Oracle E-Business Suite
Trust But Verify

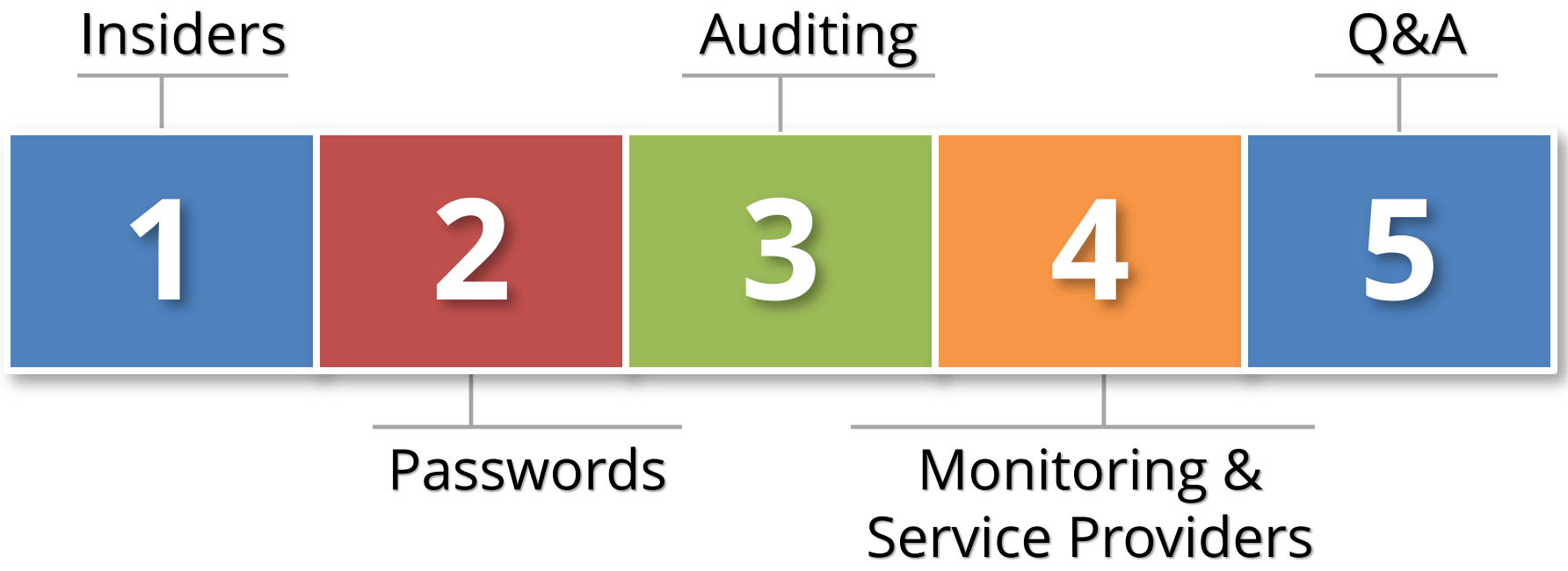
November 20, 2013

Mike Miller
Chief Security Officer
Integrigy Corporation

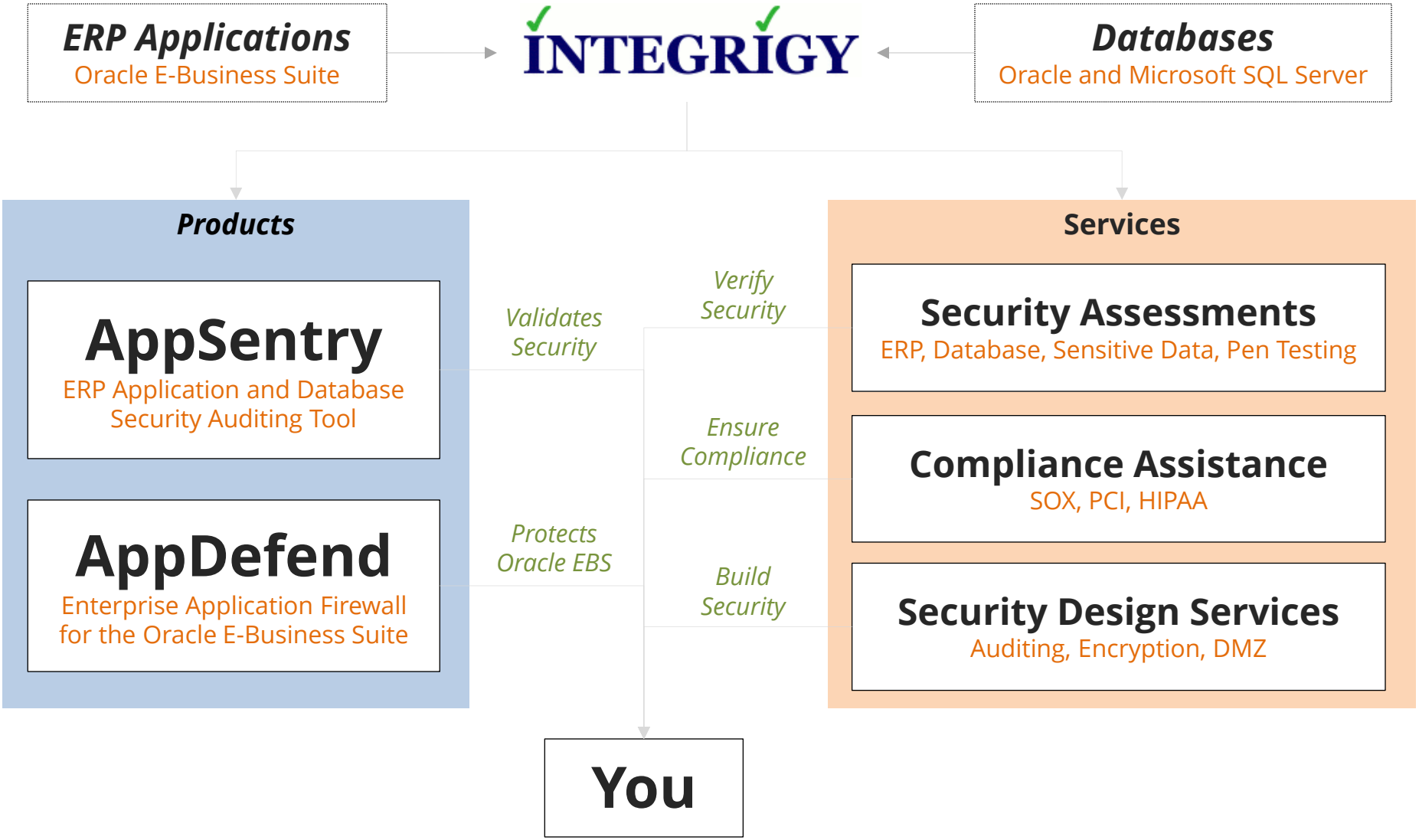
Stephen Kost
Chief Technology Officer
Integrigy Corporation

