ORACLE

Oracle Database and DORA

Strengthening security, resilience, and compliance posture

June, 2026, Version 1.0

Public

Purpose statement

This document provides an overview of Oracle Database security features and related products, and explains how they may help organizations address selected requirements of the European Union's Digital Operational Resilience Act (DORA). It is intended to help security and risk stakeholders evaluate options to reduce risk and improve regulatory compliance in Oracle Database environments.

This technical brief is designed for CISOs, database administrators (DBAs), and security architects responsible for Oracle AI Database environments who need both near-term improvements and a sustainable path to comprehensive security.

The guidance reflects current best practices and Oracle product capabilities as of the publication date. Because security threats continue to evolve, organizations should regularly assess their security posture and recovery capabilities.

Disclaimer

This document in any form, software or printed matter, contains proprietary information that is the exclusive property of Oracle. Your access to and use of this confidential material is subject to the terms and conditions of your Oracle software license and service agreement, which has been executed and with which you agree to comply. This document is not part of your license agreement nor can it be incorporated into any contractual agreement with Oracle or its subsidiaries or affiliates.

Some of the Oracle Database Security technologies may or may not be relevant based upon an organization's specific environment. Oracle always recommends testing security solutions within your specific environment to ensure that performance, availability, and integrity are maintained.

The information in this document does not constitute legal advice. Organizations should consult their own legal counsel the to determine the content, interpretation and applicability of any law or regulation including how such law or regulation may apply to their use of Oracle's products or services.

ORACLE

Contents

Executive summary

The EU Digital Operational Resilience Act (DORA) introduces a framework for managing ICT risk across the European financial sector. Effective January 17, 2025, it requires financial entities to strengthen resilience, improve incident detection and reporting, and demonstrate control effectiveness through ongoing testing and oversight.

Financial services often rely on data stored in relational databases to support operations such as transactions, risk management, and regulatory reporting. As a result, database security and availability can influence an organization's ability to meet DORA requirements. Gaps in access control, auditing, or data protection can increase the likelihood of unauthorized access, delayed incident detection, or incomplete reporting.

Oracle Database can help organizations address these requirements by enforcing security controls within the database engine. This approach applies consistent policies across application, user, and administrative access paths and provides detailed visibility into database activity, including SQL execution, privileged access, and configuration changes. By operating close to the data and supporting separation of duties, these controls can help reduce the risk of circumvention, including by highly privileged users.

Oracle Database provides integrated capabilities across key DORA domains, including encryption, access control, auditing, monitoring, and resilience. Services such as Oracle Data Safe and Oracle Audit Vault and Database Firewall support continuous monitoring and reporting, while high availability and recovery solutions help organizations maintain operations and meet recovery objectives.

Together, these capabilities support a practical, database-centric approach to improving operational resilience and generating evidence to support compliance reporting.

Overview of DORA

DORA at a glance

The EU Digital Operational Resilience Act, regulation (EU) 2022/2554[1] on digital operational resilience for the financial sector, commonly known as DORA, was adopted in November 2022 and became applicable from 17 January 2025. It consolidates and supersedes certain national and sector-specific ICT risk guidelines that previously applied to EU financial entities, replacing them with a single, directly applicable legislative framework.

DORA is a regulation that applies directly as law in all EU member states without requiring transposition. Non-compliance could result in supervisory sanctions, such as financial penalties or public censure.

Scope of application

DORA applies to a broad category of financial entities, including credit institutions, payment institutions, electronic money institutions, investment firms, crypto-asset service providers, central securities depositories, insurance and reinsurance undertakings, and credit rating agencies.

DORA pillars

DORA establishes a framework built around several pillars that together define digital operational resilience. These pillars introduce requirements that financial entities must implement in a proportionate and risk-based manner:

- **ICT risk management**
  Financial entities are required to implement an ICT risk management framework that includes governance, policies, procedures, and controls to protect systems and data. This framework must address the full lifecycle of ICT risk, including identification, protection, detection, response, and recovery.
- **Incident detection and reporting**
  DORA introduces requirements for detecting, classifying, and reporting ICT-related incidents. Financial entities must establish processes to identify incidents quickly, assess their impact, and report major incidents to competent authorities within defined timelines.
- **Digital operational resilience testing**
  Financial entities must regularly test their ICT systems and controls to identify vulnerabilities and validate resilience capabilities. Testing ranges from basic assessments to advanced threat-led penetration testing for critical entities.
- **ICT third-party risk management**
  DORA places strong emphasis on managing risks associated with ICT third-party service providers.
- **Information and intelligence sharing**
  DORA encourages financial entities to share cyber threat intelligence and participate in collaborative security efforts to improve collective resilience across the sector.

