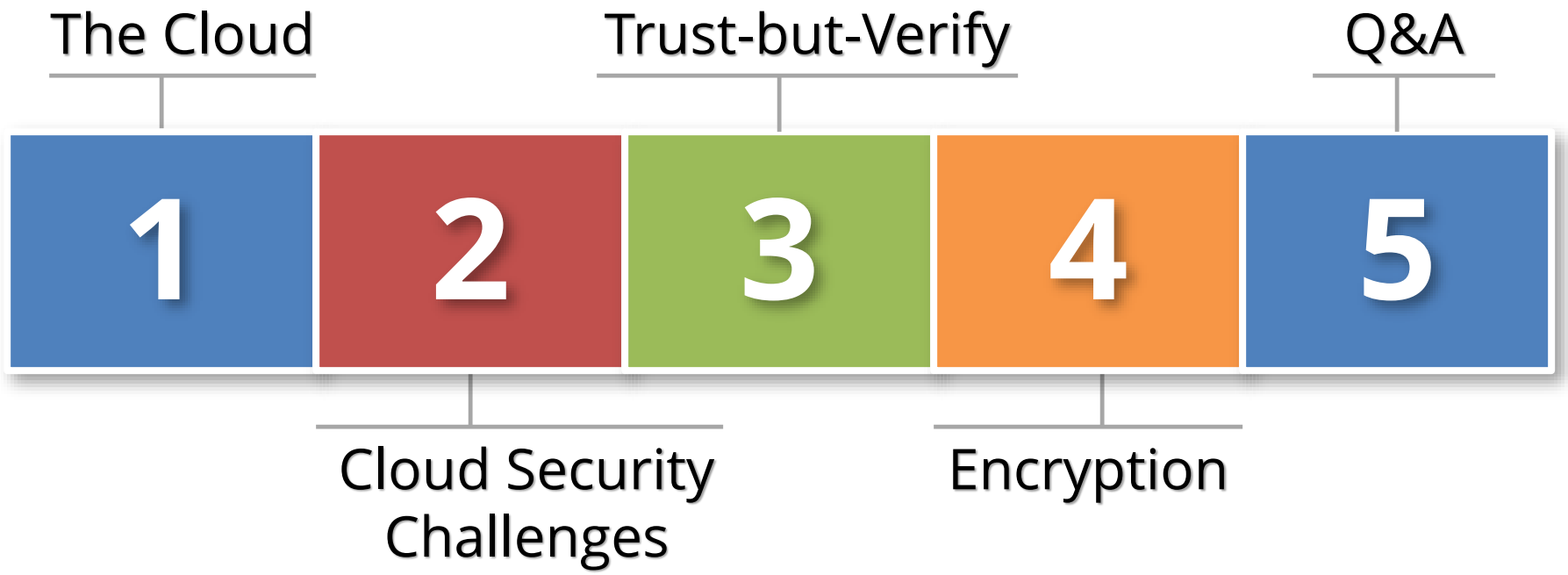
Securing Oracle E-Business Suite in the Cloud

November 18, 2015

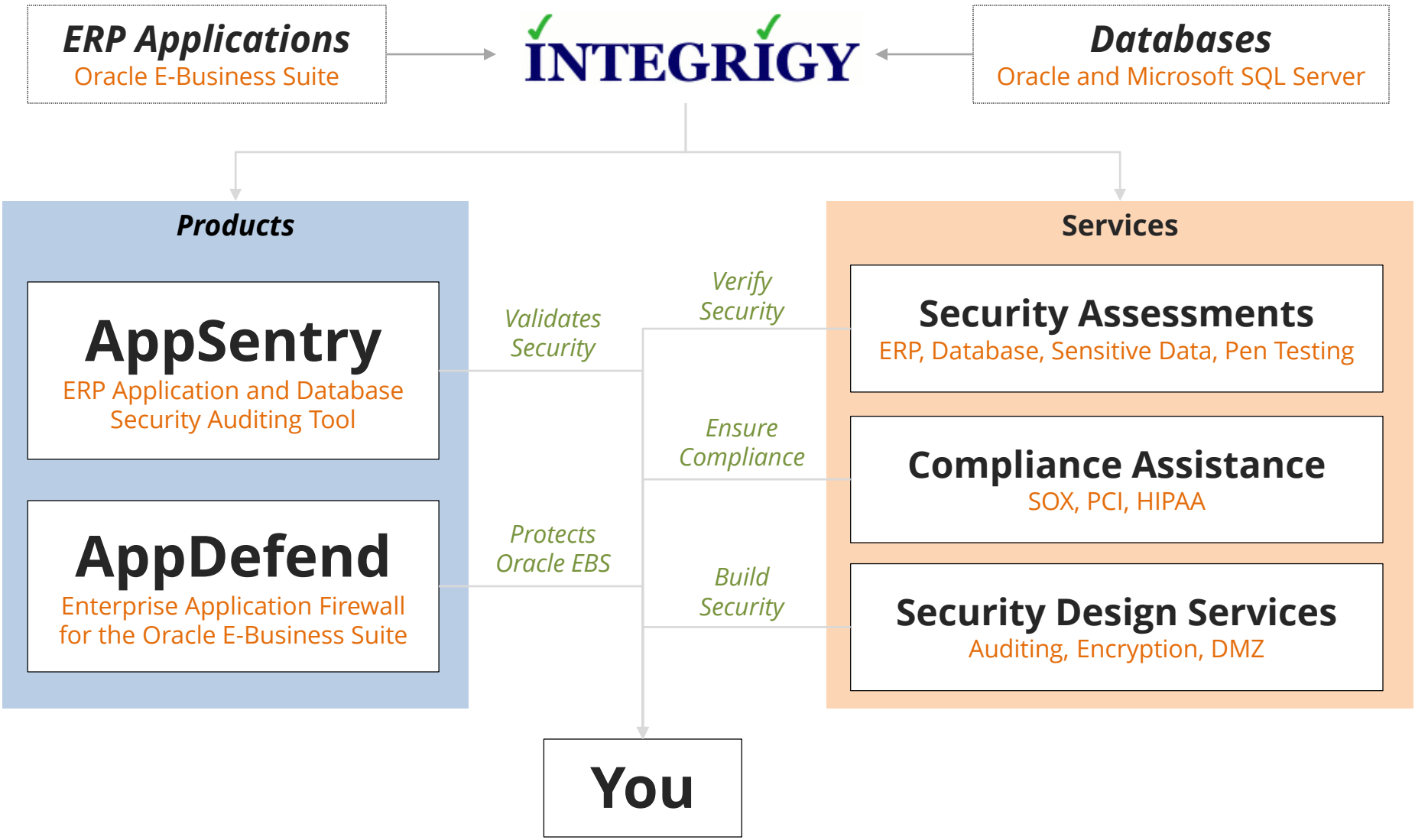
Stephen Kost
Chief Technology Officer
Integrigy Corporation

