# Versa Sovereign SASE and DORA Compliance

## Addressing EU financial sector resilience requirements with Versa Sovereign SASE

The Digital Operational Resilience Act (DORA) establishes binding requirements for how EU financial entities manage Information and Communication Technology (ICT) risk, maintain operational resilience, and oversee technology providers. Meeting these obligations requires infrastructure that supports secure operations, incident response, resilience testing, and regulatory auditability across the ICT environment. Versa Sovereign SASE delivers a complete SASE stack purpose-built for regulated organizations, keeping data, control, and management planes within EU jurisdiction while supporting managed or on-premises deployment models. For organizations subject to DORA, Versa offers a direct path to compliance without sacrificing the security capabilities or operational flexibility that modern critical infrastructure demands.

## The DORA framework

The Digital Operational Resilience Act (DORA) (Regulation (EU) 2022/2554), effective January 17, 2025, establishes a unified framework for ICT risk management and operational resilience across the EU financial sector, covering financial entities and critical ICT service providers.

DORA consolidates existing sector-specific requirements into a single regulation focused on six core areas:

- ICT risk management: Governance, risk frameworks, asset visibility, access controls, threat detection, incident response, backup and recovery, and continuous improvement
- ICT incident management and reporting: Defined processes for classifying, managing, and reporting major ICT incidents to regulators
- Operational resilience testing: Regular testing of ICT systems and processes, including Threat-Led Penetration Testing (TLPT) for significant entities
- ICT third-party risk management: Oversight of technology providers, including contractual, audit, concentration risk, and exit strategy requirements
- Information sharing: Voluntary cyber threat intelligence sharing between financial entities
- Oversight of critical ICT providers: EU-level supervisory oversight for providers designated as systemically critical

Unlike regulations focused primarily on data protection, DORA targets operational resilience directly, requiring financial entities to demonstrate secure, resilient, and auditable ICT operations across their networks, systems, and third-party technology environments.

## Versa Sovereign SASE

Against this regulatory backdrop, Versa Sovereign SASE delivers an architecture purpose-built to meet stringent operational, security, and governance requirements, providing full networking and security capabilities while keeping data, control, and operations within sovereign boundaries.

A deployment model of the VersaONE Universal SASE Platform, it addresses a key limitation of traditional cloud SASE: even with local points of presence, traffic inspection, policy decisions, and platform management may still depend on infrastructure outside the intended jurisdiction.

Versa Sovereign SASE aligns all three planes of the SASE architecture within a sovereign operating environment:

- **Control plane:** Identity validation, policy evaluation, and connection decisions occur within the designated sovereign environment.
- **Data plane:** Traffic inspection, threat protection, and content filtering are executed at local PoPs, with no traffic hairpinned outside the jurisdiction for processing.
- **Management plane:** Platform administration, logging, configuration, and operational access remain locally governed.

In the EU, Versa's Sovereign SASE-as-a-Service is available with all operations, data processing, and support governed under EU law, independent of Versa's global cloud infrastructure. For organizations requiring complete infrastructure control, Versa Sovereign SASE is also available for on-premises or private EU cloud deployment.

## DORA requirements mapped to Versa Sovereign SASE

The following table illustrates how Versa Sovereign SASE capabilities can support customer implementation of DORA operational resilience and ICT risk management requirements.

| DORA requirement | Versa Sovereign SASE capability | Outcome |
|---|---|---|
| **Chapter II - ICT Risk Management** | | |
| **Art. 5 – Governance & organization** | Management dashboard with RBAC and segregation of duties; unified policy management across all security and networking functions | Supports management body accountability for ICT risk with auditable governance controls and defined operational roles |
| **Art. 5 – Governance & organization** | VersaONE unified platform with NGFW, ZTNA, SWG, IPS, ATP; centralized audit logs and dashboards; all planes operating within sovereign boundaries | Supports implementation of a centralized ICT risk management architecture with unified visibility and policy enforcement |
| **Art. 7 – ICT systems, protocols & tools** | Secure SD-WAN with automated failover and multi-path resilience; Perfect Forward Secrecy and AES-256 encryption; geo-redundant gateways | Supports resilient ICT connectivity and secure communications through redundancy and modern cryptographic controls |
| **Art. 8 – Identification** | Automated device discovery and fingerprinting; CASB shadow IT discovery; application visibility with DPI; UEBA behavioral baselining | Identifies and classifies ICT assets, cloud dependencies, and anomalous access patterns to support asset and risk inventory |