The regulation requires financial entities to ensure that systems supporting critical functions remain **secure, reliable, and recoverable under adverse conditions**.

DORA emphasizes not only the implementation of controls but also the ability to demonstrate their effectiveness through testing, monitoring, and reporting.

Why database security is central to ICT risk management

DORA's focus on digital operational resilience makes the security and resilience of underlying data platforms an important consideration in a financial entity's broader ICT risk management framework. Databases frequently support important business processes and the transactional data used to deliver financial services. Weaknesses affecting database

availability, integrity, confidentiality, or recoverability can contribute to service disruption, incorrect processing, data loss, or other issues.

For this reason, financial entities should address database security and resilience as part of their DORA-aligned ICT risk management program, alongside application, infrastructure, network, identity, cloud, operational, and third-party controls.

Database controls across the digital operational resilience lifecycle

DORA requires financial entities to manage ICT risk through a lifecycle that includes identifying critical assets and dependencies, protecting ICT systems and data, detecting anomalous activity, responding to and recovering from ICT-related events, testing resilience, and demonstrating control effectiveness. Because Oracle Database environments often store regulated data, support important business services, and enforce privileged and application access paths, database controls can contribute across several parts of that lifecycle.

Database-related security, integrity, and availability events can be relevant inputs to a financial entity's ICT risk management, operational resilience, incident assessment, and recovery processes, depending on the event's facts and impact. The scenarios below illustrate why database-layer controls for encryption, access governance, secure connectivity, monitoring, configuration management, backup validation, and recovery readiness are important to a DORA-aligned operational resilience program.

Consider the following illustrative scenarios:

- **A ransomware attack affects a production database supporting payment processing, resulting in service unavailability or degradation.** This type of event may require assessment under the financial entity's ICT incident and recovery processes, particularly where important business services or recovery objectives are affected.
- **A privileged database administrator, or a threat actor using compromised credentials, attempts to access or modify transaction records.** This type of activity may affect data integrity and may require analysis of user activity, privilege use, access paths, and affected data.
- **An SQL injection attack against a database-connected application results in suspected unauthorized access to, or exfiltration of, customer personal data.** This type of event may require assessment under applicable ICT incident, privacy, and data protection processes.
- **A misconfigured database replication setup causes divergence between primary and standby systems.** This type of issue may affect recovery readiness or the organization's ability to meet recovery objectives during a disaster recovery event.

Oracle Database controls may help reduce exposure to these database-layer risks and provide evidence that supports operational response, recovery, remediation, control testing, and, where required, the financial entity's own incident assessment and escalation processes.

The case for built-in database security

Security controls deployed outside the database, such as network monitoring, application-layer firewalls, or external audit collection agents, provide important but inherently partial visibility. They rely on observing traffic across specific network paths and may have limited coverage of database activity executed through administrative tools, local connections, or internal database mechanisms that do not traverse monitored layers. These approaches can also introduce operational dependencies, including agent management and infrastructure alignment.

Database-native security controls, by contrast, are enforced within the database engine itself. They apply consistently across access paths — including application connections, administrative tools, and internal database processes — and operate with full session context, including user identity, application attributes, SQL activity, and data interactions. By embedding controls close to the data, this approach strengthens visibility and reduces reliance on external monitoring points.

This level of coverage and contextual awareness is aligned with DORA's emphasis on comprehensive ICT risk management, detection, and auditability, where effectiveness depends on the ability to monitor and control critical systems without gaps in visibility.

Oracle Database security capabilities

Oracle's industry-leading security portfolio can help organizations meet DORA's requirements through layered, integrated controls and specialized solutions.

Access control and least privilege

Oracle Database Vault enforces separation of duties and restricts privileged user access to sensitive data. Administrative users can be prevented from accessing application data unless explicitly authorized through policy, reducing the likelihood of insider threats and privilege misuse.

Database Vault also supports enforcement of trusted access paths, so that sensitive operations can only be performed through approved applications or connection methods. In addition, command rules can restrict the execution of high-risk operations, helping to prevent unauthorized or disruptive changes to database structures and configurations.

