Le misure di sicurezza, i problemi sul tavolo e le prime cose da fare

Alessandro Vallega
Security Business Development Oracle Europe WCEs
Clusit Board of Directors
Oracle Community for Security Chairman
Founder of EuroPrivacy.info

ORACLE

General disclaimer

The following is intended to outline our general product direction. It is intended for information purposes only, and may not be incorporated into any contract. It is not a commitment to deliver any material, code, or functionality, and should not be relied upon in making purchasing decisions. The development, release, and timing of any features or functionality described for Oracle's products remains at the sole discretion of Oracle.

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 use of any third party service, including Oracle public Cloud services.

GDPR

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)

Accountability

- Art. 5.2: The controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1 (‘accountability’).
- Art. 24 Responsibility of the controller: be able to demonstrate that processing is performed in accordance with this Regulation.

Audit

- Art. 28 (ma 3.h. The process and contribu
- Art. 39 (a protection officer) O has the task to (related audits;
- Art. 58 (upervisor authorit) to carry out inve *form of data pro*

Key concepts

Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including inter alia as appropriate:

(a) the pseudonymisation and encryption of personal data;

(b) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;

(c) the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;

(d) a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

Art. 32 Security of Processing

Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including inter alia as appropriate:

(a) the p[illegible]

(b) the [illegible] processing syste[illegible]

(c) the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;

(d) a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

Controller = our customer

Processor = its oursourcer or cloud provider

Technical measures for processors = embedded in "our products"

Appropriate to the risk = use a lot of intelligence

Art. 32 Security of Processing

Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including inter alia as appropriate:

State of the art = what's good today may not be enough tomorrow → Security in the Architecture

Costs of implementation = balance of interests and Security in the Architecture

Likelihood and severity → risk attitude, assessment, DPIA

(a) t… c…

(b) t… i… a… essing s…

(c) the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;

(d) a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

Art. 32 Security of Processing

Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including inter alia as appropriate:

(a) the pseudonymisation and encryption of personal data;

(b) the abili[illegible] ensure the ongo[illegible] confidentiality, integrity, availability and resilience of processing syste[illegible]

(c) the [illegible] ss to personal data in a timely manner in the event of a ph[illegible]

(d) a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

Inter alia = among other; for example

Encryption = Advanced Security and other (...)

Art. 32 Security of Processing

Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the co[illegible]cessor shall implement appropriate technical and organisational measu[illegible] of security appropriate to the risk, including inter alia as appropriate:

Confidentiality, Integrity → Security Solutions

(a) the pseudonymisation and encryptio[illegible] personal data;

(b) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;

(c) the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;

Availability → HA, BC, DR products, example ZDLRA

(d) a process for regularly testing, assessing and evaluating th[illegible]chnical and organisational measures for ensuring the security of the pr[illegible]

Art. 32 Security of Processing

2. (…) risks (…) in particular from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed.

3. Adherence to an approved code of conduct (…) or an approved certification mechanism (…) may be used as an element by which to demonstrate compliance with the requirements set out in paragraph 1 of this Article.

There is still a lot to be defined

But there will be a large use of:
- **Risk analysis**
- **Security best practices**
- **Security concepts**
- **Security professionals**

Art. 32 Security of Processing

- Strong / Multilevel / Federated Authentication
- Adaptive / Fine Grained Access Control
- Segregation of Duties
- Need to Know / Least Privilege
- Accountability / Log Management

