Omada

WHITE PAPER

Cybersecurity and Identity Governance in **Financial Institutions:**

Proactive Strategies for DORA and NYCRR 500 Compliance

Table of Contents

Introduction 1

Overview of DORA 2

Overview of NYCRR 500 3

- Timelines and Repercussions of Non-Compliance 5
- Comparison Matrix: DORA vs. NYCRR 500 6

Recommendations for Financial Entities 8

Technical Requirements at a Glance 9

- DORA Technical Requirements 9
- NYCRR 500 Technical Requirements 10

Importance of Adopting Comprehensive Identity Governance Measures 11

Suggestions for EU Entities on Preparing for DORA 11

Conclusion 12

Introduction

Cyberattacks in the financial sector have more than doubled since the pandemic, with losses reaching $2.5 billion since 2020, according to the IMF's Global Financial Stability Report 2024 [1]. In response both the European Union and the United States, regulators are taking proactive measures to strengthen cybersecurity and resilience. Initiatives like the **Digital Operational Resilience Act (DORA) in the EU and the New York State Department of Financial Services (NYDFS) Cybersecurity Regulations (NYCRR 500)** in the U.S., emphasize the importance of robust identity governance and cybersecurity programs.

These regulations require financial institutions to assess their cybersecurity risks, implement comprehensive mitigation programs, and protect customer information and IT systems. Senior management must champion these efforts, with annual compliance certifications required. The message is clear: institutions must act swiftly and decisively to safeguard operations and customer trust.

Cybersecurity and Identity Management in the Financial Sector

Cybersecurity has become a cornerstone of the modern financial sector, safeguarding critical infrastructure, securing sensitive data, and maintaining the integrity of financial systems worldwide. The rapid pace of digital transformation has introduced new challenges, including rising cyber threats like phishing attacks, ransomware, and data breaches. These incidents can jeopardize customer trust, damage reputation, and result in financial loss and regulatory consequences. Central to mitigating these risks is the effective management of digital identities and access rights within organizations. Effective Identity Governance and Administration (IGA) is key to mitigating these risks by controlling user access to critical systems and reducing the risk of insider threats. In response to these challenges, global regulators are intensifying their focus on cybersecurity and identity management, mandating stringent measures to ensure the resilience of financial institutions.

Regulations like DORA and NYCRR 500 are two significant regulations that address these concerns and emphasize the importance of robust identity governance and access controls. DORA establishes a unified framework for Information and Communication Technology (ICT) risk management, enhancing operational resilience and requiring strong identity governance across financial entities and third-party providers. NYCRR 500 enforces stringent cybersecurity and access management practices, focusing on safeguarding customer data and financial stability. Together, these regulations highlight the importance of comprehensive identity governance and cybersecurity measures to protect financial institutions and the broader financial system from evolving cyber threats and operational disruptions.

[1] https://www.imf.org/en/Publications/GFSR/Issues/2024/10/22/global-financial-stability-report-october-2024

Overview of DORA

Purpose

DORA serves as a landmark regulation within the European Union, designed to fortify ICT risk management capabilities and identity governance practices within the financial sector. Its inception is a direct response to the escalating frequency and sophistication of cyber threats that have the potential to destabilize financial markets and compromise sensitive data. DORA's primary aim is to establish a cohesive and comprehensive framework for managing these risks, ensuring that the EU's financial entities operate within a resilient digital environment. Beyond enhancing operational resilience, DORA seeks to harmonize the myriads of existing regulations across EU member states, addressing inconsistencies and gaps that have historically complicated compliance efforts for financial institutions. Central to this is the emphasis on effective identity governance, ensuring that access to critical systems and data is appropriately controlled and monitored.