Oracle Deep Data Security and **Oracle Label Security** extend this model by enabling fine-grained, context-aware access control based on user identity, roles, and data classification.

Data protection and encryption

Oracle Advanced Security, including Transparent Data Encryption (**TDE**), protects data at rest.

Oracle Key Vault centralizes encryption key management, helping improve governance and simplify compliance with regulatory requirements.

Native Network Encryption (NNE) or **TLS** protects data in transit.

Quantum readiness and cryptographic agility

As encryption standards and threat models evolve, financial entities need the ability to adapt cryptographic controls without redesigning their database estate. Commission Delegated Regulation (EU) 2024/1774, the ICT risk management RTS[2] under DORA, reflects that expectation by reinforcing resilient encryption, cryptographic controls, and key-management policies in a changing threat landscape. Cryptographic agility is therefore not only a future-looking topic; it is part of the evidence financial institutions should be able to demonstrate under DORA today.

The most immediate and concrete risk is harvest now, decrypt later (HNDL): adversaries may capture encrypted database traffic or archived sensitive data today and hold it until quantum computing capabilities make decryption feasible. This threat is already active. Data is being collected now, regardless of when quantum capability matures. It is especially acute for banks, insurers, payment providers, and market infrastructures that retain sensitive records for extended periods. The European Union's own post-quantum cryptography (PQC) migration roadmap, coordinated through ENISA and aligned with NIST's finalized PQC standards, establishes a clear policy direction: organizations should begin inventorying cryptographic dependencies and prioritizing migration of long-lived sensitive data now, rather than waiting for a future inflection point (sometimes referred to as "Q-Day") to force action.

Oracle Database helps organizations prepare through a layered approach to data-at-rest protection, key governance, and modern encrypted connectivity. **Advanced Security Transparent Data Encryption** with AES-256 helps protect database files, backups, and exports. **Oracle Key Vault** supports separation of keys from encrypted data, lifecycle management, rotation, and recovery. **TLS 1.3** helps modernize encrypted database connections and, where supported, can provide a path toward quantum-safe or hybrid key exchange. Oracle AI Database 26ai supports ML-KEM for TLS 1.3 key exchange and ML-DSA for digital signatures, enabling phased migration of database clients and servers.

Practical DORA-oriented actions begin with establishing a cryptographic inventory or Cryptographic Bill of Materials (CBOM) to identify algorithms, key lengths, certificate lifetimes, and dependencies across the database estate. This is the most auditable starting point and the foundation for everything that follows. Long-retention and databases with high-value data should be classified as the primary HNDL risk surface and prioritized for migration. From there, organizations should standardize on AES-256 for TDE, backups, exports, and wallets, and migrate database connectivity (network encryption) to TLS 1.3 as a baseline modernization step.

Monitoring, auditing, and detection

Oracle Database Security Central and **Oracle Data Safe** provide centralized audit collection, audit policy provisioning, alerting, and compliance reporting, on-premises or in the cloud.

These capabilities help provide continuous visibility into database activity, enable rapid detection of anomalous behavior, and support regulatory reporting requirements.

Risk assessment and configuration management

Oracle Database Security Central, **Oracle Data Safe,** and Database Security Assessment Tool (**DBSAT**), are designed to evaluate database configurations, identify vulnerabilities, and provide remediation guidance.

High availability and business continuity

Oracle Active Data Guard and **Real Application Clusters** (RAC) can support high availability and continuity of operations in line with DORA resilience objectives.

Backup, recovery, and cyber resilience

Oracle Zero Data Loss Recovery Appliance (ZDLRA) helps provide continuous data protection at the transaction level, immutable backup storage, and automated validation of backup integrity.

Oracle Zero Data Loss Autonomous Recovery Service (ZRCV) delivers these capabilities as a managed cloud service, enforcing immutability and continuous validation.

Together, these solutions are designed to ensure that recovery processes are reliable, secure, and verifiable.

Oracle Database capabilities

The following sections explain how Oracle Database security capabilities may help organizations implement, validate, and demonstrate operational resilience in line with certain DORA requirements. This mapping focuses on areas where database controls play a direct role, highlighting practical relevance for architects, DBAs, and security teams.