Phil Reimann
Director of Business Development
Integrigy Corporation

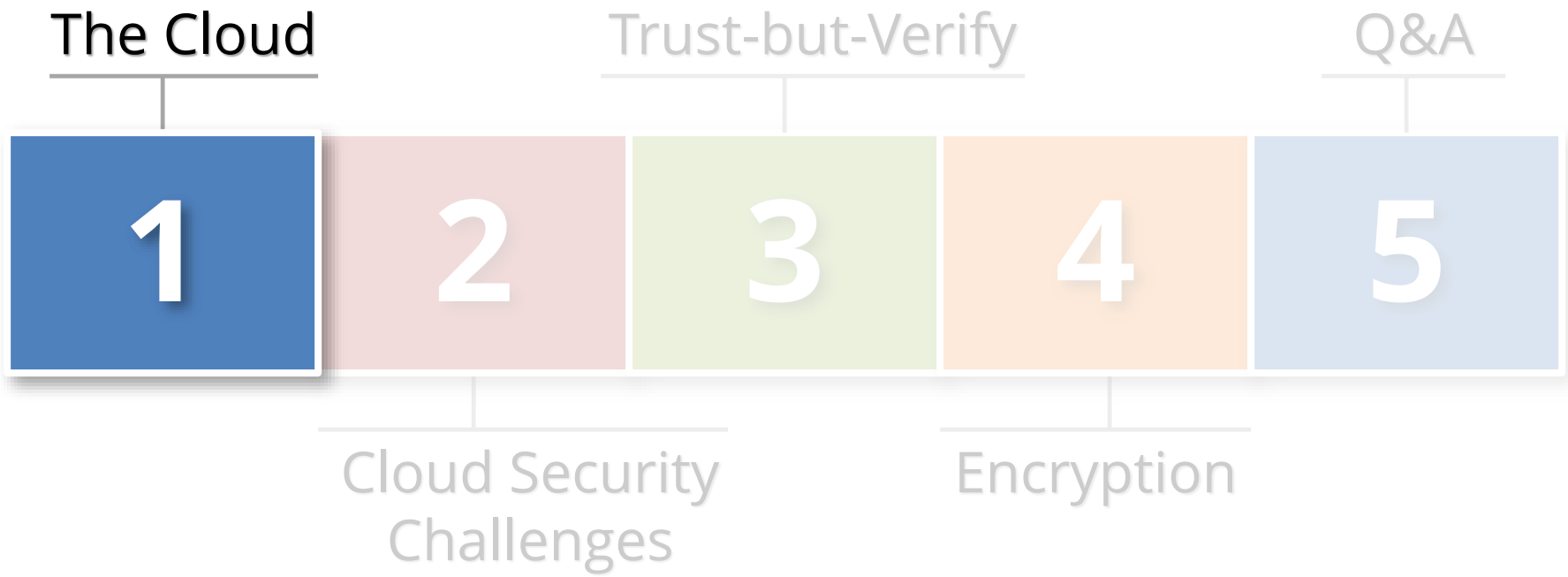
Agenda


The Cloud
Trust-but-Verify
Q&A
1
2
3
4
5
Cloud Security Challenges
Encryption

About Integrigy



Agenda

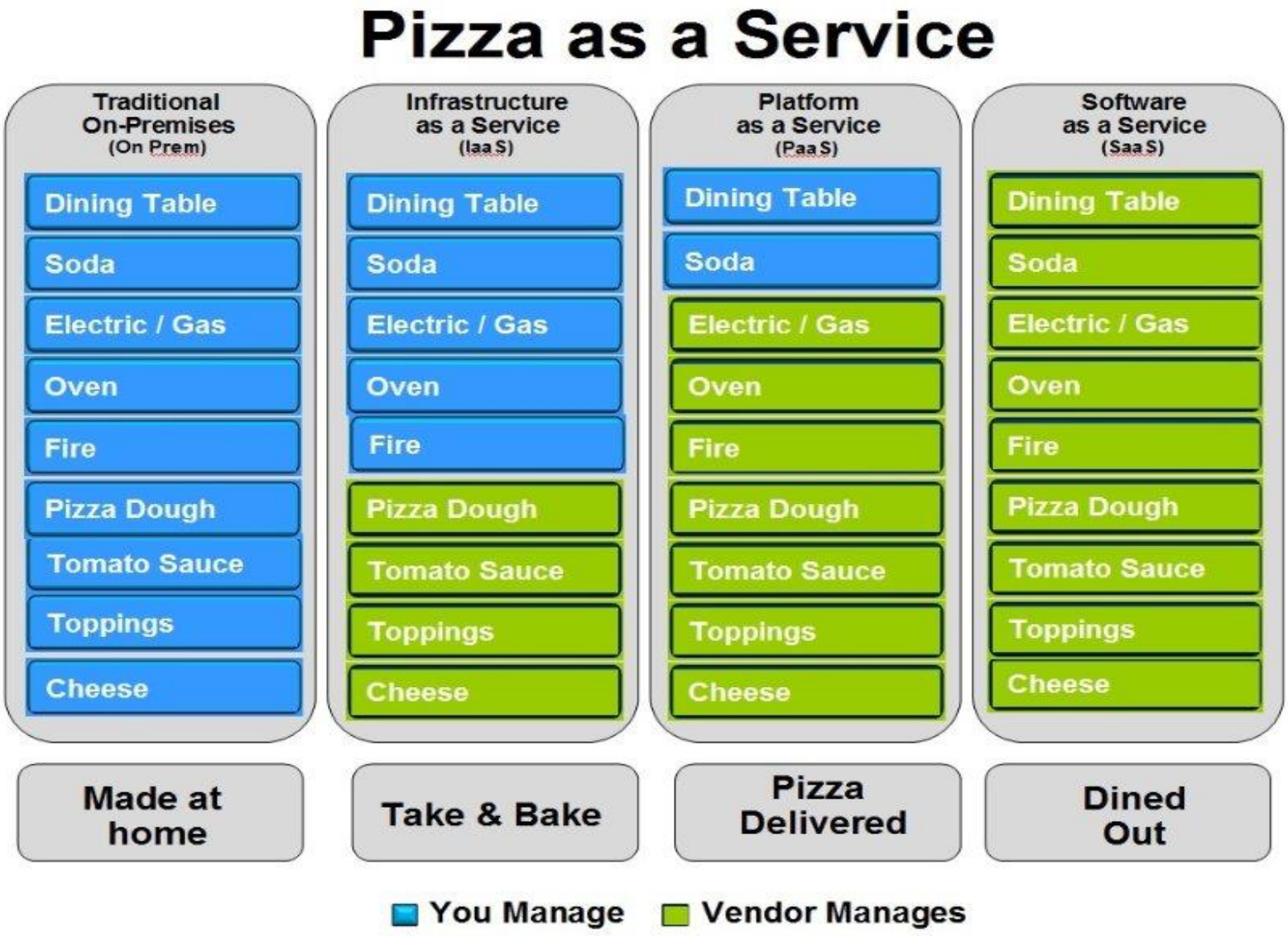

The Cloud
Trust-but-Verify
Q&A
1
2
3
4
5
Cloud Security Challenges
Encryption

What is the Cloud?

- **Clouds are not new**
  - "Infrastructure as a Service" (IAAS) and "Platform as a Service" (PAAS) have been around for decades
  - Used to be called "Hosting" or "Out-Sourcing"
  - Software as a Service (SAAS) is what is new

- **What are the differences?**
