Digital Operational Resilience Act (D.O.R.A.)

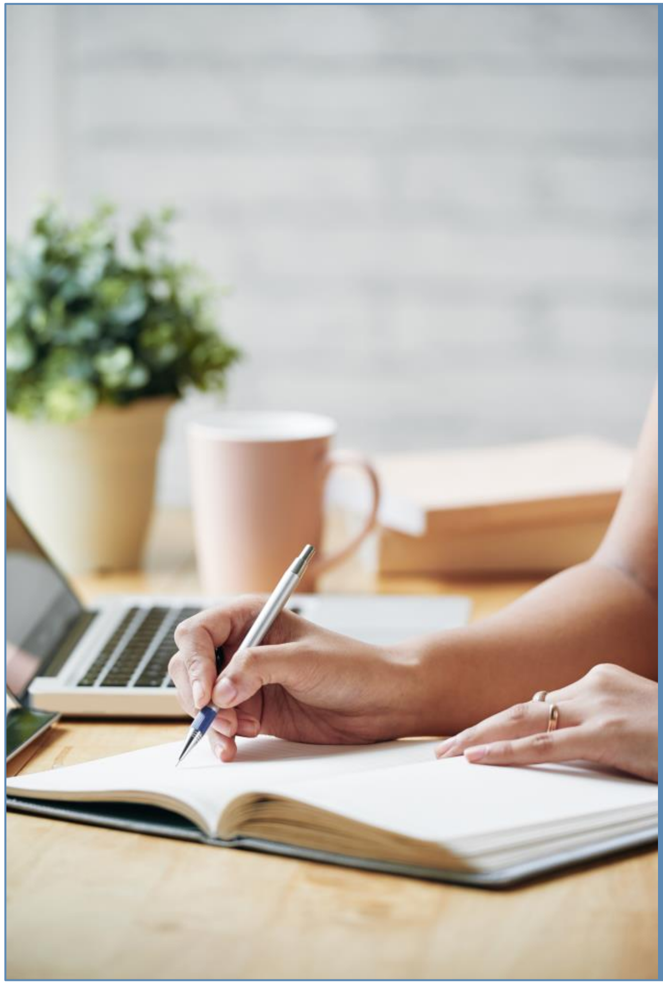
May - 2024

ALVAREZ & MARSAL

Alvarez & Marsal

LEADERSHIP. ACTION. RESULTS.℠

Agenda



What is DORA?

How does it impact you?

How can A&M help.

Introduction to A&M.

What is DORA?

What is D.O.R.A. (Digital Operational Resilience Act)?

- Financial entities must follow rules for the protection, detection, containment, recovery and repair capabilities against ICT[1]-related incidents.
- DORA explicitly refers to ICT risk and sets rules on ICT **risk-management**, **incident reporting, operational resilience[2] testing** and ICT **third-party risk monitoring.**
- DORA came into force on January16th, 2023, but **organizations have until January 2025 to become compliant.**

1. ICT has three components: **information technology** equipment (computers and related hardware); **communications** equipment; and software.
   - ICT infrastructure is used in: Contact/Call Centers, Automated Clearing House Systems (ACHS), Electronic Fund Transfers (EFT), Online Corporate Investment Banking, Corporate Intranet Systems.
   - ICT systems are used for handling telecommunications, broadcast media, intelligent building management systems, network-based control and monitoring functions, and other forms of communication.
2. Operational resiliency: to avert, act, recuperate, and learn from operational disruptions.

- For **U.S. banks**, compliance with DORA is **crucial** when they offer financial services within the EU or engage with EU financial entities as third-party service providers.