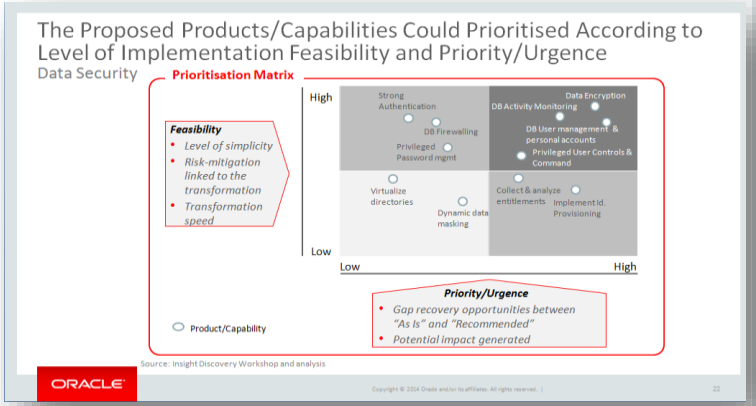
- Encryption
- Anonymization and Pseudinymization
- Segregation of Environment
- Secure Configuration Management / Hardening
- Attestation & Role Management

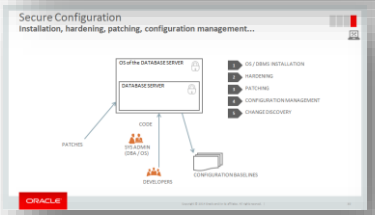
Some security best practices

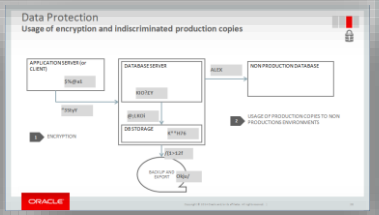
WHEN DID YOU REVIEW YOUR ORACLE DATABASE FOR SECURITY THE LAST TIME?

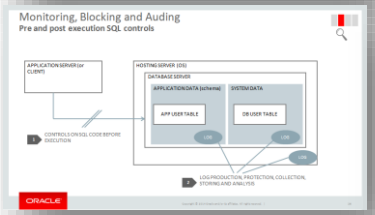
Are you worried about "Loss of Confidentiality", "Loss of Integrity", and "Loss of Availability" and impact on the Company ability to execute its business, be fined or suffer a fraud with economical consequences?

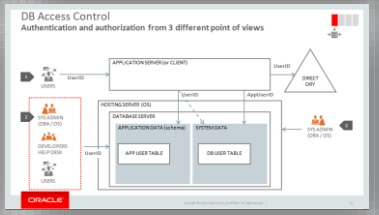
Oracle offers you a free evaluation of your database security!





