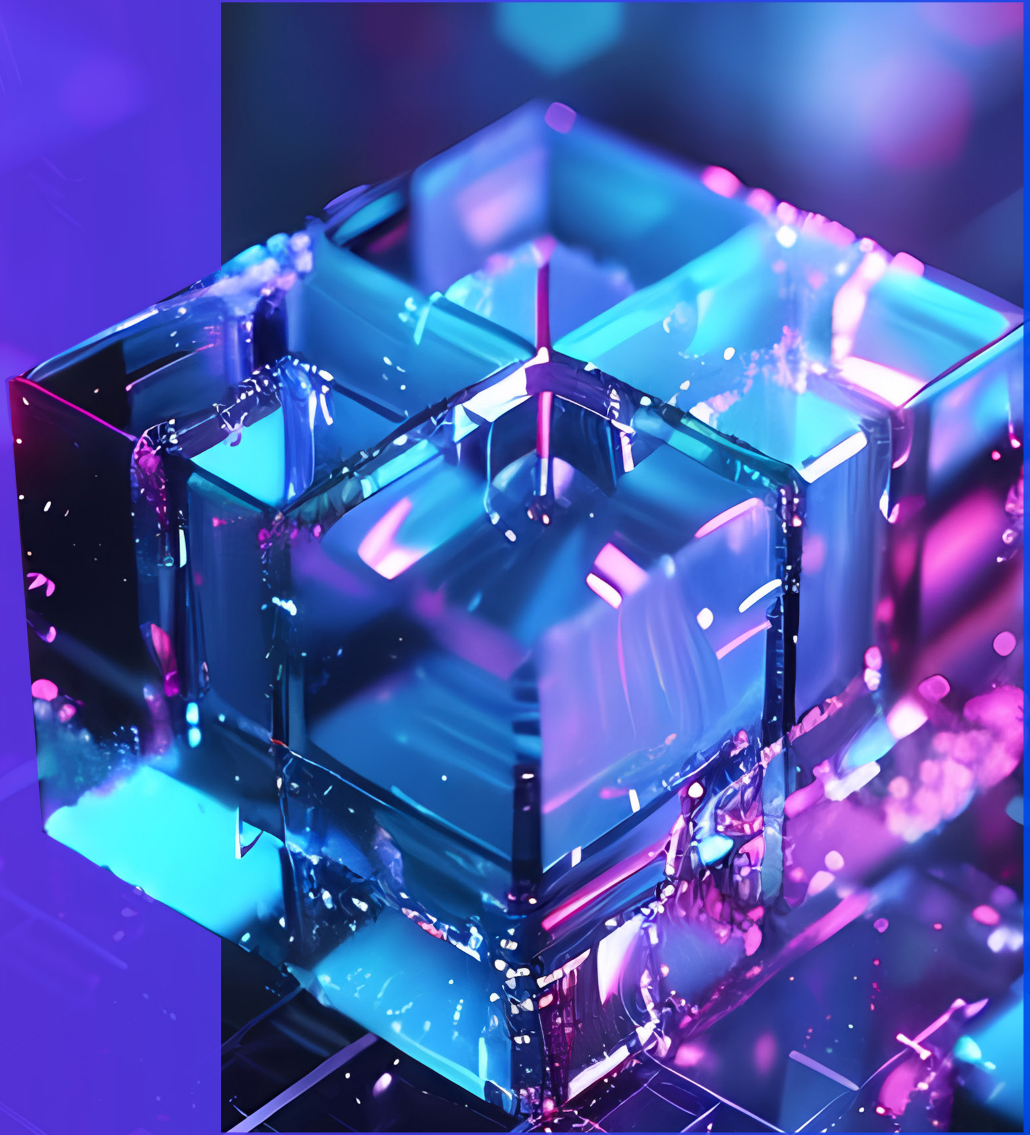
KPMG | servicenow

Rise to the challenge of DORA compliance



KPMG International

kpmg.com/servicenow

Rise to the challenge of DORA compliance with KPMG and ServiceNow

In today’s rapidly changing business environment, operational resilience is more critical than ever. Increasing cyber threats such as ransomware and sophisticated Generative AI phishing attacks are putting businesses at risk. To create this resilience, organizations need to take a proactive, end-to-end approach to managing cyber risks, moving beyond static, siloed risk and compliance management. Different industries have attempted this over the years, particularly in the areas of cyber security, business continuity, and disaster recovery, but the approach has been inconsistent and, in many cases, ineffective.

