

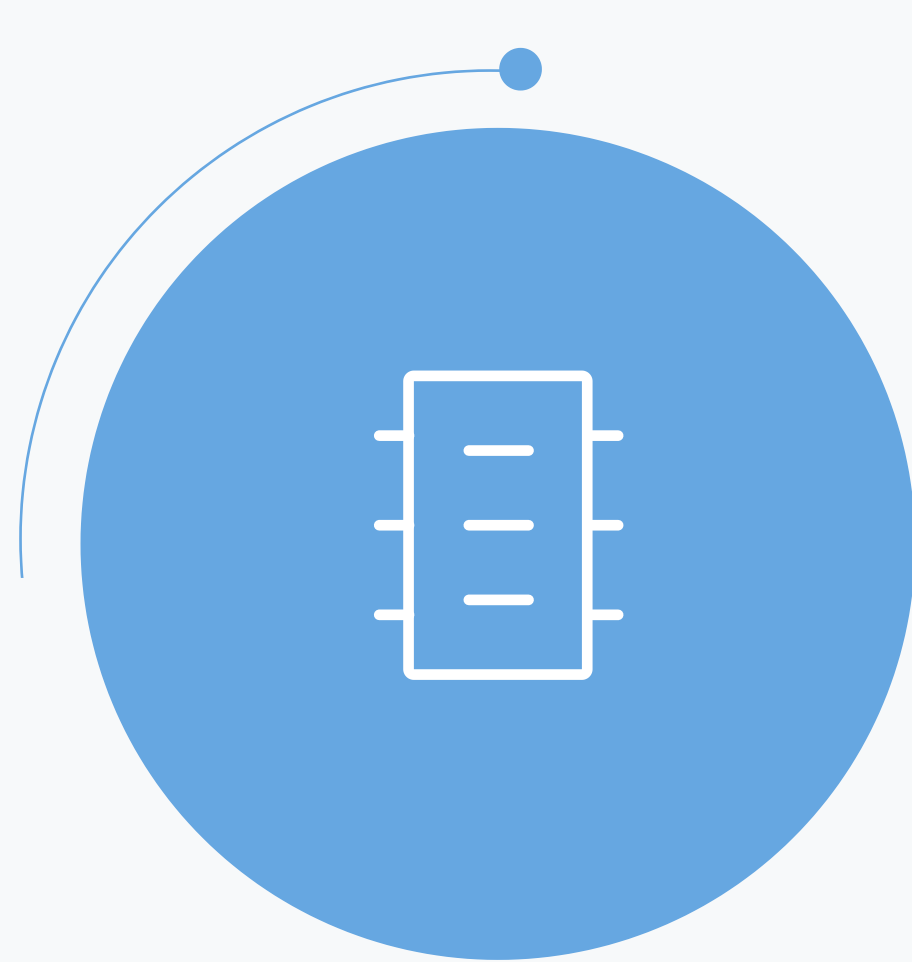
Operational Resilience and the **Five Pillars** of EU DORA

The Digital Operational Resilience Act (DORA) requires more than a checklist, it requires organizations to demonstrate that they can withstand, respond to, and recover from ICT-related disruption.

Achieving this demands a connected approach to governance, performance, risk, and compliance across the five pillars of digital operational resilience.



