DigiCert Group

Compliance with EU DORA

DigiCert ONE solutions for reliability and security

digicert®

January 2025

WHITEPAPER

digicert

Compliance with EU DORA

DigiCert ONE solutions for reliability and security

Summary

Financial services may be the most regulated industry of all. From security standards for payments systems to anti-money laundering requirements, there are plenty of reasons why financial services need mature risk management programs. The Digital Operational Resilience Act (DORA) in the European Union aims to rationalise information and communication technology risk management across the financial system. It outlines a risk management framework - complete with oversight, incident reporting obligations, and information sharing. The EU adopted DORA in December 2022 with the full weight of the regulation going into effect from January 17, 2025.

Scope

DORA applies to a huge swath of the financial industry. The full list of affected company types is in Article 2 paragraph 1 of the legislation. It applies to nontraditional financial firms like those dealing with crypto currency and third-party providers of information and communication technology (ICT) services. However, many of the requirements relate to practices that firms may already be doing for existing compliance obligations or their own governance.

A general outline of the DORA regulation can be found in Chapter I, Article 1:

- Have in place an internal governance and control framework for ICT risk management
- Report major ICT-related incidents and voluntary notification of significant cyber threats to authorities
- Report major operational or security payment-related incidents to the competent authorities, whether ICT-related or not
- Broadly test security practices and controls
- Share information in relation to cyber threats and vulnerabilities
- Manage third-party risk associated with ICT providers

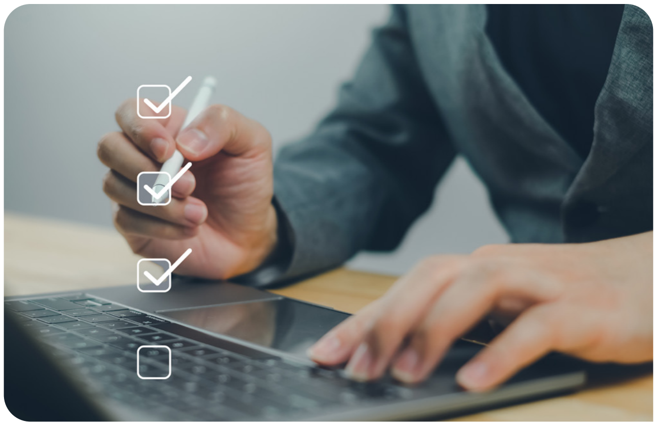
Impact

Of course, with added oversight and potential fines for non-compliance, DORA adds to the risk equation. For example, Article 1 paragraph 1 includes a requirement that entities report “major operational or security payment-related incidents to the competent authorities”. Lapses that organisations could silently recover from now must be reported and could result in fines. This also means that risks an organisation previously deemed acceptable may now be a gap that needs to be immediately addressed.

Next steps

If your organisation has not already adopted a risk management framework like ISO 27001 or NIST 800-53 it is beyond time to get started. For those with a framework in place, do a gap assessment to identify any deficiencies between your current practices and those required under DORA. Create a plan to close those gaps and start executing it. Be sure to document your process so you have evidence of your plan and your progress.

Risks that a business unit previously accepted could now be unacceptable simply because of the disclosure requirement. Prioritise legacy systems and other chronic sources of high administrator effort, instability, and vulnerabilities for review and upgrades.



DigiCert solutions

DigiCert partners with leading financial institutions around the world to enhance the security and availability of their essential systems. The DigiCert ONE platform with DigiCert's expertise in public key infrastructure and certificate lifecycle management helps to:

- Eliminate outages caused by expired certificates
- Improve ability to remediate security issues related to digital certificates
- Automate identities across users, devices and machines to strengthen authentication and secure communication
- Manage vulnerabilities in the software your organisation develops
- Protect authenticity and integrity of software and documents

Articles 1-3, outages and other incidents

Articles 1-3 of the DORA include requirements for notifying authorities of security incidents and outages impacting ICT and payment systems. Note that a failure affecting the latter may not impact the former. Article 3 contains the definitions of these incidents:

- (8) 'ICT-related incident' means a single event or a series of linked events unplanned by the financial entity that compromises the security of the network and information systems, and have an adverse impact on the availability, authenticity, integrity or confidentiality of data, or on the services provided by the financial entity
- (9) 'operational or security payment-related incident' means a single event or a series of linked events unplanned by the financial entities referred to in Article 2(1), points (a) to (d), whether ICT-related or not, that has an adverse impact on the availability, authenticity, integrity or confidentiality of payment-related data, or on the payment-related services provided by the financial entity

With DigiCert Trust Lifecycle Manager, organisations can build a complete inventory of their digital certificates and use automation, alerting & reporting to get ahead of outages and security incidents caused by expired certificates, certificate revocations, and other emergency changes.

