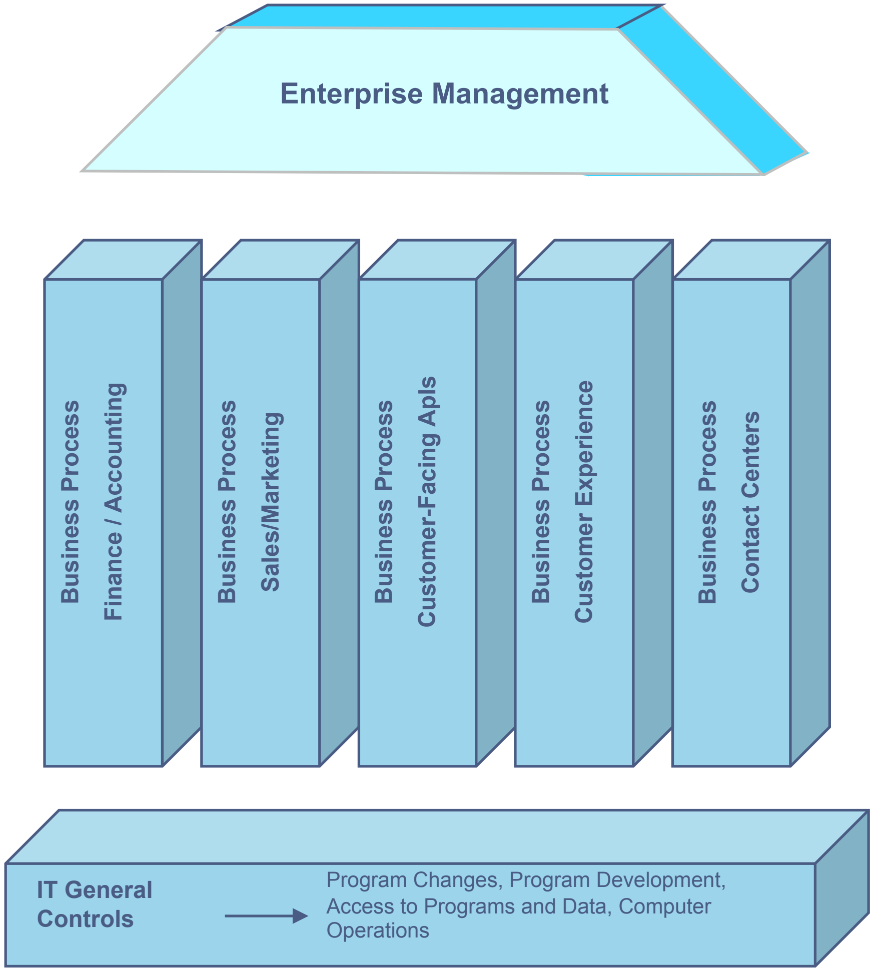
Fraud and Role of Information Technology

September 2008

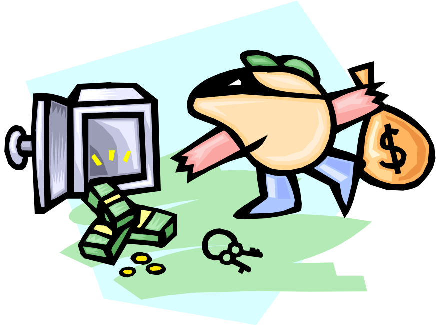
Agenda

- IT Value Proposition

Prior Interpretations of Internal Control Structure Have Addressed Three Separate Parts Which Were Audited Somewhat Independently. But This Is No Longer Possible – Technology Has Changed Our World


Enterprise Management
Business Process Finance / Accounting
Business Process Sales/Marketing
Business Process Customer-Facing Apls
Business Process Customer Experience
Business Process Contact Centers
IT General Controls
Program Changes, Program Development, Access to Programs and Data, Computer Operations

While Audit Approaches Toward Fraud Have Changed, So Have the Tools and Approaches Taken By Today's Fraudster



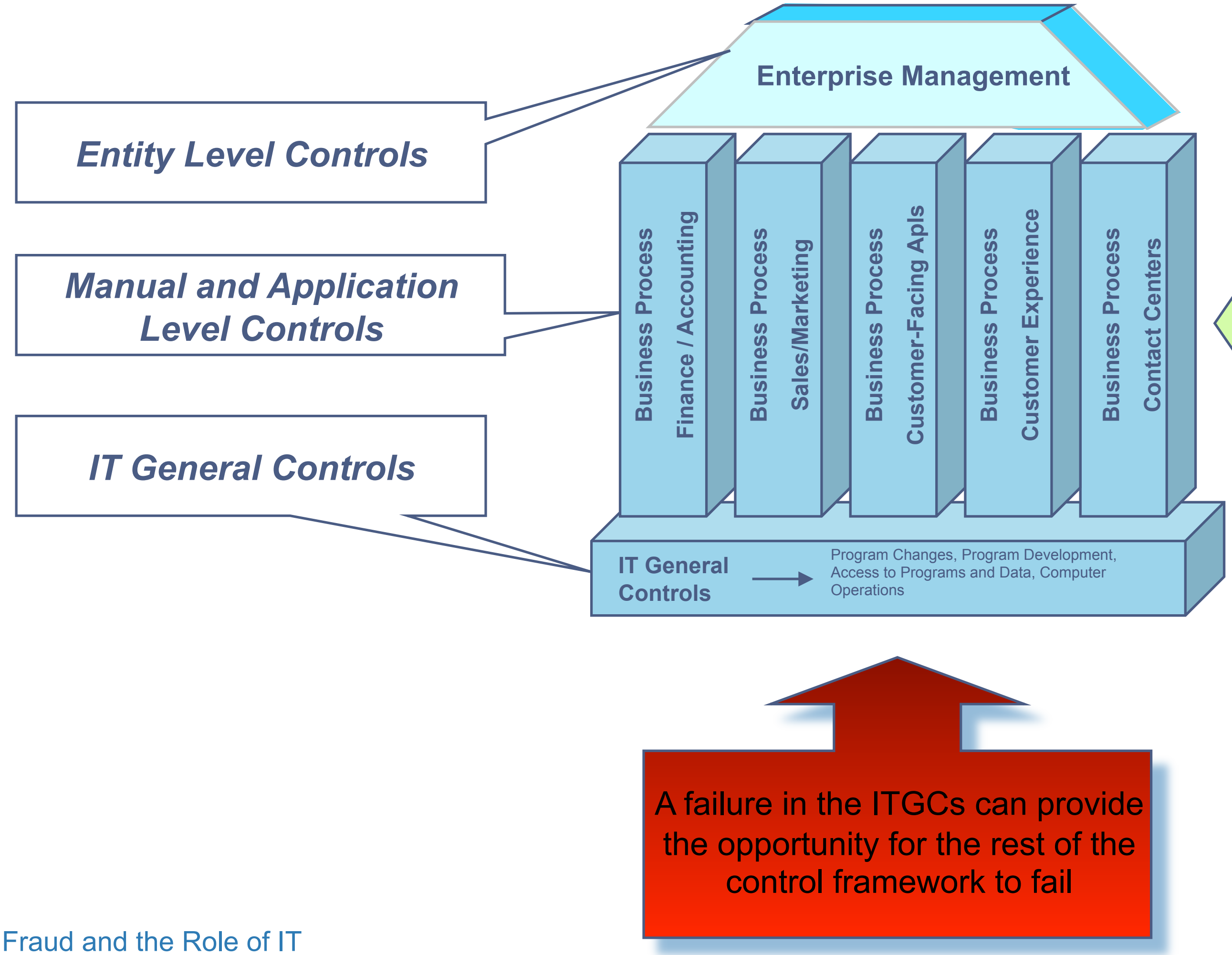
Fraud is now committed using

As Companies Implement New Manual Fraud Controls, Our Fraudster Has Also Used Automated Means To Override Them. We Have To Both Validate That Current **Key** Controls Work and Think Of **New Ways** These Perpetrators May Challenge Them in the Future