  - Number of lawyers and length of contract
  - Division of responsibilities

Clouds Defined As Pizza

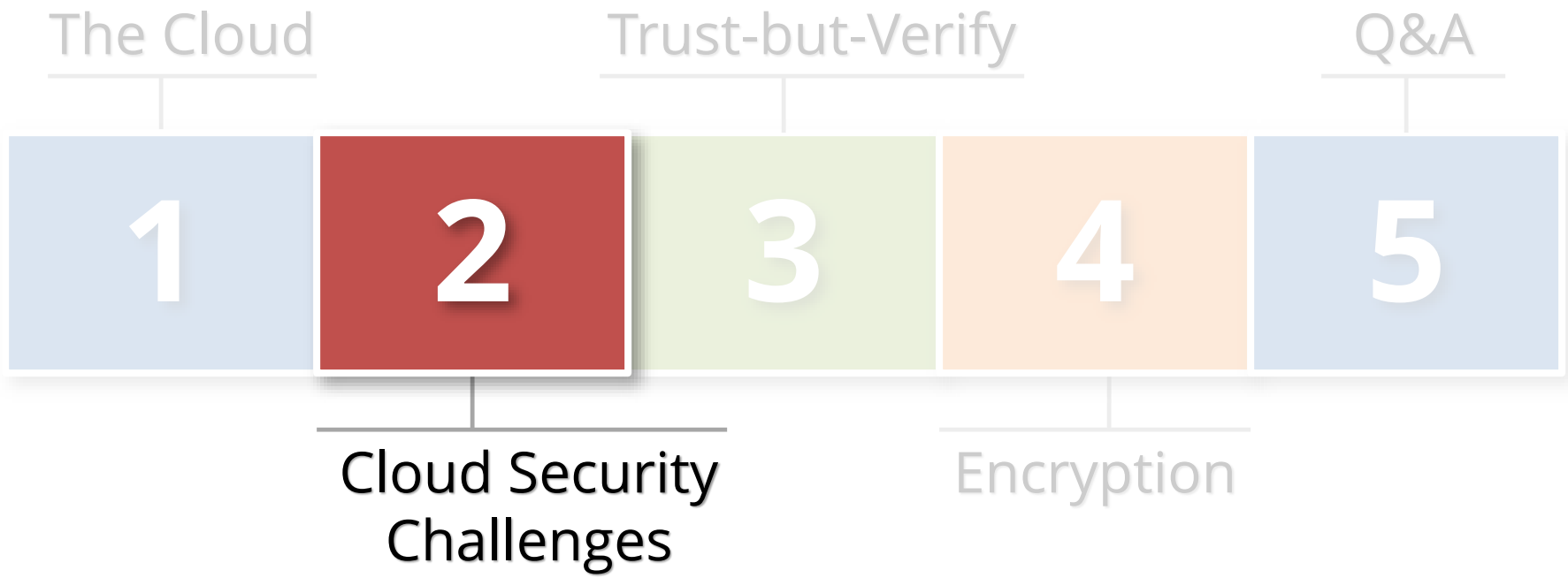


Oracle E-Business Suite in the Cloud

- **Platform as a Service (PAAS)**
  - Fully integrated 3rd party service offering
    - Hosting, DBA, and application support

- **Infrastructure as a Service (IAAS)**
  - Hybrid or multivendor solution
    - Data center (hosting)
    - DBA & Application support managed services
    - Network

Agenda


The Cloud
Trust-but-Verify
Q&A
1
2
3
4
5
Cloud Security Challenges
Encryption

Does the Cloud Change Security?

