eBOOK

EXPLORING DORA

A Guide to the Digital Operational Resilience Act

Commvault®

Contents

An Overview of the

Digital Operational Resilience Act

The Digital Operational Resilience Act (DORA), required of financial entities in the European Union, went into effect January 17, 2025. Banks, insurance companies, and information and communications technology (ICT) third-party service providers are among the institutions that must comply with its provisions, which are designed to enable cyber resiliency.

It's crucial for all stakeholders to understand the key provisions and the impact they will have on the financial ecosystem.

A deeper dive into the main components of DORA and what they mean for the industry

01 Risk Management Requirements

DORA introduces stringent requirements for financial entities to establish and maintain robust digital operational resilience frameworks. This means that firms must have comprehensive policies in place to manage ICT risks. These policies should cover the entire lifecycle of ICT systems, from development and deployment to maintenance and decommissioning. Financial entities are expected to regularly review and update their risk management strategies to adapt to new and emerging threats.

02 Incident Reporting

One of the pivotal elements of DORA is the obligation for financial entities to report significant cyber incidents to their respective regulatory authorities within specific timelines. This provision is designed to enable a timely flow of information between financial institutions and financial supervisors, which is crucial for managing systemic risks and enhancing the overall resilience of the financial sector. The act, together with supporting technical standards, specifies the types of incidents that must be reported, the reporting timelines, and the detailed information that must be included in the reports.

03 Digital Operational Resilience Testing

To verify that financial entities can effectively withstand and recover from ICT disruptions, DORA mandates regular testing of digital resilience. This includes a range of testing activities, such as vulnerability assessments, penetration testing, and scenario-based exercises. These tests are designed not only to identify vulnerabilities in ICT systems and processes, but to assess the effectiveness of the entity's preventive, detection, response, and recovery capabilities; identify gaps in those capabilities; and close them to ultimately improve resilience.

04 Third-Party Risk Management

Recognizing the increasing reliance on third-party ICT service providers, DORA sets out specific requirements for managing risks associated with these external parties. Financial entities must carefully select and monitor their service providers to ensure they comply with high resilience standards. They must conduct thorough due diligence before entering into agreements and continuously monitor the service providers' performance and compliance with contractual obligations.

05 Oversight Framework

DORA establishes an oversight framework that allows European supervisory authorities to directly oversee critical ICT third-party service providers. This framework is intended to compel providers to adhere to stringent resilience standards, given their importance to the financial sector. The oversight includes regular assessments and, if necessary, the imposition of remedial actions to address identified deficiencies.

Penalties for Noncompliance

Noncompliance with DORA can result in significant penalties, which are crucial in maintaining the integrity and effectiveness of the act.

These can vary depending on the severity and nature of the offense. They are designed to be dissuasive and proportionate to the financial strength and size of the entity, as well as the extent of the disruption caused by noncompliance.