Failed ITGCs can Adversely Impact our Integrated Audit

Types of Controls

General Business Activities



Enterprise Management

Entity Level Controls

Manual and Application Level Controls

IT General Controls

Business Process Finance / Accounting

Business Process Sales/Marketing

Business Process Customer-Facing Apls

Business Process Customer Experience

Business Process Contact Centers

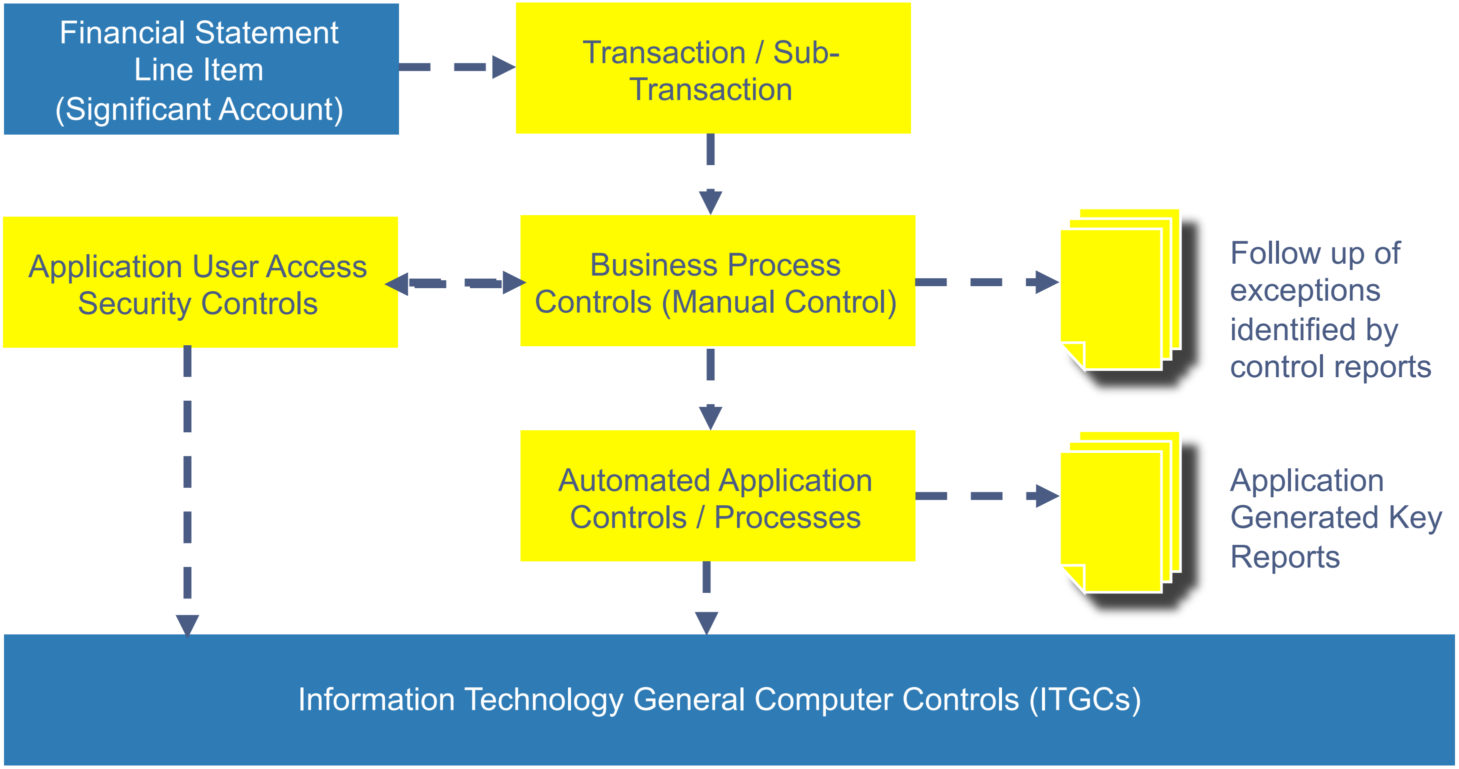
IT General Controls → Program Changes, Program Development, Access to Programs and Data, Computer Operations

A failure in the ITGCs can provide the opportunity for the rest of the control framework to fail

AS5's Focus Includes:

- Identifying risks and controls related to financial reporting.
- Understanding and leveraging company level controls and their relationship to financial statement assertions.
- Understanding the role of relevant information technology general controls for both automated and IT dependent controls and processes.
- Evaluating, validating and documenting our conclusion on the operating effectiveness of the key controls

Along with ITGCs, Addressing Fraud in the Integrated Audit Includes Evaluating Key Application Controls and Application User Access Security Controls and Their Role in the Key Business Process Controls



Financial Statement Line Item (Significant Account)

Transaction / Sub-Transaction

Application User Access Security Controls

Business Process Controls (Manual Control)

Follow up of exceptions identified by control reports

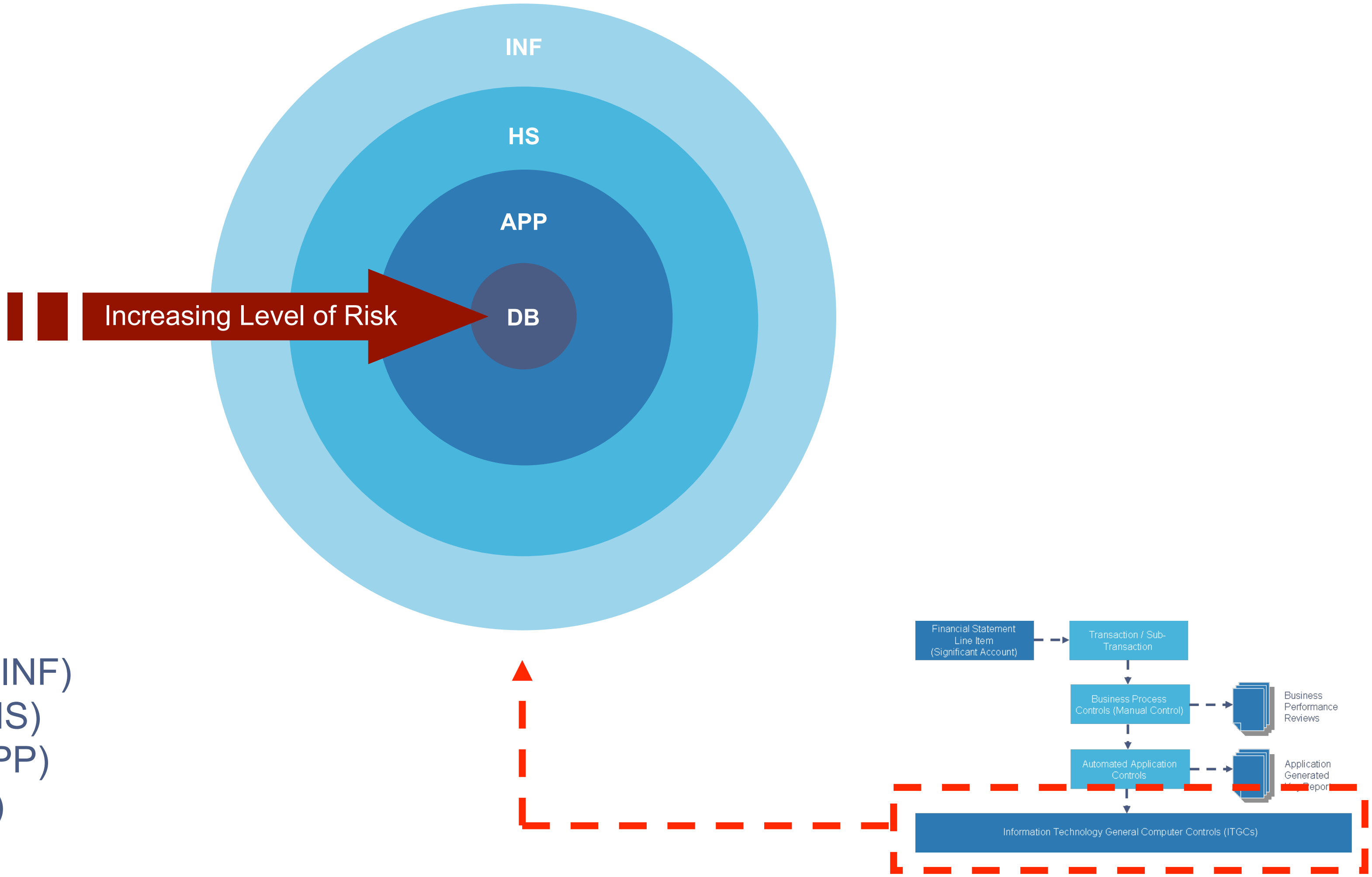
Automated Application Controls / Processes

