Runecast

Navigating DORA for MSPs

The introduction of the Digital Operational Resilience Act (DORA) by the European Union presents complex challenges for Managed Service Providers (MSPs) in the financial sector.

This eBook is designed to guide MSPs through the intricacies of DORA, offering clear strategies and insights to navigate this new regulatory landscape effectively.

INTRODUCTION TO DORA AND HOW IT'S DIFFERENT

The Digital Operational Resilience Act (DORA) is a new regulatory framework introduced by the European Union to enhance the operational resilience of the financial sector. It aims to ensure that financial institutions are able to withstand and recover from a wide range of ICT disruptions, including cyberattacks, natural disasters, and power outages.

DORA builds upon existing cybersecurity frameworks and standards, such as ISO 27001, NIST Cybersecurity Framework, and PCI DSS. However, it goes beyond these frameworks by introducing additional requirements specifically tailored to the financial sector.

Aspect	DORA	ISO 27001/NIST/CIS
Primary Focus	Digital operational resilience specifically in the financial sector.	Broader focus on information security and cybersecurity across various industries.
Industry Specificity	Tailored for financial services.	Applicable to a wide range of industries, not specific to finance.
Key Requirements	Emphasis on ICT risk management, incident reporting, resilience testing, managing third-party risks.	Focus on establishing and maintaining security practices, risk management, and control frameworks.
Third-Party Management	Specific stringent requirements for managing and monitoring third-party risks, especially MSPs.	General requirements for managing third-party information security risks.
Reporting Requirements	Mandatory incident reporting within strict timelines specific to the financial sector.	Incident management and response; specific reporting requirements vary.
Compliance Enforcement	Mandatory for relevant entities in the EU financial sector.	Often voluntary, but can be required for contracts or regulatory reasons.

DORA's Mandate for MSPs in BFSI

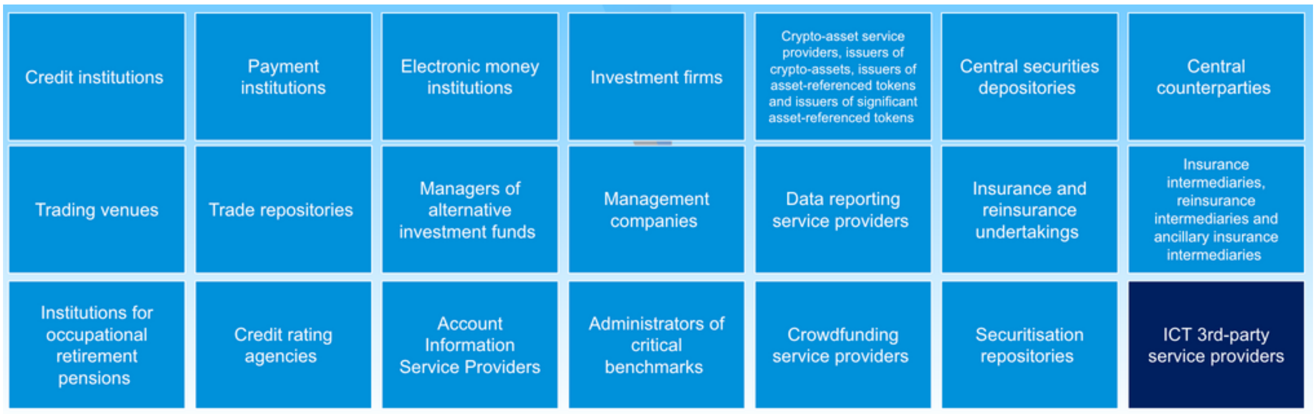
For managed service providers (MSPs) serving the Banking, Financial Services, and Insurance (BFSI) sector, compliance with the Digital Operational Resilience Act (DORA) is not just critical, it's **mandatory**. MSPs are key in managing ICT infrastructure for financial institutions, directly impacting the sector's resilience and regulatory adherence.

