BULLWALL

DORA QUICK REFERENCE GUIDE

QUICK OVERVIEW OF DORA REQUIREMENTS

DORA mandates that financial entities (banks, insurers, investment firms, etc.) establish and maintain resilient ICT systems and tools that reduce the risk and impact of cyber threats.
Key pillars include:

1. ICT Risk Management
2. ICT-Related Incident Management
3. Digital Operational Resilience Testing
4. ICT Third-Party Risk
5. Information Sharing

BULLWALL'S ALIGNMENT WITH DORA PILLARS

1 ICT Risk Management (Articles 5–14)

BullWall helps by:

- **Mitigating the risk of ransomware,** which is one of the most destructive ICT threats.
- Acting as a **compensating control** for failed perimeter or endpoint defenses.
- Providing **real-time monitoring of file activity** on file shares and servers, helping organizations **identify anomalies early.**

DORA requires a defense-in-depth approach. BullWall strengthens the detection and containment layer of this stack.

2 ICT-Related Incident Management (Articles 15–20)

BullWall supports this by:

- **Automatically containing ransomware attacks within seconds.**
- Logging all events, including encryption attempts and devices/users involved.
- Sending real-time alerts to SOC/SIEM/SOAR tools, supporting **incident response plans.**

This aids in meeting DORA's requirement for early detection, effective containment, and timely response to major ICT-related incidents.

3 Digital Operational Resilience Testing (Articles 21–24)

BullWall can:

- Be included **in red team or threat-led penetration tests** (TLPT), such as **TIBER-EU.**
- Validate how effectively the organization can detect and contain ransomware scenarios during resilience testing.

DORA emphasizes simulating severe threat scenarios. BullWall supports real-world testing by triggering or containing actual encryption behavior.

4 ICT Third-Party Risk (Articles 25–39)

Indirect support:

- BullWall monitors **network shares and file servers,** which can help detect ransomware introduced through **third-party integrations.**
- Its logs and alerts can inform **supply chain attack investigations.**

5 Information Sharing (Articles 40–41)

BullWall supports this by:

- Providing detailed forensic data and logs of ransomware incidents, which can be shared with peers, regulators, or industry bodies as part of **collective threat intelligence sharing.**

SUMMARY TABLE

DORA Pillar	BullWall Contribution
ICT Risk Management	Real-time ransomware detection and containment, strengthens ICT controls
ICT Incident Management	Rapid containment, detailed logs, SOC/SIEM integration for response workflows
Operational Resilience Testing	Supports red teaming and simulation of ransomware attack scenarios
ICT Third-Party Risk	Detects threats on shared drives where third-party access may occur
Information Sharing	Provides forensic logs and attack telemetry for regulators or ISACs

FINAL TAKEAWAY

BullWall is not a complete DORA compliance platform, but it **plays a crucial role in ransomware-specific resilience.** It aligns especially well with DORA's focus on:

- Reducing impact from **disruptive cyber events**
- Ensuring **continuity of critical business services**
- Demonstrating **technical capability and preparedness** under real-world threat scenarios

ABOUT BULLWALL

BullWall is a cybersecurity solution provider with a dedicated focus on protecting data and critical IT infrastructure during active ransomware attacks. We are able to contain both known and zero-day ransomware variants in seconds, preventing both data encryption and exfiltration.

BullWall is your last line of defense for active attacks.

Learn more at www.bullwall.com.

BULLWALL

Version 2025.07