Article 9, Protection and prevention

Article 9, Protection and prevention, includes high level guidance for the confidentiality, integrity, authenticity and availability of data – in use, at rest, and in transit. Financial institutions of all sizes use public key infrastructures (PKI) to support strong authentication of users and machines and facilitate encrypting communications among them.

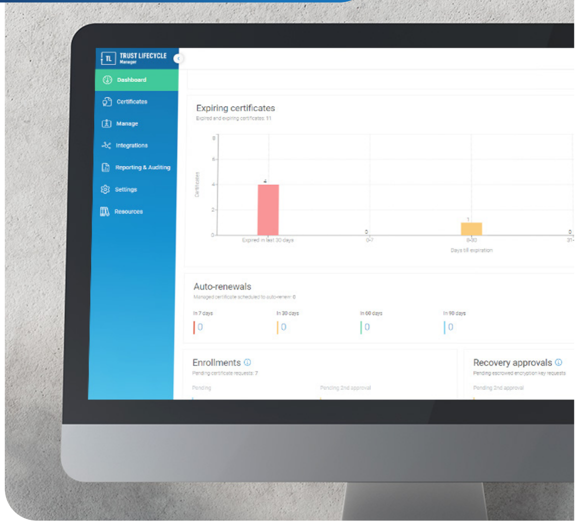
DigiCert Trust Lifecycle Manager combines PKI as-a-Service, agnostic certificate lifecycle management, and robust integrations to support secure identities and workloads across users, clouds, and on-premises infrastructure.

Article 11, response and recovery

Also related to PKI is the need to respond quickly to compromised certificates, certificate revocation incidents, and the rare but disruptive distrust of a public certificate authority.

The centralised inventory and automation capabilities of DigiCert Trust Lifecycle Manager empower organisations to swiftly isolate, contain, and remediate these issues while eliminating much of the manual effort typically required to resolve them.

DigiCert Trust Lifecycle Manager combines PKI as-a-Service, agnostic certificate lifecycle management, and robust integrations to support secure identities and workloads



Expiring certificates
Expired and expiring certificates: 11

Auto-renewals
Managed certificate scheduled to auto-renew: 0

In 7 days 0
In 30 days 0
In 60 days 0
In 90 days 0

Enrollments
Pending certificate requests: 7
Pending
Pending 2nd approval

Recovery approvals
Pending escrowed encryption key requests
Pending 2nd approval

Article 25, vulnerability management and security testing

One of the most expansive sections of the DORA is Article 25, Paragraph 1. It specifies categories of tests for ICT tools and systems.

> …appropriate tests, such as vulnerability assessments and scans, open source analyses, network security assessments, gap analyses, physical security reviews, questionnaires and scanning software solutions, source code reviews where feasible, scenario-based tests, compatibility testing, performance testing, end-to-end testing and penetration testing.

Fulfilling these categories of tests spans an entire security program, bridging the physical and digital realms. An interesting callout are the references to software scanning and source code reviews. Software development lifecycles and software supply chains are increasingly subject to industry and regulatory requirements, and the necessary controls extend beyond traditional Application Security Testing tools.

DigiCert Software Trust Manager combines enterprise code signing with multiple software scanning techniques to govern code signing processes and check software packages for malicious or vulnerable components. It includes code signing key and certificate management, software composition analysis, software bill of materials, and threat scanning into a policy-based approach. Software Trust Manager is easily integrated into software development processes and automated CI/CD environments to proactively manage risk of software supply chain incidents.

Tools, methods, processes, and policies

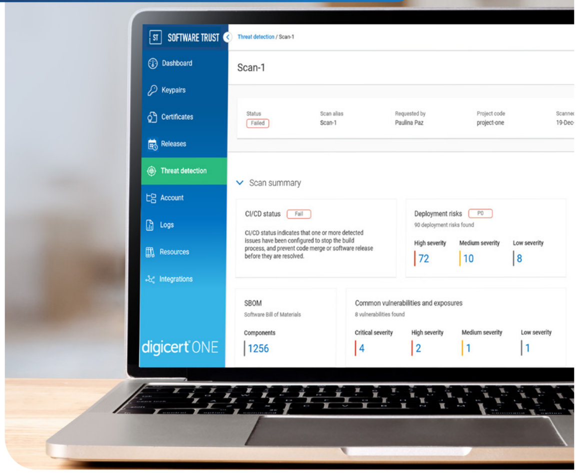
The EU published supplemental information regarding the technical and other controls necessary for compliance with the DORA.