| DORA requirement | Versa Sovereign SASE capability | Outcome |
|---|---|---|
| **Art. 9 – Protection & prevention** | ZTNA with continuous posture assessment; MFA; DLP with pre-defined patterns (PII, GDPR, PCI-DSS); GenAI Firewall; SWG; localized control plane with access decisions contained within sovereign boundaries | Enforces least-privilege access, strong authentication, and data protection controls with policy decisions governed entirely within the sovereign environment |
| **Art. 10 – Detection** | UEBA with AI-powered anomaly detection; ATP with multi-AV, AI/ML, and sandboxing; NG-IPS; DNS tunnel detection; DEM for performance anomalies; all mapped to MITRE ATT&CK | Provides continuous, real-time detection of threats and ICT anomalies with structured classification aligned to a standardized threat framework |
| **Art. 11 – Response & recovery** | SD-WAN automated failover; geo-redundant gateways with active-active HA; ATP containment actions; micro-segmentation to limit blast radius; recovery operations governed within the sovereign management plane | Supports rapid containment, response, and recovery workflows within jurisdictional boundaries |
| **Art. 12 – Backup & recovery procedures** | Configuration backup and restore; localized logging and configuration data within the sovereign management plane | Supports recovery of network and security policy state with backup assets stored within the sovereign jurisdiction |
| **Art. 13 – Learning & evolving** | UEBA and ATP post-incident MITRE ATT&CK mapping; continuous threat intelligence feed updates; centralized security reports and dashboards | Enables structured post-incident review and continuous improvement of ICT risk controls based on current threat intelligence |
| **Art. 14 – Communication** | Centralized alerting and reporting; SIEM integration via IPFIX, Syslog, and VMS | Supplies timely, structured security event data to support internal and external crisis communication processes |
| **Chapter III - ICT Incident Management & Reporting** | | |
| **Art. 17 – Incident management process** | UEBA and ATP real-time alerting with automated classification; NG-IPS and DNS security event logs; SIEM streaming via IPFIX, Syslog, NetFlow, and PCAP; per-module dashboards | Supports early warning, structured incident logging, and defined response roles to meet DORA's incident management process requirements |
| **Art. 18 – Incident classification** | DEM for operational impact quantification; ATP and UEBA severity scoring with MITRE ATT&CK mapping; per-service reporting | Provides structured severity and impact data to support classification of ICT-related incidents against DORA criteria |
| **Art. 19 – Reporting of major incidents** | Comprehensive logging via IPFIX, Syslog, NetFlow, and PCAP; SIEM integration via VMS; all log data stored and processed within the sovereign jurisdiction | Provides centralized logging for evidence collection and regulatory incident reporting workflows, while maintaining log processing within the sovereign jurisdiction |

| DORA requirement | Versa Sovereign SASE capability | Outcome |
|---|---|---|
| **Chapter IV – Digital Operational Resilience Testing** | | |
| **Art. 24–25 – Digital operational resilience testing** | ZTNA network segmentation for controlled test environments; RBAC to isolate testing from production; MITRE ATT&CK mapping for test scoping; ATP and IPS baseline data for vulnerability assessments | Enables structured resilience and vulnerability testing with controlled blast radius and documented configuration history for gap analysis |
| **Art. 26 – Threat-Led Penetration Testing (TLPT)** | MITRE ATT&CK-aligned threat intelligence for test scoping; ZTNA micro-segmentation for isolated test environments; TLPT telemetry and results remain within the sovereign boundary | Supports TLPT activities by enabling isolated test environments and localized telemetry handling within sovereign deployment models |
| **Chapter V – ICT Third-Party Risk Management** | | |
| **Art. 28 – Third-party risk management** | CASB shadow IT discovery; SSPM and CSPM posture monitoring; API-based data protection across IaaS and SaaS; Sovereign SASE-as-a-Service operating within EU jurisdiction | Surfaces and monitors third-party ICT dependencies while supporting EU-governed contractual and operational arrangements for critical networking and security services |
| **Art. 29 – ICT concentration risk** | CASB, CSPM, and SSPM visibility across the cloud service landscape; Sovereign SASE architecture operating independently of Versa's global shared infrastructure | Provides operational transparency, sovereign deployment options, and reduced dependency on globally shared infrastructure |
| **Art. 30 – Key contractual provisions** | Sovereign SASE-as-a-Service with EU-governed operations, localized data processing, and support; RBAC and audit trail supporting audit rights provisions; local control/management plane with verifiable operational access controls | Supports DORA contractual and oversight requirements through EU-governed operations, localized processing, audit logging, and operational access controls |
| **Art. 31–44 – Critical ICT provider oversight** | Sovereign SASE contracted through EU legal entity with localized operations; logging and audit trail supporting regulatory information requests; EU-governed support and operational contacts | Provides documented evidence of operating model that supports regulatory assessments and oversight engagements |
| **Chapter VI – Information Sharing** | | |
| **Art. 45 – Information sharing** | Threat intelligence feeds (file reputation, DNS, ATP); SIEM streaming via IPFIX, Syslog, and VMS; MITRE ATT&CK alignment for standardized threat exchange; threat telemetry retained within the sovereign jurisdiction | Enables participation in sector threat-sharing arrangements while minimizing cross-border telemetry transfers |

# Why DORA-regulated organizations choose Versa

DORA compliance requires infrastructure that can demonstrate operational control, resilience, and auditability across the networking and security stack. As the first-to-market vendor for Sovereign SASE, Versa delivers a deployment model purpose-built for regulated organizations that need operational independence and sovereign control.

Key reasons financial entities choose Versa Sovereign SASE for DORA compliance:

- Full-stack sovereignty: Data, control, and management planes remain within EU-hosted and controlled infrastructure
- Complete SASE capabilities: Integrated ZTNA, NGFW, SWG, CASB, DLP, IPS, ATP, and SD-WAN within sovereign environments
- Auditable governance: Logging, RBAC, and SIEM integration support regulatory reporting and third-party oversight
- Flexible deployment: Available as a managed service, on-premises deployment, or private EU cloud deployment

Request a demo to see Versa Sovereign SASE in action.

Explore Versa Sovereign SASE.

Versa Networks, Inc
2550 Great America Way, Suite 350
Santa Clara, CA 95054
Tel: +1 408.385.7660
Email: info@versa-networks.com
www.versa-networks.com

**About Versa**
Versa, a global leader in SASE, enables organizations to create self-protecting networks that radically simplify and automate their network and security infrastructure. Powered by AI, the VersaONE Universal SASE platform delivers converged SSE, SD-WAN, and SD-LAN solutions that protect data and defend against cyberthreats while delivering a superior digital experience. Thousands of customers globally, with hundreds of thousands of sites and millions of users trust Versa with their mission critical networks and security.



Part# SB_SOV-SASE-DORA-CMP-01.0