



ORACLE[®]

Protection of Personal Information (PoPI) Compliance

DANNY ILIC

Information Security Strategist



The Protection of Personal Information Bill - PoPI

- The Protection of Personal Information Bill, 2009, is intended to promote the protection of personal information processed by public and private bodies; to introduce information protection principles so as to establish minimum requirements for the processing of personal information; to provide for the establishment of an Information Protection Regulator; to provide for the issuing of codes of conduct; to provide for the rights of persons regarding unsolicited electronic communications and automated decision making; to regulate the flow of personal information across the borders of the Republic; and to provide for matters incidental thereto.



PoPI Principles

<p>Principle 1: Accountability</p>	<p>The party or institution that holds personal information must give effect to the principles for the protection of personal information as set out in the Bill.</p>
<p>Principle 2: Processing Limitation</p>	<p>Personal information must be collected directly from the data subject and may only be processed with the consent of the data subject, or where it is necessary to comply with a legal obligation, public law duty or contractual obligation.</p>
<p>Principle 3: Specific Purpose</p>	<p>Personal information must be collected for a specific, explicitly defined and legitimate purpose. The data subject should be aware of the purpose for which the information is collected, and who the likely recipients of the information will be.</p>
<p>Principle 4: Further Processing Limitation</p>	<p>Personal information may not be processed further in a way that is incompatible with the purpose for which the information was collected initially. Thus, if information was processed for the purpose for which it was collected, it may only be processed further if it can be shown that the purpose for the further processing is compatible with the original purpose. The Bill provides guidelines to assist with such an assessment</p>



PoPI Principles

<p>Principle 5: Information quality</p>	<p>The person or institution that determines the purpose and means for processing personal information should ensure that the information is complete, not misleading, up to date and accurate.</p>
<p>Principle 6: Openness</p>	<p>Personal information may only be collected if the Commission was notified. Also, where personal information of a data subject is collected, the person or institution responsible for such collection must ensure that the data subject is aware of:</p> <p>The fact that the information is being collected;</p> <ul style="list-style-type: none"> • The name and address of the person or institution collecting the information; • Whether or not the supply of the information by that data subject is voluntary or mandatory and the consequences of failure to reply; and • Where the collection of information is authorised or required under any law, the particular law to which the collection is subject.
<p>Principle 7: Security Safeguards</p>	<p>The Bill requires the implementation of technical and organisational measures to secure the integrity of personal information, and to guard against the risk of loss, damage or destruction of personal information. Also, personal information should also be protected against any unauthorised or unlawful access or processing</p>
<p>Principle 8: Individual Participation</p>	<p>A data subject is entitled to the particulars of his or her personal information held by any institution or person, as well as to the identity of any person that had access to his or her personal information. The data subject is also entitled to require the correction of any information held by another party.</p>