That’s why the European Union has introduced regulations such as the Digital Operational Resilience Act (DORA) and the Network and Information Security Directive (NIS2) to combat the ever-present spectre of cyber disruption. DORA, in particular, formalizes the approach to operational resilience for financial institutions, rather than leaving it up to each financial organization to define their own approach. The goal of DORA is to provide a prescriptive framework for resilience — including how to prepare for disruptions, how to act when disruptions occur, and how to report disruptions — through a combination of proactive and reactive capabilities.

In today’s rapidly changing business environment, operational resilience is more critical than ever. Increasing cyber threats such as ransomware and sophisticated Generative AI phishing attacks are putting businesses at risk.

DORA creates significant new challenges for financial organizations

The breadth and depth of DORA places a major strain on financial businesses, requiring them to define robust methodologies to address gaps in their current processes and to consolidate their tooling to ensure situational awareness. While operational resilience is not foreign to most mature financial companies, it would be wrong to assume resilience is the same as compliance with the entire DORA framework. DORA goes far beyond what has been traditionally addressed by existing resilience programs, especially in the areas of reporting critical incidents as well as information exchange and reporting, which today are only partially addressed or handled informally.

Furthermore, the rigid, end-to-end regulatory structure is incompatible with historically siloed approaches to IT disciplines such as incident management, business continuity management, disaster recovery, security operations, and risk and compliance management. For example, despite having a long history advising clients in these areas, KPMG firms needed to combine and reinvent how these disciplines can better flow together, creating new processes, teams, and departments to better support clients.

> **DORA goes far beyond what has been traditionally addressed by existing resilience programs.**

Success requires the right methodology and technology

A detailed methodology is required for true operational resilience (and DORA compliance). This methodology needs to provide a systematic and structured approach to identifying, assessing, and monitoring digital operational risks. This includes:

- Identifying critical processes and services that need to be protected.
- Implementing risk identification and assessment processes.
- Reducing the likelihood of identified risks through controls and other mitigation initiatives.
- Monitoring the entire value chain of suppliers of critical processes and services.
- Creating effective business continuity and disaster recovery plans.
- Continuously testing digital resiliency measures and continuity plans.
- Providing transparency about digital resilience status through reporting.
- Proactively monitoring for new and emerging digital threats.

However, while the financial sector is used to being heavily regulated and has strong policies, processes, and controls in place, KPMG professionals' experience with clients is that these are often disjointed. Proactively mitigating risk while ensuring business continuity requires a methodology that creates alignment across processes, disciplines, and departments. Resilience is inherently dependent on seamless flows of data across the organization to create situational awareness, and it requires cross-functional collaboration.

Enabling technology is also critical. This technology must drive end-to-end operational resilience process flows and provide effective data analysis to support risk-informed decision making:

- Just like an effective methodology, effective technology should aim to **break down data silos**, overcoming existing layers and barriers to provide the end-to-end visibility of information needed to identify potential threats and create situational awareness across the organization. It should also be able to analyze and present this data in a comprehensible manner to simplify compliance with DORA's extensive transparency and reporting requirements.
- To provide transparency and allow operational resilience to scale efficiently, the technology also has to **automate and monitor key processes**. This includes activities such as resolving system vulnerabilities, monitoring risks in real time, enforcing policies and

practically monitoring controls, automating testing, managing incident responses, and capturing and exercising business continuity plans. Automation also increases speed, allowing businesses to identify and respond to issues and breaches in real time, minimizing or preventing disruptions.