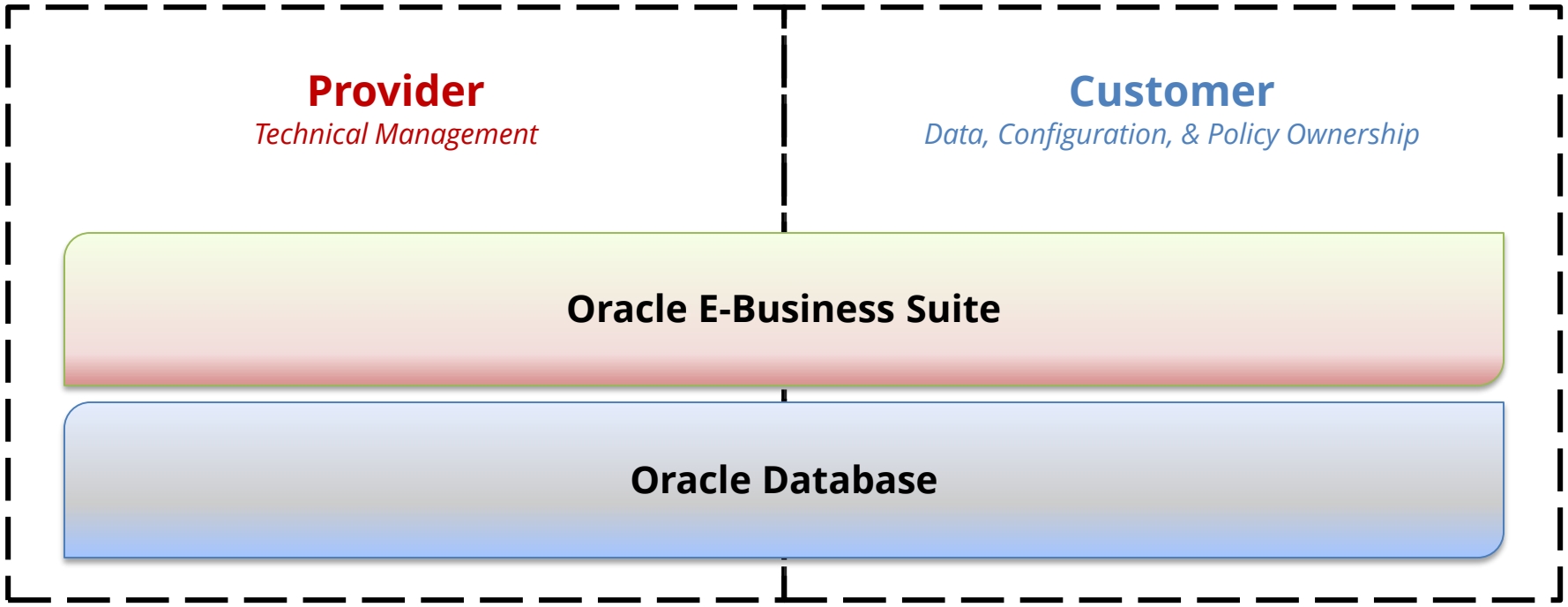
No

Data Ownership

- **Using the Cloud does not fundamentally change ownership of data**
  - You own your data
  - You are responsible for your data
- **Legal and compliance mandates flow out and down to your vendor(s)**
  - “Onward transfer” is your responsibility
- **Cloud extends only what should already be in place to protect YOUR data**
  - Effective security & trust-but-verify

Cloud Requires Redrawing Responsibility Lines

- Customers own the application, data, and configurations
- Cloud provider supplies infrastructure and managed services
- Responsibilities will vary among providers and customers



Its not this simple…

Sample Division of Responsibilities

		Oracle E-Business Suite Technical Components				
		Oracle E-Business Suite	Database	Application Server	Operating System	Network
Operational Processes	1. Account Security	User Management	Database Security	Network and Web	OS Security	Network
		Segregation of Duties				
	2. Data Security	Data Management and Privacy	Database Access and Privileges	Web Access	File Permissions	Encryption
	3. Auditing	Application Auditing	Database Auditing	Web Logging	OS Auditing	Network Auditing
	4. Monitoring and Troubleshooting	Application	Database	Web and Forms	Operating System	Network
	5. Change Management	Object Migrations	Change Control	Change Control	Change Control	Change Control
		Application Configuration	Database Configuration			
	6. Patching	Application Patches	Database Patches	Application Server Patches	OS Patches	Firmware Patches
	7. Development	Application	Database	Web Web Services and SOA	Shell and File Transfer	Testing