5 Essential Components

Policies and Procedures

Document, Evaluate, Verify and Conclude

People

Align required skills and competencies with staff

Automate

Controls, Approvals and Business flows

Plan, Forecast and Monitor

Create, Manage, Update and Report

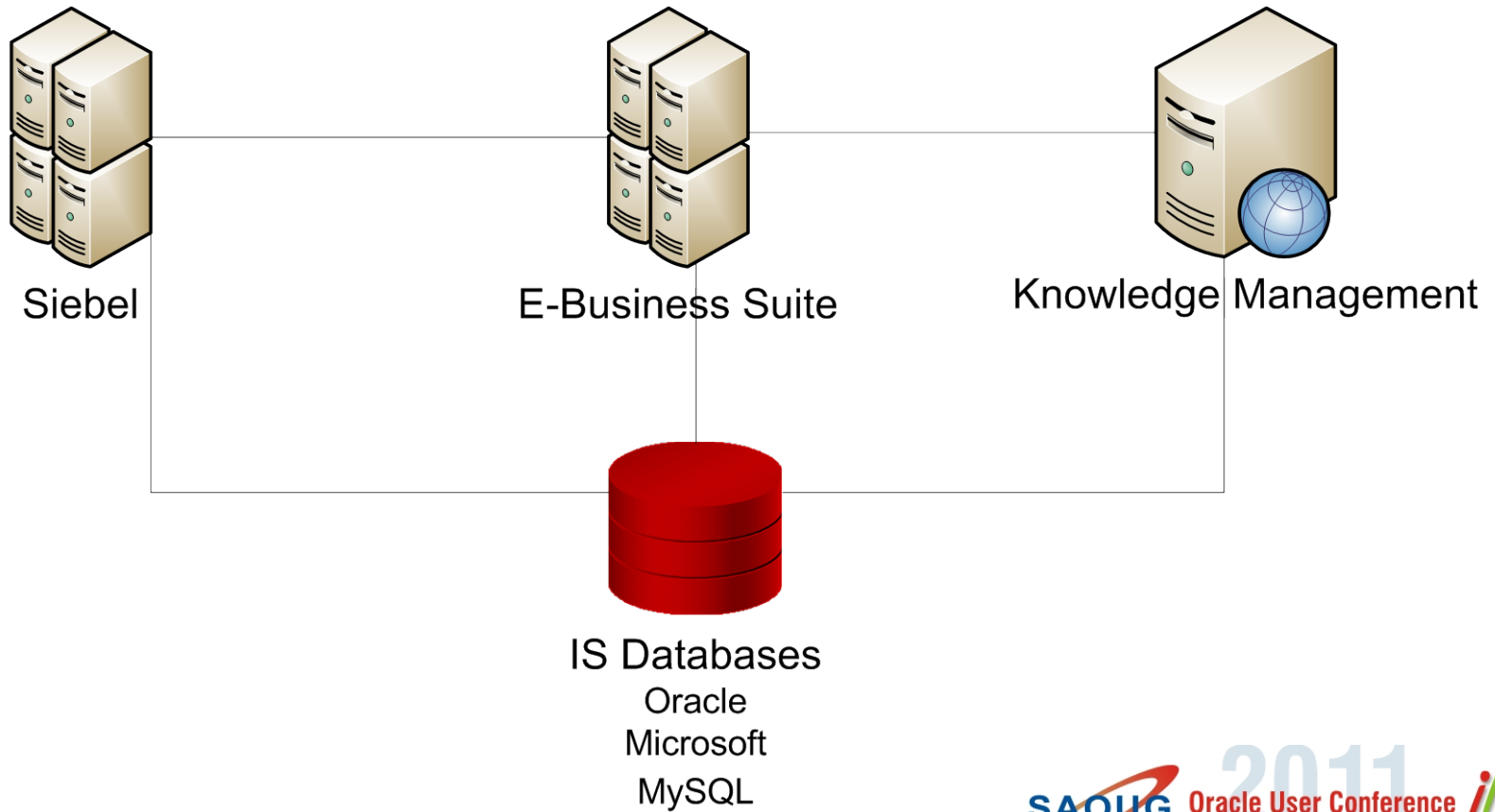
Secure IT Infrastructure

User Access and Provisioning, Data Security, Availability



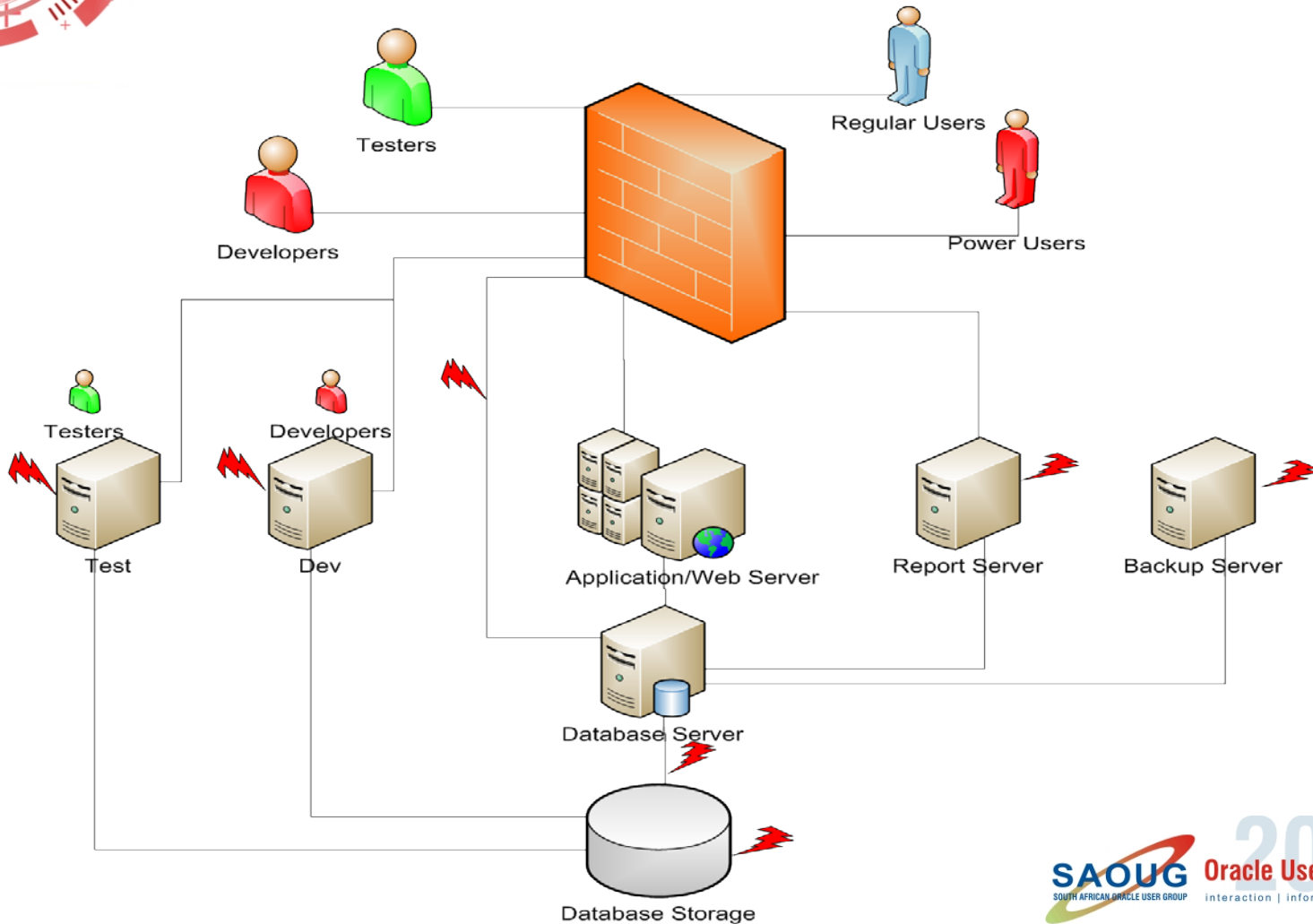


IS Systems with Personal Data Where PoPI will Apply





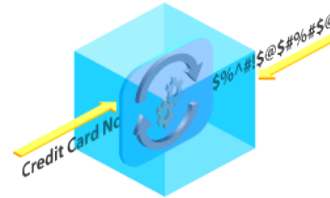
Areas Where Personal Data Can Be Accessed



Strategy - Protect Personal Data “Data Lifecycle Protection”



On the network



In the Data Store



On POS device



Backup/Storage



In email



Benefits of Unified Approach



- A unified security infrastructure provides...
 - A framework to meet stringent PoPI requirements
 - Robust, highly available security services that can be leveraged by all systems
 - Sustainability & Scalability to support business
- Which leads to...
 - Lowest total cost of ownership
 - Increased business agility
 - Opportunity for new revenue channels



Oracle Can Help with PoPI Requirements



Principle 1 - Accountability

- This requires policies and procedures to be reviewed and implemented.