**ICT Risk
Management**



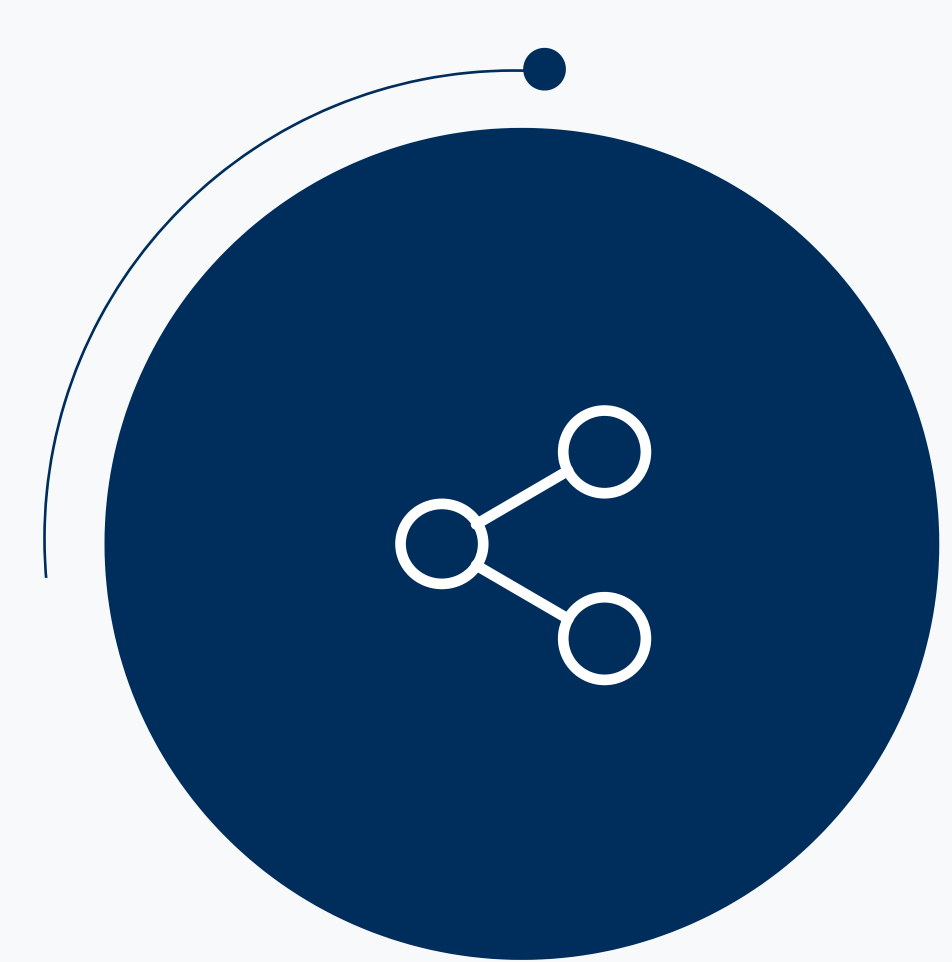
**ICT Incident
Management
& Reporting**



**Digital
Operational
Resilience
Testing**



**ICT
Third-party
Risk**



**Information
Sharing**



ICT Risk Management

ICT risk management provides the foundation for DORA by helping organizations identify, manage, and monitor risks across the technology and services critical to their operations. It does this by connecting critical business services with their underlying systems, processes, data, and dependencies to create a clear, connected view of operational risk.

ICT Incident Management & Reporting

ICT incident management and reporting supports DORA by enabling organizations to detect, classify, respond to, and report significant ICT incidents in a timely and coordinated manner.

It does this by connecting incident detection and response to the affected business service, its dependencies, and accountable teams, ensuring faster decisions, coordinated action, and continuous learning from every incident.



Digital Operational Resilience Testing

Digital operational resilience testing supports DORA by helping organizations regularly test and validate whether critical business services can withstand and recover from disruptive events.

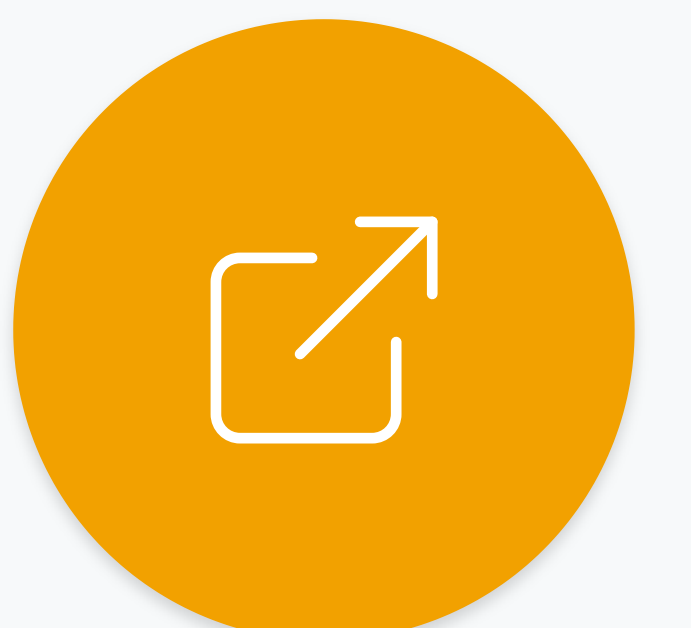
It does this by using realistic, service-centric scenarios to test dependencies, identify weaknesses, measure resilience, and ensure findings lead to continuous improvements.



ICT Third-party Risk

ICT third-party risk management supports DORA by helping organizations manage and maintain oversight of the risks and dependencies associated with external ICT service providers.

It does this by creating a clear, connected view of third-party relationships, their obligations, dependencies, and concentration risks throughout the entire provider lifecycle, from onboarding to exit.



Information-sharing

Information-sharing supports DORA by helping organizations strengthen collective resilience through the timely exchange of relevant cyber threat intelligence and good practices.

It does this by connecting external threat intelligence with internal operations, enabling organizations to identify relevant risks and translate insights into timely, targeted defensive actions.