CHAPTER 1
QUICK START GUIDE

Snapshot of DORA

The Digital Operational Resilience Act (DORA) represents a significant regulatory development aimed at enhancing the resilience of the European financial sector against information and communications technology (ICT) disruptions.

This EU regulation entered into force on 16 January 2023 and will become **legally enforceable from 17 January 2025.** It encompasses all financial institutions within the EU and extends to relevant third-party service providers, including managed service providers (MSPs).



Credit institutions	Payment institutions	Electronic money institutions	Investment firms	Crypto-asset service providers, issuers of crypto-assets, issuers of asset-referenced tokens and issuers of significant asset-referenced tokens	Central securities depositories	Central counterparties
Trading venues	Trade repositories	Managers of alternative investment funds	Management companies	Data reporting service providers	Insurance and reinsurance undertakings	Insurance intermediaries, reinsurance intermediaries and ancillary insurance intermediaries
Institutions for occupational retirement pensions	Credit rating agencies	Account Information Service Providers	Administrators of critical benchmarks	Crowdfunding service providers	Securitisation repositories	ICT 3rd-party service providers

Top 5 Things MSPs Need to Know

Preparation for DORA's Full Effectiveness: Although DORA is already legally binding, it becomes legally enforceable on 17 January 2025. This period leading up to 2025 is crucial for MSPs to align their practices and prepare thoroughly for the regulations that DORA will enforce.

Critical Role of MSPs: MSPs are integral to the ICT infrastructure of financial institutions. Under DORA, their role in ensuring operational resilience against a wide spectrum of ICT threats—including cyberattacks, natural disasters, and human error—is emphasized.

Wide-Ranging Scope: DORA's approach to operational resilience covers various ICT risks. MSPs must develop and maintain a comprehensive ICT risk management framework that aligns with DORA's standards to ensure compliance.

Mandatory Incident Reporting: Prompt reporting of ICT incidents to financial clients and relevant authorities is a key requirement under DORA. MSPs must establish mechanisms for timely incident detection, reporting, and response.

Continuous Compliance Journey: Compliance with DORA is not a one-off task but an ongoing commitment. MSPs should institute a robust and dynamic compliance program to adapt to evolving requirements and maintain operational resilience consistently.

CHAPTER 2
EMBRACING YOUR ROLE UNDER DORA

MSPs as Vital Pillars of Financial Services Industry

The Digital Operational Resilience Act (DORA) recognizes the crucial role that managed service providers (MSPs) play in safeguarding the ICT infrastructure of financial institutions. As the custodians of critical financial data and operations, MSPs bear a significant responsibility in ensuring the resilience of the financial sector against ICT disruptions.

DORA outlines a comprehensive framework for MSPs to enhance their operational resilience and contribute to the overall stability of the financial services sector. By proactively addressing ICT risks, conducting thorough resilience testing, and fostering open collaboration with financial institutions, MSPs play a pivotal role in preventing and mitigating ICT disruptions. In doing so, they not only safeguard the financial sector from potential losses and reputational damage but also protect their own interests and contractual obligations.

Key Obligations for DORA Compliance

To fulfill their obligations under DORA, MSPs must implement robust ICT risk management practices, including:

Risk Identification and Assessment: Thoroughly identifying and assessing potential ICT risks that could impact financial clients. This involves analyzing the likelihood and potential impact of various threats, such as cyberattacks, natural disasters, and human error.

Risk Mitigation Controls: Implementing effective risk mitigation controls to reduce the likelihood and impact of identified ICT risks. These controls may include access controls, data encryption, security awareness training, and regular system updates.

Risk Monitoring and Review: Continuously monitoring and reviewing ICT risks to ensure that mitigation controls are effective and that emerging risks are promptly addressed. This ongoing assessment enables MSPs to adapt their risk management strategies proactively.

Incident Reporting Protocols: Establishing clear and concise incident reporting protocols to promptly notify financial clients and relevant authorities of any ICT incidents. This timely communication is crucial for effective incident response and recovery.

