WHITEPAPER

# DISASTER RECOVERY & DORA COMPLIANCE IN 2025

# EXECUTIVE **SUMMARY**

In today's increasingly digital and interconnected financial landscape, disaster recovery (DR) is more critical than ever. Financial services companies must ensure that they can quickly recover from unexpected disruptions while adhering to **regulatory standards**.

With the introduction of the Digital Operational Resilience Act (DORA), which mandates enhanced operational resilience for financial institutions, organizations must focus on both **business continuity** and regulatory compliance to **safeguard their data** and operations.

This whitepaper explores how DORA compliance intersects with disaster recovery strategies and provides actionable insights into building a robust DR framework that meets the demands of 2025.

STEFANO SORDINI
FOUNDER & CEO

# UNDERSTANDING **DISASTER RECOVERY**

Disaster recovery refers to the set of policies, tools, and procedures that ensure an organization can **quickly recover** its IT infrastructure and data in the event of a disaster. For financial services, this means protecting sensitive data, maintaining access to applications, and ensuring that **critical services remain operational**, even during catastrophic events.

## Key Components of Disaster Recovery

### Data Protection

Ensuring that all critical financial data is regularly backed up and securely stored.

### Cloud and Hybrid Solutions

Leveraging cloud-based services for scalability, reliability, and speed in disaster recovery.

### System Availability

Implementing redundant systems and infrastructure to ensure uninterrupted access to services.

### Network Continuity

Utilizing failover mechanisms to switch to backup systems if primary networks are compromised.

# INTRODUCTION TO **DORA COMPLIANCE**

The Digital Operational Resilience Act (DORA) is a European Union regulation designed to ensure that financial entities can manage and recover from operational disruptions. DORA emphasizes cybersecurity, third-party vendor management, and the establishment of comprehensive recovery processes.

## DORA Requirements

**Incident Reporting:**
Financial institutions must report severe operational incidents to regulators within a set time frame.

**Third-Party Risk Management:**
Firms must assess the resilience of third-party providers to ensure their operations do not disrupt service.

**Business Continuity:**
A detailed business continuity plan that includes disaster recovery and testing protocols.

**Resilience Testing:**
Financial entities must regularly test their systems to ensure they can maintain operations during crises.

**DORA DEADLINE**
Institutions must meet key DORA requirements by 2025. This will include updates to their risk management frameworks and DR processes.

# HOW DR STRATEGIES **MEET DORA REQUIREMENTS**

**Data Backup and Recovery:**
DORA mandates that financial entities must ensure their systems and data are resilient. A robust DR plan ensures that systems can quickly recover from an incident.

**System Redundancy:**
DORA requires firms to mitigate third-party risks. By using redundant systems and cross-regional cloud backups, companies can reduce the likelihood of single points of failure.

**Incident Reporting:**
Regular testing of DR systems ensures that when an incident occurs, it is promptly detected, mitigated, and reported in compliance with DORA.

## Case Study Example

A leading European financial institution faced significant downtime due to a cyberattack. By adopting cloud-based disaster recovery solutions, they were able to **recover key services in under four hours**. The integration of **automated failover** processes aligned perfectly with DORA's resilience testing guidelines.

# BEST PRACTICES **FOR DORA-COMPLIANT DISASTER RECOVERY**

### Real-Time Monitoring

Implement continuous monitoring to detect vulnerabilities before they cause significant disruptions.

### Frequent Backup

Perform regular data backups with a focus on ensuring that backup data can be quickly restored.

