Privacy

Insider Threats

Compliance

ORACLE

AUDIT VAULT

Dražen Pataric
Senior Sales Consultant
Oracle Hrvatska

HrOUG – 12. konferencija

Rovinj, 16. – 20. listopada 2007.

Oracle – 25 Plus Years of Security Leadership

Audit Vault
Database Vault
Content DB, Records DB
Secure Enterprise Search
Thor & Octet String (IdM Acquisitions)
Phaos, Oblix, (IdM Acquisitions)
Database CC Security Eval #18 (10g R1)
Transparent Data Encryption
VPD Column Sec Policies
Fine Grained Auditing (9i)
1st Database Common Criteria (EAL4)
Oracle Label Security (2000 8.1.7)
Virtual Private Database (1998)
Enterprise User Security (8i)
Database Encryption API
Kerberos Support (8i)
Support for PKI
Radius Authentication
Network Encryption (Oracle7)
Oracle Advanced Security introduced
First Orange Book B1 evaluation (1993)
Trusted Oracle7 MLS DB
Government customer (CIA – Project Oracle)

Sigurnost - zašto, kako?

razlozi …

1. Volja uprave

2. Zakoni, regulative

i rješenje …

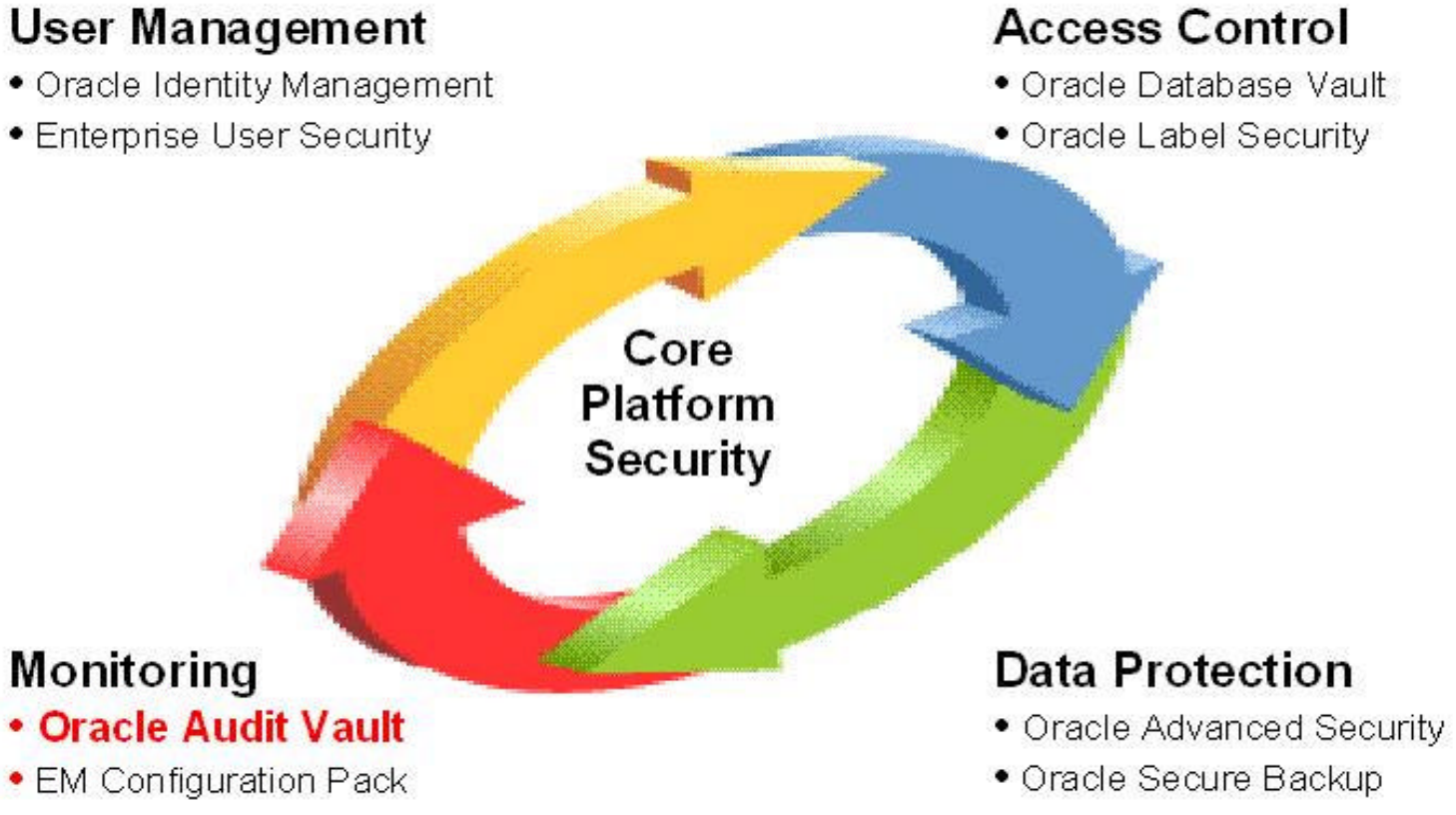
1. Pravila

2. Procedure

3. Provjera

Audit Vault

- **Monitoring alat**



Audit Vault

glavna funkcija u sigurnosnom dijelu sustava

Tocka na i

N E P O R E C I V O S T

Tehnicki problem sigurnosti

PROTURJECNOST

- **Aplikacija – omogucava da se nešto može**
- **Sigurnost – osigurava da se nešto NE može**
- **Neporecivost – netko je ipak ... a tko i što ?**

Izazovi auditinga

- fizicke razine sigurnosti -

Podaci na disku

Podaci u poslužitelju (OS)

Podaci u bazi

Podaci na mreži

Podaci u aplikaciji

Izazovi auditinga

- tko neovlašteno pristupa podacima -

Prijetnje izvana
- hakeri

Prijetnje iznutra
- nezadovoljni zaposlenici

Po Gartner-u:

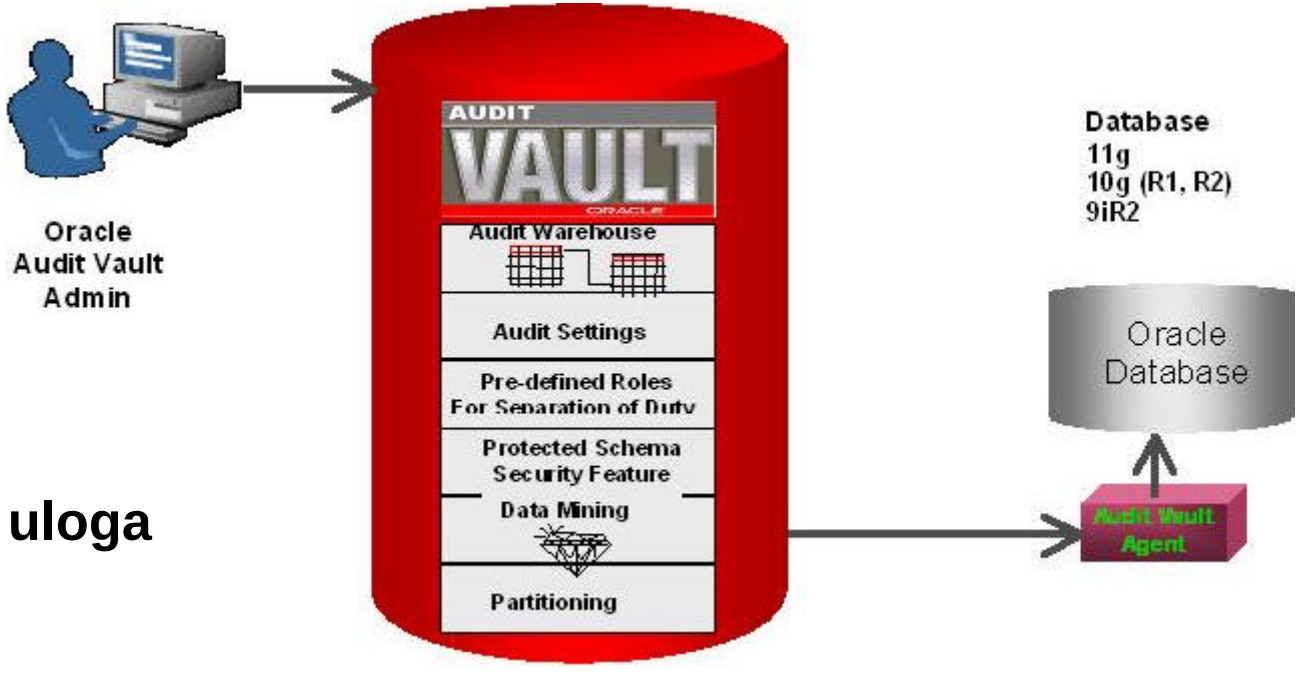
- preko 70% prijetnje IZNUTRA

Izazovi auditinga

- neovisnost -

Aplikacija na zasebnom poslužitelju

Struktura Audit Vaulta



Podjela uloga

Funkcionalnost AV

- zaštita repozitorija -
- BI nad skladištem -

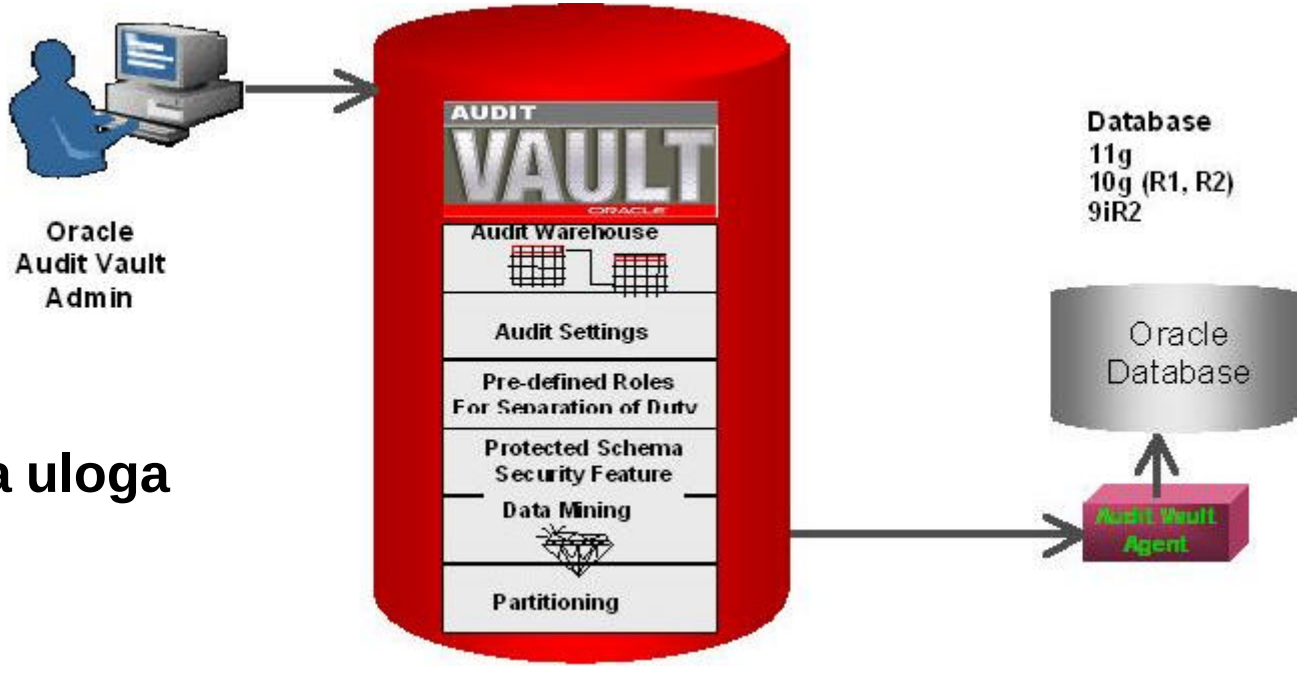
Network Encryption

Database Vault

Partitioning

