

Preparing for the Security Audit

Is your ERP Ready

Mike Hoskin

Q Software



NCOAUG
NORTH CENTRAL ORACLE APPS USER GROUP
TRAINING DAY
AUGUST 1, 2019

NCOAUG

NORTH CENTRAL ORACLE APPS USER GROUP

TRAINING DAY

AUGUST 1, 2019



Objectives – to Understand

The Business Perspective of ERP Fraud

How to Prepare for an ERP Audit

Reporting on ERP Security

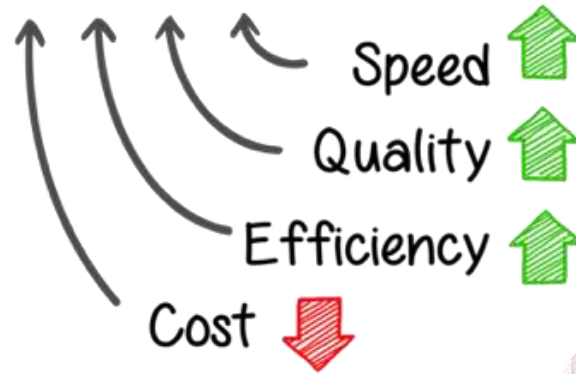
The Role of Automation

Contents

Introduction & Objectives
The Business Issues
IT & Audit – Working Together
Application Security Controls
Configuration Management
Auditing your ERP
Efficiencies
Summary

Why do you have an ERP System?

Performance



What Can Happen?

Theft of IPR
Accidental Data Error
Process Error
Change Control Mistake
Financial Manipulation
Fraud