Application Generated Key Reports

Information Technology General Computer Controls (ITGCs)

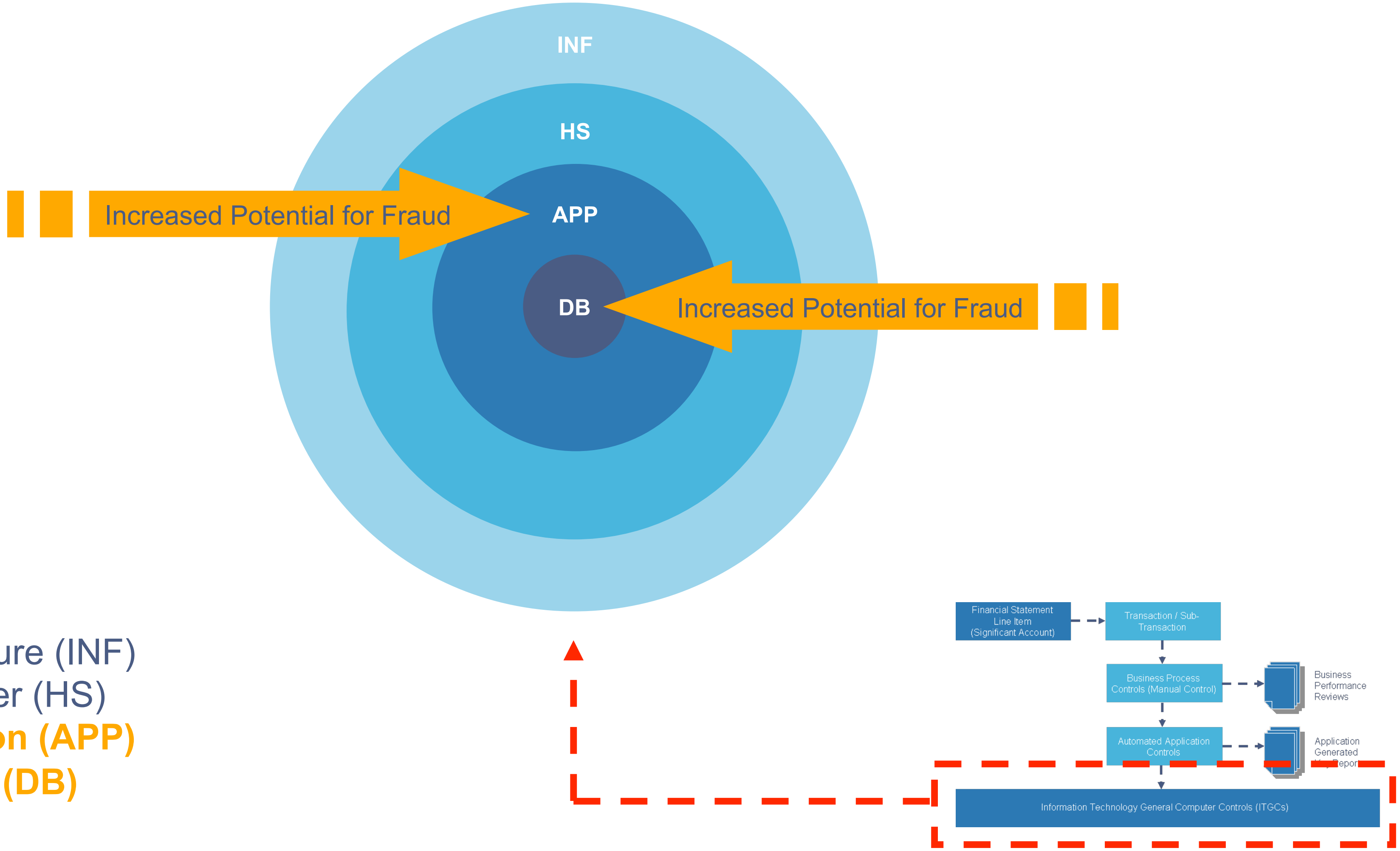
Each of the Areas in Yellow Offer the Potential Fraudster Opportunities to Commit Fraud. Deficiencies in These Areas Can Impact Our Substantive Testing Plan and our Fraud Procedures Including Journal Entry Testing

Layers of ITGCs and their relative risk


INF
HS
APP
DB
Increasing Level of Risk
Financial Statement Line Item (Significant Account)
Transaction / Sub-Transaction
Business Process Controls (Manual Control)
Business Performance Reviews
Automated Application Controls
Application Generated Key Report
Information Technology General Computer Controls (ITGCs)

Infrastructure (INF)
Host Server (HS)
Application (APP)
Database (DB)

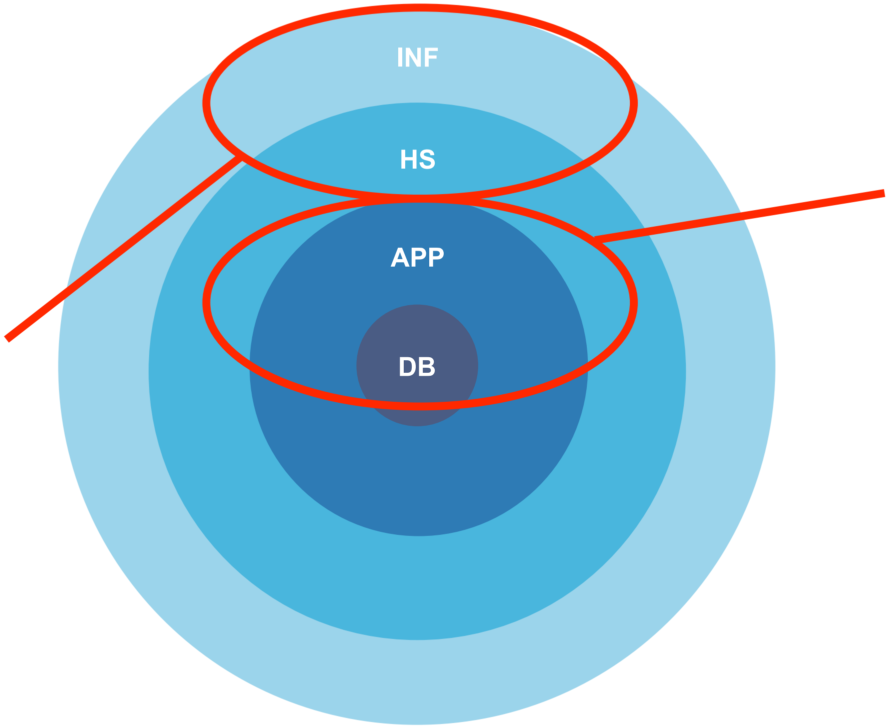
Layers within ITGCs Which may be Prone to Higher Fraud Risks


INF
HS
APP
DB
Increased Potential for Fraud
Increased Potential for Fraud
Financial Statement Line Item (Significant Account)
Transaction / Sub-Transaction
Business Process Controls (Manual Control)
Business Performance Reviews
Automated Application Controls
Application Generated Key Reports
Information Technology General Computer Controls (ITGCs)

Infrastructure (INF)
Host Server (HS)
Application (APP)
Database (DB)