Encryption and cryptography

Using encryption to secure data at rest, in transit, and in use is common, if not expected practice, across the financial industry. An encryption system is only as strong as the management of the associated cryptographic keys. In this way, Articles 6 and 7 of the technical standards combine to require the application of encryption, lifecycle management of keys, and all associated policies.

Trust Lifecycle Manager allows organisations to centrally enforce policies to govern digital certificates across the enterprise including certificate issuance, renewal, and revocation. Importantly, it does not impede de-centralised ownership and use of certificates by different business units. What's more, Software Trust Manager, another solution in the DigiCert ONE platform, can augment Trust Lifecycle Manager with code signing key management and access control capabilities purpose-built for software development environments.

DigiCert Software Trust Manager combines enterprise code signing with multiple software scanning techniques to govern code signing processes and check software packages for malicious or vulnerable components.



Threat detection / Scan-1

Scan-1

Status: Failed
Scan alias: Scan-1
Requested by: Paulina Paz
Project code: project-one
Scanned: 19-Dec

Scan summary

CI/CD status: Fail
CI/CD status indicates that one or more detected issues have been configured to stop the build process, and prevent code merge or software release before they are resolved.

Deployment risks: P0
90 deployment risks found

High severity	Medium severity	Low severity
72	10	8

SBOM
Software Bill of Materials
Components: 1256

Common vulnerabilities and exposures
8 vulnerabilities found

Critical severity	High severity	Medium severity	Low severity
4	2	1	1

Vulnerability and patch management

Regulatory requirements are expanding the scope of vulnerability management programs to include the software development lifecycle, with DORA one of the recent examples. Article 10, paragraph 2(d) requires organisations to:

- Track the usage of:
  - Third-party libraries, including open-source libraries, used by ICT services supporting critical or important functions;
  - ICT services developed by the financial entity itself or specifically customised or developed for the financial entity by an ICT third-party service provider;

The need to track the usage of third-party software components with the other patch management and vulnerability disclosure requirements in this section can be addressed with Software Bills of Material (SBOMs), Software Composition Analysis (SCA) and scanning final software builds for malware and known vulnerabilities that may have been introduced by accident or by malice.

Software Trust Manager combines enterprise code signing and software security scans with signing certificate and key management to create a policy-driven approach to securely developing and releasing software. Integrating Software Trust Manager into your software development lifecycle (SDLC) and continuous integration/continuous deployment (CI/CD) pipelines provides an automated way to govern code signing and routinely evaluate vulnerabilities in software releases.

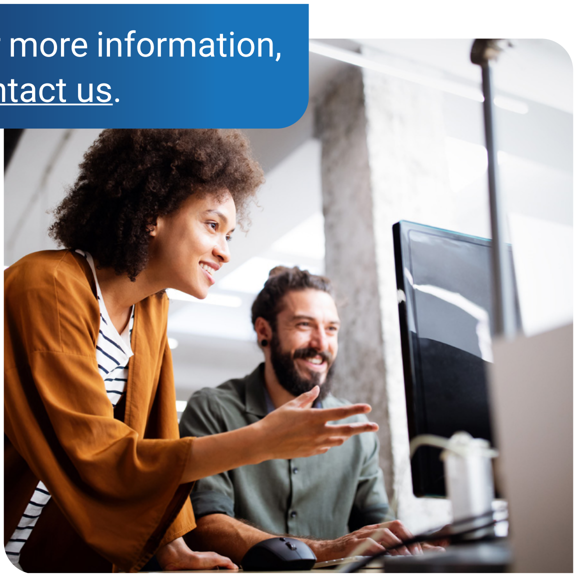
Conclusion

The DORA mandates a comprehensive approach to cybersecurity and operational resilience across financial systems. This includes requirements to put in place risk management frameworks, prevention and detection controls, report incidents, and regular tests of security measures.

By leveraging DigiCert's solutions to modernise public key infrastructures, financial institutions can:

- Enhance Security: Implement strong authentication and encryption to protect sensitive data.
- Improve Resilience: Manage and quickly respond to risks associated with cyberattacks and operational disruptions.
- Streamline Operations: Automate certificate management and software security processes.
- Ensure Compliance: Track adherence to DORA's regulatory requirements through audit logs.