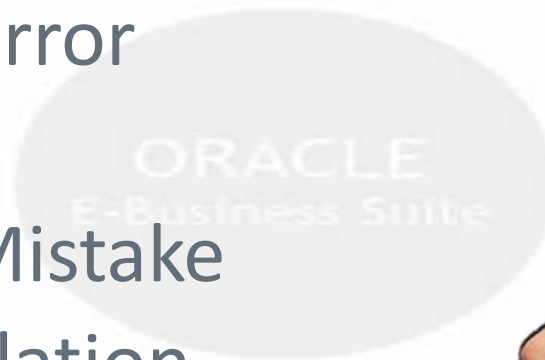
Procurement



Manufacturing



Fulfillment



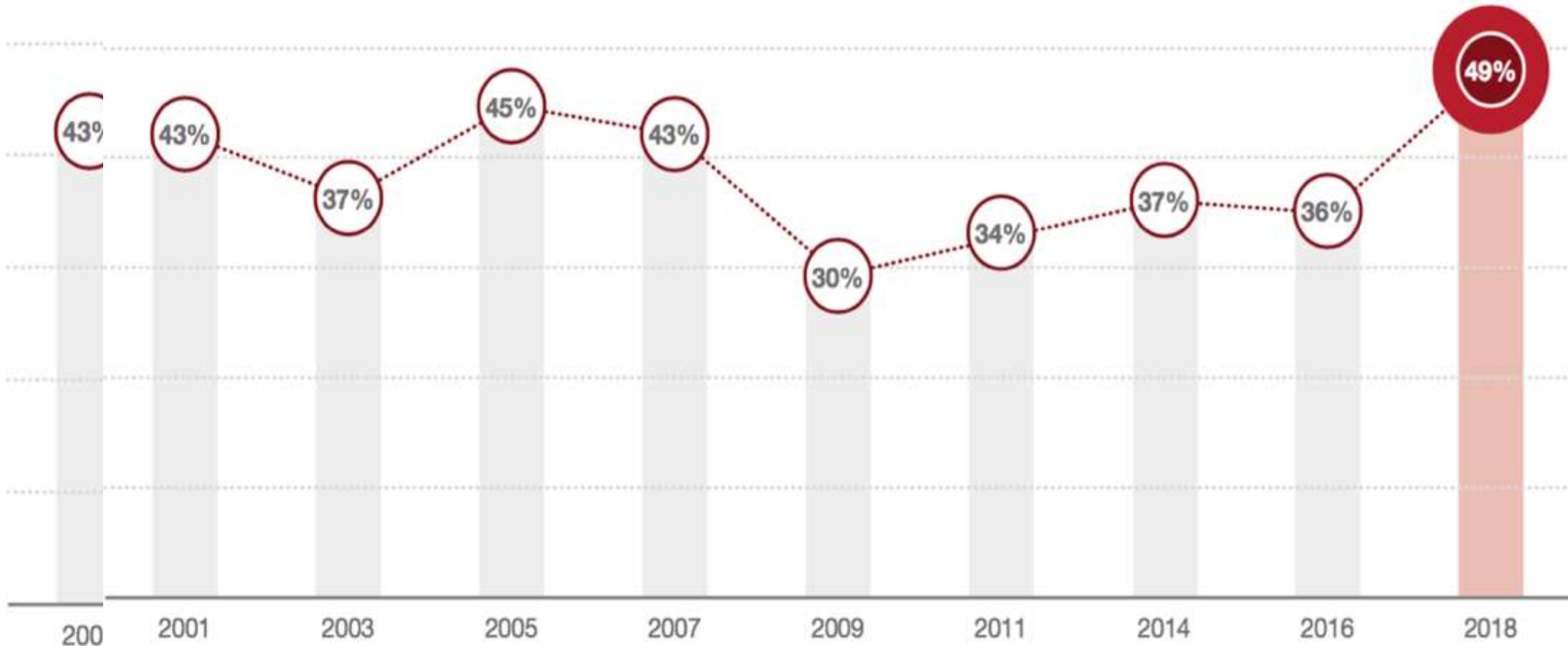
Customer Relationship Management



Customer Service



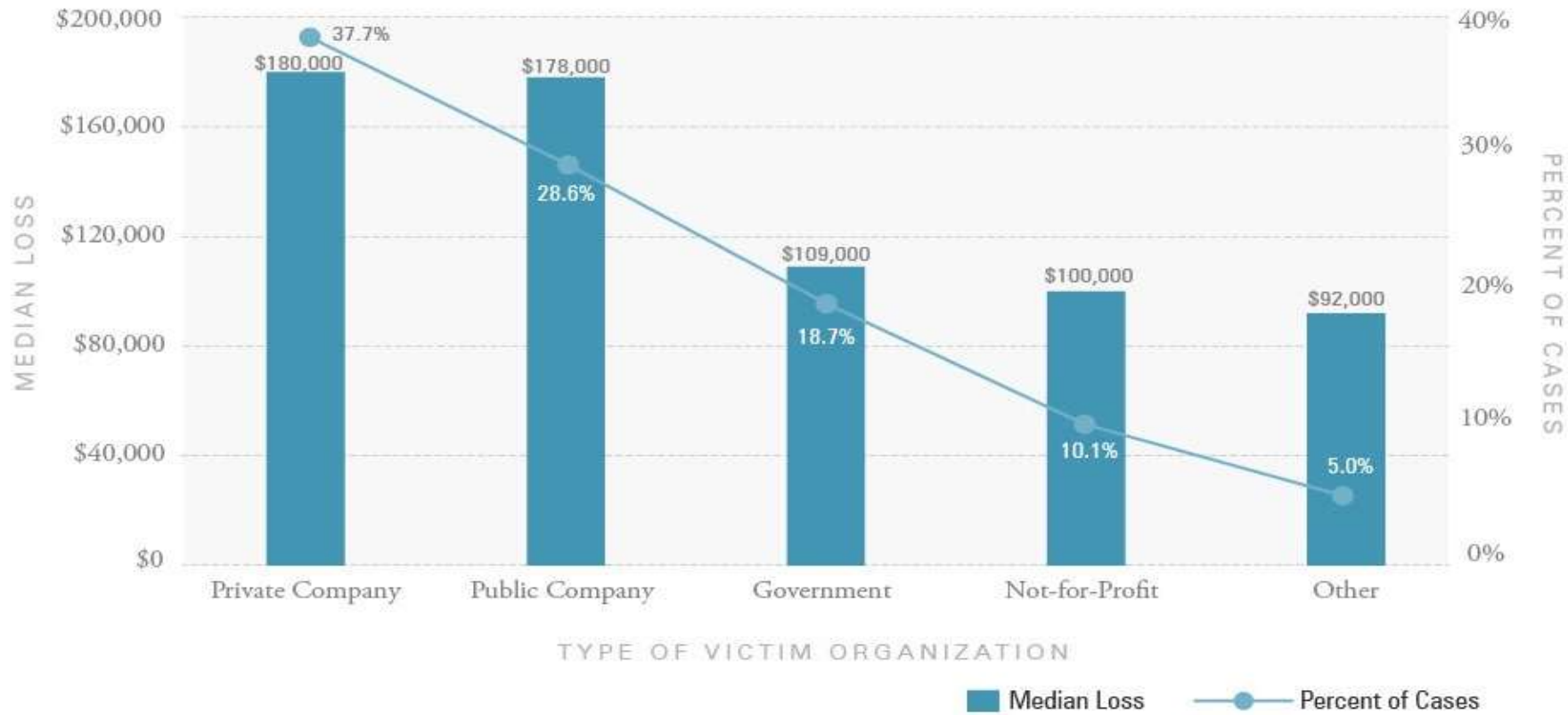
Has your company experienced Fraud?



