# Oracle Database Security – How much would you like?

**DOAG + SOUG Security-Lounge**

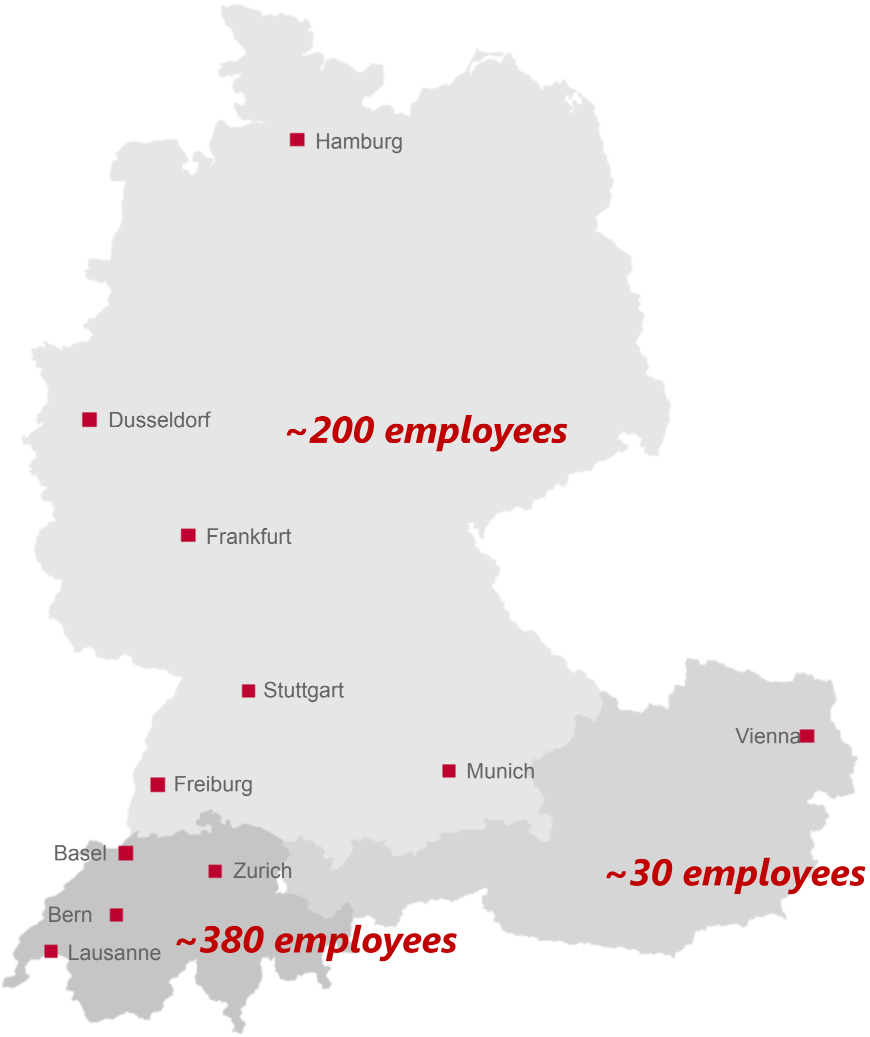
Stefan Oehrli
Senior Consultant
Discipline Manager
Trivadis AG

Basel 24. April 2012

BASEL BERN LAUSANNE ZÜRICH DÜSSELDORF FRANKFURT A.M. FREIBURG I.BR. HAMBURG MÜNCHEN STUTTGART WIEN

trivadis
makes IT easier.

# Trivadis facts & figures



11 Trivadis locations with more than 600 employees

Financially independent and sustainably profitable

Key figures 2011

- Revenue CHF 104 / EUR 84 Mio.
- Services for more than 800 clients in over 1,900 projects
- 200 Service Level Agreements
- More than 4,000 training participants
- Research and development budget: CHF 5.0 / EUR 4 Mio.

# Why we are special

**Customer-specific solution competence and vendor independence**

- offers substantiated techniques and skills as well as self-developed approaches
- guarantees repeatable quality and a safe execution

**Technology competence**

- offers more than 18 years of expertise in Oracle and Microsoft
- has its own Technology Center and strives for technological excellence

**Solution and integration expertise**

- has a wide and cross-sectorial customer basis and more than 1900 projects every year spanning a broad range of goals, complexity and corresponding framework conditions
- Combines technological expertise with an understanding of the specific business needs of the client

**Support for the entire IT project lifecycle**

- has a modular portfolio of services for the entire IT project lifecycle
- provides the appropriate combination of solutions and services for every „level of maturity“