Resilience Testing: Conducting regular resilience testing exercises to evaluate the ability of systems and processes to withstand ICT disruptions. These tests should simulate various scenarios to assess the effectiveness of risk management strategies and incident response plans.

Collaboration with Financial Institutions: Fostering close collaboration with financial clients to share information on cyber threats, vulnerabilities, and incident response plans. This collaboration facilitates joint risk management strategies and enhances overall resilience.

COMPLIANCE PROGRAM CHECKLIST

To ensure seamless compliance with DORA, MSPs should implement a comprehensive compliance program that encompasses the following steps:

☑ **Conduct a Comprehensive ICT Risk Assessment:** Perform a thorough risk assessment to identify, assess, and prioritize ICT risks across all systems, applications, and data assets.

☑ **Develop an ICT Risk Management Framework:** Establish a robust risk management framework that outlines clear procedures for risk identification, assessment, prioritization, mitigation, monitoring, and review, while also emphasizing the importance of assigning ownership and accountability for these tasks.

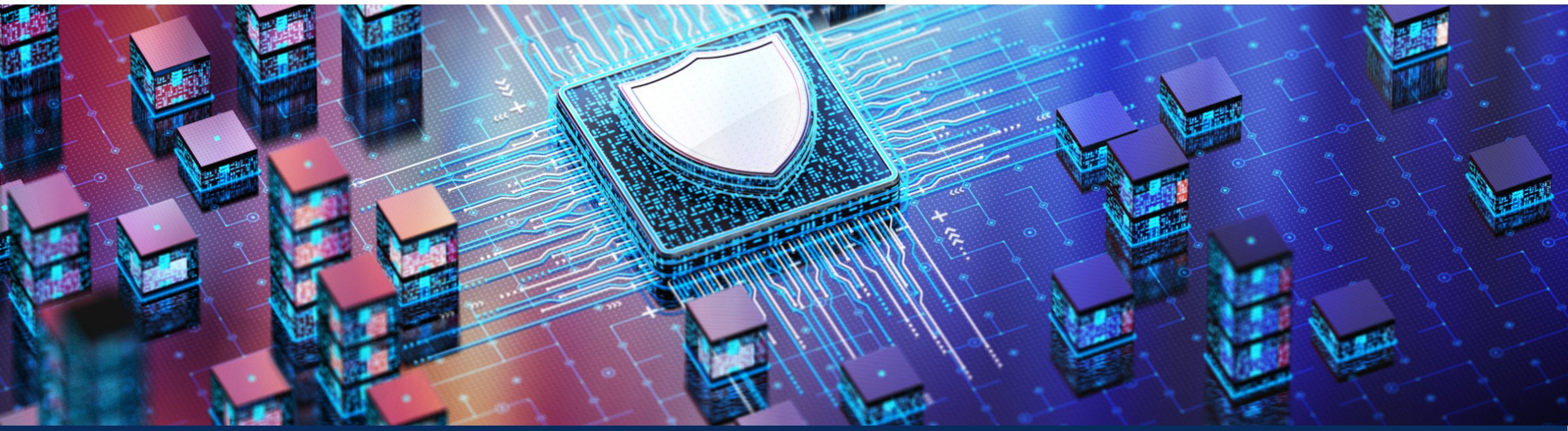
☑ **Implement Incident Response Procedures:** Develop and implement clear, well-defined incident response procedures that outline roles, responsibilities, and communication protocols for handling ICT incidents effectively.

☑ **Provide DORA Awareness Training:** Provide comprehensive training to all staff on DORA requirements, their roles and responsibilities, and the importance of incident reporting and collaboration with financial institutions.

☑ **Maintain Compliance Documentation:** Maintain detailed records of all compliance activities, including risk assessments, incident reports, testing results, and staff training records.

☑ **Conduct Regular Internal Audits:** Conduct regular internal audits to evaluate the effectiveness of risk management practices, incident response procedures, and overall compliance with DORA requirements.

