AKAMAI BRIEF

DORA Compliance: Pillar-by-Pillar

With the Digital Operational Resilience Act (DORA) now enforceable, financial entities and ICT (information and communications technology) third-party service providers operating in the EU are playing by a new rulebook. The new requirements may already be in effect, but their breadth and complexity mean that many financial institutions will continue working towards full DORA compliance over the coming months and years.

Key DORA compliance considerations

This article outlines key considerations to support DORA compliance. While not exhaustive, this is intended as an aid to highlight actions that may help financial entities move closer to compliance.

Working towards DORA compliance can help organisations better mitigate risk, secure critical data, become more resilient against evolving threats, and benefit from increased visibility of networks, systems, and processes.

While the path to DORA compliance may be complex and costly, it also offers an opportunity to create a unified, comprehensive security framework that may help an organisation be set up for future success.

Action	Why it's important	Solutions
PILLAR 1: ICT risk management		
Restrict lateral movement by workload.	Contains incidents, protects critical data flows, and minimises downtime and potential business impact.	Microsegmentation with workload-specific policies, east-west traffic inspection via internal firewalls, identity-based access control (IBAC), Zero Trust Network Access (ZTNA), software-defined networking (SDN), privileged access management (PAM), endpoint detection and response (EDR)
Limit user access to necessary applications based on role and identity.	Provides a targeted and methodical approach for protecting critical assets by controlling who can access what. Prevents unauthorised access and gives you granular control over users and system access.	Role-based access control (RBAC), identity and access management (IAM), Zero Trust Network Access (ZTNA), single sign-on (SSO), multi-factor authentication (MFA), and privileged access management (PAM)
Remove ID and password access, replacing it with MFA.	Protects against compromised credentials.	Multi-factor authentication, single sign-on (SSO), passwordless authentication (e.g., biometrics, FIDO2 keys), conditional access policies requiring MFA, privileged access management (PAM) with MFA for elevated access, and mobile push or hardware token-based MFA solutions

Action	Why it's important	Solutions
Ensure visibility into all ICT assets, from servers and networks to applications.	Effective risk management begins with the ability to identify and control specific vulnerabilities across all assets at any point in time. Monitoring and visibility are key.	Configuration management database (CMDB), IT asset management (ITAM), security information and event management (SIEM), network detection and response (NDR), endpoint detection and response (EDR), application performance monitoring (APM), cloud security posture management (CSPM), application security posture management (ASPM), and data security posture management (DSPM)
Secure data transmission.	Sensitive data, including personally identifiable information (PII), financial records, and transactional data, needs to be handled confidentially.	Strong encryption protocols, VPNs, TLS, Secure File Transfer Protocols, endpoint encryption, PKI, and others
PILLAR 2: ICT-related incident management and reporting		
Segment boundaries.	Speeds up detection, response, and recovery processes by quickly containing and isolating incidents.	Microsegmentation, network segmentation, next-gen firewalls, access control lists (ACLs), software-defined networking (SDN), Zero Trust Network Access
Create the ability to isolate compromised segments without disrupting broader operations.	Ensures rapid response to incidents.	Microsegmentation, software-defined networking (SDN), endpoint detection and response (EDR), network access control (NAC), Zero Trust Network Access (ZTNA), virtual LANs (VLANs)
Restrict access to sensitive information and critical applications.	Reduces the likelihood of a threat.	Role-based access control (RBAC), multi-factor authentication (MFA), Zero Trust Network Access (ZTNA), identity and access management (IAM), privileged access management (PAM), network and microsegmentation
Employ real-time threat detection and response.	A quick response to ICT incidents is essential for limiting their impact. Detailed threat intelligence and logging information may also be helpful for reporting.	Security information and event management (SIEM), endpoint detection and response (EDR), extended detection and response (XDR), intrusion detection and prevention systems (IDPS), threat intelligence integration and feeds, security orchestration, automation, and response (SOAR), behavioural analytics and anomaly detection, deception, and threat hunting services