As D.O.R.A. comes into force in January 2025, US Banks with an EU Footprint are under high pressure

Key facts about the Digital Operational Resilience Act (DORA)

WHAT YOU NEED TO KNOW

- DORA aims to introduce a **comprehensive framework on digital operational resilience** for European financial institutions
- The objective of DORA is to ensure that the financial sector in Europe is able to **effectively manage ICT and cybersecurity risks**, including those arising from third parties
- DORA is a **key milestone for the future of cloud technology** in financial services
- **Penalties** for non-compliance: **1% of global average daily revenue** for up to 6 months and potential cease-and-desist orders
- Majority of risk management professionals are only **at their beginning of their planning journey**

DORA's five pillars – broken down

ICT Governance & Risk Management

- Board Awareness, Governance Set-up, and Awareness & Training
- Digital Operational Resilience Strategy Definition
- ICT Risk Management Framework Set-Up & Implementation
- Value Chain Management Set-Up Implementation
- Crisis and Backup

Incident Management & Reporting

- Security Incident Management Framework Review
- IT Incident Management Framework Review

Operational Resilience Testing

- DORA Testing Methodology Definition and Execution
- Threat-Led Penetration Testing Management Set-Up and Implementation

ICT Information Sharing

- Cyber Threat Intelligence and Information Sharing

ICT Third-Party Risk Management

- Complete monitoring visibility of outsourced functions.
- Full-service level agreement (SLA) description.
- Indications of where data is processed/stored.

How does it impact you?

Which entities are impacted by DORA

- It covers banks, payment institutions, investment firms, crypto assets service providers and more.
- Additionally, critical **third-party ICT providers** also fall under the regulation.
    - Impacted organizations are summarized below:

Financial Entities

- Credit institutions
- Payment institutions
- Account Information service providers
- Electronic money institutions
- Insurance/Reinsurance companies
- Central Securities depositories
- Central counterparties
- Investment firms
- Trading venues
- Trade Repositories

3rd Party Services

- This includes digital services and data services provided through ICT systems to one or more internal or external users (i.e., financial entities) on an ongoing basis, including hardware as a service and hardware services.
- This means that unregulated 3rd-party service providers, e.g., cloud services, software, data analysis services or data centers, also fall within the scope of DORA.

Examples of ICT systems requiring DORA compliance

Enterprise Resource Planning (ERP) Systems

ERP systems integrate core business processes, including inventory and order management, accounting, human resources, and more. They facilitate the flow of information within an organization, ensuring that decision-making is based on accurate and real-time data. Examples include SAP, Oracle ERP Cloud, and Microsoft Dynamics 365.

Customer Relationship Management (CRM) Systems

CRM systems help businesses manage and analyze customer interactions and data throughout the customer lifecycle, with the goal of improving business relationships with customers, assisting in customer retention, and driving sales growth. These systems compile data from a range of different communication channels, including a company's website, telephone, email, live chat, marketing materials, and more

Cloud Computing Platforms

These are platforms that deliver various computing services over the internet, including storage, databases, networking, software, and analytics. These platforms enable businesses and individuals to access and use computing resources without the need for direct hardware

Online Banking Systems

Internet banking platforms allow customers to conduct financial transactions remotely using a website or a mobile application. These systems enable users to check account balances, transfer money, pay bills, and manage investments, providing convenience and accessibility

Some use cases that trigger US - DORA Compliance

Cross-border Transactions

- A U.S. bank or financial service provider sending wire transfers to any financial institution within the EU or uses other financial market infrastructures, i.e., trading platforms and/or central securities depositories; means the ICT systems enabling these transactions need to withstand, respond to, and recover from ICT-related disruptions and fall under DORA compliance.
- A U.S. financial institution that routes trade orders to its EU subsidiary or parent company, fall under the scope of DORA. These transactions involve cross-border digital communication and require the operational resilience of the systems managing these trades, the EU counterpart is subject to DORA, and by extension, the U.S. institution must align with DORA's requirements to maintain the operational integrity of its EU partner.

Client Onboarding

- Setting up/onboarding an EU client with U.S.-based settlement instructions involves processing personal and financial data across borders. This scenario requires robust ICT systems to manage data securely and efficiently. Under DORA, the operational resilience of these systems is crucial, as any disruption can affect the financial stability of the EU client and, by extension, the EU financial market.
- A U.S. financial institution using cloud services to store or process data for EU clients, the operational resilience of these cloud services must comply with DORA. This includes ensuring the security and availability of data hosted on cloud platforms.