Table 1: DORA Articles and Oracle Database Security Capabilities

Article	Key Requirements	Oracle Database security capability	Why

Art. 6	Financial entities shall have a sound, comprehensive and well-documented ICT risk management framework that includes strategies, policies, procedures, and tools to protect all information and ICT assets	Database security assessments with Oracle Data Safe, Oracle Database Security Central, or Oracle DBSAT posture assessment outputs.	Provides a unified view of fleet security posture, assesses configurations against benchmarks Center for Internet Security (CIS) and Security Technical Implementation Guide (STIG), and tracks security improvements and drift over time to support an ICT risk management framework. A database security baseline and continuous monitoring are typically core technical inputs into an ICT risk management framework.
Art. 7	Ensure ICT systems, protocols, and tools are appropriate, resilient, and support the ICT risk framework	Run latest versions with current Release Updates; deploy on Engineered Systems or Autonomous Database for scalable, resilient operations with autoscaling and HA failover; adopt Maximum Availability Architecture (MAA) best practices.	Database platform readiness and resilience are part of ICT tooling capability required by an ICT risk management framework.
Art. 8	Identify and classify ICT-supported business functions, assets, and dependencies	Database Security Assessments with Data Safe, Database Security Central, or DBSAT discovery/assessment outputs;	Asset identification depends on visibility into database estates, configurations, and sensitive data footprint.
Art. 9(1)	Continuous monitoring and control of ICT systems; minimize ICT risk through security tools and procedures	Oracle Data Safe, Oracle Database Security Central, Unified Auditing.	Provides continuous activity monitoring, database traffic inspection, and centralized auditing to detect and address risk in real time.
Art. 9(2)	Ensure resilience, continuity, availability, and CIA (confidentiality, integrity, availability) of data. Maintain high standards of availability, authenticity, integrity, and confidentiality of data at rest, in use, and in transit.	Oracle Maximum Availability Architecture (MAA), Oracle Maximum Security Architecture (MSA), Autonomous Database. Oracle Advanced Security Transparent Data Encryption (TDE), Oracle Key Vault (OKV), Database Vault. TLS, Native Network Encryption (NNE). MFA, Kerberos, PKI certificates, Microsoft Active Directory, RADIUS authentication.	MAA provides high availability, resilience, business continuity, and automated recovery for continuous database operations. MSA provides Oracle best practices for database security. Autonomous Database automates patching, hardening, and recovery to reduce operational risk. TDE protects data at rest, while TLS and NNE protect data in transit. OKV centralizes encryption key management, ensuring keys remain separate from protected data. TDE and OKV render stolen data unusable, helping mitigate extortion and data theft risks. Database Vault enforces separation of duties and restricts privileged user access to sensitive data. MFA, Kerberos, PKI, Active Directory, and RADIUS strengthen user and

			system authentication, supporting data authenticity and access control.
Art. 9(2)	Protect data at rest, in use, and in transit	Transparent Data Encryption (TDE), Oracle Key Vault, TLS / Native Network Encryption.	Encrypts sensitive data across its lifecycle, reducing risk of data breaches and enhancing compliance posture.
Art. 9(3)(a)	Secure data transfer mechanisms	TLS / Native Network Encryption.	Protects data in motion, reducing the risk of interception or tampering during transmission.
Art. 9(3)(b)	Prevent data loss, corruption, unauthorized access, and system flaws	Oracle Database Vault, Privileged Access Controls, Deep Data Security.	Enforces least privilege, separation of duties, and reduces likelihood of insider threats or misuse.
Art. 9(3)(d)	Protect against risks from data management and human error	Oracle Data Safe (user risk analysis), Database Vault, auditing policies.	Identifies risky users, enforces controls, and reduces impact of misconfigurations or human mistakes.
Art. 9(4)(a)	Information security policy covering data and ICT assets	Oracle Data Safe, Oracle Database Security Central, Oracle DBSAT.	Helps define, assess, and enforce consistent security policies across databases.
Art. 9(4)(b)	Network and infrastructure security; isolation during cyber-attacks	Database Security Central Database Firewall (SQL Firewall for 26ai databases), network segmentation, Zero Trust architecture.	Enables detection and blocking of malicious traffic and supports isolation of compromised systems.
Art. 9(4)(c)	Access control policies (least privilege, access rights management)	Oracle Identity & Access Management, Privilege Analysis, Oracle Database Vault, Oracle Deep Data Security.	Enforces strict access governance and reduces unauthorized access risks.
Art. 9(4)(d)	Strong authentication and cryptographic controls	Kerberos, PKI, RADIUS, Multi-factor authentication for local users, Advanced Security (TDE AES-256) and Oracle Key Vault.	Implements strong authentication and centralized key management for encryption.
Art. 9(4)(e)	Secure change management for ICT systems	Oracle Data Safe baselines drift reporting and alerts; Oracle Database Security Central baselines and drift reporting and alerts.	Enables controlled, auditable changes to database configurations and helps reduces risk of misconfigurations.
Art. 9(4)(f)	Patch and vulnerability management	Oracle Critical Patch Updates (CPU), Autonomous Database auto-patching.	Keeps systems up to date to help reduce exposure to known vulnerabilities with minimal operational overhead.
Art. 10	Implement detection mechanisms for anomalous activity and ICT incidents	Oracle Database Security Central auditing/monitoring and rule-based alerts; Oracle Data Safe Activity Auditing and Alerts; Enterprise Manager monitoring metrics.	Centralizes audit data, monitors database traffic in near-real-time to block SQL injection and provides interactive reports and alerts to detect and understand malicious behavior.

