Top Ten Fraud Risks in the Oracle E-Business Suite

Jeffrey T. Hare, CPA CISA CIA
Industry Analyst, Author, Consultant
ERP Risk Advisors

Stephen Kost
Chief Technology Officer
Integrigy Corporation

February 24, 2011

Speakers

Jeff Hare

ERP Risk Advisors

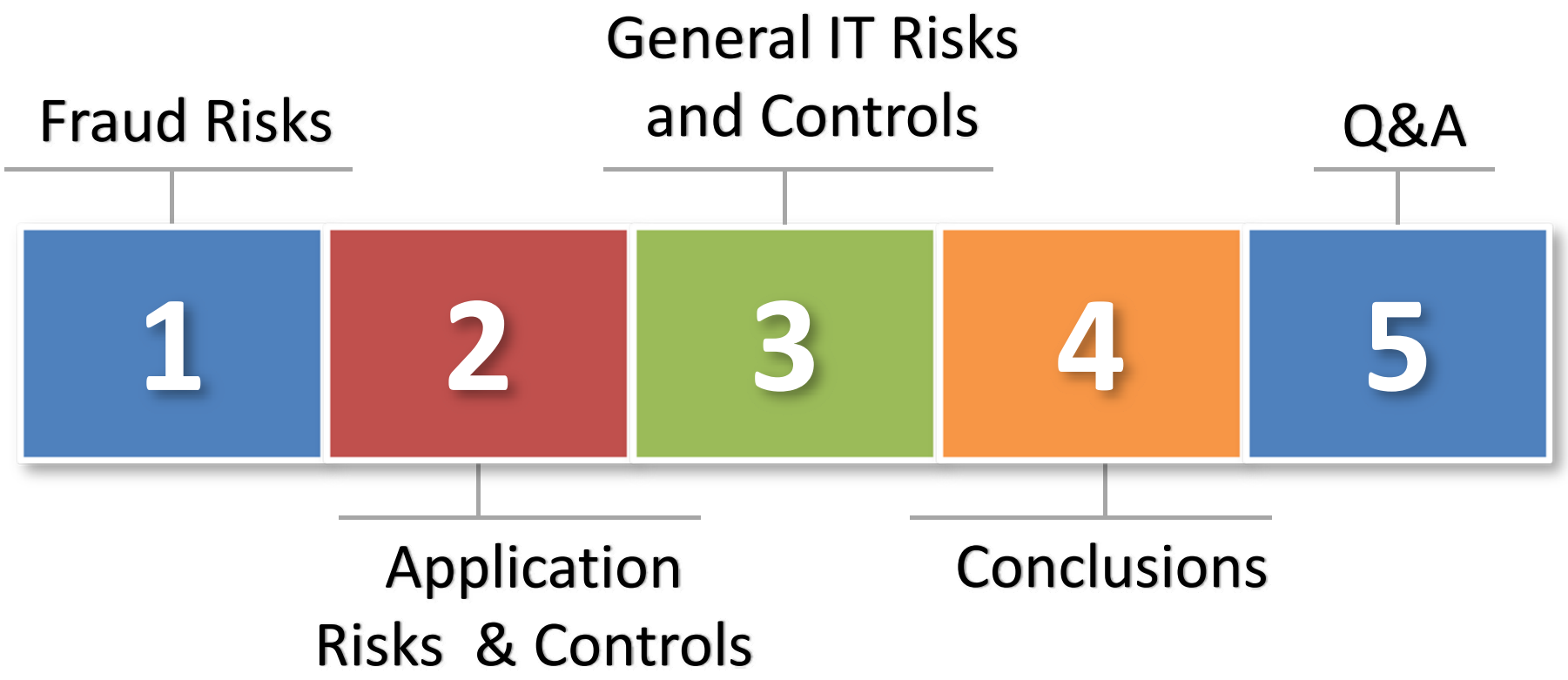
- Founder of ERP Risk Advisors / ERP Seminars and Oracle User Best Practices Board
- 14 years working with Oracle EBS as client and consultant
- Experience includes Big 4 audit, 6 years in CFO/Controller roles – both as auditor and auditee
- Author – *Oracle E-Business Suite Controls: Application Security Best Practices*