However, based on experience with clients, the IT toolbox today is just as fragmented as the existing operational resilience methodologies it supports. This creates a major dilemma. IT systems grow organically over time and represent major investments — investments that can't simply be discarded and replaced. What is needed is a platform that can bring together existing systems, creating end-to-end visibility and automating a comprehensive set of operational resilience processes. Ideally, this platform should also already exist in-house to leverage existing investments and accelerate implementation.

Together, KPMG and ServiceNow help address the challenges of DORA compliance

As trusted advisors, KPMG professionals have long experience helping clients address complex, transformative risk, compliance, cyber security and resilience issues. This has given KPMG firms the insights and experience needed to help financial organizations successfully drive cross-functional operational resilience programs. At the same time, ServiceNow provides a unified platform that brings together end-to-end information and workflows, and which offers advanced operational resilience capabilities that cover the full set of core DORA requirements.

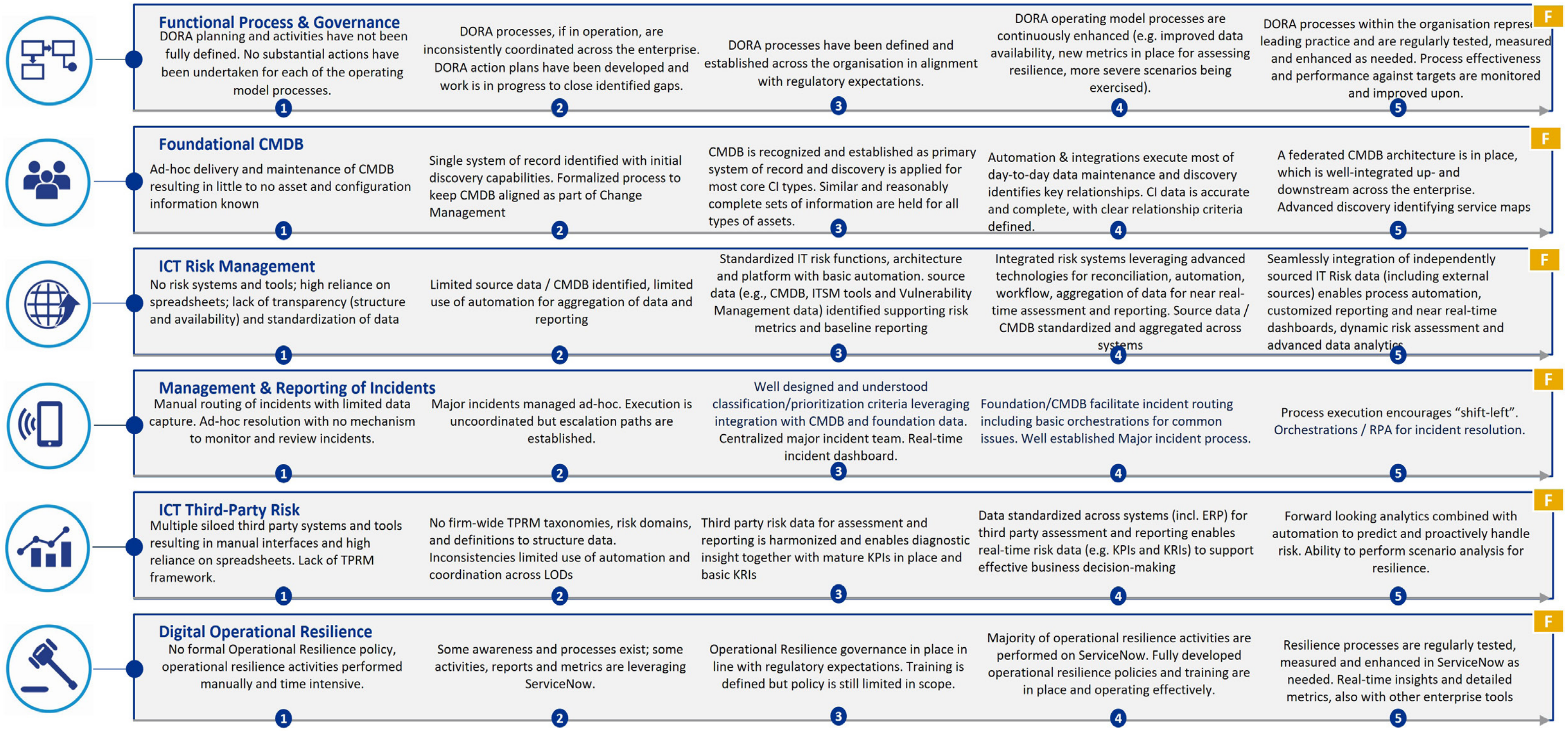
KPMG and ServiceNow have also enjoyed a close alliance partnership for more than a decade, spanning IT, risk, cyber security, HR, ESG, and other areas. This alliance is further strengthened by the ubiquitous nature of the ServiceNow platform — many KPMG clients already have ServiceNow in their IT ecosystem, which KPMG professionals have often helped to implement. Our collaboration on helping clients address DORA challenges and achieve operational resilience has only served to strengthen this relationship. The combination of this alliance, KPMG professionals' deep industry experience, ServiceNow's comprehensive capabilities, and the opportunity to leverage an existing technology platform investment make KPMG and ServiceNow the natural choice for financial institutions looking to strengthen their operational resilience and achieve DORA compliance.