### Regular Testing

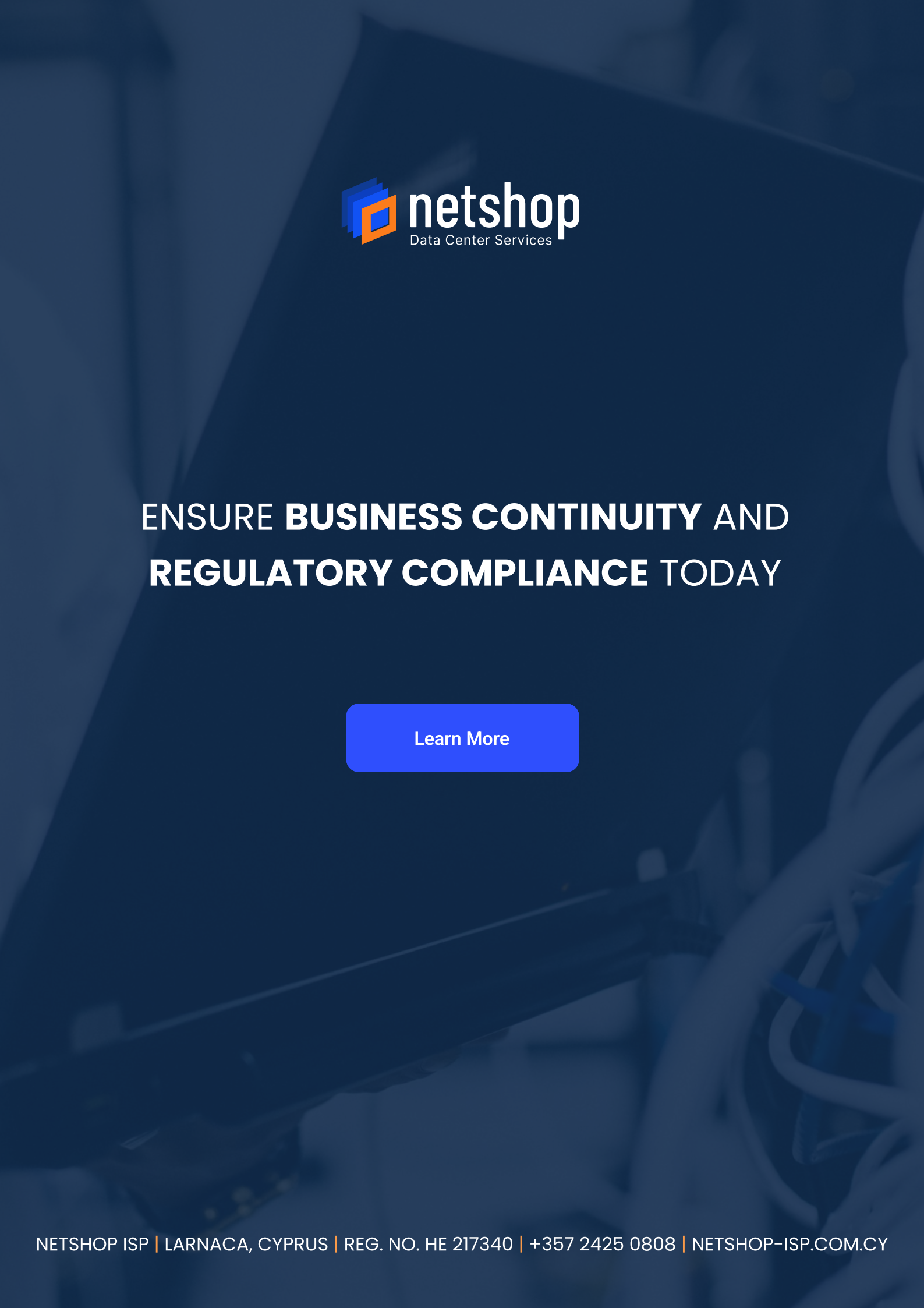
Test recovery processes at least once a year to ensure systems are resilient against various types of disruptions (natural disasters, cyberattacks, etc.).

### Third-Party Vendor Audits

Conduct thorough audits of third-party vendors to ensure they meet the necessary security and operational standards.

**Need Help with DORA Compliance?**

Contact our Specialists for a free advise!


netshop
Data Center Services
ENSURE BUSINESS CONTINUITY AND
REGULATORY COMPLIANCE TODAY
Learn More
NETSHOP ISP | LARNACA, CYPRUS | REG. NO. HE 217340 | +357 2425 0808 | NETSHOP-ISP.COM.CY