IT and Business Process Redundant and Compensating Controls

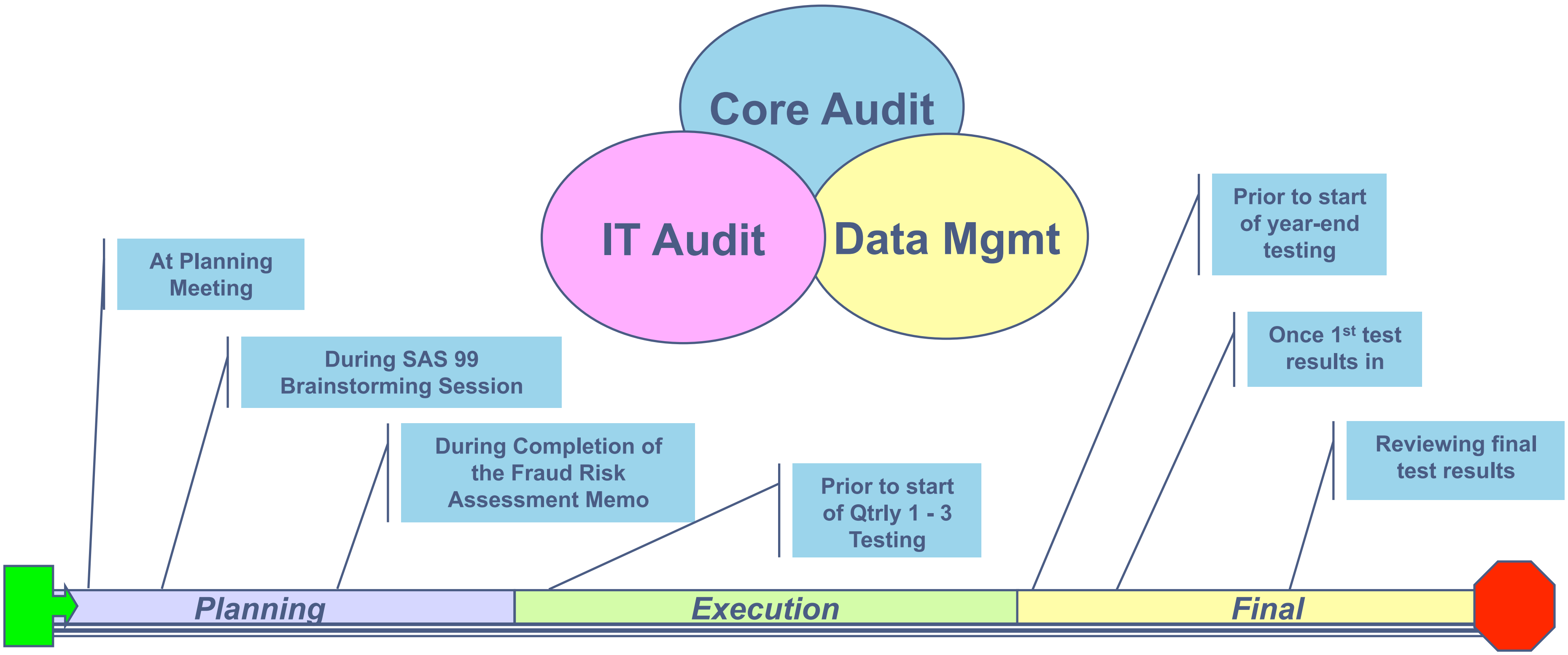
Some relative considerations on the risk and potential mitigation of IT General Controls issues



Some deficiencies in these areas would not have a direct impact on data or a financial statement assertions and may be mitigated by other IT General Controls at the Application and Database layer

Some deficiencies in these areas may be determined to have a direct impact on data or a financial statement assertion and need to be evaluated in the context of the business process redundant and compensating controls

Effective Auditing in a Complex IT Environment Requires Effective Coordination Among All Specialist Groups


Core Audit
IT Audit
Data Mgmt
At Planning Meeting
During SAS 99 Brainstorming Session
During Completion of the Fraud Risk Assessment Memo
Prior to start of Qtrly 1 - 3 Testing
Prior to start of year-end testing
Once 1st test results in
Reviewing final test results
Planning
Execution
Final

Typical Audit Process Timeline

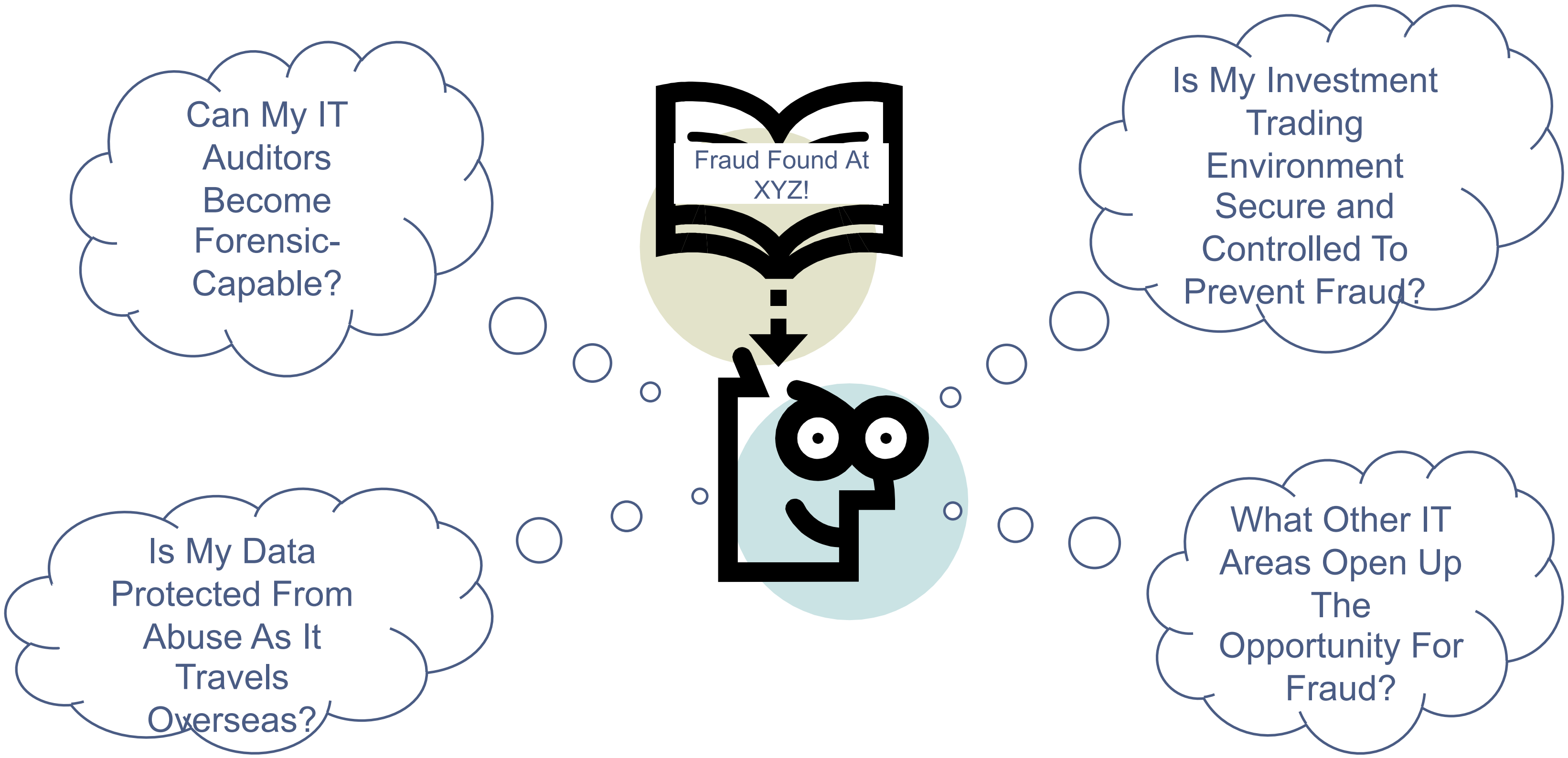
Meeting the Requirements of SEC and PCAOB Regulations (SAS 99, AS5) Efficiently and Effectively Makes Close Coordination Important

Value Drivers for IT Audit Coordinated Involvement In the Integrated Audit

IT Audit's involvement can serve to expand and strengthen the audit team's understanding of the overall business processes and controls as well as the integration of financial processes with systems.

- We can help determine whether Fraud Risks are completely identified, presented to the Audit Team to be addressed in a coordinated manner and tested in an efficient, effective manner.
- We can address the concerns noted in the PCAOB 4010 report regarding fraud detection and how it can be applied to engagements.
- With IT Audit's coordinated involvement, we can identify and respond with integrated audit procedures to unique areas of fraud risk in systems and business processes.
- Many IT Audit professionals have industry specific business process skills that can be deployed on engagements to drive an integrated effort and improve audit quality.
- Including IT Audit's understanding of the application systems architecture when developing SAS 99 testing, we can facilitate focused testing based upon risk.

Along with Enhanced Delivery in the Integrated Audit Environment, Numerous Other Areas Exist to Add Value



Can My IT Auditors Become Forensic-Capable?