Outsourcing

- 30% of the total outsourcing budget of significant EU banks is concentrated on ten providers, most of which are headquartered outside the EU (**mainly in the United States**).
- Approximately 22% of all outsourced critical services in the EU are offered from non-EU countries, predominantly from the United Kingdom **and the United States.**

How can A&M help?

Benefits in using A&M for your DORA implementation

A&M's key differentiator is the combination of Regulatory and Technical expertise with a Business perspective that shapes the C-level agenda…

Deep regulatory knowledge

Our team brings senior regulators, with experience in overseeing governance and risk management arrangements for insurers on top of regulatory experts

Business Focus

As per A&M's DNA, financial impacts and focus on business continuity and containing operational disruptions are core in our approach

Strong cyber-security expertise

Our Cyber team has an extensive track record on cybersecurity (including I.T. infrastructure assessments, risk assessments, penetration testing and reviews)

Our differentiated approach shapes the way we would support DORA

- Assess the right and specific ambition for DORA requirements
- Oversee the right gap-analysis between the current situation and the targeted ambition
- Define a high-level, ambitious and realistic implementation plan, timeline and related key milestones
  - Ensure DORA's appropriation within Business-As-Usual of impacted functions across the three lines of defense.
- Assess realistic project and run costs and maximizing the captured value
- Setup project governance and execution structure that would secure the on-time, on quality and at right cost delivery
- Lead and follow the implementation phase as a C-level active tower control, collaborating with internal teams and any required external providers
- Deep-dive assistance on h specific topics as need-be and relevant (ex : management training , interactions with regulators (challenge and rehearsals), cyber security tests

There are pitfalls in DORA implementations – A&M detects them early and benefits from the experience of other regulatory programs

Common pitfalls to avoid	A&M view on key success factors
Lack of focus	Right focus through hierarchization of risks
Overkill due to 100% of regulatory requirements	Right level of compliance – serving the purpose
Lack of clarity and honesty	Right narrative with regulators
Creating a bureaucratic setup	Right implementation and run cost
Follow-up post go-live project and sub-project costs	Right appropriation and embedding

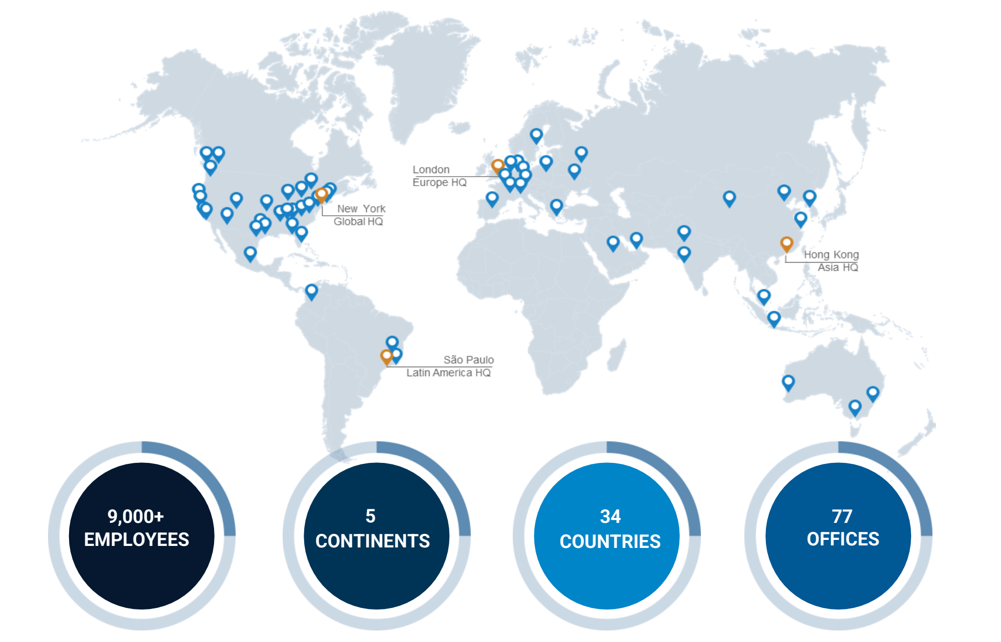
We consider avoiding duplicated efforts within the organization while considering other similar European regulations is a key success factor to consistently deliver DORA on-time, on quality and at a controlled cost