# AGENDA

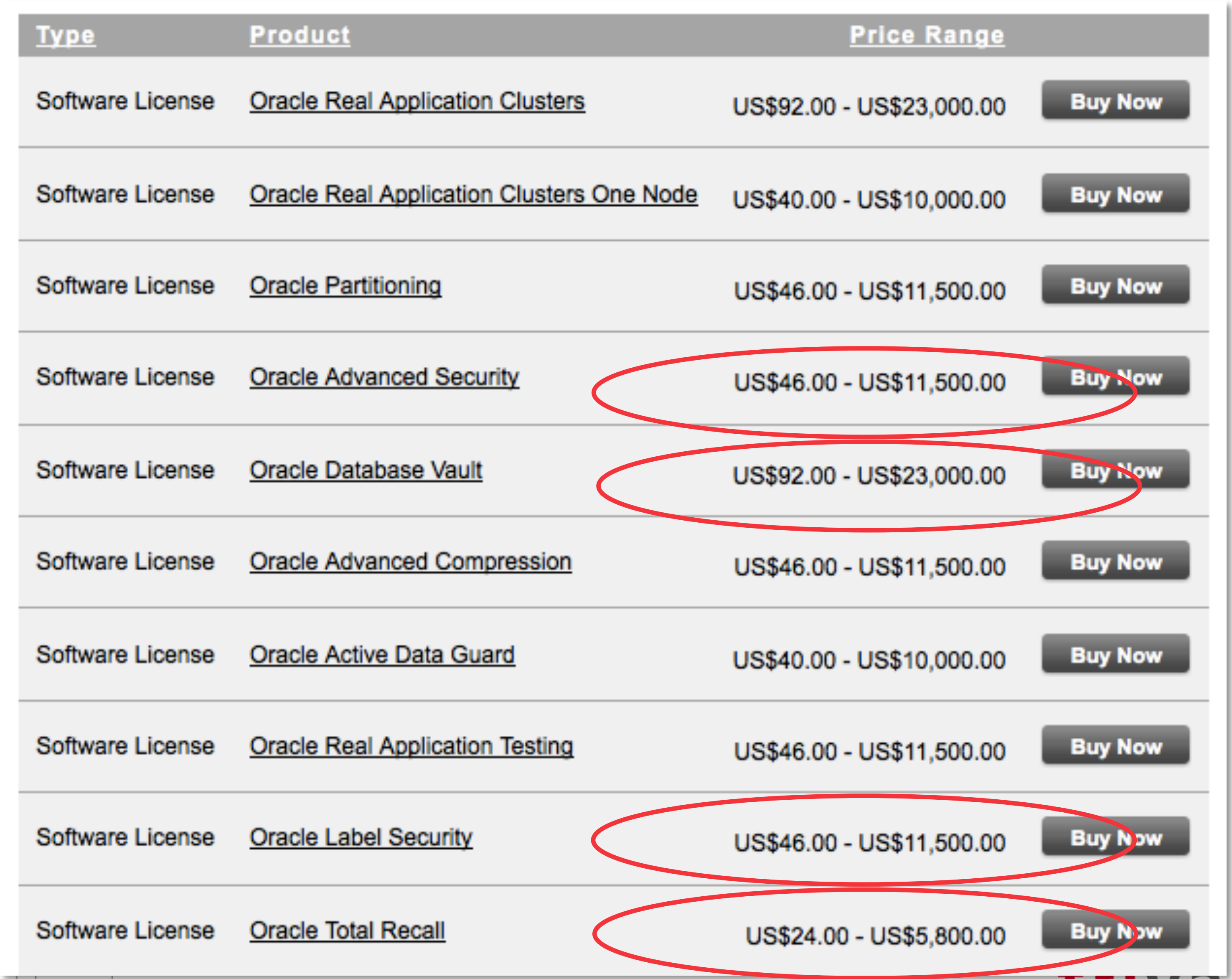
1. Overview
2. Risk analysis and categorization
3. Risk Matrix
4. Risk minimization
5. Review

# Overview

- Oracle offers several features within the database to ensure data security
  - VPD, ASO, TDE, DBV, AV, ... ☺
- Some of the feature is only available in Enterprise Edition, some require additional license
- There are also other Oracle and external products
- And of course third party solutions ...

- But what do I need for my database?
- And how many different databases do I have?

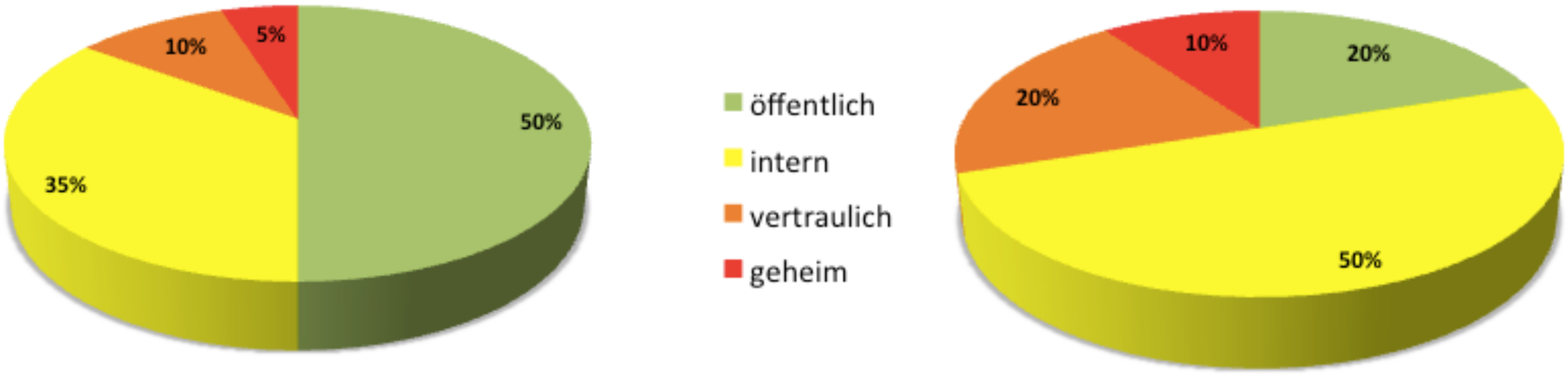
# Overview



| Type | Product | Price Range | |
|---|---|---|---|
| Software License | Oracle Real Application Clusters | US$92.00 - US$23,000.00 | Buy Now |
| Software License | Oracle Real Application Clusters One Node | US$40.00 - US$10,000.00 | Buy Now |
| Software License | Oracle Partitioning | US$46.00 - US$11,500.00 | Buy Now |
| Software License | Oracle Advanced Security | US$46.00 - US$11,500.00 | Buy Now |
| Software License | Oracle Database Vault | US$92.00 - US$23,000.00 | Buy Now |
| Software License | Oracle Advanced Compression | US$46.00 - US$11,500.00 | Buy Now |
| Software License | Oracle Active Data Guard | US$40.00 - US$10,000.00 | Buy Now |
| Software License | Oracle Real Application Testing | US$46.00 - US$11,500.00 | Buy Now |
| Software License | Oracle Label Security | US$46.00 - US$11,500.00 | Buy Now |
| Software License | Oracle Total Recall | US$24.00 - US$5,800.00 | Buy Now |

# Overview

- Do you know you data?
- respectively its sensitivity?
- How much of our data is public, confidential, internal or secret?
- Like this?
- or more like this?