Stephen Kost

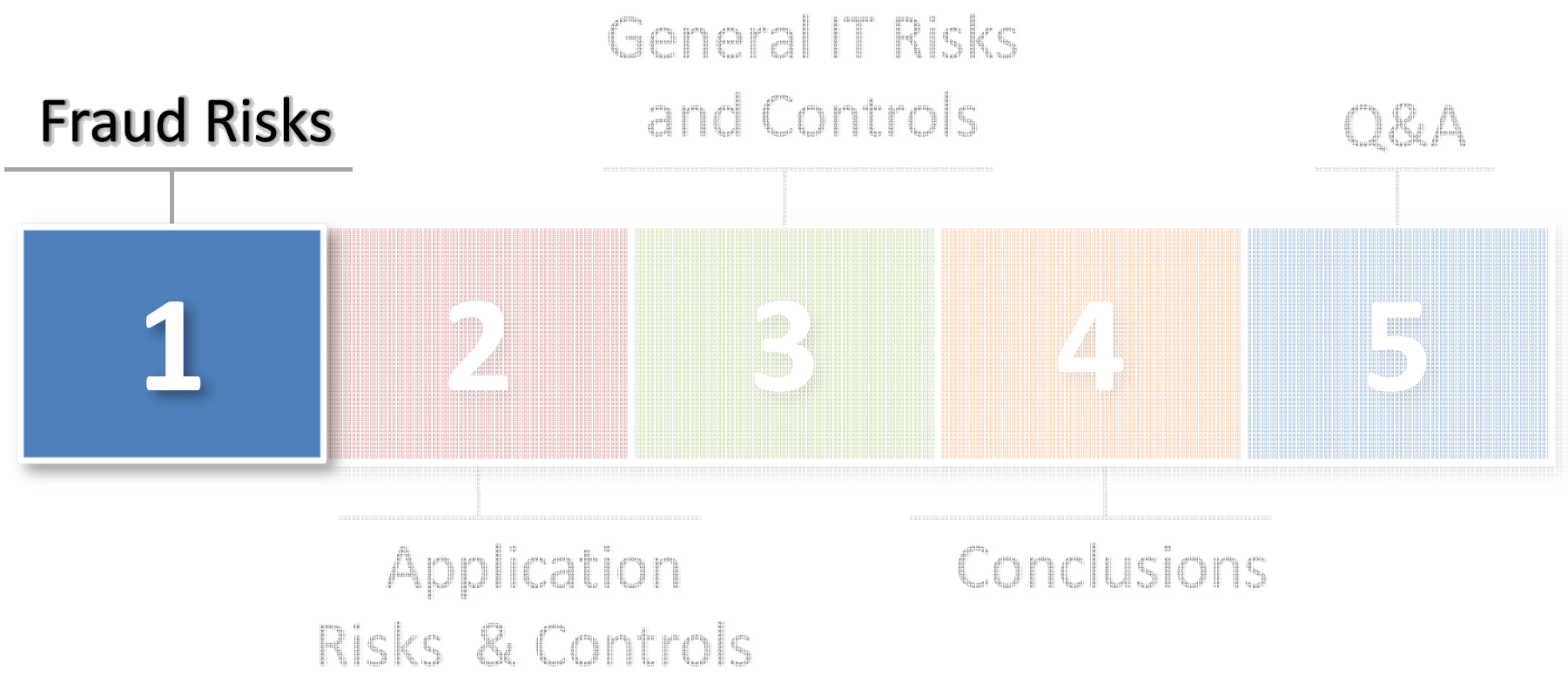
Integrigy Corporation

- CTO and Founder
- 16 years working with Oracle and 12 years focused on Oracle security
- DBA, Apps DBA, technical architect, IT security, …
- Integrigy Consulting – Oracle EBS security assessments and services
- Integrigy AppSentry – Oracle EBS Security Assessment and Audit Tool

Agenda


Fraud Risks
General IT Risks and Controls
Q&A
1
2
3
4
5
Application Risks & Controls
Conclusions