Provider

Shared

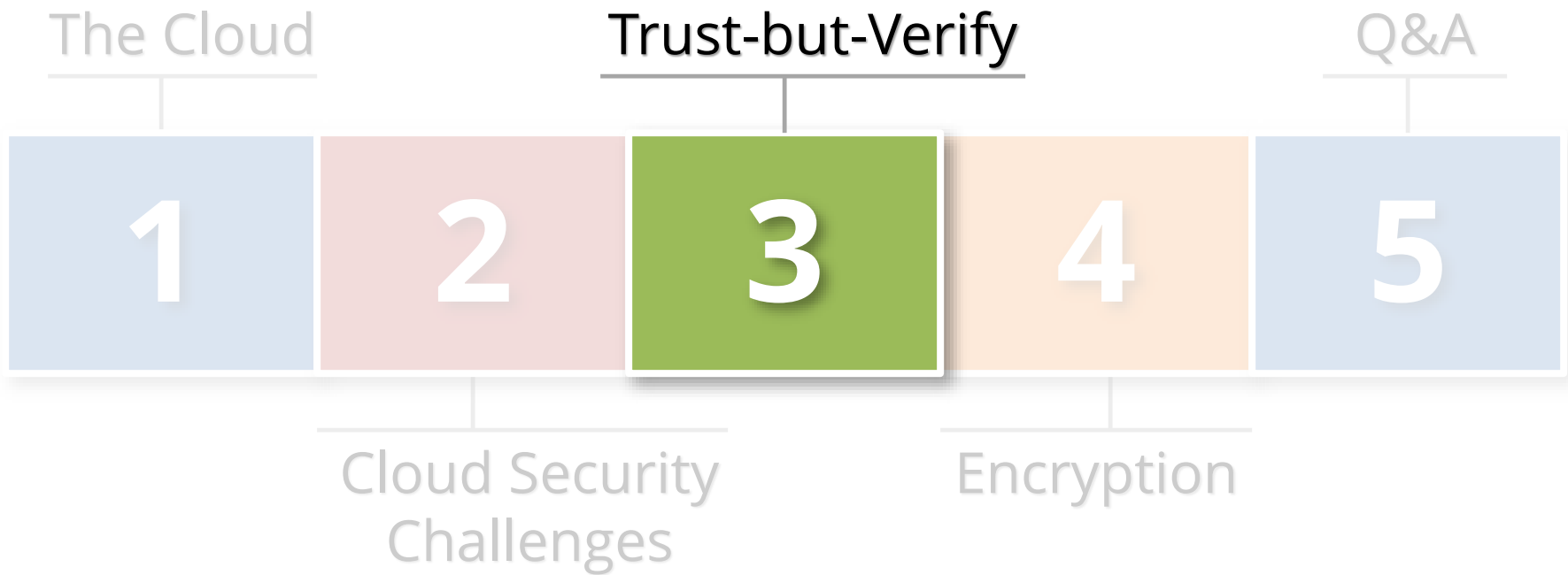
Customer

How to Secure E-Business in the Cloud?

- **Redraw lines of responsibility**
  - Differs PAAS vs. IAAS

- **Must "Trust-but-Verify" 3rd parties and associated lines of responsibilities**
  - Requires new skills and support services:
    - IT & E-Business Support
    - Procurement/Vendor management
    - Legal & compliance

Agenda


The Cloud
Trust-but-Verify
Q&A
1
2
3
4
5
Cloud Security Challenges
Encryption

Clouds Create More Insiders

- **Insiders include**
  - DBAs
  - Application Administrators
  - System Administrators
  - Developers
  - Contractors
  - Vendors
- **Number of insiders can range greatly**
  - Cloud providers usually have a very large number of insiders

Insider Threats Cannot Be Avoided

- **Need to guard against insider threat**
  - Prevent unauthorized access and breaches
  - Ensure policies and procedures are adhered to
  - Eliminate poor or risky behaviors

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

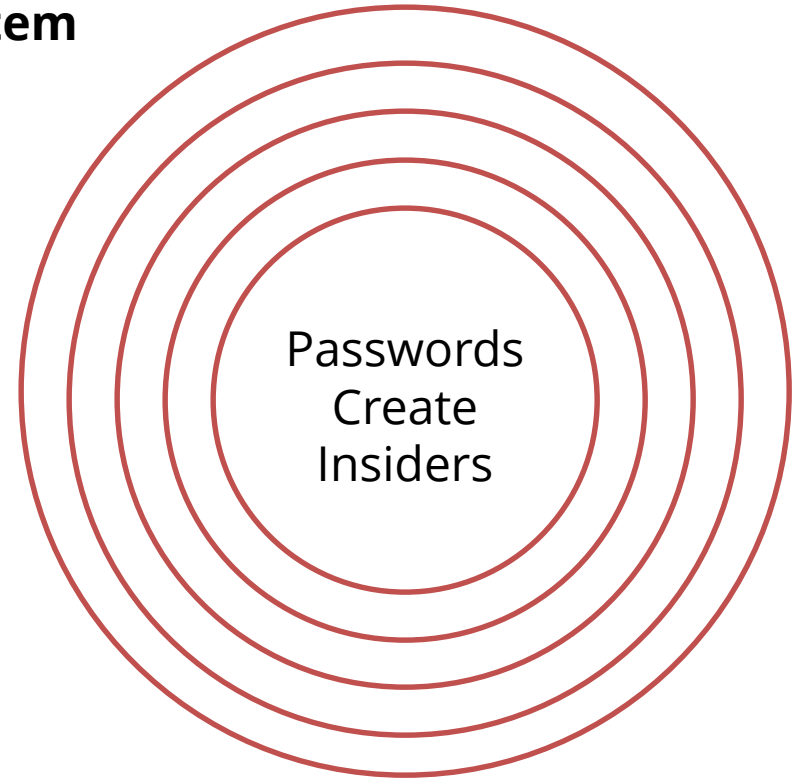
Oracle EBS Generic Privileged Accounts

Oracle E-Business Suite	**SYSADMIN** *seeded application accounts*
Oracle Database	**APPS, APPLSYS** **SYS, SYSTEM** *Oracle EBS schemas (GL, AP, ...)*
Operating System *(Unix and Linux)*	**root** **oracle, applmgr**

