Advanced Customer Services

Helping to Address EU General Data Protection Requirements Using Oracle Advanced Customer Services and Oracle Security Solutions

ORACLE WHITE PAPER | MARCH 2018

Disclaimer

The purpose of this document is to help organizations understand how Oracle security solutions can be utilized to help you comply with applicable European Union (EU) General Data Protection requirements. Some of the security solutions described in this document may or may not be relevant based upon an organization’s specific environment and needs. Oracle always recommends testing security solutions within your specific environment to ensure that performance, availability, and integrity are maintained.

Further, the information in this document is not intended and may not be used as legal advice about the content, interpretation or application of laws, regulations and regulatory guidelines. Customers and prospective customers should seek their own legal counsel about the applicability of laws and regulations to their processing of personal data, including the usage of any vendor’s products or services

Table of Contents

Introduction

With all the activity around the new EU General Data Protection Regulation (GDPR), some organizations are scrambling to understand the impact it will have, including but not limited to:

- Reviewing and modifying organizational processes, applications, and systems
- New and more stringent privacy and security requirements
- Potential fines up to 4% of annual revenue turnover and legal costs and recourse

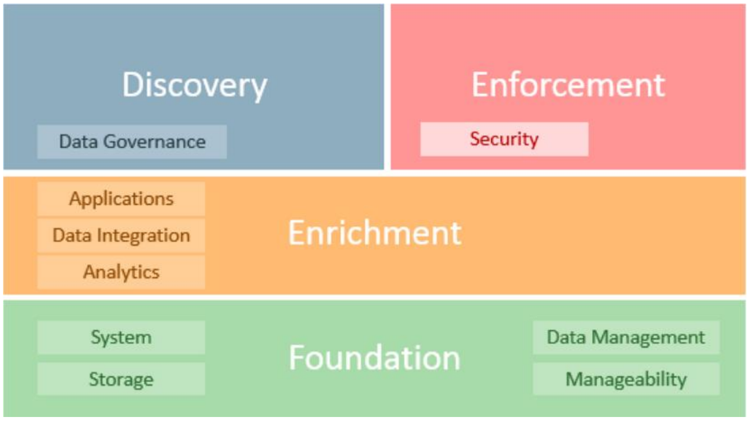
Addressing GDPR compliance requires a coordinated strategy involving different organizational entities, including security, IT, legal, human resources, marketing and others. The subject matter may involve information collected from various system users (e.g., customers and employees), as well as different technologies used. Organizations should therefore have a clear strategy and action plan to address the GDPR requirements with an eye towards the 25 May 2018 effective date.

Leveraging our experience built over the years and our technological capabilities, Oracle is committed to help customers implement a strategy designed to address many of their GDPR security requirements. This document explains:

- How Oracle Security solutions can be used to implement a security framework that can help address GDPR requirements
- How Oracle Advanced Customer Services may support partners and customers in order to enable Oracle security solutions

Oracle Solutions and GDPR

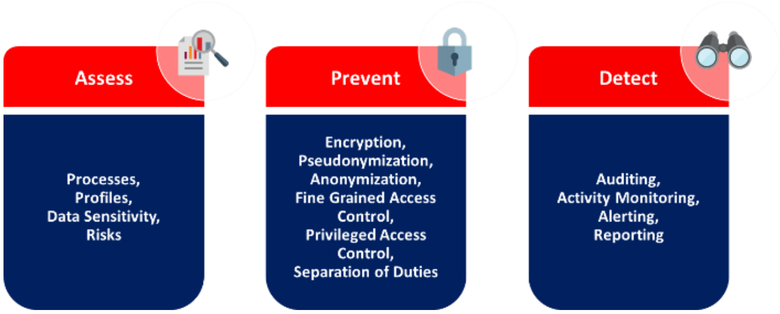
Oracle has an extensive value proposition to help our customers address their GDPR requirements involving data inventory, risk awareness, application modification, and architecture integration. The following diagram provides a high-level representation of Oracle's solutions framework, which includes a wide range of products and cloud services.



The white paper "Helping Address GDPR Compliance Using Oracle Security Solutions" available on the http://www.oracle.com/goto/gdpr area provides in depth details on Oracle Solutions to address discovery, enforcement, enrichment and foundation areas of focus. The following sections focus on Advanced Customer Services to support security enforcement.

Oracle Security Products that Can Help Address GDPR Requirements

Oracle provides on-premises and cloud security products for hybrid cloud environments that are designed to help protect data, manage user identities, and monitor and audit IT environments. These products and services address three main areas of focus for GDPR:



- The **Assess** pillar focuses on identifying the risks to personal data and laying out a clear course of action.
- The **Prevent** pillar captures the techniques, controls and mitigations to that can protect personal data.

- The **Detect** pillar highlights the reporting and audit requirements designed to ensure that unauthorized access to personal data is recorded and reported on so that further action can be taken in order to address accountability related requirements.

The following table provides a brief product description organized by the type of security measure. Each product provides more functionality than described, so be sure to ask your Oracle sales representative for more details.