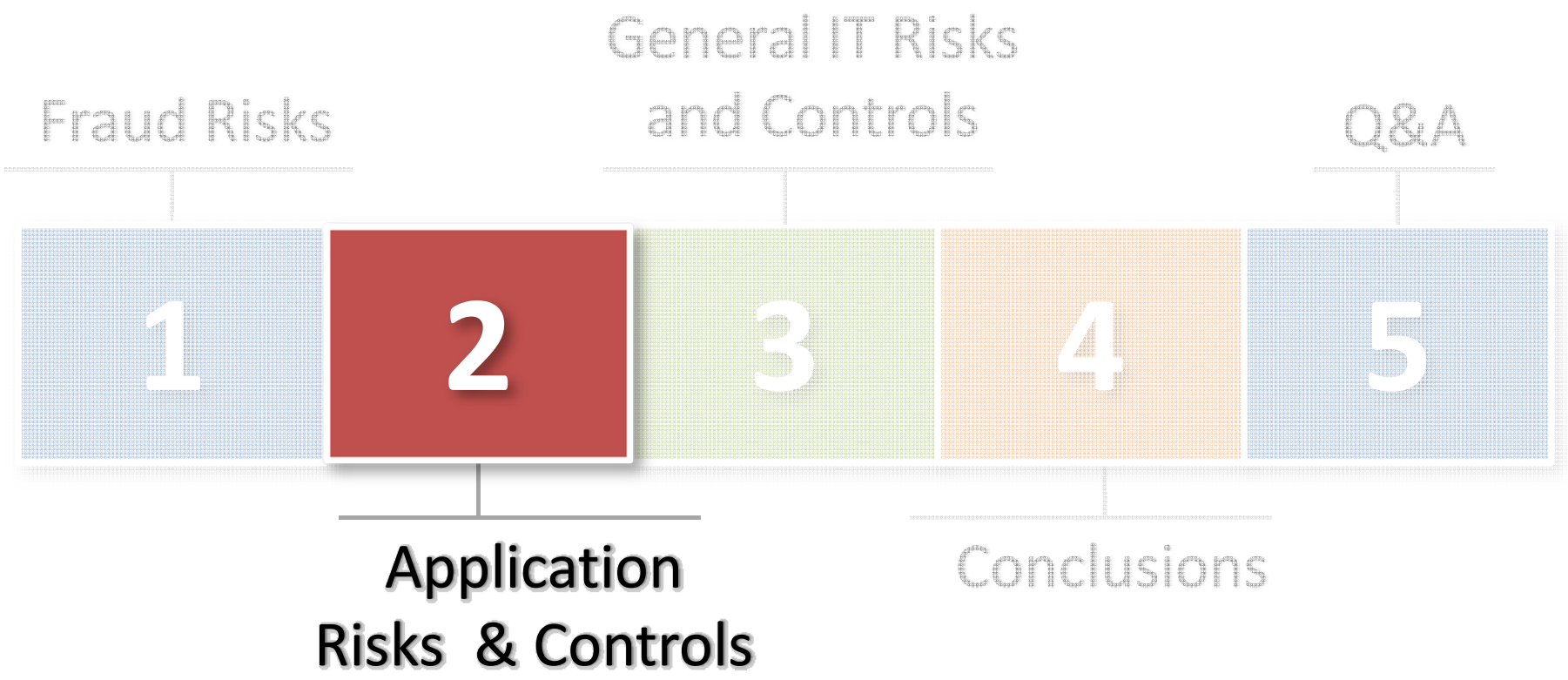
Agenda


Fraud Risks
General IT Risks and Controls
Q&A
1
2
3
4
5
Application Risks & Controls
Conclusions

Fraud – Procure to Pay (PTP)

- **There are various fraud risks in the PTP process. Here are some samples:**
  - ACH file is altered after it is generated from the AP system
  - *Fictitious vendor created in system*
  - *Fictitious bank account is set up for fictitious or valid vendor*
  - Check stock is used to generate check that is not recorded in AP system
  - Address is changed on check while check is being written
  - Check voided in AP system
  - Invoice approvers signature is falsified
  - Invoice distribution coded to wrong account
  - Falsified supplier master, bank account, or invoice information entered by AP clerk without any documentation

