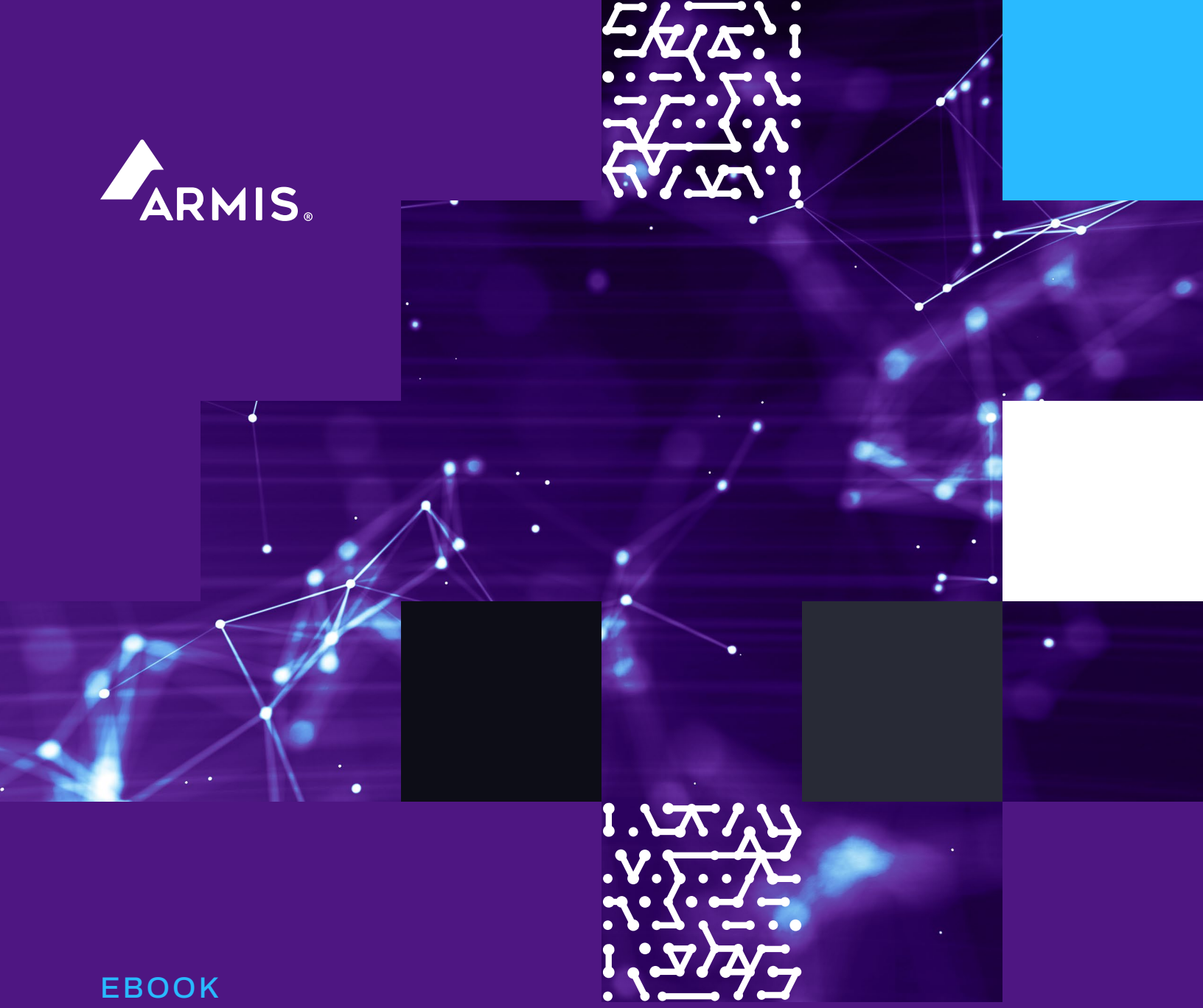


EBOOK

Strengthening Cybersecurity and Operational Resilience in the Financial Sector

Adhering to the Digital Operational Resilience Act (DORA) Framework with Armis

© Copyright Armis 2025

Table of Contents

© Copyright Armis 2025

Foreword

This ebook serves as a technical guide, outlining how Armis empowers financial organizations to map their cybersecurity initiatives to the requirements outlined by DORA. Through an examination of the act's regulatory articles and corresponding Armis capabilities, this ebook delineates a framework that facilitates seamless alignment between regulatory compliance and cybersecurity practices.

Introduction

Recent years have witnessed a string of high-profile outages and business disruptions at European banks, underscoring the significant threat posed by the lack of resilience within the industry. In response to these challenges and with the aim of bolstering the stability, security, and competitiveness of the European financial sector, the European Council has taken decisive action. This has involved consolidating existing national regulations to create more robust operational resilience across the financial services sector.

88%

of CISOs believe DORA will enhance resilience.