Fraud Found At XYZ!

Is My Investment Trading Environment Secure and Controlled To Prevent Fraud?

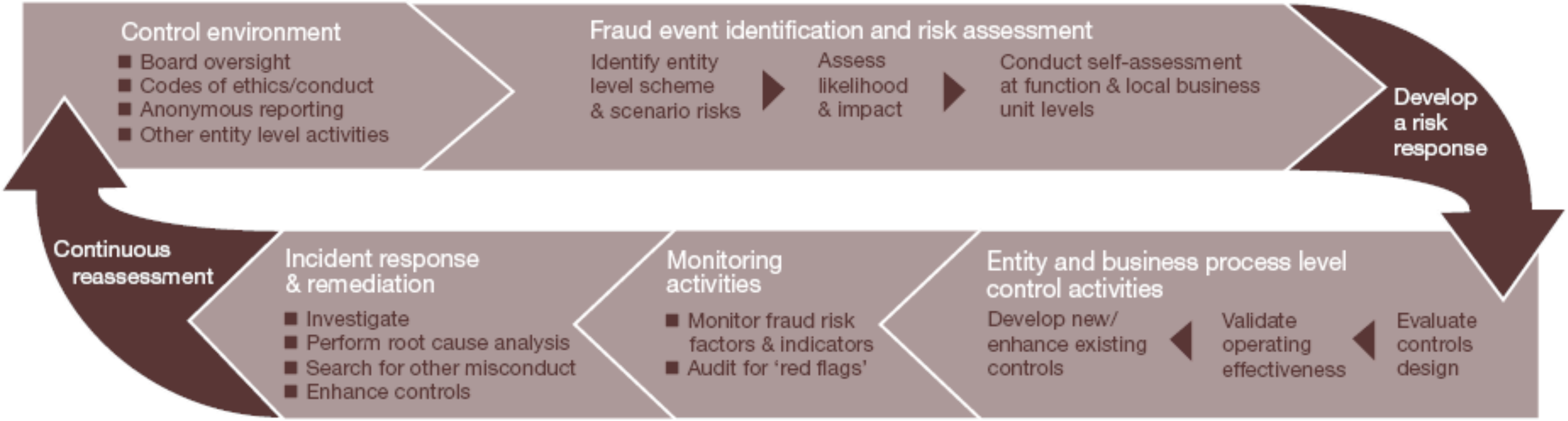
Is My Data Protected From Abuse As It Travels Overseas?

What Other IT Areas Open Up The Opportunity For Fraud?

We Only Have to Think of the Challenges Faced In Meeting Other Regulatory Requirements

Making The Vision A Reality

Overall Anti-Fraud Framework



Control environment
- Board oversight
- Codes of ethics/conduct
- Anonymous reporting
- Other entity level activities

Fraud event identification and risk assessment

Identify entity level scheme & scenario risks ▶ Assess likelihood & impact ▶ Conduct self-assessment at function & local business unit levels

Develop a risk response

Entity and business process level control activities

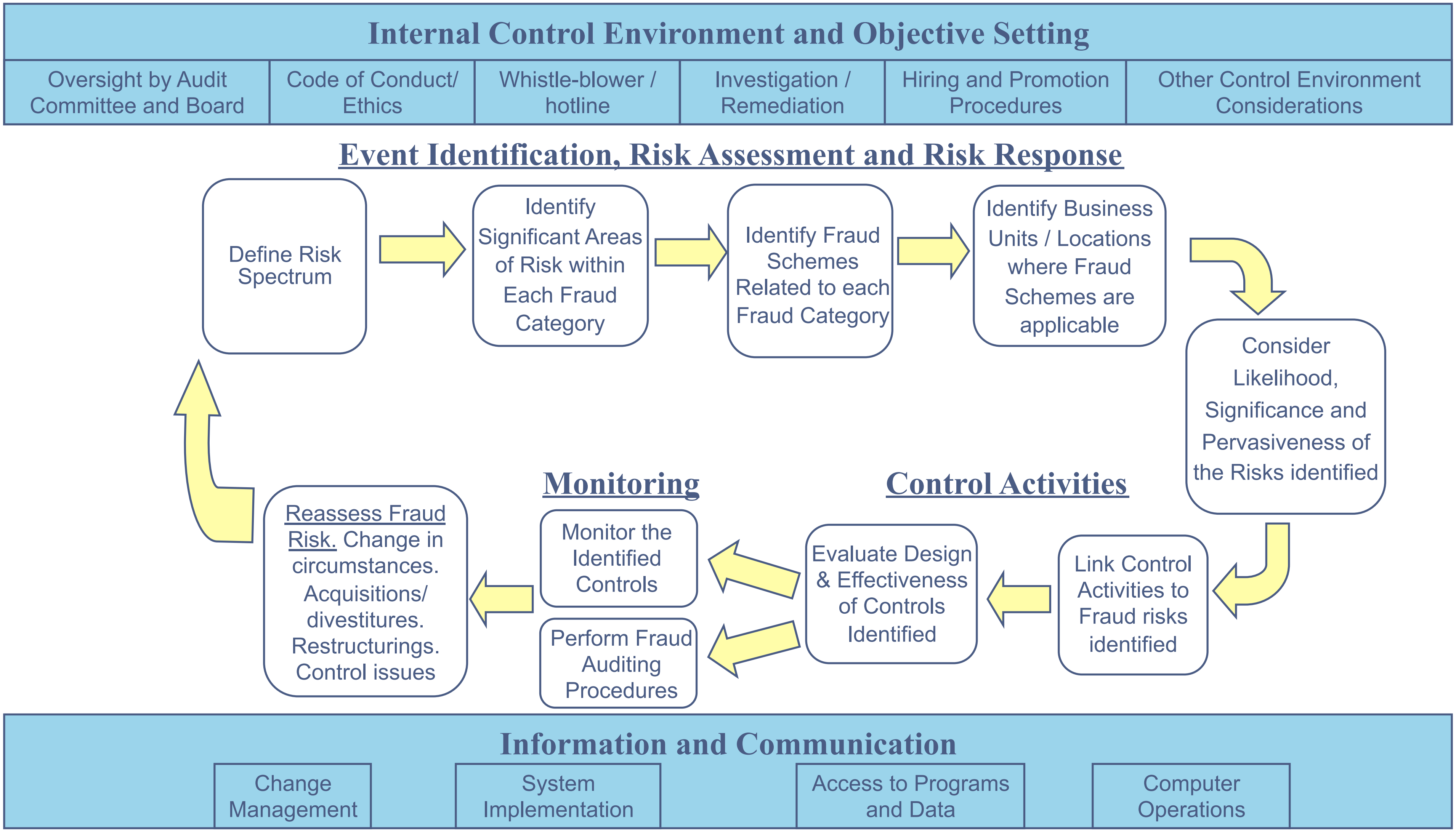
Evaluate controls design ◀ Validate operating effectiveness ◀ Develop new/ enhance existing controls

Monitoring activities
- Monitor fraud risk factors & indicators
- Audit for 'red flags'

Incident response & remediation
- Investigate
- Perform root cause analysis
- Search for other misconduct
- Enhance controls

Continuous reassessment

Developing a Fraud Risk Response



Internal Control Environment and Objective Setting

Oversight by Audit Committee and Board	Code of Conduct/ Ethics	Whistle-blower / hotline	Investigation / Remediation	Hiring and Promotion Procedures	Other Control Environment Considerations