# AGENDA

1. Overview
2. Risk analysis and categorization
3. Risk Matrix
4. Risk minimization
5. Review

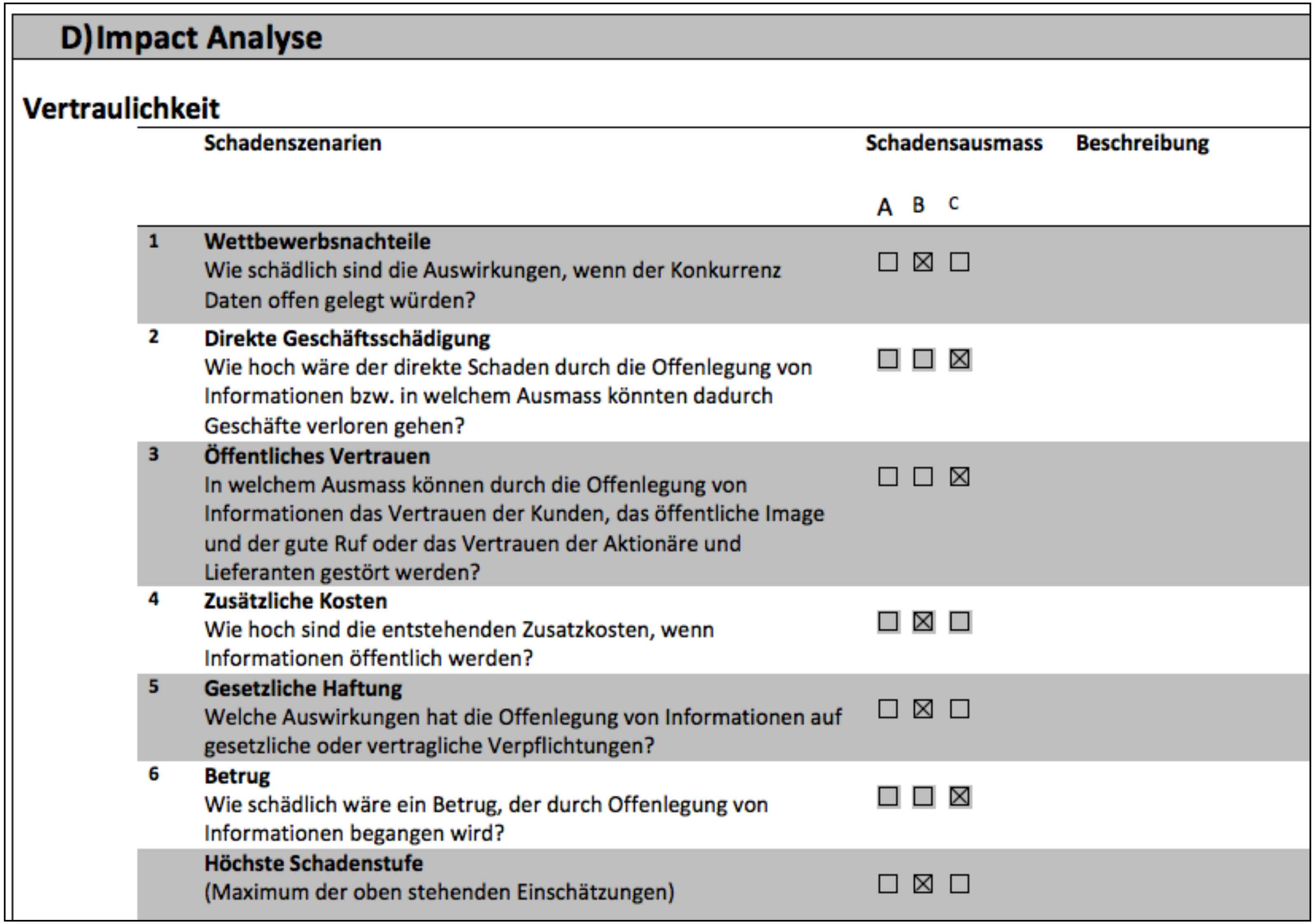
# Risk analysis and categorization

- The data owner (application owner) must know and define the sensitiveness of his data
- It is not always an easy job, everybody think his data is the most important and most critical,…
- Therefore it is advisable to perform a risk analysis
- At Trivadis we use the Trivadis First Cut Risk analysis
  - Easy to perform
  - In "Business-Language"
  - Risks are identified quickly
  - Does not go into the technical details, but afterwards its clear on what to focus

# Risk analysis and categorization

- Topics that are questioned (i.e.):
  - Are personal data or sensitive personal data processed (Healthcare, Religion, ...)?
  - What happens in case of loss of confidentiality? (competitive disadvantages, business damage, disorder of public trust, liability, ...)?
  - What happens in case of loss of integrity? (wrong management decisions, additional costs, business interruption)?
  - What happens in case of loss availability (recover data and service, ...)?
- The data owner is rating all points in a 3-point scale (from not critical over critical to business critical)
- It is also possible to deposit values for material damage that often helps in assessing