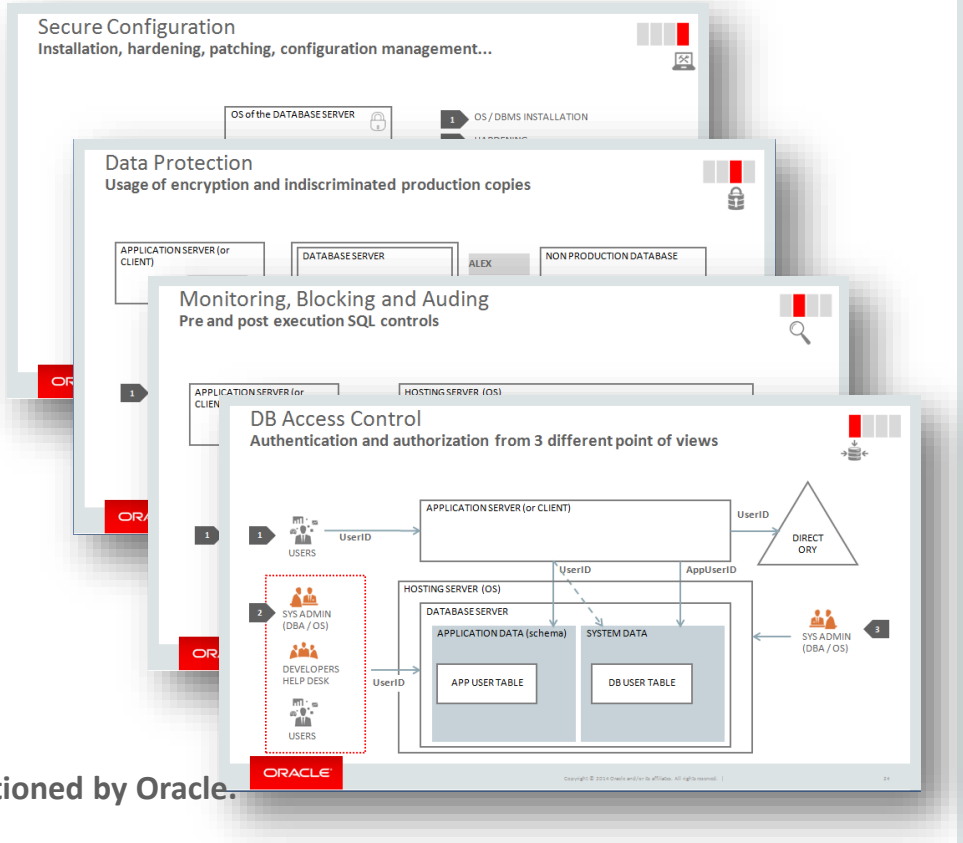






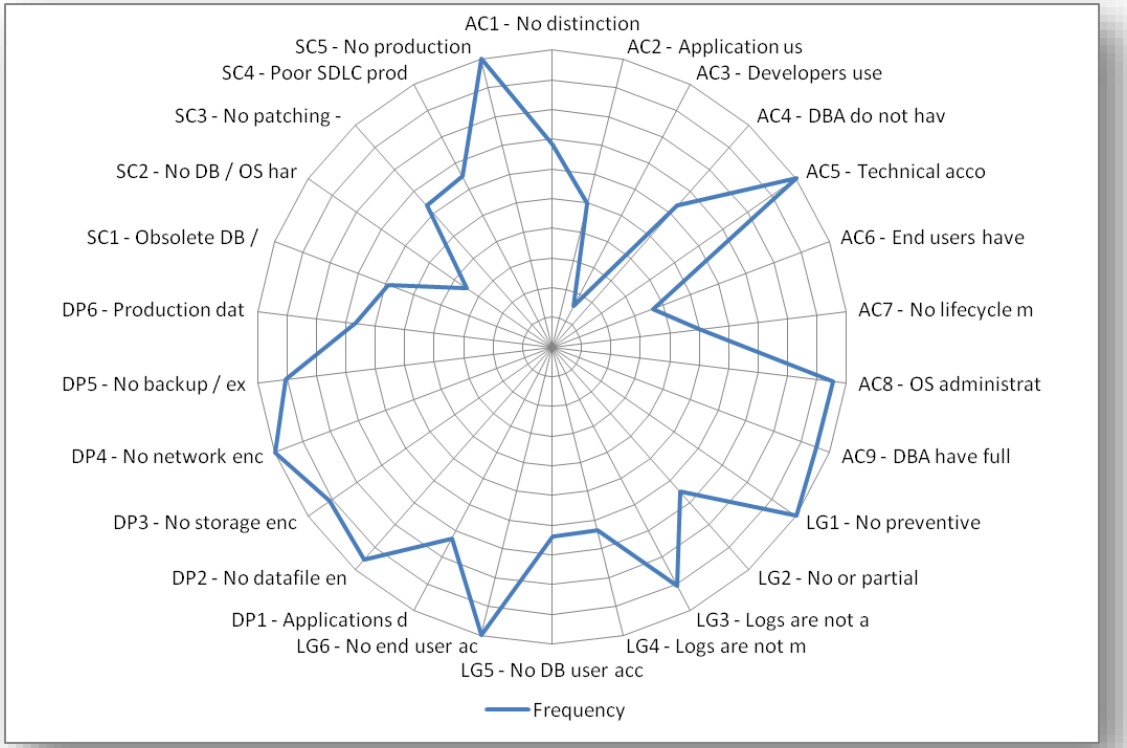
Database Security Maturity Evaluation and Assessement