Event Identification, Risk Assessment and Risk Response

Define Risk Spectrum

Identify Significant Areas of Risk within Each Fraud Category

Identify Fraud Schemes Related to each Fraud Category

Identify Business Units / Locations where Fraud Schemes are applicable

Consider Likelihood, Significance and Pervasiveness of the Risks identified

Control Activities

Link Control Activities to Fraud risks identified

Evaluate Design & Effectiveness of Controls Identified

Monitoring

Monitor the Identified Controls

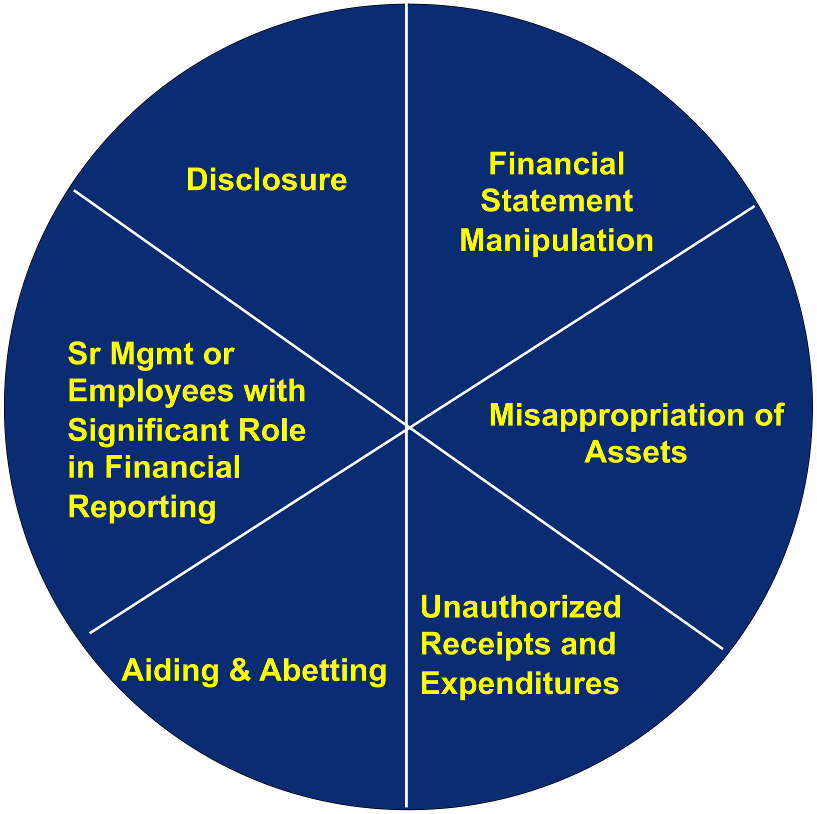
Perform Fraud Auditing Procedures

Reassess Fraud Risk. Change in circumstances. Acquisitions/ divestitures. Restructurings. Control issues

Information and Communication

Change Management	System Implementation	Access to Programs and Data	Computer Operations

Fraud Schemes and Audit Risk Response


Disclosure
Financial Statement Manipulation
Misappropriation of Assets
Unauthorized Receipts and Expenditures
Aiding & Abetting
Sr Mgmt or Employees with Significant Role in Financial Reporting

Financial Statement Audit

- Procedures designed to provide reasonable assurance that financial statements free of material misstatements due to fraudulent financial reporting or misappropriation of assets
- Does not extend to other categories of fraud or misconduct
- Limited to fraud risks, having potential material financial statement impact

Internal Controls Audit

- Management must develop pervasive and specific programs and control activities to prevent and timely detect
- Auditor evaluates design and validates effectiveness of management’s antifraud programs and controls
- Limited to fraud and misconduct risks, having potential material financial statement impact

Evaluating Antifraud Programs and Controls

Control / Internal Environment

- Tone at top
- Code of conduct/ethics
- Ethics hotline
- Hiring and promotion
- Oversight committee
- Investigative process
- Remediation

Fraud Risk Assessment

- Systematic process
- Level within agency
- Likelihood and significance

Control Activities

- Linking controls to identified fraud risks

Information / Communication

- Information systems & technology
- Knowledge management
- Training

Monitoring

- Ongoing monitoring by management
- Separate "after the fact" evaluations by internal audit

Evaluating Antifraud Programs and Controls

Internal Environment

Tone at Top

Codes of Conduct / Ethics

- Should apply to all accounting and financial oversight personnel
- Must be communicated effectively

Anonymous Reporting

- Audit committee oversight and independent of management

Hiring and Promotion Procedures

- Background investigations for persons of trust
- Also consider process for agents, vendors, etc.

Audit Committee Oversight

- Passive not adequate
- Active discussion of fraud

Investigation / Remediation

- Standard investigative process
- Adequate remediation to prevent recurrence

Evaluating Antifraud Programs and Controls

Assessing Fraud Risks

Systematic Rather Than Haphazard or Informal

Address All Categories of Fraud

- Misappropriation of assets
- Financial statement manipulation
- Unauthorized receipts and expenditures
- Fraud by senior management
- Aiding and abetting
- Disclosure fraud

Business Unit and Significant Account

Likelihood and Significance

- "More than remote"
- "More than inconsequential" financial statement impact

Evaluating Antifraud Programs and Controls

Linking Control Activities

Management Should Identify Processes, Controls, and Other Procedures That Are Needed to Mitigate Identified Risks

- Very broad, e.g., approvals, authorizations, verifications, reconciliations, segregation of duties, reviews of operating performance, background investigations, physical security

Should Occur Throughout Organization, at All Levels and in All Functions

Evaluating Antifraud Programs and Controls

Information Communication

Information Systems & Technology Controls

- Technology enabled fraud , e.g., holding books open
- Prevention and detection of unauthorized access
- Inappropriate modification of computer programs
- System override
- Ability to investigate computer misuse

Knowledge Management

- Identified fraud risks
- Strengths and weaknesses of antifraud control activities
- Suspicions and allegations about fraud; and
- Remediation efforts

Training

- Frequency
- Scope and sufficiency

Evaluating Antifraud Programs and Controls

Fraud Monitoring and Auditing

Management: On-going, Day to Day Monitoring

- **Embedded into normal operating activities**
- **Includes regular management and supervisory activities**
- **Should leverage available information technology**

Internal Audit: After The Fact Evaluation

- **Contingent upon risk and effectiveness of ongoing monitoring**
- **Address fraud risk in planning and executing internal audit cycle**
- **IA includes experienced fraud risk professionals**
- **Fraud auditing ≠ forensic investigation**
- **Fire safety experts vs. “Fire-fighters”**

Forensic Investigation

- **Detailed review of the event**
- **Leverage the information technology based audit trails**
- **Facilitating the root cause identification**

The Role of Information Technology

The Role of Information Technology

Planning

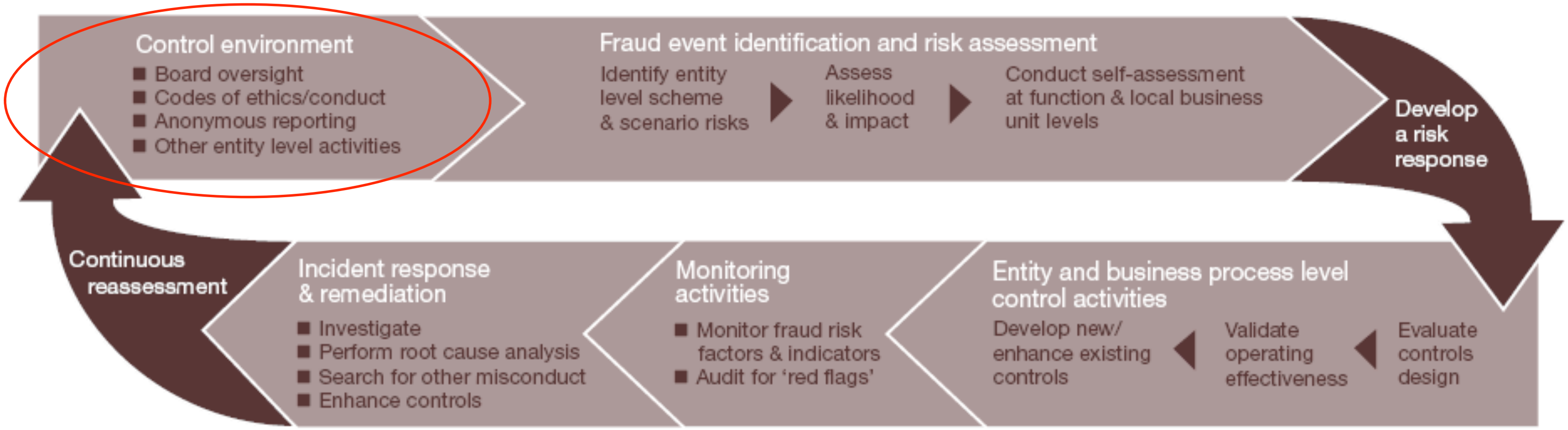
- **Participating in the Fraud Risk assessment and brainstorming processes**
- **Identifying IT specific risks and relevant IT control activities**
- **Understanding the business process control reliance on application systems and reports**
- **Understanding the thresholds that business process controls operate and where they are fallible**
- **Understanding areas of potential override inside or outside of the application systems**