43%

of UK financial institutions would not meet the initial DORA deadline.

https://www.orangecyberdefense.com/uk/insights/dora-43-of-uk-financial-services-unprepared-for-eu-regulation-censuswide-survey-finds

The culmination of these efforts is the Digital Operational Resilience Act (DORA), a comprehensive framework designed to manage Information and Communication Technology (ICT) risk for European financial institutions. With provisions encompassing cybersecurity, incident response, outsourcing, and data governance, DORA mandates a multifaceted approach to safeguarding critical infrastructure and customer data against cyber threats and operational disruptions. As financial organizations strive to align their cybersecurity strategies with these requirements, they need advanced technological solutions that offer a holistic, proactive approach to security measures.

© Copyright Armis 2025

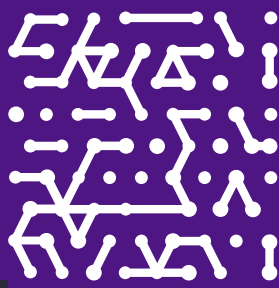
Bridge the Gap Between DORA's Theoretical Framework and Practical Application

Breaking down and understanding the articles that make up DORA is paramount for those tasked with safeguarding digital operations within their organizations. The regulation is structured around five essential pillars that address protecting the digital operational landscape in a holistic way. These pillars are foundational components that require meticulous integration into digital operational risk management frameworks.

In the following sections, we will dissect each pillar, offering insights into the objectives and implications of each. Moreover, we aim to bridge the gap between DORA's theoretical framework and practical application by showcasing how Armis' innovative platform can be leveraged to achieve and maintain compliance. This ebook serves as a roadmap that highlights Armis capabilities to technical professionals navigating the complexities of DORA. When put into action, it offers real world guidance to ensure that your infrastructure is not only compliant with DORA but also robust enough to thrive in the face of growing cyber threats.

The Five Pillars of the DORA Framework

The DORA framework is structured around five foundational pillars, each designed to address the diverse aspects of digital operational resilience in the financial sector. These pillars provide a comprehensive blueprint for organizations to meet the regulatory requirements. Below is an overview of each pillar and its significance. It's worth mentioning at this point that the DORA framework is vast and varied. While Armis can and should be considered an MVP on the team, adhering to DORA must include people processes and additional support.



© Copyright Armis 2025

1

Identification and Classification of ICT (Information and Communication Technology) Risk:

This pillar emphasizes the importance of identifying, classifying, and managing the various ICT risks that could potentially disrupt digital operations. It encourages organizations to continuously monitor and assess their digital landscapes to identify vulnerabilities and threats.

2

Incident Reporting and Management:

A critical component of the DORA framework, this pillar focuses on the establishment of robust processes for the timely detection, reporting, and management of ICT-related incidents. It mandates that organizations maintain an efficient incident response mechanism to minimize impact and restore operations swiftly.

3

Digital Operational Resilience Testing:

To ensure that digital systems and processes are resilient to disruptions, this pillar mandates regular testing of the resilience of ICT systems. It includes vulnerability assessments, penetration testing, and scenario-based testing to evaluate the effectiveness of digital defenses.

4

ICT Third-Party Risk Management:

Acknowledging the interconnected nature of digital operations, this pillar highlights the need for comprehensive oversight and management of third-party service providers. It mandates that organizations establish and enforce strict third-party risk management policies to safeguard against vulnerabilities and potential security gaps introduced through external partnerships.

5

Information and Intelligence Sharing:

Recognizing the collective benefit of shared intelligence, this pillar encourages organizations to participate in information-sharing platforms. Sharing insights about threats, vulnerabilities, and incidents can bolster the collective digital resilience of the financial sector by fostering a collaborative approach to cyber defense.

© Copyright Armis 2025

These pillars collectively provide a strategic framework for organizations to manage and mitigate ICT risk. By adhering to these principles, entities within the financial sector can fortify their operational infrastructure, ensuring continuity and integrity in the face of digital challenges.

Consequence of non-compliance: 2%

Entities violating the act may incur fines up to 2% of their average daily global turnover from the previous year, applied daily until compliance is achieved.

The Imperative of Compliance

Let's take a moment to look at Article 50 in the DORA framework- an in depth outline of disciplinary measures for entities that fail to meet its requirements. These measures include immediate cessation of non-compliant activities, orders to stop practices that violate the regulations, the execution of remedial actions to ensure adherence, and the mandate to allow inspection of telecommunication data for investigative purposes.

Moreover, DORA necessitates the publication of public notices identifying entities that do not comply and detailing their regulatory breaches. It is critical for essential Information and Communications Technology (ICT) third-party service providers, utilized by financial institutions, to align with DORA's stringent regulations. Failure to comply incurs periodic penalty payments enforced by the Lead Overseer, amounting to 1% of the provider's average daily global turnover from the previous year, accumulating daily until compliance is achieved, up to a maximum of six months.

To cultivate a culture of transparency and accountability in the financial sector, competent authorities are required to publicly disclose any decisions related to administrative penalties on their official digital channels. This approach ensures that the financial ecosystem operates within a framework of trust and integrity, highlighting the vital importance of operational resilience in the digital era.

