PeopleSoft

How to Control and Secure Your DBAs and Developers

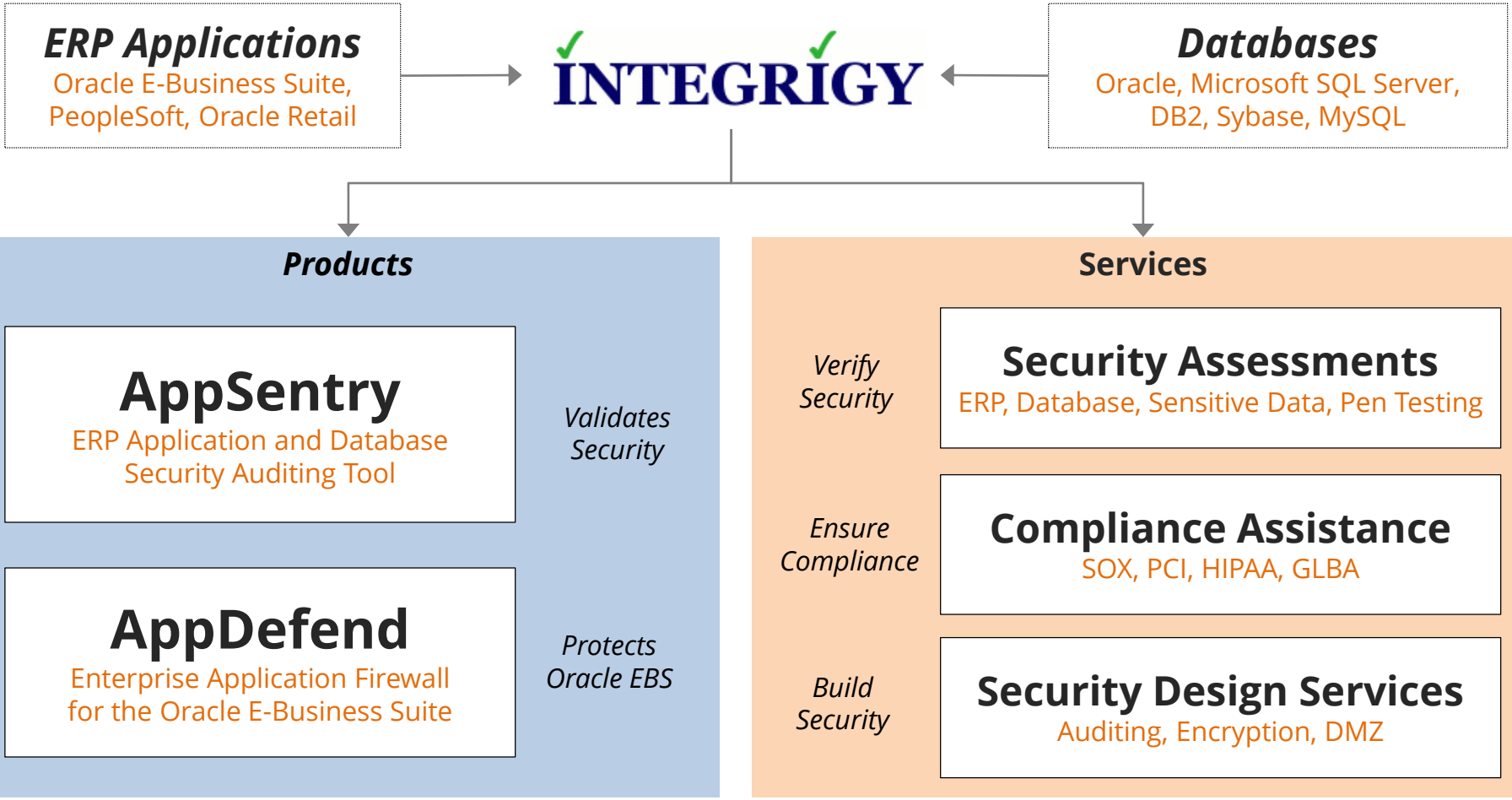
March 9, 2017

Mike Miller
Chief Security Officer
Integrigy Corporation

Stephen Kost
Chief Technology Officer
Integrigy Corporation

Phil Reimann
Director of Business Development
Integrigy Corporation

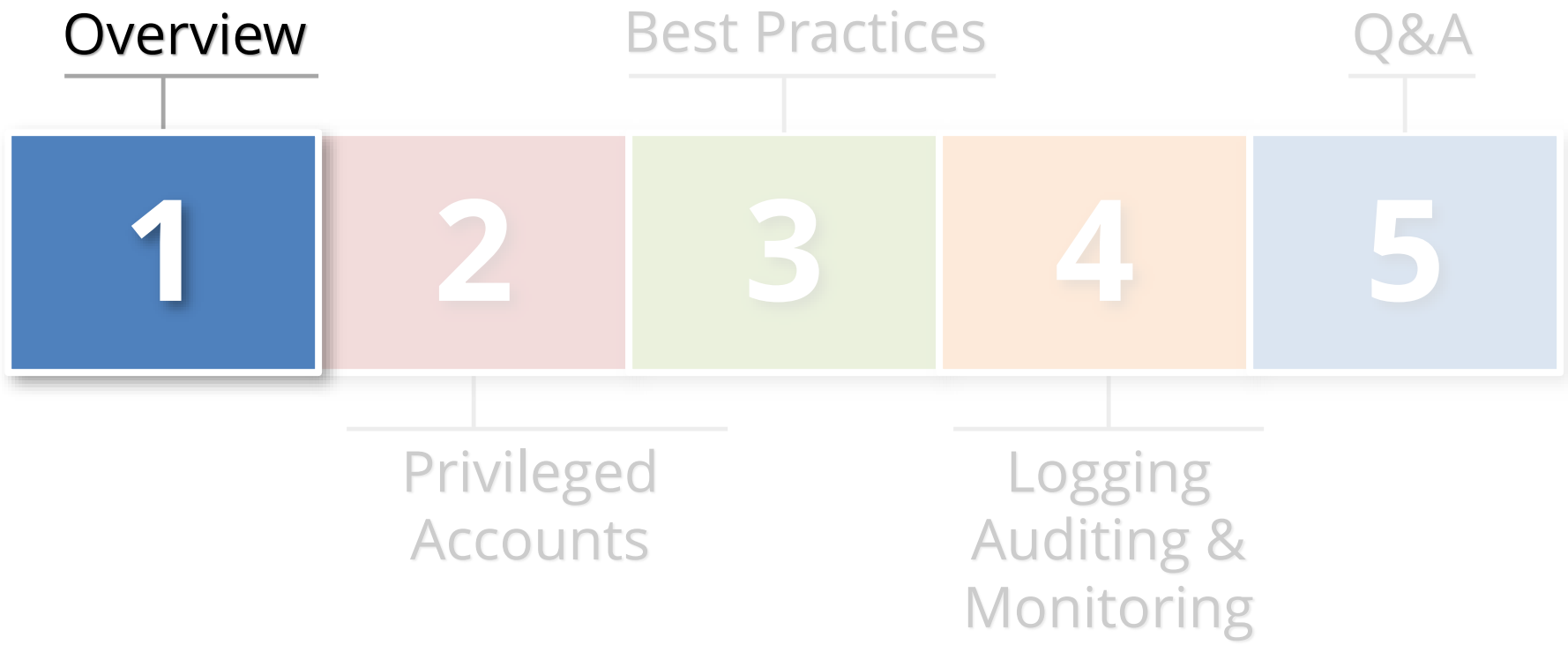
About Integrigy



Agenda


Overview
Best Practices
Q&A
1
2
3
4
5
Privileged Accounts
Logging Auditing & Monitoring