Scope

DORA casts a wide net over the EU's financial landscape, applying to a broad spectrum of entities. This includes traditional financial institutions such as banks, insurance companies, and investment firms, as well as non-traditional entities that are increasingly integral to the financial ecosystem, like crypto-asset service providers and crowdfunding platforms. Additionally, DORA's scope spans to critical third-party ICT service providers, including cloud services and data centers, which play a pivotal role in the operational infrastructure of financial entities. By encompassing these providers, DORA acknowledges the interconnected nature of modern financial services and the external risks that third-party partnerships can introduce. Importantly, DORA emphasizes the need for robust identity governance practices across all these entities, ensuring consistent and effective management of user identities and access rights.

Current Status

Since its proposal by the European Commission in September 2020 and formal adoption in November 2022, DORA has been on a path towards full implementation. Financial entities and their critical third-party ICT service providers are mandated to comply with DORA's requirements by January 17, 2025. This timeline provides a transition period for institutions to align their ICT risk management and identity governance practices with DORA's standards. Currently, the European Supervisory Authorities (ESAs) — which include the European Banking Authority (EBA) —the European Securities and Markets Authority (ESMA), and the European Insurance and Occupational Pensions Authority (EIOPA)-, are diligently drafting the regulatory technical standards (RTS) and implementing technical standards (ITS) that will define DORA's provisions . These standards, expected to be finalized in 2024, will outline the specific technical and operational measures financial institutions must adopt to achieve full compliance, including those related to identity governance and administration. Additionally, the European Commission is developing an oversight framework for critical ICT providers, further reinforcing DORA's comprehensive approach to digital operational resilience and identity governance in the financial sector.

Overview of NYCRR 500

Purpose

NYCRR 500, is a regulatory framework, by the New York State Department of Financial Services, aimed at bolstering the cybersecurity and identity governance practices of financial entities operating within the state of New York. Its goal is to ensure robust defenses against cyber threats, protecting sensitive customer information and the overall stability of the financial system. New York is committed to setting cybersecurity and identity governance standards to address evolving digital threats.

Scope

NYCRR 500 applies to all financial entities operating under New York's Banking Law, the Insurance Law, or the Financial Services Law. This comprehensive regulation is applied universally regardless of whether these entities are regulated by other government bodies.
Amendments provide limited exemptions based on size and financial thresholds. Specifically, entities with fewer than 20 employees and contractors, less than $5 million in gross annual revenue over the last three fiscal years, or less than $15 million in year-end total assets may qualify for exemptions. This tailored approach balances the operational realities of smaller financial entities, while still maintaining a robust defense against cyber threats across the financial sector.

Current Status

Recent 2023 amendments to NYCRR 500 introduced stringent requirements aimed at bolstering the cybersecurity and identity governance framework of regulated financial entities, specifically targeting Class A companies, which are larger entities meeting specific criteria based on revenue, assets, or number of customers.
All covered entities must complete independent cybersecurity audits by external auditors annually to ensure impartial evaluations. They are also required to conduct yearly risk assessments, with Class A companies engaging external experts for these assessments every three years or when significant business or technology changes present new cybersecurity risks.

A notable enhancement in NYCRR 500 is the mandate for Class A companies to implement robust IGA practices, specified in section 500.3. This includes creating comprehensive policies and procedures to ensure access rights are assigned, reviewed, and revoked in a timely manner. Regular access reviews must be conducted, leveraging automated solutions where possible, to validate that users have the correct access privileges based on their roles and responsibilities. The regulation also emphasizes segregation of duties to prevent conflicts of interest and reduce the risk of fraudulent activities.

NYCRR 500 underscores the importance of robust IGA, independent audits, and risk assessments to tackle evolving cyber threats. These measures align with Zero Trust principles and digital resilience, enabling New York's financial entities to mitigate unauthorized access risks while leading in cybersecurity and identity governance, to protect critical systems and customer data.

