Convegno Annuale AISIS

Innovazione digitale a supporto dei Pdta

Diritto alla Cura o diritto alla Privacy?

Alessandro Vallega
Security Business Developer Europe South Oracle;
Clusit Board of Directors;
Oracle Community for Security chairman

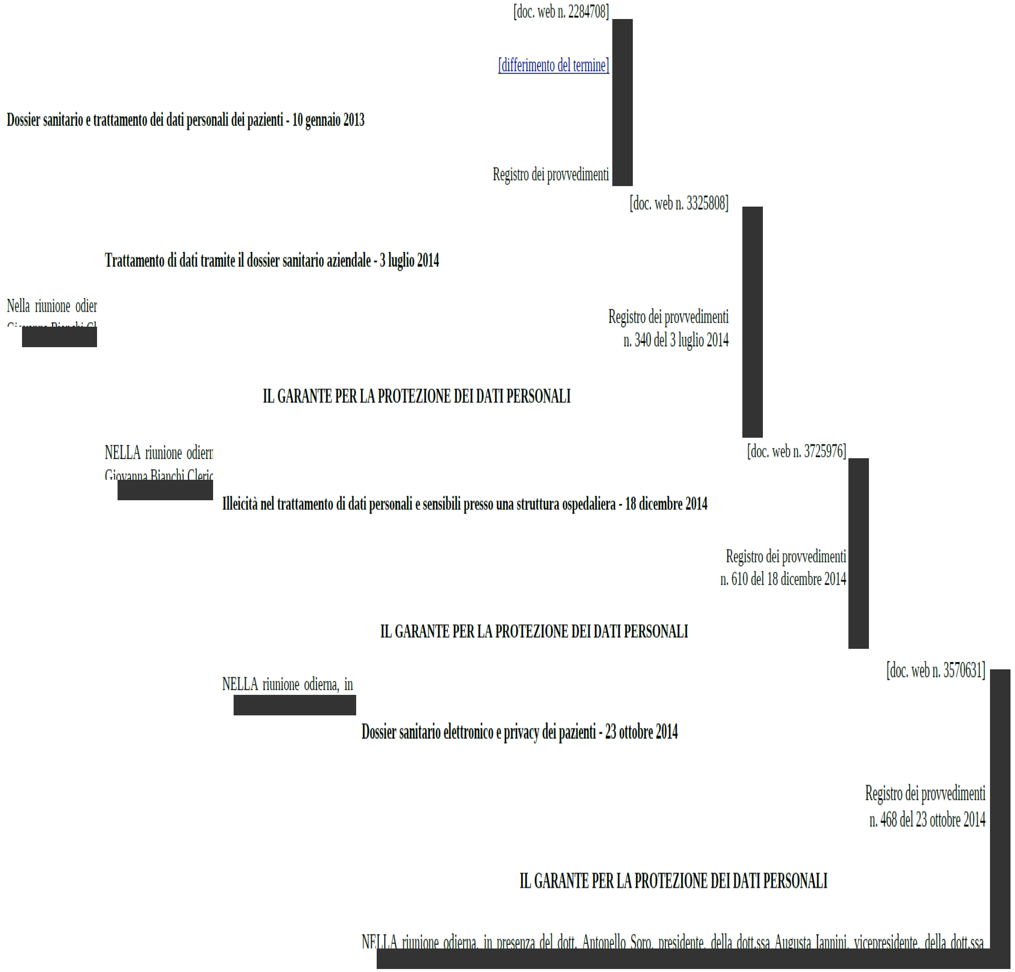
Napoli, 22 e 23 ottobre 2015
Hotel Ramada

Agenda

- The case of some italian hospitals and the Authority’s stance
- Database Security Maturity Evaluation
- Database INsecurity practices
- Security in the Architecture

The case of some Italian hospitals

Inspections and decisions



[doc. web n. 2284708]

[differimento del termine]

Dossier sanitario e trattamento dei dati personali dei pazienti - 10 gennaio 2013

Registro dei provvedimenti

[doc. web n. 3325808]