© PwC 2018 Crime & Fraud Survey

Fraud – The Business Suffers

Figure 38: Type of Victim Organization—Frequency and Median Loss



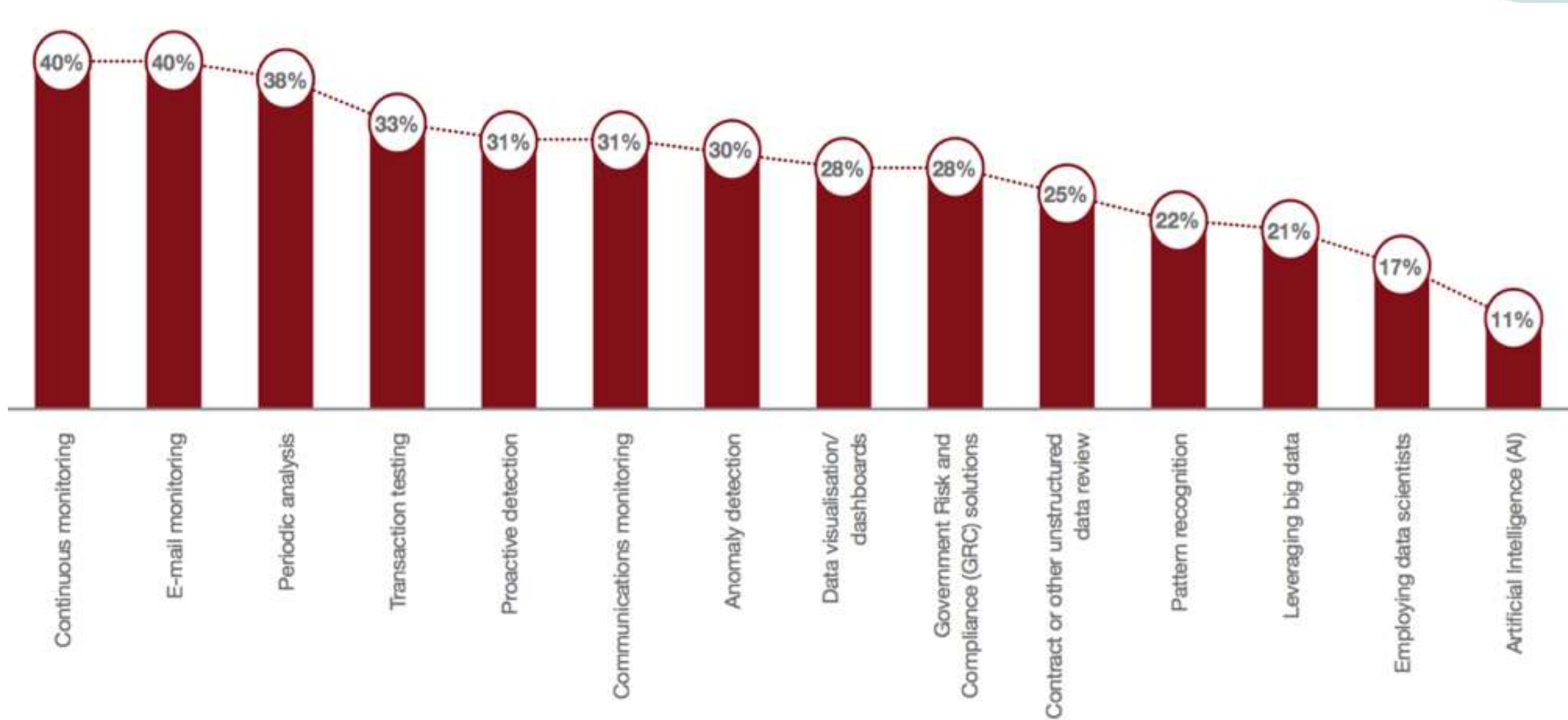
© 2016 Association of Certified Fraud Examiners, Inc. All rights reserved.

