DATASHEET

DORA Compliance

Transform Your DORA Journey with Mimecast.

The Problem

The Digital Operational Resilience Act (DORA) marks a critical turning point for financial institutions in the European Union. As the January 17, 2025, compliance deadline approaches, organizations face unprecedented pressure to transform their digital resilience frameworks. The stakes are significant - non-compliance brings fines up to 2% of global annual turnover, operational restrictions, and lasting reputational damage that erodes customer trust.

What makes DORA particularly challenging is its sweeping scope. Financial institutions must navigate complex requirements across ICT risk management, incident reporting, and third-party oversight. The regulation demands substantial organizational changes and expertise that many organizations struggle to develop internally. As financial institutions grapple with these interconnected challenges while managing their critical ICT providers, the path to compliance requires careful navigation through a complex regulatory landscape that leaves no room for error.

2% FINE

of global turn over due to noncompliance[1]

$6.08 MILLION

average cost of a data breach[2]

1M€

fine for individuals[3]

[1] https://www.avenga.com/magazine/guide-to-doras-penalties/

[2] https://securityintelligence.com/articles/cost-of-a-data-breach-2024-financial-industry/

[3] https://securityintelligence.com/articles/cost-of-a-data-breach-2024-financial-industry/

The Solution

Mimecast delivers a comprehensive solution framework that addresses DORA compliance requirements. Our platform combines advanced collaboration security with multi-layered file inspection capabilities, powered by AI and threat intelligence, to protect complex email environments. Through seamless integration with existing security infrastructure, automated remediation and robust threat intelligence sharing capabilities provide detection and monitoring, enabling organizations to gain holistic threat visibility with contextual email telemetry and priority-based alerting.

Organizations can maintain uninterrupted communication access regardless of the originating event. Continuous learning through Mimecast Human Risk Management capabilities ensures users are aware of the latest threats and engaged at the point of risk. Backup and recovery ensure critical communication data can be restored regardless of the originating event. This integrated approach aids organizations in their DORA compliance and provides a strategic advantage in managing their digital operational resilience.

Key Benefits

- **Risk Visibility.** Get unprecedented visibility into human risk within your organization, compiled based on user behavior and real-world threats.
- **Adaptive actions.** Tackle unsafe behaviors with timely feedback and engaging training, delivered to those who need it, when they need it.
- **Proactive controls.** Mitigate human risk across your security landscape by proactively adjusting security controls to better protect users.

DORA Compliance Made Simple: The Mimecast Advantage

At Mimecast, we recognize that DORA compliance demands a multifaceted solution framework. Our comprehensive approach addresses both technical requirements and policy-aligned controls through integrated ICT risk management that encompasses protection, prevention, detection, continuous learning, and robust backup and recovery capabilities. Here's how we help financial entities meet DORA's critical requirements:

Protection and Prevention

Our advanced collaboration security is designed to keep even the most complex email environments secure through its multi-layered inspection capabilities, powered by traditional defenses, threat intelligence, and advanced AI. Every element of an email is inspected in real-time, stopping threats before they reach your inbox. Mimecast seamlessly integrates with your existing security stack while providing automated remediation capabilities. This enables IT and security teams to effectively control risk while taming complexity, empowering your organization to defend against sophisticated email attacks without compromising business continuity. Through Incydr, organizations gain comprehensive visibility into data exposure, eliminating potential blind spots. The system intelligently differentiates between genuine threats and low-risk events, optimizing time spent on investigating critical IP theft incidents through advanced content inspection and contextual analysis. Through our technology partners automated network isolation capabilities are available to effectively contain potential cyber incidents.

Detection and Monitoring

Integration is core at Mimecast, and we value threat intelligence sharing with third-party tools. This enables organizations to enhance their security posture by leveraging collective intelligence from multiple sources, providing holistic threat visibility and contextual email telemetry The generation of priority-based alerting and automated data exchange accelerates investigations while reducing manual effort through response actions, allowing security teams to respond more effectively to emerging threats.

Response and Recovery

Continuity guarantees uninterrupted communication access during both planned and unplanned outages. Supported by geographically dispersed data centers and backed by a 100% service availability SLA, this capability is essential for financial entities requiring continuous operations under DORA's framework.

Continuous Learning and Evolution

Mimecast Engage transforms potential security vulnerabilities into organizational strengths through targeted training and risk scoring. The Human Risk Management capabilities provide detailed insights into employee behaviors and risk profiles encompassing your security tools, delivering customized security awareness training that adapts to emerging threats.

Comprehensive Backup and Recovery

Sync and Recover enables swift operational restoration following accidental data loss or malicious actions. This specifically addresses email-based threats like ransomware, offering rapid, granular recovery of mailboxes, calendars, and tasks, with configurable retention policies.

Additionally, our tools are designed to support your audit, integrated logging, and threat sharing requirements, enabling organizations to meet and maintain compliance. By partnering with Mimecast, financial entities can confidently address DORA compliance while enhancing their overall digital operational resilience. Our solutions not only help meet regulatory requirements but also provide a strategic advantage in managing ICT risk in today's complex digital environment.

DORA Article	Details
9 - Protection and prevention	Collaboration Security • AI-powered protection against phishing and BEC attacks through relationship analysis and NLP • Multi-layered malware defense with sandboxing, URL security, and QR code protection • Centralized web console for cross-platform management with automated IAM sync and intelligent routing Data Protection • AI-powered content inspection detects sensitive data and IP in exfiltrated files • Combines standard and custom risk indicators to identify unauthorized transfers of privileged content and proprietary information • Evaluates content sensitivity, file metadata, and classification for comprehensive exfiltration detection
10 - Detection	• Two-way threat intelligence sharing across security platforms enables real-time synchronization between endpoints, firewalls, and email security • Comprehensive integration across threat sharing, investigation, daily tasks, and automated response • SOAR and XDR platform integrations enable automated threat remediation, reducing response times from hours to minutes
11 - Response and Recovery	• Seamless integration Microsoft Outlook with cross-platform support (mobile, web, Mac), full email functionality with SMS notifications • Advanced email monitoring with admin-defined thresholds and automated alerts • Targeted continuity event management for individuals or groups, maintaining security while enabling automatic mailbox synchronization for quick recovery
12 - Backup policies and procedures, restoration and recovery procedures and methods	• Monitor inbound and outbound email using admin-defined thresholds • Receive automated alerts provide an event-specific console displaying key information and one-click activation of an alternate mail path • Rapidly trigger continuity events when primary email systems are offline • Invoke continuity events for individuals or groups without triggering an organization-wide event • Maintain full email security protection during continuity events • Reduce cleanup time through automatic mailbox synchronization
13 - Learning and evolving	• Comprehensive risk scoring based on real/simulated phishing data to identify organizational threats and high-risk employees • Real-time behavioral coaching through micro-learning modules and nudges, reinforcing security best practices • Quick-start automated security awareness program with industry compliance and phishing simulation capabilities

About Mimecast

Secure human risk with a unified platform.

Mimecast’s connected human risk management platform prevents sophisticated threats that target human error. By gaining visibility into human risk across your collaboration landscapes you can protect your organization, safeguard critical data, and actively engage employees to reduce risk and enhance productivity.