Criteria for Class A Companies

Under the proposed amendments to 23 NYCRR 500, a Class A company is defined as a covered entity that meets one or more of the following criteria:

1. **Size Based on Employees or Revenue:**
    - **Employees:** The company has over 2,000 employees, averaged over the last two fiscal years, including employees of both the covered entity and all of its affiliates.
    - **Revenue:** The company has over $1 billion in gross annual revenues averaged over the last three fiscal years from all business operations of the covered entity and its affiliates.
2. **Status as a Larger Financial Institution:**
    - The company is a banking organization as defined in New York Banking Law, which includes entities like commercial banks, trust companies, and private bankers.
    - The company is a foreign banking organization licensed under New York Banking These amendments introduce the concept of "Class A companies," which are larger entities meeting specific criteria based on revenue, assets, or number of customers. Law to operate through a branch, agency, or commercial lending company.
3. **Insurance Companies:**
    - The company is an insurance entity with annual premiums written in New York State exceeding $1 billion, averaging over the last three years.

Timelines and Repercussions of Non-Compliance

DORA

DORA sets a compliance deadline of January 17, 2025, for EU financial institutions and critical third-party ICT providers to align their operations with DORA's stringent requirements including identity governance and administration. This transition period is critical for entities to assess and update their ICT risk management and governance frameworks to comply with DORA's standards.

Non-compliance with DORA can lead to serious consequences, including penalties and corrective actions. After the deadline, regulators will enforce compliance, requiring entities to address security gaps, fix vulnerabilities, and impose penalties, which can include administrative and, in some cases, criminal actions. Critical ICT providers, identified by the European Commission, will be overseen by European Supervisory Authorities (ESAs), which can issue fines of up to 1% of the provider's average daily global turnover, potentially applied daily for up to six months until compliance is achieved.

NYCRR 500

NYCRR 500 requires regulated entities to meet deadlines set by the New York State Department of Financial Services for implementing cybersecurity and identity governance measures. These deadlines are part of a phased approach, allowing organizations to gradually adopt the required practices. Firms must closely follow these timelines to ensure compliance with requirements, including those for IGA and other essential cybersecurity controls.

Failure to comply with NYCRR 500 can result in financial penalties, regulatory actions, or even the loss of their authorization to operate in the state. In addition to financial repercussions, non-compliance can lead to reputational damage with customers and the broader financial community. The New York State Department of Financial Services may also enforce actions, such as suspending operations, requiring the correction of deficiencies, or mandating additional cybersecurity and identity governance measures.

Comparison Matrix: DORA vs. NYCRR 500

Comparison Matrix: DORA vs. NYCRR 500		
Aspect	**DORA**	**NYCRR 500**
Jurisdiction	European Union (EU) member states.	State of New York, USA.
Scope	Applies to a wide range of financial entities, incluwWding banks, insurance companies, investment firms, crypto-asset service providers, and critical third-party ICT service providers.	Applies to financial entities operating under the Banking Law, Insurance Law, or Financial Services Law within New York State, including banks, insurance companies, and other financial services firms.
Objective	Enhance digital operational resilience across the EU's financial sector by standardizing ICT risk management and identity governance practices.	Strengthen cybersecurity and identity governance practices among New York financial entities to protect sensitive data and ensure system stability.
Implementation Deadline	Compliance required by **January 17, 2025.**	The last amendment to NYCRR500 took effect November 1, 2023. General compliance is required by **April 29, 2024,** which is 180 days after the effective date.
Entity Classification	No specific classification; however, critical entities have additional obligations, especially critical third-party ICT providers.	Introduces **Class A companies**, which are larger entities meeting specific criteria based on employees, revenue, or status as major financial institutions, subject to enhanced requirements.
Identity Governance Emphasis	Strong emphasis on identity governance and access management across all entities to ensure appropriate access controls and monitoring.	Mandates robust Identity Governance and Administration (IGA) practices, especially for Class A companies, including automated access controls and regular access reviews.
Risk Management Framework	Requires comprehensive ICT risk management frameworks, including mapping of ICT assets, risk assessments, and implementation of controls.	Requires entities to maintain a cybersecurity program based on periodic risk assessments, addressing identified risks with appropriate controls.
Senior Management Accountability	Management bodies are directly responsible for ICT risk management and identity governance, including oversight and approval of policies.	Requires senior management and board of directors to be involved in cybersecurity and identity governance efforts, including annual certification of compliance.