Trattamento di dati tramite il dossier sanitario aziendale - 3 luglio 2014

Nella riunione odier

Registro dei provvedimenti
n. 340 del 3 luglio 2014

IL GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

NELLA riunione odiern
Giovanna Bianchi Cleric

[doc. web n. 3725976]

Illeicità nel trattamento di dati personali e sensibili presso una struttura ospedaliera - 18 dicembre 2014

Registro dei provvedimenti
n. 610 del 18 dicembre 2014

IL GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

NELLA riunione odierna, in

[doc. web n. 3570631]

Dossier sanitario elettronico e privacy dei pazienti - 23 ottobre 2014

Registro dei provvedimenti
n. 468 del 23 ottobre 2014

IL GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

NELLA riunione odierna, in presenza del dott. Antonello Soro, presidente, della dott.ssa Augusta Iannini, vicepresidente, della dott.ssa

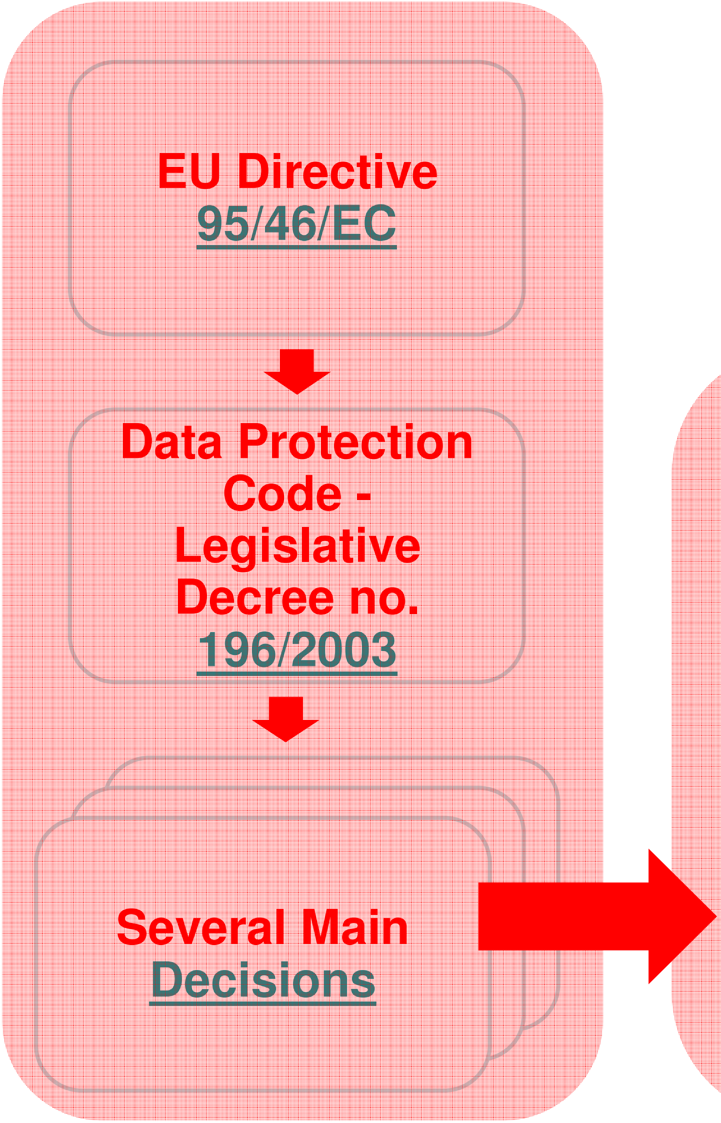
- Several inspections in the last year in the healthcare sector
- Findings
  - Illicit processing of personal data
- Consequences:
  - Mandatory remediation programs
  - Fines to the hospital
  - Possible lawsuits to top management

Common findings

- Lack in the processes related to the information provided to the data subject
- Lack in the processes related to the collection of the informed consent (in Italy must be provided in writing)
- Non restricted access to health data of the patiences by different doctors, nurses and administrative personnel
  - And “Oscuramento and Oscuramento dell’Oscuramento” not implemented
- No logging of the accesses to health data*