> **KPMG and ServiceNow have also enjoyed a close alliance partnership for more than a decade, spanning IT, risk, cyber security, HR, ESG, and other areas.**

An aligned approach to methodology and technology

KPMG has developed Target Operating Models (TOMs) covering the gamut of processes that are relevant to DORA. These TOMs are based on hundreds of projects successfully executed by KPMG firms with clients across the globe, represent detailed leading practices down to the individual process level, and provide a pragmatic five-step maturity model that allows financial organizations to grow their operational resilience capabilities over time. They are also designed to work seamlessly with ServiceNow operational resilience capabilities, creating the crucial methodology/technology alignment needed to drive success.

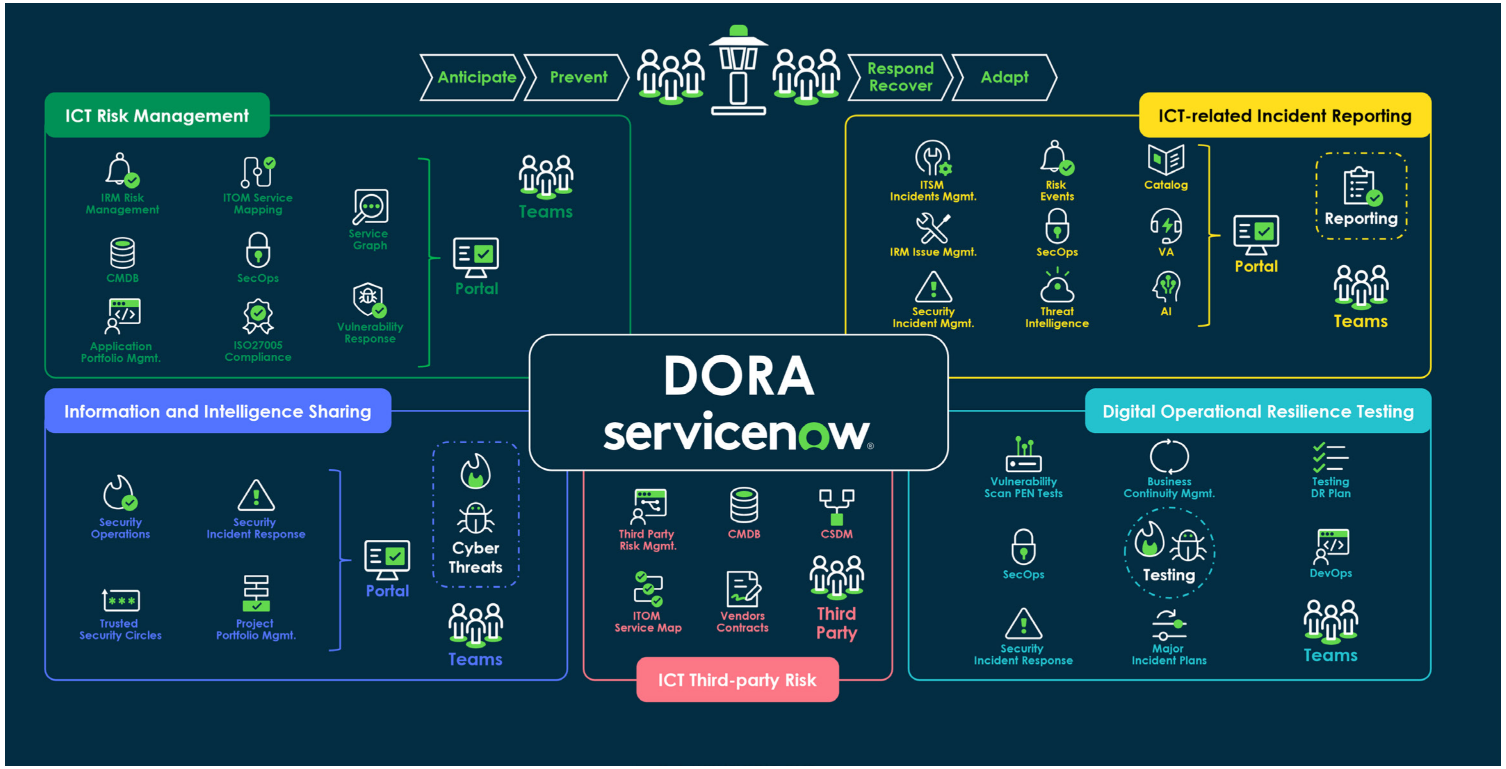
Target Operating Models deliver leading-practice processes