		Autonomous Database has proactive monitoring of events, service metrics and performance.	
Art. 11	Implement response and recovery measures to restore operations after ICT incidents	Data Guard failover/switchover operations; Zero Data Loss Recovery Appliance (ZDLRA) / Zero Data Loss Autonomous Recovery Service (ZRCV) for recovery readiness and validation. Autonomous AI Database built-in high availability, self-healing infrastructure and database provide automatic recovery for server and storage failures.	Database response and recovery capabilities are required to restore critical services after ICT incidents.
Art. 12	Develop and document backup policies and procedures, restoration, and recovery procedures to ensure the restoration of ICT systems with minimum downtime	ZDLRA / ZRCV enable validated backups and point-in-time recovery with subsecond RPO, continuous anomaly detection, immutability, and fast RTO via virtual full backups. Cyber Vault (air-gapped) and Clean Room / Isolated Recovery Environment support secure recovery; enforce separation of duties and encryption. Autonomous AI Database automates backups.	Provides high-performance, synchronized, and immutable backups that help mitigate ransomware risks. Enables data restoration with minimal loss and downtime to maintain business continuity.
Art. 13	Learn from incidents and tests and evolve controls accordingly	Database Security assessments with Oracle Data Safe, Oracle Database Security Central, or Oracle DBSAT posture assessment outputs.	Repeatable assessment and reporting enable evidence-based improvement of database controls over time.
Art. 24	Perform digital operational resilience testing as part of the ICT risk management framework	Data Safe and Database Security Central assessments as technical inputs; Data Safe masking and discovery features (for safer test data).	Testing programs often depend on safe data handling and configuration validation to remove avoidable weaknesses.

Implementation considerations

Organizations can use the mapping above as a control reference and translate it into an implementation plan based on database criticality, data sensitivity, and operational resilience requirements. A practical starting point is to identify the Oracle databases supporting critical or important functions and assess their security posture. From there, organizations can prioritize controls that reduce the highest-impact risks: encryption and key management for sensitive data, least-privilege and separation-of-duties controls for

privileged access, centralized auditing and monitoring for detection and evidence generation, and validated backup and recovery capabilities for resilience.

Financial entities may begin with security assessments using Oracle Data Safe, Oracle Database Security Central, or DBSAT; enforce data protection using TDE, TLS, and Oracle Key Vault; restrict privileged access using Oracle Database Vault and privilege analysis; centralize audit and monitoring through Oracle Data Safe, Oracle Database Security Central, and Unified Auditing; and validate recovery readiness using Oracle Data Guard, ZDLRA, or ZRCV. The output should be measurable evidence: assessment reports, configuration baselines, audit records, alert history, access reviews, backup validation results, and recovery-test outcomes.

Governance and compliance reporting

DORA establishes a supervisory framework in which financial entities must be able to demonstrate the effectiveness of their ICT risk management controls. During investigations or on-site inspections, regulators may expect evidence not only of defined security policies, but also of their consistent implementation and ongoing operation. The ability to show that database security configurations are regularly assessed, that deviations are identified and remediated, and that access and activity are comprehensively logged is central to this process.

Point-in-time audits — for example, a security assessment conducted once per year — may be insufficient on their own to demonstrate sustained control effectiveness. DORA emphasizes continuous monitoring, periodic review, and ongoing improvement of controls. As a result, financial entities would benefit from capabilities that support the generation of continuous compliance evidence, rather than relying solely on periodic assessment snapshots.