Skladište podataka

Struktura Audit Vaulta



Podjela uloga

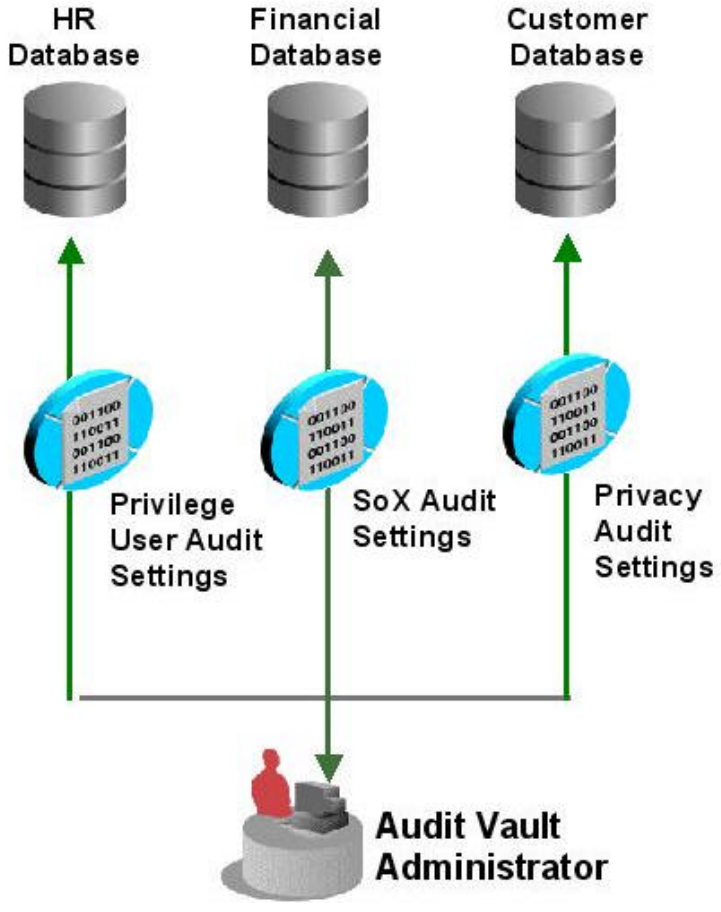
Funkcionalnost AV

- pravila auditinga -

Preko politika

- skupovi pravila
- mogu se kombinirati

jednostavno propagiranje na ciljnu bazu – preko agenata



Podjela uloga

Funkcionalnost AV

- izvori auditinga -

Audit trail u bazi

- obican i FGA