* this is now regulated in the new Authority decision about Dossier sanitario

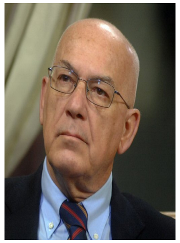
Anticipating the EU DP Act



EU Directive 95/46/EC

Data Protection Code - Legislative Decree no. 196/2003

Several Main Decisions



- Key concepts of the new regulation are anticipated into the Italian law with the tool of “main decisions”; for example the databreach notification act for healthcare, telco and internet providers, and (partially) banking
- Security controls are increased in certain cases such as enhanced end to end logging to enforce accountability (banking and healthcare)

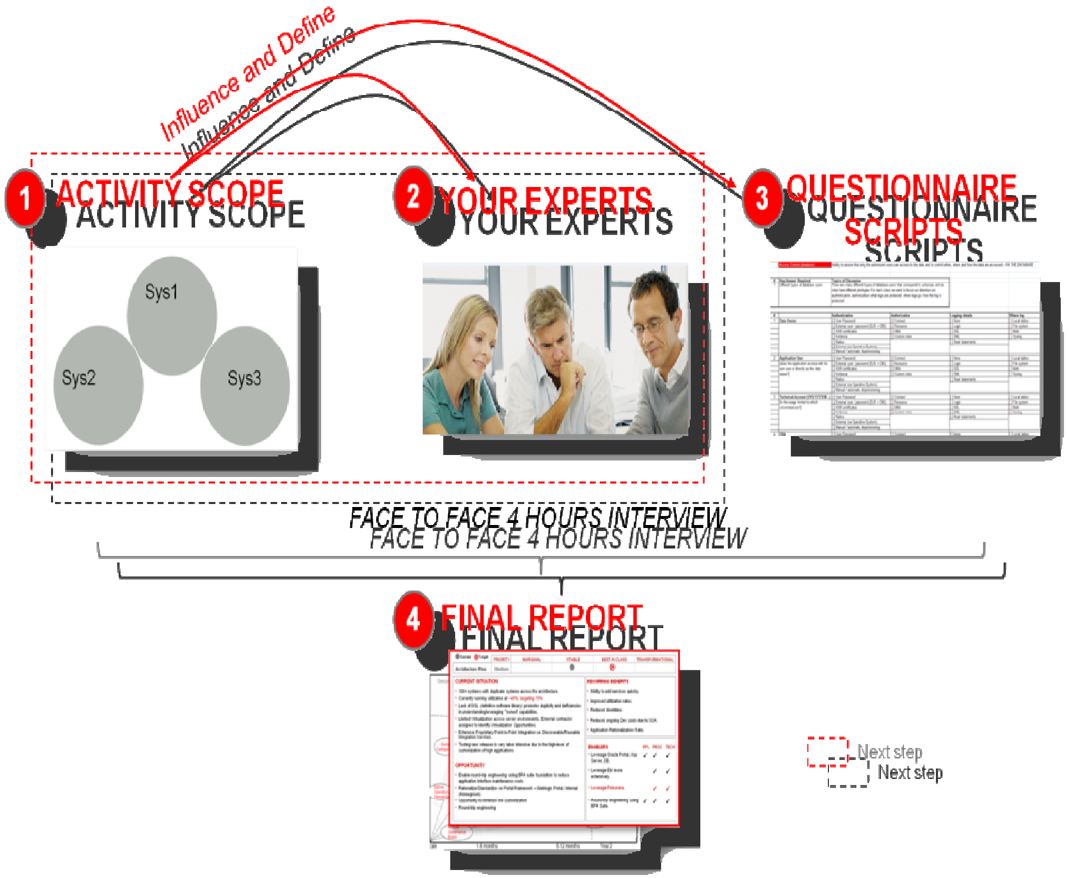
Database Security Maturity Evaluation

Security Maturity Evaluation

Oracle Europe best practice

Executed at 30+ Oracle largest customers in all sectors:

- Banks
- Insurances
- Telco
- Oil and Gas
- Utilities
- Hospitals
- Public Sector