	1	2	3	4	5
Functional Process & Governance	DORA planning and activities have not been fully defined. No substantial actions have been undertaken for each of the operating model processes.	DORA processes, if in operation, are inconsistently coordinated across the enterprise. DORA action plans have been developed and work is in progress to close identified gaps.	DORA processes have been defined and established across the organisation in alignment with regulatory expectations.	DORA operating model processes are continuously enhanced (e.g. improved data availability, new metrics in place for assessing resilience, more severe scenarios being exercised).	DORA processes within the organisation represe leading practice and are regularly tested, measured and enhanced as needed. Process effectiveness and performance against targets are monitored and improved upon.
Foundational CMDB	Ad-hoc delivery and maintenance of CMDB resulting in little to no asset and configuration information known	Single system of record identified with initial discovery capabilities. Formalized process to keep CMDB aligned as part of Change Management	CMDB is recognized and established as primary system of record and discovery is applied for most core CI types. Similar and reasonably complete sets of information are held for all types of assets.	Automation & integrations execute most of day-to-day data maintenance and discovery identifies key relationships. CI data is accurate and complete, with clear relationship criteria defined.	A federated CMDB architecture is in place, which is well-integrated up- and downstream across the enterprise. Advanced discovery identifying service maps
ICT Risk Management	No risk systems and tools; high reliance on spreadsheets; lack of transparency (structure and availability) and standardization of data	Limited source data / CMDB identified, limited use of automation for aggregation of data and reporting	Standardized IT risk functions, architecture and platform with basic automation. source data (e.g., CMDB, ITSM tools and Vulnerability Management data) identified supporting risk metrics and baseline reporting	Integrated risk systems leveraging advanced technologies for reconciliation, automation, workflow, aggregation of data for near real-time assessment and reporting. Source data / CMDB standardized and aggregated across systems	Seamlessly integration of independently sourced IT Risk data (including external sources) enables process automation, customized reporting and near real-time dashboards, dynamic risk assessment and advanced data analytics
Management & Reporting of Incidents	Manual routing of incidents with limited data capture. Ad-hoc resolution with no mechanism to monitor and review incidents.	Major incidents managed ad-hoc. Execution is uncoordinated but escalation paths are established.	Well designed and understood classification/prioritization criteria leveraging integration with CMDB and foundation data. Centralized major incident team. Real-time incident dashboard.	Foundation/CMDB facilitate incident routing including basic orchestrations for common issues. Well established Major incident process.	Process execution encourages “shift-left”. Orchestrations / RPA for incident resolution.
ICT Third-Party Risk	Multiple siloed third party systems and tools resulting in manual interfaces and high reliance on spreadsheets. Lack of TPRM framework.	No firm-wide TPRM taxonomies, risk domains, and definitions to structure data. Inconsistencies limited use of automation and coordination across LODs	Third party risk data for assessment and reporting is harmonized and enables diagnostic insight together with mature KPIs in place and basic KRIs	Data standardized across systems (incl. ERP) for third party assessment and reporting enables real-time risk data (e.g. KPIs and KRIs) to support effective business decision-making	Forward looking analytics combined with automation to predict and proactively handle risk. Ability to perform scenario analysis for resilience.
Digital Operational Resilience	No formal Operational Resilience policy, operational resilience activities performed manually and time intensive.	Some awareness and processes exist; some activities, reports and metrics are leveraging ServiceNow.	Operational Resilience governance in place in line with regulatory expectations. Training is defined but policy is still limited in scope.	Majority of operational resilience activities are performed on ServiceNow. Fully developed operational resilience policies and training are in place and operating effectively.	Resilience processes are regularly tested, measured and enhanced in ServiceNow as needed. Real-time insights and detailed metrics, also with other enterprise tools

