HYCU®

Getting started with DORA compliance

Your guide to meeting business continuity and resilience requirements in EU regulation.

CHECKLIST

01

Before We Start...

DORA covers a broad range of requirements, from incident response, to threat prevention. Specific to data protection, many organizations are unprepared to meet business continuity and resilience requirements. In fact, many companies aren't even aware that they are responsible for the compliance and data protection of their SaaS applications!

To understand your responsibility when it comes to SaaS and cloud data, read about the **Shared Responsibility Model** by scanning the QR code below.

Learn about the Shared Responsibility Model and avoid critical mistakes

Checklist

Meet DORA backup, disaster recovery and digital resilience requirements

Business continuity, backup, and testing are critical requirements you will have to meet with DORA.

How many boxes does your organization check today?

Getting Started Risk Assessment

- □ Create framework to identify and map all ICT services (ex. Atlassian Cloud, AWS, Salesforce, etc.)
- □ Leverage or build auditing templates to evaluate each ICT accross security, detection, response, and business continuity.
- □ Assign specific stakeholders responsible for data protection operations across all SaaS applications in use
- □ Leverage tools for continuous monitoring of ICTs and regularly document changes in your tech stack - accross all departments

Backup requirements

- □ Schedule daily backups for each instance and application in your environment
- □ Ensure backup copies are accessible in the event of an outage or cyber threat
- □ Define a minimum frequency of the backups based on the application
- □ Ensure the backup system is running outside and detached from from the primary SaaS applications.
- □ Store backups offsite in S3-compatible storage, independent of the primary SaaS applications.
- □ Enable immutability on the backup storage target in case of a cyber event
- □ Backup storage site must meet residency requirements (if applicable)
- □ Implement and maintain multi-factor authentication, encryption, and network segmentation to safeguard backup integrity and confidentiality.

Incident response & recovery

- □ Assign recovery SLAs in proportionality with the critical nature of the application
- □ Develop and regularly update disaster recovery plans that include templates for different incident scenarios. Ensure these plans are comprehensive and tailored to organizational needs.
- □ Conduct periodic training and simulations to enhance staff preparedness for incident response. Focus on roles, responsibilities, and actions for effective incident management.

Demonstrable recovery & reporting

- □ Maintain documentation and records to demonstrate compliance with DORA requirements, ensuring readiness for audits and inspections.
- □ Leverage advanced tools for continuous monitoring and real-time reporting of backup and recovery activities, enhancing decision-making and incident response capabilities.

HYCU®

Take control of your data

Discover DORA compliance gaps and turn on data protection with this free SaaS discovery tool