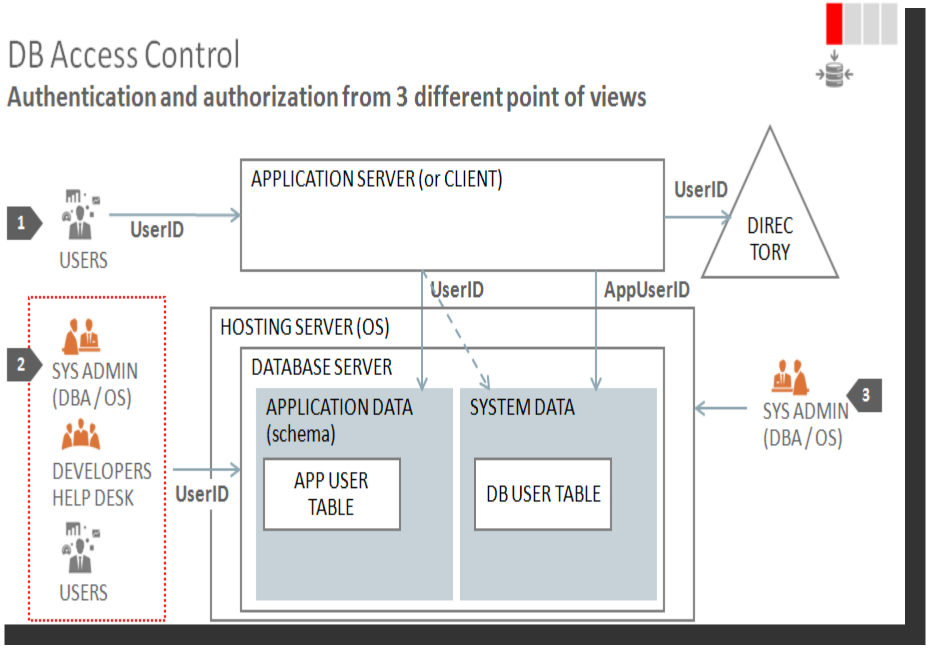
Our tool is your people!

Database Security Maturity Knowledge Areas

	DB Access Control	**Monitoring / Blocking and Audit**	**Data Protection**	**Secure Configuration**
DB Security	Ability to assure access only to authorized users and to control when/where/how the data are accessed	Ability to analyze the transactional activities (threats/blocks) and to view current transactional activities and historical information	Processes and controls to secure storage, transmission and accessing of an organization’s data throughout its lifecycle	Process and controls to assure DB configuration for security and compliance

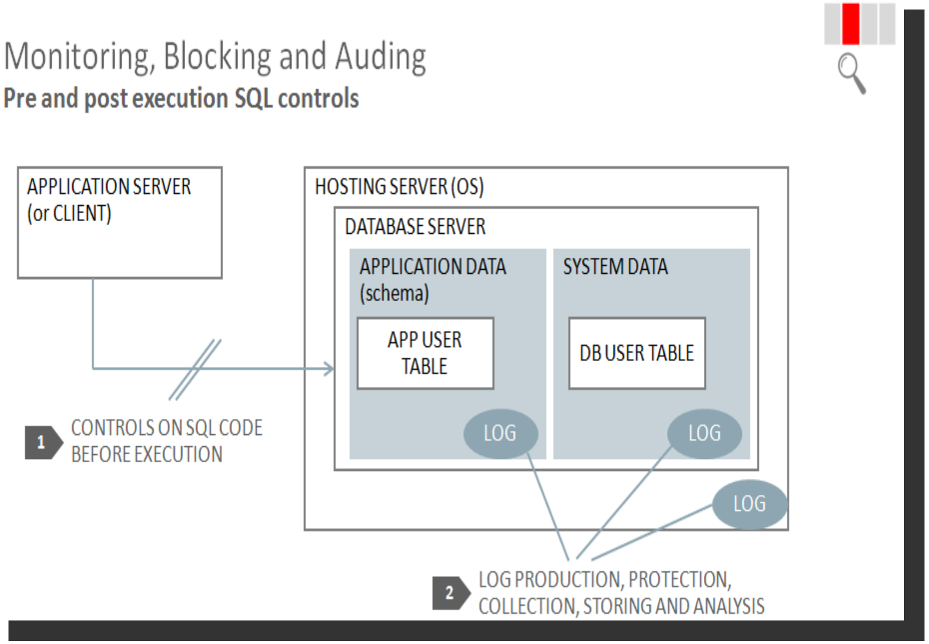
Database INsecurity Practices

Most Common Mistakes (1/4)