Aud datoteke a disku

Redo datoteke

Podjela uloga

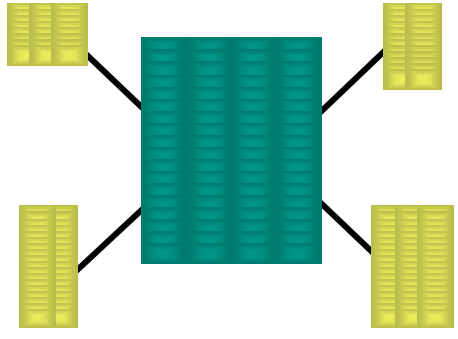
Audit Vault – analiza i izvještaji

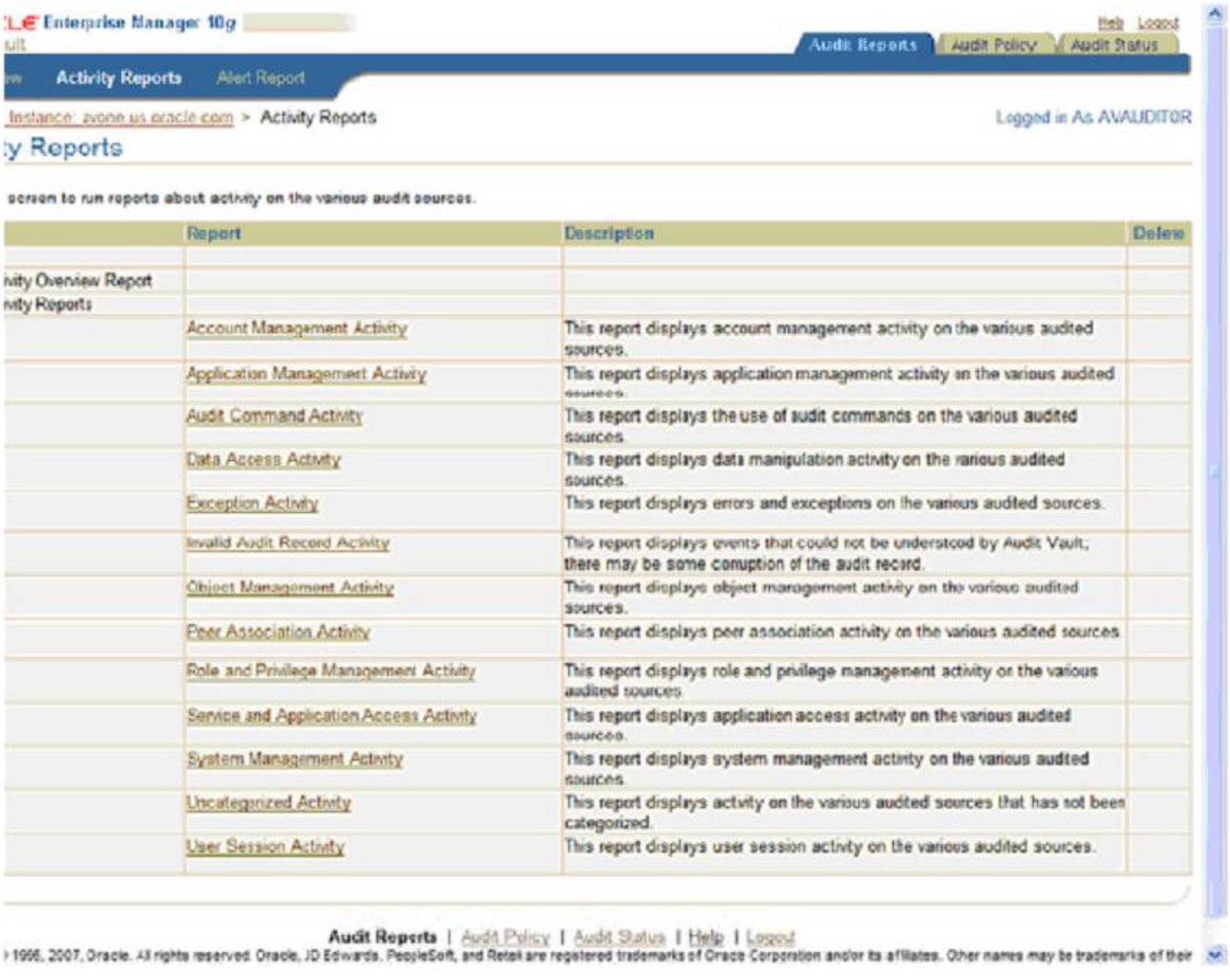
- Ugradena analiza
- Ugradeni izvještaji
- Ugraden sustav uzbunjivanja

- A ako to nije dosta ?
  - mogucnost pristupa preko BI alata (BI Publisher, BI Suite)
  - Korelirani izvještaji