# Risk analysis and categorization

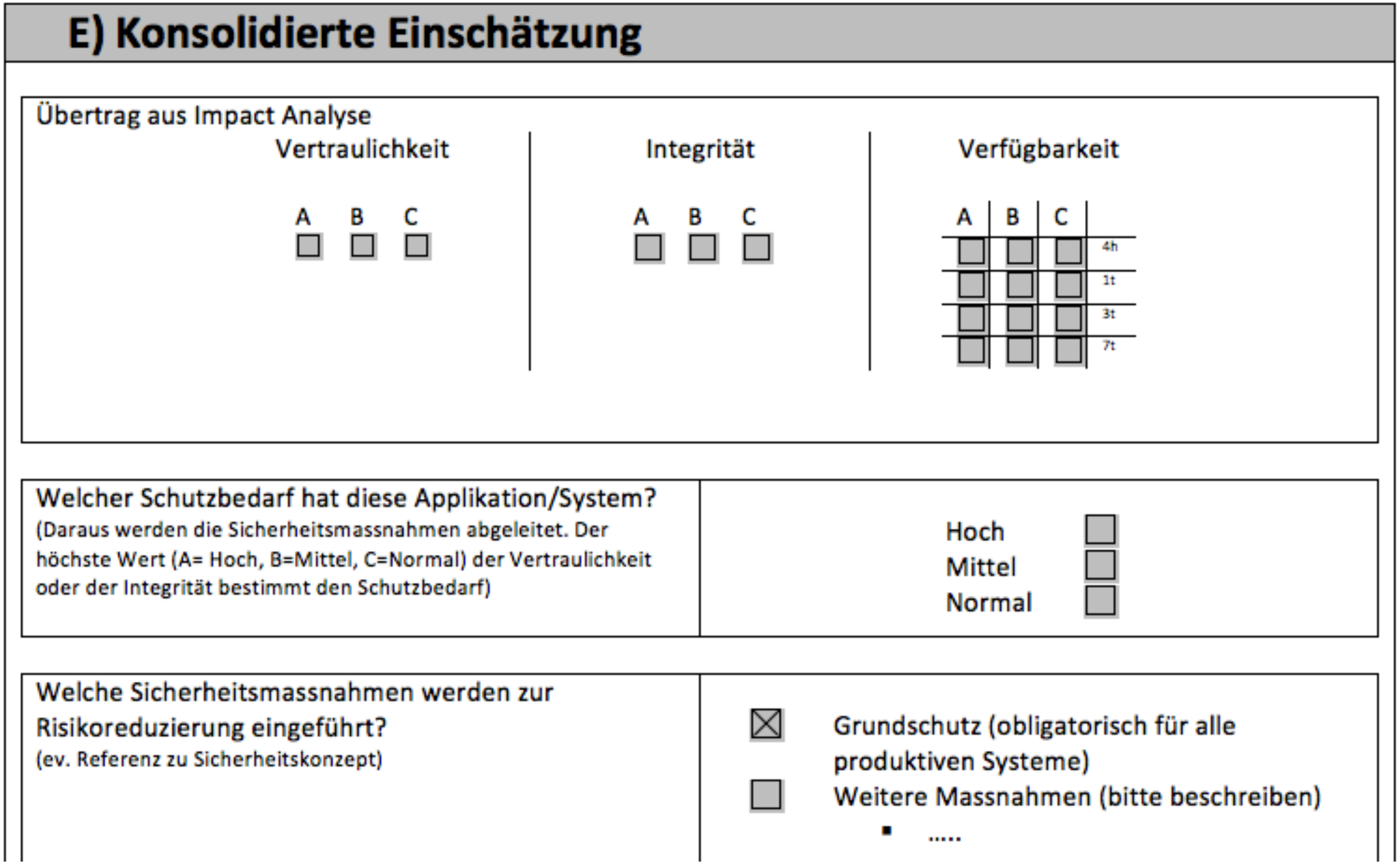


## D) Impact Analyse

### Vertraulichkeit

| | Schadenszenarien | Schadensausmass | | | Beschreibung |
|---|---|---|---|---|---|
| | | A | B | C | |
| 1 | **Wettbewerbsnachteile**<br>Wie schädlich sind die Auswirkungen, wenn der Konkurrenz Daten offen gelegt würden? | ☐ | ☒ | ☐ | |
| 2 | **Direkte Geschäftsschädigung**<br>Wie hoch wäre der direkte Schaden durch die Offenlegung von Informationen bzw. in welchem Ausmass könnten dadurch Geschäfte verloren gehen? | ☐ | ☐ | ☒ | |
| 3 | **Öffentliches Vertrauen**<br>In welchem Ausmass können durch die Offenlegung von Informationen das Vertrauen der Kunden, das öffentliche Image und der gute Ruf oder das Vertrauen der Aktionäre und Lieferanten gestört werden? | ☐ | ☐ | ☒ | |
| 4 | **Zusätzliche Kosten**<br>Wie hoch sind die entstehenden Zusatzkosten, wenn Informationen öffentlich werden? | ☐ | ☒ | ☐ | |
| 5 | **Gesetzliche Haftung**<br>Welche Auswirkungen hat die Offenlegung von Informationen auf gesetzliche oder vertragliche Verpflichtungen? | ☐ | ☒ | ☐ | |
| 6 | **Betrug**<br>Wie schädlich wäre ein Betrug, der durch Offenlegung von Informationen begangen wird? | ☐ | ☐ | ☒ | |
| | **Höchste Schadenstufe**<br>(Maximum der oben stehenden Einschätzungen) | ☐ | ☒ | ☐ | |

# Risk analysis and categorization



## E) Konsolidierte Einschätzung

Übertrag aus Impact Analyse

Vertraulichkeit

| A | B | C |
|---|---|---|
| □ | □ | □ |

Integrität

| A | B | C |
|---|---|---|
| □ | □ | □ |

Verfügbarkeit

| A | B | C | |
|---|---|---|---|
| □ | □ | □ | 4h |
| □ | □ | □ | 1t |
| □ | □ | □ | 3t |
| □ | □ | □ | 7t |

| | |
|---|---|
| **Welcher Schutzbedarf hat diese Applikation/System?**<br>(Daraus werden die Sicherheitsmassnahmen abgeleitet. Der höchste Wert (A= Hoch, B=Mittel, C=Normal) der Vertraulichkeit oder der Integrität bestimmt den Schutzbedarf) | Hoch □<br>Mittel □<br>Normal □ |
| **Welche Sicherheitsmassnahmen werden zur Risikoreduzierung eingeführt?**<br>(ev. Referenz zu Sicherheitskonzept) | ☒ Grundschutz (obligatorisch für alle produktiven Systeme)<br>□ Weitere Massnahmen (bitte beschreiben)<br>▪ ..... |

# Classification

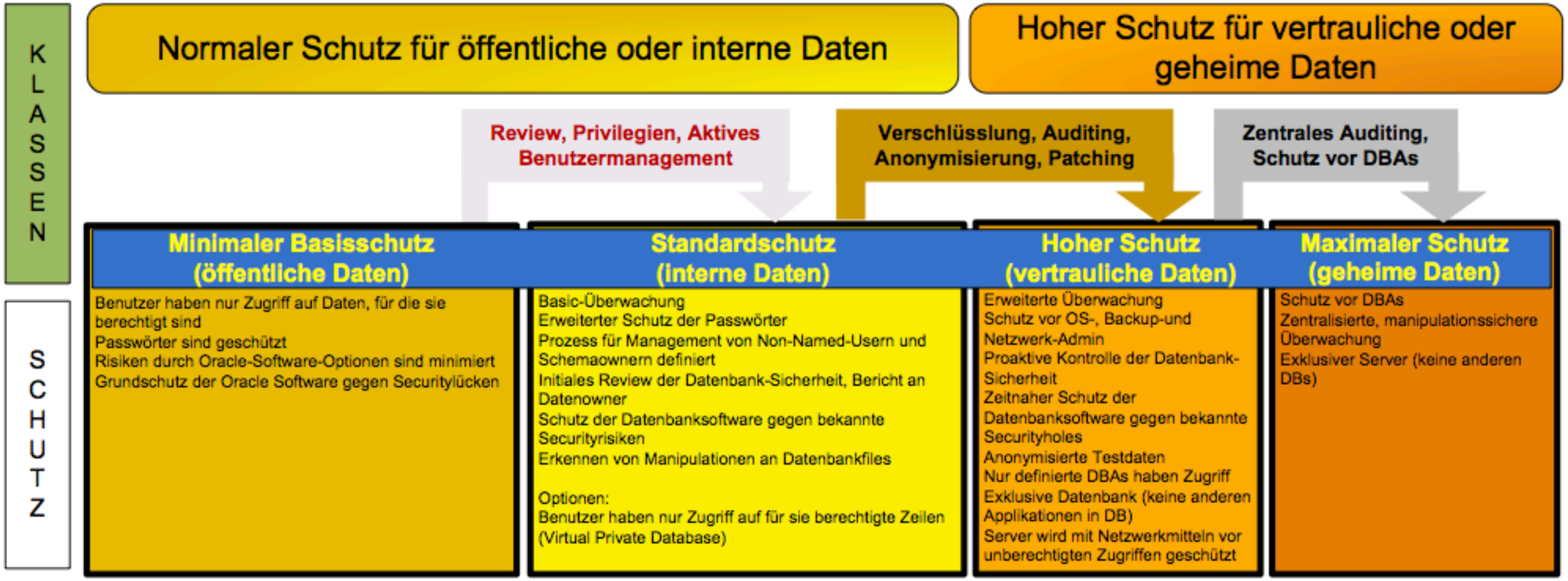
- By the risk analysis is the classification of data (-bases) into security classes possible
- Typically one uses the following classes:
  - Public (data is visible over the internet but definitely not manipulated)
  - Internal (data can be accessed by any employee)
  - Confidential (data can only be accessed by defined circle of employees)
  - Secret (If they are lost, this could endanger the existence of the company, e.g. the recipe for Coca Cola)