- From DBSecurity Maturity Evaluations / Assessments
- More info*:
  - A 6 pages document in Italian with Most Common Mistakes http://bit.ly/MCM2016b (this is part of the Clusit ICT Security Report 2016)
  - A 30' video on MCM
    - YouTube (in Italian) http://bit.ly/MCMVIDEO



* **Note that these are third-party resources not officially sanctioned by Oracle.**

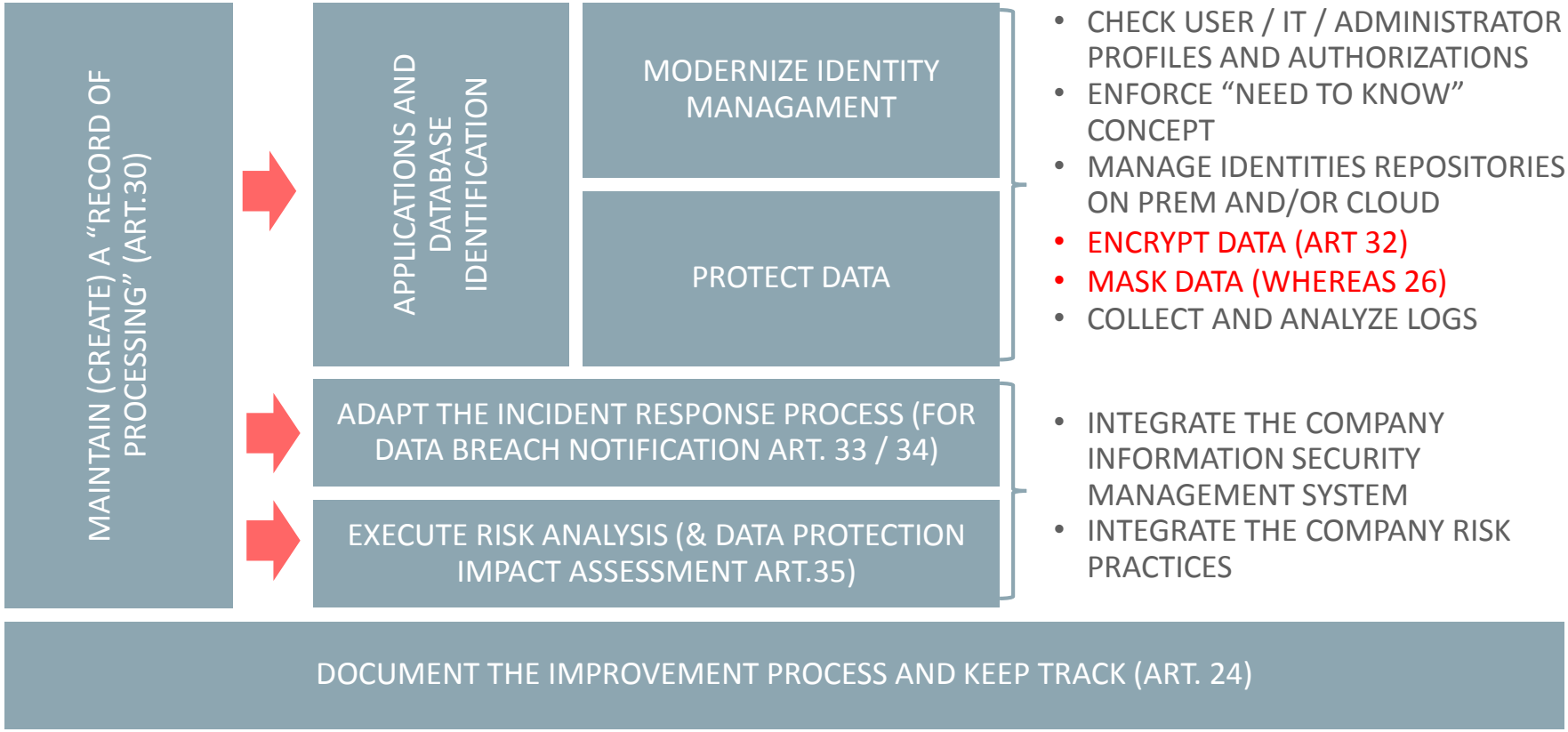
We have been told that there is much room for improvement