schema repozitorija objavljena u dokumentaciji

Star schema




Enterprise Manager 10g
Help Logout
Audit Reports
Audit Policy
Audit Status
Activity Reports
Alert Report
Instance: avone.us.oracle.com > Activity Reports
Logged in As AVAUDITOR
y Reports
screen to run reports about activity on the various audit sources.
Report
Description
Delete
ivity Overview Report
ivity Reports
Account Management Activity
This report displays account management activity on the various audited sources.
Application Management Activity
This report displays application management activity on the various audited sources.
Audit Command Activity
This report displays the use of audit commands on the various audited sources.
Data Access Activity
This report displays data manipulation activity on the various audited sources.
Exception Activity
This report displays errors and exceptions on the various audited sources.
Invalid Audit Record Activity
This report displays events that could not be understood by Audit Vault; there may be some corruption of the audit record.
Object Management Activity
This report displays object management activity on the various audited sources.
Peer Association Activity
This report displays peer association activity on the various audited sources
Role and Privilege Management Activity
This report displays role and privilege management activity on the various audited sources.
Service and Application Access Activity
This report displays application access activity on the various audited sources.
System Management Activity
This report displays system management activity on the various audited sources.
Uncategorized Activity
This report displays activity on the various audited sources that has not been categorized.
User Session Activity
This report displays user session activity on the various audited sources.
Audit Reports | Audit Policy | Audit Status | Help | Logout
1996, 2007, Oracle. All rights reserved. Oracle, JD Edwards, PeopleSoft, and Retek are registered trademarks of Oracle Corporation and/or its affiliates. Other names may be trademarks of their

Privileged Users Activity - Past 24 Hours: JTAYLOR, SYSTEM, SYS

Privileged user activity over the past 24 hours: JTAYLOR, SYSTEM, SYS

Audit Source	User	Audit Event Category	Audit Event	Object	Client Host
VMSSRC2.ORACLE.COM	JTAYLOR	OBJECT MANAGEMENT	DROP TABLE	SCOTT.EMP1	vipshah-lap2
VMSSRC2.ORACLE.COM	JTAYLOR	OBJECT MANAGEMENT	DROP TABLE	SCOTT.EMP2	vipshah-lap2
VMSSRC2.ORACLE.COM	JTAYLOR	OBJECT MANAGEMENT	CREATE TABLE	SCOTT.EMP2	vipshah-lap2
VMSSRC2.ORACLE.COM	JTAYLOR	OBJECT MANAGEMENT	CREATE TABLE	SCOTT.EMP1	vipshah-lap2
VMSSRC2.ORACLE.COM	JTAYLOR	OBJECT MANAGEMENT	ALTER TABLE	SCOTT.EMP1	vipshah-lap2
VMSSRC2.ORACLE.COM	JTAYLOR	OBJECT MANAGEMENT	ALTER TABLE	JTAYLOR.EMP1	vipshah-lap2
VMSSRC2.ORACLE.COM	JTAYLOR	OBJECT MANAGEMENT	CREATE TABLE	SCOTT.EMP1	vipshah-lap2
VMSSRC2.ORACLE.COM	JTAYLOR	OBJECT MANAGEMENT	DROP TABLE	SCOTT.EMP1	vipshah-lap2
VMSSRC2.ORACLE.COM	JTAYLOR	USER SESSION	LOGON		vipshah-lap2
ORCL.US.ORACLE.COM	JTAYLOR	DATA ACCESS	SELECT	SH.SALES	raclinux1.us.oracle.com
ORCL.US.ORACLE.COM	JTAYLOR	USER SESSION	LOGON		raclinux1.us.oracle.com
VMSSRC2.ORACLE.COM	SYS	USER SESSION	LOGON		vipshah-lap2
ORCL.US.ORACLE.COM	sys	USER SESSION	SUPER USER LOGON		
ORCL.US.ORACLE.COM	/	USER SESSION	SUPER USER		

Audit Vault - zašto je važan?

- **Osigurava neporecivost**
- **Neovisan alat**
- Od koga štiti
  i od privilegiranih korisnika
- Zadovoljenje regulativa, podjela uloga

- Forenzika – tko je što i kada ?
  (postavke sustava i auditing-a)

Koji je cilj sigurnosti?

- Ukupno sigurnosno stanje i miran san vlasnika kompanija
- Zadovoljenje sigurnosnih propisa i regulativa

- Mogucnost provjere dogadaja
- Podjela uloga i odgovornosti
- Cijena ukradenog podatka

ORACLE

Information Company

ORACLE

Security Company

Pitanja ?