By adhering to these steps, MSPs can not only demonstrate their commitment to DORA compliance but also ensure their own compliance against the regulation.



CHAPTER 3
ACTIONABLE COMPLIANCE STRATEGIES FOR MSPS

The Digital Operational Resilience Act (DORA) has introduced significant requirements for managed service providers (MSPs) to enhance their ICT risk management practices and contribute to the overall resilience of the financial sector. While compliance with DORA may seem daunting, MSPs can implement actionable strategies to effectively meet the regulatory requirements and achieve a robust cybersecurity posture.

Embrace Risk Management as a Core Business Function

DORA emphasizes the importance of proactive risk management as a cornerstone of compliance. MSPs should integrate risk management into their core business processes, ensuring that ICT risks are systematically identified, assessed, and mitigated throughout the organization. This proactive approach enables MSPs to address potential threats before they escalate into significant incidents. Moreover, MSPs can distinguish themselves in the marketplace, transforming risk management into a key aspect of their value proposition to clients.

Establish a Comprehensive ICT Risk Management Framework

A well-structured ICT risk management framework provides a structured approach to identifying, assessing, prioritizing, and mitigating ICT risks. This framework should outline clear roles and responsibilities, define risk assessment methodologies, establish incident reporting procedures, and facilitate regular risk reviews.

Implement Robust Risk Mitigation Controls

To effectively reduce the likelihood and impact of ICT risks, MSPs should implement a range of risk mitigation controls. These controls may include:

- **Access controls:** Restricting access to sensitive systems and data to authorized personnel only.
- **Data encryption:** Encrypting sensitive data at rest and in transit to protect against unauthorized access.
- **Security awareness training:** Educating staff on cybersecurity best practices and common cyber threats.
- **Regular system updates:** Promptly applying security patches and updates to address vulnerabilities.
- **Network segmentation:** Segregating networks to minimize the spread of potential infections.
- **Regular vulnerability assessments:** Conducting periodic assessments to identify and address security vulnerabilities proactively.
- **Attack surface reduction:** Actively managing and minimizing the number of accessible entry points to reduce the potential attack vectors for cyber threats.

Prioritize Regular Resilience Testing

Resilience testing is crucial for evaluating the effectiveness of risk management strategies and incident response plans. MSPs should conduct regular resilience testing exercises to simulate ICT disruptions and assess their ability to withstand and recover from such events. These tests should cover a range of scenarios, including cyberattacks, natural disasters, and human error.

Foster Open Collaboration with Financial Clients

Effective collaboration with financial clients is essential for shared risk management and incident response. MSPs should establish clear communication channels with clients to share information on cyber threats, vulnerabilities, and incident response plans. This collaboration enables joint risk assessments, coordinated testing exercises, and a unified approach to ICT resilience.

Cultivate a Culture of Resilience

Instilling a culture of resilience within the organization is paramount for long-term compliance with DORA. MSPs should promote cybersecurity awareness among all staff, encourage open communication about potential risks, and emphasize the importance of prompt incident reporting. This culture of resilience fosters a proactive approach to ICT risk management and contributes to a more secure environment for both the MSP and its financial clients.

CHAPTER 4:
INCIDENT HANDLING AND COMMUNICATION: A GUIDE FOR MSPS

Managed service providers (MSPs) play a critical role in ensuring the resilience of the financial sector by providing essential ICT services to financial institutions. However, as a result of their reliance on ICT, MSPs are also vulnerable to ICT disruptions, which can have a significant impact on their clients' operations. Therefore, it is crucial for MSPs to have robust incident handling and communication strategies in place to effectively manage ICT incidents and minimize disruptions to their clients.

Incident Handling Essentials

Prompt Identification and Classification: Upon identifying an ICT incident, MSPs should promptly classify the incident based on its severity, potential impact, and urgency. This classification will help prioritize incident response efforts and ensure that resources are allocated effectively.

Incident Response Plan Activation: Once an incident has been classified, MSPs should activate their incident response plan. This plan should outline clear roles and responsibilities, communication protocols, and mitigation strategies for different types of incidents.