Phil Reimann
Director of Business Development
Integrigy Corporation

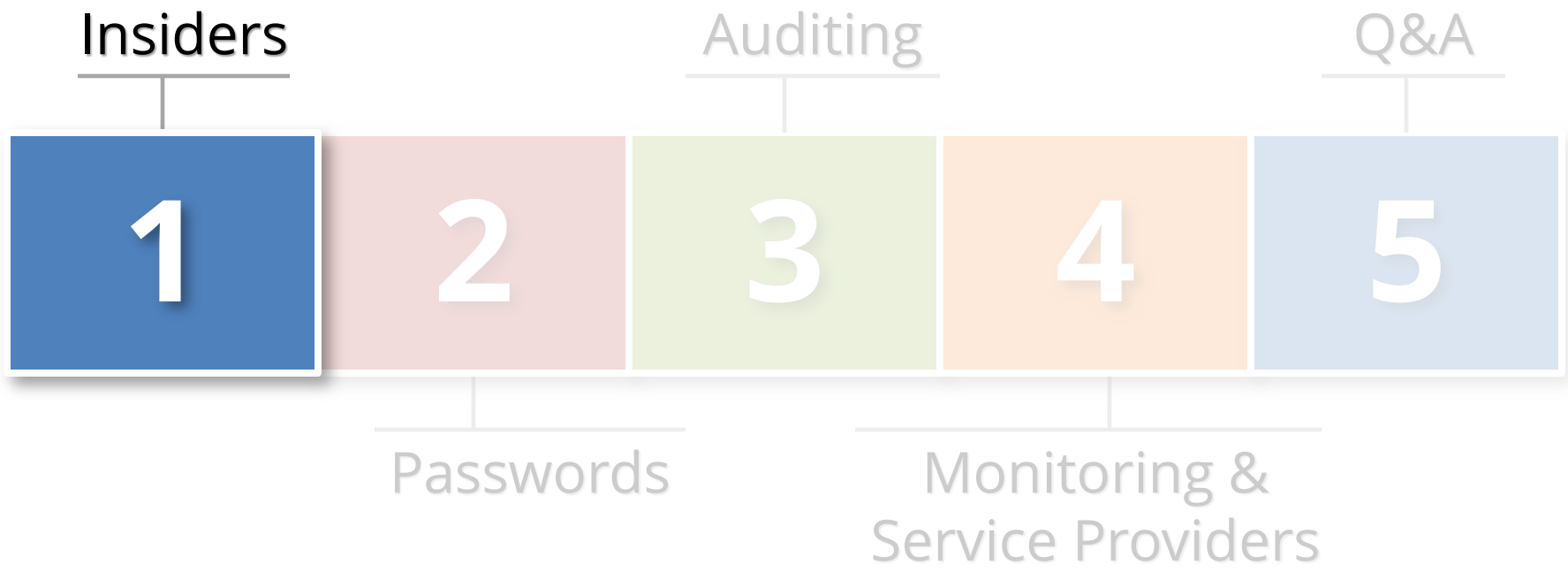
Agenda


Insiders
Auditing
Q&A
1
2
3
4
5
Passwords
Monitoring &
Service Providers

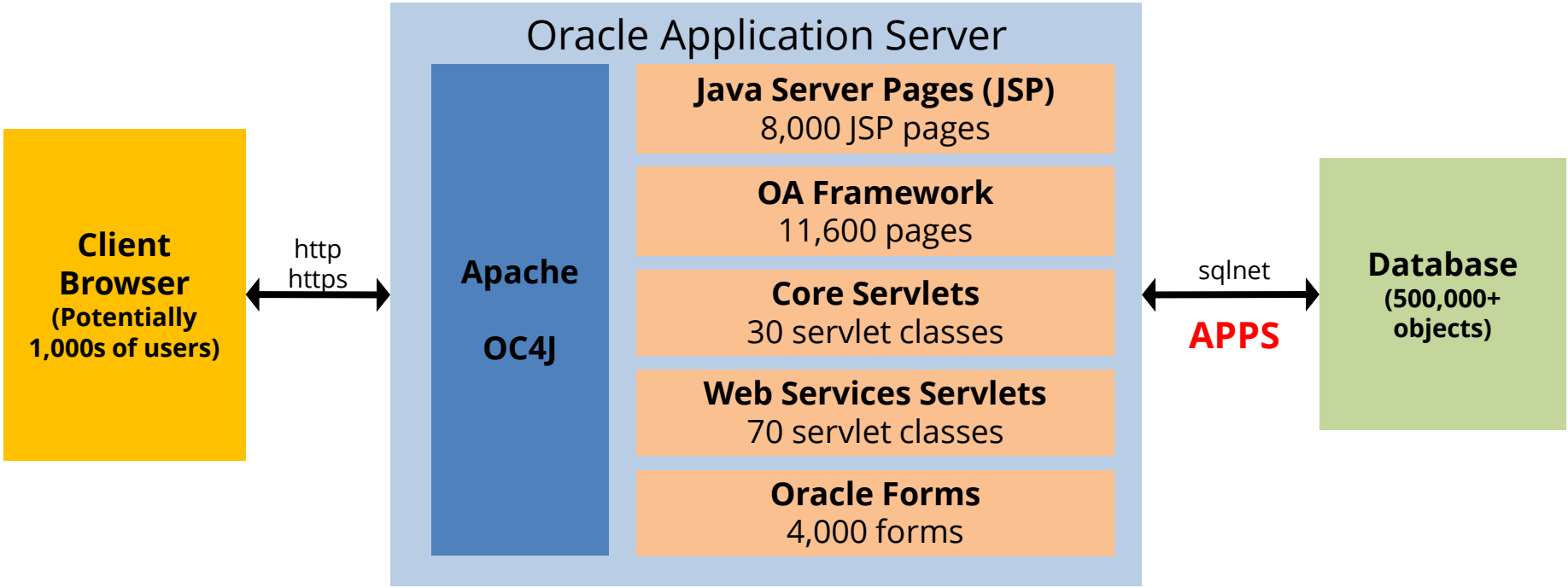
About Integrigy



Agenda


Insiders
Auditing
Q&A
1
2
3
4
5
Passwords
Monitoring &
Service Providers

Oracle E-Business Suite



- Oracle EBS installs all modules (250+) and **all web pages** with each installation
- Large and complex application - security is an on-going effort