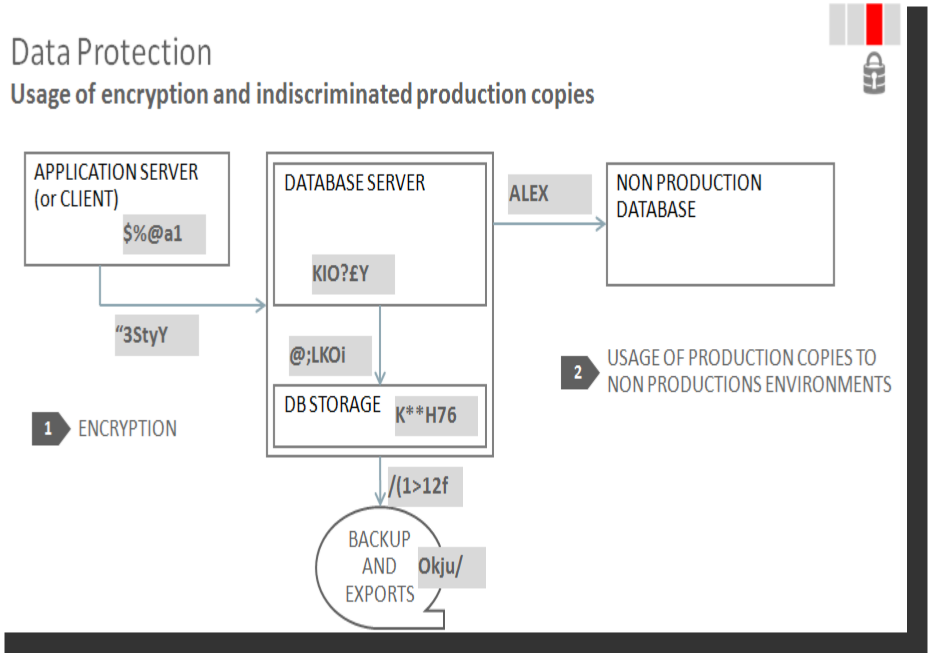
- No distinction between Application User and Schema Owner (AC1)
- Application user credential not protected in the application server (AC2)
- Developers use application user credential (AC3)
- DBA do not have personal accounts and use technical accounts (AC4)
- Technical accounts defined with a human algorithm and never changed (AC5)
- End users have direct access to the DB bypassing the application (AC6)
- No lifecycle management for DB users (AC7)
- OS administrators can escalate their privileges to DBA (AC8)

Most Common Mistakes (2/4)


Monitoring, Blocking and Auding
Pre and post execution SQL controls
APPLICATION SERVER (or CLIENT)
HOSTING SERVER (OS)
DATABASE SERVER
APPLICATION DATA (schema)
APP USER TABLE
SYSTEM DATA
DB USER TABLE
LOG
LOG
LOG
1 CONTROLS ON SQL CODE BEFORE EXECUTION
2 LOG PRODUCTION, PROTECTION, COLLECTION, STORING AND ANALYSIS