Containment and Control: The primary focus of initial incident response should be to contain the incident and prevent further damage or disruption. This may involve isolating affected systems, disabling network access, or revoking user privileges.

Eradication and Recovery: Once the incident has been contained, MSPs should focus on eradicating the root cause and restoring affected systems to normal operation. This may involve removing malicious software, patching vulnerabilities, or restoring data from backups.

Documentation and Post-Incident Analysis: Throughout the incident response process, MSPs should maintain detailed documentation of their actions, decisions, and observations. This documentation will be crucial for post-incident analysis, identifying lessons learned, and improving future incident response efforts.

Incident Communication Strategies

Open and Transparent Communication: MSPs should maintain open and transparent communication with their clients throughout the incident response process. This includes providing regular updates on the status of the incident, the steps being taken to resolve it, and the expected timeline for recovery.

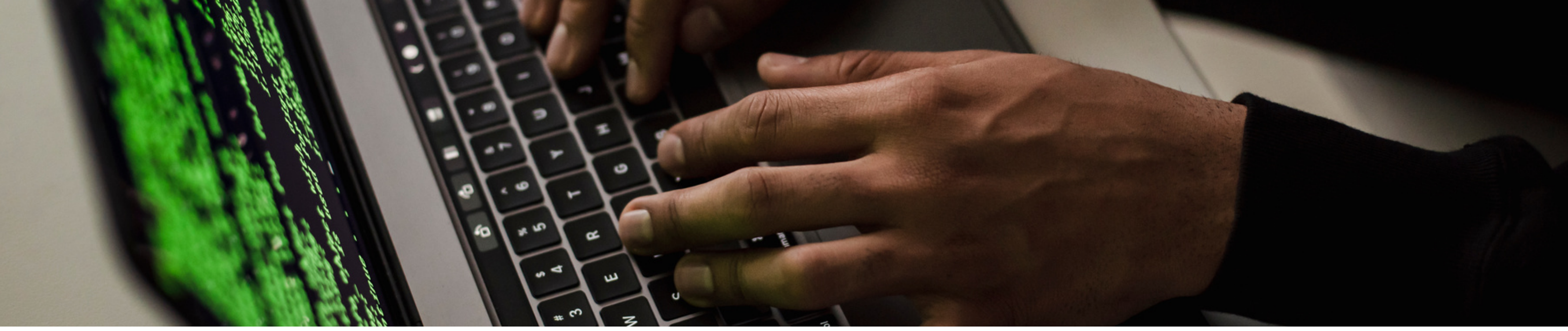
Clear and Consistent Messaging: MSPs should use clear and consistent language when communicating with clients about ICT incidents. This will help to avoid confusion, panic, or misunderstandings.

Establish a Single Point of Contact: MSPs should designate a single point of contact (SPOC) for all incident communication with clients. This will ensure that there is a clear and centralized channel for information sharing and inquiries.

Proactive Communication: MSPs should not wait for clients to inquire about the status of an incident. They should proactively communicate with their clients regularly, even if there is no significant change in the situation.

Client Feedback and Concerns: MSPs should be receptive to feedback and concerns from their clients throughout the incident response process. They should address any questions or concerns promptly and openly.

By implementing effective incident handling and communication strategies, MSPs can minimize the impact of ICT disruptions on their clients' operations and maintain their reputation as trusted providers of ICT services.



CHAPTER 5
PRACTICAL RESILIENCE TESTING: ENHANCING MSP PREPAREDNESS

Resilience testing is an integral component of DORA compliance for managed service providers (MSPs). It plays a crucial role in evaluating the effectiveness of ICT risk management practices and ensuring that MSPs can withstand and recover from ICT disruptions. By conducting regular resilience testing exercises, MSPs can identify potential vulnerabilities, assess the impact of various scenarios, and refine their incident response strategies.