Aspect	DORA	NYCRR 500
Technical Testing Requirements	Mandates regular testing, including vulnerability assessments and **threat-led penetration testing (TLPT)** every three years for critical entities.	Requires regular penetration testing and vulnerability assessments; does not specifically mandate TLPT but emphasizes frequent testing and monitoring.
Incident Reporting	Structured incident reporting with specific timelines for initial (within 24 hours), intermediate (within 72 hours), and final reports to regulators (within 1 month).	Requires prompt notification to NYDFS within **72 hours** of determining a cybersecurity event has occurred; focuses on timely reporting to regulators.
Third-party Risk Management	Extends requirements to critical third-party ICT service providers, including oversight and contractual obligations to ensure compliance.	Requires entities to assess and manage risks posed by third-party service providers, including due diligence and contractual safeguards.
Information Sharing	Encourages voluntary information sharing among financial entities to improve collective cybersecurity posture.	Does not explicitly promote information sharing between entities; focuses on individual entity compliance and security.
Enforcement and Penalties	Enforcement by competent authorities in each EU member state; critical ICT providers supervised by European Supervisory Authorities (ESAs). Penalties can include fines up to **1% of average daily worldwide turnover,** possibly applied daily until compliance.	Enforcement by the New York State Department of Financial Services. Penalties can include substantial fines, license revocation, and other regulatory actions based on the severity of non-compliance.
Exemptions	Limited; certain provisions may not apply to small entities, but overall, DORA has broad applicability.	Provides limited exemptions for smaller entities based on size and financial thresholds (e.g., fewer than 20 employees, less than $5 million in gross annual revenue).
Overall Theme	Harmonization of cybersecurity and operational resilience practices across the EU financial sector, with a strong emphasis on identity governance and third-party risk management.	Strengthening cybersecurity and identity governance within New York's financial sector, focusing on protecting customer data and ensuring the integrity of financial systems.

Recommendations for Financial Entities on Aligning with Both DORA and NYCRR 500

☐ **Conduct Comprehensive Risk Assessments**	Begin with a thorough risk assessment to identify vulnerabilities within your ICT and identity governance frameworks. This assessment should inform the development of a tailored cybersecurity and identity governance program that addresses specific risks identified in your operational and technological environments.
☐ **Develop and Implement Robust Cybersecurity and Identity Governance Policies**	Craft comprehensive policies that encompass aspects such as identity lifecycle management, access certification, segregation of duties, and policy management. Ensure these policies are regularly reviewed and updated to reflect changing threat landscapes and regulatory requirements.
☐ **Ensure Senior Management Engagement**	Foster a culture of cybersecurity awareness and accountability at all levels, with senior management playing a pivotal role in championing cybersecurity and identity governance initiatives and ensuring regulatory compliance.
☐ **Leverage Advanced Identity Governance Solutions**	Invest in an advanced and modern IGA solution, which can significantly enhance your ability to manage user identities, access rights, and compliance with policies. These solutions enable automated provisioning and deprovisioning, role-based access control, access certification campaigns, and segregation of duties enforcement, aligning with regulatory emphasis on effective identity governance.

Technical Requirements at a Glance

DORA Technical Requirements

ICT Risk Management and Governance

DORA mandates that the management bodies of financial entities are directly responsible for ICT risk management and identity governance. This includes the development of comprehensive risk management frameworks that map ICT systems, identify critical assets, and assess dependencies. Entities must also establish policies and procedures for effective identity governance, ensuring that user access rights are appropriately assigned, monitored, and reviewed. This encompasses the entire identity lifecycle, from onboarding to offboarding, and includes regular certification of access rights to prevent accumulation of excessive privileges.