# AGENDA

1. Overview
2. Risk analysis and categorization
3. Risk Matrix
4. Risk minimization
5. Review

# Risk matrix (1)

- Head of the matrix defines the classes and risks which have to be reduced

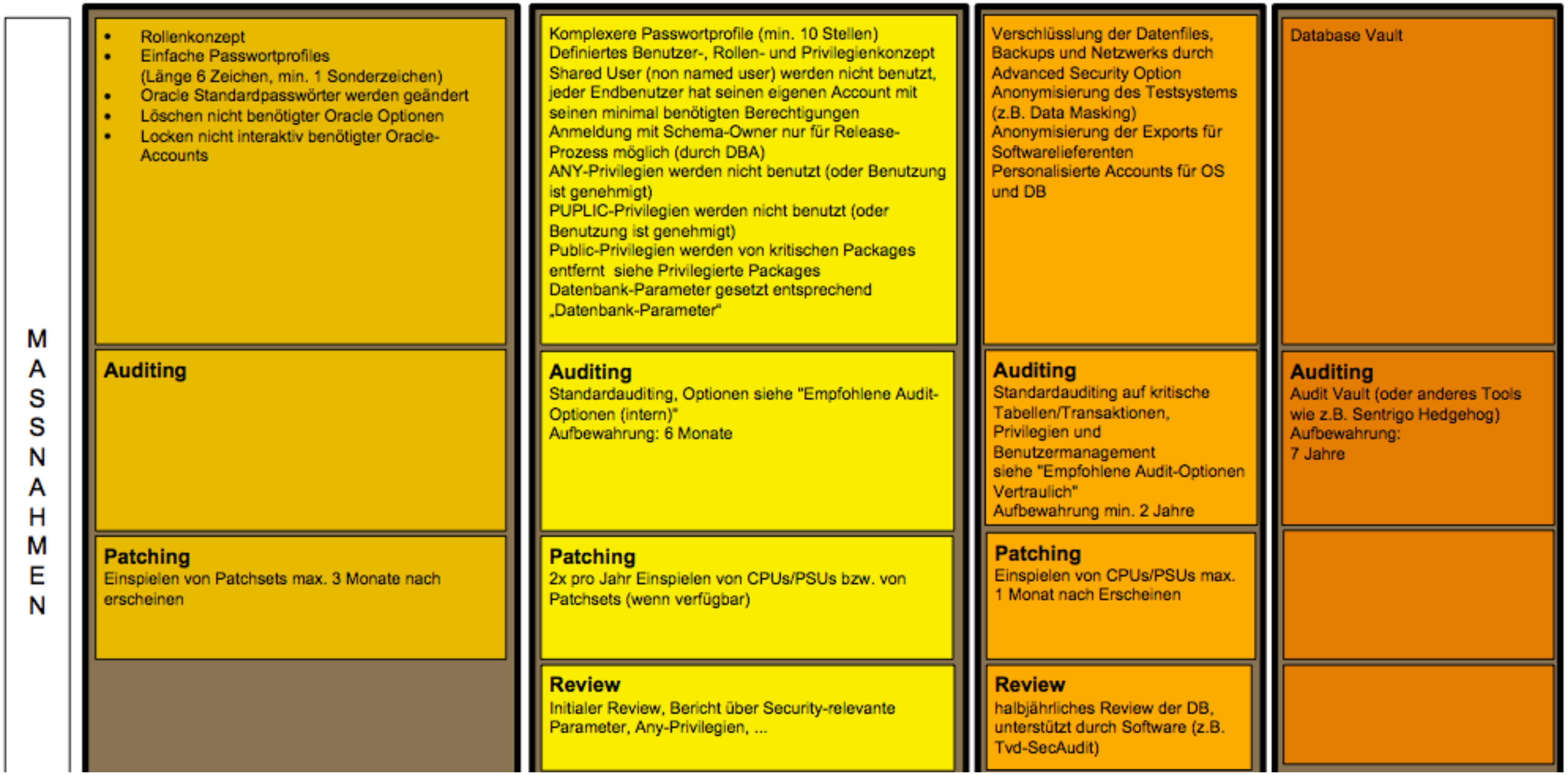


KLASSEN
Normaler Schutz für öffentliche oder interne Daten
Hoher Schutz für vertrauliche oder geheime Daten
Review, Privilegien, Aktives Benutzermanagement
Verschlüsslung, Auditing, Anonymisierung, Patching
Zentrales Auditing, Schutz vor DBAs
SCHUTZ

| Minimaler Basisschutz (öffentliche Daten) | Standardschutz (interne Daten) | Hoher Schutz (vertrauliche Daten) | Maximaler Schutz (geheime Daten) |
|---|---|---|---|
| Benutzer haben nur Zugriff auf Daten, für die sie berechtigt sind<br>Passwörter sind geschützt<br>Risiken durch Oracle-Software-Optionen sind minimiert<br>Grundschutz der Oracle Software gegen Securitylücken | Basic-Überwachung<br>Erweiterter Schutz der Passwörter<br>Prozess für Management von Non-Named-Usern und Schemaownern definiert<br>Initiales Review der Datenbank-Sicherheit, Bericht an Datenowner<br>Schutz der Datenbanksoftware gegen bekannte Securityrisiken<br>Erkennen von Manipulationen an Datenbankfiles<br><br>Optionen:<br>Benutzer haben nur Zugriff auf für sie berechtigte Zeilen (Virtual Private Database) | Erweiterte Überwachung<br>Schutz vor OS-, Backup-und Netzwerk-Admin<br>Proaktive Kontrolle der Datenbank-Sicherheit<br>Zeitnaher Schutz der Datenbanksoftware gegen bekannte Securityholes<br>Anonymisierte Testdaten<br>Nur definierte DBAs haben Zugriff<br>Exklusive Datenbank (keine anderen Applikationen in DB)<br>Server wird mit Netzwerkmitteln vor unberechtigten Zugriffen geschützt | Schutz vor DBAs<br>Zentralisierte, manipulationssichere Überwachung<br>Exklusiver Server (keine anderen DBs) |