© Copyright Armis 2025

Armis Centrix™ Helps Financial Services Align With DORA

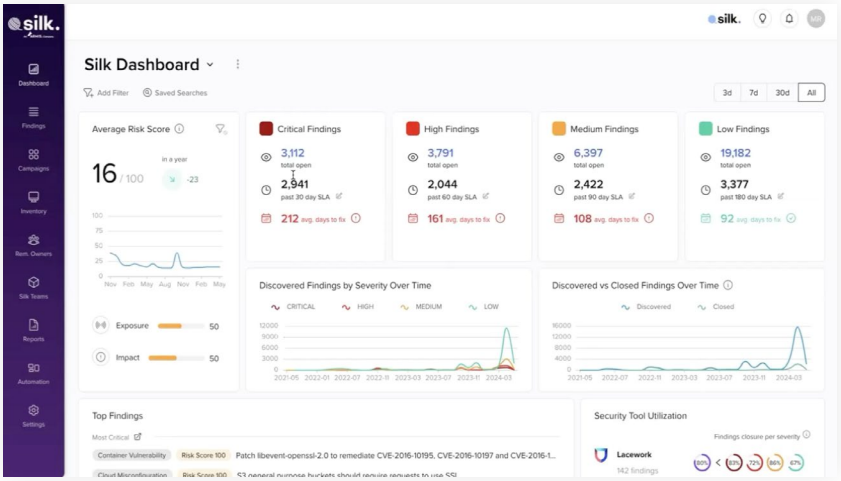
AI driven Asset Intelligence Engine tracking 4 billions of assets allows you to benefit for accurate, collaborative data gathered from financial institutions globally.

Data source agnostic, covering financial assets and risks from infrastructure to code to cloud, ensuring robust security and compliance.

Prioritize security findings and operationalize remediation, allowing financial institutions to efficiently address uncovered security threats, safeguard sensitive information and maintain trust.

Attack Preemption with Early Warning, empowering banks and investment firms to proactively address potential threats before they materialize.

Efficient asset management, gap analysis and compliance monitoring, providing financial services with the tools needed to optimize performance and meet regulatory requirements seamlessly.

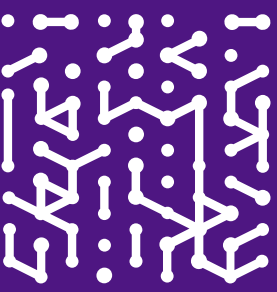


© Copyright Armis 2025

Aligning With The DORA Framework

The below table dives into how Armis Centrix™ helps organizations align with the DORA articles:

Pillar	Identifier	Text	How does Armis help
ICT Risk Management (framework)	**6.2**	The ICT risk management framework shall include at least strategies, policies, procedures, ICT protocols and tools that are necessary to duly and adequately protect all information assets and ICT assets, including computer software, hardware, servers, as well as to protect all relevant physical components and infrastructures, such as premises, data centres and sensitive designated areas, to ensure that all information assets and ICT assets are adequately protected from risks including damage and unauthorised access or usage.	You cannot protect all assets unless you indentify and contextualize them all. Armis will discover all assets connected to your network.credentials or brute-force attempts.
ICT Risk Management (framework)	**6.3**	In accordance with their ICT risk management framework, financial entities shall minimise the impact of ICT risk by deploying appropriate strategies, policies, procedures, ICT protocols and tools. They shall provide complete and updated information on ICT risk and on their ICT risk management framework to the competent authorities upon their request.	Armis can meet the Tools requirement laid out in the orginal question. Armis tooling can then be used to provide data collection, consolidation and presentation, to enable monitoring and orchestration to support the other requirments required here: “”deploying appropriate strategies, policies, procedures, ICT protocols”” Armis’ cloud-based risk analysis engine risk assesses every device in your environment. Risk scores are continually updated as Armis receives new information on new or emerging risk factors. The risk score is the result of various characteristics of the device (make, model, OS), what software each device is running, vulnerabilities, the presence of security controls as well as how the asset is behaving. All data captured, processed or deduced in Armis is available for reports. Every report is wholly customisable and can be generated manually or scheduled for email delivery, daily, weekly or monthly. Additionally, Armis has an API and out of box integrations which can be leveraged to pull reporting data for enrichment of external data systems (SIEM, ITAM, CMDB etc). “