Incident Reporting

Financial institutions are required to implement systems for the continuous monitoring, management, and reporting of ICT-related incidents, including those stemming from identity-related breaches. This includes the classification of incidents and the submission of detailed reports to regulators and, where necessary, affected clients and partners. The reporting process is structured to include initial, intermediate, and final reports, providing comprehensive insights into incident management and resolution.

Digital Operational Resilience Testing

Regular testing of ICT systems is a cornerstone of DORA, aimed at evaluating the effectiveness of cybersecurity measures and identifying vulnerabilities. Entities must conduct vulnerability assessments, scenario-based testing, and, for those deemed critical to the financial system, threat-led penetration testing (TLPT) every three years, involving critical ICT providers in the process. These tests should include assessments of identity governance controls to ensure that access rights are properly managed and that there are no weaknesses that could be exploited by malicious actors.

Third-party Risk Management

DORA extends its requirements to include the management of risks associated with third-party ICT service providers. Financial entities are expected to actively manage these relationships, ensuring that contractual arrangements cover exit strategies, performance targets, and compliance with security, accessibility, and integrity standards. This includes verifying that third-party providers have robust identity governance practices in place, as their security posture can directly impact the financial entity's risk exposure.

Information Sharing

The regulation encourages financial entities to participate in voluntary threat intelligence sharing arrangements. This aims to foster a collaborative approach to cybersecurity, enabling entities to learn from both internal and external ICT-related incidents while ensuring the protection of sensitive information in line with existing data protection regulations. Sharing information about identity-related threats and vulnerabilities can enhance the overall security posture of the financial sector.
aging credentials securely, ensuring secure remote access, and monitoring third-party activities are critical components in safeguarding against potential security breaches.

Technical Requirements at a Glance

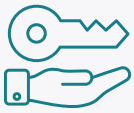
NYCRR500 Technical Requirements

Cybersecurity Policy

Entities are required to develop and maintain comprehensive cybersecurity policies that address various aspects of their information security program, including identity governance and administration. These policies should be reflective of the entity's risk assessment and cover areas such as data governance, access controls, and incident response. The policies must outline procedures for assigning, reviewing, and revoking access rights, ensuring that identity governance practices are consistently applied across the organization.

Penetration Testing and Vulnerability Assessments

NYCRR 500 emphasizes the importance of regular penetration testing and vulnerability assessments to identify potential security weaknesses. Entities must integrate these practices with assessments of their identity governance controls to ensure that any vulnerabilities related to user access and privileges are identified and remediated promptly.



Access Privileges and Management

The regulation mandates strict adherence to the principles of zero trust and least privilege, requiring entities to implement controls that limit access based on necessity and duration of need. This includes managing, reviewing, and monitoring all access rights, not just privileged access, and eliminating unnecessary privileges. Entities are required to conduct periodic access reviews to validate that users have appropriate access based on their roles and responsibilities, and to ensure that access is revoked promptly when no longer needed.

Application Security and Third-party Service Provider Security

NYCRR 500 requires entities to secure application development and manage the security of third-party service providers. This involves ensuring that identity governance controls are embedded within application security practices, and that third-party providers adhere to robust identity governance standards. Managing credentials securely, ensuring secure remote access, and monitoring third-party activities are critical components in safeguarding against potential security breaches.

Multi-Factor Authentication (MFA) and Monitoring

The enforcement of Multi-Factor Authentication (MFA) across all access points, coupled with comprehensive monitoring of user activities, forms a critical aspect of NYCRR 500's requirements. Entities must deploy MFA to mitigate unauthorized access risks and implement solutions for the real-time monitoring of activities involving sensitive systems and data. This includes monitoring for anomalous access patterns that could indicate compromised identities or insider threats.