# Risk matrix (2)

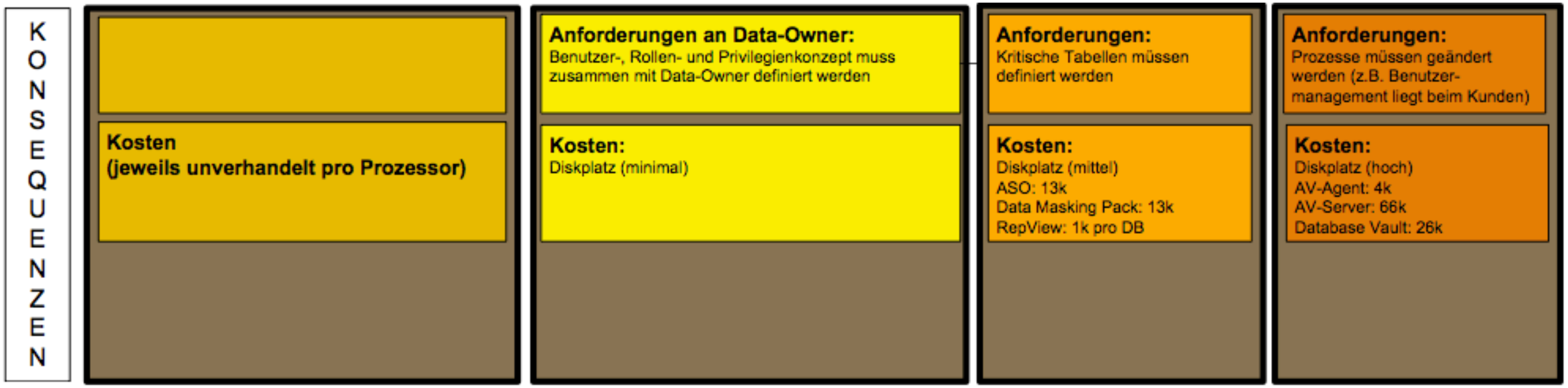
- In the further steps security measures are defined which are used to reduce the risks



| | | | | |
|---|---|---|---|---|
| MASSNAHMEN | • Rollenkonzept<br>• Einfache Passwortprofiles (Länge 6 Zeichen, min. 1 Sonderzeichen)<br>• Oracle Standardpasswörter werden geändert<br>• Löschen nicht benötigter Oracle Optionen<br>• Locken nicht interaktiv benötigter Oracle-Accounts | Komplexere Passwortprofile (min. 10 Stellen)<br>Definiertes Benutzer-, Rollen- und Privilegienkonzept<br>Shared User (non named user) werden nicht benutzt, jeder Endbenutzer hat seinen eigenen Account mit seinen minimal benötigten Berechtigungen<br>Anmeldung mit Schema-Owner nur für Release-Prozess möglich (durch DBA)<br>ANY-Privilegien werden nicht benutzt (oder Benutzung ist genehmigt)<br>PUPLIC-Privilegien werden nicht benutzt (oder Benutzung ist genehmigt)<br>Public-Privilegien werden von kritischen Packages entfernt siehe Privilegierte Packages<br>Datenbank-Parameter gesetzt entsprechend „Datenbank-Parameter" | Verschlüsslung der Datenfiles, Backups und Netzwerks durch Advanced Security Option<br>Anonymisierung des Testsystems (z.B. Data Masking)<br>Anonymisierung der Exports für Softwarelieferenten<br>Personalisierte Accounts für OS und DB | Database Vault |
| | **Auditing** | **Auditing**<br>Standardauditing, Optionen siehe "Empfohlene Audit-Optionen (intern)"<br>Aufbewahrung: 6 Monate | **Auditing**<br>Standardauditing auf kritische Tabellen/Transaktionen, Privilegien und Benutzermanagement<br>siehe "Empfohlene Audit-Optionen Vertraulich"<br>Aufbewahrung min. 2 Jahre | **Auditing**<br>Audit Vault (oder anderes Tools wie z.B. Sentrigo Hedgehog)<br>Aufbewahrung:<br>7 Jahre |
| | **Patching**<br>Einspielen von Patchsets max. 3 Monate nach erscheinen | **Patching**<br>2x pro Jahr Einspielen von CPUs/PSUs bzw. von Patchsets (wenn verfügbar) | **Patching**<br>Einspielen von CPUs/PSUs max. 1 Monat nach Erscheinen | |
| | | **Review**<br>Initialer Review, Bericht über Security-relevante Parameter, Any-Privilegien, ... | **Review**<br>halbjährliches Review der DB, unterstützt durch Software (z.B. Tvd-SecAudit) | |

# Risk matrix (3)

- It is important to define the consequences (and costs)



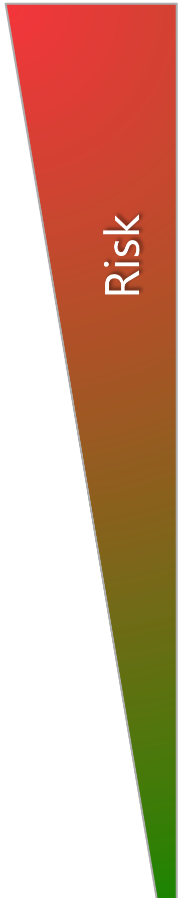
| KONSEQUENZEN | | | | |
|---|---|---|---|---|
| | | **Anforderungen an Data-Owner:**<br>Benutzer-, Rollen- und Privilegienkonzept muss zusammen mit Data-Owner definiert werden | **Anforderungen:**<br>Kritische Tabellen müssen definiert werden | **Anforderungen:**<br>Prozesse müssen geändert werden (z.B. Benutzer-management liegt beim Kunden) |
| | **Kosten**<br>**(jeweils unverhandelt pro Prozessor)** | **Kosten:**<br>Diskplatz (minimal) | **Kosten:**<br>Diskplatz (mittel)<br>ASO: 13k<br>Data Masking Pack: 13k<br>RepView: 1k pro DB | **Kosten:**<br>Diskplatz (hoch)<br>AV-Agent: 4k<br>AV-Server: 66k<br>Database Vault: 26k |