Bottom line, A&M can help with:

1. Assess where you are as it relates to DORA compliance, across the 5 pillars.
2. Develop a roadmap towards compliance.
3. Establish, staff and manage the program to execute the roadmap.
4. Devise the mechanism(s) for ongoing reporting and incident management to regulators.

Who is A&M?

A&M has global presence, broad client base, and integrated capabilities

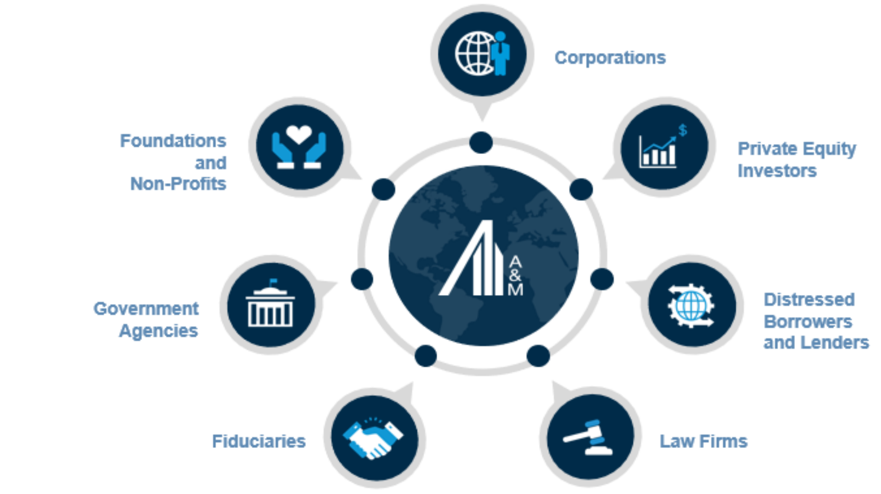


9,000+ EMPLOYEES

5 CONTINENTS

34 COUNTRIES

77 OFFICES



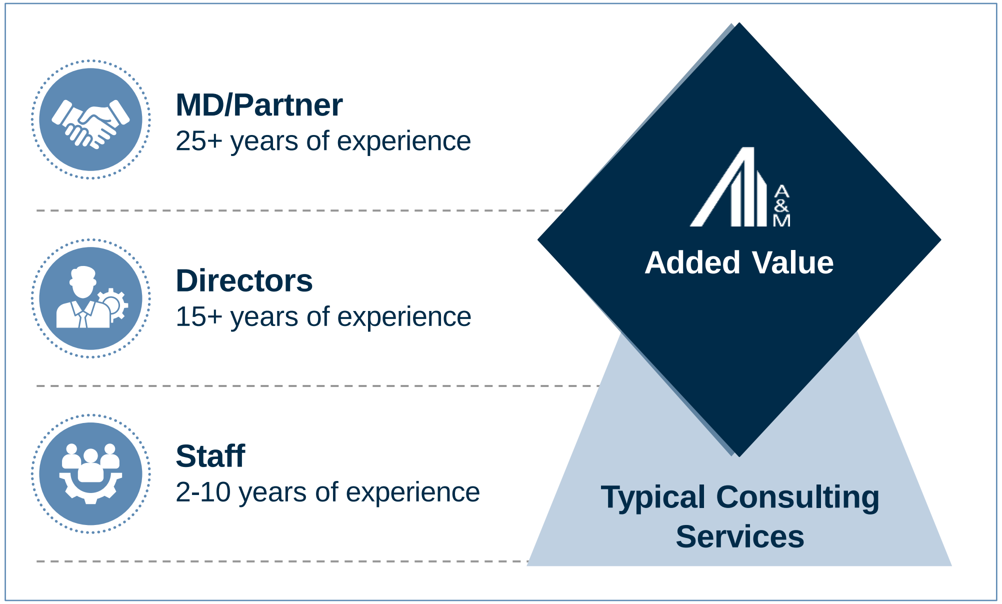
43%	58	44	167	26 of 30
Of the Fortune Global 500	Of the Fortune 100	Of the FTSE 100	Of the S&P 500	Of Global SIFI Banks