Insider Threat Cannot Be Avoided

- **Insiders include**
  - DBAs, administrators, developers, staff, contractors and vendors
- **Number of insiders can range greatly**
- **If hosted, can have a very large number of insiders**

Rocket Scientists

Horde of Zombies

Insider Threats Cannot Be Avoided

- **How do you guard against insider**
  - Unauthorized access and breeches
  - Not following policies and procedures
  - Poor or risky behaviors

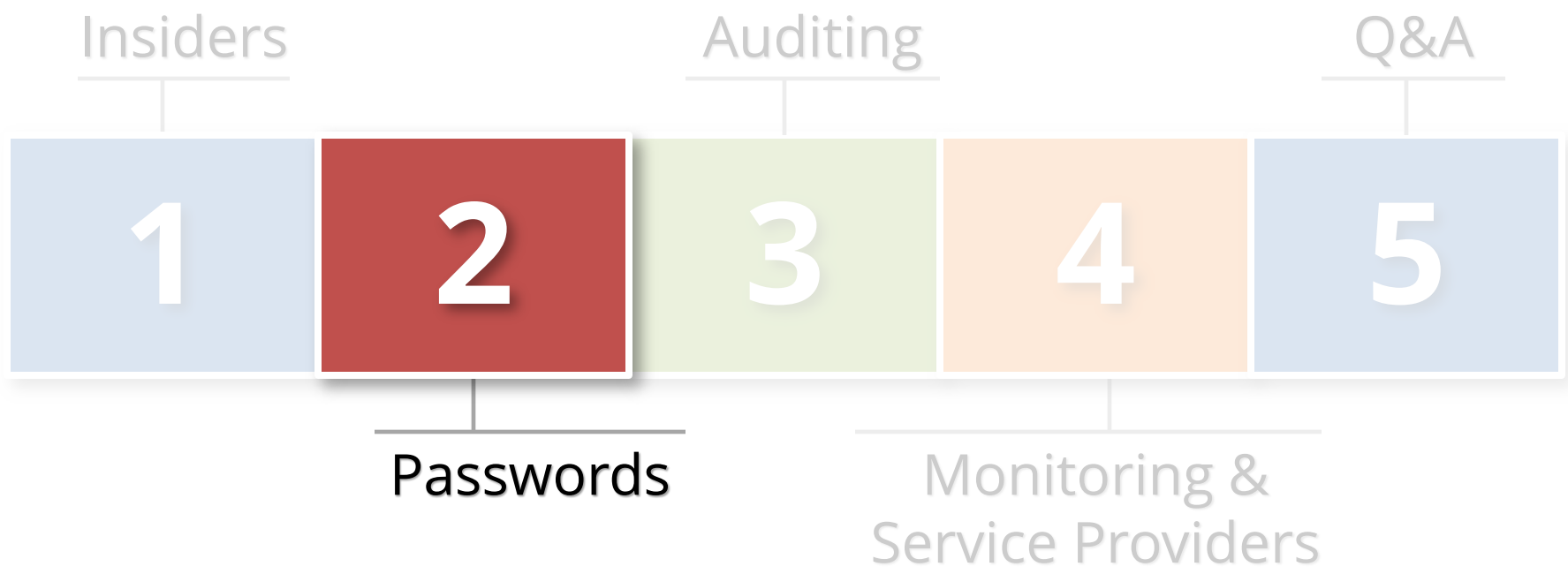
- **How do you trust insiders?**
  - Trust but verify