Oracle E-Business Suite Trust Perimeter

Passwords define the Trust Perimeter

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



Oracle E-Business Suite
- System Admin
- Generic accounts
- 40+ default accounts

Environments
- Production
- Test
- Development

Teams
- Developers
- Contractors
- Support & QA

Oracle E-Business Suite Cloud Perimeter

- IAAS extends perimeter, PAAS even more
- 24x7 SLAs will greatly extend trust perimeter

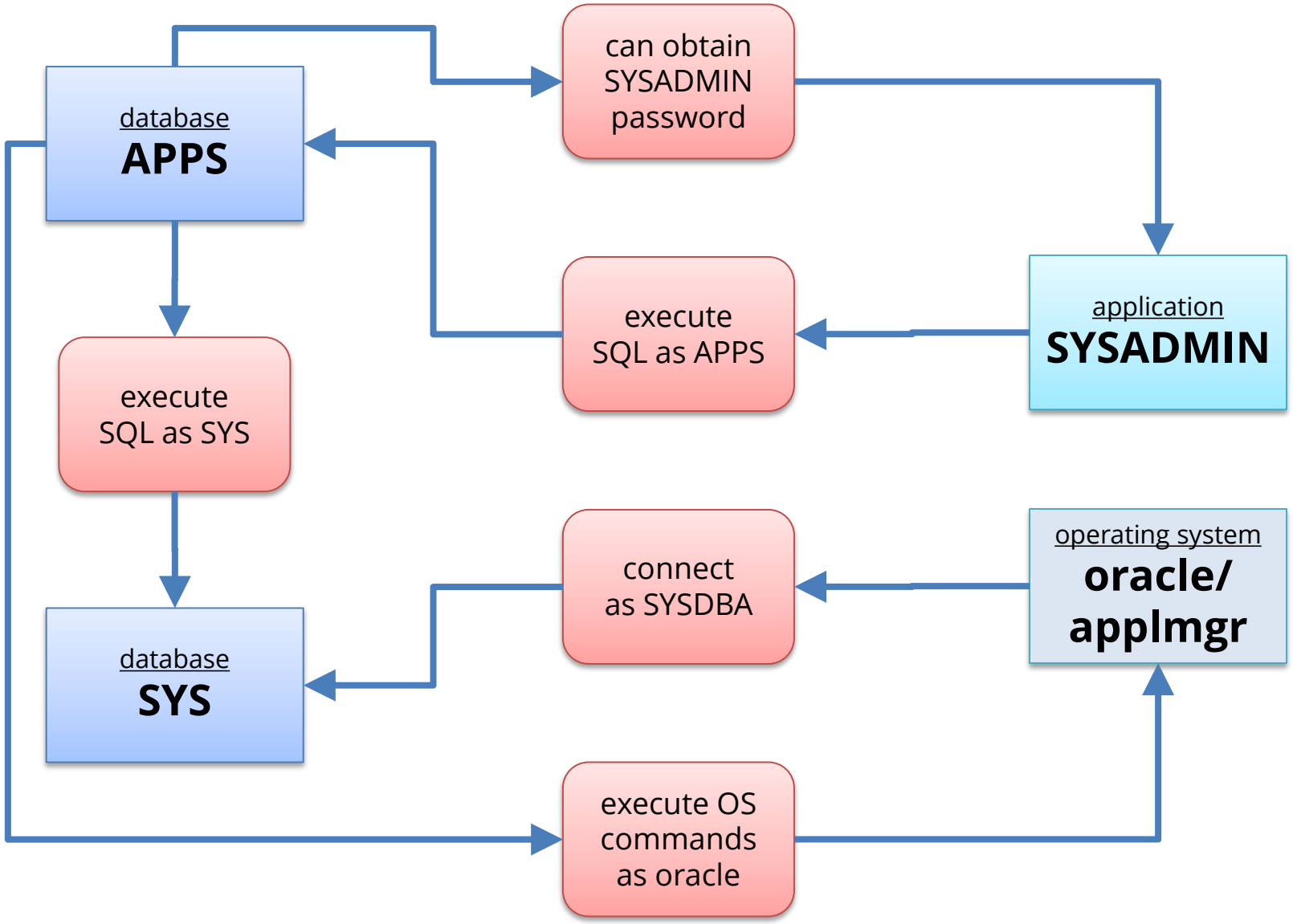
Data Center
- Location
- Floor/section
- Cage access

Administrators
- DBAs
- O/S Admins
- Sysadmin

Infrastructure
- Storage
- Network
- Hypervisor
- Backup

Offshore
- Office(s)
- 1:10 on-shore
- Contractors of the contractors

Generic Privileged Account Inter-Dependency



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

- **Use service providers who regularly produce SOC reports**
  - Management commitment
  - Request SOC reports annually
- **Use 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

Verify Trust of Service Providers

- **Verifying your service provider's supply chain**
  - Are they outsourcing key services?
- **Writing verification 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