Compliance reporting

Oracle Data Safe is a unified, cloud-based security service that provides continuous assessment, monitoring, and governance of Oracle Database instances both on-premises, in Oracle Cloud Infrastructure, and multicloud.

Oracle Data Safe provides the following capabilities directly relevant to compliance evidence generation:

Data Safe Capability	Compliance Evidence Value
Security Assessments	Automated security assessments on scheduled basis; findings categorized as High, Medium, Low risk; delta reports highlighting configuration changes

	between assessment runs; timestamped, exportable PDF/HTML reports suitable for regulatory submission.
User Risk Assessments	Evaluation of all database user accounts against risk indicators: over-privileged roles, DBA role grants, password policies, default passwords, dormant accounts. Enables demonstration that user access rights are reviewed on a continuous basis.
Activity Auditing *Log collection & alerts*	Continuous collection and centralization of database audit logs, combined with pre-defined and custom alerting on suspicious activities such as privileged access, failed authentication spikes, bulk data movement, and unauthorized schema changes. Provides verifiable evidence of comprehensive activity monitoring, audit trail completeness, and timely detection of anomalous behavior for regulatory review.
SQL Firewall Violations Report	Centralized reporting of SQL Firewall violation events across managed databases, providing an aggregate view of attempted policy violations — input to incident detection and classification processes.
Data Discovery and Classification	Identification of sensitive data columns using predefined classifiers for financial, personal, and regulated data categories; feeds directly into encryption and access control policy decisions and provides data map evidence.
Data Masking	Evidence that sensitive data is systematically protected outside production environments through masking. Provides demonstrable controls for data minimization, non-production data protection, and reduced exposure of sensitive data in line with regulatory expectations.

Oracle Database Security Central provides enterprise-scale compliance reporting across heterogeneous database estates. Oracle Database Security Central built-in report library includes compliance-oriented reports to support common regulatory frameworks. For DORA specifically, Oracle Database Security Central supports the following reporting:

- **Privileged User Activity Reports:** Complete records of all DBA-level activity across the database estate, with session detail, executed commands, and objects accessed.
- **Data Access Reports:** Audit-quality records of which accounts accessed which tables, when, and what data was returned or modified.
- **Failed Login and Authentication Reports:** Consolidated view of authentication failures — essential input to DORA's incident classification process for detecting credential-stuffing or brute-force attacks.
- **Configuration Change Reports:** Records of all DDL and security configuration changes, timestamped and attributable to specific user accounts.
- **Cross-Database Correlation:** AVDF's correlation capability allows security analysts to reconstruct the full path of a suspicious activity across multiple database systems.

Illustrative examples

Example 1: A large EU banking group operates a hybrid Oracle estate (cloud and on-premises) with multiple transactional systems

A large EU banking group operates a hybrid Oracle estate spanning on-premises and cloud environments, supporting critical functions such as payments processing, lending systems, and customer data platforms. The organization needed to strengthen its ability to demonstrate consistent ICT risk management, resilient recovery capabilities, and continuous security monitoring across a distributed database landscape in line with DORA requirements.

Approach

- **Baseline Risk & Security:** Register and continuously assess all Oracle Databases with Data Safe for posture monitoring;
- **Resilient Backups:** Deploy ZDLRA on-prem and ZRCV in the cloud. Configure encrypted, immutable backup with automatic validations and frequent recovery drills.
- **Access & Privileges:** Restructure DBA roles and privileges using Privilege Analysis and Data Safe insights; Enforce separation of duties and privileged users access control using Database Vault.
- **Auditing:** Collect and centralize Unified Audit logs using Data Safe; monitor/alert on abnormal activity or privilege escalation.
- **Testing & Drills:** Schedule annual resilience tests using ZDLRA's restore validation features; document results and remediation actions.
- **Governance & Reporting:** Leverage Data Safe dashboards and ZDLRA compliance reports in risk committee meetings; produce evidence for supervisory review and incident reporting.

Outcome

The bank reports that it strengthened its alignment with DORA requirements while improving operational resilience, reducing recovery times, and increasing transparency for internal stakeholders and regulators.

Example 2: A European insurance provider centralizes audit and monitoring to help meet DORA reporting requirements

A large EU-based insurance group operates multiple Oracle databases supporting policy administration, claims processing, and customer data management across several Member States. The organization faced challenges in demonstrating consistent audit coverage and timely incident detection across distributed environments. In addition, strict data sovereignty requirements and internal "hold your own records" policies required that all monitoring, audit, and assessment data remain under direct control and not be transferred to external cloud services.

