

# THE KEY TO COMPLIANCE

In the next two years, financial firms and technology companies doing business in Europe are required to comply with regulations designed to safeguard the European financial ecosystem from cyberattacks and disruptions. It is crucial to understand the specific requirements relevant to your business for a seamless compliance process. The implementation of a solution such as IZBR is a great safeguard to ensure continuous resiliency and availability of critical applications.



### An All-Hazards Approach to Protection & Disaster Recovery

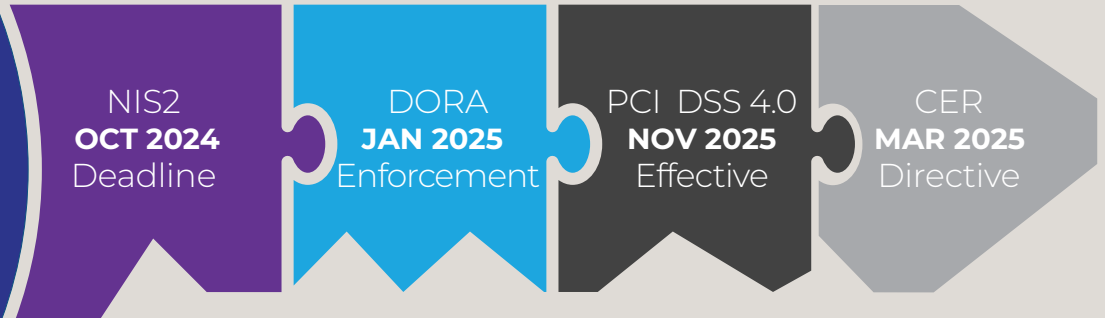
NIS2 Article 21 2.c  
Cybersecurity risk management measures

### The Right Tools and Policies in Place to Quickly & Confidently Recover

DORA Article 7  
ICT systems, protocols and procedures.

### Established Resilience Testing Procedures

DORA Article 11  
Response and Recovery



### Confidence That All Critical Data is Backed up & Protected

DORA Article 12  
Backup policies and recovery methods

### Ability To Surgically Recover Specific Data Sets in An Isolated Recovery Setting

DORA Article 12  
Backup policies and recovery methods

### An Inventory of Critical Data and Dependencies For All Applications

DORA Article 12  
Backup policies and recovery methods



21CS.com • 1.800.555.6845

Strengthen Your **Cyber Resiliency** Strategy with **IZBR**