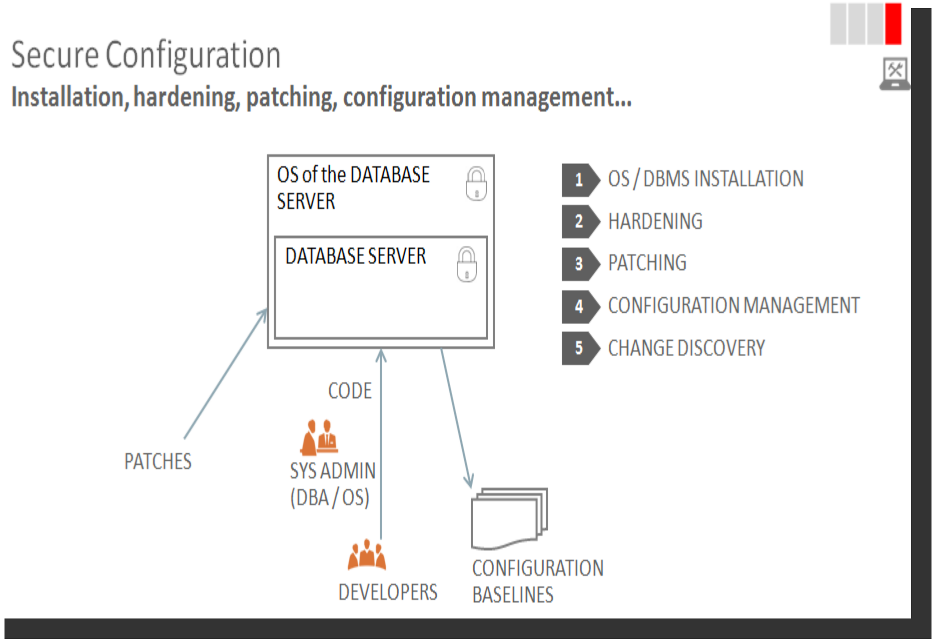
- No preventive SQL controls (LG1)
- No or partial and inconsistent logs (LG2)
- Logs are not analyzed (LG3)
- Logs are not managed (LG4)
- No DB user accountability (LG5)
- No end user accountability (LG6)

Most Common Mistakes (3/4)


Data Protection
Usage of encryption and indiscriminated production copies
APPLICATION SERVER (or CLIENT)
$%@a1
"3StyY
DATABASE SERVER
KIO?£Y
@;LKOi
DB STORAGE
K**H76
/(1>12f
BACKUP AND EXPORTS
Okju/
ALEX
NON PRODUCTION DATABASE
1 ENCRYPTION
2 USAGE OF PRODUCTION COPIES TO NON PRODUCTIONS ENVIRONMENTS

- Applications do not encrypt (DP1)
- No datafile encryption (DP2)
- No storage encryption (DP3)
- No network encryption (DP4)
- No backup / export encryption (DP5)
- Production data copied to development environments (DP6)

Most Common Mistakes (4/4)



Secure Configuration

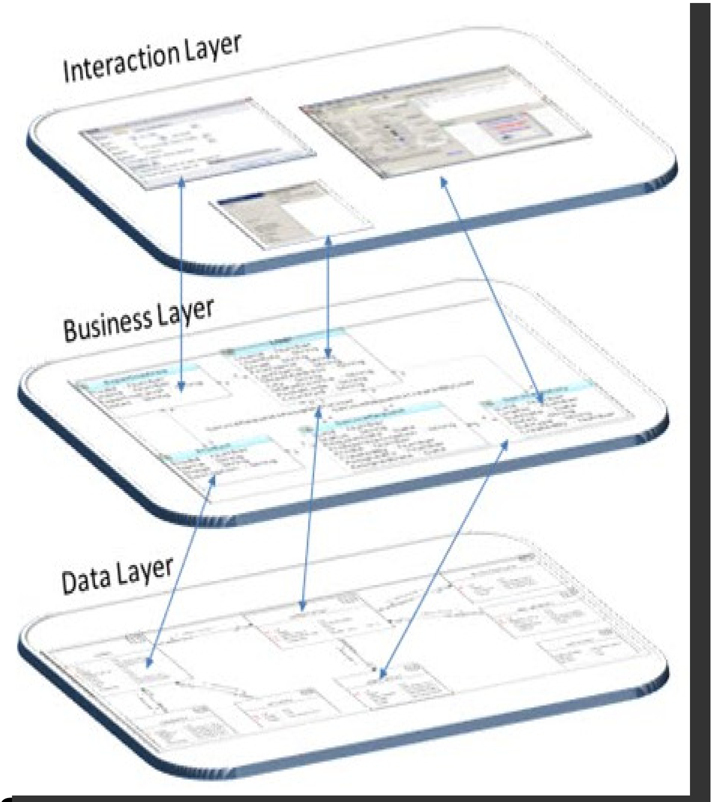
Installation, hardening, patching, configuration management...