Trust But verify

Goal of this presentation

1. Use the perspective of an internal auditor
2. Offer a basic strategy to establish and maintain a trust perimeter for insiders
3. Share a few specific tips and recommendations from Integrigy's consulting engagements

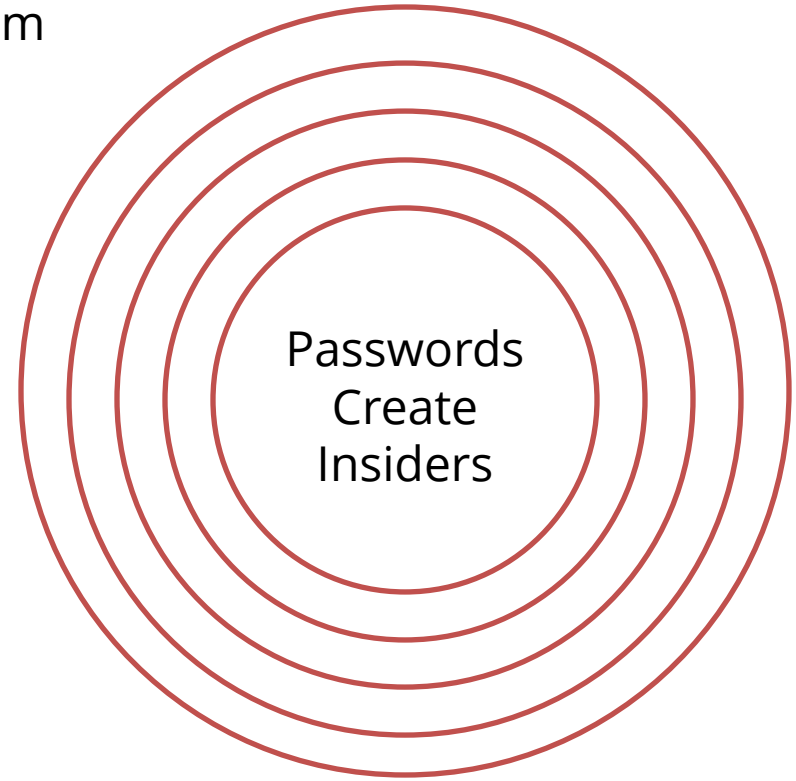
Agenda


Insiders
Auditing
Q&A
1
2
3
4
5
Passwords
Monitoring &
Service Providers

Define Trust Perimeter with Passwords

Step One Define the Password Trust Perimeter

DB & Operating System
- 300+ accounts
- Generic accounts
- Staff accounts



Oracle E-Business
- System Admin
- Generic Accounts
- 40+ Default Accts

Environments
- Production
- Test
- Development

Remote
- Hosted/Cloud
- Offshore DBA
- Developers

Appropriate Trust

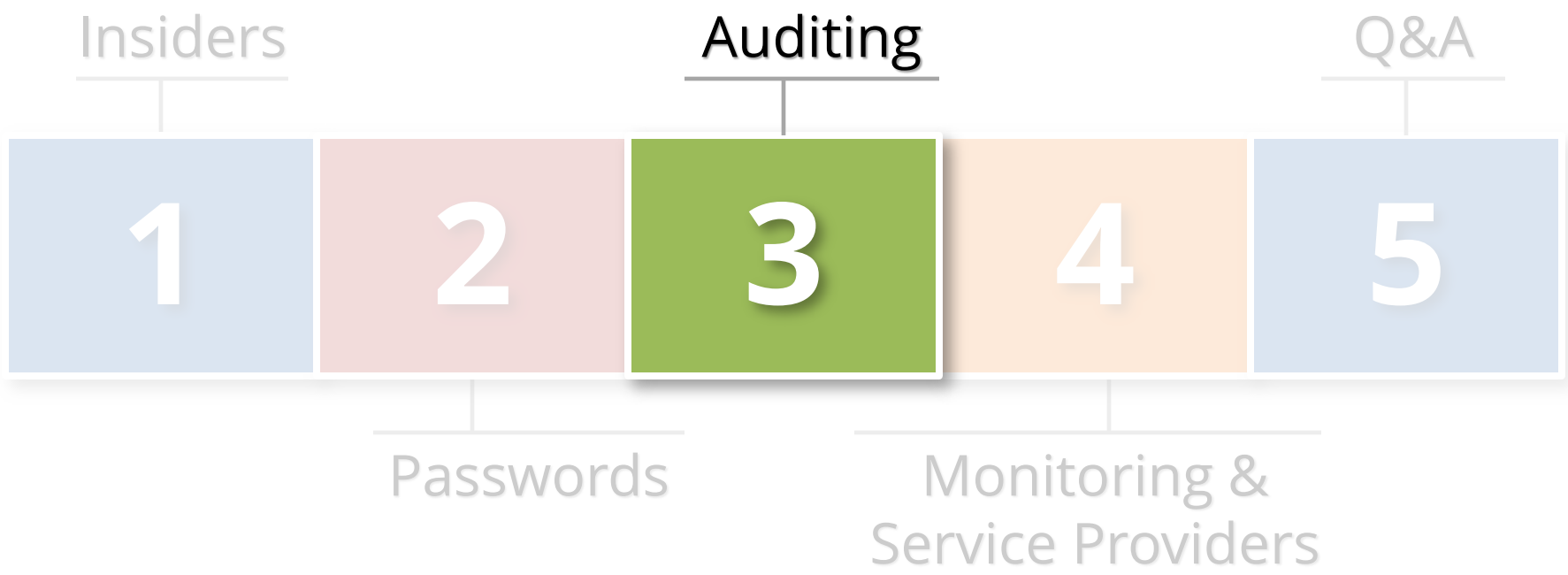
- **Review business need and terms of access for each account**
  - Appropriate and responsible

- **Revise and monitor password rights**
  - People will complain

Additional Steps

- **Use a password vault application with strong reporting capabilities**
- **Where direct access is not required use random, long strings for passwords**
- **Use “half passwords” - assign one half a key password to two different people**

Agenda


Insiders
Auditing
Q&A
1
2
3
4
5
Passwords
Monitoring &
Service Providers

Two Steps to Verify Trust for EBS Insiders

Enable Forms auditing

- User, Responsibility, Forms

Review and carefully monitor administration menus