The ServiceNow platform delivers comprehensive technology that complements these TOMs, leveraging industry-leading ServiceNow workflows and advanced integration capabilities to drive unified, end-to-end workflows and bring together data from underlying IT systems. Its operational capabilities — including Integrated Risk Management, Third-Party Risk Management, Business Continuity Management, Security Operations, IT Operations Management, IT Service Management, and Operational Resilience — work seamlessly together, sharing data on a single platform to deliver complete coverage across all required DORA business services.

ServiceNow automates all key DORA processes



Let's recap

Today, financial service providers face an increasingly hostile cyber landscape punctuated by a broad range of cyber threats. The EU has introduced DORA, a stringent regulatory framework, in order to ensure these institutions remain resilient in the face of these risks. This represents a huge challenge for the European finance industry, given both the broad scope and prescriptive nature of DORA.

In particular, DORA goes far beyond existing approaches to operational resilience, requiring financial services providers to take a holistic approach, break down existing data and process silos, and move from a more reactive stance to one that is both proactive and transparent.

Together, KPMG and ServiceNow help clients address these challenges. KPMG professionals have deep expertise in risk management and provide proven structured methodologies for addressing operational resilience, while ServiceNow offers a unified platform that breaks down data and process barriers, and delivers a comprehensive set of capabilities covering all key DORA requirements. Combined with a deep and ongoing alliance between KPMG and ServiceNow, this offers financial institutions the opportunity to turn the challenge of DORA compliance into an opportunity to strengthen their resilience — increasing both customer trust and shareholder value.

Contact us

Andrew VanWagoner
EMA ServiceNow Platform Lead
KPMG in the UK
E: andrew.vanwagoner@kpmg.co.uk

Sébastien Fix
Director, KPMG Advisory | Head of ServiceNow IRM & ESG
KPMG in Norway
E: sebastien.fix@kpmg.no

kpmg.com/servicenow

The information contained herein is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although we endeavor to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act on such information without appropriate professional advice after a thorough examination of the particular situation.

Throughout this communication, "we", "us" and "our" refers to KPMG and ServiceNow.

"KPMG" refers to the global organization or to one or more of the member firms of KPMG International Limited ("KPMG International"), each of which is a separate legal entity. KPMG International Limited is a private English company limited by guarantee and does not provide services to clients. For more detail about our structure please visit kpmg.com/governance.

Designed by Evalueserve.
Publication name: Rise to the challenge of DORA compliance | Publication number: 139586-G | Publication date: September 2024