Kiteworks

DORA Compliance Best Practices Checklist

Mitigate ICT Risk and Demonstrate DORA Compliance

Financial services organizations operating in the European Union must mitigate Information and Communication Technology (ICT) risk, a critical component of the Digital Operational Resilience Act (DORA) compliance process. Follow these best practices to achieve risk mitigation and accelerate the compliance process:

- **1. Understand DORA Requirements:**
  Review the ICT risk management requirements until you genuinely understand them. Studying the regulations, guidelines, and directives provided by relevant regulatory authorities, such as the European Banking Authority (EBA) or other competent authorities.

- **2. Conduct Risk Assessments:**
  Administer comprehensive risk assessments of your ICT systems and operations to identify potential vulnerabilities, threats, and impacts. Risk assessments should cover areas such as cybersecurity, data protection, operational resilience, and service continuity.

- **3. Develop Risk Management Frameworks:**
  Establish robust risk management frameworks tailored to your organization›s ICT environment and business objectives. These frameworks should include policies, procedures, and controls for identifying, assessing, mitigating, and monitoring ICT risks effectively.

- **4. Implement Controls and Safeguards:**
  Implement appropriate controls and safeguards to mitigate identified ICT risks. Controls and safeguards include cybersecurity controls, access controls, encryption mechanisms, incident response procedures, and business continuity plans.

- **5. Enhance Cybersecurity Measures:**
  Implement defenses against cybersecurity-related risks, such as malware, phishing attacks, ransomware, and insider threats. Measures include multi-factor authentication, network segmentation, intrusion detection systems, and security awareness trainings.

- **6. Ensure Data Protection and Privacy Compliance:**
  Align data protection efforts to data privacy requirements specified in DORA and other relevant regulations like GDPR, DPA 2018, BDSG, and several others. Implement appropriate data protection measures, conduct privacy impact assessments, and ensure lawful processing of PII.

- **7. Establish Incident Response Capabilities:**
  Develop robust incident response capabilities to detect, respond to, and recover from ICT incidents and disruptions effectively. This includes forming incident response teams, defining escalation procedures, and conducting regular incident response exercises and simulations.

- **8. Monitor and Report Compliance:**
  Continuously monitor ICT risk management activities to ensure ongoing compliance with DORA requirements. Establish mechanisms for reporting ICT risk-related issues to senior management, regulatory authorities, and other stakeholders as required.

- **9. Engage in Regulatory Dialogue:**
  Actively engage in regulatory dialogue and collaboration with relevant regulatory authorities to ensure alignment with DORA requirements and expectations. Participate in industry forums, working groups, and consultations to stay informed about regulatory developments and best practices.

- **10. Continuous Improvement:**
  Lastly, foster a culture of continuous improvement in ICT risk management by regularly reviewing and enhancing policies, procedures, and controls based on emerging threats, lessons learned from incidents, and changes in the regulatory landscape.