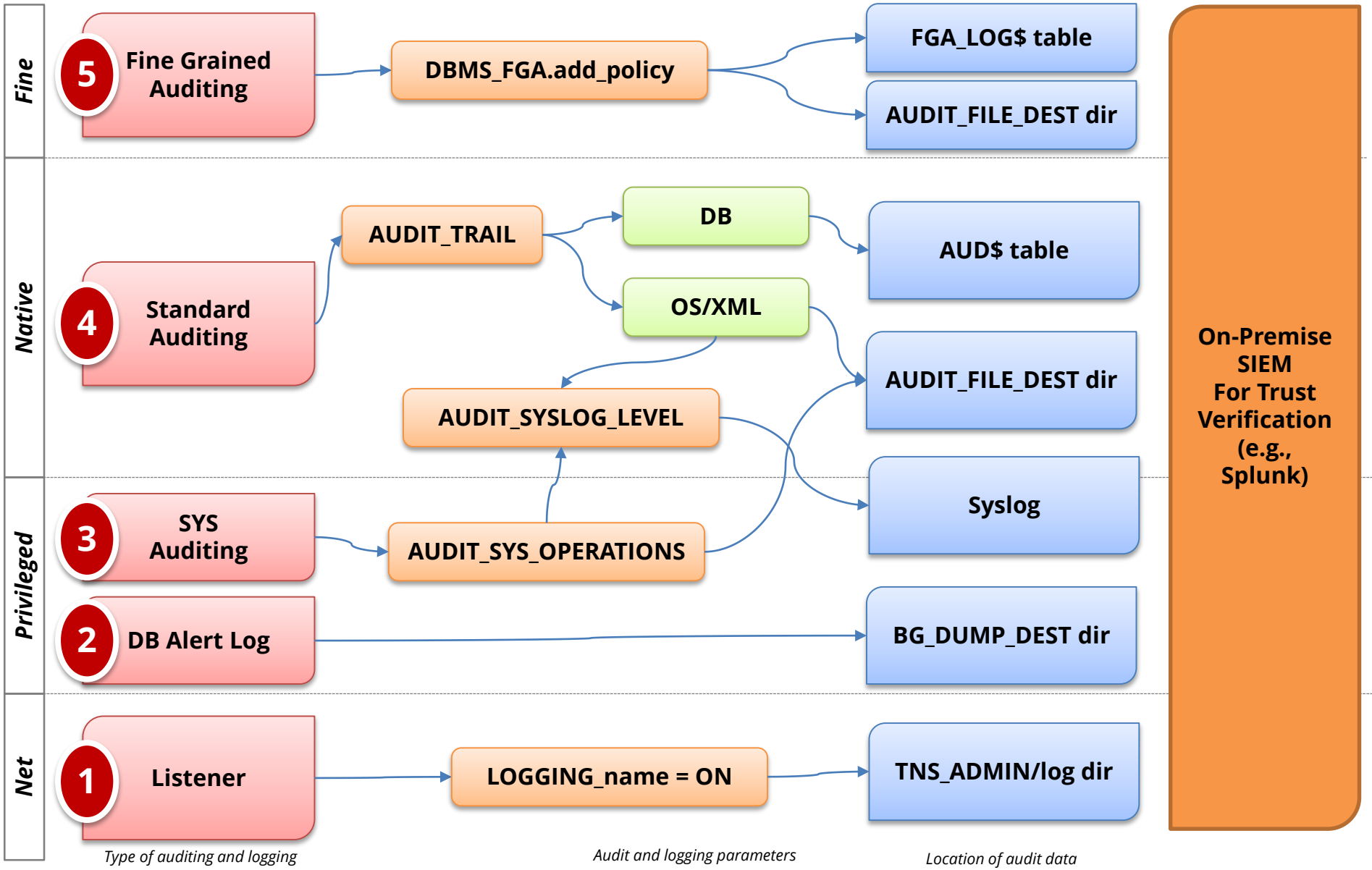
Compliance Challenges

- **Oracle E-Business Suite by default does not meet most compliance standards**
  - HIPAA, SOX, PCI
- **Some customers need to meet more than one standard**
- **Hosting can complicate reporting**
  - Majority of requirements owned by client
  - Many shared responsibilities

Trust-But-Verify Best Practices

- **Require adherence to PCI standard (credit card security) even if not a processing cards**
  - Well documented and consistent set of standards
- **Consider independent security assessments**
  - In-house technical and security expertise?
- **Request audit trails and logs for insider operating system and/or database activity**
  - Require Syslog feeds to on premise logging solution