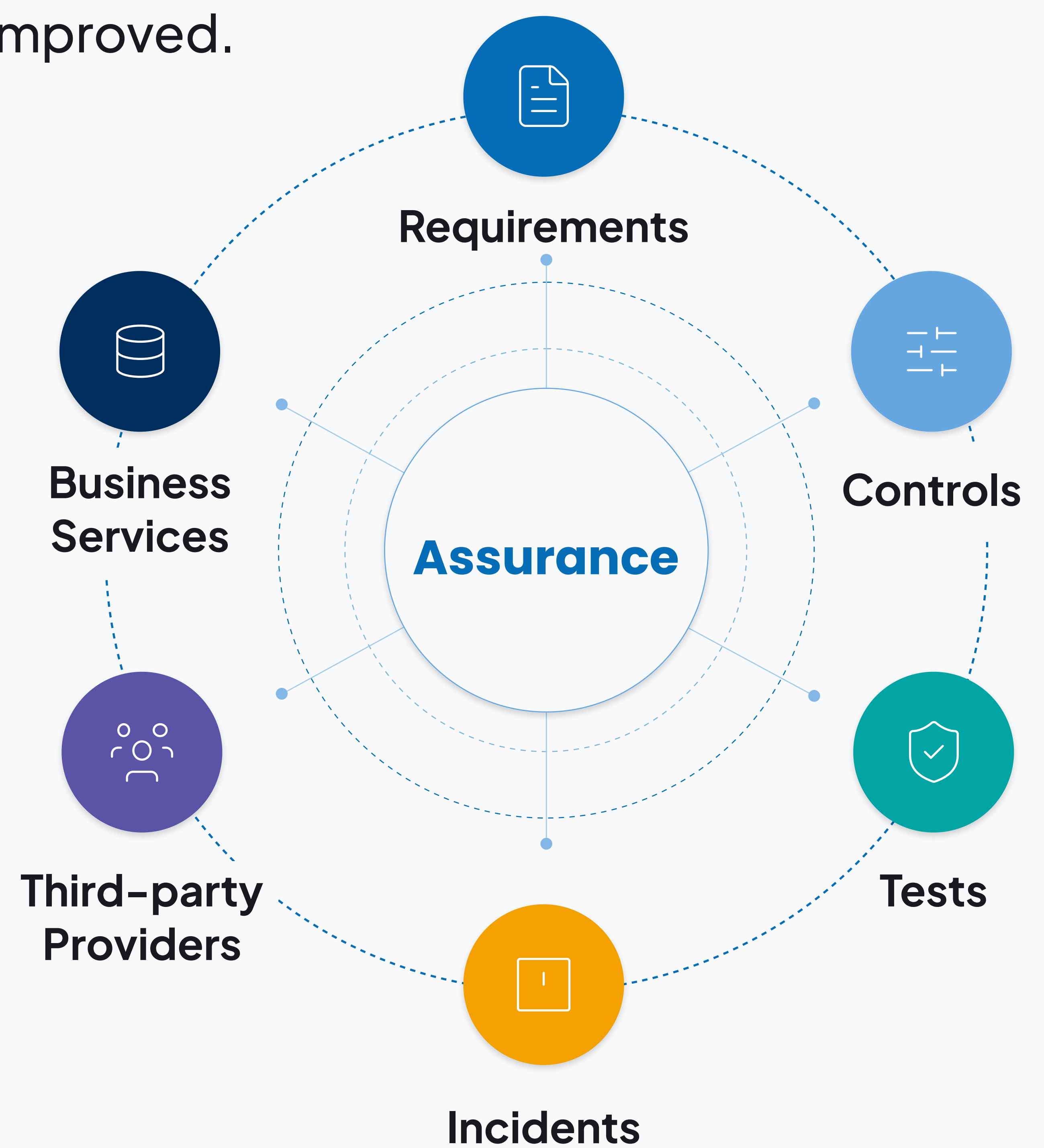
Operational Resilience with Assurance by Design

DORA requires more than compliance, it requires organizations to demonstrate that operational resilience is actively governed, tested, and continuously improved.

How Corporater Helps

GPRC brings governance, performance, risk, and compliance together to create a clear, evidence-based view of operational resilience.

By connecting requirements to controls, tests, incidents, third parties, and business services, organizations can provide assurance by design and give leaders the insight they need to see, decide, and act with confidence.



Operationalizing DORA

Corporater helps organizations operationalize EU DORA requirements by establishing and documenting a digital operational resilience program that strengthens capabilities for:

- Protecting ICT services
- Detecting disruptions
- Containing incidents
- Recovering operations
- Repairing ICT-related incidents

Explore Corporater Operational Resilience Software.

[Explore the solution →](#)