INTERNAL CONTROL WEAKNESSES WERE RESPONSIBLE FOR NEARLY HALF OF FRAUDS

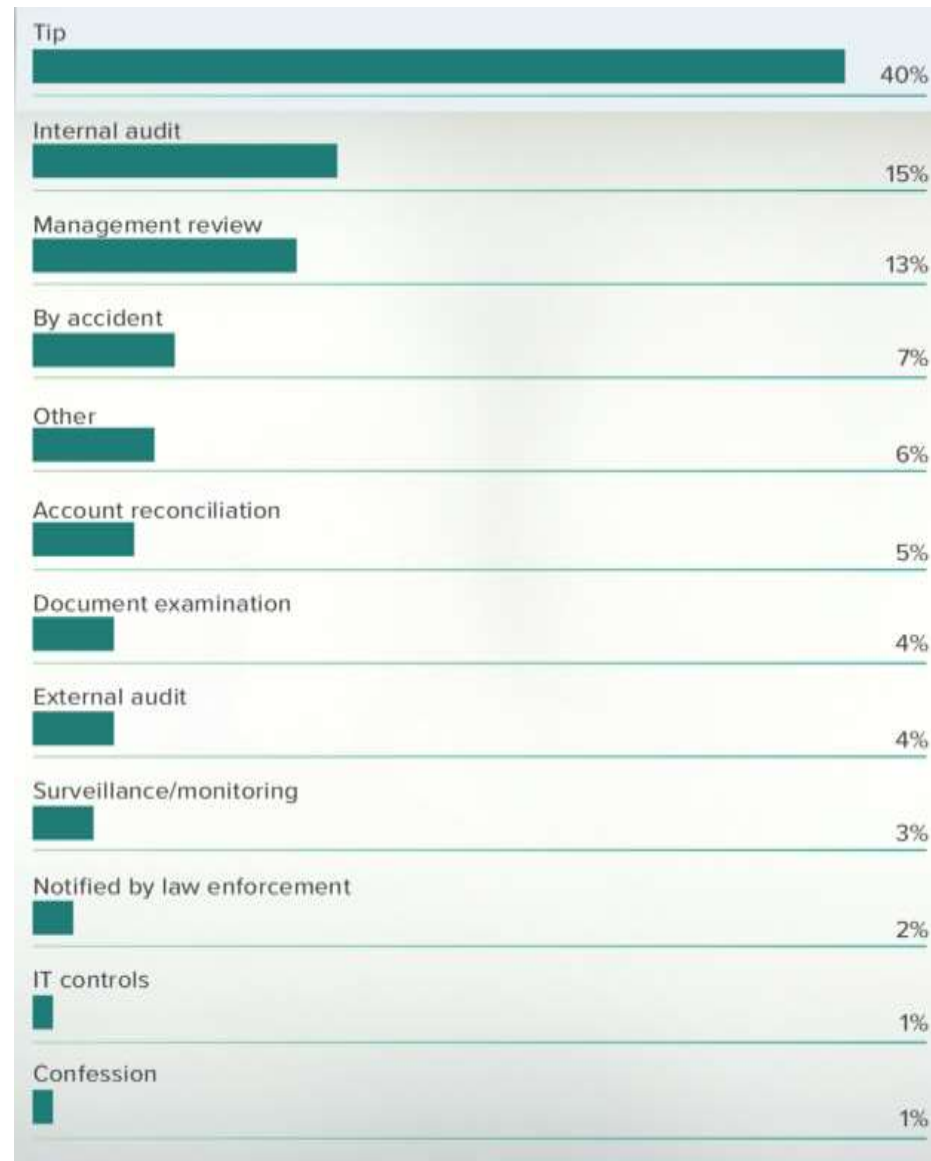


© ACFE 2018

Tools to Combat Fraud



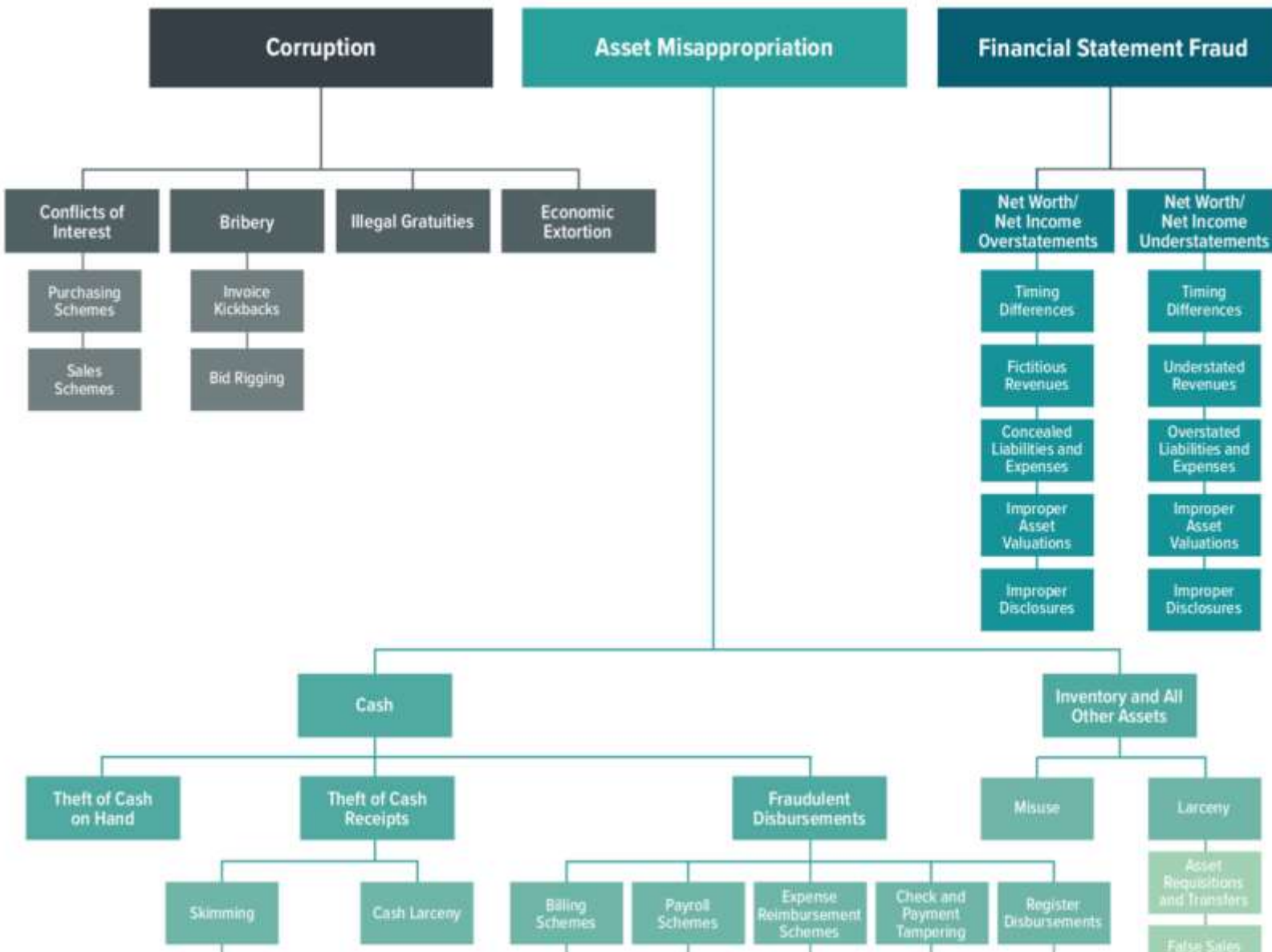
How are Frauds Detected



© ACFE 2018

Types of Fraud

© ACFE 2018



Contents


Introduction & Objectives
The Business Issues
IT & Audit – Working Together
Application Security Controls
Configuration Management
Auditing your ERP
Efficiencies
Summary

IT – it's a Strange Language



Educate Yourself
& Them

Market – When do Companies Engage?

- Strategic Planning 
- New Implementation or Upgrade
- Pre IPO
- M&A
- “The Auditors are Coming”
- “We Failed our Audit”

How to Get the Business Involved & Committed?