© Copyright Armis 2025

Pillar	Identifier	Text	How does Armis help
ICT Risk Management (framework)	**6.4**	Financial entities, other than microenterprises, shall assign the responsibility for managing and overseeing ICT risk to a control function and ensure an appropriate level of independence of such control function in order to avoid conflicts of interest. Financial entities shall ensure appropriate segregation and independence of ICT risk management functions, control functions, and internal audit functions, according to the three lines of defence model, or an internal risk management and control model.	Armis can feed into a network segmentation program and monitor for deviations from rules. The aspect of this that speaks to people and process governance can also be managed by behavior monitoring with Armis. Armis provides capabilities to map asset connections and communication routes.
ICT Risk Management (framework)	**6.5**	The ICT risk management framework shall be documented and reviewed at least once a year, or periodically in the case of microenterprises, as well as upon the occurrence of major ICT-related incidents, and following supervisory instructions or conclusions derived from relevant digital operational resilience testing or audit processes. It shall be continuously improved on the basis of lessons derived from implementation and monitoring. A report on the review of the ICT risk management framework shall be submitted to the competent authority upon its request.	Here we see the request for human process design that delivers continual improvement, Armis has the capacity to provide and feed infomation into the model assessment. Armis can additionally be used to continuously monitor implemented tooling.
ICT Risk Management (framework)	**6.6**	The ICT risk management framework of financial entities, other than microenterprises, shall be subject to internal audit by auditors on a regular basis in line with the financial entities' audit plan. Those auditors shall possess sufficient knowledge, skills and expertise in ICT risk, as well as appropriate independence. The frequency and focus of ICT audits shall be commensurate to the ICT risk of the financial entity.	ICT auditors can continuously access real-time asset risk data using Armis ready to use dashboards or by leveraging the intuitive Armis query language, to make audit tasks faster and more efficient to complete.
ICT Risk Management (framework)	**6.7**	Based on the conclusions from the internal audit review, financial entities shall establish a formal follow-up process, including rules for the timely verification and remediation of critical ICT audit findings.	Armis integrates with existing security controls, enforcement and ticketing tools, giving customers the ability to report on efforts to remediate critical ICT audit findings relating to ICT asset risk.
ICT Risk Management (framework)	**6.8**	The ICT risk management framework shall include a digital operational resilience strategy setting out how the framework shall be implemented. To that end, the digital operational resilience strategy shall include methods to address ICT risk and attain specific ICT objectives, by:	This requirement must be built on a foundation of "knowing what ICT assets exist in your organisation"

© Copyright Armis 2025

Pillar	Identifier	Text	How does Armis help
ICT Risk Management (framework)	**6.8.c**	setting out clear information security objectives, including key performance indicators and key risk metrics;	Armis can generate reports and dashboards to track key ICT asset risk metrics and demonstrate progress on exposure reduction. Armis will correlate and normalise data from multiple sources in order to continuously validate the security controls required by compliance regulations (NIST, CIS control, ISO 27001, etc.) are present and configured to function correctly.
ICT Risk Management (framework)	**6.8.d**	explaining the ICT reference architecture and any changes needed to reach specific business objectives;	Armis can enrich discovered assets with business application context, in order visualise whether ICT assets support Important Business Applications and to enable risk based prioritisation.
ICT Risk Management (ICT systems, protocols and tools)	**7.1**	In order to address and manage ICT risk, financial entities shall use and maintain updated ICT systems, protocols and tools that are:	Armis can be used to monitor how tooling is operating.
ICT Risk Management (ICT systems, protocols and tools)	**7.1.a**	appropriate to the magnitude of operations supporting the conduct of their activities, in accordance with the proportionality principle as referred to in Article 4;	Armis serves 30% of Fortune100 and over 1000 enterprises across the globe. The Armis Centrix™ AI-powered Asset Intelligence Engine stops 500,000 attacks a month and continuously analyses: Billion of assets, 320B micro behavior models, 500B events per day, 850M vulnerabilities.
ICT Risk Management (ICT systems, protocols and tools)	**7.1.b**	reliable;	Armis can be used to monitor how tooling is operating.
ICT Risk Management (Identification)	**8.1**	As part of the ICT risk management framework referred to in Article 6(1), financial entities shall identify, classify and adequately document all ICT supported business functions, roles and responsibilities, the information assets and ICT assets supporting those functions, and their roles and dependencies in relation to ICT risk. Financial entities shall review as needed, and at least yearly, the adequacy of this classification and of any relevant documentation.	Armis creates a complete and continuous asset inventory and associated network activities. • Providing a real-time, context rich, record for every asset. • Analysing network traffic and building a complete network map • Tracking every asset connection to/from other assets, virtual and physical segments and external internet