Execution

- **Including key IT organizational personnel in fraud inquiries**
- **Directing testing efforts leveraging an understanding of the information system's interconnectivity and operation**
- **Assessing IT control activities**
- **Suggesting improvements in IT control activities and information retention requirements**

Guiding Principle is Integration and Alignment

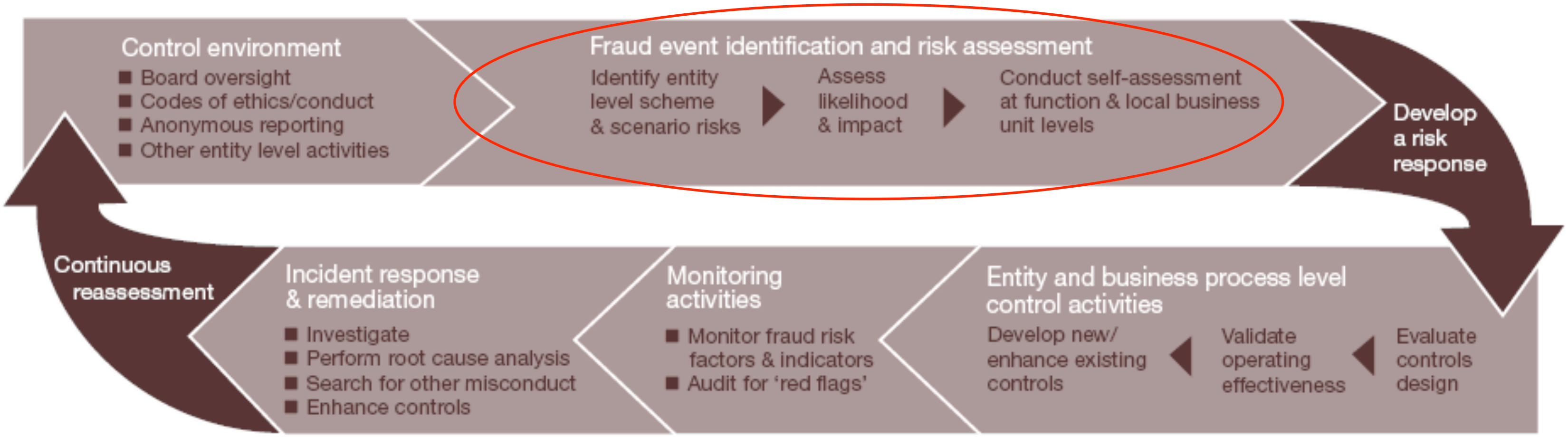
Anti-Fraud Framework – The Role of IT


Control environment
■ Board oversight
■ Codes of ethics/conduct
■ Anonymous reporting
■ Other entity level activities
Fraud event identification and risk assessment
Identify entity level scheme & scenario risks
Assess likelihood & impact
Conduct self-assessment at function & local business unit levels
Develop a risk response
Entity and business process level control activities
Evaluate controls design
Validate operating effectiveness
Develop new/ enhance existing controls
Monitoring activities
■ Monitor fraud risk factors & indicators
■ Audit for 'red flags'
Incident response & remediation
■ Investigate
■ Perform root cause analysis
■ Search for other misconduct
■ Enhance controls
Continuous reassessment

IT Control Environment

- ***Organization monitoring against objectives***
- ***IT personnel understand their responsibility to internal control***
- ***Reporting of significant IT events and failures to senior management***
- ***Promotion of the company culture of integrity***

Anti-Fraud Framework – The Role of IT


Control environment
■ Board oversight
■ Codes of ethics/conduct
■ Anonymous reporting
■ Other entity level activities
Fraud event identification and risk assessment
Identify entity level scheme & scenario risks
Assess likelihood & impact
Conduct self-assessment at function & local business unit levels
Develop a risk response
Entity and business process level control activities
Evaluate controls design
Validate operating effectiveness
Develop new/ enhance existing controls
Monitoring activities
■ Monitor fraud risk factors & indicators
■ Audit for 'red flags'
Incident response & remediation
■ Investigate
■ Perform root cause analysis
■ Search for other misconduct
■ Enhance controls
Continuous reassessment

Fraud Event Identification and IT Risk Assessment:

- ***Participate and Complete Fraud Risk Assessment***
  - ***Identify potential scenarios integrating the IT point of view***
  - ***Determine IT integration points and risk areas***
    - ***Directing the scope of manual efforts (e.g. SAS99 Journal Entry testing)***
    - ***Confirming the reliance on key IT systems***

Facilitating Brainstorming

Professional skepticism and a consideration of fraud possible in every process. Critical evaluation is necessary.

Considerations:

- Prior years experience
- General risk profile
- Industry / Geographic issues
- Incentives (not just formal compensation plans)
- Pressures
- Prior year deficiencies
- Previously reported misconduct

Risks identified during Sarbanes testing of controls

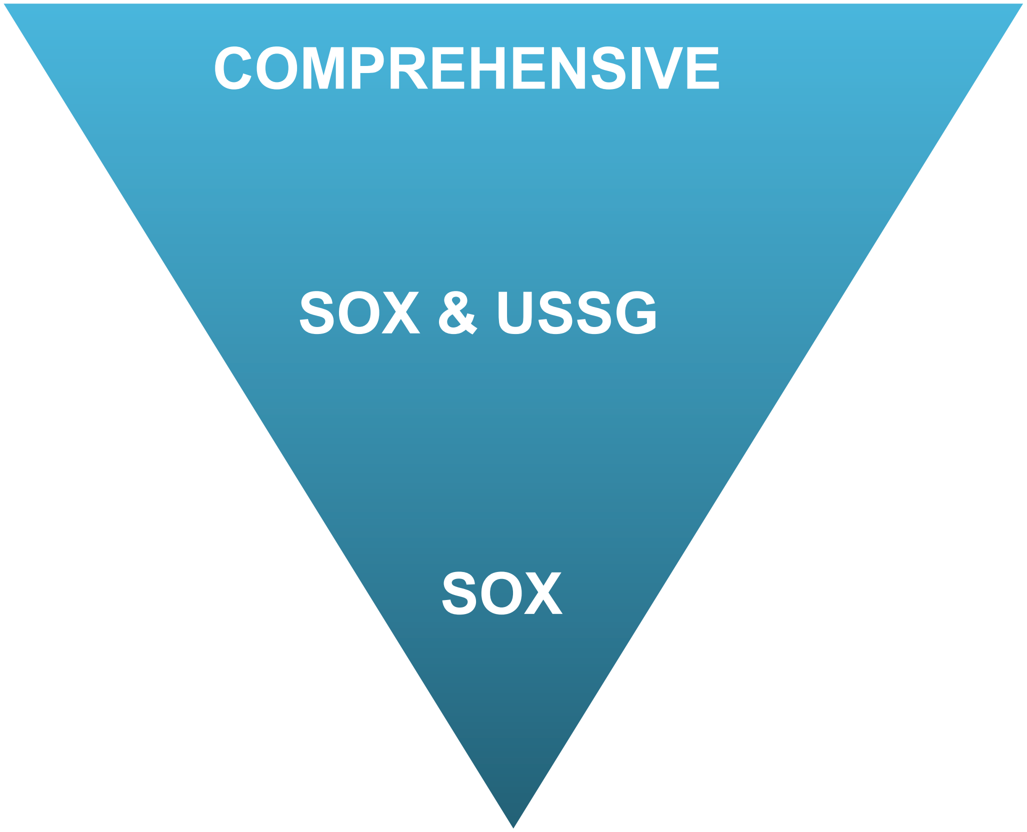
Internal Audit / Management Assessment

No Consideration of Controls During Brainstorming

<u>Include knowledgeable representative from audit specialist groups – particularly IT</u>