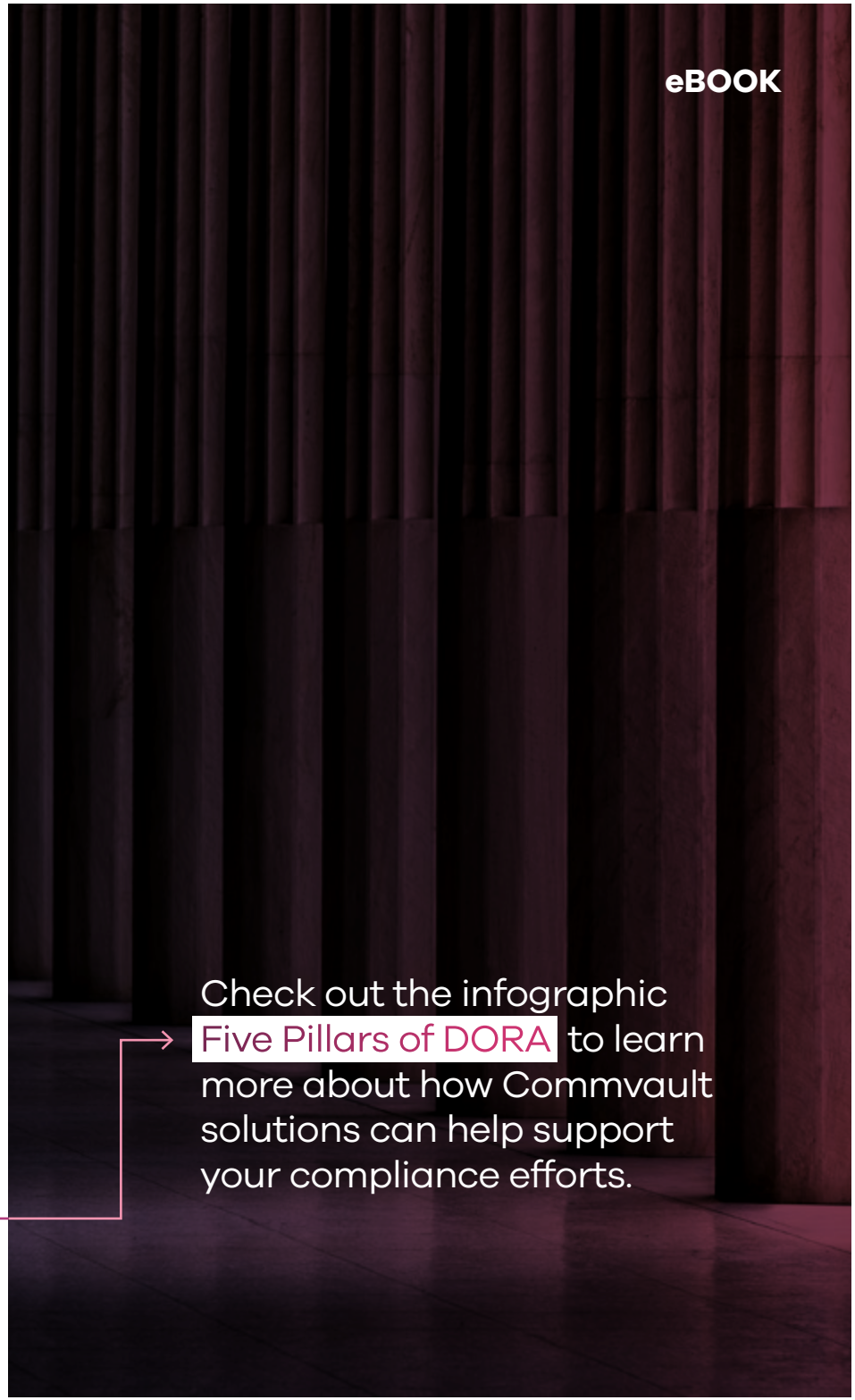
For minor infringements, financial entities might face warnings or reprimands. More serious breaches can result in hefty fines. In cases of repeated noncompliance or particularly egregious breaches, regulatory authorities have the power to impose additional sanctions. These can include the revocation of licenses, temporary bans on conducting certain business activities, or other restrictions necessary to protect the financial system.

eBOOK

Positive Impact
Positive Impact
Positive Impact
Positive Impact

Positive Impact on Financial Stability

The introduction of DORA marks a significant step forward in the quest for greater digital operational resilience in the financial sector. By setting out clear requirements, the EU aims to safeguard the sector from ICT-related disruptions and threats. This comprehensive approach not only enhances the security of individual institutions but also bolsters the stability of the financial system as a whole.



Check out the infographic Five Pillars of DORA to learn more about how Commvault solutions can help support your compliance efforts.

Commvault®

eBOOK

Nine Steps on the path to Compliance

Nine steps you should take to comply with DORA and bolster your organization's digital operational resilience

01

Understand the scope and requirements of DORA

DORA applies to a wide range of entities, including banks, insurance companies, and investment firms, as well as critical third-party service providers, such as cloud computing services. Understand the obligations it entails, such as incident reporting, digital operational resilience testing, and management of ICT third-party risks.

