



Unveiling the Magic of

# DORA

Digital Operational Resilience Act





# Unveiling the Digital Shield

## DORA



The Digital Operational Resilience Act (DORA) is a regulation from the European Union designed to ensure the operational resilience of digital services in the financial sector.



# Why We Need DORA?



## Why DORA is Essential:

- **Cyber Threats:** Rising cyber-attacks on financial systems.
- **Operational Continuity:** Ensures financial services remain functional during disruptions.
- **Standardization:** Harmonizes ICT risk management across the EU.



# Who Must Follow DORA?


Banks  
Insurance Companies  
Investment firms  
Payment Service Providers  
Crypto-Asset Service Providers

If you're  
part of the  
EU financial  
sector, DORA  
applies to  
you!





# When DORA Applies



DORA applies continuously from its enforcement date, covering daily operations, system changes, and during any cyber security incidents.



# What Does DORA Protect?

## Information Covered

- Customer Data
- Operational Data
- ICT Systems.
- Cybersecurity Data

DORA safeguards all critical data and systems vital for financial stability.



# DORA's Specific Coverage Areas

## Coverage Areas:

- ICT Systems and Networks
- Data Management
- Cybersecurity Measures
- Third-Party Management
- Incident Response

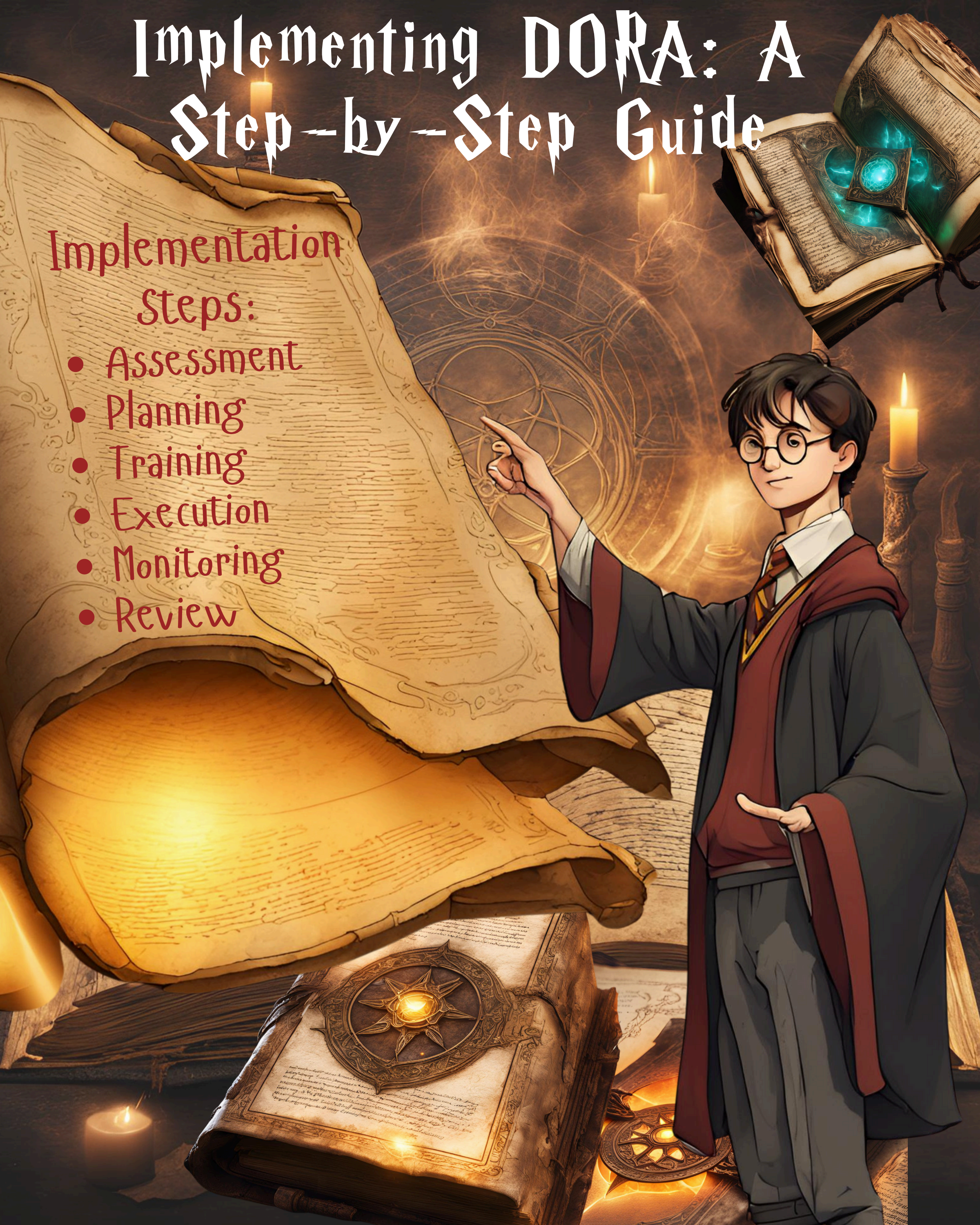
DORA covers all aspects of your digital operations, ensuring comprehensive protection and resilience.



