

WHITE PAPER

DISASTER RECOVERY & DORA COMPLIANCE IN 2025

```
<standard input>:18641: warning [p 269, 7.5l]
: can't break line
  -flvar-visibility=[public|protected|private|package]
  -freplace-objc-classes
  -fzero-link -gen-decls
  -Wassign-intercept -Wno-protocol
  -Wselector
  -Wstrict-selector-match
  -Wundeclared-selector

Language Independent Options
  -fmessage-length=n
```

```
line "cmatrix -b")
ERROR: apport (pid 18449) Thu Mar 16 11:44:58
2017: debug: session gdbus call: (true,)

ERROR: apport (pid 18449) Thu Mar 16 11:44:58
2017: apport: report /var/crash/_usr_bin_cmatrix.1000.crash already exists and unseen, doing nothing to avoid disk usage DoS
ERROR: apport (pid 18485) Thu Mar 16 11:44:59
2017: called for pid 18484, signal 8, core limit 0
ERROR: apport (pid 18485) Thu Mar 16 11:44:59
2017: executable: /usr/bin/cmatrix (command line "cmatrix -b")
```

```
20 20 20 20 |5(
00000dc0 20 65 78 65 63
20 20 20 20 | exec 4-1
00000dd0 20 20 20 20
7a 31 20 2d |
00000de0 63 64 66 71 20
20 65 63 68 |cdfg
00000df0 6f 20 24 3f 20
26 2d 20 7c |n 57
00000e00 0a 20 20 20 20
20 20 20 20 |
00000e10 20 65 76 61
20 2d 20 2d |eval
```

```
R      F 0 ,      m N S v | A ,
\      # e Y s      F r B d - v ; >
pty    x b # p      4 l + B l Y U y
9      b , ? ,      [ @ V c ( ;
IO     <      0 F 6 K X X l r x w 3
3      ! 3 ) ( @ F 6 K X X l r x w 3
ro     0 b P ' L      & H D < @ q % L $ +
00     S , - / /      } " e n B " > K $
00     n      ( ? R ) % b g > Y C
00     9 d ,      > @ f M b
00     V @      v B u I A >
n      n      ( ? R ) % b g > Y C
```

```
xlllllllolloclllloolllooooodxo
Oxxxxxxxdddxddxxxxxxddkkkkkkd
Kkkk0k0000000000kkkkkkkkkkkkkkk
kk000000000000kkkkkkkkkkkkkkkkk
kk000000kkkkkkkkkkkkkkkkkkkkkkk
kkkkkkkkkkkkkkkkkkkkkkkkkkkkkkk
```

```
Screen must be at least 80 columns wide
```

```
EAFNOSUPPORT 97 Address family not supported
by protocol
ENOSR 3 Resource temporarily unavailable
EXDEV 18 Cross-device link
EREMOTE 12 Remote file system error
ENOLINK 67 Link has been severed
EPROTOTYPE 91 Protocol wrong type for socket
ENETUNREACH 113 Network unreachable
ENOTSUP 95 Operation not supported
ENFILE 23 Too many open files in system
EL2HLT 42 Hardware not synchronized
ELIB5CN 81 .lib section in a.out corrupted
EDQUOT 122 Disk quota exceeded
```

```
A: 184.7 V: 209.9 A-V:-25.123 ct:-14.229 354
```

```
netcon1@ubuntu
The key's randomart image is:
+---[DSA 1024]-----+
|====0...
|+..+ 0..
|+...0..
|+...+..
|*+...+ .5
|oBo* .-
|====0...

```

CPU [|||||||||||||||||||||||||||||||||100%] Tasks: 133
Mem [|||||||||||||||||||||||||||||631M/973M] Load average: 0.00
Swp [|||||||||||||||||432M/1022M] Uptime: 0:00

PID	USER	PRI	NI	VIRT	RES	SHR	S
55531	netcon1	39	19	23992	2568	2300	R
55705	netcon1	39	19	23992	2576	2344	R
47651	netcon1	20	0	65012	31712	2704	R
4826	netcon1	20	0	655M	25200	11900	S

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!





ENSURE **BUSINESS CONTINUITY** AND **REGULATORY COMPLIANCE** TODAY

[Learn More](#)