Agenda


Fraud Risks
General IT Risks and Controls
Q&A
1
2
3
4
5
Application Risks & Controls
Conclusions

Supplier Master Maintenance

- **The creation of a fictitious supplier in the AP system is one of the most significant risks**
  - PO's w/ two way match
  - Invoices approved within approval limit
  - Invoice with falsified signature
  - 3-way match with auto-receipts (i.e. drop ship)
  - Invoice data entered without supporting invoice

Bank Account Maintenance

- **The creation of a fictitious bank account in the AP system is one of the most significant risks**
  - Allows you to associate with one or more suppliers in 11i
  - Set up at the supplier level in R12
  - Allows ACH transactions to be created and re-routed to fraudulent bank account
  - Circumvents other controls

Poor Policies and Procedures

- **Policies and procedures need to be risk-based. Identify the risks and design appropriate controls**
  - Policy – all new suppliers and changes to suppliers should have some level of validation (i.e. I9, EIN verification, D&B, website, third party verification, validation of data entry)
  - Policy – all new bank accounts and changes to bank accounts should be verified (i.e. secure fax, call back to verify fax, validation of data entry)

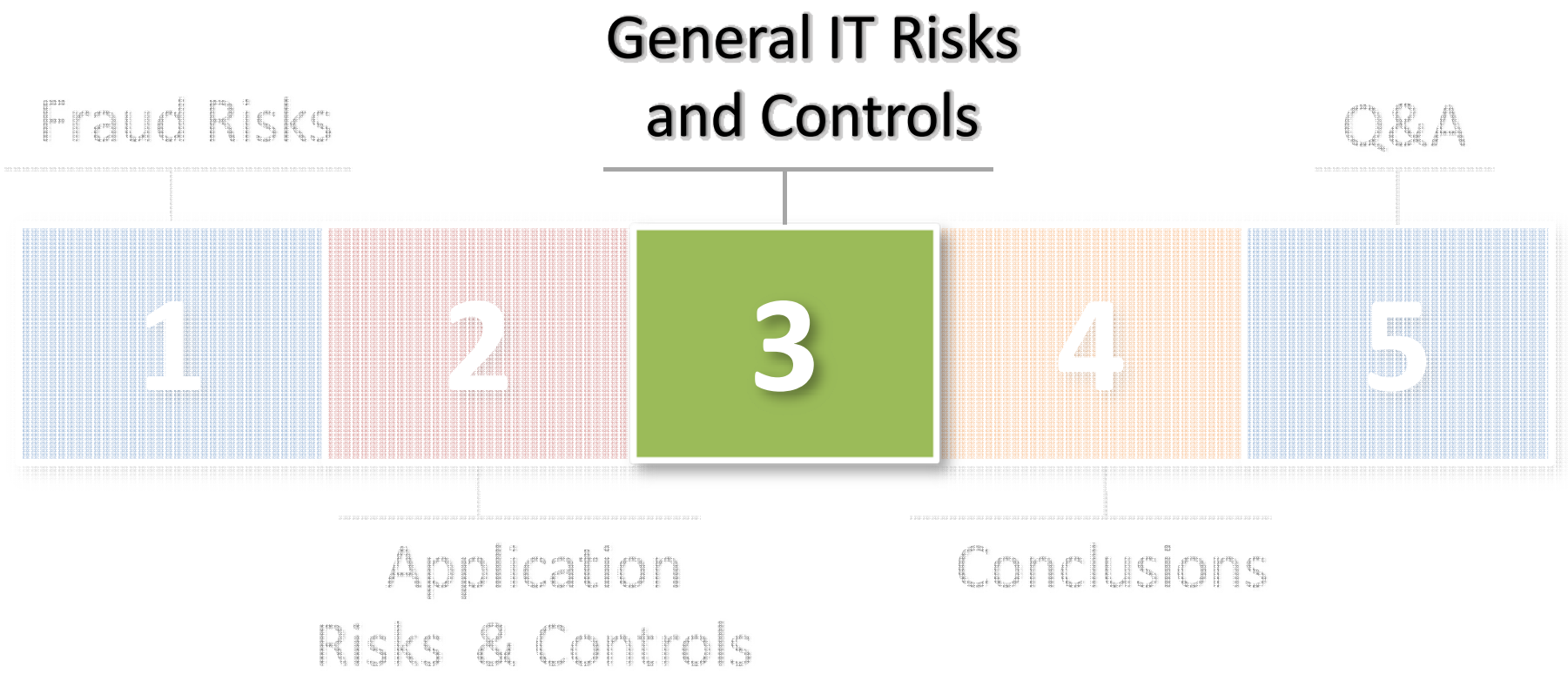
Poor Policies and Procedures

- **Policies and procedures need to be risk-based. Identify the risks and design appropriate controls**
  - Policy – verification of ACH files (amounts)
  - Policy – identified protocol for wires
  - Policy – use of positive pay for all checks
  - Policy – approval authority established by Board
  - Policy – 100% of all bank and suppliers adds and changes are audited before payments made

Lack of Application Controls Monitoring

- **Monitoring of key application controls (manual and automated)**
  - Those that are automated by configuration
    - Allow address change – payables options
    - PO Line Types
    - PO Document Types
  - Those that are set by policy
    - Don’t allow suppliers/bank accounts to be set up/changed without approved paperwork
    - Override of matching requirements when entering a Purchase Order

Agenda


General IT Risks and Controls
Fraud Risks
Q&A
1
2
3
4
5
Application Risks & Controls
Conclusions

General IT Controls

- **Be aware of general IT controls that can allow data to be updated outside of policy**
  - Direct database updates
  - Use of SQL forms
  - Use of seeded / vendor supplier accounts – at application and database levels
  - Password resets
  - Shared logins