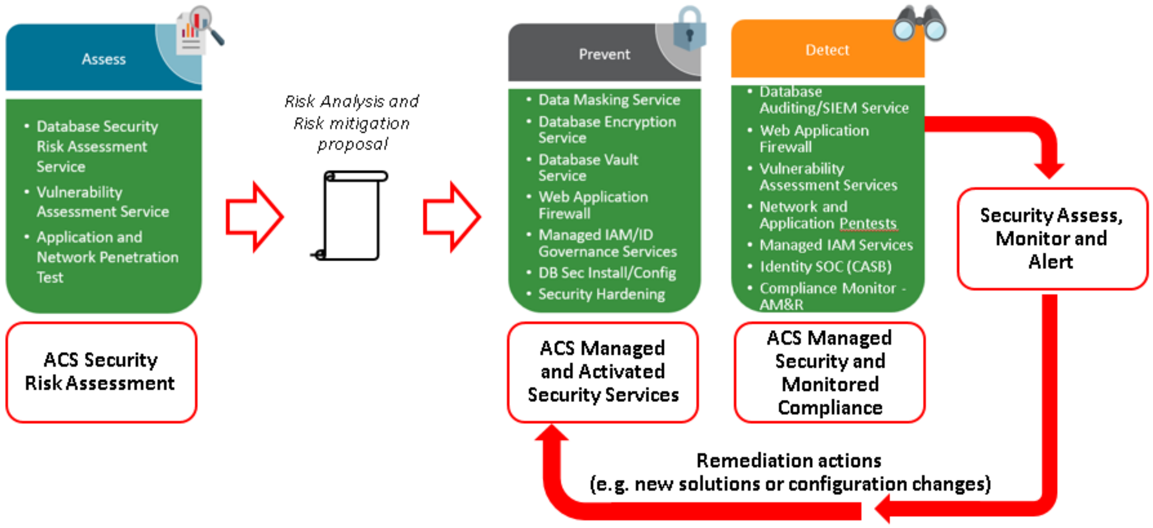
ORACLE SECURITY SOLUTIONS THAT CAN HELP ADDRESS GDPR

Oracle Product	Security Measure	Cloud Service	Short Description
Advanced Security	Protect the data		Encrypt Oracle Databases transparently and redact sensitive application data
Key Vault	Protect the data		Manage encryption key lifecycle as well as passwords, certificates and more.
Data Masking and Subsetting	Protect the data		Anonymize production data for testing and development environments.
Database Vault	Access controls		Control privileged user access using least privilege and separation of duties enforcement.
Identity Cloud Service	Access controls	X	Manage identities from the cloud for hybrid access, authorization, authentication, provisioning, and Single Sign On (SSO).
Identity Governance	Access controls		Manage the identity lifecycle: user administration, privileged account management, and identity intelligence.
Access Management	Access controls		IT asset protection and identity federation for multiple scenarios.
Directory Services	Access controls		Manage large, fast read-write user directories.
Label Security	Access controls		Allow individual data records to be labeled with metadata that describes the characteristics of the data, and then enforces access to those records based on the metadata.
Audit Vault and Database Firewall	Monitor, Block and Audit		Centralized auditing, monitoring, reporting, and alerting of anomalous database activity management.
Security Monitoring and Analytics Cloud Service	Monitor, Block and Audit	X	Monitor security incidents across heterogeneous and hybrid cloud environments.
CASB Cloud Service	Monitor, Block and Audit	X	Discover unsanctioned cloud services and implement consistent security policies across sanctioned SaaS, PaaS, and IaaS environments.
Configuration and Compliance Cloud Service	Secure Configuration	X	Implement and maintain continuous configuration and compliance settings for IT assets.
Enterprise Manager: Configuration Mgmt.	Secure Configuration		Check that IT assets are installed and configured in accordance with industry and Oracle recommended practices

Oracle Advanced Customer Services Can Help Address the GDPR Challenge

The first part of this white paper describes how Oracle provides security solutions for on-premises, hybrid, and cloud environments. The following part of the document describes how Oracle Advanced Customer Services (ACS) provide security services to deploy and manage Oracle security solutions, helping customers address their GDPR compliance. Detailed descriptions of ACS security services may be found on the Advanced Customer Services web page.

Oracle ACS offers proven security services that are specifically focused on managing these Oracle security solutions. These security services have been designed to address the three main pillars of GDPR security: **Assess, Prevent, and Detect**.


Assess
• Database Security Risk Assessment Service
• Vulnerability Assessment Service
• Application and Network Penetration Test
ACS Security Risk Assessment
Risk Analysis and Risk mitigation proposal
Prevent
• Data Masking Service
• Database Encryption Service
• Database Vault Service
• Web Application Firewall
• Managed IAM/ID Governance Services
• DB Sec Install/Config
• Security Hardening
ACS Managed and Activated Security Services
Detect
• Database Auditing/SIEM Service
• Web Application Firewall
• Vulnerability Assessment Services
• Network and Application Pentests
• Managed IAM Services
• Identity SOC (CASB)
• Compliance Monitor - AM&R
ACS Managed Security and Monitored Compliance
Security Assess, Monitor and Alert
Remediation actions
(e.g. new solutions or configuration changes)

Oracle ACS offerings are focused on both database and application security designed to protect against threats both to the data layer and the application points of access and associated vulnerabilities. Understanding that customers may have both Oracle Cloud and on-premises deployments, ACS security services apply to both deployment options.