Proper Planning - Together
Understand the risks
Understand the benefits
Know that there is automation
Education & Communication



Tips | Business Language

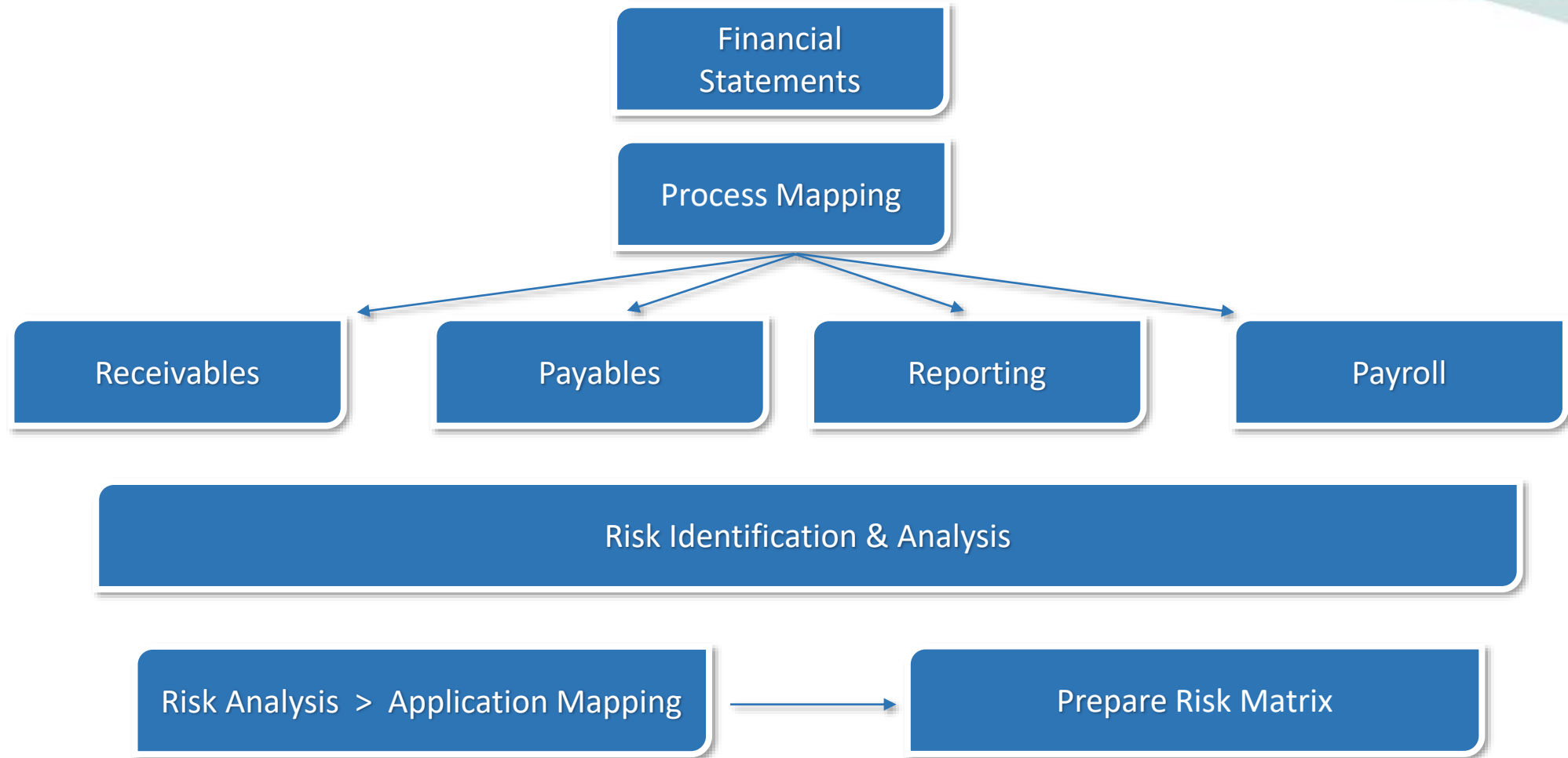
Are we talking about the same thing?

Standardize descriptions

Average Segregation of Duties rules = 25 (start small)



Assessing Risk



Education – Joint Understanding

Audit

External Audit

IT General Controls

Access & SoD

IT

Cloud

Security Setup

Configuration Management

Joint Understanding of Risks



Contents

Introduction & Objectives
The Business Issues
IT & Audit – Working Together
Application Security Controls
Configuration Management
Auditing your ERP
Efficiencies
Summary

Application Security

User Authorization
Access
Segregation of Duties
Role Design
Auditing & Reporting
Compliance





Your Risk Model

Ranking	Description	Risk / Impact	Action	Responsibility
Critical	Approve Pay Rates & Employee Master Data Maintenance	An individual with this access could approve salary/wage rate increases and update HR master data without any independent review.	Remediate	Payroll Manager
High	Approve Invoices (Vendor Payments) & Approve Purchase Orders	An individual could approve a fictitious or inappropriate purchase order and enter an invoice against that order. This covers two of the three-way match controls, thereby weakening the three-way match control.	Mitigate	Controller
High	Cash Disbursement & Create / Maintain Bank Accounts	An individual could create a fictitious bank account which appears to be part of the company and re-direct funds to this bank account by authorizing cash disbursements records.	Remediate or Mitigate	Controller

Benefits of RBAC (Role Based Access Control)

Efficient Security Mgmt.