1 OS / DBMS INSTALLATION
2 HARDENING
3 PATCHING
4 CONFIGURATION MANAGEMENT
5 CHANGE DISCOVERY

- Obsolete DB / OS releases (SC1)
- No DB / OS hardening (SC2)
- No patching (SC3)
- Poor SDLC production promotion and SoD (SC4)
- No production user, privileges, db objects change control (SC5)

Security in the Architecture

Hospitals working in these areas

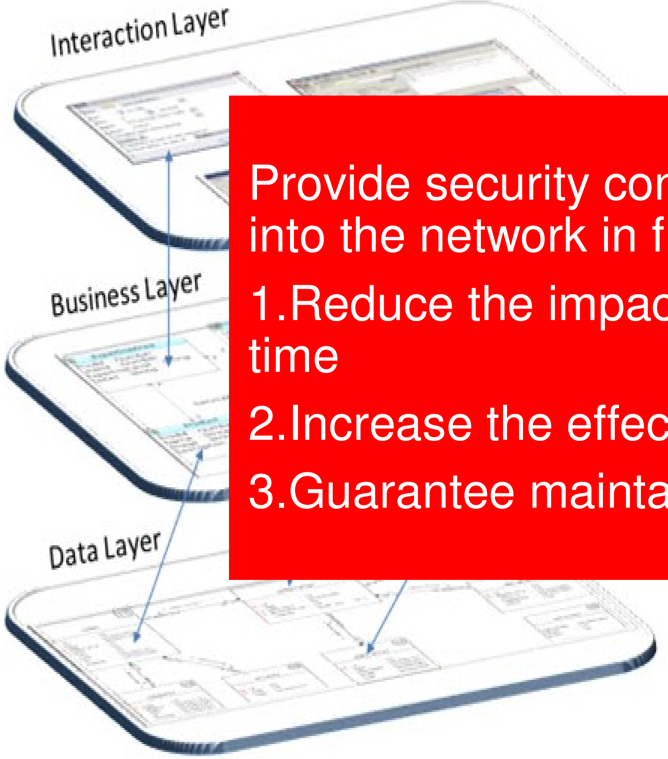


Source: On Philosophy and Software Design

Source: On Philosophy and Software Design

1. DB version upgrade
2. Transparent Data Encryption
3. End User Identifier
4. Enhanced Logging
5. FlashBack
6. DB User account attestation
7. DB User account centralization into LDAP
8. DB Masking
9. DB Administrator Access Control

Hospitals working in these areas:



1. DB version upgrade
2. Transparent Data Encryption

tion

ization into

8. DB Masking
9. DB Administrator Access Control

Provide security controls into the database layer and into the network in front of the database allows:

1.Reduce the impact on the applications, cost and time

2.Increase the effectiveness of the security measure

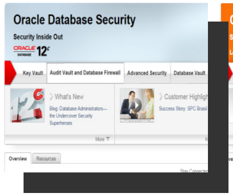
3.Guarantee maintainability and future requirements

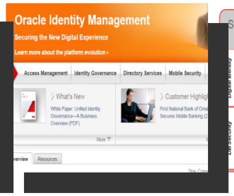
Source: On Philosophy and Software Design

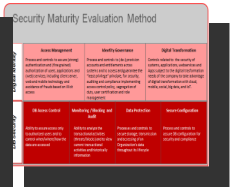
Source: On Philosophy and Software Design

Contact me

[LinkedIn](#)
[twitter.com/U3L4](#)
[alessandro.vallega@oracle.com](#)




Oracle Identity Management
Securing the New Digital Experience



Stay up to date with our
EuroPrivacy.info blog

Born from [Clusit](#), [Aused](#), and
[Oracle Community for Security](#)

Grazie dell'attenzione e buon lavoro