Agenda


Overview
Best Practices
Q&A
1
2
3
4
5
Privileged Accounts
Logging Auditing & Monitoring

{ generic privileged account }

application, database, or operating system account used for administration by **multiple people** and has **significant privileges**

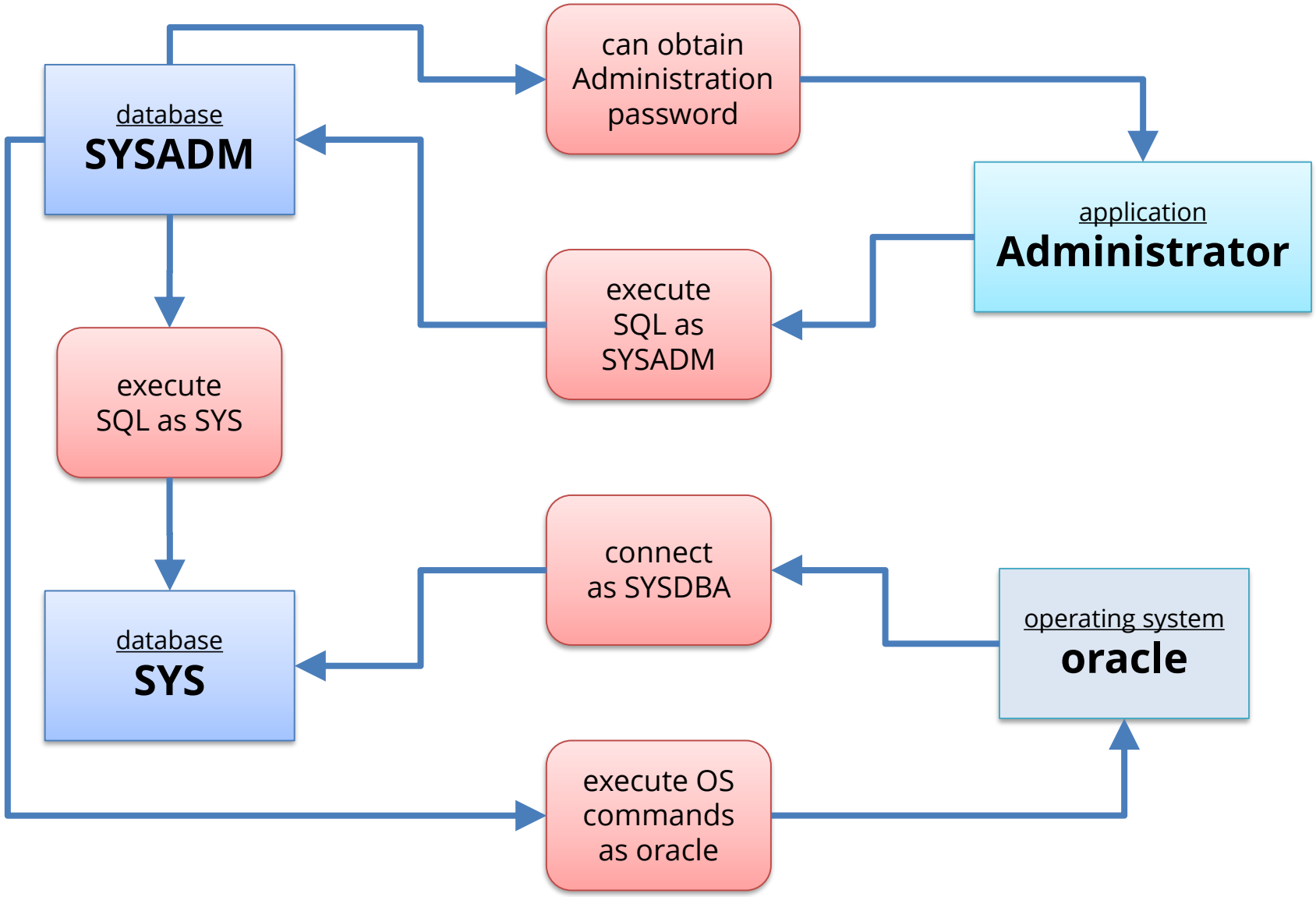
Generic Privileged Accounts

- **PeopleSoft is defined by generic privileged accounts in each layer of the technology stack**
  - Multiple highly privileged accounts
  - Generic accounts that must be used to manage the application and database
- **Majority of all data breaches committed by insiders**
  - Some intentional
  - Most accidental

