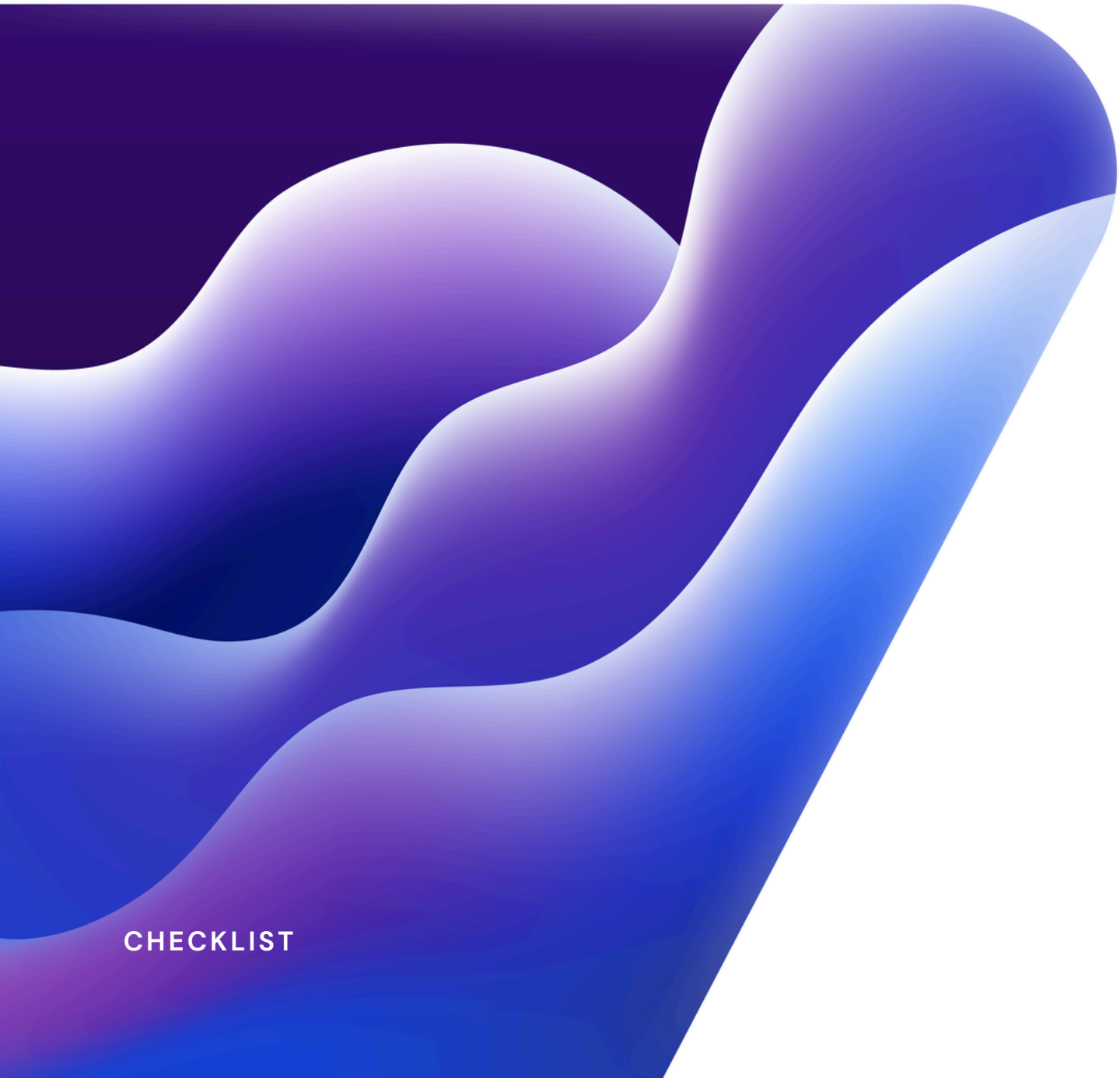
HYCU®

Atlassian Cloud NIS2 & DORA

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



CHECKLIST

HYCU®

01

Before We Start...

NIS2 and DORA regulation cover a broad range of requirements, from incident response, to threat prevention. However, specific to data protection, many organizations are unprepared to meet business continuity and resilience requirements. In fact, many companies aren't aware that they are still responsible for the compliance and data protection of their SaaS applications! To understand your responsibility in Atlassian, read about the **Atlassian Cloud Shared Responsibility Model** by scanning the QR code below.

Read the Atlassian Shared Responsibility Model

Checklist

Meet NIS2 & DORA BC/DR and digital resilience requirements

Business continuity, backup, and testing are critical requirements you will have to meet with NIS2 and DORA.

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 Atlassian and other business applications
- [ ] Leverage tools for continuous monitoring of ICTs and regularly document changes in your tech stack - accross all departments
- [ ] Maintain documentation and records to demonstrate compliance with NIS2 and DORA requirements, ensuring readiness for audits and inspections.

Backup requirements

- [ ] Schedule daily backups for each instance and application in Atlassian Cloud
- [ ] 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 Atlassian
- [ ] Store backups offsite, outside of Atlassian in S3-compatible storage.
- [ ] 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 NIS2 and 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

Get started and scan the QR code below or contact us at hycu.com/contact-us