
- Information Assurance
- Training & Capacity Building
- Digital Investigations
- Penetration Testing
- Resilience Testing

What are the main challenges in implementing DORA?

Coordinating a wide range of stakeholders across the business—including cybersecurity, risk management, procurement, legal, and IT—can cause challenges when attempting to align new policies and processes.

Third-party risk management is another significant challenge posed by DORA. This is often a neglected area, with third parties often poorly managed or structured, meaning it's difficult to get a comprehensive overview.

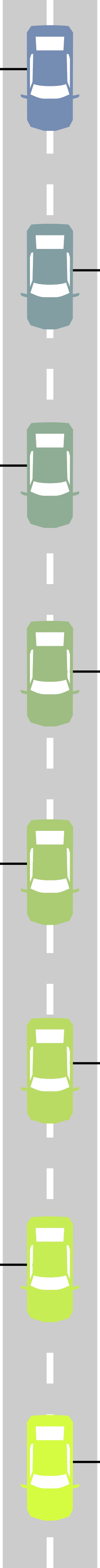
PGI can support organisations with the implementation of new policies and processes to mitigate risks. We also support with third-party vendor risk assessments to help clients get a clear insight of their supplier's security position.

One partner for all your DORA requirements

Whether you need support with identifying gaps in compliance, assessing your third-party vendors or implementing new policies or processes, PGI has a team of specialists with extensive experience across cybersecurity and digital resilience, so you can confidently achieve and maintain compliance through one trusted partner.

If you're not sure where to start, PGI can support you with a thorough gap analysis which will provide you with actionable insights into areas that need improvement so that you can prioritise and address any identified gaps to achieve compliance.

The Road to Achieving DORA Compliance



Scoping your requirements

Consultation: Our experts will meet with you to discuss support areas and your business requirements.
Gap analysis: We will conduct an assessment to identify all areas needing improvement.

Prioritisation

Detailed report: We provide a detailed report of all gaps and offer our recommendations.
Prioritisation: Gaps are prioritised based on their impact on compliance and operational resilience.

Strategic planning

Customised strategy: We create a tailored implementation plan aligned to your operations.
Timeline: We will establish a clear timeline with milestones to track your progress towards compliance.

Implementation

Framework creation: We help you to implement new policies and procedures that meet DORA requirements.
Regular updates: Policies are continuously reviewed and updated.

Continuous improvement

Staff training: We will conduct comprehensive training for staff to ensure they are fully equipped and understand the new policies and procedures.
Simulations and drills: We implement regular simulations and drills to test incident response and operational resilience plans.
Continuous learning: We promote a culture of continuous learning and improvement.

Ongoing support and consultancy

Expert guidance: We will provide close support and guidance throughout the process to address any challenges or changes to requirements.
Regular check-ins: We schedule regular check-ins to review progress towards DORA compliance and any adjustments needed.
Audit preparation: We help you to prepare for internal and external audits.
Review: We continuously refine and improve policies, procedures, and practices.

Measuring success

Performance metrics: It's important that you're able to measure and monitor the effectiveness of your new processes. We will help you to establish key performance indicators (KPIs) to monitor performance.
Reporting: We provide regular updates on compliance status and ensure timely, accurate incident reporting.

Completion

Final evaluation: We hold a final meeting to confirm with you that the work has been completed effectively and to a high standard.

Why choose PGI to support you with DORA?

Expertise in digital resilience:
Our team of specialists have extensive experience in digital resilience, incident response, information assurance and cybersecurity.

One supplier for all your business needs:
At PGI, our experts boast a wide range of expertise across cybersecurity and digital investigations, so you only need one partner for all your security needs.

Tailored implementation plans:
We understand that every organisation is unique. We offer customised digital resilience frameworks that align with your business needs, ensuring a seamless integration of DORA requirements.

End-to-end support:
From initial assessment to final certification, PGI provides close and continuous support, including consultancy, policy development, training, and audit preparation.

Ongoing compliance management:
We help our clients to maintain DORA compliance through regular testing, audits, risk management, and continuous improvement processes.

Incident response expertise:
We help organisations develop tailored incident response plans, ensuring you can quickly and effectively respond to digital disruptions specific to your industry.

Regulatory knowledge:
Our consultants are passionate about what they do. We stay up to date with the latest regulatory changes, ensuring you are always aligned with current DORA standards.

Proven track record:
We have successfully guided organisations through complex compliance processes, making us a trusted partner for achieving DORA compliance.