© Copyright Armis 2025

Pillar	Identifier	Text	How does Armis help
ICT Risk Management (Identification)	**8.2**	Financial entities shall, on a continuous basis, identify all sources of ICT risk, in particular the risk exposure to and from other financial entities, and assess cyber threats and ICT vulnerabilities relevant to their ICT supported business functions, information assets and ICT assets. Financial entities shall review on a regular basis, and at least yearly, the risk scenarios impacting them.	Armis will continously identify on-device risk factors such as EOL/EOS Operating Systems/ Applications, Vulnerabilities, use of default credentials, missing or malfunctioning security agents, or use of insecure protocols. Armis Centrix™ for Actionable Threat Intelligence allows insights into vulnerabiities that are hitting your industry peers so you can take proactive remediation steps. Armis will also continuously identify network risks such as external facing assets, open ports and poor network segmentation.
ICT Risk Management (Identification)	**8.3**	Financial entities, other than microenterprises, shall perform a risk assessment upon each major change in the network and information system infrastructure, in the processes or procedures affecting their ICT supported business functions, information assets or ICT assets.	Armis' cloud-based risk analysis engine risk assesses every device in your environment on a continual basis. Therefore up to date risk information is immediately available to risk auditors before, during and after any major change in the network and information system infrastructure.
ICT Risk Management (Identification)	**8.4**	Financial entities shall identify all information assets and ICT assets, including those on remote sites, network resources and hardware equipment, and shall map those considered critical. They shall map the configuration of the information assets and ICT assets and the links and interdependencies between the different information assets and ICT assets.	Armis will identify ALL assets regardless of type. Asset context derived from integrations, as well as network traffic connectivity can be used to map the asset to its specific business context or service.
ICT Risk Management (Identification)	**8.5**	Financial entities shall identify and document all processes that are dependent on ICT third-party service providers, and shall identify interconnections with ICT third-party service providers that provide services that support critical or important functions.	Armis will discover all interdependencies including remote accesses to systems. The platform is also able to identify interconnections with ICT third-party service providers that provide services that support critical or important functions.

© Copyright Armis 2025

Pillar	Identifier	Text	How does Armis help
ICT Risk Management (Identification)	**8.6**	For the purposes of paragraphs 1, 4 and 5, financial entities shall maintain relevant inventories and update them periodically and every time any major change as referred to in paragraph 3 occurs.	Armis will continously identify on-device risk factors such as EOL/EOS Operating Systems/ Applications, Vulnerabilities, use of default credentials, missing or malfunctioning security agents, or use of insecure protocols. Armis will also continuously identify network risks such as external facing assets, open ports, poor network segmentation as well as detecting threats, exploit attempts, and suspicious/anomalous behavior.
ICT Risk Management (Identification)	**8.7**	Financial entities, other than microenterprises, shall on a regular basis, and at least yearly, conduct a specific ICT risk assessment on all legacy ICT systems and, in any case before and after connecting technologies, applications or systems.	Armis' cloud-based risk analysis engine risk assesses every device in your environment on a continual basis. Therefore up to date risk information is immediately available for any ICT risk assessment.
ICT Risk Management (Protection and prevention)	**9.1**	For the purposes of adequately protecting ICT systems and with a view to organising response measures, financial entities shall continuously monitor and control the security and functioning of ICT systems and tools and shall minimise the impact of ICT risk on ICT systems through the deployment of appropriate ICT security tools, policies and procedures.	Armis will continously identify on-device risk factors such as EOL/EOS Operating Systems/ Applications, Vulnerabilities, use of default credentials, missing or malfunctioning security controls, or use of insecure protocols. Armis will also continuously identify network risks such as external facing assets, open ports, poor network segmentation as well as detecting threats, exploit attempts, and suspicious/ anomalous behavior.
ICT Risk Management (Protection and prevention)	**9.2**	Financial entities shall design, procure and implement ICT security policies, procedures, protocols and tools that aim to ensure the resilience, continuity and availability of ICT systems, in particular for those supporting critical or important functions, and to maintain high standards of availability, authenticity, integrity and confidentiality of data, whether at rest, in use or in transit.	Armis will continously identify on-device risk factors such as EOL/EOS Operating Systems/ Applications, Vulnerabilities, use of default credentials, missing or malfunctioning security controls, or use of insecure protocols. Armis will also continuously identify network risks such as external facing assets, open ports, poor network segmentation as well as detecting threats, exploit attempts, and suspicious/anomalous behavior.

© Copyright Armis 2025

Pillar	Identifier	Text	How does Armis help
ICT Risk Management (Protection and prevention)	**9.4.a**	develop and document an information security policy defining rules to protect the availability, authenticity, integrity and confidentiality of data, information assets and ICT assets, including those of their customers, where applicable;	This requirement is about defining policy and process, Armis has the ability to be a part of that solution once the definiing stage has taken place.
ICT Risk Management (Protection and prevention)	**9.4.b**	following a risk-based approach, establish a sound network and infrastructure management structure using appropriate techniques, methods and protocols that may include implementing automated mechanisms to isolate affected information assets in the event of cyber-attacks;	With network traffic analysis Armis can apply signature-based detection of network exploit attempts using deep packet inspection, identify IOCs (indicators of compromise) in communication attempts to malicious or suspicious domains/hosts. Pre-built policies can be enabled to trigger an apropriate action including instructing a enforcement mechanism such as WLC, firewall, NAC to protect the network from an infected device.
ICT Risk Management (Protection and prevention)	**9.4.c**	implement policies that limit the physical or logical access to information assets and ICT assets to what is required for legitimate and approved functions and activities only, and establish to that end a set of policies, procedures and controls that address access rights and ensure a sound administration thereof;	With Armis' deep understanding of asset context, risk and network connectivity, IT & Security teams can intelligently segment networks by creating Access Control Lists (ACL). This can be done using policies to automatically send intelligent triggers to existing network enforcement systems such as WLC, firewall, NAC and switch or leveraging the Armis API framework to feed asset data to microsegmentation platforms. Armis can also provide monitoring and policy control over this process.
ICT Risk Management (Protection and prevention)	**9.4.e**	implement documented policies, procedures and controls for ICT change management, including changes to software, hardware, firmware components, systems or security parameters, that are based on a risk assessment approach and are an integral part of the financial entity's overall change management process, in order to ensure that all changes to ICT systems are recorded, tested, assessed, approved, implemented and verified in a controlled manner;	Armis will continously identify on-device risk factors such as EOL/EOS Operating Systems/ Applications, Vulnerabilities, use of default credentials, missing or malfunctioning security controls, or use of insecure protocols.