- Who can change menus and edit users

Additional Steps

- **Generic accounts**
  - Review, remove or restrict
- **Protect production data**
  - Access to production by developers and testers
- **Protect sensitive data**
  - Sensitive data must be redacted, masked or scrambled in non-production databases

Where is Sensitive Data in Oracle EBS?

Credit Card Data	`iby_security_segments (encrypted)`
	`ap_bank_accounts_all`
	`oe_order_headers_all`
	`aso_payments`
	`oks_k_headers_*`
	`oks_k_lines_*`
	`iby_trxn_summaries_all`
	`iby_credit_card`

Social Security Number
(National Identifier)
(Tax ID)
	`per_all_people_f`
	`hr_h2pi_employees`
	`ben_reporting`
	`ap_suppliers`
	`ap_suppliers_int`
	`po_vendors_obs`

Bank Account Number	`ap_checks_all`
	`ap_invoice_payments_all`
	`ap_selected_invoice_checks_all`

Protected Health Information (PHI)	Order Management Accounts Receivables Human Resources

Where else might be Sensitive Data?

Custom tables

- Customizations may be used to store or process sensitive data

"Maintenance tables"

- DBA copies tables to make backup prior to direct SQL update
- hr.per_all_people_f_011510

Interface tables

- Credit card numbers are often accepted in external applications and sent to Oracle EBS

Oracle EBS Flexfields

- It happens – very hard to find

Interface files

- Flat files used for interfaces or batch processing

Log files

- Log files generated by the application (e.g., iPayment)