Action	Why it's important	Solutions
Consider putting in place advanced threat hunting with remediation.	Proactively detects risks.	Threat hunting services and managed security service providers (MSSPs)
PILLAR 3: Digital operational resilience testing		
Simulate failure within segmented parts of the network.	Provides a real-time view of operational resilience.	Integration with a modelling tool to show full path resilience and enforcement points Chaos engineering tools, network simulation and sandbox environments, software-defined networking (SDN), red/blue team exercises, disaster recovery and failover testing, security lab environments
Run stress tests and attack simulations on a regular basis.	Highlights deficiencies in networks, applications, and critical systems. Allows you to make necessary adjustments quickly and build adaptive response strategies, strengthening your ability to mitigate threats as they evolve.	Ransomware playbook and tabletop exercises for red, blue, and purple teams Regular pen testing, breach and attack simulation, vulnerability scanning tools and posture assessments, DDoS simulation, automated attack simulation
Use ZTNA and MFA for resilience testing.	By maintaining strict access policies during simulated incidents or disruptions, you get a true picture of your security status.	Zero Trust Network Access (ZTNA), multi-factor authentication (MFA), identity and access management (IAM), security information and event management (SIEM), microsegmentation
Control access to key applications and resources under stress.	Enhances the reliability and readiness of your defences.	Zero Trust Network Access (ZTNA), multi-factor authentication (MFA), role-based access control (RBAC), privileged access management (PAM), identity and access management (IAM), network and microsegmentation, load balancers, and web application and API protection (WAAP)
Test preparedness for a distributed denial-of-service (DDoS) attack.	Helps pinpoint vulnerabilities and optimise resilience strategies.	DDoS simulation and testing, Cloud-based DDoS protection, web application firewalls (WAF), traffic scrubbing centres, network behaviour analytics and anomaly detection tools, incident response playbooks and tabletop exercises, and red team exercises

Action	Why it's important	Solutions
PILLAR 4: Management of third-party risk		
Segment environments where third-party vendors or applications interact.	Speeds up detection, response, and recovery processes by quickly containing and isolating incidents.	Microsegmentation with identity-based policies, virtual LANs (VLANs), demilitarised zones (DMZs), firewall with granular access controls, Zero Trust Network Access (ZTNA), network access control (NAC), dedicated VPN gateways
Secure internet access for all external communications.	Ensures that third parties only connect through secured, controlled pathways.	Secure web gateways (SWG), cloud access security brokers (CASB), DNS security, next-generation firewalls with URL filtering (NGFWs), encrypted communications (e.g., HTTPS, TLS 1.2/1.3), email security gateways with encryption, Zero Trust Network Access (ZTNA)
Enable real-time continuous monitoring of third-party access.	Immediately detects and safeguards against risks coming from ICT providers or their external vendors.	Microsegmentation, analytics portal, and custom WAAP rules Security information and event management (SIEM), identity and access management (IAM), privileged access management (PAM), user and entity behaviour analytics (UEBA), Zero Trust Network Access (ZTNA), network access control (NAC), and endpoint detection and response (EDR)
PILLAR 5: Information sharing		
Segment sensitive data and restrict access to authorised users only.	Reduces the likelihood of a threat.	Data classification and labelling, microsegmentation with data-centric policies, role-based access control (RBAC), identity and access management (IAM), data loss prevention (DLP), and privileged access management (PAM)
Ensure that both internal and external information sharing happens via secure channels.	Reduces the risk of sensitive data being compromised.	End-to-end encryption (e.g., TLS 1.2/1.3, S/MIME), Secure File Transfer Protocols (e.g., SFTP, FTPS), encrypted email solutions, virtual private networks (VPNs), secure web gateways (SWG), and data loss prevention (DLP)

Action	Why it's important	Solutions
Enable secure access to communication platforms.	Reduces the risk of sensitive data being compromised.	Multi-factor authentication (MFA), identity and access management (IAM), single sign-on (SSO), Zero Trust Network Access (ZTNA), endpoint security controls, encrypted communication platforms, and secure web gateways (SWG)
Enforce identity verification.	Strengthens trust in the information-sharing process while protecting data integrity.	Multi-factor authentication (MFA), identity and access management (IAM), single sign-on (SSO), privileged access management (PAM), biometric authentication (e.g., fingerprint, facial recognition), digital certificates and public key infrastructure (PKI), and directory services (e.g., Active Directory, Microsoft Entra ID)
Securely share data across borders with others in the financial community on emerging threats, vulnerabilities, and attack patterns.	Spreads threat intelligence across different geographies, creating rapid responses and collective defence strategies.	Threat intelligence platforms, encrypted communication channels (e.g., TLS, S/MIME, VPN), information sharing and events (e.g., FS-ISAC), data classification and access controls, Secure File Transfer Protocols (e.g., SFTP, FTPS), cross-border data sharing policies

Notice: *The information provided here is for general informational purposes only. It should not be construed as legal advice and does not create any commitments from Akamai. Laws and regulations can vary, and legal interpretations may change over time. No guarantees are made regarding the accuracy, completeness, or suitability of the information provided. If you require legal advice or have specific legal concerns, please consult with a qualified legal professional who can provide advice tailored to your situation and jurisdiction.*


| Published 05/25