02

Conduct a comprehensive risk assessment

You must identify, document, and manage all risks related to your ICT systems and services. A thorough assessment involves mapping out all digital assets, evaluating the risks associated with each asset, and understanding the potential impact of ICT disruptions on your services and operations. Regularly update to reflect new technologies, processes, and emerging threats.

03

Strengthen ICT security measures

You need to deploy advanced cybersecurity technologies in areas such as risk identification, protection and prevention, detection, response and recovery, and finally, backup.

DORA is adamant about the importance of testing. You must conduct regular security audits and penetration testing to identify and address vulnerabilities but also test and document your organization's operational resilience. Confirm your security policies and procedures are up to date and in line with industry best practices.

Steps continued on next page →

04 Develop and test an incident response plan

Establish and maintain procedures to be followed in the event of an ICT-related incident, so that you have a quick and organized response that minimizes impact. Your plan should include clear roles and responsibilities, communication strategies, and recovery procedures. Conduct regular training and simulation exercises so the response team is well-prepared to handle potential incidents.

05 Enable resilience of critical functions

Your critical functions must be able to withstand and recover from ICT disruptions. Design systems and processes that are resilient and can continue to operate under adverse conditions. Build redundancies into critical systems, and implement backup solutions to maintain data integrity and availability. Clearly define recovery objectives and regularly test your recovery plans.

06 Manage third-party risks

Conduct thorough due diligence when selecting providers, and continuously monitor their performance and compliance with internal ICT risk management framework and relevant security standards. Contracts should include clear terms regarding data protection, incident reporting, and audit rights. Have a contingency plan in case the third party fails to deliver the required service.

Steps continued on next page →

07

Implement governance and oversight

Define the roles and responsibilities of all parties involved in managing ICT risks. Senior management should be actively involved in overseeing the organization's digital operational resilience. Provide regular reports to senior management, detailing risk management efforts, incident reports, and compliance.

08

Prepare for reporting and auditing

DORA mandates regular reporting on ICT risk management, incidents, and audit findings. Have mechanisms in place to collect the necessary data and generate reports in a timely manner. Be prepared for external audits by regulators or independent auditors, keeping all documentation and evidence of compliance readily available.

09

Foster a culture of resilience

It is crucial to raise awareness about the importance of digital operational resilience and train employees on their roles in maintaining it. Encourage proactive identification and management of risks and promote continuous improvement of resilience strategies.