IT Security

- **IT security**
  - IT security (below the application level) is critical to preventing and detecting fraud in the PTP cycle because of the back door and often undetectable nature of the access
- **Adhere to the Oracle Best Practices for Oracle EBS security**
  - See Metalink documents 189367.1 and 403537.1
  - Written by Integrigy
  - Oracle has not updated since 2007
- **Perform periodic security reviews and assessment**
  - Validate compliance against security best practices

Oracle EBS Password Decryption

- **Oracle EBS end-user application passwords stored encrypted, not hashed**
  - Account passwords stored in FND_USER table
  - Procedure to decrypt passwords well documented and published on the Internet
  - Google “Oracle Applications password decryption”
- **Secure hashing of passwords is optional and must be enabled by DBA – including in R12**
  - See Integrigy whitepaper for recommendations

Oracle EBS Password Decryption

- **Must have access to encrypted passwords in the FND_USER table – always for APPS_READ accounts**
  - May be production or any test or development database unless passwords are explicitly changed during cloning
  - Must have some direct database access to either production, test, or development
- **Google detailed procedure from Internet**
- **Run SQL to get APPS password from user with known password – either yours or GUEST**
- **Run SQL to get all other users passwords**
- ✓ **Login to production as any user**

Seeded Application and Database Accounts

- **Application Accounts**
  - Oracle EBS delivered with up to **40 seeded application accounts**
  - Some seeded application accounts are active
  - Some seeded application accounts have significant privileges
  - Most seeded applications have default passwords

- **Database Accounts**
  - Oracle EBS database delivered with up to **300 database accounts**
  - All database accounts have default passwords
  - All database accounts are active
  - Almost all database accounts significant privileges

Seeded Application Account Responsibilities

Active Application Account	Default Password	Active Responsibilities
ASGADM	WELCOME	▪ SYSTEM_ADMINISTRATOR ▪ ADG_MOBILE_DEVELOPER
IBE_ADMIN	WELCOME	▪ IBE_ADMINISTRATOR
MOBADM	MOBADM	▪ MOBILE_ADMIN ▪ SYSTEM_ADMINISTRATOR
MOBILEADM	WELCOME	▪ ASG_MOBILE_ADMINISTRAOTR ▪ SYSTEM_ADMINISTRATOR
OP_CUST_CARE_ADMIN	OP_CUST_CARE_ADMIN	▪ OP_CUST_CARE_ADMIN
OP_SYSADMIN	OP_SYSADMIN	▪ OP_SYSADMIN
WIZARD	WELCOME	▪ AZ_ISETUP ▪ APPLICATIONS FINANCIALS ▪ APPLICATION IMPLEMENTATION

