



# Governance, Risk and Compliance solution for DORA

Powered by:



[www.valiantys.com](http://www.valiantys.com) | [www.lansweeper.com](http://www.lansweeper.com) | [www.hycu.com](http://www.hycu.com) | [www.appfire.com](http://www.appfire.com)

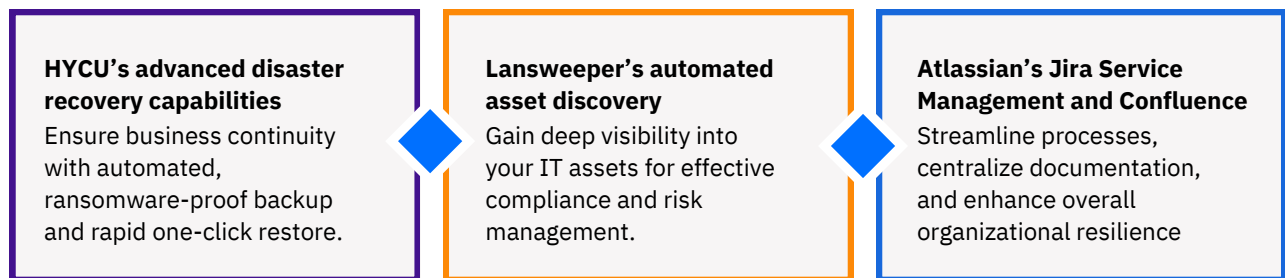
## Empowering Business Continuity with Integrated Compliance

### Business challenge:

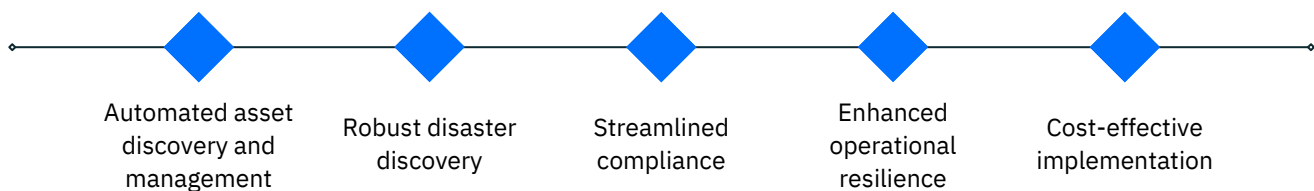
Meeting the stringent requirements of the Digital Operational Resilience Act (DORA) while ensuring business continuity.

### Solution offered:

Valiantys GRC solution, powered by **HYCU**, **Lansweeper**, and **Appfire** offers a comprehensive approach to enhancing IT resilience and efficiency. By leveraging:



This integrated solution provides a powerful framework for:



Ready to enhance your IT resilience and achieve DORA compliance?  
Schedule a demo with Valiantys today.



# Checklist: Meet NIS2 & DORA BC/DR requirements

Business continuity, backup, & testing are critical requirements needed to meet NIS2 and DORA

## Getting Started - Risk Assessment

- ◇ Create framework to identify and map all ICT services (ex. Atlassian Cloud, AWS, Salesforce, etc.)
- ◇ Leverage tools for continuous monitoring of ICTs and regularly document changes in your tech stack - across all departments
- ◇ Leverage or build auditing templates to evaluate each ICT across security, detection, response, and business continuity
- ◇ 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 Store backups offsite, outside of Atlassian in S3-compatible storage
- ◇ 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
- ◇ 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

- ◇ Leverage advanced tools for continuous monitoring and real-time reporting of backup and recovery activities, enhancing decision making and incident response capabilities
- ◇ Maintain documentation and records to demonstrate compliance with NIS2 and DORA requirements, ensuring readiness for audits and inspections

**Ready to enhance your IT resilience and achieve DORA compliance?**  
**Schedule a demo with Valiantys today.**