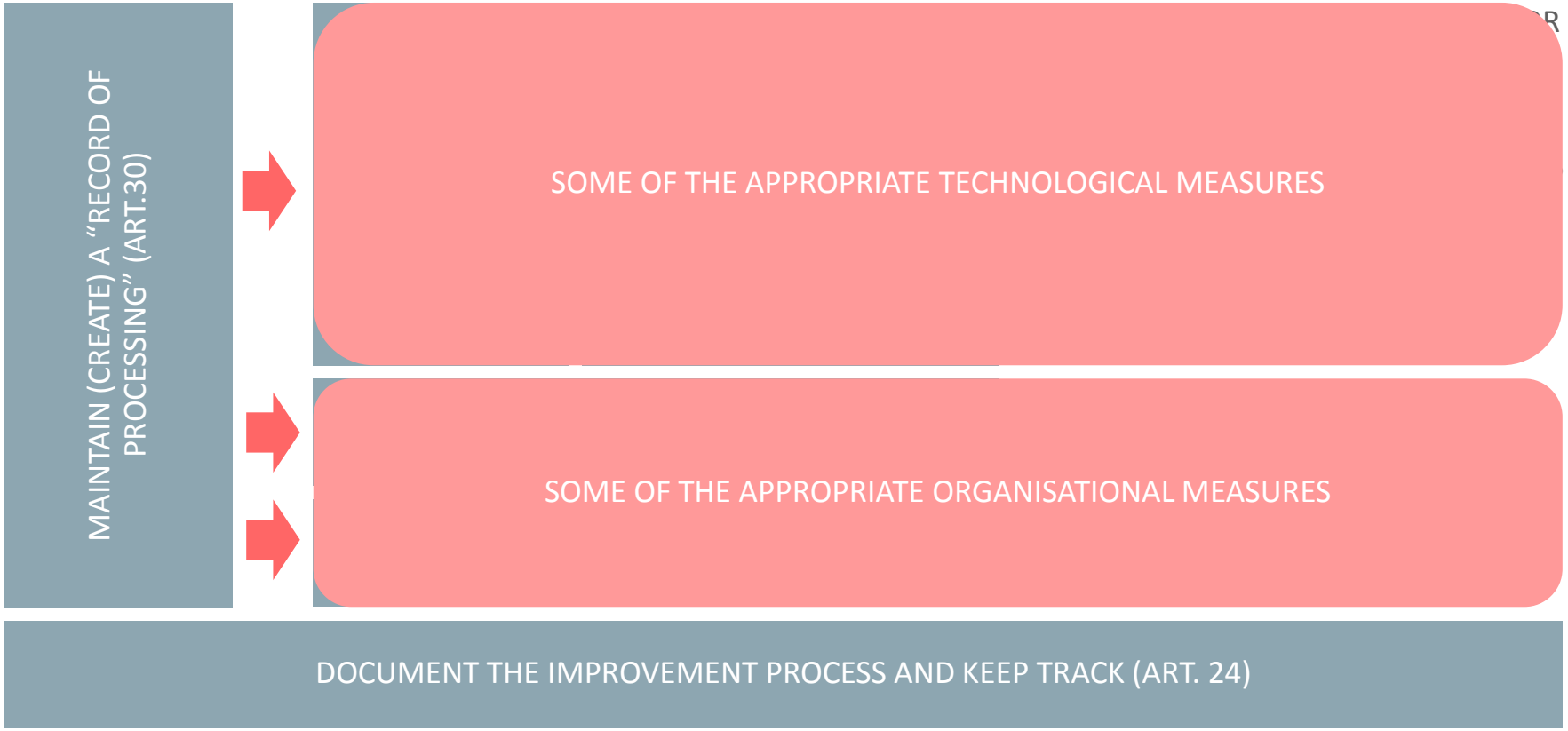
For example:

- Shared passwords
- No log
- No patching
- No encryption
- Excessive privileges
- Poor DB and application access control

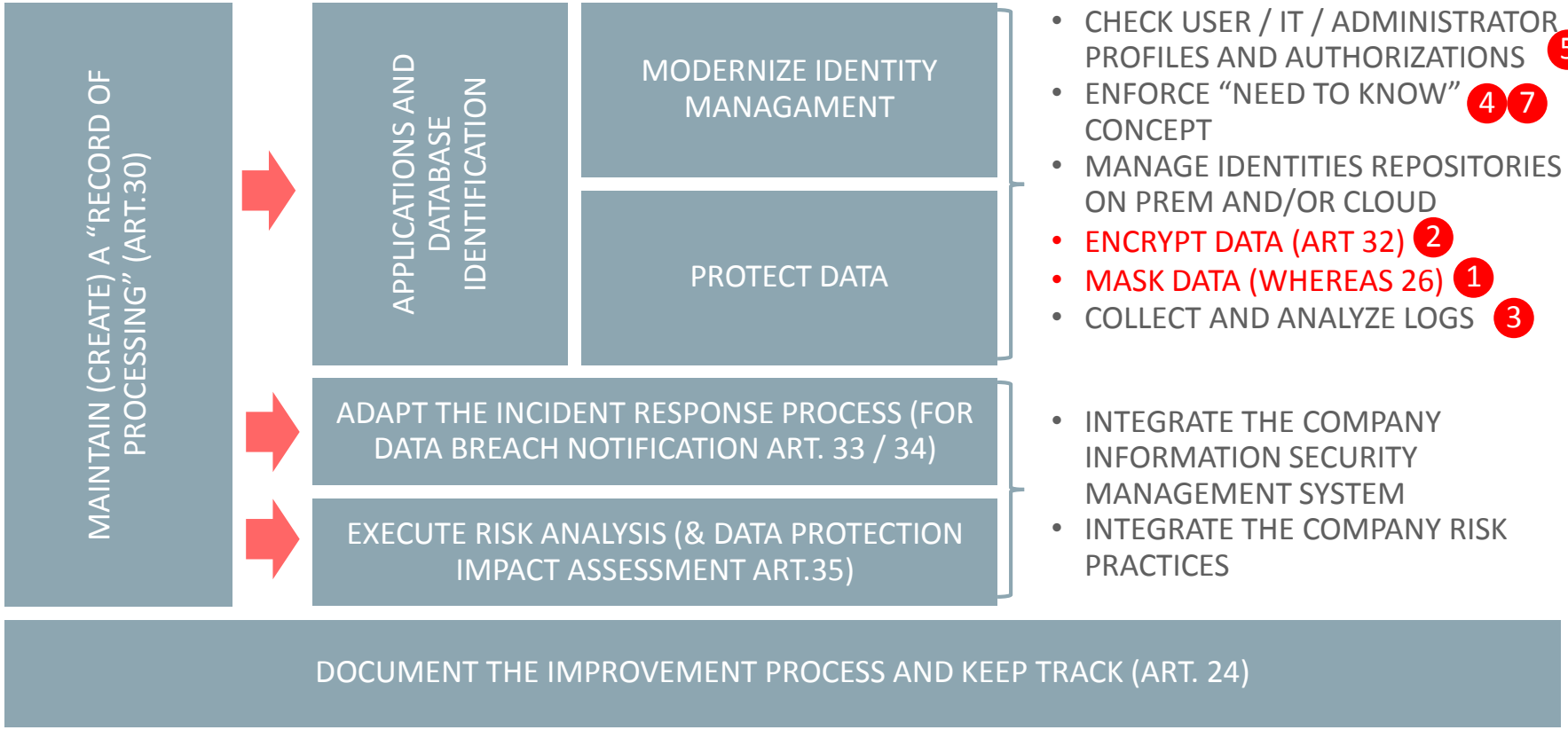
Some of the most frequent errors



First steps of a process



First steps of a process



First steps of a process

LAST_NAME	SSN	SALARY
AGUILAR	203-33-3234	40,000
BENSON	323-22-2943	60,000

Production

LAST_NAME	SSN	SALARY
ANSKEKSL	323-23-1111	60,000
BKJHHEIEDK	252-34-1345	40,000

Non-production

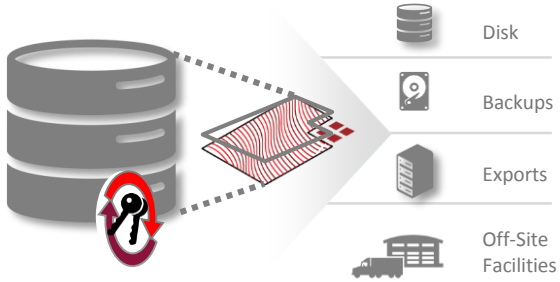
1

Data Masking & Subsetting Pack

- **Protects data that needs to be beyond Production boundaries**
- Replaces sensitive application data
- Detects/Preserves referential integrity
- Extensible template library and formats
- Integrates with Real Application Testing