As well as offering services for all deployment options, Oracle ACS also provides flexibility on consumption of security services with two methods of delivery.

» **Managed Security Services** provide both implementation of Oracle security and continuous monitoring, management, and reporting 24/7, designed to help ensure that the implemented security features and services remain effective, not just effective at a point in time.

Managed Security Services are proven in assisting customers with ongoing security challenges by providing the industry expertise, process experience and advanced tooling and monitoring to manage Oracle security end-to-end for our customers. Managed Security Services cover both database and application security providing a wide range of security services to protect your personal data from the point of application access right through to the data layer.

For example, using “Managed Database Audit” not only is Oracle Database Audit Vault installed and configured against the target database(s) but it is also connected into Oracle ACS’ central Security Incident and Event Monitoring system to filter events and raise alerts on anomalous access attempts. Reports and service management review meetings provide oversight of these events and recommendations for next step actions. Managed Security Services are available for all three pillar categories of GDPR: Assess, Prevent, and Detect.

- **Security Activation Services** – Customers who prefer to manage database security themselves can opt to subscribe to ACS security implementation/activation services where the security product is installed and configured and following successful completion of the activation project, the customer becomes responsible for on-going management and monitoring of the security solution. These are one-time services that provide one-time activation of Oracle database security and associated features according to Oracle and industry recommended practices for: Database Encryption, Database Audit Vault and Database Firewall, Key Vault, Database Vault, Database Label Security, Database Subsetting, and Masking.

  Security Activation services focus on the prevent pillar with supporting services in the detect pillar of GDPR. Which Oracle Security solutions are these services targeted at? Oracle database and database security options, Oracle Audit Vault and Database Firewall, Oracle Enterprise Managed Data Masking and Sub-setting, Oracle Management Cloud Security Monitoring and Analytics and Configuration and Compliance, Oracle Identity Management Suite, Oracle Identity Cloud Service, and Oracle Cloud Access Security Broker (CASB).

  As standard all ACS security services are delivered remotely.

Assess Pillar: ACS Security Assessment Services

To assess the vulnerabilities in an Oracle database or in an Oracle platform, ACS recommends an initial risk and/or vulnerability assessment to establish the risk profile and provide recommendations to further protect the application and database.

Oracle Database Security Risk Assessment

The “Oracle Database Security Review” service is a comprehensive database analysis and configuration review, designed to address security vulnerabilities according to industry and Oracle recommended practices and to identify Oracle Database security options and products on order to manage identified vulnerability issues.

This database technical assessment provides answers to many database security questions:

- Have you verified that your database is configured according to Oracle security recommended practices?
- Have you identified and fixed all the critical security patches and upgrades that place systems at risk?
- Are proper security logging and auditing techniques in place?
- Is there a mitigation plan available to deal with security critical issues?

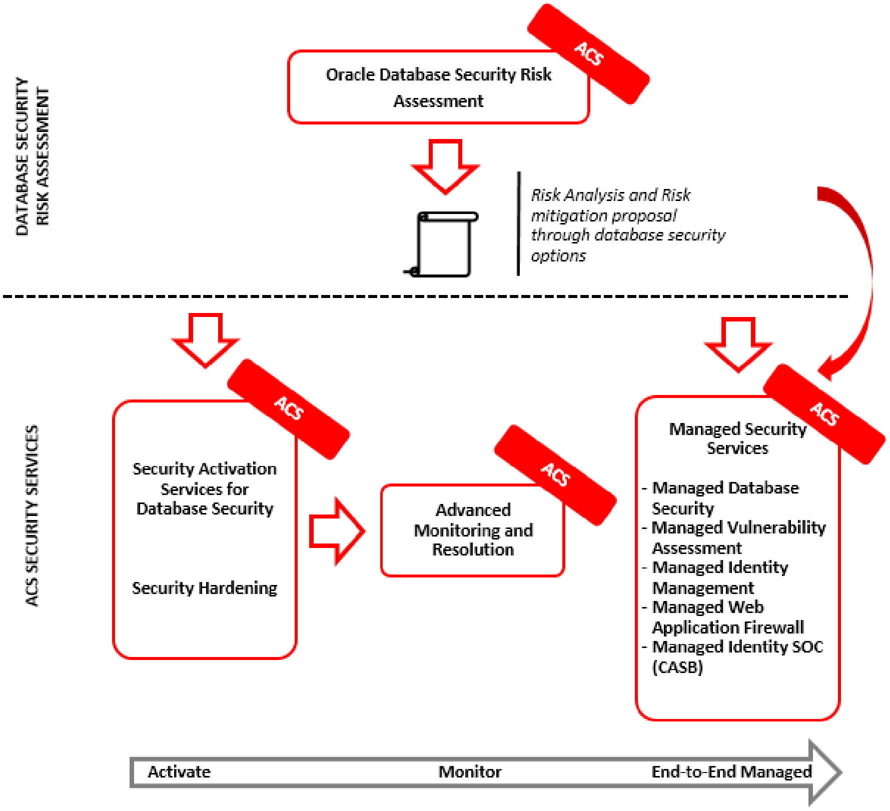
Areas reviewed are shown in the following table.