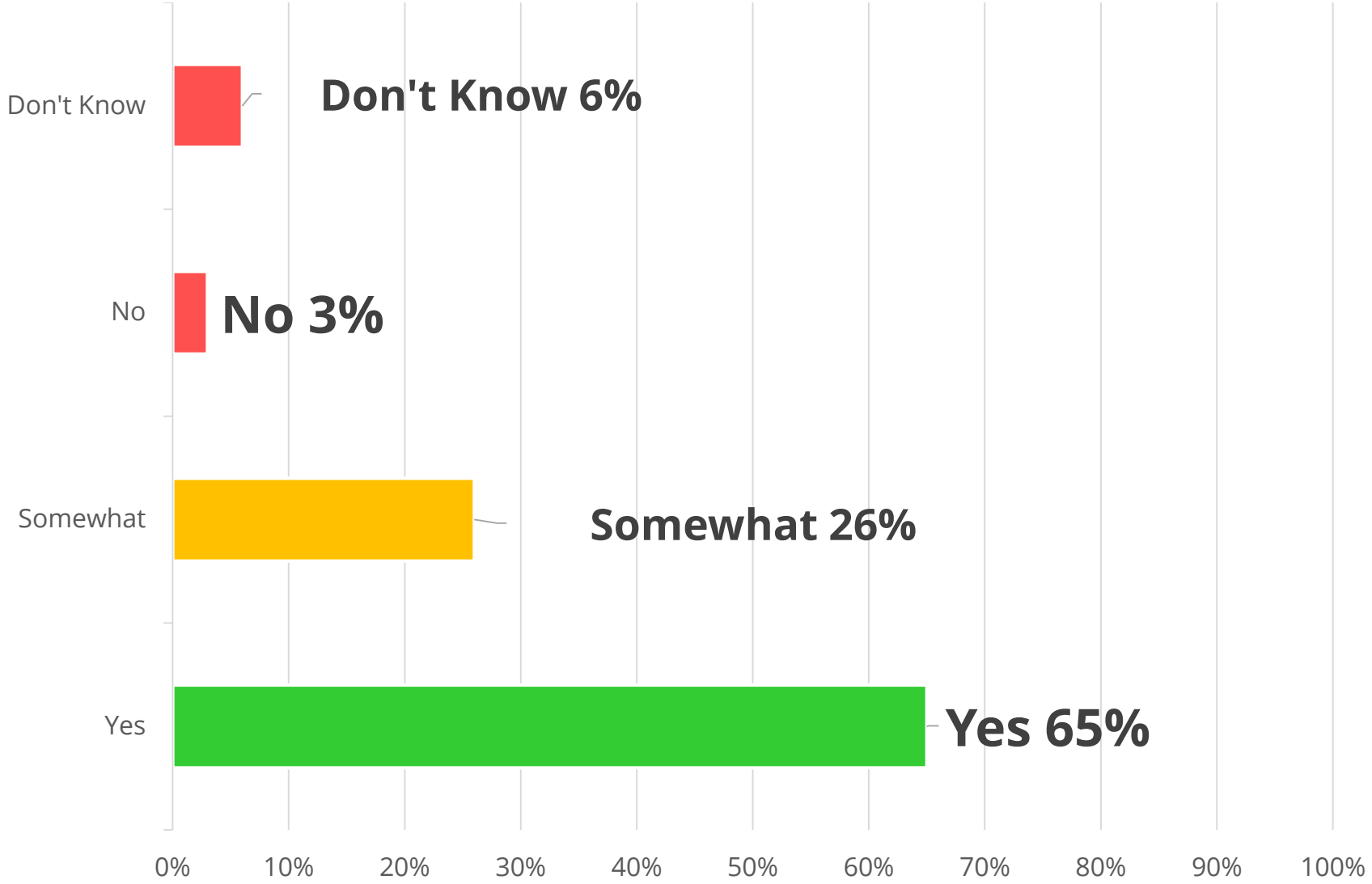
PeopleSoft Generic Privileged Accounts

PeopleSoft Application	**Administrator, Guest,** **Web Profile, Scheduler** *seeded application accounts*
Oracle Database	**SYSADM, PEOPLE** **SYS, SYSTEM**
Operating System *(Unix and Linux)*	**root** **oracle**

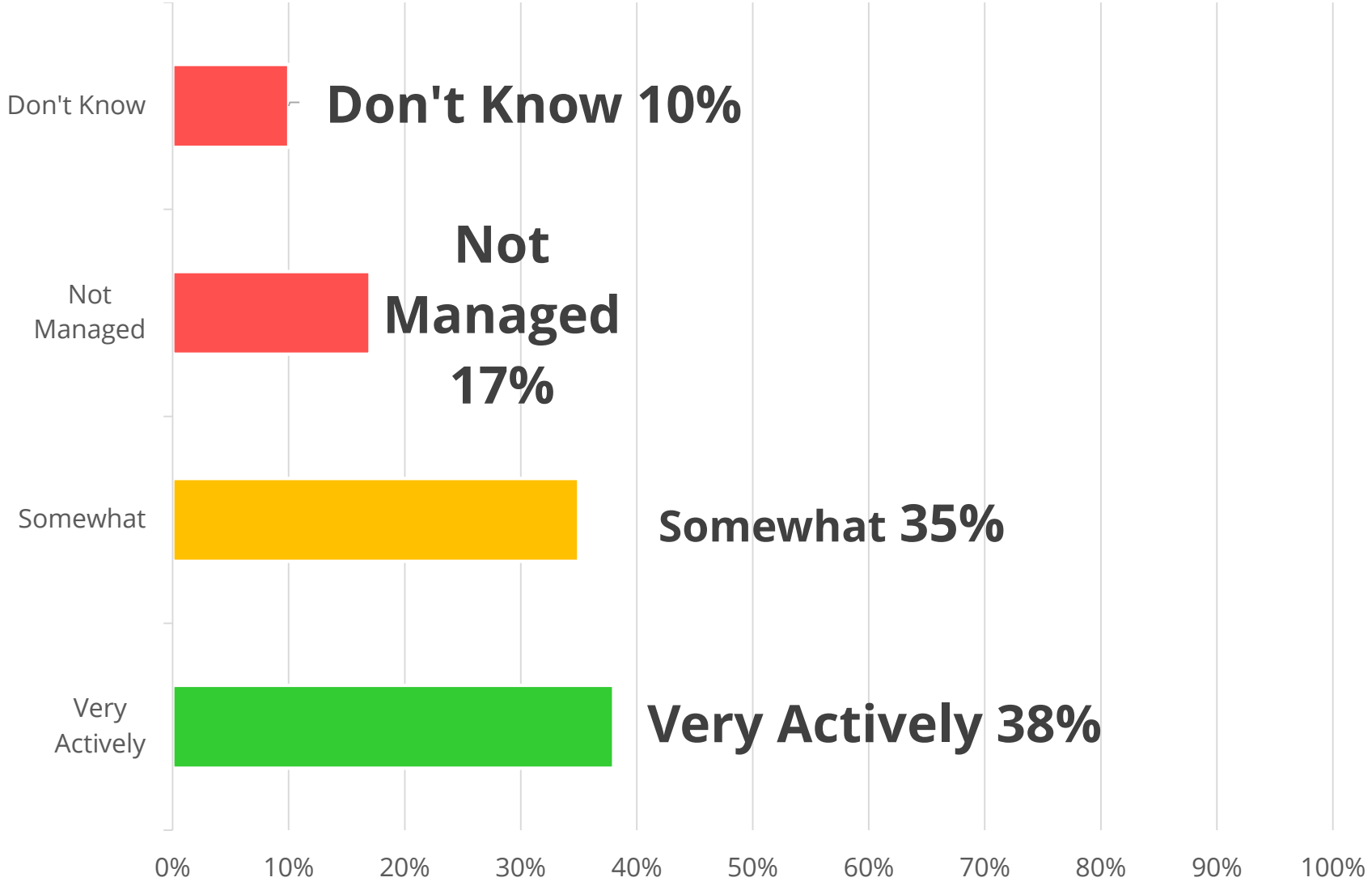
Generic Privileged Account Inter-Dependency



How Concerned About Privileged Accounts?