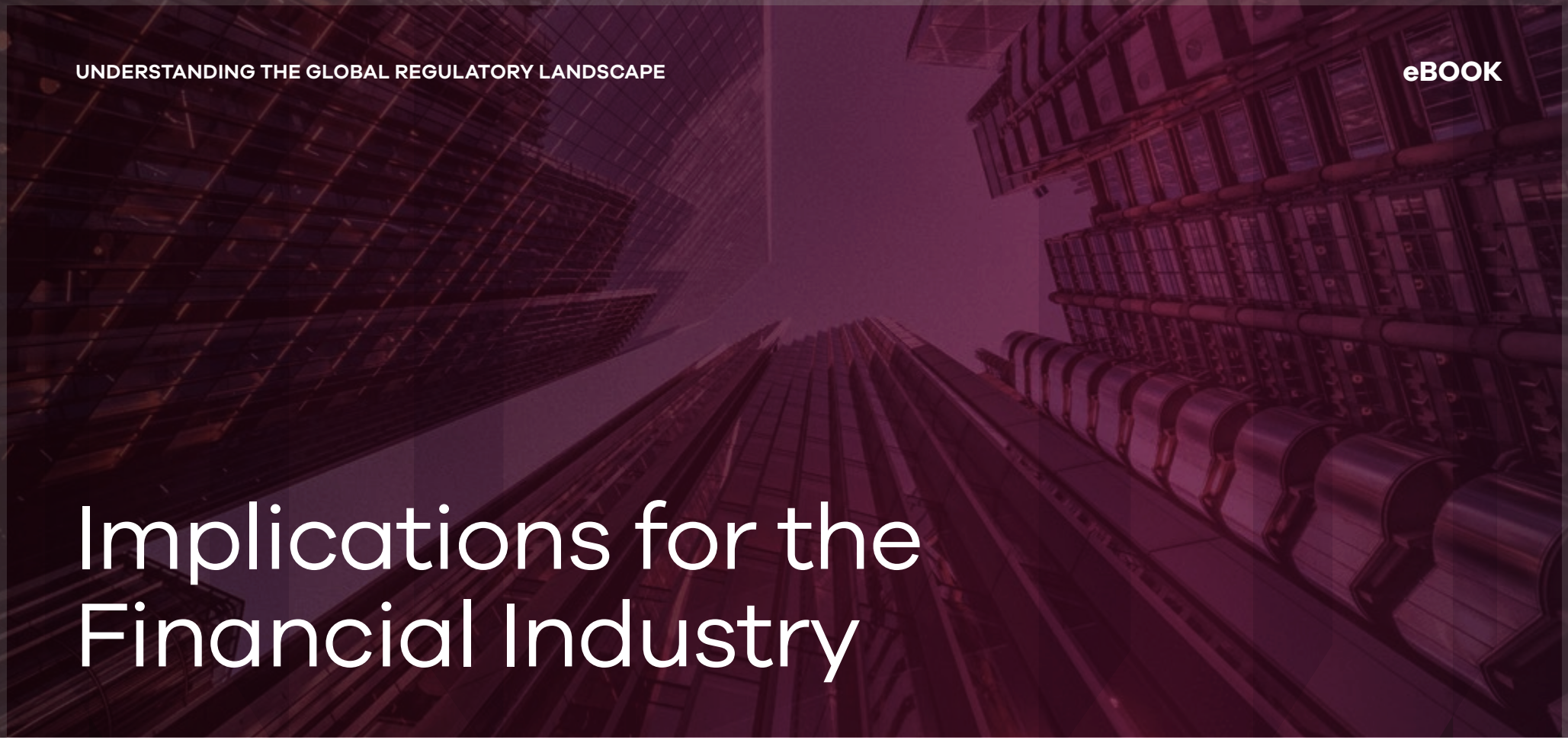
By following these steps, you will not only be prepared to comply with DORA but also will enhance your organization's overall digital operational resilience, protecting you and your customers from the adverse effects of ICT disruptions.

As digital transformation continues to evolve, staying ahead in terms of compliance and resilience will provide a competitive edge and better position your company for long-term sustainability.

Understanding the Global Regulatory Landscape

The importance of robust regulatory frameworks to increase the stability and security of financial systems cannot be overstated. Let's explore how DORA – which the European Commission introduced as part of the Digital Finance Package in September 2020 – compares to other major regulations globally.

Regulation	What is it?	Scope	Incident Reporting Requirements
Digital Operational Resilience Act (EU)	A set of stringent requirements to establish and maintain robust digital operational resilience frameworks and ICT risk management policies	Required for financial entities, including banks, insurance companies, and ICT third-party service providers of financial entities, operating in the EU	Mandatory
National Institute of Standards and Technology Cybersecurity Framework (U.S.)	Guidelines for managing and reducing cybersecurity risks	Voluntary, for any industry. While not a regulatory requirement, it is widely adopted by U.S. financial institutions. U.S. government agencies and contractors handling federal data are often required to follow NIST guidelines.	Encouraged but not required
General Data Protection Regulation (EU)	Another significant EU regulation, primarily focused on data protection and privacy	Applies to all organizations processing personal data of EU citizens	Mandatory
Basel III from the Basel Committee on Banking Supervision (Global) Note: The latest provisions were implemented in the EU on January 1, 2025. (U.S. to follow by July 1, 2025; U.K. by January 1, 2027.)	A global set of international regulatory standards to strengthen regulation, supervision, and risk management. Focused on capital adequacy, stress testing, and market liquidity risk, as well as operational resilience.	Specific to internationally active banks	Mandatory
Financial Conduct Authority Operational Resilience Framework (U.K.)	A separate operational resilience framework, which shares similarities with DORA	Financial entities in the U.K.	Mandatory



Implications for the Financial Industry

For financial entities operating across multiple jurisdictions, compliance with diverse regulatory frameworks can be challenging.

