The Digital Operational Resilience Act (DORA) is a European Union (EU) regulation that aims to strengthen the IT security of financial entities of the European financial market by ensuring that it can withstand severe operational disruptions caused by cyber threats or incidents. ARCON's highly mature Identity and Access Management (IAM) along with enterprise risk remediation solutions can help the financial organizations of Europe to comply with the mandates of DORA and build a cyber resilience.

Table of Content

Overview

The Digital Operational Resilience Act (DORA) is an EU regulation that entered into force on 16 January 2023 and will be applicable as of 17 January 2025.

It aims at strengthening the IT security of financial entities such as banks, insurance companies and investment firms and making sure that the financial sector in Europe is able to stay resilient in the event of a severe operational disruption.

DORA brings harmonisation of the rules relating to operational resilience for the financial sector applying to 20 different types of financial entities and ICT third-party service providers.

Why is DORA needed?

The financial sector is increasingly dependent on technology and on tech companies to deliver financial services. This makes financial entities vulnerable to cyber-attacks or incidents.

When not managed properly, ICT risks can lead to disruptions of financial services offered across borders. This in turn, can have an impact on other companies, sectors and even on the rest of the economy, which underlines the importance of the digital operational resilience of the financial sector.

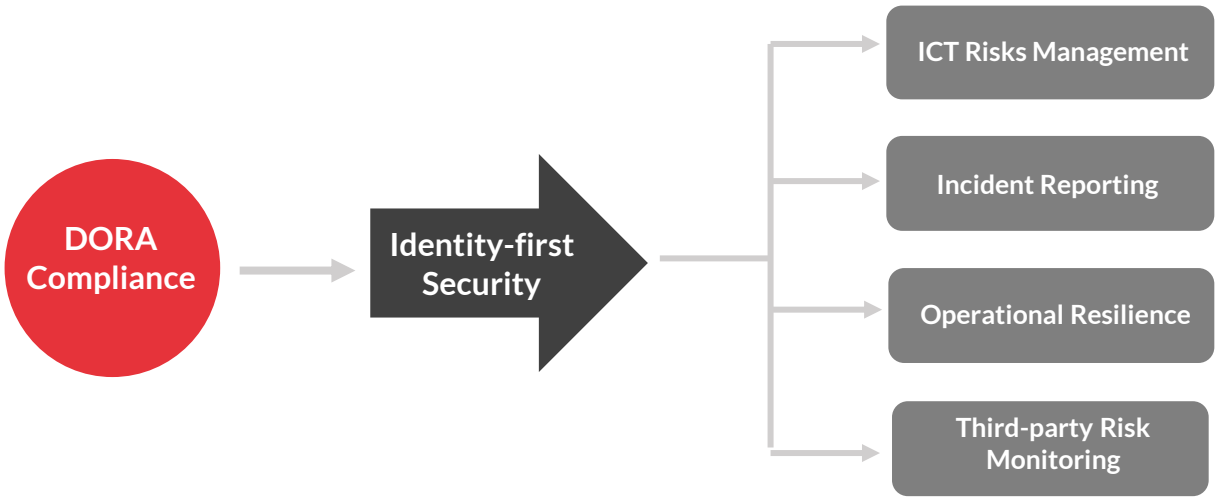
Identity-first Security is at the Forefront of IT Security Initiatives

The number of digital identities is proliferating in any typical midsize and large enterprise IT setup. The increased influence of hybrid work environments, the advent of cloud computing, and exponential growth in business automation processes have led to a drastic change in IT environments, which now require lots of users with both human and non-human identities to perform different IT tasks.

DORA compliance regulation demands tracking, evaluating, and managing potential risks arising from distributed IT infrastructure and third-party service providers for which identity security plays a pivotal role, especially the privileged identity. Indeed, a privileged account often includes permissions that allow changes to be made to settings, such as security configurations. By nature, privileged accounts have the greatest potential for operational risk, reputational risk, loss of intellectual property, loss of regulated data or even, in the case of cyber-physical incidents resulting in catastrophic loss.

Today, identity-first security strategy is at the forefront of IT security initiatives because the essence of identity-first security lies in continuous monitoring and context-wise controls. ARCON suite of solutions helps in building the foundation of identity-first security posture by offering basic and advanced features and functionalities to address access control challenges in IT environment. The access control mechanisms of ARCON solutions offer:

- Implementing continuous identity threat analytics and orchestration
- Ensuring regular certification and recertification of digital identities
- Establishing centralized control to control, manage and monitor all sorts of identities- converged identity approach
- Verifying the trust of an identity using context-based authentication
- Enforcing just-in-time access to systems



DORA Checklist and Role of ARCON Solutions

In this compliance mapping paper, we have discussed the requirements of DORA in the below table and how ARCON suite of solutions helps organisations to meet the regulatory requirements.

ICT risk management Overview	ARCON's capabilities
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. Organizations must implement measures to minimize cyber risks, including incident management, supply chain security, network security, access control, and encryption.	▪ Access control ▪ Secure remote access ▪ Password rotation ▪ Privilege Account discovery ▪ Implementing session controls, isolation and monitoring ▪ Implementing FIM controls on critical assets ▪ Implementing API security ▪ Secure file transfer mechanisms ▪ Implementing perimeter controls ▪ Implementing controls for local account management ▪ Implementing ARCON EPM for admin account credential management(desktops/laptops) ▪ Implementing ARCON SCM (Security Compliance Management) ▪ Implementing controls for machine-to-machine access ▪ Implementing controls with ticketing systems ▪ Implementing SIEM capabilities ▪ Secure incident response capabilities for critical events ▪ Secure access logs, audit logs, command logs, video monitoring logs

ICT third-party risk management Overview	ARCON's capabilities
Methods and approaches for tracking, evaluating, and managing potential risks linked to third-party service providers	▪ Implementing controls for 3rd party remote access ▪ Implementing ARCON EPM for vendors/3rd party contractors for security checks ▪ Implementing session isolation, controls and monitoring ▪ Enforcing adaptive MFA for access ▪ Enable controls for access to third party SaaS consoles ▪ Implement User access governance procedures for secure governance of 3rd party access

Information sharing Overview	ARCON's capabilities
Methods and approaches for tracking, evaluating, and managing potential risks linked to third-party service providers	▪ Enforcing automated reporting for critical activities ▪ Enforcing SIEM controls ▪ Reporting with ARCON PAM Vault reports, Security reports, Compliance reports, Monitoring logs, audit logs ▪ Enforcing strict controls for incident response and access reviews ▪ Implementing ARCON MyVault for data/file sharing capabilities ▪ Automating controls for anomalous privileged activities

Conclusion

The financial market of Europe aims to eliminate complexities, enhance resilience, and standardize risk management practices across the EU financial systems. ARCON solutions are essential part of complying with DORA regulations including ICT risk management, ICT third-party risk management and information sharing requirements.

about ARCON

ARCON is a leading Information Risk Management solutions provider specializing in Privileged Access Management and Continuous Risk Assessment solutions.

ARCON Privileged Access Management (PAM) is a leading global product and a robust solution that mitigates risks arising out of privilege identity and access management.

Connect with us