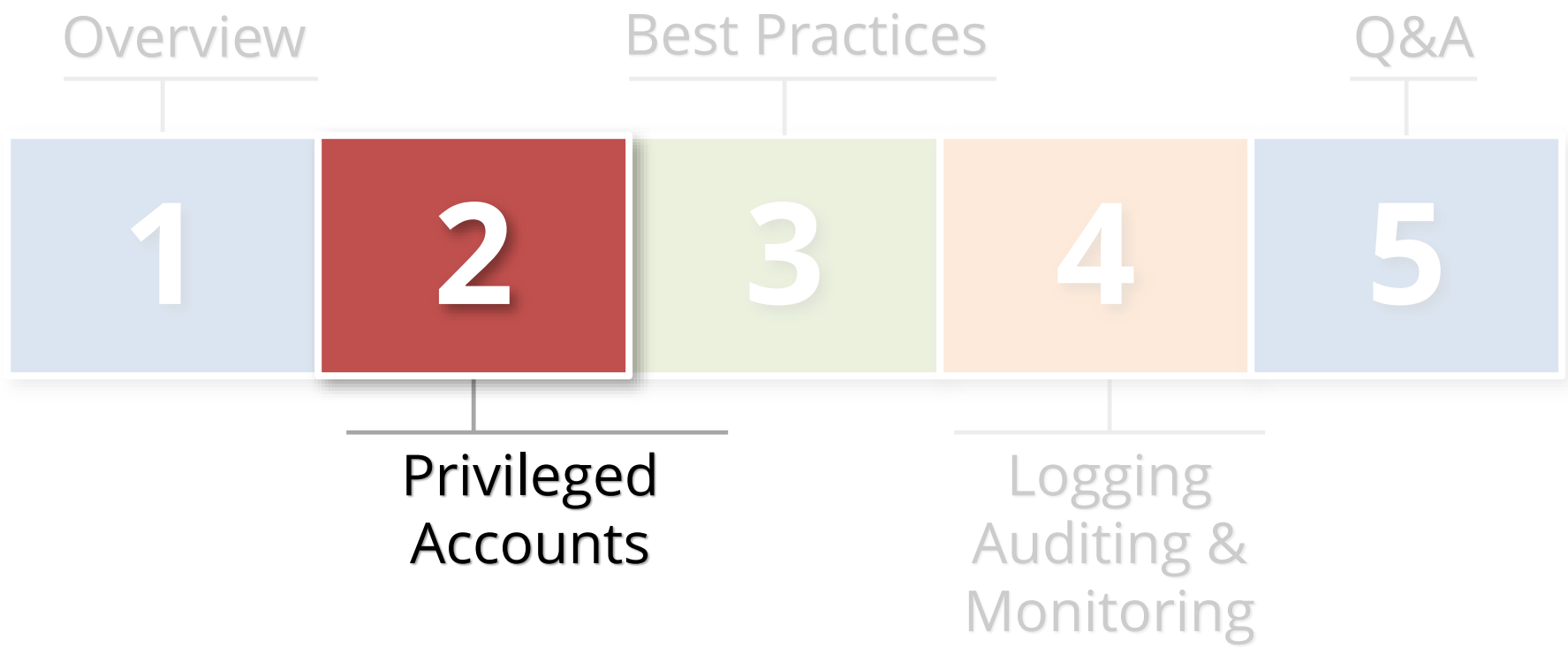
How Actively Managed are Privileged Accounts?



Security 101

- **Restrict access**
  - Physical and Logical (network)
- **Least privilege & use of generic accounts**
  - Everyone should not have access to everything
- **Password governance**
  - Common sense is not all the common
- **Trust-but-verify**
  - Logging and auditing

Agenda


Overview
Best Practices
Q&A
1
2
3
4
5
Privileged Accounts
Logging Auditing & Monitoring

Generic
Privileged
Accounts

PEOPLESOFT

More than Administrator Role

- **Twenty Five (25+) power user roles need to be secured**
  - See table below
- **Who might have access?**
  - Application administrators
  - Application DBAs
  - Support and power users
  - Helpdesk
  - Consultants and subcontractors

ADMINISTER_SECURITY	MAINTAIN_SECURITY	PTPP_PORTAL_ADMIN
APPLICATION_DESIGNER	MANAGE_INTEGRATION_PROCESS	QUERY
APPLICATION_ENGINE	MANAGE_INTEGRATION_RULES	QUERY_MANAGER
CUBE MANAGER	MASS_CHANGE	TI_INTEGRATION
DATA_MOVER	NVISION	TREEMANAGER
DEFINITION_SECURITY	OBJECT_SECURITY	UTILITIES
FPY_INTEGRATION	PORTAL_ADMIN	WEB_PROFILE
FT_INTEGRATION	PROCESS_SCHEDULER	WORKFLOW_ADMINISTRATOR
IMPORT_MANAGER)		

PeopleSoft Power Users

Control	▪ Power user accounts should only be used for a few specific functions – named accounts for all other administration activities ▪ Change ticket required for all use in production ▪ Use custom generic, less privileged account for scheduled concurrent programs and proxy user ▪ Change password when cloning ▪ Frequently rotate passwords (90 days) ▪ **Manage password** in password vault *[Vault]*
Log & Monitor	▪ Implement auditing for all usage *[Framework]* ▪ Alert on login and monitor all usage
Audit	▪ Check last password change date ▪ Verify password complexity and length settings ▪ Interview to determine how passwords are controlled

Seeded Generic Application Accounts

- **Twenty Five (27+) generic accounts created by installation**
  - See table below
- **Who might have access?**
  - Application administrators
  - Application DBAs
  - Support, helpdesk, power users
  - Consultants and subcontractors

BELHR	JCADMIN1	PSJPN
CAN	NLDHR	PSPOR
CFR	PS	TIME
CNHR	PSCFR	UKHR
ESP	PSDUT	UKNI
FRA	PSESP	USA
FRHR	PSFRA	HSHR
GER	PSGER	WEBGUEST
GRHR	PSINE	WEBMODEL

Seeded Generic Accounts

Control	▪ **End-date** per best practices if not explicitly required per documentation ▪ Use complex passwords ▪ As of PeopleTools 8.53 all User IDs are installed with unique site specific passwords
Log & Monitor	▪ Implement auditing for all usage or access *[Framework]* ▪ Alert on any attempt to externally access (DMZ)
Audit	▪ Review usage of accounts for external access (DMZ) ▪ Check end-date and last use ▪ Check last password change date ▪ Check for new seeded accounts after any major patches or upgrades