Default Oracle Password Statistics

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

Oracle Database Password Brute Forcing

- **Must have access to database password hashes in the DBA_USER view – typical for APPS_READ accounts**
  - May be production or any test or development database unless passwords are explicitly changed during cloning
  - Must have some direct database access to either production, test, or development
- **Query the DBA_USER view**
  - select * from sys.dba_users;
- **Google “oracle password cracker”**
  - Download one of a dozen free tools
- **Run cracker and find any default or weak database passwords**
  - Done off-line so no audit trail or other indicator
  - Run for a week on your “gaming” machine to get 8 or less character passwords

✓ **Login to production database account with significant privileges**

Direct Database Access

- **Database access is a key problem**
  - APPS_READ
  - Read only accounts often created with read to all data
- **Access to sensitive data by generic accounts**
  - Granularity of database privileges, complexity of data model, and number of tables/views make it difficult to create limited privilege database accounts
  - Must use individual database accounts with roles limiting access to data along with other security

Privileges and Access in Oracle EBS

- **Many generic and privileged accounts in application and database**
  - **Database - APPS, SYS, SYSTEM, APPLSYS, …**
  - **Application - SYSTEM, GUEST**
  - DBAs must use generic accounts for many maintenance activities
  - Generic application accounts used for scheduling key batch processes
- **Limited auditing and control over the use of generic accounts**
  - No auditing is enabled by default in database or application
  - Auditing on transactions often a major performance impact

How to control and monitor the DBAs

- **DBAs must use generic accounts for many maintenance activities**
  - **Operating System**: oracle, applmgr
  - **Database**: APPS, SYS, SYSTEM and seldom any other accounts
  - **Application**: SYSADMIN – must be used very occasionally

Monitor usage of generic accounts only by named individuals	possible
Activity by generic accounts	possible, can be costly
Activity by a named individual using a generic account	very difficult, very costly