Oracle Database Auditing



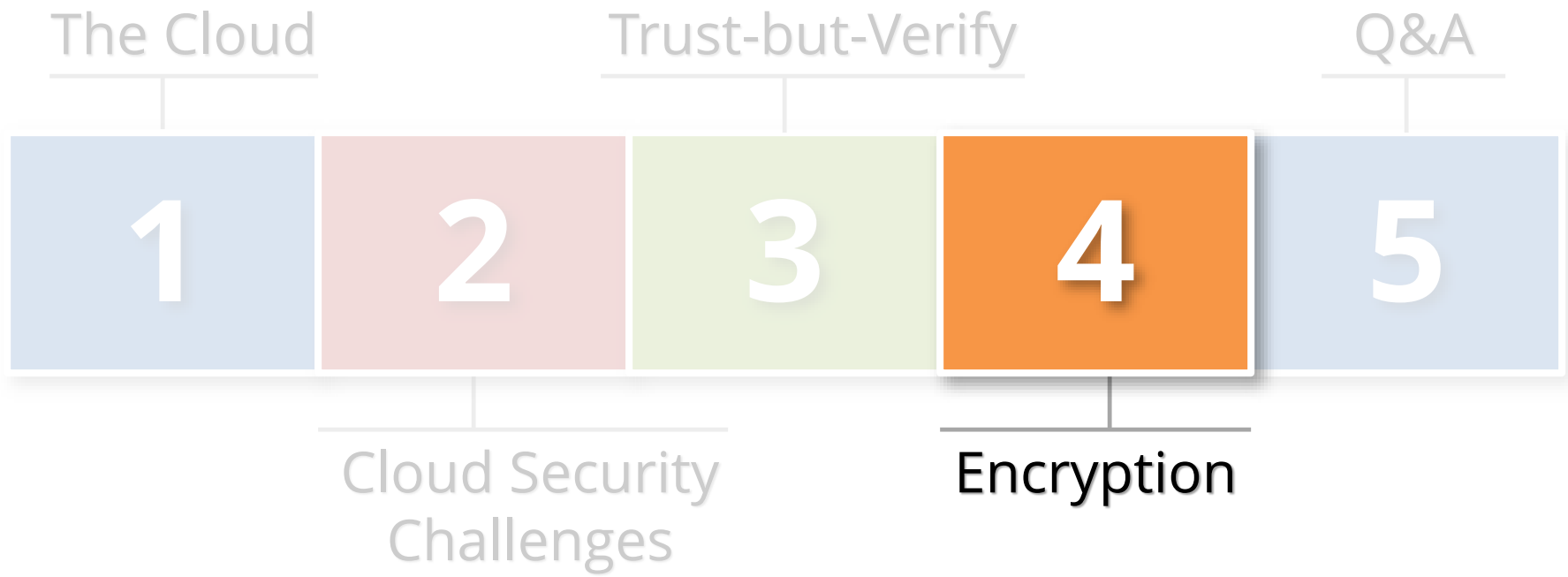
Trust-But-Verify

- **Risks to Oracle E-Business Suite in the Cloud**
  - How do guard against authorized changes and access
  - How to identify poor or risky behaviors
  - How to meet compliance requirements (SOX, HIPAA, PCI)

- **Use policy of Trust-but-Verify**
  - Implement log and audit framework
  - Build security monitoring, alerting and audit programs using log and audit framework
  - Regular assessments (e.g. Integrigy to professionally verify)

- **Integrigy Framework for Oracle E-Business Suite logging and auditing**
  - Whitepaper: http://www.integrigy.com/security-resources/guide-auditing-oracle-applications

Agenda


The Cloud
Trust-but-Verify
Q&A
1
2
3
4
5
Cloud Security Challenges
Encryption

Oracle E-Business Suite Encryption

- **In-Motion**
  - Use SSL
- **At-Rest**
  - Use File system (TDE) encryption
  - Don’t forget about backups, VM images, etc.
- **In-Use**
  - No protection (APPS)

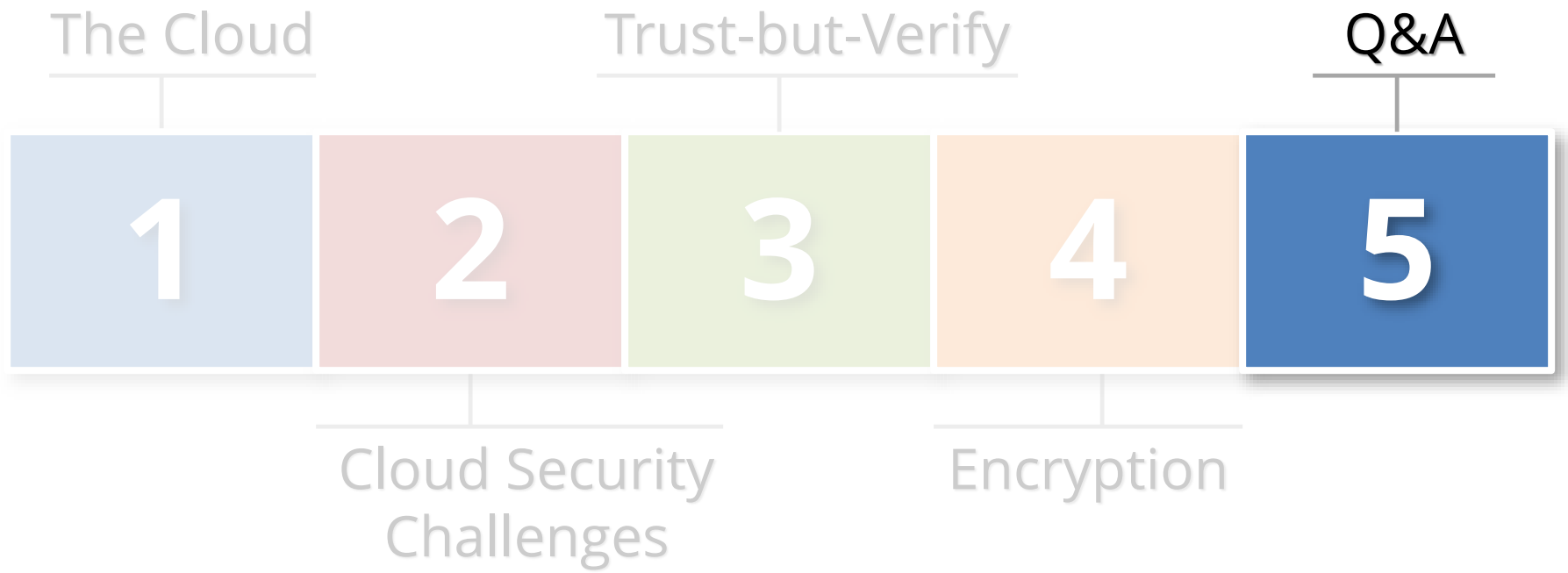
Does Encryption Make Clouds Safer?

- **What does Encryption provide?**
  - Confidentiality and Integrity
  - Not at cost of Availability
- **Does encryption protect sensitive data?**
  - Sort of - coarse-grained file access control only
  - Little to no protection against abuse by privileged users
  - Access to Oracle wallets controls everything
- **Key management determines success**
  - You and only you can should control the keys
  - Recommend use of Hardware Security Module

Hardware Security Modules (HSM)

- **HSMs are physical devices**
  - Secure storage for encryption keys
  - Secure computational space (memory) for encryption and decryption
- **Oracle TDE fully certified to use HSMs**
  - More secure alternative to the Oracle wallet
  - Several third party vendors
    - Vormetric
- **Using HSMs for E-Business in the Cloud**
  - Must be fully in your control, you own your data
  - No protection for APPs password

Agenda


The Cloud
Trust-but-Verify
Q&A
1
2
3
4
5
Cloud Security Challenges
Encryption

Contact Information

Stephen Kost

Chief Technology Officer

Integrigy Corporation

web: **www.integrigy.com**

e-mail: **info@integrigy.com**

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

youtube: **youtube.com/integrigy**