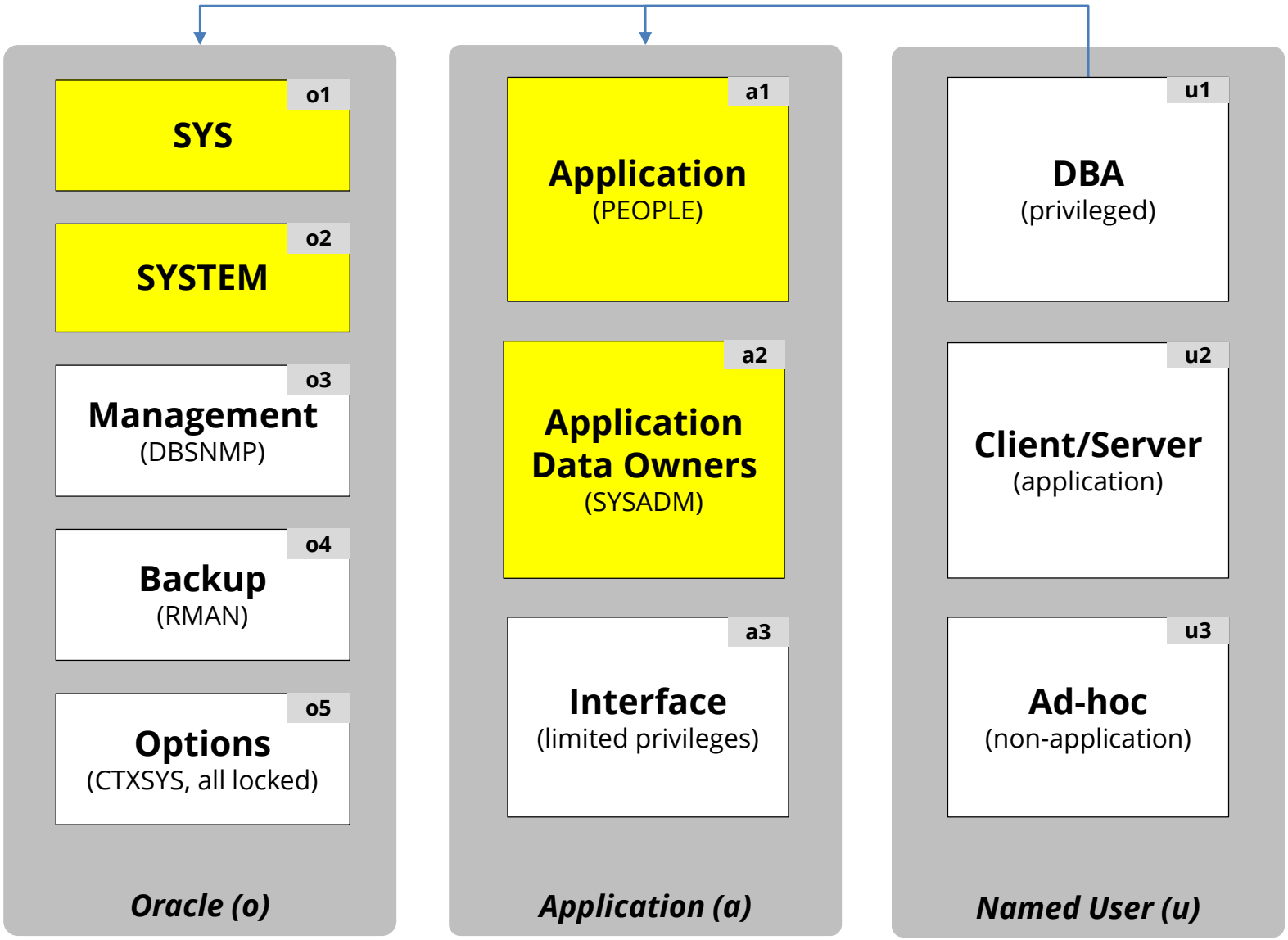
PeopleTools Access

Control	▪ Ensure access is **appropriate** ▪ Don't forget about SQR folder access and error correction mode
Log & Monitor	▪ Implement auditing for all usage or access *[Framework]* ▪ Alert on any attempt to access externally (DMZ)
Audit	▪ Review usage of accounts for external access (DMZ) ▪ Check end-date, last use, last password change date

Generic
Privileged
Accounts

DATABASE

Integrigy Database Account Classification (Oracle)



PeopleSoft Database Accounts

Oracle Database	**SYS**	▪ Owner of database ▪ Must be used for some operations
	SYSTEM	▪ Generic DBA account
PeopleSoft	**SYSADM**	▪ Must be used for maintenance ▪ SYSADM can access all data, including encrypted sensitive data ▪ Should not be directly accessed
	PEOPLE	▪ Application Connect Id account for all access
	Integration Broker (IB)	▪ Significant privileges ▪ Change using PeopeTools only

Oracle Database Account Passwords

Database Account	Default Password	Exists in Database %	Default Password %
SYS	CHANGE_ON_INSTALL	100%	3%
SYSTEM	MANAGER	100%	4%
DBSNMP	**DBSNMP**	**99%**	**52%**
OUTLN	**OUTLN**	**98%**	**43%**
MDSYS	MDSYS	77%	18%
ORDPLUGINS	ORDPLUGINS	77%	16%
ORDSYS	ORDSYS	77%	16%
XDB	CHANGE_ON_INSTALL	75%	15%
DIP	DIP	63%	19%
WMSYS	WMSYS	63%	12%
CTXSYS	**CTXSYS**	**54%**	**32%**

* Sample of 120 production databases

SYS Database Account

Control	▪ **Control password** with password vault *[Vault]* ▪ SYS should only be used for a few specific functions – named DBA accounts for all other database management activities ▪ Change ticket required for use in production ▪ Change password when cloning
Log & Monitor	▪ Implement auditing for logins, key security and change management events *[Framework]* ▪ AUDIT_SYS_OPERATIONS = TRUE ▪ Reconcile usage to change tickets
Audit	▪ Check last password change date ▪ Interview to determine how password is controlled

SYSTEM Database Account

Control	▪ **Control password** with password vault *[Vault]* ▪ **SYSTEM should only be used for PS administration and patching** – named DBA accounts for all other database management functions ▪ Change password when cloning
Log & Monitor	▪ Implement auditing for logins, key security and change management events *[Framework]* ▪ Reconcile usage to change tickets
Audit	▪ Check last password change date ▪ Interview to determine how password is controlled

SYSADM Database Account

Control	▪ **Manage password** with password vault *[Vault]* ▪ **SYSADM should only be used for PS administration and patching** – named DBA accounts for all other database management functions ▪ Use custom database profile with no lockout but strong password controls ▪ Change password when cloning
Log & Monitor	▪ Implement auditing for logins, key security and change management events *[Framework]* ▪ Monitor closely for failed logins *[Framework]* ▪ **Attempt to reconcile** DBA usage to change tickets
Audit	▪ Check last password change date ▪ Review logins to see who else is using ▪ Interview to determine how password is controlled

Database Accounts – General IT Controls

Database Password Profiles

- Create organizational database password profiles for service and named users
- Assign these profiles to all accounts
- Never use the DEFAULT profile – routinely check for any accounts assigned
- Use custom password verify function that meets organizational password policy

Database Accounts – General IT Controls

Default Database Passwords

- Routinely check for default database passwords
- Check after all database upgrades and after major PS patches
- Use a tool like AppSentry rather than DBA_USER_WITH_DEFPWD that checks all accounts for many passwords