Approach

- **Centralized Audit & Monitoring:** Deploy Oracle Database Security Central to aggregate and manage Unified Audit data from Oracle Databases.
- **Activity Visibility & Alerting:** Configure alerting for high-risk activities, including privileged user access, anomalous query patterns, bulk data access, and failed authentication events.
- **Separation of Duties & Access Control:** Implement Database Vault to enforce least privilege and prevent unauthorized access to sensitive insurance and customer data, including restrictions on DBA activity.
- **SQL Threat Protection:** Enable SQL Firewall policies to monitor and block unauthorized or anomalous SQL traffic, reducing exposure to injection-based attacks.
- **Incident Detection & Reporting:** Use Database Security Central reporting and alerting capabilities to support identification, classification, and escalation of ICT-related incidents.
- **Compliance Evidence & Governance:** Generate scheduled audit reports and activity summaries to support internal audit, risk committees, and supervisory review; retain audit history to support forensic investigations and regulatory inquiries.

Outcome

The organization reports it improved its ability to detect and respond to database-related security events, strengthened audit trail consistency across environments, and enhanced its capability to produce timely, structured evidence for DORA-aligned incident reporting and supervisory review.

Conclusion

DORA represents a major shift in how financial institutions must manage and demonstrate operational resilience. Compliance is no longer defined by policies or periodic controls alone. It requires proving that systems remain secure, monitored, and recoverable under real-world conditions.

The database supports key business processes is an important enforcement point for security controls. Weaknesses at the database layer, including gaps in access control, audit visibility, data protection, or recovery readiness, can increase the impact of ICT-related events. Strong database-native controls may help organizations protect sensitive data, detect suspicious activity, preserve audit evidence, and support incident management.

Oracle Database can help organizations address these requirements through an integrated, database-native security architecture. Key capabilities include:

- **Access control and separation of duties:** Oracle Database Vault restricts privileged access and help reduce the risk of insider threats and unauthorized data exposure.
- **Data protection:** Transparent Data Encryption (TDE), Oracle Key Vault, and network encryption protect sensitive data across its lifecycle, supporting confidentiality and integrity requirements.
- **Monitoring and audit:** Oracle Database Security Central, Oracle Data Safe, and Unified Auditing provide continuous monitoring, centralized audit collection, and real-time alerting to support supervisory review and incident reporting.
- **Resilience and recovery:** Oracle Active Data Guard, Real Application Clusters (RAC), Oracle Zero Data Loss Recovery Appliance (ZDLRA), and Zero Data Loss Autonomous Recovery Service (ZRCV) deliver high availability, immutable backups, and rapid recovery.

Because these capabilities operate as part of a unified platform, enforcing controls close to the data and consistently across all access paths, organizations reduce reliance on fragmented external tools and strengthen their overall security posture.

DORA alignment is not a one-time project. It is an ongoing discipline. Oracle Database security solutions provide the technical foundation to continuously assess risk, validate recovery, and generate the evidence financial institutions need to demonstrate control effectiveness and build systems that are not just compliant, but resilient by design.

ORACLE

References

(1) **EU DORA Regulation (EU 2022/2554)**
https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32022R2554

(2) **Commission Delegated Regulation (EU 2024/1774)**
DORA RTS on ICT risk management tools, methods, processes, and policies
https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32024R1774

Learn more

- **Database Security: A Technical Primer – Seventh Edition (2026)**
  https://download.oracle.com/database/oracle-database-security-primer.pdf
- **Oracle.com for datasheets, technical briefs, FAQ, documentation, references, blogs, forums, and demonstrations for Oracle Database Security products:**
  https://www.oracle.com/security/database-security/
- **Oracle Blog: Securing Oracle AI Database 26ai for the Quantum Era**
  https://blogs.oracle.com/database/oracle-ai-database-26ai-pqc
- **Oracle Blog: Both is better - Oracle AI Database 26ai adds hybrid-mode quantum-resistant support**
  https://blogs.oracle.com/database/hybrid-pqc

Connect with us

Call **+1.800.ORACLE1** or visit **oracle.com**. Outside North America, find your local office at: **oracle.com/contact**.

blogs.oracle.com facebook.com/oracle twitter.com/oracle