Resilience Testing Methodologies

Vulnerability Assessments: Vulnerability assessments involve identifying and evaluating weaknesses in ICT systems, networks, and applications. These assessments can be conducted using automated tools or manual testing methods.

Penetration Testing: Penetration testing, also known as pen testing, simulates cyberattacks to test the effectiveness of security controls and identify exploitable vulnerabilities. Pen testers employ various hacking techniques to gain unauthorized access to systems and data.

Scenario-Based Testing: Scenario-based testing involves simulating realistic ICT disruptions, such as power outages, natural disasters, and large-scale cyberattacks. These scenarios allow MSPs to assess their ability to withstand and recover from various types of events.

Red Teaming Exercises: Red teaming exercises involve hiring a team of cybersecurity professionals to act as an adversarial group, attempting to compromise the MSP's systems and data using sophisticated techniques. This approach provides a more realistic simulation of a real-world cyberattack.

Incident Response Testing: Incident response testing evaluates the effectiveness of the MSP's incident response plan by simulating real-world incidents and measuring the team's response time, decision-making, and recovery capabilities.

Failover and Disaster Recovery Testing: This involves testing the MSP's ability to seamlessly switch to a backup system (failover) and recover critical functions after a disaster. It ensures that there are effective processes in place for data backup, system recovery, and maintaining business continuity during and after a major disruption.

Conducting Effective Resilience Testing Exercises

Define Clear Objectives: Before conducting a resilience testing exercise, MSPs should clearly define the objectives of the test, identifying the specific areas they want to assess and the potential risks they want to evaluate.

Establish a Testing Plan: A comprehensive testing plan should outline the scope of the exercise, the scenarios to be simulated, the roles and responsibilities of participants, and the evaluation criteria.

Engage Experienced Testers: Resilience testing should be conducted by experienced and qualified cybersecurity professionals who can effectively simulate real-world threats and provide valuable insights.

Maintain Confidentiality: The results of resilience testing exercises should be treated with utmost confidentiality to protect sensitive information and prevent potential exploitation by malicious actors.

Continuous Improvement: Resilience testing is an ongoing process, and MSPs should regularly review and update their testing methodologies to reflect evolving threats and technologies.

Evaluating Resilience Testing Results

Identify Vulnerabilities and Gaps: Analyze the results of resilience testing exercises to identify any vulnerabilities, gaps in security controls, or weaknesses in incident response procedures.

Prioritize Remediation: Prioritize the remediation of identified vulnerabilities based on their severity and potential impact. Develop action plans to address the issues promptly and effectively.

Enhance Incident Response Plans: Incorporate lessons learned from resilience testing into incident response plans. Update procedures, improve communication protocols, and enhance training programs to strengthen the overall incident response capability.

Measure Improvement: Track progress over time to measure the effectiveness of resilience testing and identify areas for further improvement.

By conducting regular resilience testing exercises and effectively evaluating the results, MSPs can proactively enhance their preparedness for ICT disruptions, minimize their risk profile, and maintain the resilience of the financial sector.

Collaboration Agreements with Financial Entities

MSPs should establish clear collaboration agreements with their financial clients to facilitate effective risk management, incident response, and DORA compliance. These agreements should outline:

Joint Planning and Information Sharing: MSPs and clients should establish protocols for sharing information on cyber threats, vulnerabilities, and incident response plans.

Regular Communication and Coordination: Both parties should maintain open communication channels to discuss risk management strategies, compliance progress, and any emerging concerns.

Joint Testing and Assessments: MSPs and clients should collaborate on joint resilience testing exercises and assessments to ensure alignment and identify areas for improvement.

Escalation Procedures: Clear escalation procedures should be defined to address critical issues or non-compliance concerns promptly.

By carefully reviewing and amending existing contracts, incorporating DORA-compliant clauses, and establishing clear collaboration agreements, MSPs can navigate the legal and contractual landscape effectively and ensure compliance with the regulatory framework.

