How to deal with DORA

Here is a corporate anecdote. During a virtual board meeting, the CEO needed to share a critical presentation. Everyone was on Zoom, waiting. He fumbled with the laptop, tapping and swiping like he was trying to swat a fly. "Can anyone see my screen?" he asked. Silence. Then a tiny voice from off-camera said: "Dad, you're on the calculator app." While everyone laughed, the CEO sighed. "I hate it when I can't figure out how to operate the controls and my tech support guy is asleep," he said. "He's 10 and it's past his bedtime."

If that anecdote made you blink, these statistics should make you think: the data management software market in Asia-Pacific excluding Japan and China is set to cross US$13.7 billion by 2028 — up from about US$7.5 billion in 2024 — growing at a compound annual growth rate (CAGR) of 15.7% during the period, according to International Data Corp (IDC).

"This growth is driven by the integration of AI (artificial intelligence) and Gen AI (generative AI) into enterprise workflows, which demands scalable, real-time data pipelines for analytics and automation," says IDC.

"Organisations are also prioritising cloud-native platforms and metadata-driven integration tools to modernise infrastructure and unify data across silos. Regulatory pressures and the need for secure, intelligent data governance further reinforce this momentum."

Companies are increasingly adopting hybrid data strategies, combining on-premises infrastructure with rapid migration to public cloud services. Public cloud deployments are set to grow at a CAGR of 31.1%, significantly outpacing on-premises growth, which remains flat, particularly in data lakes, NoSQL databases and serverless integration tools. "Sectors such as banking, government and manufacturing continue to invest in on-premises systems due to compliance, latency and operational control requirements," IDC notes.

DISSECTING DORA

So far so good. But now comes the Digital Operational Resilience Act (DORA), a European Union regulation to help boost the digital operational readiness of financial entities. It wants these entities to withstand, respond to and recover from tech disruptions such as cyberattacks or system failures. While DORA came into effect on Jan 17, 2025, its impact and relevance is just being felt across Asia-Pacific, including Asean.

DORA covers a range of financial entities — banks, insurance companies, investment firms, brokerages and others. It also impacts third-party information and communications technology (ICT) service providers that support financial entities. Three European supervisory authorities regulate DORA: the European Banking Authority (EBA), European Securities and Markets Authority (ESMA) and European Insurance and Occupational Pensions Authority (EIOPA). An important milestone was crossed in April 2025 when financial entities were required to identify their critical ICT service providers and submit contractual information to regulators.

This is where the shoe bites, despite DORA being limited to the EU. That is because of the tight integration of supply chains and ICT enablement across key countries in Asia-Pacific, including Asean. Supporting organisations in the region now need to prepare for digital operational resilience testing and incident reporting as well as ensuring contracts with third-party tech providers meet stringent DORA regulations.

Financial institutions in this region are investing in automated governance, risk compliance platforms, AI-driven threat detection and monitoring tools to meet DORA requirements.

FREEPIK

"Regulatory bodies across Singapore, Australia, India and Hong Kong are also advancing mandates that reflect DORA's principles. These include the Monetary Authority of Singapore's Technology Risk Management guidelines, Australia's CPS 230 and strengthened incident disclosure requirements in India and Hong Kong," says IDC.

The complication: Gen AI is increasingly being used in companies with or without management approval. Research and advisory firm Gartner says AI applications introduce new attack surfaces in the application development lifecycle. That needs dedicated and innovative security measures.

"There are many stakeholders involved in AI projects, each with different priorities. Unfortunately, it is not as simple as splitting responsibilities because there are some overlaps too," says Jeremy D'Hoinne, a vice-president at Gartner.

"Most companies have an AI committee in charge of the decisions. Chief information security officers (CISOs) must also be part of this committee."

D'Hoinne says there are four ways to prevent data risks: monitor usage and detect anomalies; access rules and security controls; transform by masking, encrypting and synthetising; and avoid using data where possible to only expose data that is necessary. "CISOs must also maintain AI literacy on AI evolution to continually adapt security practices," he advises.

How are financial institutions in the EU dealing with DORA? At some institutions, uncertainty over scoping has led to increased budget allocations.

"Typically, an institution might have earmarked €5 million to €15 million for its DORA programme strategy, planning, design and orchestration. But early estimates for full implementation costs are coming in at 5 to 10 times that range. One large financial institution reported that its final planned DORA implementation spend amounted to nearly €100 million, split between programme orchestration and tech control upgrades," says a McKinsey report.

BEST PRACTICES

No doubt companies in Asean and Asia-Pacific will also need to prepare for DORA and its implications. Here are six best practices from McKinsey — in alphabetical order — to get your organisation DORA-ready as soon as possible.

- Appoint a single accountable programme owner. While DORA affects multiple functions, a single accountable owner should provide a single point of coordination. This approach will sharpen strategic oversight and lead to better prioritisation and communication throughout the implementation.
- Build resilience. Take a risk-based approach to resilience, identifying the most critical processes and prioritising capability requirements according to risk. This means not creating "one control requirement set to rule them all" but defining risk-differentiated policies and controls based on the business value of different processes. Such an approach should yield a more streamlined, efficient application of DORA requirements, optimising both DORA spend and time to compliance.
- Collaborate even with competitors. Business leaders may feel it is counter-intuitive to collaborate with competitors on regulatory alignment, but information sharing can actually streamline the implementation process and build trusted networks. The power and impact of cross-industry collaboration on security and regulatory topics is beneficial across the board whether with competitors or business partners.
- Drive transformation from the top. Senior managers need to formulate a clear strategy, enhanced by programmatic support structured around the business and its priorities. Regulators' expectations will be relevant in this context. In one recent example, the regulator requested evidence that IT risk management efforts were business-led and involved leaders from the business. Linking regulatory remediation deliverables to business objectives is key to measuring resilience success, which is possible only when business colleagues are at the helm in driving implementation.
- Explicitly define what "done" means when DORA requirements are met and risk is mitigated. Often in the course of regulatory and remediation programmes, organisations run into the risk of increasing the list of requirements and lengthening timelines. This may occur when internal stakeholders attempt to add their own priorities to the list, thereby increasing the time and effort required. By agreeing from the outset on how to define "done" a company can save months of programme extension, spend and iteration.
- Foster digital trust by using DORA principles. ICT service providers and financial institutions can use DORA to boost transparency and build trust in their digital products and services. As quality, resilience and security improve, so will uptime, access and fraud-mitigation outcomes. Thus, digital trust can become a value differentiator for customers.

The bottom line: Security and compliance automation platforms are evolving from basic checklist-based tools into advanced, real-time trust management systems. They now support continuous control monitoring, automated evidence collection and scalable audit readiness. They also leverage application programming interface-driven architectures to provide real-time visibility into security and regulatory compliance across complex, multi-cloud environments.

As regulatory requirements become more demanding, vendors need to integrate capabilities such as unified risk assessment, policy enforcement and third-party trust workflows. This shift will enable security teams to accelerate audit cycles, reduce manual overhead and be proactive on compliance and risk management issues.

Since we started with a corporate anecdote, let's end with another. During a virtual conference with investors, the CEO was explaining quarterly growth when a loud crash echoed through his mic. "Sorry," he said, forcing a smile. "My kids are ... redecorating." Seconds later, a dart hit him on the forehead. He flinched, knocked over his water, reached for the aspirin bottle on his desk and popped two pills. "When you get a headache, take two aspirin and keep away from children," he sighed. "I do just what the label on the bottle advises." E

Raju Chellam is editor-in-chief of AI Ethics & Governance Body of Knowledge and chair of cloud and data standards at ITSC in Singapore