Generic
Privileged
Accounts

OPERATING SYSTEM

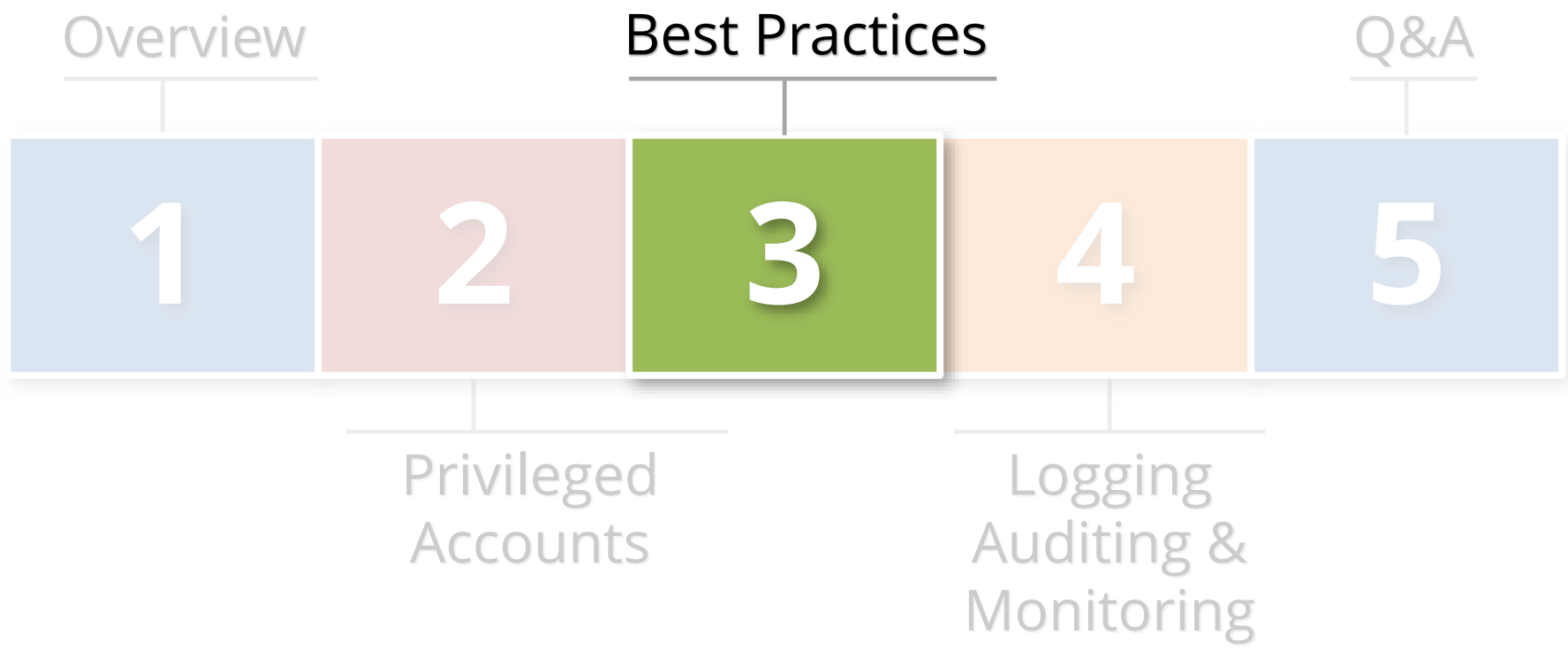
Oracle Account

Control	▪ **Control password** with password vault *[Vault]* ▪ **Prevent direct logins to oracle account** ▪ DBAs should have named OS accounts ▪ Require DBAs to use to su, sudo, or PowerBroker to access oracle and applmgr accounts ▪ Enforce a chain-of-trust – named user → generic user ▪ No developer access to production server OS
Log & Monitor	▪ Implement auditing at the OS level for all user logins ▪ Use keystroke or command logging if required ▪ Alert on direct logins to oracle or applmgr
Audit	▪ Check last password change date ▪ Interview to determine how password is controlled

Operating System – General IT Controls

- **DBAs should never have root access**
  - Require segregation of duties for operating system
- **DBAs should have named OS accounts**
  - Integrate with LDAP or Active Directory for authentication and access control
- **Avoid SSH key or trust logins**
  - Limit any use of password-less logins between servers
  - Do not allow for highly privileged accounts
  - Always use passphrases

Agenda


Overview
Best Practices
Q&A
1
2
3
4
5
Privileged Accounts
Logging Auditing & Monitoring

Best Practices to Control Privileged Accounts

- **Use a Bastion host (virtual desktop) for direct O/S and/or database access**
  - Restrict network access and/or database ACLs
  - Two-fact authentication to access
  - Use SSH Keys for appropriate O/S accounts
  - Install key logger
- **Consider Oracle Database Vault**
  - Additional license but comes with pack for PeopleSoft

Control Passwords to Control Privileged Accounts

- **Change defaults and don't use weak passwords**
  - Use a random password generator
- **Use different passwords for production**
  - Change all passwords when clone
- **No hardcoding of passwords**
  - E.g. where possible consider password vault APIs and Oracle Wallet(s)
- **Use approach of need-to-know and least privilege**
  - Separation of duties and job function
  - Minimum of PS, Database and O/S

Control Passwords to Control Privileged Accounts

- **Periodically inventory privileged and generic accounts**
  - Ask questions, cull and document
  - Take names and assign owners
- **Control passwords per risk classification of the account**
  - Rotate, expiry, complexity, length and half-passwords
  - One size does not fit all
- **Adopt formal privileged account and password policy**
  - Train and enforce
  - Make it real

Best Practices to Control Privileged Accounts

- **Do you have a policy to change privileged password when somebody leaves?**
  - Vendors included: managed services, hosting and cloud providers
- **Does your password policy govern generic privileged accounts or does it forbid them?**
- **When was the last time audited all privileged generic accounts?**
- **What is your policy for SSH logins?**

Best Practice: Use a Password Vault

- **Vaults are purpose built solutions for enterprise password management**
  - Sophisticated security
  - Robust standard reports
  - Built to support meet compliance requirements
- **Shrink trust perimeter and increase governance of privileged accounts**
  - Add all accounts passwords except those owned by named individuals
  - All service accounts
  - All generic accounts
  - Phased implementation (controlled vs. managed)