© Copyright Armis 2025

Pillar	Identifier	Text	How does Armis help
ICT Risk Management (Protection and prevention)	**9.5**	For the purposes of the first subparagraph, point (b), financial entities shall design the network connection infrastructure in a way that allows it to be instantaneously severed or segmented in order to minimise and prevent contagion, especially for interconnected financial processes.	NDR capabilities can be leveraged to monitor the networks and what is traversing links. Armis can continuously identify network risks such as external facing assets, open ports, poor network segmentation as well as detecting threats, exploit attempts, and suspicious/anomalous behaviour.
ICT Risk Management (Detection)	**10.1**	Financial entities shall have in place mechanisms to promptly detect anomalous activities, in accordance with Article 17, including ICT network performance issues and ICT-related incidents, and to identify potential material single points of failure. All detection mechanisms referred to in the first subparagraph shall be regularly tested in accordance with Article 25.	Armis will continuously identify network risks such as external facing assets, open ports, poor network segmentation as well as detecting threats, exploit attempts, and suspicious/ anomalous behaviour.
ICT Risk Management (Detection)	**10.2**	The detection mechanisms referred to in paragraph 1 shall enable multiple layers of control, define alert thresholds and criteria to trigger and initiate ICT-related incident response processes, including automatic alert mechanisms for relevant staff in charge of ICT-related incident response.	Armis will integrate with existing ICT platforms, existing enforcement and ticketing tools, to establish end-to-end workflows and true risk lifecycle management in a phased and continuous manner: • Monitor: Find and classify all connected assets and track the network connections • Discover Exposures: Identify and aggregate risk findings, vulnerabilties and highlight security control gaps • Detect Threats: Detect suspicious and malicious threat activities • Prioritize most urgent based on the likelihood to be exploited and the business impact • Orchestrate remediation and enforcement actions to reduce risk and block threats
ICT Risk Management (Detection)	**10.3**	Financial entities shall devote sufficient resources and capabilities to monitor user activity, the occurrence of ICT anomalies and ICT-related incidents, in particular cyber-attacks.	Armis empowers SOC/SIEM platform teams to accelerate ICT incident triage, drive threat investigation, containment, and hunts based upon device level incident details such as device type, classification, threats, and vulnerabilities across all asset types. Armis automated ticketing integration can open an Incident workflows in platforms such as ServiceNow with comprehensive device and incident details such as the device type, classification, threats, vulnerabilities, included in the ticket creation logic to accelerate incident response.

© Copyright Armis 2025

Pillar	Identifier	Text	How does Armis help
ICT Risk Management (Response and Recovery)	**11.2.b**	quickly, appropriately and effectively respond to, and resolve, all ICT-related incidents in a way that limits damage and prioritises the resumption of activities and recovery actions;	Armis empowers SOC/SIEM platform teams to accelerate ICT incident triage, drive threat investigation, containment, and hunts based upon device level incident details such as device type, classification, threats, and vulnerabilities across all asset types. Armis automated ticketing integration can open an Incident workflows in platforms such as ServiceNow with comprehensive device and incident details such as the device type, classification, threats, vulnerabilities, included in the ticket creation logic to accelerate incident response.
ICT Risk Management (Response and Recovery)	**11.5**	As part of the overall business continuity policy, financial entities shall conduct a business impact analysis (BIA) of their exposures to severe business disruptions. Under the BIA, financial entities shall assess the potential impact of severe business disruptions by means of quantitative and qualitative criteria, using internal and external data and scenario analysis, as appropriate. The BIA shall consider the criticality of identified and mapped business functions, support processes, third-party dependencies and information assets, and their interdependencies. Financial entities shall ensure that ICT assets and ICT services are designed and used in full alignment with the BIA, in particular with regard to adequately ensuring the redundancy of all critical components.	Armis is able to deliver actionable threat intelligence and use data gathered from other industry dfisruptions and known exploitabilites to enable BIA. Armis can map the criticality of identified and mapped business functions. With Armis Centrix™ for Actionable Threat Intelligence, you can ensure your OT organization is always leveraging the most up-to-date protection to mitigate the risk associated with high stakes vulnerabilities. Transcend traditional security measures and proactively identify preparatory indicators of attacks and exploits.
ICT Risk Management (Backup policies and procedures, restoration and recovery procedures and methods)	**12.3.1**	When restoring backup data using own systems, financial entities shall use ICT systems that are physically and logically segregated from the source ICT system. The ICT systems shall be securely protected from any unauthorised access or ICT corruption and allow for the timely restoration of services making use of data and system backups as necessary.	Armis can be used as part of a network segmentation program, Armis is also able to monitor traffic across network boundaries, but I think this is talking more about a design that delivers a seperate and unbreached ICT function.