However, DORA builds upon existing industry best practices and aligns with elements of other regulatory frameworks, facilitating an integrated approach to ICT risk management and operational resilience. While financial entities have flexibility in structuring their ICT risk management models, they must follow DORA's core requirements, including stringent incident reporting and third-party risk oversight.

Hear more about emerging mandates from our partners at Harvard Business Review in this video:

Anticipating the Next Era of Modern Compliance

Building Cyber Resilience

Recovery Strategies for DORA Compliance

Financial institutions have long had a mandate to protect their data and infrastructure from threats, but DORA aims to increase overall resilience.

Here's how the provisions will affect an organization's resilience strategies:

01 **Incident Response Plan**

An incident response plan should outline the steps to be taken immediately after an incident, including containment, eradication, and recovery. Under DORA, they must be more detailed and regularly tested. This includes clear roles and responsibilities, communication protocols, and regular drills.

02 **Data Backup and Recovery**

DORA puts increased emphasis on data integrity and availability. Organizations must implement robust backup solutions, regularly test recovery procedures, and maintain redundant systems to minimize downtime.

03 **Third-Party Risk Management**

DORA mandates that financial entities verify ICT third-party providers comply with resilience standards, making vendor oversight more critical than ever. Effective risk management includes vendor due diligence (with a thorough assessment of security posture), clear contractual requirements, and ongoing monitoring to verify compliance.

04 **Regular Audits and Assessments**

DORA requires regular internal and external audits as well as risk assessments to identify potential threats.

05 **Employee Training and Awareness**

Employees are often the first line of defense against cyber threats. Education can help create a culture of vigilance and resilience – and reduce the risk of human error. Under DORA, organizations must facilitate regular training, awareness campaigns, and simulated attacks.

Implementing DORA-Compliant Cyber Recovery Strategies

While the advent of DORA may change some elements of your overall strategy, the basic framework of implementing a plan should be the same. Here are the steps you can take to keep your cyber recovery plan in compliance:

Assess current capabilities to identify gaps and areas for improvement.

Develop a comprehensive plan that addresses all aspects of DORA, including incident response, data backup, third-party risk management, and training.

Allocate resources, including budget, personnel, and technology, to implement your plan.

Test and refine your plan. Continuous improvement is key to maintaining operational resilience.

Document all aspects of your cyber recovery plan – including policies, procedures, and test results – to demonstrate compliance.

From Compliance to Cyber Resilience

DORA fundamentally reshapes how financial entities approach cybersecurity and operational resilience, emphasizing proactive risk management and stringent compliance requirements.

By enhancing incident response plans, implementing robust data backup and recovery solutions, managing third-party risks, conducting regular audits and assessments, and providing comprehensive training and awareness, organizations can build resilient cyber recovery strategies that not only comply with DORA but also enhance long-term operational stability.

Learn how Commvault solutions can help you comply with DORA and enhance your cyber resilience by reading our solution brief:

Using Commvault Cloud to Assist in DORA Compliance

The Role of Data Management

in Regulatory Compliance

Data management is at the heart of DORA's regulatory requirements. Financial institutions must have robust data management practices to maintain the accuracy, integrity, and availability of data. This is crucial for several reasons:

Risk Mitigation

Effective data management helps identify and mitigate potential risks. By maintaining accurate and up-to-date data, institutions can quickly detect anomalies and take corrective actions to prevent operational disruptions.

Compliance Reporting

DORA mandates detailed incident reporting and regular assessments of ICT risk management. Accurate data is essential for generating these reports and confirming that they meet regulatory standards.

Operational Efficiency

Well-managed data can streamline operations, reduce redundancies, and improve decision-making processes. This not only enhances compliance but also could boost overall business performance.

Customer Trust

With data breaches and cyberattacks commonplace, maintaining the security and privacy of customer data is paramount. DORA's data management requirements are aimed at maintaining customer trust.