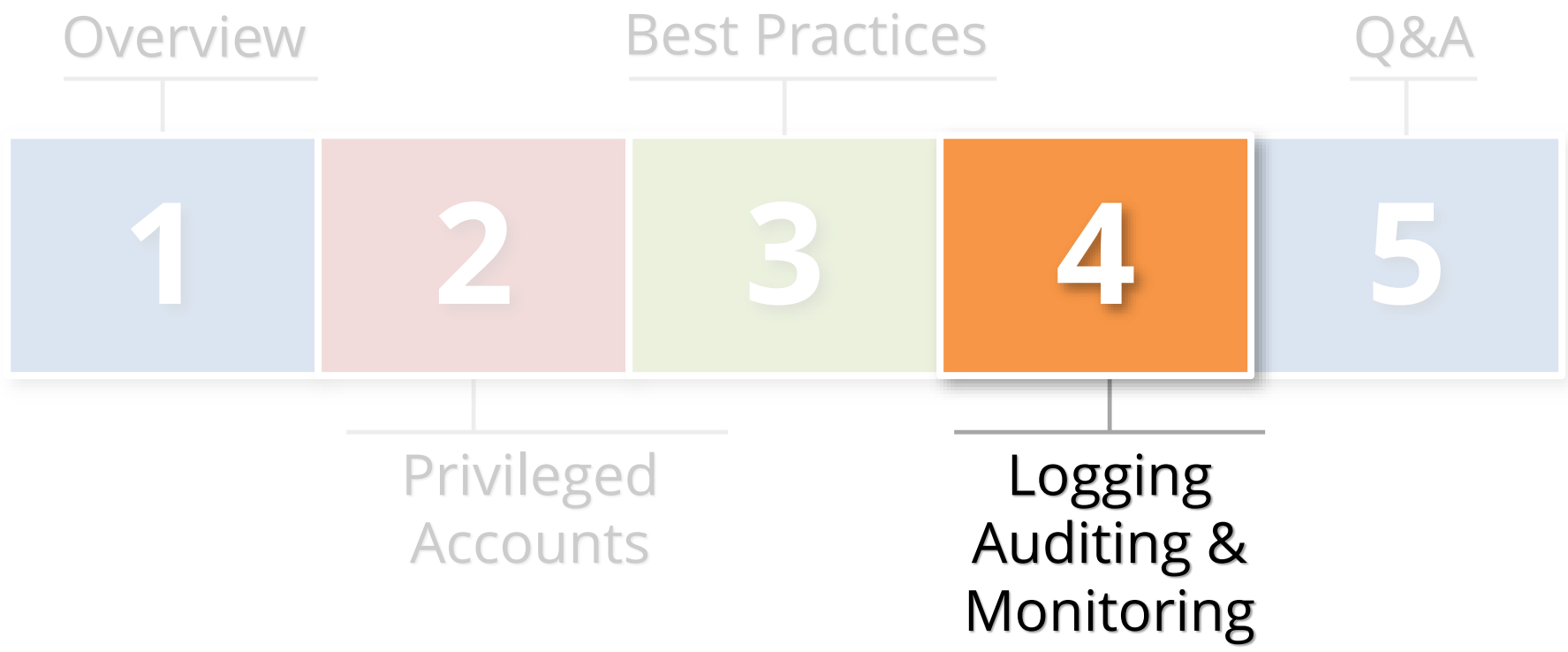
Password Vault Recommendations

- **Add field for ticket number for password pulls**
  - Required freeform text field to start
- **Use for password expiry and rotation process**
- **Use for password creation and reset process**
- **Use for Rescue ID workflow process**
- **Log using Syslog (e.g. to Splunk)**
  - Pass ticket number for password pull

Best Practice: Access Management Policy

- **Implement an overall access management policy based on IT Security policies and compliance requirements**
  - E.g. SOX/CoBit, PCI, HIPAA, 21 CFR 11
- **Make part of overall Database security Program**
  - Access Management is only one component
- **Consider Access Management engagement**
  - Audit and recommendations

Agenda


Overview
Best Practices
Q&A
1
2
3
4
5
Privileged Accounts
Logging Auditing & Monitoring

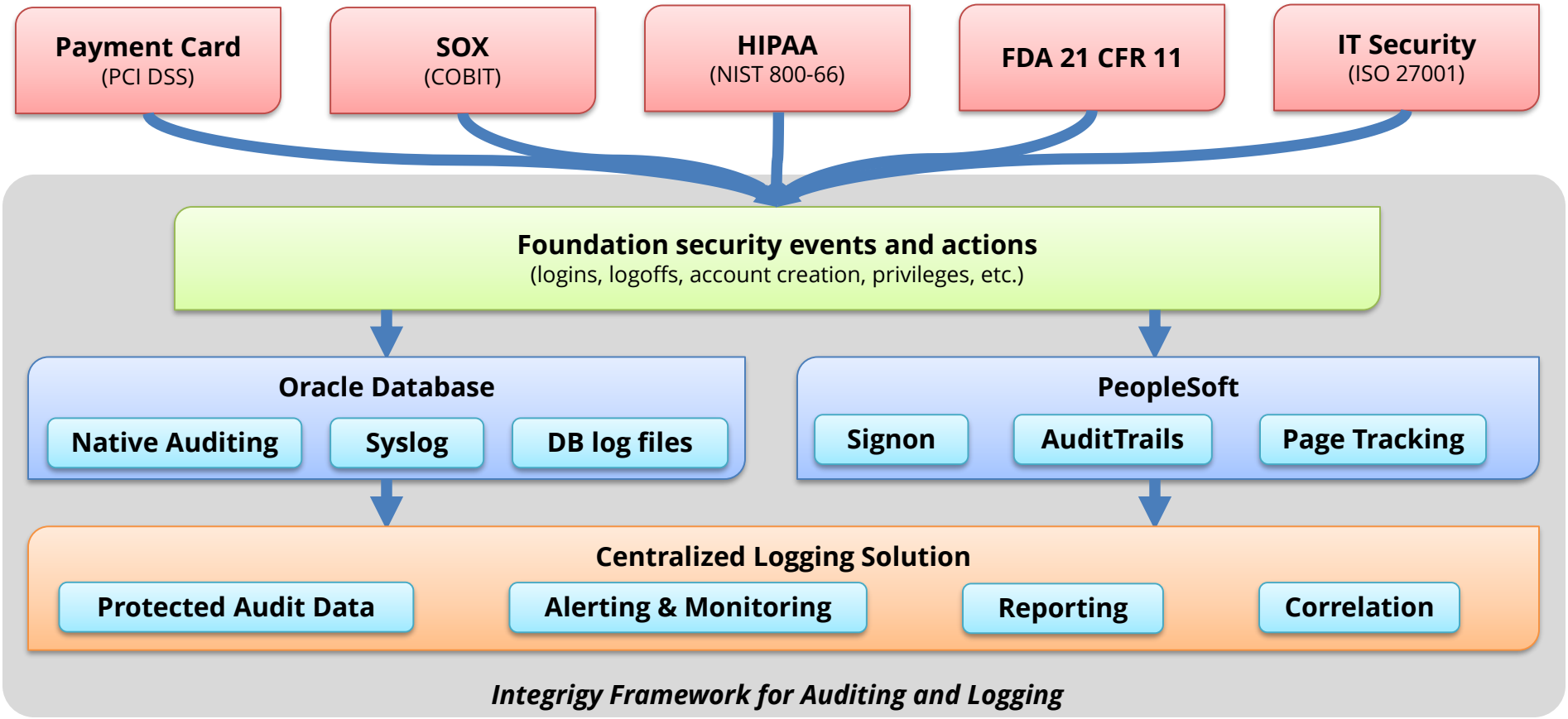
Logging and Auditing Is The Key

- **Access management success or failure largely based on logging and auditing**
  - No other way
- **Constantly log activity**
  - Focus on key events
  - Audit with reports
  - Alert in real-time

Auditing and Logging the PeopleSoft

- **The Oracle database and PeopleSoft offer rich log and audit functionality**
  - **Most organizations do not fully take advantage**
- **Requirements are difficult**
  - Technical, Compliance, Audit, and Security
- **Integrigy has a framework**
  - Already mapped to PCI, HIPAA, SOX and 21 CFR 11

Integrigy Framework for Auditing and Logging



Integrigy Framework for Auditing and Logging

Foundation Security Events and Actions

The foundation of the framework is a set of key security events and actions derived from and mapped to compliance and security requirements that are critical for all organizations.