Incident Response and Business Continuity Management

Entities must have in place incident response plans and business continuity management strategies to effectively address and recover from cybersecurity incidents, including those related to identity governance failures. This includes the development of templates and checklists that outline roles, responsibilities, and steps for containment and recovery. Ensuring that identity governance processes are included in incident response plans is essential for timely detection and mitigation of identity-related incidents.

Importance of Adopting Comprehensive Identity Governance Measures

Holistic Security Posture
Integrating comprehensive identity governance measures is essential for creating a holistic security posture that can effectively counteract sophisticated cyber threats and align with regulatory requirements. Effective IGA practices reduce the risk of unauthorized access, data breaches, and insider threats by ensuring that access rights are appropriate and up to date.

Regulatory Compliance
Adopting advanced identity governance technologies and practices ensures compliance with both DORA and NYCRR 500, mitigating the risk of penalties associated with non-compliance. It demonstrates a commitment to safeguarding sensitive data and maintaining operational integrity.

The detailed technical requirements of both DORA and NYCRR 500 underscore a shared objective:
To enhance the cybersecurity, operational resilience, and identity governance of the financial sector.

While each set of regulations has its unique focus and jurisdictional scope, together they reflect a broader global trend towards strengthening the digital defenses and identity management practices of financial institutions.

Suggestions for EU Entities on Preparing for DORA

Establish a Robust ICT and Identity Governance Framework
Align your ICT risk management and identity governance strategies with DORA's requirements by establishing a framework that encompasses risk identification, assessment, and mitigation processes, ensuring continuous improvement and adaptation to emerging threats.

Engage in Digital Operational Resilience and Identity Governance Testing
Regularly perform resilience testing, including assessments of your identity governance controls, to evaluate the effectiveness of your cybersecurity defenses and identify areas for enhancement. This includes conducting access reviews and segregation of duties analyses to detect and remediate any inappropriate access rights.

Manage Third-party Risks
Develop a comprehensive third-party risk management program that evaluates and monitors the cybersecurity and identity governance practices of your ICT service providers, ensuring they meet DORA's standards and contribute positively to your overall operational resilience.

By following these concrete steps, financial entities can not only align with the regulatory stars of DORA and NYCRR 500 but also fortify their defenses against the cosmic challenges posed by cyber threats. This strategic alignment ensures the protection of sensitive data, the resilience of financial operations, and the maintenance of customer trust in an increasingly digitalized world.

Conclusion

As cyber threats continue to evolve, regulations like DORA and NYCRR 500 have become essential in fortifying the financial sector's cybersecurity and identity governance practices. These regulations push financial institutions to adopt a comprehensive approach to risk management, resilience, and incident response—ensuring sensitive data is protected and systems remain stable in the face of growing threats.

For financial institutions, complying with these regulations isn't just about meeting legal requirements—it's about taking a proactive stance to defend against the ever-changing landscape of cyber risks. Implementing strong cybersecurity and identity governance frameworks not only avoids penalties but also demonstrates a firm commitment to safeguarding customer data and maintaining the integrity of operations.

At the heart of this defense is a multi-layered security strategy. By prioritizing identity governance, robust access controls, and Zero Trust principles, organizations can better protect themselves against cybercriminals seeking to exploit valuable data. By understanding how cybercriminals monetize stolen data and selecting the right monitoring solutions, institutions can build a resilient defense and stay one step ahead of evolving threats.

This is a critical moment for the financial sector—not just to comply, but to lead the charge in setting the standard for cybersecurity excellence.

About Omada

Omada Identity simplifies Identity Governance by providing a full-featured, cloud-native IGA solution that streamlines the complex processes of managing user identities, access, and entitlements. With a focus on automation and user-centric design, Omada reduces manual tasks and enhances operational efficiency, ensuring that organizations can easily enforce security policies, comply with regulations, and manage user access at scale. By leveraging advanced technologies such as AI-driven decision-making and role-based access control (RBAC), Omada enables businesses to achieve stronger security, better compliance, and improved user experiences—without the complexities traditionally associated with identity governance.

www.omadaidentity.com