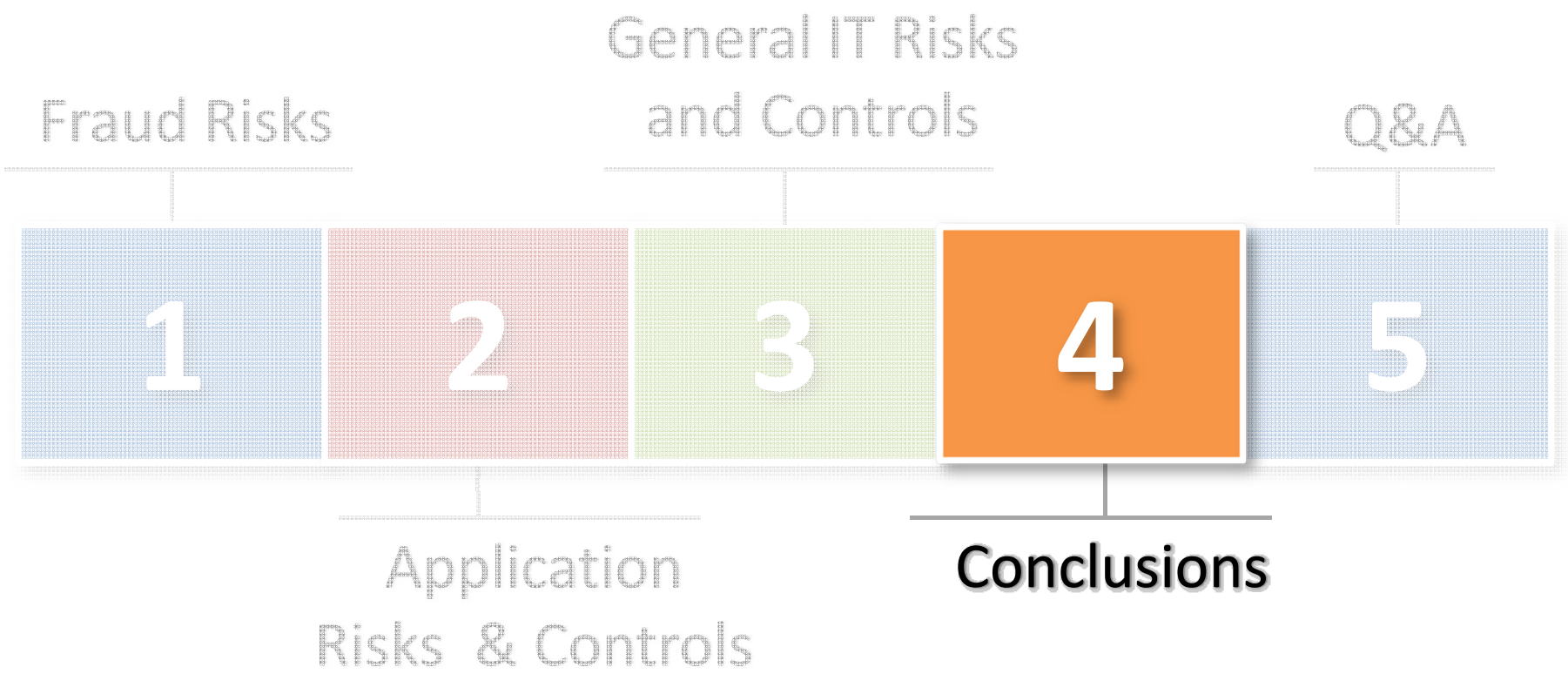
Forms that Allow SQL

- **Allow adhoc SQL statements to be executed within them (over 30 forms)**
- **Could be used to update high risk data such as supplier addresses and bank accounts**
- **May not have any audit trail (before/after values) created to know who made the update**
- **Examples include:**
  - Alerts
  - Collection Plans

Forms that Allow SQL

- Applications
- Attribute Mapping
- Attribute Mapping Details
- Audit Statements
- Business Rule Workbench
- Create QuickPaint Inquiry
- Custom Stream Advanced Setup
- Defaulting Rules
- Define Assignment Set
- Define Data Group
- Define Data Stream
- Define Descriptive Flexfield Segments
- Define Dynamic Resource Groups
- Define Function
- Define Pricing Formulas
- Define Pricing Formulas
- Define Security Profile
- Define Validation Templates
- Define Value Set
- Define WMS Rules
- Dynamic Trigger Maintenance
- Foundation Objects
- PL/SQL tester
- QA - Collection Plan Workbench
- Register Oracle IDs
- SpreadTable Diagnostics Form
- Spreadtable Metadata Administration
- Workflow Activity Approval Configuration Framework
- Workflow Process Configuration Framework
- Write Formula

Agenda


Fraud Risks
General IT Risks and Controls
Q&A
1
2
3
4
5
Application Risks & Controls
Conclusions

Jeff's Conclusions

- **Fraud prevention and detection requires a comprehensive approach including the following:**
  - Well-designed processes and controls
  - Monitoring of sub-material fraud risk and non-key controls
  - Closing known back-door loopholes (i.e. effective IT security)
- **Vulnerabilities in any of these will give a fraudster a foothold that can be exploited**