- Supports masking of non-Oracle databases
- Can provide a relationally intact and yet fractional representation of production data for test and develo[p] ORACLE FUSION APPLICATIONS ORACLE E-BUSINESS SUITE

Masking Data for Nonproduction Use

ORACLE



Applications

ORACLE JDEDWARDS SIEBEL SAP PeopleSoft.

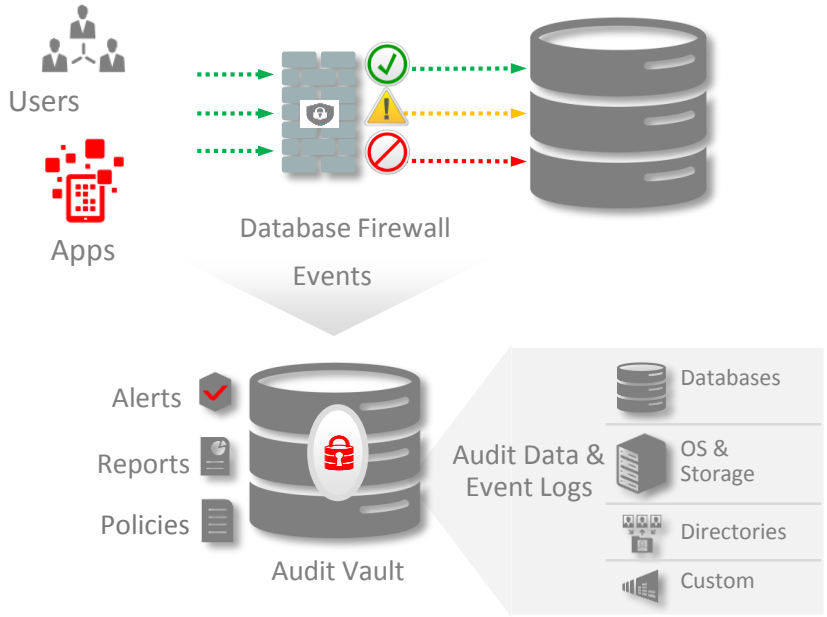
2

Advanced Security Option

- **Address regulations where data privacy is key**
- **Prevent access to data-at-rest**
- Encrypt tablespaces or columns
- Requires no application changes
- Built-in two-tier key management
- "Near Zero" overhead on SPARC and Intel processors
- Integrated with Oracle technologies
  - Oracle Key Vault, Exadata, Compression, ASM, GoldenGate, DataPump, log file