Key Data Management Requirements Under DORA

Data Governance
Establish a clear and comprehensive data governance framework. This includes defining roles and responsibilities, setting data policies, and making sure that your data management practices are integrated into your overall risk management strategy.

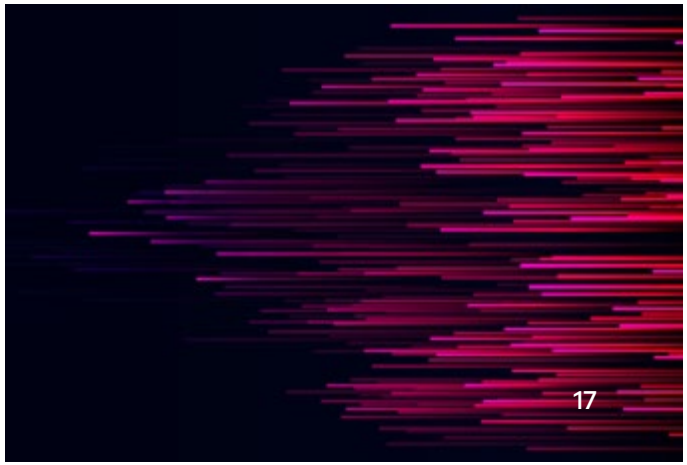
Data Availability
Data must be available and accessible when needed. This involves having reliable backup and recovery systems, as well as disaster recovery plans.

Data Quality
Verify that data is accurate, complete, and consistent. This involves implementing data validation processes, regular data audits, and using advanced analytics to monitor data quality.

Data Privacy
Comply with data privacy regulations, such as the GDPR. Make sure you have a valid legal basis for processing personal data, anonymize data where necessary, and provide transparency to customers about how their data is used.

Data Security
Implement robust security measures to protect data from unauthorized access, breaches, and cyber threats. This includes encryption, access controls, and regular security assessments.

Data Lifecycle Management
Manage the entire lifecycle of data, from creation to disposal. This includes data retention policies, data archiving, and secure data deletion practices.



Best Practices for Data Management

To better understand how to implement DORA's data management requirements, let's look at some best practices:

- Use data quality metrics to monitor the accuracy, completeness, and consistency of your data. These metrics can help you identify and address data issues proactively. Improved data quality leads to better decision-making and more reliable compliance reporting.
- Implement automated data validation processes to confirm data is accurate and complete before it is used. This reduces the risk of human error and keeps your data consistently validated.
- Use role-based access controls and multi-factor authentication to protect sensitive data from unauthorized access. Enhanced security measures reduce the risk of data breaches and confirm that only authorized personnel can access sensitive information.

Implementing Data Management Practices

Implementing effective data management practices to comply with DORA involves several steps:

1. **Conduct a thorough assessment** of your current data management practices to identify gaps and areas for improvement. Develop a comprehensive plan that aligns with DORA's requirements and your business objectives.
2. **Invest in advanced data management technologies,** such as data lakes, data warehouses, and data governance tools. These technologies can help automate data validation, security, and privacy processes, making compliance more manageable.
3. **Educate employees** on the importance of data management and the specific requirements of DORA. Foster a culture of data responsibility and awareness.
4. **Conduct regular audits and reviews** of your data management practices to maintain ongoing compliance. Use the results of these audits to make continuous improvements.
5. **Maintain third-party oversight** of any service providers you rely on for data management. They also must comply with DORA. This includes conducting due diligence, signing service-level agreements, and monitoring their performance regularly.

Data Management Challenges and Solutions

While implementing DORA's data management requirements can be daunting, there are ways to overcome these obstacles:

Challenge	Solution
Data silos: When data is stored in isolated systems and departments, it's difficult to verify data consistency and availability.	Implement a **centralized data management system** that integrates data from various sources to help break down silos and keep data consistent and accessible.
Resource constraints: Smaller financial institutions may lack the resources to invest in advanced data management technologies and training.	Consider **outsourcing data management to third-party service providers** that specialize in compliance and have the necessary resources and expertise.
Complexity of regulations: DORA is a complex regulatory framework with many requirements. Understanding and implementing these requirements can be overwhelming.	Seek the help of **regulatory compliance experts** and use **compliance management software** to simplify the process.