CHAPTER 6
AUDIT PREPARATION AND REGULATORY SCRUTINY

The Digital Operational Resilience Act (DORA) has introduced a heightened focus on regulatory scrutiny for managed service providers (MSPs) operating within the European Union. To ensure ongoing compliance with DORA and effectively manage regulatory audits, MSPs should implement a comprehensive audit preparation strategy.

Audit Readiness Checklist

Establish a DORA Compliance Team: Form a dedicated team responsible for overseeing DORA compliance, including risk management, incident response, and audit preparation.

Document ICT Risk Management Framework: Maintain detailed documentation of the MSP's ICT risk management framework, including risk identification, assessment, mitigation, monitoring, and review procedures.

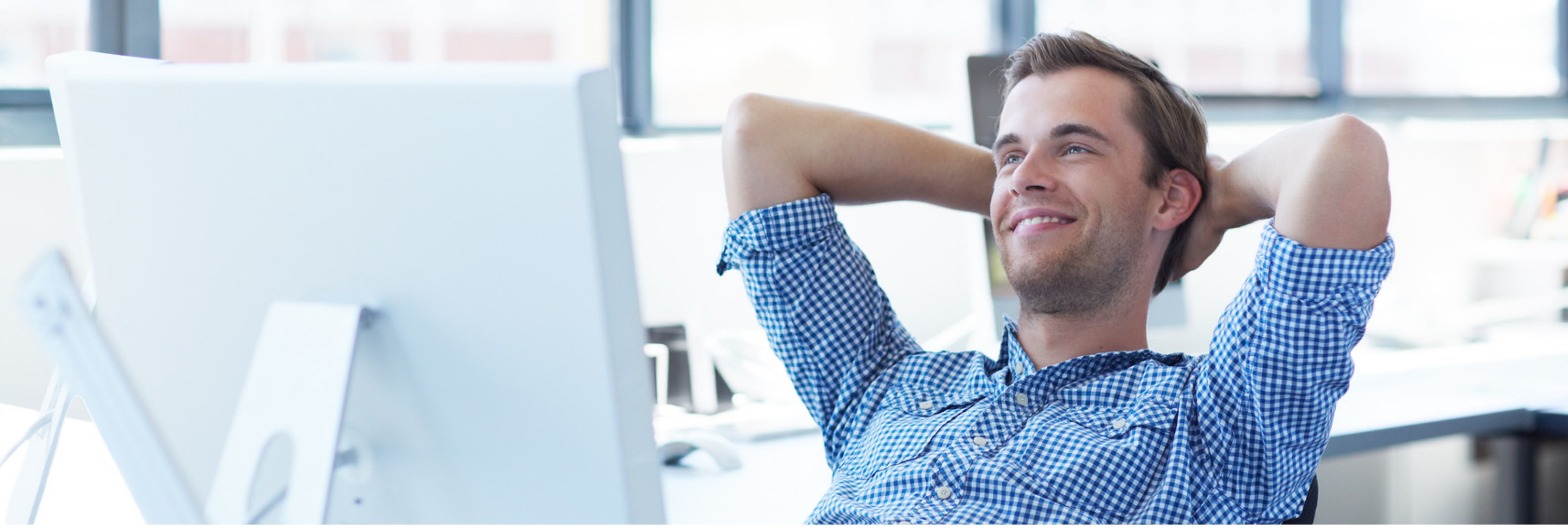
Record Resilience Testing Activities: Document all resilience testing exercises, including the scope, scenarios, results, and lessons learned.

Maintain Incident Response Logs: Keep comprehensive logs of all ICT incidents, including descriptions, response actions, and timelines for resolution.

Review Data Protection Practices: Regularly review data protection practices to ensure compliance with applicable data protection laws, such as the General Data Protection Regulation (GDPR).

Regularly Review Regulatory Updates: Stay informed about evolving regulatory requirements and industry best practices related to DORA compliance.

Conduct Internal Audits: Conduct regular internal audits to identify potential gaps and areas for improvement in DORA compliance.