Principle 2 - Processing Imitation

- Policy and procedures for “consent management”
- Oracle Audit Vault for centralization of audits to monitor data
- Oracle Database Vault can control access to the data



Principle 3 - Specific purpose

- Policy and procedures for the collection of data
- Oracle Audit Vault for centralization of audits to monitor data
- Oracle Database Vault can control access to the data



Principle 4 - Further Processing Limitation

- Policy and procedures for the processing of data
- Oracle Audit Vault for centralization of audits to monitor the data



Principle 5 - Information Quality

- Policy and procedures for the processing of data



Principle 6 - Openness

- Policy and procedures for the collection of data and to inform the subject
- Oracle Audit Vault for centralization of audits to monitor data – making sure that the data is not collected for any other purpose
- Oracle Database Vault can control access to the data – making sure that the data is only accessed by the correct person and the correct time



Principle 7 - Security Safeguards

- Policy and procedures for securing the data
- Oracle Audit Vault for centralization of audits
- Oracle Database Vault to control access to the data
- Oracle Advanced Security Option can encrypt DBA traffic to database
- Oracle Transparent Data Encryption encrypts data at rest
- Oracle Secure Backup encrypts tape backups
- Oracle Database Masking – for test and dev environments
- Oracle Identity and Access Management
 - Centralizes web security
 - Proof of compliance
 - Provides Attestation
 - Automates enabling/disabling accounts
 - Helps with “Orphaned account” issues
- Oracle Label Security provide stronger internal controls

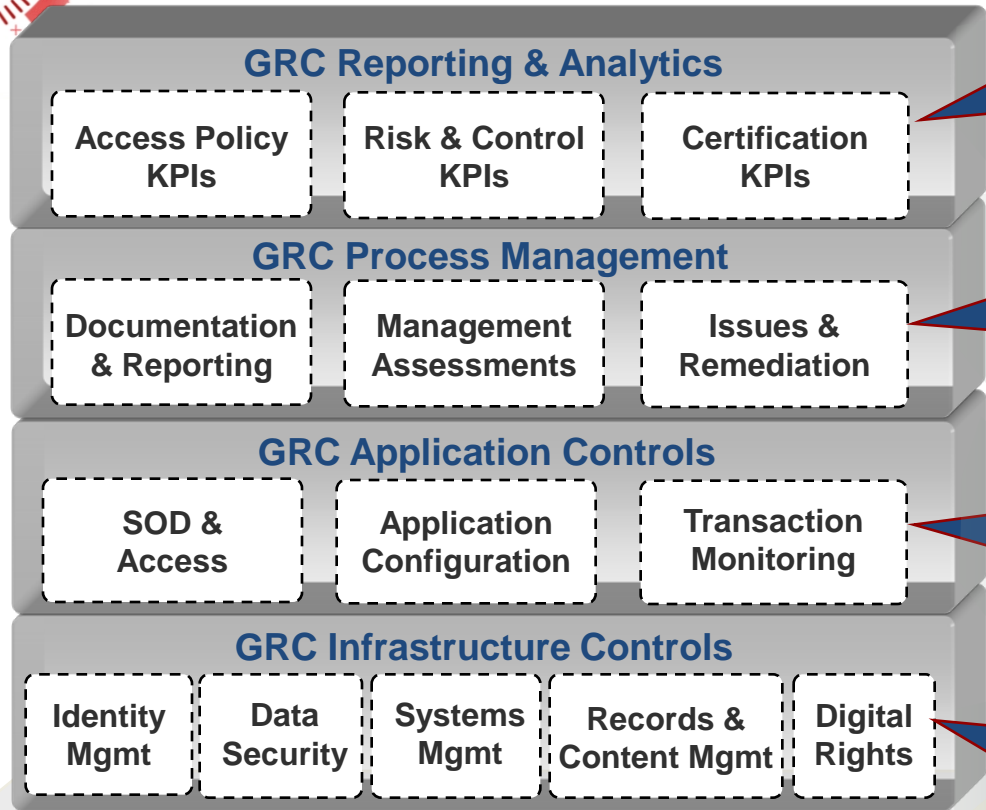


Principle 8 - Individual Participation

- Policy and procedures for securing the data
- Oracle Audit Vault for centralization of audits
- Oracle Database Vault to control access to the data