E1 - **Login**	*E8* - **Modify role**
E2 - **Logoff**	*E9* - **Grant/revoke user privileges**
E3 - **Unsuccessful login**	*E10* - **Grant/revoke role privileges**
E4 - **Modify auth mechanisms**	*E11* - **Privileged commands**
E5 - **Create user account**	*E12* - **Modify audit and logging**
E6 - **Modify user account**	*E13* - **Create, Modify or Delete object**
E7 - **Create role**	*E14* - **Modify configuration settings**

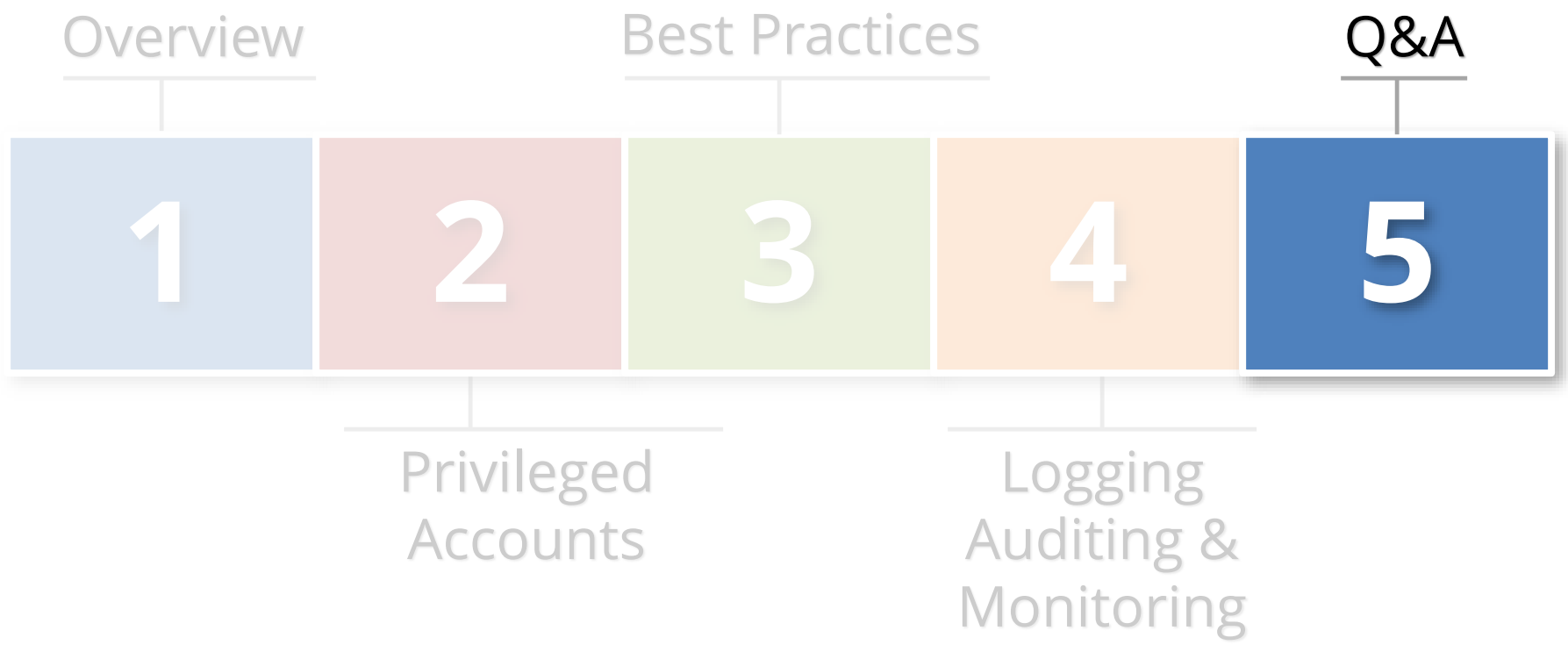
Foundation Security Events Mapping

Security Events and Actions	PCI DSS 10.2	21 CFR Part 11	SOX (COBIT)	HIPAA (NIST 800-66)	IT Security (ISO 27001)	FISMA (NIST 800-53)
E1 - Login	10.2.5	11.10(e)(d)	A12.3	164.312(c)(2)	A 10.10.1	AU-2
E2 - Logoff	10.2.5	11.10(e)	DS5.5	164.312(c)(2)	A 10.10.1	AU-2
E3 - Unsuccessful login	10.2.4	11.10(e) 11.300(d)	DS5.5	164.312(c)(2)	A 10.10.1 A.11.5.1	AC-7
E4 - Modify authentication mechanisms	10.2.5	11.10(e)(d) 11.300(b)	DS5.5	164.312(c)(2)	A 10.10.1	AU-2
E5 – Create user account	10.2.5	11.10(e) 11.100(a)	DS5.5	164.312(c)(2)	A 10.10.1	AU-2
E6 - Modify user account	10.2.5	11.10(e) 11.100(a)	DS5.5	164.312(c)(2)	A 10.10.1	AU-2
E7 - Create role	10.2.5	11.10(e)	DS5.5	164.312(c)(2)	A 10.10.1	AU-2
E8 - Modify role	10.2.5	11.10(e)	DS5.5	164.312(c)(2)	A 10.10.1	AU-2
E9 - Grant/revoke user privileges	10.2.5	11.10(e)	DS5.5	164.312(c)(2)	A 10.10.1	AU-2
E10 - Grant/revoke role privileges	10.2.5	11.10(e)	DS5.5	164.312(c)(2)	A 10.10.1	AU-2
E11 - Privileged commands	10.2.2	11.10(e)	DS5.5	164.312(c)(2)	A 10.10.1	AU-2
E12 - Modify audit and logging	10.2.6	11.10(e)	DS5.5	164.312(c)(2)	A 10.10.1	AU-2 AU-9
E13 - Objects Create/Modify/Delete	10.2.7	11.10(e)	DS5.5	164.312(c)(2)	A 10.10.1	AU-2 AU-14
E14 - Modify configuration settings	10.2.2	11.10(e)	DS5.5	164.312(c)(2)	A 10.10.1	AU-2

Integrigy Framework Maturity Model

Level 1	Enable **baseline auditing and logging** for application/database and implement security monitoring and auditing alerts
Level 2	Send audit and log data to a **centralized logging** solution outside the Oracle Database and PeopleSoft
Level 3	Extend logging to include **functional logging** and more complex alerting and monitoring

Agenda


Overview
Best Practices
Q&A
1
2
3
4
5
Privileged Accounts
Logging Auditing & Monitoring

Contact Information

Mike Miller

Chief Security Officer

Integrigy Corporation

web: **www.integrigy.com**

e-mail: **mike.miller@integrigy.com**

blog: **integrigy.com/oracle-security-blog**

youtube: **youtube.com/integrigy**