A&MPLIFY BY ALVAREZ & MARSAL	Corporate Performance Improvement	Tax	Disputes & Investigations	Valuation	Restructuring & Turnaround	Regulatory & Risk Advisory	Private Equity Services
• Digital Growth & Strategy • Digital Talent & Culture • Artificial Intelligence & Analytics • Customer Experience • Data Platforms	• Corporate Transformation • CFO Services • Digital & Technology Services • Talent, Org.& People • Supply Chain Services	• Federal • State & Local • Transfer Pricing • Research Credits & Incentives • Merger Integration	• Disputes • Investigations & Compliance • Forensic Technology • Fiduciary Services • Global Cyber Risk & Incident Response Investigations	• Complex Financial Instruments • Financial & Tax Reporting Valuation • Structured Finance & Capital Equipment	• Corporate Finance • Claims Management Services • Creditor Advisory • Debt Advisory • Insolvency	• Banking • Corporate Risk Management • Diversified Financials • Insurance Regulatory	• Buy-side Integrated Due Diligence • Divestiture Services • Portfolio Operations Improvement • ESG Services

A&M sets itself apart from other strategy consultancy firms by not only providing strategic advice but also actively engaging in implementation

Why is Alvarez & Marsal "different"?

A&M difference delivery model



Difference in the way we work

We combine …

- **… structured analytics with profound functional and industry experience**: senior professionals out of consulting and industry (former operators, practical delivery approach).
- **… candid advise and cultural sensitivity:** our promise is to be respectful but bold, candid and provocative to the benefit of our clients.
- **… financial impact-driven:** we link and prioritize all project activities to EBIT and cash. Our allegiance is to the facts and our only bias is to action.
- **… conceptual strength with focus on execution and results**: we develop pragmatic concepts fast and focus on rapid delivering with instant results.

WHO A&M is ….

LEADERSHIP

Experienced in industry and embedded in your organization

HOW A&M works ….

ACTION

Delivered quickly, decisively, and practically

WHAT A&M delivers ….

RESULTS

Linked to top and bottom-line performance

The A&M Difference

A&M adds substantial value to any complex situation

LEADERSHIP

- Focusing senior resources at every stage of the delivery process
- Forging consensus around credible, executable solutions
- Engaging and partnering with your organization

SENIOR RESOURCE DEPTH

- Executives drawn from both industry and professional services firms
- Majority of our professionals (Director grade and above) have extensive Board-level operational experience
- Global reach

MANAGING COMPLEXITY

- Proven track record in managing complex, high-profile situations
- Delivery through assured leadership and execution
- Development of strategic and corporate finance options in cooperation with management to support the business plan

SPEED, EXECUTION AND ACTION

- Focus on delivering rapid results with overarching focus on improving bottom-line results
- Coordinate short- and medium-term objectives and credible plans with achievable milestones

OPERATIONAL HERITAGE

- Proven, fact-based approach
- Over 30 years of operational experience
- Ability to provide seasoned interim executives for rapid implementation

PRACTICAL BOTTOM-LINE ORIENTATION

- Keen awareness of what can be implemented in a turnaround environment
- Strong focus on improving bottom-line results
- Able to achieve business transformation with restructuring speed

A
&
M