Clarity

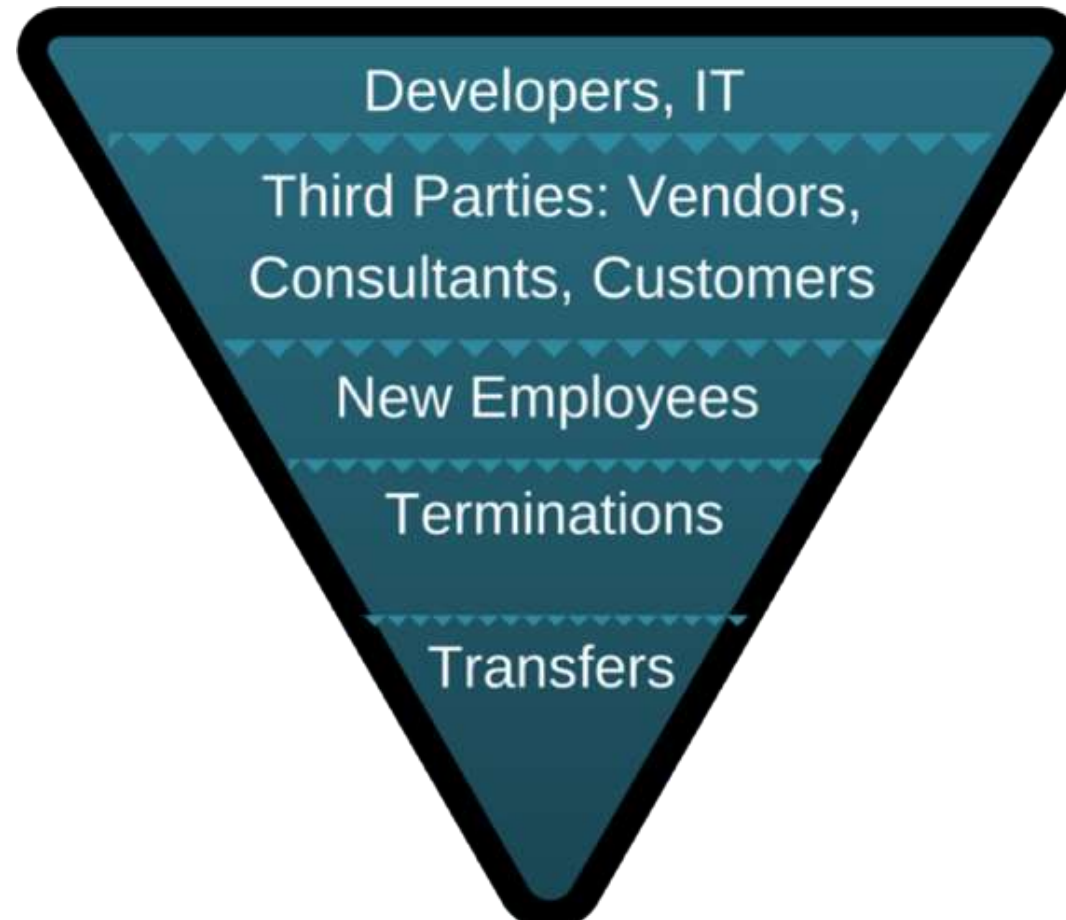
Optimum Performance

Integrity

Flexibility

Scalability

Review Risk – Who Needs Access?



Least Privilege

Planning AppSec – 8 Essentials

1. Role Design

Take care with Seeded Content

2. Base on Processes

Reduce Security Management

4. Data Roles

Business Units, Countries, Divisions

5. Segregation of Duties

Reduce likelihood of Fraud

6. Continuous Monitoring

Second line of Defense

7. Processes - Provisioning & Role Maintenance

IT General Controls

8. Periodic Review

Involve the Business

9. Automate your Audit

Have to know your starting point



Contents

Introduction & Objectives
The Business Issues
IT & Audit – Working Together
Application Security Controls
Configuration Management
Auditing your ERP
Efficiencies
Summary

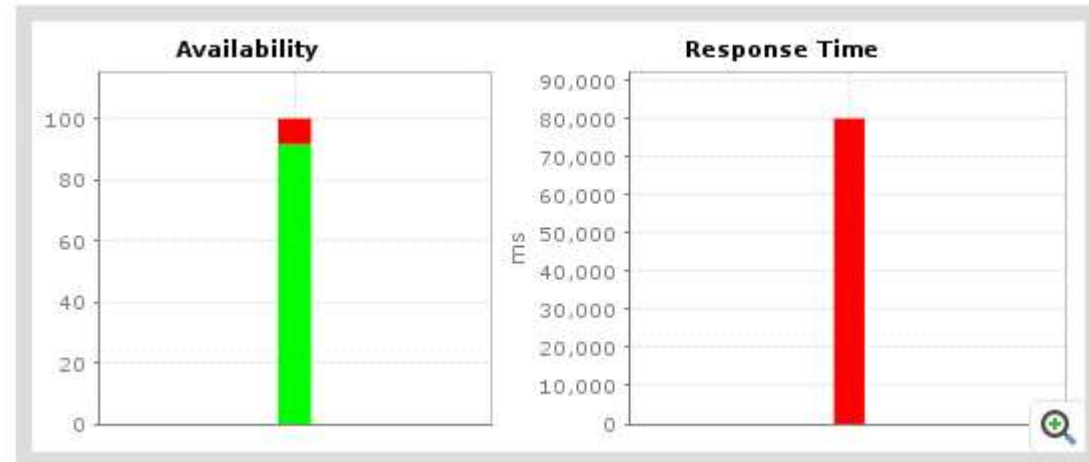
ERP Configuration Management

Monitor

- Security
- Application
- Database

Maintain

- Patching
- Upgrades



Common Application Control Activities - Examples

Determining whether sales orders are processed within the parameters of customer credit limits

