



How ThingsRecon Capabilities Support DORA Compliance

DORA requirements put a strong focus on ongoing resilience, third-party dependency transparency, and structured incident readiness.

ThingsRecon helps meet DORA requirements by:



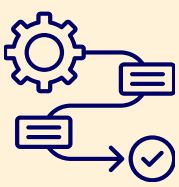
Mapping all internet-facing and third-party assets in real time



Prioritising risks based on exposure and business proximity



Providing context-rich reporting for internal and regulatory reviews



Offering non-intrusive, agentless scanning that integrates into existing workflows

DORA Requirement

ICT Asset Management

Article 8(4): Identify all information and ICT assets and map their configuration and interdependencies.

Article 8(6): Maintain inventories, update them periodically, and whenever any major changes occur.

Continuous Monitoring of ICT Risk

Article 8: Continuously identify all sources of ICT risk.

Article 9: Continuously monitor and control ICT security and functioning.

Article 10: Have mechanisms to promptly detect anomalous activities.

Third-party risk visibility

Article 28: Maintain a register of all contractual arrangements with ICT third-party service providers.

Article 30: Ensure contractual rights for monitoring, auditing, and obtaining information from providers.

Risk-Based Prioritisation

Article 18: Classification of ICT-related incidents and cyber threats.

Article 24: A risk-based approach to conducting digital operational resilience testing.

Incident Prevention & Mitigation

Article 17: Track, log, and classify ICT-related incidents. Identify, document, and address root causes to prevent recurrence. Put in place early warning indicators.

Reporting Obligations

Article 19: Reporting of major ICT-related incidents and voluntary notification of significant cyber threats.

Article 20: Standardized reporting templates.

Geographic Data Controls

Articles 28-30: Understand the location of service providers and their subcontractors.

Article 29: Assess ICT concentration risk.

What ThingsRecon Delivers

Automated Asset Discovery and Supply Chain Mapping continuously identify domains, IPs, APIs, certificates, and connections, including third-party and forgotten infrastructure.

Continuous external discovery of both your own attack surface and your connected vendors, including shadow IT and unmanaged assets, helps maintain real-time visibility into exposure to identify anomalies.

Supply chain discovery gives actionable visibility into vendor and supplier risk, with Digital Proximity scoring to understand how deeply each is integrated and what impact they could have.

Risk scoring engine with 100+ cyber hygiene indicators, including missing or misconfigured HTTP headers, weak or outdated SSL/TLS protocols, insecure forms, to support evidence-based prioritisation and mitigation efforts.

Contextual risk reports and remediation recommendations show which assets, vendors, or misconfigurations are most critical, helping you act before incidents happen.

Reporting insights that plug into GRC, SIEM, or EASM workflows to streamline documentation, support audits, and board or executive reporting.

Geo-located scanning and global points of presence help respect data residency requirements and support compliance with specific sovereignty needs.