For more information, contact us.



Technical standards and DigiCert capabilities matrix

Regulatory technical standard	
Article 6 Encryption and cryptographic controls	
1. As part of their ICT security policies, procedures, protocols, and tools referred to in Article 9(2) of Regulation (EU) 2022/2554, financial entities shall develop, document, and implement a policy on encryption and cryptographic controls.	Trust Lifecycle Manager enables centralised monitoring and enforcement of encryption policies related to digital certificates used to identifying users and machines, encrypting data in transit, and generating digital signatures.
Article 7 Cryptographic key management	
2. Financial entities shall identify and implement controls to protect cryptographic keys through their whole lifecycle against loss, unauthorised access, disclosure, and modification.	The DigiCert ONE employs Hardware Security Modules for private and secret key storage. Software Trust Manager, for example, includes a cloud-based HSM for securely storing private code signing keys.
3. Financial entities shall develop and implement methods to replace the cryptographic keys in the case of loss, or where those keys are compromised or damaged.	Trust Lifecycle Manager and Software Trust Manager provides automated, bulk, and individual replacement of certificates and associated keypairs based on time interval, compromise or other logic.
4. Financial entities shall create and maintain a register for all certificates and certificate-storing devices for at least ICT assets supporting critical or important functions. Financial entities shall keep that register up to date.	Trust Lifecycle Manager provides continuous inventory of all digital certificates in your enterprise, regardless of the issuing Certificate Authority. It uses a variety of methods including direct integration with vulnerability management platforms and third party CAs.
5. Financial entities shall ensure the prompt renewal of certificates in advance of their expiration.	The DigiCert ONE platform automates certificate lifecycle management across a variety of use cases including enterprise infrastructure, software code signing, connected devices, user authentication, and document signing.
Article 10 Vulnerability and patch management	
1. As part of the ICT security policies, procedures, protocols, and tools referred to in Article 9(2) of Regulation (EU) 2022/2554, financial entities shall develop, document, and implement vulnerability management procedures.	Software Trust Manager provides two kinds of analysis to identify potential issues in the software your organisation creates: Software Composition Analysis to identify open-source and third-party software and to check for known vulnerabilities. Static analysis on binaries to identify vulnerabilities, potential malware and exposed secrets. Both processes create a Software Bill of Materials (SBOMs) that can be compared to ensure no extra components were inserted in the SDLC process.
2. (A) identify and update relevant and trustworthy information resources to build and maintain awareness about vulnerabilities;	DigiCert has partners who actively maintain vulnerability and malware databases that we use for software threat scanning and notification of new vulnerabilities.

Technical standards and DigiCert capabilities matrix (continued...)

2 (d) track the usage of: (i) third-party libraries, including open-source libraries, used by ICT services supporting critical or important functions; (ii) ICT services developed by the financial entity itself or specifically customised or developed for the financial entity by an ICT third-party service provider;	Software Trust Manager generates a Software Bill of Material (SBOM) to identify the components your software contains or references. The same scanning process also detects known vulnerabilities and potentially malicious code as part of a vulnerability management program for the software your organisation develops.
2 (e) establish procedures for the responsible disclosure of vulnerabilities to clients, counterparties, and to the public;	Software Trust Manager generates SBOMs that you can sign and publish with each release to aid vulnerability management and disclosure.
Article 12 Logging	
2(c)(iii) the requirement to log events related to all of the following: change management;	DigiCert ONE, which includes Trust Lifecycle Manager and Software Trust Manager, provides granular logging and alerting of events like certificate renewal, key rotation, software signing, and other security and administrative activities.
Article 13 Network security management	
(d) the identification and implementation of network access controls to prevent and detect connections to the financial entity's network by any unauthorised device or system, or any endpoint not meeting the financial entity's security requirements;	Trust Lifecycle Manager is tightly integrated with endpoint management technologies like Microsoft InTune and infrastructure management solutions like Terraform to automate management certificates used to authenticate users and machines to enterprise networks.
(e) the encryption of network connections passing over corporate networks, public networks, domestic networks, third-party networks, and wireless networks, for communication protocols used, taking into account the results of the approved data classification, the results of the ICT risk assessment and the encryption of network connections referred to in Article 6(2);	The discovery capabilities of Trust Lifecycle Manager ensure your network endpoints have valid certificates necessary to facilitate encrypted communications (TLS).