Tips for a Smooth Audit Experience

Proactive Communication: Ensure open and ongoing communication with financial clients and regulators during the audit process. Provide clear, concise, and timely responses to any inquiries.

Demonstrate Compliance: Be ready to show compliance with DORA requirements. This includes presenting detailed documentation, test results, incident response logs, and evidence of continuous monitoring of internal compliance.

Address Findings Effectively: Quickly respond to any audit findings or issues of non-compliance. Implement corrective actions and document these improvements to demonstrate your commitment to compliance.

Continuous Improvement: Treat audits as opportunities for ongoing improvement. Utilize audit findings to refine risk management practices, enhance resilience, and continuously create compliance evidence. This approach not only addresses current compliance needs but also prepares for future audits and regulatory changes.

By implementing a comprehensive audit preparation strategy, MSPs can effectively manage regulatory scrutiny, address potential compliance issues promptly, and maintain the trust of their financial clients.

CHAPTER 7
EMBRACING CHANGE AND FOSTERING INNOVATION UNDER DORA

While DORA introduces new regulatory requirements for managed service providers (MSPs) specifically serving Banking, Financial Services, and Insurance (BFSI) customers, it also presents an opportunity to enhance cybersecurity posture, strengthen resilience, and maintain a competitive edge in the financial sector. By adapting to regulatory changes and fostering innovation, MSPs can navigate DORA effectively and continue to deliver high-quality ICT services to their financial services clients.

Adapting to Regulatory Changes

1. **Stay Informed:** Continuously monitor regulatory updates and proactively adapt ICT risk management practices, incident response plans, and data protection measures to align with evolving requirements.
2. **Collaborate with Regulators:** Establish open communication channels with regulatory bodies to clarify requirements, seek guidance, and demonstrate a commitment to compliance.
3. **Engage Industry Experts:** Seek advice from cybersecurity experts and industry peers to stay abreast of best practices and identify effective compliance strategies.
4. **Invest in Training and Awareness:** Provide comprehensive training to all staff on DORA requirements, their roles and responsibilities, and the importance of incident reporting and collaboration with financial institutions.

Fostering Innovation Within Compliance

1. **Embrace Technology Advancements:** Explore and adopt new technologies, such as artificial intelligence, machine learning and automation, to enhance risk management, threat detection, and incident response capabilities.
2. **Develop Innovative Solutions:** Collaborate with financial clients to develop innovative ICT solutions that address emerging risks and enhance operational resilience.
3. **Contribute to Industry Standards:** Actively participate in industry forums and standards bodies to shape the future of cybersecurity and resilience frameworks.
4. **Showcase Compliance as a Value Proposition:** Highlight DORA compliance as a competitive advantage, demonstrating a commitment to providing secure and resilient ICT services to financial clients.

By embracing regulatory changes, fostering innovation, and continuously improving their cybersecurity posture, MSPs can not only comply with DORA but also position themselves as trusted partners in the financial sector, driving innovation and resilience for the benefit of their clients and the broader financial ecosystem.

STREAMLINE YOUR DORA COMPLIANCE WITH AUTOMATED AUDITING

Runecast ensures continuous compliance auditing across hybrid environments, whether on-premises, OS, cloud, or containers – and can also run air-gapped for the most sensitive environments. It provides detailed historical insights and a comprehensive, regularly updated library of compliance standards, as well as custom profiles for any specific organizational needs. With robust integration capabilities, including diverse export options and a powerful API, Runecast simplifies the integration of compliance data with other essential tools, optimizing compliance management for any IT infrastructure.

SCHEDULE A 1:1 DEMO WITH A RUNECAST EXPERT

Runecast

Gartner
COOL VENDOR
2020

FROST & SULLIVAN
BEST PRACTICES
AWARDS

Runecast Solutions Ltd.

124 City Road,
London, EC1V 2NX
United Kingdom

Runecast Solutions Inc.

300 Delaware Ave
Suite 210, Box #241
Wilmington, DE 19801
USA