# Implementing DORA: A Step-by-Step Guide

## Implementation Steps:

- Assessment
- Planning
- Training
- Execution
- Monitoring
- Review





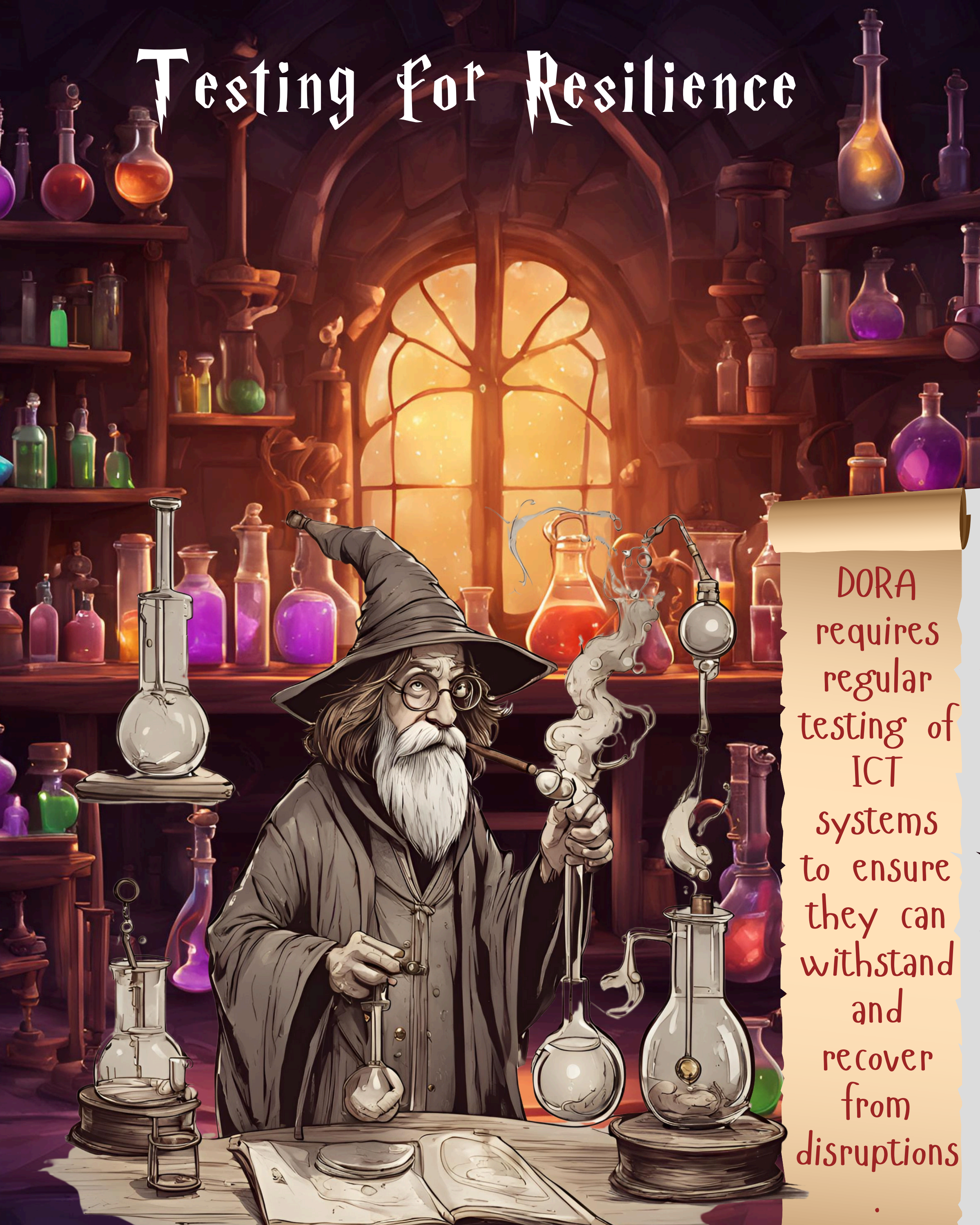


# Reporting Incidents Under DORA

DORA mandates timely reporting of major ICT-related incidents, including the nature, impact, and measures taken to resolve them.



# Testing For Resilience



DORA  
requires  
regular  
testing of  
ICT  
systems  
to ensure  
they can  
withstand  
and  
recover  
from  
disruptions



# Handling Third-Party Risks

DORA requires financial entities to ensure that their third-party service providers comply with ICT risk management and resilience standards.





# Getting Ready For DORA Compliance

## Preparation Steps:

- Assess Current Practices
- Implement Required Changes
- Train Staff
- Engage Third Parties

Preparation is the key to ensuring seamless compliance with DORA and safeguarding your organization against digital threats.



# Thank You For Joining Our Magical Journey!

For more details, guidance, and resources on DORA compliance, reach out to us.

FOLLOW US ON



## SECURITY & PRIVACY MADE EASY