Database Assessment Category	DBSRA Included
Installation and Patching	🟢
Oracle Software File and Directory Permissions	🟢
Database User Access	🟢
Roles & Privileges	🟢
Database Parameter Settings	🟢
Database Profile Settings	🟢
Auditing and Logging	🟢
Public Objects Review	🟢
System Connections	🟢
Restricted Super-User (SYS) Tables/Views	🟢
Database Tablespace Storage	🟢

Risk Profile and Remediation Recommendations

Two deliverables are provided as part of this service and delivered in password protected encrypted format: An Executive Summary Report highlighting key findings with severity and remediation steps and a Detailed Technical Report with assessment checks and results providing an audit report of the assessment process. This service is delivered remotely using specialized tools and highly skilled Oracle engineers.

The risk assessment highlights areas of risk and supporting services recommended to address those risks, as the following flow diagram shows.


DATABASE SECURITY
RISK ASSESSMENT
Oracle Database Security Risk Assessment
ACS
Risk Analysis and Risk mitigation proposal through database security options
ACS SECURITY SERVICES
ACS
Security Activation Services for Database Security
Security Hardening
ACS
Advanced Monitoring and Resolution
ACS
Managed Security Services
- Managed Database Security
- Managed Vulnerability Assessment
- Managed Identity Management
- Managed Web Application Firewall
- Managed Identity SOC (CASB)
Activate
Monitor
End-to-End Managed

Further assessment services are available to provider wider security risk assessment beyond the database context:

- **Web Application Vulnerability Assessment Service -** Periodic vulnerability scans are executed against internet facing web applications to detect vulnerabilities using specialized tools. Customer is provided with the raw scan report, technical, and executive summary reports along with recommendations and remediation guidance
- **Vulnerability Assessment Service -** Periodic vulnerability tests are executed against internal facing hosts using specialized tools. Customer is provided with the raw scan report, technical, and executive summary reports along with recommendations for remediation and tracking of existing remediation activities
- **Penetration testing -** Application and Network Penetration Test performed by an Oracle ethical hacking team. Detailed test report is provided.

Prevent Pillar: ACS Security Prevention Services

Security hardening is the first and mandatory activity that must be executed to secure databases, systems, operating systems, etc. For customers taking ACS Managed Applications or PaaS Services Security Hardening is built into the service. For customers wishing to manage their own applications or databases a Security Design and Hardening activation service is available.

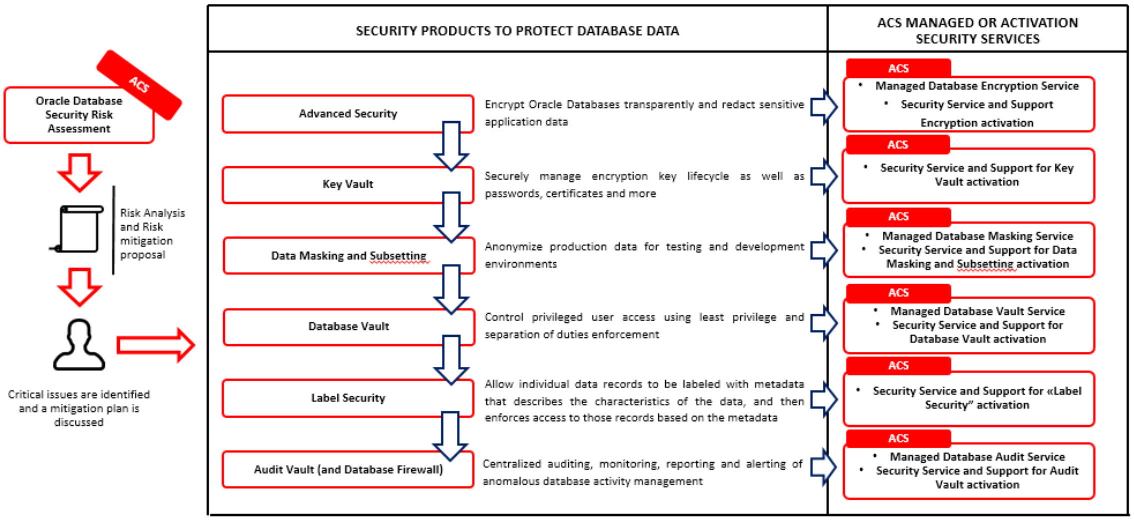
Oracle Database Security Design Support and Hardening Support

Database Hardening is a database tuning technique, based on recommended security practices, designed to close off common vulnerabilities. The process checks and ensures that default passwords, system ID's, and ports have been changed. The tuning also involves checking and removing unnecessary packages and installing DB security patches. Useless or vulnerable services are disabled and password enforcement and public privileges are scrutinized. Logging and auditing techniques are also examined, and settings modified as required.

The focus of the service is to harden Oracle Database, Oracle Exadata, Oracle SuperCluster and/or Oracle Operating System Security Configurations.

Following security hardening, focus shifts to measures to data protection and control of access to data using Oracle security products and solutions that have been identified during the security risk.