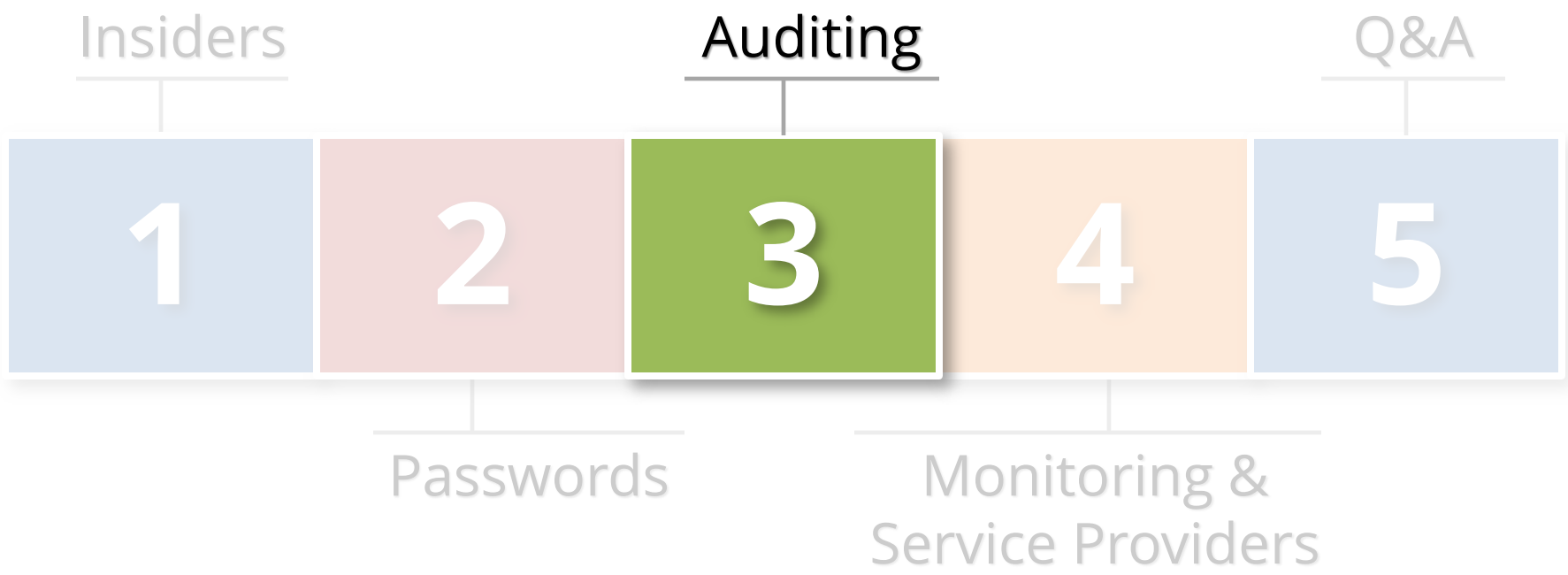
Database

File System

Other Ideas

- **Create custom Oracle Alerts for real-time event auditing and monitoring**
- **Create custom reports for audit activity**
- **Break up system administration menus by function**
- **Audit menu functions**

Agenda


Insiders
Auditing
Q&A
1
2
3
4
5
Passwords
Monitoring &
Service Providers

Verify Trust for Database Access

- **Direct database access is the biggest insider threat**
  - What accounts are used to directly access
  - Who is using the accounts
  - Where are they logging in from

Insider Database Access

- **If automation tools used for cloning and patching, review accounts used**
  - Appropriate privileges by the appropriate staff
  - How is security and logging provided
- **Also confirm who can access**
  - Virtual Machine images
  - Backup tapes/files

Three Steps To Verify Insider Database Trust

1. **Enable standard database auditing**
   - Need to protect the audit trail
2. **Manually review database privileges**
   - No standard method to review database privileges
3. **Create individual user database accounts**
   - Associate user account with roles to limit access to data

Also Consider for Database Trust Verification

- **With Oracle Enterprise license**
  - Fine Grained Access Control (FGAC)
  - Fine Grained Auditing (FGA)
- **Additional Oracle license cost**
  - Audit Vault and Database Vault
  - Oracle Advanced Security Option (ASO)
    - Transparent Data Encryption (TDE)
    - Data redaction and data masking

Also Consider for Database Trust Verification

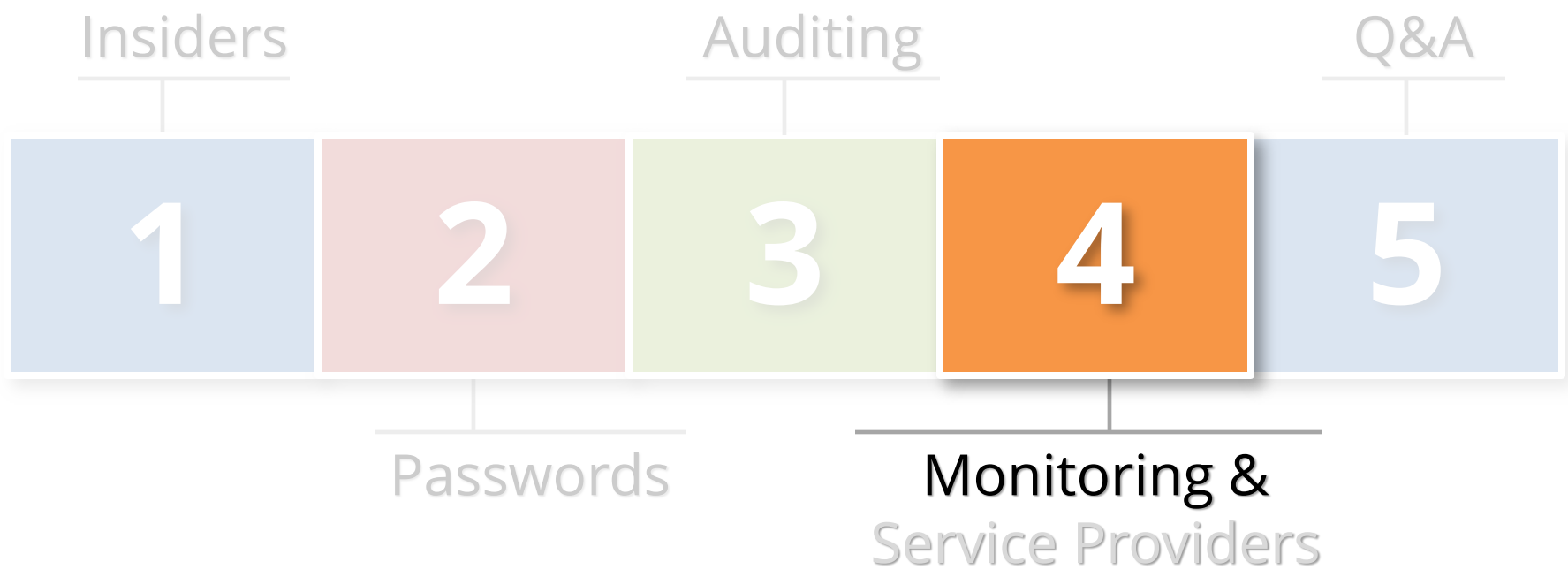
- **Automation tools**
  - Automation removes direct access need
  - Can also detect and report on change
  - Tools such as
    - Oracle Enterprise Management Packs for E-Business
    - Quest Stat
    - Kintana (formerly Chain Link)