Data Management Is Key to DORA Compliance

Effective data management is crucial for compliance with DORA and for maintaining the trust and confidence of customers and regulators. By implementing robust data governance, maintaining data quality and security, and staying ahead of regulatory trends, financial institutions can not only meet DORA's requirements but also gain a competitive edge in the digital age.

DORA's data management requirements are not just a regulatory burden but an opportunity to improve operational efficiency, mitigate risks, and build a more resilient and trustworthy financial institution. Embrace these requirements and use them as a catalyst for positive change in your organization.

Risk Management and DORA

Preparing for the Unexpected

Whether it's a sudden market shift, a cybersecurity breach, or a regulatory change, the unexpected can strike at any moment. Being prepared is key to navigating these challenges successfully. This is where risk management and DORA come into play.

What Is Risk Management?

Risk management is the process of identifying, assessing, and prioritizing risks followed by the application of resources to minimize, monitor, and control the probability or impact of unfortunate events. Effective risk management isn't just about avoiding disasters; it's about creating a robust framework that supports your strategic goals and enhances your decision-making.

Risk management helps protect your organization's assets, including financial resources, physical property, and reputation. By identifying potential threats, you can take proactive steps to mitigate them.

Investors, customers, and employees are more likely to trust and support an organization that demonstrates a strong commitment to risk management. Understanding risks helps you make better strategic decisions, allocate resources more effectively, and focus on areas that truly matter.

How DORA Aligns with Risk Management

DORA and risk management are closely aligned, as both focus on preparing for and mitigating potential disruptions. Here's how DORA's components fit into a broader risk management strategy:

1. DORA requires financial entities to establish a comprehensive **risk management framework** with policies, procedures, and controls to identify, assess, and manage risks.
2. Timely and accurate **incident reporting** is crucial for maintaining operational resilience. By reporting incidents, you can quickly address issues and learn from them, reducing the likelihood of similar events in the future.
3. **Regular testing and exercises** are essential for verifying that your systems and processes can handle disruptions. This might include simulated cyberattacks, system outages, or other scenarios.
4. DORA emphasizes the importance of managing **third-party dependencies** so that the risk they might pose to your operational resilience is acceptable. Just as with data management, this involves conducting due diligence, establishing service-level agreements, and monitoring performance.

Risk Management Practices to Help You Maintain DORA Compliance

1. Stay informed: Keep up to date with the latest regulatory changes and industry best practices. This will help you stay ahead of the curve and confirm your risk management framework remains effective.
2. Collaborate: Work closely with other departments and stakeholders to create and maintain a holistic approach to risk management. Collaboration can help you identify and address risks that might otherwise go unnoticed.
3. Continuous improvement: Risk management is an ongoing process. Regularly review and update your risk management approach so that it stays relevant to the current state of your organization.
4. Technology investment: Invest in the right technology to support your risk management efforts. This might include risk management software, cybersecurity tools, and data analytics platforms.
5. Cultural shift: Foster a culture of operational resilience. Encourage employees to report potential risks and participate in risk management activities.

Protect Your Organization with a Proactive Approach

Risk management and DORA are powerful tools for preparing for the unexpected. By establishing a robust risk management framework and maintaining DORA compliance, you can help protect your organization's assets, maintain stakeholder confidence, and achieve your strategic goals.

DORA: An Investment That Pays Dividends

As the regulatory landscape continues to evolve, it's essential to stay informed and adapt your strategies accordingly. By complying with the requirements of DORA, you better prepare your organization to withstand, respond to, and recover from cyber incidents, ultimately safeguarding your operations and reputation.

Remember, the key to success is a proactive and continuous approach to cyber recovery, data management, and risk management. With the right tools and strategies, you can turn potential threats into opportunities for growth and improvement.

eBOOK

Download the eBook **Mastering DORA: Strategies for Digital Operational Resilience** to learn how Commvault solutions can help you meet specific provisions within DORA.

commvault.com | 888.746.3849 | get-info@commvault.com

Commvault®