© Copyright Armis 2025

Pillar	Identifier	Text	How does Armis help
ICT Risk Management (Learning and evolving)	**13.2.2**	The post ICT-related incident reviews referred to in the first subparagraph shall determine whether the established procedures were followed and the actions taken were effective, including in relation to the following:	Aiding the process after a incident, to review the response and actions and look for improvements.
ICT Risk Management (Learning and evolving)	**13.2.a**	the promptness in responding to security alerts and determining the impact of ICT-related incidents and their severity;	Improves efficiency of response and triage of incidents and anomalies.
ICT Risk Management (Learning and evolving)	**13.2.b**	the quality and speed of performing a forensic analysis, where deemed appropriate;	Improves efficiency of response, 'speed of' and triage of incidents and anomalies.
ICT Risk Management (Learning and evolving)	**13.2.c**	the effectiveness of incident escalation within the financial entity;	Improves efficiency of response and triage of incidents and anomalies.
ICT Risk Management (Learning and evolving)	**13.7**	Financial entities, other than microenterprises, shall monitor relevant technological developments on a continuous basis, also with a view to understanding the possible impact of the deployment of such new technologies on ICT security requirements and digital operational resilience. They shall keep up-to-date with the latest ICT risk management processes, in order to effectively combat current or new forms of cyber-attacks.	Armis can help with this, using ATI to help financial instituitions keep ahead of new vulnerabilities. This can be achieved through the concept of collaborative data that is also seen in action with the Armis Asset intelligence Engine, a database that gives you the contextual knowledge of billions of known assets globally.

© Copyright Armis 2025

Pillar	Identifier	Text	How does Armis help
ICT Risk Management (Simplified ICT risk management framework)	**16.1.b**	continuously monitor the security and functioning of all ICT systems;	Armis will continously identify on-device risk factors such as EOL/EOS Operating Systems/ Applications, Vulnerabilities, use of default credentials, missing or malfunctioning security controls, or use of insecure protocols. Armis will also continuously identify network risks such as external facing assets, open ports, poor network segmentation as well as detecting threats, exploit attempts, and suspicious/ anomalous behaviour.
ICT Risk Management (Simplified ICT risk management framework)	**16.1.d**	allow sources of ICT risk and anomalies in the network and information systems to be promptly identified and detected and ICT-related incidents to be swiftly handled;	Armis empowers SOC/SIEM platform teams to accelerate ICT incident triage, drive threat investigation, containment, and hunts based upon device level incident details such as device type, classification, threats, and vulnerabilities across all asset types. Armis automated ticketing integration can open an Incident workflows in platforms such as ServiceNow with comprehensive device and incident details such as the device type, classification, threats, vulnerabilities, included in the ticket creation logic to accelerate incident response.
ICT Risk Management (Simplified ICT risk management framework)	**16.1.g**	test, on a regular basis, the plans and measures referred to in point (f), as well as the effectiveness of the controls implemented in accordance with points (a) and (c);	Gap Analysis is a key core functionality of the Armis Platform and enables continuous testing.
Digital operational resilience testing (General requirements for the performance of digital operational resilience testing)	**24.1**	For the purpose of assessing preparedness for handling ICT-related incidents, of identifying weaknesses, deficiencies and gaps in digital operational resilience, and of promptly implementing corrective measures, financial entities, other than microenterprises, shall, taking into account the criteria set out in Article 4(2), establish, maintain and review a sound and comprehensive digital operational resilience testing programme as an integral part of the ICT risk-management framework referred to in Article 6.	Armis addresses key challenges faced by Financial Services organisations with regards ICT risk-management: • Attack Surface Expansion: Armis ensures that organizations continuously see, secure, protect and manage all critical assets. • Asset Inventory: Inability to create an accurate asset inventory can undermine an organisation's entire risk management program. • Risk Management: The need to prioritize risks based on likelihood to be exploited, business impact and compensating security controls. • Compliance Requirements: Need to report on cybersecurity governance capabilities, procedures, and strategies.