# AGENDA

1. Overview
2. Risk analysis and categorization
3. Risk Matrix
4. Risk minimization
5. Review

# Risk minimization - Authentication

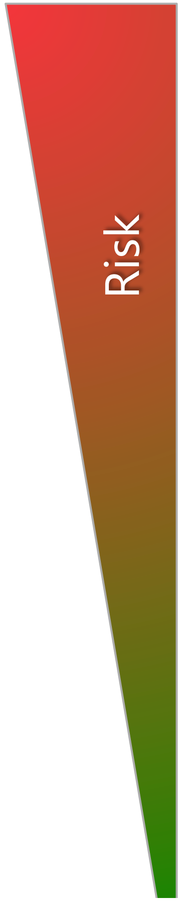
- All user are using a common / application user
- Each user has his own personal account
  - In the database and on the OS
- There is a central account management
  - Manage a central directory
  - Login through directory
    - E.g. Enterprise Users
  - Or provisioning of user into the databases
    - E.g. CUA4DB (Centralized User Administration for Database
- Strong authentication (more than just username and password)



- **Attention: Authentication is the basis for everything else!**

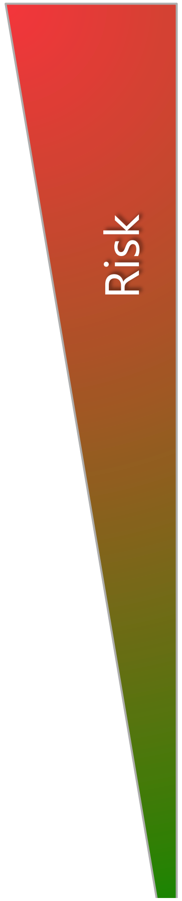
# Risk minimization - Passwords

- There is no password rule
- A password complexity rule exists
  - Minimal length
  - Numbers, special characters,….
  - Common words are not allowed
- **All** passwords must be changed on a regular basis
  - Passwords may not used again
  - Passwords must distinct from the old passwords
- Not interactive unused accounts are locked (or an impossible password is set)
  - Also valid for oracle default schema’s



# Risk minimization – Data access

- User can access / modify any data
- User can only access data for which the have privileges (on table level):
  - Role concept
  - No public grants
- User can only access data for which the have privileges (on table level (on row level):
  - Virtual Private Database (Security Policies)
  - Label Security
- Administrators do only have limited access
  - Database Vault
  - Encryption before data is stored in the database (Encrypted by the application or a encryption appliance like SafeNet)
  - Tokenization

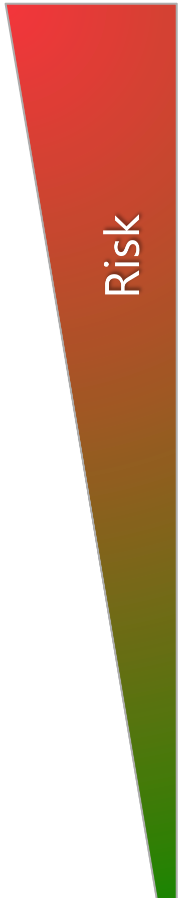


# Risk minimization – Data access - Comments

- It important to see how somebody has gained access to data :
  - Table owner
  - Direct grant on the table
  - Over a role (cascades)
  - Public grants
  - Over a view or a package
  - Using system privileges (select any table)
  - Using high privileges / roles (DBA, SYSDBA)
- Do not forget role changes (trainees do have the most rights…)
- Use tools to analyze data access an privileges e.g. Oracle Identity Analytics

# Risk minimization - Auditing

- No auditing
- Only basic operations are audited  (e.g.. connect)
- Audit critical operations
  - Use of ANY privileges
  - User- and role management
  - SYSDBA access
- Access on critical objects are monitored
  - Critical objects are defined
  - Rules when access must be audited are defined
- Central Auditing
  - Oracle Audit Vault
  - SYSLOG Auditing
  - McAfee Database Activity Monitoring

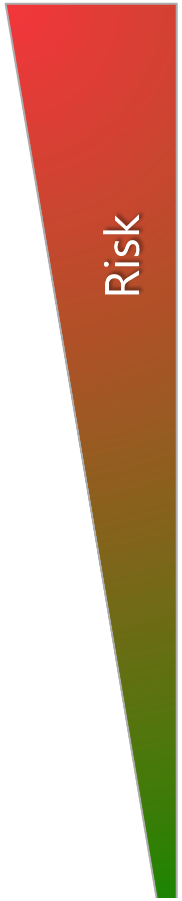


# Risk minimization - Auditing - Comments

- It’s common to audit only certain conditions
  - Use Fine Grained Auditing (FGA)
- Regularly review audit data
  - Reporting functionality when using a central auditing tool (Oracle Audit Vault)
  - Interpretation / Tools when using SYSLOG server
  - Manuel reporting if audit is stored in a database
  - Raise alarms for problems / violations!
- And how long should the audit data be kept?
  - Defined retention policies for raw data and reports
  - Automated Housekeeping
  - Archiving

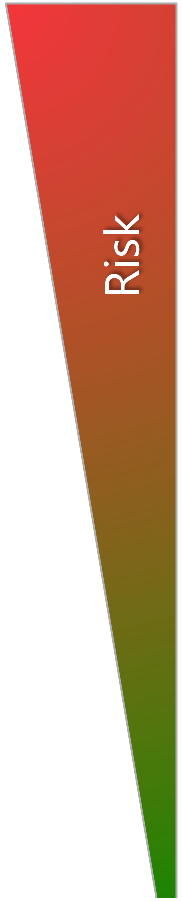
# Risk minimization - Patching

- Security patch’s and patch sets are not installed
- Regularly installation of patch sets (11.2.0.**3**)
- Regularly of CPUs or PSUs
- Prompt installation of all CPUs resp. PSUs
  - E.g. max. one month after CPUs has been released
- Virtual Patching
  - McAfee Database Activity Monitoring (additional protection for CPU/PSU)



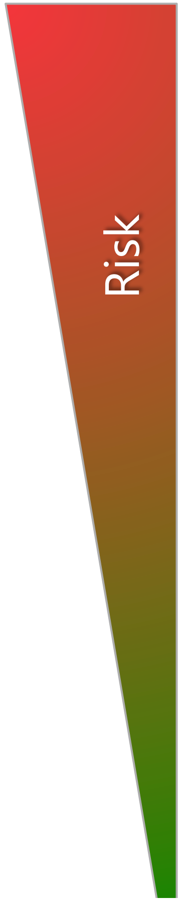
# Risk minimization – Oracle Software & Optionen

