Kiteworks

How to Mitigate Third Party Risk for DORA Compliance: A Best Practices Checklist

Adhering to DORA›s third party risk management requirements involves implementing a series of best practices designed to identify, assess, and mitigate risks effectively. These third-party risk management best practices are actionable steps that every IT, risk, and compliance professional should consider:

- **1. Conduct Thorough Due Diligence:** Assess a third-party provider's operational resilience, data protection measures, and overall risk profile. Examine their financial stability, compliance history, and cybersecurity protocols as well.
- **2. Establish Clear Contracts:** Ensure all third-party contracts include specific clauses relating to risk management, data protection, and DORA compliance. Clearly define roles, responsibilities, and expectations.
- **3. Implement Continuous Monitoring:** Set up mechanisms for continuous monitoring of third-party activities and performance. This can include regular audits, performance reviews, and real-time monitoring of key risk indicators.
- **4. Assess Risk Periodically:** Conduct periodic risk assessments to evaluate the impact of third-party providers on your organisation's operational resilience. This helps in identifying new risks and assessing the effectiveness of existing mitigation strategies.
- **5. Develop Incident Response Plans:** Collaborate with third party vendors to develop and test incident response plans. Ensure these plans are aligned with your organisation's overall incident management framework and DORA requirements.
- **6. Foster Strong Relationships:** Build and maintain strong relationships with your third-party providers. Build and maintain communication channels; regular engagement can help identify and address potential risks.
- **7. Maintain Documentation:** Keep detailed records of all risk management activities, assessments, and mitigation measures. This documentation is crucial for demonstrating compliance during regulatory audits and assessments.
- **8. Review and Update Policies:** Regularly review and update your third-party risk management policies to reflect changes in the regulatory landscape, emerging threats, and lessons learned from past incidents.