© Copyright Armis 2025

Pillar	Identifier	Text	How does Armis help
Digital operational resilience testing (General requirements for the performance of digital operational resilience testing)	**24.5**	Financial entities, other than microenterprises, shall establish procedures and policies to prioritise, classify and remedy all issues revealed throughout the performance of the tests and shall establish internal validation methodologies to ascertain that all identified weaknesses, deficiencies or gaps are fully addressed.	Armis addresses key challenges faced by Financial Services organisations with regards ICT risk-management: • Attack Surface Expansion: In a rapidly evolving, perimeter-less world Armis ensures that organizations continuously see, secure, protect and manage all critical assets. • Asset Inventory: Inability to create an accurate asset inventory can undermine an organisation's entire risk management program • Risk Management: The need to prioritize risks based on likelihood to be exploited, business impact and compensating security controls • Compliance Requirements: Need to report on cybersecurity governance capabilities, procedures, and strategies
Digital operational resilience testing (General requirements for the performance of digital operational resilience testing)	**24.6**	Financial entities, other than microenterprises, shall ensure, at least yearly, that appropriate tests are conducted on all ICT systems and applications supporting critical or important functions.	Armis addresses key challenges faced by Financial Services organisations with regards ICT risk-management: • Monitoring tooling operations • Attack Surface Expansion: In a rapidly evolving, perimeter-less world Armis ensures that organizations continuously see, secure, protect and manage all critical assets. • Asset Inventory: Inability to create an accurate asset inventory can undermine an organisation's entire risk management program • Risk Management: The need to prioritize risks based on likelihood to be exploited, business impact and compensating security controls • Compliance Requirements: Need to report on cybersecurity governance capabilities, procedures, and strategies
Digital operational resilience testing (Testing of ICT tools and systems)	**25.1**	The digital operational resilience testing programme referred to in Article 24 shall provide, in accordance with the criteria set out in Article 4(2), for the execution of 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.	Armis addresses key challenges faced by Financial Services organisations with regards ICT risk-management: • Attack Surface Expansion: In a rapidly evolving, perimeter-less world Armis ensures that organizations continuously see, secure, protect and manage all critical assets. • Asset Inventory: Inability to create an accurate asset inventory can undermine an organisation's entire risk management program • Risk Management: The need to prioritize risks based on likelihood to be exploited, business impact and compensating security controls • Compliance Requirements: Need to report on cybersecurity governance capabilities, procedures, and strategies

© Copyright Armis 2025

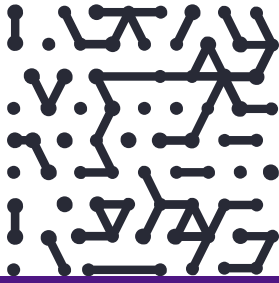
Pillar	Identifier	Text	How does Armis help
Digital operational resilience testing (Testing of ICT tools and systems)	**25.2**	Central securities depositories and central counterparties shall perform vulnerability assessments before any deployment or redeployment of new or existing applications and infrastructure components, and ICT services supporting critical or important functions of the financial entity.	Can show gap analysis of what has been scanned and what has not. Also can ensure that all elements of newly deploy system or applications are being appropriately monitored or queried.
Digital operational resilience testing (Advanced testing of ICT tools, systems and processes based on TLPT)	**26.2**	Each threat-led penetration test shall cover several or all critical or important functions of a financial entity, and shall be performed on live production systems supporting such functions. Financial entities shall identify all relevant underlying ICT systems, processes and technologies supporting critical or important functions and ICT services, including those supporting the critical or important functions which have been outsourced or contracted to ICT third-party service providers. Financial entities shall assess which critical or important functions need to be covered by the TLPT. The result of this assessment shall determine the precise scope of TLPT and shall be validated by the competent authorities.	Armis Centrix™ for Actionable Threat Intelligence is an optional integration and introduces a paradigm shift. Whereas traditional security goes to work when an attack is launched, actionable threat intelligence enables organizations to find potential threats before they are ever launched and before their environment is ever impacted. In many cases, months earlier. In fact, Armis has hundreds of instances where customers were proactively alerted to a threat before a CVE was issued.
Digital operational resilience testing (Advanced testing of ICT tools, systems and processes based on TLPT)	**26.8.c**	specific ICT risk profile, level of ICT maturity of the financial entity or technology features involved.	The Armis Platform can evidence levels of security maturity within an organisation. This helps build your security strategy against frameworks such as NIST, ISO 27001 etc.

© Copyright Armis 2025

Conclusion

DORA presents a comprehensive regulatory framework that significantly enhances the digital operational resilience of organizations within the financial sector. By closely aligning with the five foundational pillars of DORA, Armis provides a robust solution platform that not only meets many of the regulatory requirements but also empowers organizations to proactively manage and mitigate ICT risks. The integration of Armis' advanced capabilities into your risk management strategy ensures a comprehensive approach to achieving compliance with DORA.

From identifying and managing ICT risks to enhancing incident response mechanisms and fostering a culture of collaborative intelligence sharing. The mirroring of Armis' capabilities to the DORA framework equips organizations to not only survive in an increasingly digital and interconnected landscape but to thrive.



Armis, the cyber exposure management & security company, protects the entire attack surface and manages an organization's cyber risk exposure in real time.

In a rapidly evolving, perimeter-less world, Armis ensures that organizations continuously see, protect and manage all critical assets - from the ground to the cloud. Armis secures Fortune 100, 200 and 500 companies as well as national governments, state and local entities to help keep critical infrastructure, economies and society stay safe and secure 24/7.

Armis is a privately held company headquartered in California.

1.888.452.4011

Website
Platform
Industries
Solutions
Resources
Blog

Try Armis
Demo
Free Trial