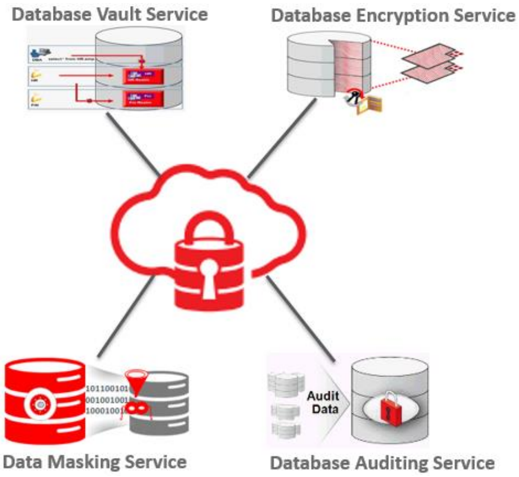
The following diagram provides an overview highlighting the mapping between Oracle database security options and products (that address GDPR issues) and ACS security services to manage or activate them.


ACS
Oracle Database Security Risk Assessment
Risk Analysis and Risk mitigation proposal
Critical issues are identified and a mitigation plan is discussed

SECURITY PRODUCTS TO PROTECT DATABASE DATA		ACS MANAGED OR ACTIVATION SECURITY SERVICES
Advanced Security	Encrypt Oracle Databases transparently and redact sensitive application data	ACS • Managed Database Encryption Service • Security Service and Support Encryption activation
Key Vault	Securely manage encryption key lifecycle as well as passwords, certificates and more	ACS • Security Service and Support for Key Vault activation
Data Masking and Subsetting	Anonymize production data for testing and development environments	ACS • Managed Database Masking Service • Security Service and Support for Data Masking and Subsetting activation
Database Vault	Control privileged user access using least privilege and separation of duties enforcement	ACS • Managed Database Vault Service • Security Service and Support for Database Vault activation
Label Security	Allow individual data records to be labeled with metadata that describes the characteristics of the data, and then enforces access to those records based on the metadata	ACS • Security Service and Support for «Label Security" activation
Audit Vault (and Database Firewall)	Centralized auditing, monitoring, reporting and alerting of anomalous database activity management	ACS • Managed Database Audit Service • Security Service and Support for Audit Vault activation

Managed Security Services

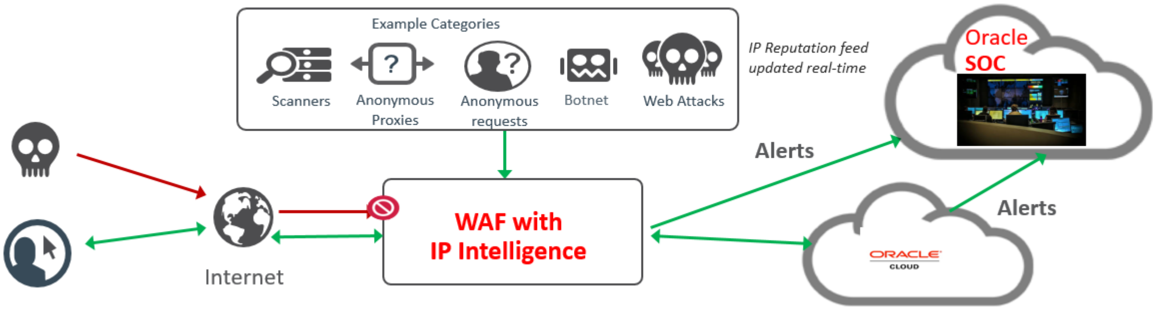
The following ACS Managed Security Services are designed to install, design and configure, and deploy a specific Oracle security solution (e.g. transparent encryption, masking, etc.) but also to provide an “end-to-end” management of the Oracle security solution itself, ensuring that the controls implemented are effective not just at the point of configuration but for the duration of the service:



- **Managed Security Database Encryption Service** – Designed to protect your sensitive personal data using the Oracle Transparent Data Encryption (TDE) database security feature, this service provides complete management, monitoring and reporting of TDE including patching and key management.
- **Managed Security Database Vault Service** – Enables segregation of duties and specific role based access to database domains using Oracle Database Vault. This service includes the design of domains and realms, access testing, management, monitoring and reporting.
- **Managed Security Data Masking Service** – Addresses the challenge of personal data moving from production to non-production environments as part of standard project lifecycle activities. Anonymizing data in required as part of this process to ensure non-privileged access to personal data is avoided in project environments. This one-time setup service manages the creation and test of data masking scripts to mask your personal data and integrates these scripts into the ACS Oracle Enterprise Manager (OEM) Data Subsetting and Masking based refresh process. Once integrated into OEM database refreshes from production to non-production will have data masking applied.

Securing personal data at the database level is a security fundamental. Additionally, attacks through the point of application access and vulnerabilities in the environment running the database and application should also be addressed. Managed Application Security Services address these areas by providing robust ongoing security solutions to protect applications from external attack and provide vulnerability assessment and integrity monitoring of the application environment.

- **Managed Identity Security Services** – Identity management provides a key role in addressing authentication, authorization and governance of users accessing applications containing personal data. However, Identity Management can be complex to configure without skilled resources. ACS Managed Identity Security Services have been developed over many years to enable customer to uptake Oracle Identity Management solutions including Identity Cloud Service without the need to develop an internal competency to setup and manage ongoing Oracle's underlying identity products and services. Further details on Managed Identity Security Services can be found on the Advanced Customer Services web page.
- **Managed Security Web Application Firewall Service** – Help protect your internet-facing applications from attack. This service includes Web Application Firewall policy setup, monitoring and integration into ACS SIEM, management and ongoing reporting of alerts.