Making sure goods and services are only procured with an approved purchase order

Monitoring segregation of duties based on defined job responsibilities

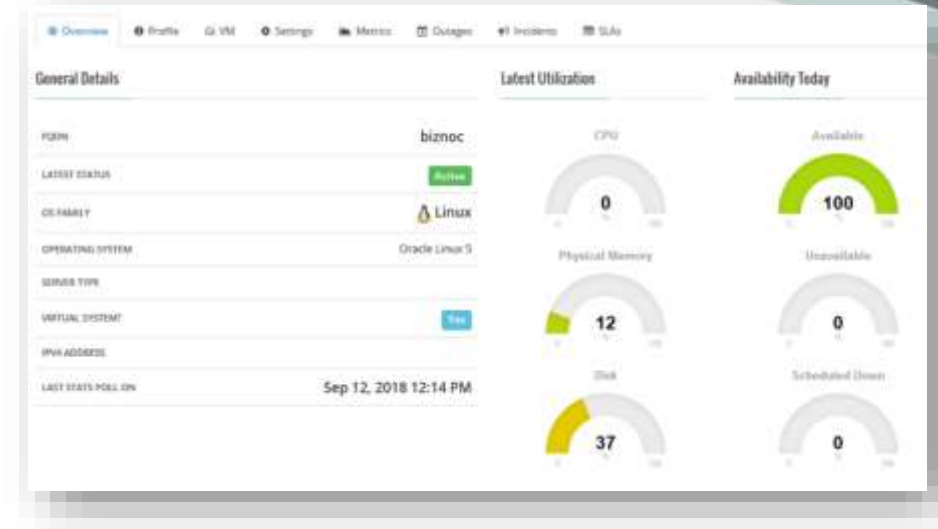
ERP Configuration Management

Authorize & Test

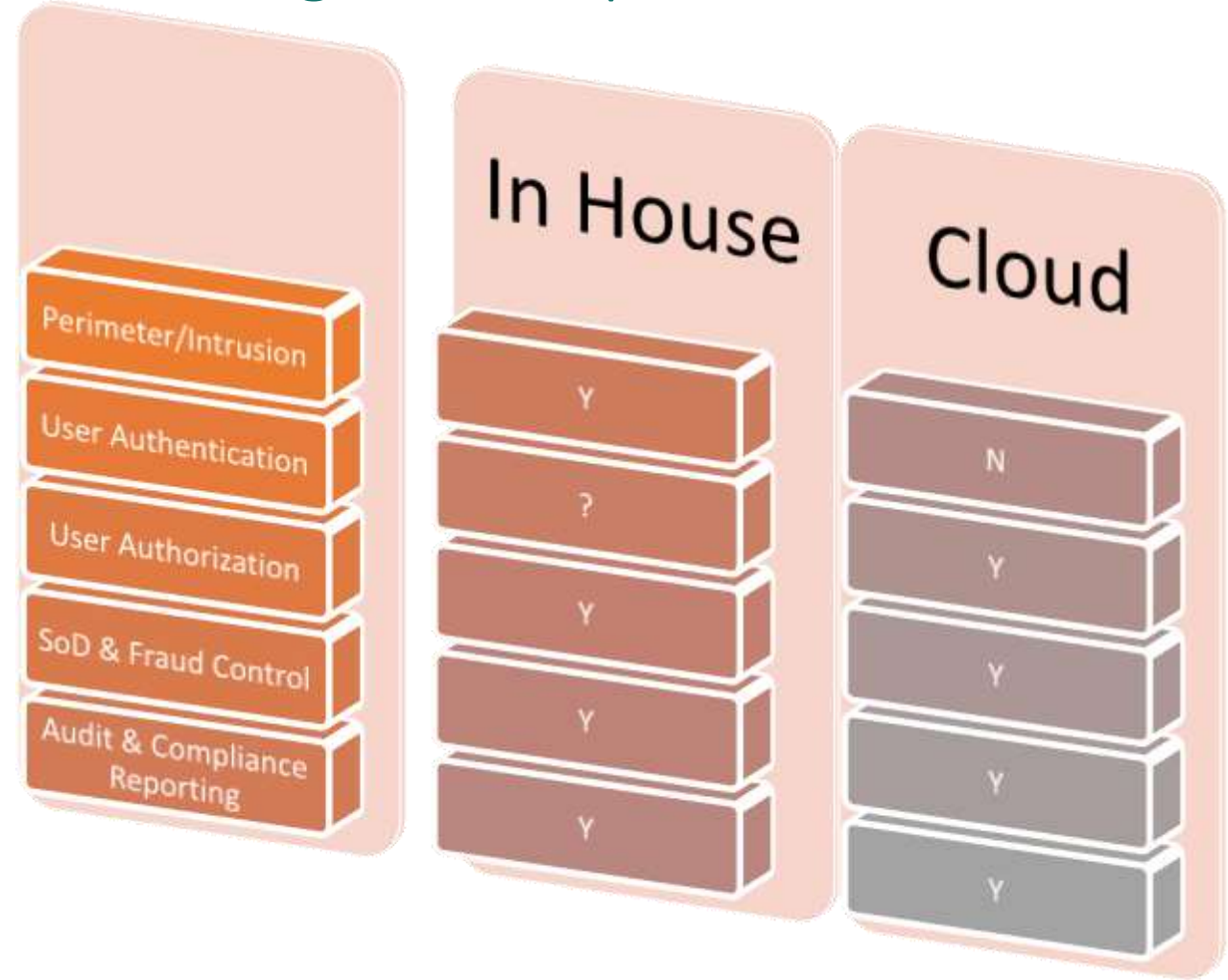
- Upgrades & Fixes
- Configuration of Processes

Database Access

- Direct SQL Access



The Responsibility for Risk gets Complicated



Contents

Introduction & Objectives
The Business Issues
IT & Audit – Working Together
Application Security Controls
Configuration Management
Auditing your ERP
Efficiencies
Summary

Auditing – what do we Need?