- Any Software and options are installed
- Only required options are installed in the database
  - Critical e.g. Java, XDB, …
- Only required software is installed in the oracle home
- Required options are harden
  - No public grants (regularly done by default for some options)
  - Role concept, grant privileges to user only if the require the functionality
  - Network Callouts (Mail, TCP, …) are limited



# Risk minimization – Parameter

- Initialization parameter can have any values
- Define a baseline for security critical parameters, eg
  - 07_DICTIONARY_ACCESSIBILITY
  - AUDIT_SYS_OPERATIONS, AUDIT_TRAIL
  - DB_BLOCK_CHECKING
  - REMOTE_OS_AUTHENT
  - REMOTE_OS_ROLES
  - UTL_FILE_DIR
- Enforce baseline
- Exceptions must be (eg required by an application) justified and documented



# Risk minimization – more options

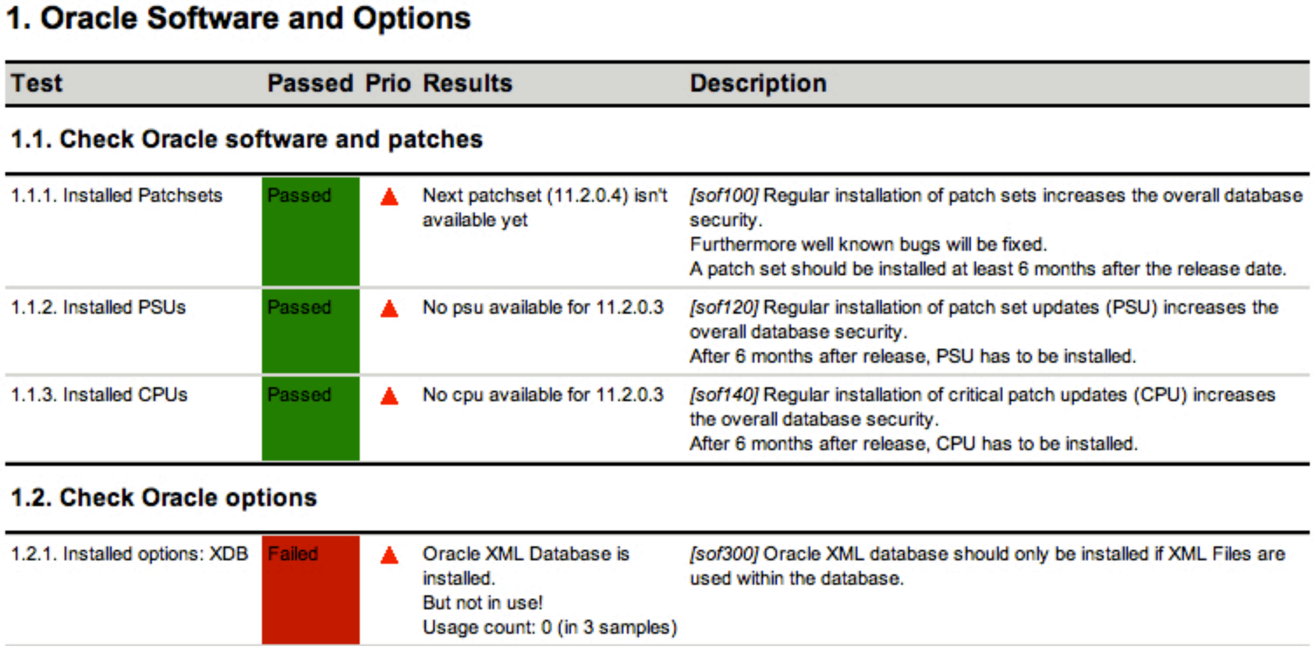
- Network:
  - Database Firewall (Oracle, Imperva)
  - Encryption (Advanced Security Option)
  - Zoning concept
- Release Management:
  - Who can when access as schema owner (which should be locked anyway)
  - Documentation of processes
- Anonymizing test data (Oracle Data Masking)
- Protect data files, exports, dumps and backup with encryption

# AGENDA

1. Overview
2. Risk analysis and categorization
3. Risk Matrix
4. Risk minimization
5. Review

# Verify the defined security measures

- Compliance with the defined security measures should be checked on a regular basis or even automatically
- Tor this purpose Trivadis offers TVDSecAudit©



### 1. Oracle Software and Options

| Test | Passed | Prio | Results | Description |
|---|---|---|---|---|
| **1.1. Check Oracle software and patches** | | | | |
| 1.1.1. Installed Patchsets | Passed | ▲ | Next patchset (11.2.0.4) isn't available yet | *[sof100]* Regular installation of patch sets increases the overall database security.<br>Furthermore well known bugs will be fixed.<br>A patch set should be installed at least 6 months after the release date. |
| 1.1.2. Installed PSUs | Passed | ▲ | No psu available for 11.2.0.3 | *[sof120]* Regular installation of patch set updates (PSU) increases the overall database security.<br>After 6 months after release, PSU has to be installed. |
| 1.1.3. Installed CPUs | Passed | ▲ | No cpu available for 11.2.0.3 | *[sof140]* Regular installation of critical patch updates (CPU) increases the overall database security.<br>After 6 months after release, CPU has to be installed. |
| **1.2. Check Oracle options** | | | | |
| 1.2.1. Installed options: XDB | Failed | ▲ | Oracle XML Database is installed.<br>But not in use!<br>Usage count: 0 (in 3 samples) | *[sof300]* Oracle XML database should only be installed if XML Files are used within the database. |

- http://www.trivadis.com/produkte/datenbank-tools/tvd-secaudittm.html

# Conclusion:

Security must be implemented comprehensively in many places.

First of all you have to know what you need

This is not always easy…

But we are happy to assist you ☺

?

Questions?

trivadis
makes IT easier.
ection Workshop
trivadis
makes IT easier.

# THANK YOU.

Trivadis AG

Stefan Oehrli

Europa-Strasse 5
CH-8152 Glattbrugg

Tel. +41 44 808 70 20

stefan.oehrli@trivadis.com
www.trivadis.com
www.oradba.ch

BASEL BERN LAUSANNE ZÜRICH DÜSSELDORF FRANKFURT A.M. FREIBURG I.BR. HAMBURG MÜNCHEN STUTTGART WIEN

makes IT easier.