- **Oracle Managed Security File Integrity Monitoring Service**: Oracle Managed Security File Integrity Monitoring Service is designed to monitor, and provide alerts of, unauthorized changes to certain system and application files that could be a sign of a possible compromise to the customer services environment.

Further details on Managed Database Security Services can be found at the Oracle Managed Security Services for Oracle Cloud and On Premises data sheet.

Detect Pillar: ACS Security Detection Services

During the Assess and Prevent phases security risk analysis highlighted services to prevent access to sensitive data.

The third phase is focused on providing continuous security monitoring, audit, and mitigation and remediation planning of the target systems to detect malicious or non-authorized access to that sensitive data.

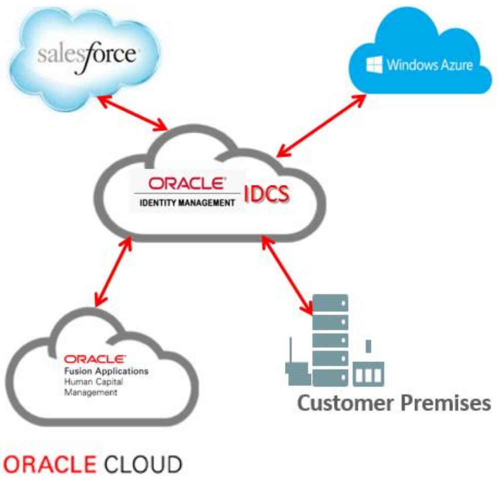
One of the challenges in implementing security is to ensure that the technical features enabled are installed and configured correctly to industry and Oracle recommended practice standards and are monitored and managed on an ongoing basis. It is important to verify that the target system does not become affected by security weaknesses over time e.g. application of patches additional configuration updates etc.

Managed Security Services

Managed Security Services have been designed to protect your key data assets auditing access to databases containing those assets with a fully managed security service (all complete end-to-end lifecycle):

- **Managed Security Database Audit Service** – Provides a complete audit service, detecting and alerting privileged access to your databases using Oracle Audit Vault. This service provides Audit Vault installation, design, configuration, test, management, ACS SIEM alerting integration, monitoring, and reporting
- **Managed Security Vulnerability Assessment Service** – Enables the environment running your application and database to have regular vulnerability assessments of the service infrastructure, detecting vulnerabilities and providing recommendation to remediate. This service includes regular vulnerability scans, scan reporting both at technical and executive summary level, remediation recommendations, and tracking of remediation activities.
- **Managed Security File Integrity Monitoring Service** – Help protect application and environment files from compromise by monitoring and alerting on unauthorized changes. This service includes the setup of policies to monitor files relating to the application and database environment, ongoing monitoring and alerting of unauthorized changes.
- **Managed Identity Management Service** – Applicable to both prevent and detect pillars, this service delivers a managed identity service from configuration through to ongoing run and maintain activities for Oracle Identity Cloud Services and Identity Suite products. Identity management and governance allows control and reporting of user authentication and authorization events.
- **Managed Identity SOC (CASB)** – Provides configuration, management and managed Security Operations Center service for Oracle Cloud Access Security Broker cloud service, addressing threats and non-compliance issues for users accessing cloud applications.

Further details on Managed Security can be found on the Advanced Customer Services web page.


salesforce
Windows Azure
ORACLE IDENTITY MANAGEMENT
IDCS
ORACLE Fusion Applications Human Capital Management
Customer Premises
ORACLE CLOUD

Compliance Monitoring Services

- **Oracle Advanced Monitoring and Resolution:** Oracle Advanced Monitoring and Resolution–Advanced Database Support helps you maximize the availability, performance, and security of your Oracle databases (10*g* or higher) with 24/7 remote database fault monitoring, accelerated response times, proactive database health checks, database security compliance reporting, remote patch deployment, and an easy-to-use service dashboard.

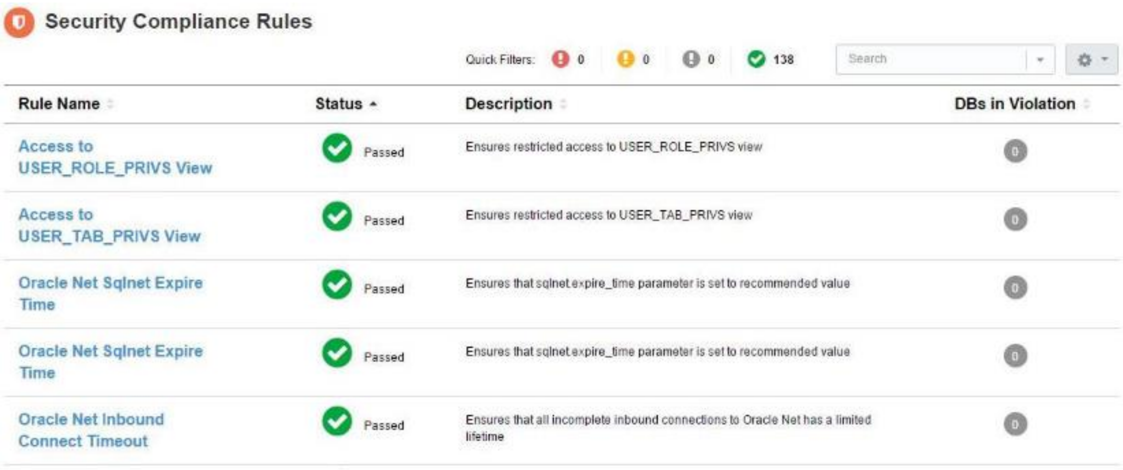
  Oracle Database Security Compliance Reporting compares your covered databases against Oracle security recommended practices for database configuration, directory and file permissions, and user access.