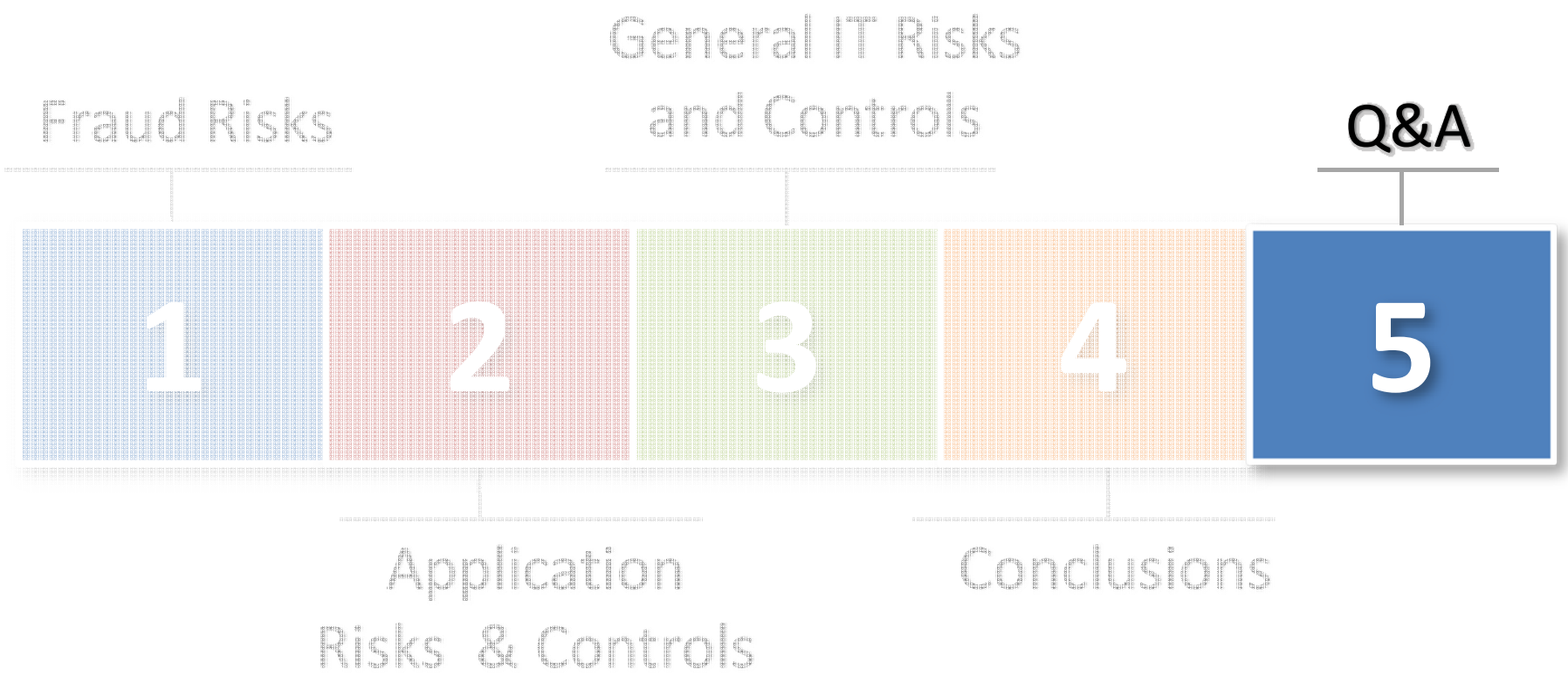
Steve's Conclusions

- **Oracle E-Business Suite security and compliance requires a team effort**
  - DBAs, IT Security and Internal Audit must work together to ensure a secure and compliant environment
- **Security is constantly changing due to application changes and new risks**
  - Periodic reviews and assessments are required
- **Security vulnerabilities must be addressed**
  - The business must prioritize security patches
- **No "silver bullet" exists for protecting the Oracle EBS**
  - A combination of policies, procedures, reviews, and tools must be put in place to address this complex environment

References and Resources

- **Integrigy's Website**
  - www.integrigy.com
  - Oracle E-Business Suite Security Whitepapers
- **ERP Risk Advisors Oracle Internal Controls and Security List Server**
  - http://groups.yahoo.com/group/OracleSox
- **ERP Risk Advisors Internal Controls Repository**
  - http://tech.groups.yahoo.com/group/oracleappsinternalcontrols
- **Jeff Hare's Book**
  - *Oracle E-Business Suite Controls: Application Security Best Practices*
- **Oracle Best Practices for Securing Oracle EBS**
  - Metalink Note IDs 189367.1 and 403537.1

Agenda


Fraud Risks
General IT Risks and Controls
Q&A
1
2
3
4
5
Application Risks & Controls
Conclusions

Speaker Contact Information

Jeffrey T. Hare
Industry Analyst, Author
ERP Risk Advisors

e-mail: jhare@erpra.net
website: www.erpra.net

Stephen Kost
Chief Technology Officer
Integrigy Corporation

e-mail: info@integrigy.com
blog: integrigy.com/oracle-security-blog
website: www.integrigy.com