Also Consider for Database Trust Verification

- **Log and Event Management Tools**
  - Purpose built reporting and correlation tools
    - Splunk
    - HP ArcSight

ArcSight™
An HP Company

Agenda


Insiders
Auditing
Q&A
1
2
3
4
5
Passwords
Monitoring &
Service Providers

Use Monitoring for Continuous Verification

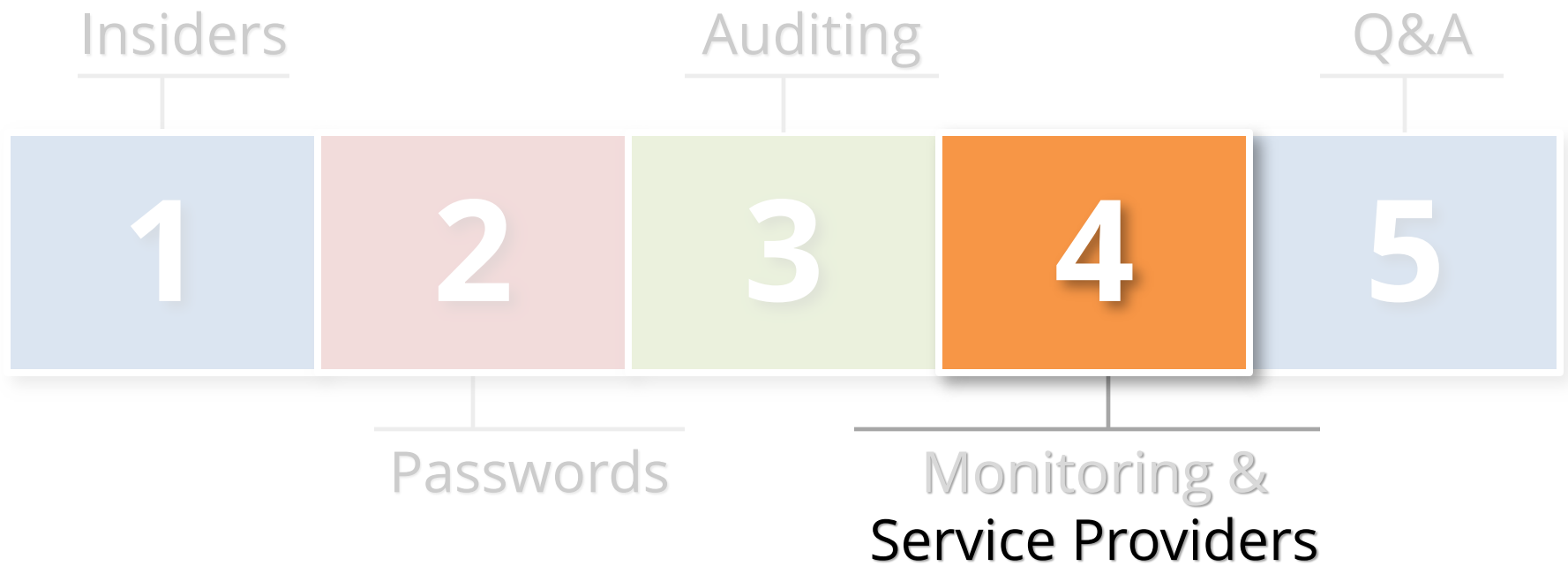
- **Monitoring is your front line defense**
  - 24x7x365 verification services

- **Monitoring can include**
  - Access control alerts
  - System administration changes
  - Account creation and modification

Verify Trust Perimeter For Monitoring

- **What accounts are used for monitoring**
  - Appropriately privileged
  - Hardcoded and/or changed regularly
- **What accounts monitoring staff use to respond to alerts**
  - Appropriately privileged
  - How are passwords pulled and how many have access
  - Is the activity audited

Agenda


Insiders
Auditing
Q&A
1
2
3
4
5
Passwords
Monitoring &
Service Providers

How to Verify Trust of Service Providers

- **Service providers introduce large numbers of insiders**
  - Large cloud vendors can have 1,000s
- **Use Service Organization Control (SOC) Reports**
  - Third party audit and attestation
  - Standard set by American Institute of CPAs
  - Much more effective than contractual or SLA reports