  Real-time status reporting of potential database issues, security compliance issues and Oracle Critical Patch Updates (CPUs) help mitigate database risks and complications. By maintaining the database at current patch levels, you can further remove complexity from supporting your database environment.

  An intuitive service dashboard is available on the Oracle Advanced Support Portal. This user interface allows a complete view of your Oracle database including:

  - Service request view: Listing and status of service requests for the monitored databases. Drill-down views to view and interact with a service request.

- Oracle database view: Listing and status of the Oracle databases including type, host name, and version. Drill-down views for database status such as space information, CPU utilization or service request status.
- Proactive database advisory view: Showing the database security compliance report, which provides details on any specific database security rules violations and number of critical patches (i.e. quarterly security Critical Patch Updates) applicable to monitored databases. Drill-down views link to specific patch sets.
- Database security compliance report: providing details on any specific database security rules violations.
- Number of critical patches (i.e. quarterly security Critical Patch Updates) applicable to monitored databases. Drill-down views link to specific patch sets.



Security Compliance Rules

Rule Name	Status	Description	DBs in Violation
Access to USER_ROLE_PRIVS View	✓ Passed	Ensures restricted access to USER_ROLE_PRIVS view	0
Access to USER_TAB_PRIVS View	✓ Passed	Ensures restricted access to USER_TAB_PRIVS view	0
Oracle Net Sqlnet Expire Time	✓ Passed	Ensures that sqlnet.expire_time parameter is set to recommended value	0
Oracle Net Sqlnet Expire Time	✓ Passed	Ensures that sqlnet.expire_time parameter is set to recommended value	0
Oracle Net Inbound Connect Timeout	✓ Passed	Ensures that all incomplete inbound connections to Oracle Net has a limited lifetime	0

Use Case Example

The following business use case is intended to illustrate how Oracle products and Oracle Advanced Customer Services can be used to make IT systems more secure and help address the EU GDPR.

The use case addresses an on-premises deployment scenario. Equally the services presented apply to an Oracle Cloud OCI or PaaS deployment model or a hybrid mix of on premise and Oracle Cloud including Cloud at Customer.

Business use case: Healthcare

The fictional organization is a large private hospital. The management of the hospital requests to a security consulting company an assessment of hospital data and processes with the following business objectives:

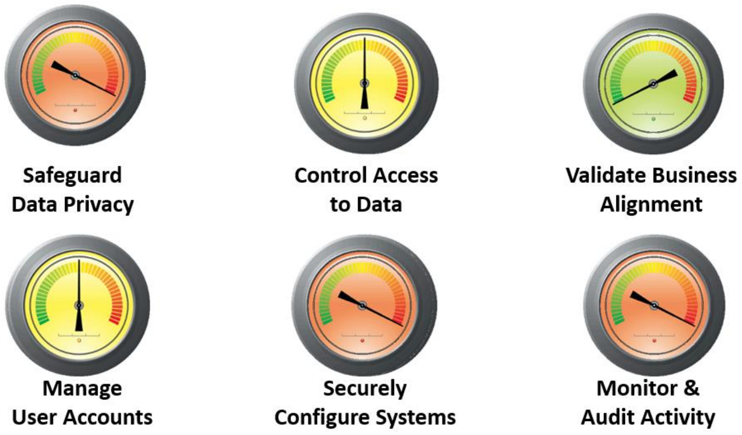
- Enable compliance with national and regional laws, including GDPR
- To be perceived as a secure and modern company, respectful of patient privacy

The security consulting team interviews hospital personnel and outsourcers identifies an Oracle E-Business suite application deployment including Oracle database with sensitive personal data (from the security point of view) stored. The E-Business application has personal data on employees, patients and also supplier data and is accessed by suppliers using the internet facing iSupplier Portal.

The security team requests an Oracle database security risk assessment from Oracle ACS to verify that security recommended practices are applied to the E-Business Suite database configuration.

Oracle ACS execute a database security risk assessment (DBSRA) performed using ACS specific tools and methodologies.

Oracle ACS produces executive and technical reports that are used to define a prioritized action plan with recommendations to remediate security risks discovered. Additionally, this data is presented in a dashboard format giving a comparative view of which security areas require immediate action (see figure below). The reports produced by the DBSRA are stored as a key component of the GDPR adjustment project to help demonstrate company accountability (as per GDPR Art. 24) and may be presented to the Board of Directors by the Data Protection Officer.



