

SOLUTION BRIEF

DORA and IGA

Stay compliant with Identity Governance and Administration



What is DORA?

The European Union's Digital Operational Resilience Act (DORA) is a regulatory framework aimed at ensuring that the financial sector within the EU can withstand and respond to information and communication technology (ICT) incidents. It focuses on enhancing the digital operational resilience of financial entities by establishing uniform requirements for the security of their digital systems.

What is IGA?

Identity Governance and Administration (IGA) is a cybersecurity domain that manages and controls digital identities and access rights across an organization. It combines identity management (IDM) and access governance to ensure that the right individuals have appropriate access to the right resources at the right times, and for the right reasons.

The intersection between DORA and IGA

The intersection of DORA and IGA lies in their mutual goal of enhancing the security and operational resilience of financial institutions through effective management of digital identities and access rights.

Areas where DORA and IGA intersect:

1) ICT Risk Management and Identity Management:

- **DORA:** Mandates robust ICT risk management frameworks, including protection against unauthorized access and ensuring that systems are resilient against cyber threats.
- **IGA:** Facilitates identity management, ensuring that only authorized individuals have access to sensitive and classified systems and data, thus reducing the risk of unauthorized access and potential cyber incidents.

2) Access Control and Compliance:

- **DORA:** Requires financial entities to comply with stringent security policies and regulatory requirements, including access control measures to protect critical data and systems.
- **IGA:** Provides the tools and processes to enforce access control policies, ensuring that access rights are granted based on roles and responsibilities and are reviewed regularly, as well as documented for compliance.

3) Governance and Policy Enforcement:

- **DORA:** Stipulates that financial entities must have a governance framework for ICT risk management, including clear policies for access control and user management.
- **IGA:** Supports governance by defining roles and responsibilities, enforcing access policies, and providing audit trails to ensure and document that governance requirements are met.

4) Attestation:

- **DORA:** Implies the need for regular reviews and updates to security policies and controls to adapt to evolving threats.
- **IGA:** Facilitates periodic attestation of user access rights, ensuring ongoing compliance with security policies and regulatory requirements.

5) Third-Party Risk Management:

- **DORA:** Requires that third-party ICT service providers meet operational resilience standards, including secure identity and access management practices.
- **IGA:** Ensures that third-party access is governed and monitored, reducing the risk of vulnerabilities introduced through external service providers.

6) Audit and Compliance Reporting:

- **DORA:** Necessitates comprehensive reporting and documentation to demonstrate compliance with resilience standards.
- **IGA:** Provides detailed audit logs and compliance reports, documenting who accessed what resources, when, and why, thus supporting DORA's compliance requirements.

How to get there?

Omada's Global Advisory Practice consists of highly skilled and experienced professional advisors who are ready to support organizations to ensure their Identity Governance and Administration solution is fit for the DORA purpose. Through well-defined and proven service packages, Omada's Global Advisory Practice will help to identify, map, align, and document what is needed to comply with DORA within the IGA domain.

Omada, a global market leader in Identity Governance and Administration (IGA), offers a full-featured, enterprise-grade, cloud-native IGA solution that enables organizations to achieve compliance, reduce risk, and maximize efficiency. Founded in 2000, Omada delivers innovative identity management to complex hybrid environments based on our proven best practice process framework and deployment approach.

Omada has implemented Identity Governance and Administration for customers across all industries and has extensive experience in facilitating a smooth and well-prioritized IGA operation.

For more information, go to www.omadaidentity.com | info@omadaidentity.com