Oracle Solutions for GRC



- ✓ Pre-built dashboards aggregate information from all sources
- ✓ Produce Attestations & disclosures
- ✓ Configure to meet your needs

- ✓ GRC system of record
- ✓ End-to-end GRC process management
- ✓ Closed-loop issue remediation

- ✓ Preventive and detective controls
- ✓ What-if risk simulation
- ✓ Automated controls testing

- ✓ Protect sensitive data
- ✓ Enforce configurations and change management
- ✓ Reduce risk of legal liability

ORACLE® Hyperion® JDE EDWARDS® PeopleSoft®

SIEBEL SAP Custom or Legacy Applications

Oracle Identity Management

deliver the
PROMISE



Provisioning & Identity Administration

Roles-based User Provisioning
Password Management
Self Service Request & Approval

Access Management

Authentication, SSO & Fraud Prevention
Authorization & Entitlements
Web Services Security
Information Rights Management

Directory Services

LDAP Storage
Virtualized Identity Access



Identity Analytics

Reporting Attestation SoD Mining

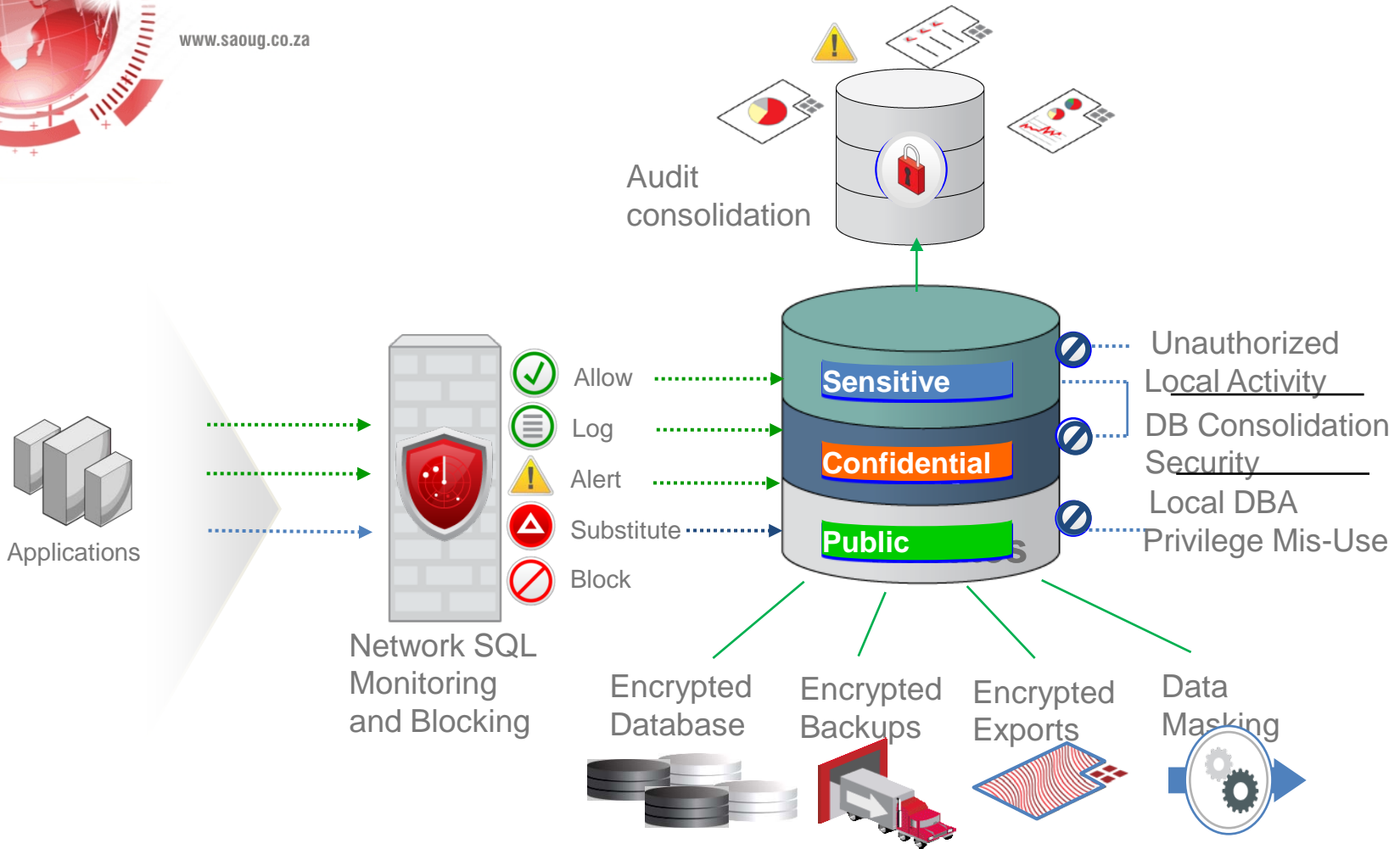


Platform Security Services

Identity Services for Developers



Big Picture



Oracle Technologies for PoPI

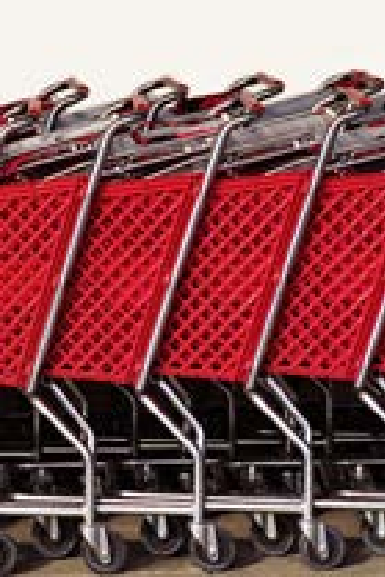
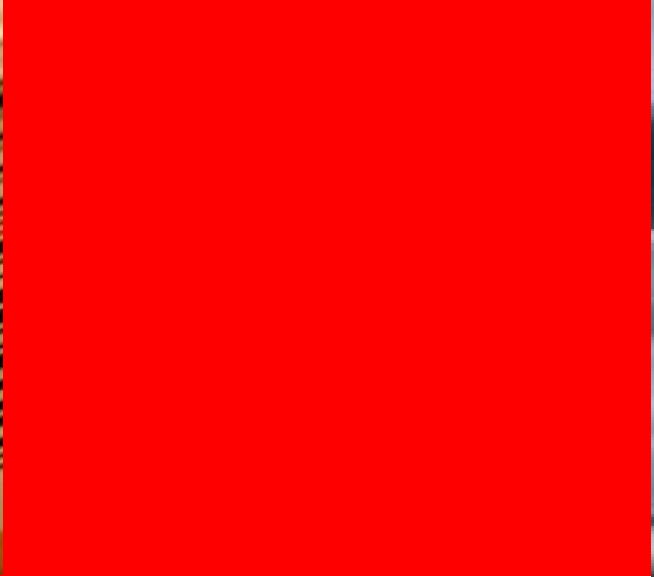


- Oracle Identity & Access Management Suite
 - Oracle Access Manager
 - Oracle Identity Manager
 - Oracle Identity Federation
 - Oracle Virtual Directory
- Oracle Label Security
- Advanced Security Option
 - Transparent Data Encryption
 - Network Encryption
 - Strong Authentication
- Oracle Database Vault
- Oracle Audit Vault
 - Options:
 - Oracle Applications
 - » Governance Risk and Compliance



Questions





ORACLE®