First Step – Prevent Services

The DBSRA recommendations lead to identifiable actions to address database security. For example:

- **Migrate to Oracle Database 12*c* from unsupported version 11**. A key part of providing a secure foundation for any application is to ensure that the latest version of underlying database is used. The ACS Database Upgrade Service was selected to take the E-Business suite database from version 11 to 12*c*.
- **Database Encryption and privileged access control using Managed Security Database Encryption and Database Vault Services**. The healthcare organization decided to encrypt database data. Managed Database Encryption service designs and enables database encryption using Oracle Advanced Security Option Transparent Database Encryption (TDE) (suggested in Art. 32) and provides ongoing management of TDE including key management, patching advisory, and regular reporting of encryption status.

  Restrictions on privileged access to database HR data is required and access restricted to privileged application users. The Managed Database Vault service was selected to design and implement the Oracle Database Vault option and managed ongoing the access realms created as part of this service.
- **Centralize database user accounts**. The organization centralized all database user accounts into a directory using a feature of the database called Enterprise User Security and an existing instance of an Oracle directory.
- **Mask data in non-production environments using Oracle Data Masking Activation Service**. The organization identified the need to eliminate access to personal HR data that was being copied from production environments to development and test. That was achieved using the Managed Data Masking Activation Service using Oracle Enterprise Manager Data Masking and Subsetting pack.
- **Re-activate logging mechanisms that had not been used for years.** Log production and analysis lays at the base of any security strategy. The organization chose to collect database logs with Oracle Audit Vault, and

systems logs with Oracle Log Analytics Cloud Service. Oracle Storage Cloud Services was then used to reduce the on-premises footprint of Audit Vault and applications log storage. Some applications have been modified to pass application user data to the database and is being used to provide accountability and an improved logging analysis. The logs are sent to Oracle ACS Security Operation Center in order to allow alerting, monitoring, and reporting.

- **Managed Security Web Application Firewall Service:** To help ensure the internet facing iSupplier Portal is protected from attack by malicious actors, Web Application Firewal (WAF) is configured to protect this application. WAF alert and log data is integrated with the ACS SIEM to ensure unauthorized access attempts are captured and can be actioned.

Second Step – Detect Services

The first step (engage ACS to manage Oracle security technologies) applied prevention services to the E-Business production and non-production databases.

The hospital Chief Information Security Officer (CISO) was also concerned that ongoing vulnerabilities and audit of the E-Business environments were taken into account. As security is a continual process rather than a point in time activity the customer was reassured that Oracle ACS has services that address this challenge by providing 24/7 vulnerability assessment and audit services.

Following discussion and recommendations from Oracle ACS the CISO mandated the inclusion of the following Managed Security Services to meet the systems ongoing risk requirements:

- **Managed Security Database Audit Service** – using this service the hospital is able to take advantage of a complete audit service detecting and alerting privileged access to its databases using Oracle Audit Vault. This service provides ACS SIEM alerting integration, monitoring and reporting.
- **Managed Security Vulnerability Assessment Service** – provides on-going vulnerability assessment of the environment in which the applications and database are running. This is a key service to ensure vulnerabilities do not get introduced into the environments weakening the overall security controls put in place. Quarterly or monthly Internal and External Vulnerability Assessment services. Customer is provided with the raw scan report, technical, and executive summary reports.

At the end of the security review, the hospital can show to security auditors:

- Technical security risk assessment reports
- A detailed technical mitigation plan to improve security on database instances where sensitive data are stored
- Attestation reports for Database Encryption and Database Vault
- An ongoing managed service to address vulnerability assessment and remediation of findings
- Continuous ongoing managed security reporting as part of the Managed Security Services for Database Encryption, Database Vault, Database Audit, Vulnerability Assessment and Web Application Firewall

In this way the hospital is able to demonstrate the many remediation actions (limited to Oracle databases) that have been done or planned to improve personal data security.

Conclusion

Non-compliance with GDPR can result in heavy fines and increased regulatory actions. More importantly, however, security breaches can damage an organization’s brand, value, and reputation. Protecting the brand requires that an organization that collects personal data must implement the GDPR requirements that apply to its operations.

Leveraging our experience built over the years and our technological capabilities, Oracle Advanced Customer Services is committed to help our customers implement a strategy using Oracle products and services designed to address many of their GDPR security requirements

Based on our experience and technological capabilities, Oracle is committed to help customers with a strategy designed to achieve GDPR security compliance. To learn more about how Oracle can help, please contact your local sales representative and visit https://oracle.com/goto/gdpr

ORACLE®

Oracle Corporation, World Headquarters
500 Oracle Parkway
Redwood Shores, CA 94065, USA

Worldwide Inquiries
Phone: +1.650.506.7000
Fax: +1.650.506.7200

CONNECT WITH US

blogs.oracle.com/oraclesecurity
facebook.com/oraclesecurity
twitter.com/oraclesecurity
oracle.com/security

Integrated Cloud Applications & Platform Services

Helping Address General Data Protection Requirements (GDPR) Compliance Using Oracle Advanced Customer Services and Oracle Security Solutions
March 2018
Author: Giancarlo Colla
Contributing Authors: Phil Sidebotham

Oracle is committed to developing practices and products that help protect the environment