AICPA
American Institute of Certified Public Accountants

Four Key Facts about SOC Reports

- **Replacement for SAS70 Report**
  - SSAE 16 SOC Report
- **Is a historical report**
  - Type I reports on a specific day
  - Type II reports on a historical period
- **SOC 1 Report –** Vendor management's discretion on what to include
  - Vendor reports differ widely
- **SOC 2 Report –** Whether or not AICPA dictated Trust Principles are being followed
  - Security, Availability, Integrity, Confidentiality and Privacy

Verify Trust of Service Providers by

- **Using service providers who regularly produce SOC reports**
  - Management commitment
- **Using providers whose SOC report works for you**
  - Read carefully and don’t assume anything
  - Clearly meets your compliance and regulatory requirements
  - Aligns with your audit and fiscal periods

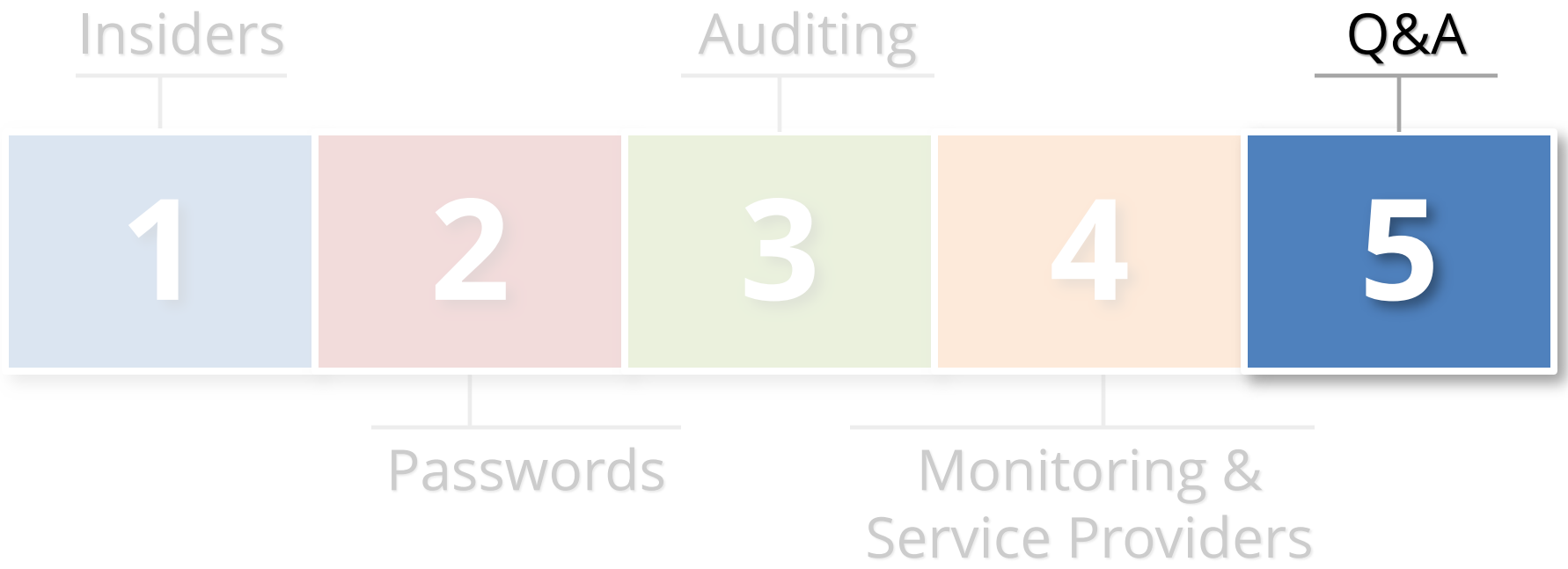
Additional SOC Reporting Considerations

- **Beware of your service provider's supply chain**
  - Are they outsourcing key services?
- **Consider writing into contract with provider**
  - Production of SOC report e.g. annually
  - Notification, if not approval, of changes to controls
- **Ask for a SOC 2 instead of SOC 1 report**
  - Review with vendor plans for SOC 2 reporting

Additional Considerations for Verifying Trust

- **Require adherence to PCI standard (credit card security) even if not a processing cards**
- **Request syslog feeds for insider operating system and/or database activity**
- **Consider independent security assessments**

Agenda


Insiders
Auditing
Q&A
1
2
3
4
5
Passwords
Monitoring &
Service Providers

Trust But Verify Summary

- **Establish a trust perimeter first through password control**
- **Setup and use auditing**
- **Understand and exploit monitoring**
- **Use SOC reports to verify trust of service providers**
- **Consider regular security assessments**

References

- **Written by Integrigy**
  - 189367.1 *Secure Configuration Guide for Oracle E-Business Suite 11i*
  - 403537.1 *Secure Configuration Guide for Oracle E-Business Suite R12*
- **Other references**
  - *Security, Audit and Control Features, Oracle E-Business Suite, A Technical and Risk Management Guide 3rd Edition*, ISACA, ISBN 978-1604201062
  - *Oracle E-Business Suite Controls: Application Security Best Practices*, Jeff T. Hare, ISBN 978-0557193134
  - *Security, Audit and Control Features, Oracle Database 3rd Edition*, ISACA, ISBN 978-1604201185
  - *SOC 2 Reporting on Controls at a Service Organization*, AICPA, ISBN 978-1-93735-060-04

More can be found here: http://www.integrigy.com/security-resources

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**