Audit Tool – Immediate & EASY!

Not driven by IT

Reporting – Standard & Enquiry

Access Controls

Segregation of Duties

Mitigation

Provisioning & Approvals



Contents of Reports



1

Audience

2

Terminology

3

Detail



Goal of Reports



“illustrate where the organization does not conform to a standard, rule, regulation or objective”



“the report must contain enough information so that the receivers of the audit report can change it”

Critical Audit Reports

Summary Report

Indicates if a violation exists on your ERP System for each rule statement

Detailed Violation Report

Breakdown of how each user violates the rule statement

Detailed Rule Report

Specifies the configuration of the rule statements

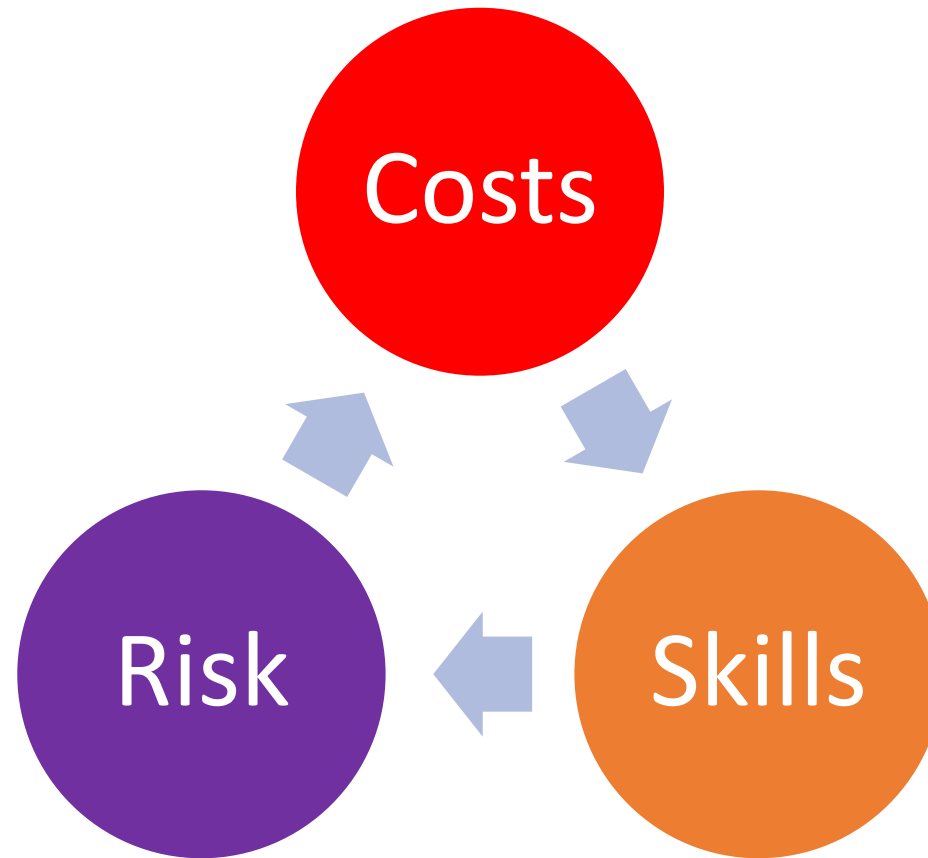
Mitigation Report

Listing of users in violation that have noted exceptions to specific rule statements

Contents

Introduction & Objectives
The Business Issues
IT & Audit – Working Together
Application Security Controls
Configuration Management
Auditing your ERP
Efficiencies
Summary

The Efficiency Conundrum



Visibility

Where are my SoD issues?

Who Owns that Issue?

What is the Business Risk?

How do I fix it?

Mitigation?

Who can Access this Critical Object, Master Data?

Periodic Access Review

Preventative vs. Detective Controls



Preventative Controls

Prevent an error from occurring within the application



Detective Controls

Detect errors based on predefined program logic

Unauthorized changes to Master Data

- Address Book and/or Vendor Bank Account details could be symptomatic of "Dummy Company" fraud
- A large increase in a Vendor Credit Limit may indicate procurement fraud
- A high percentage rise in an employee's salary may be suspicious and need investigating

Automation (AI)

- Saves time
- Checks quality
- Re-usable
- Improves accuracy



Metrics – Immediate Measures of Quality



Continuous Monitoring (catch the thieves)
Privileged User Tracking
Cloud Audit Tools – make Internal Audit Independent
Autonomous Security

Contents

Introduction & Objectives
The Business Issues
IT & Audit – Working Together
Application Security Controls
Configuration Management
Auditing your ERP
Efficiencies
Summary

Work with IT & the Business

- 🔗 Communication & Education
- 🔗 What are the Benefits to them?
- 🔗 Define Risks
- 🔗 Establish Internal Controls
- 🔗 Use External Tools



10 Best Practice Tips for ERP Security

1. Evaluate the Risks
2. Encryption & Authentication
3. Know your Business Processes
4. Audit Live Security
5. Plan your Roles - Authorization
6. A Risk Matrix (yours not someone else's)
7. Build IT General Controls
8. Use Easy Tools
9. Periodic Review – Involve the Business
10. Least Privilege



Questions