Transparent Data Encryption is Foundation

ORACLE

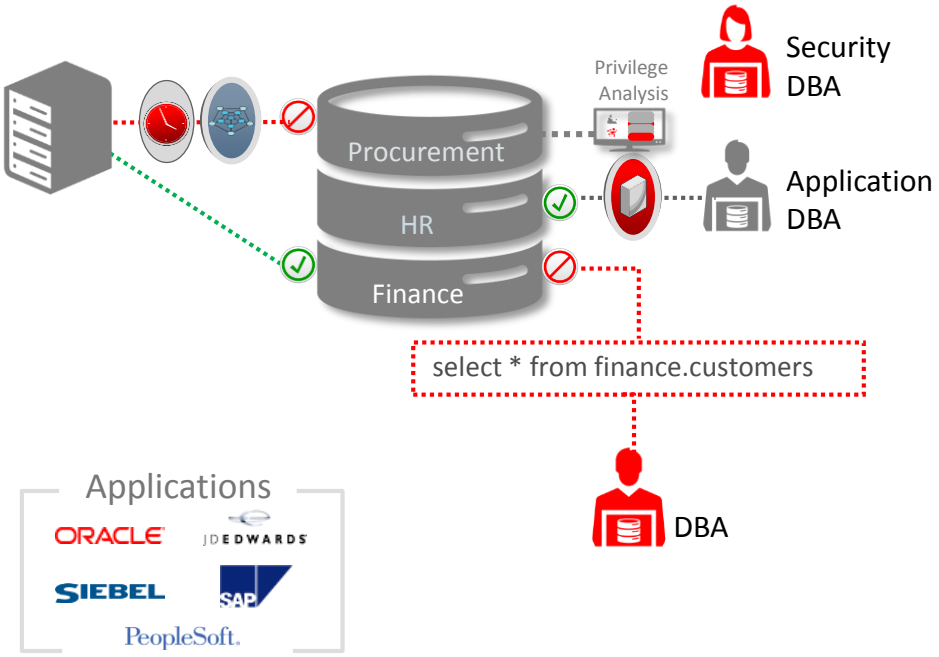


3

Audit Vault and Database Firewall

- **Central Repository of Audit Event Data**
- **Protection against #1 Web Application Security Risk – SQLinjection**
- Database Firewall can log, block or substitute incoming SQL statements
- Provides out-of-the box compliance reports for SOX, PCI, and other regulations
- Streamline audits: report generation, notification, attestation, archiving

Database Activity Monitoring and Firewall



4

Database Vault

- **Mitigate risks posed by attacks that target privileged database accounts**
- **Protect app sensitive data even by DBAs/Outsourcers/Partners**
- Realms protect sensitive schemas or objects
- Restrict Privileged Users access to realm data
- Multi-factor rules on SQL commands
- Enforce enterprise data governance, separation of duties, and least privilege

Privileged User Controls

More information (Database Security)

Accelerate Your Response to the EU General Data Protection Regulation (GDPR) http://bit.ly/2dzUdPL

More information (Identity and Access on Prem and Cloud)

5 6 7

http://bit.ly/2eao0lm

Key prospect products

- DB Security Options because they can help provide confidentiality, integrity and availability, in particular
  - Advanced Security and Key Vault to encrypt and protect the keys
  - Database Vault because it provides fine grained access control to the DB up to the level of technical account and system administrators
  - Audit Vault and DB Firewall because it can help to discover attacks and to prevent them
  - Database Masking because the GDPR promotes the use of aggregated personal data
- Identity and Access Management to guarantee and enforce proper accessibility to applications and systems
  - Identity life cycle management including deprovisioning, attestation and role mining on premise and in the cloud
  - Access management including strong and adaptive authorization and SSO on premise and in the cloud
  - API management on premise and in the cloud
- All high availability, disaster recovery and business continuity products, inter alia RAC, Data Guard, EM-DBLFM, and ZDLRA

Alessandro Vallega

LinkedIn

Twitter U3L4

alessandro.vallega@oracle.com

www.europrivacy.info

Contact me

Integrated Cloud

Applications & Platform Services


ORACLE®