Fraud Schemes and the Role of IT

Brainstorming Process



COMPREHENSIVE

SOX & USSG

SOX

Comprehensive

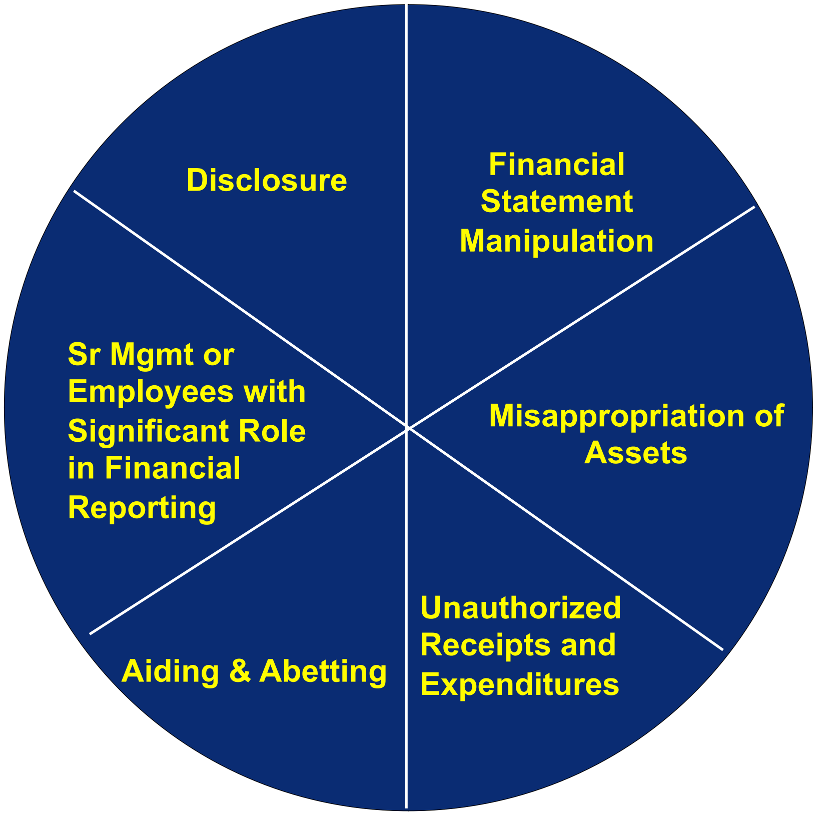
Financial Reporting & Criminal Conduct

Financial Reporting

(Minimum for SEC Registrants)

Fraud Schemes and the Role of IT

Brainstorming Process


Disclosure
Financial Statement Manipulation
Sr Mgmt or Employees with Significant Role in Financial Reporting
Misappropriation of Assets
Aiding & Abetting
Unauthorized Receipts and Expenditures

- **Implications of Fraud & Misconduct**
  - Reputation Risk
  - Operational Risk
  - Legal/Compliance Risk
  - Financial & Non-Financial Reporting
- **Motivations to Commit Fraud**
  - Incentives
  - Pressures
- **Financial Statement Manipulation**
  - Improper revenue recognition
  - Asset overstatement/Liability understatement
  - Significant management estimates
  - Inter-company and suspense accounts
  - Significant & unusual transactions
- **Asset Misappropriation**
  - Cash
  - Payroll
  - Inventory
  - Fixed Assets
- **Other "Slices" of Fraud Pie….**

Fraud Schemes and the Role of IT

Brainstorming Process

Revenue Recognition Schemes

- Bill & hold transactions
- Trade loading / channel stuffing
- Customer side agreements
- Backdating sales agreements
- Over-accrual of vendor rebates

Overstatement of Assets Schemes

- Fraudulent inventory capitalization
- Overstatement of inventory counts
- Overstatement of trade receivables
- Improper slotting fee capitalization

Misappropriation of Assets Schemes

- Cash skimming
- Inventory theft
- Sales & marketing fraud
- Outsourcing fraud

Unauthorized Receipts / Expenditures Schemes

- Improper vendor allowances
- Commercial bribery
- Justifications / rationalization

Fraud Schemes and the Role of IT

Brainstorming Process

Predicting the Unpredictable is Key

Think like the Devil when assessing fraud & misconduct risk!

How would the Devil manage your business unit?

What would happen if the Devil were a vendor or customer?

What if the Devil was an employee?

Fraud Schemes and the Role of IT

Brainstorming Process

Incentives / Pressures:

- ***Financial management pressure on IT personnel***
- ***Malicious intent***

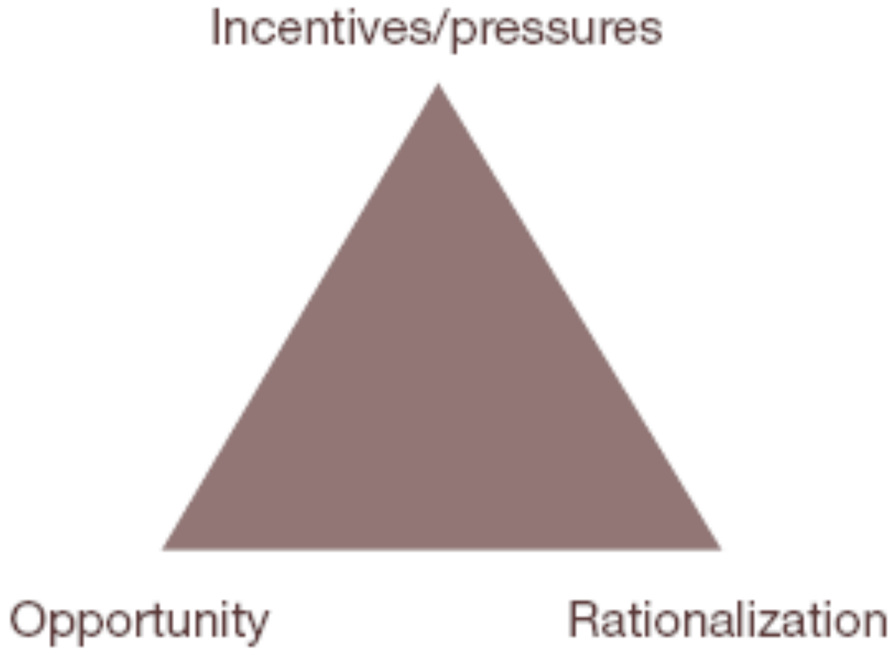
Opportunity:

- ***Super user / privileged access at the application level***
- ***Direct data access***
- ***Ability to obscure changes / logging within the system***

Rationalization:

- ***IT personnel misunderstanding the nature of changes requested***
- ***Accountability for transactions completed in the system***

Fraud triangle



Incentives/pressures

Opportunity

Rationalization

Fraud Schemes and the Role of IT

Develop a Response

Significance

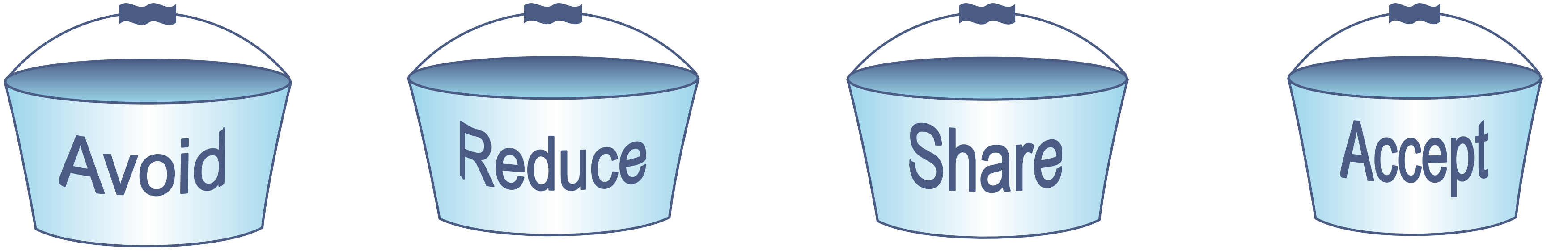
- Rankings:
  - Material (M)
  - Indirectly Material (IM)
  - More than Inconsequential (MI)
  - Inconsequential (I)
- Consider "reasonably possible" *quantitative* impact
- Consider "reasonably possible" *qualitative* impact
- Consider "reasonably possible” *indirect* impact

Inherent Likelihood

- Rankings:
  - Probable (P)
  - Reasonably Possible (RP)
  - Remote (R)
- Consider "incentives and pressures"

Fraud Schemes and the Role of IT

Develop a Response



Avoid	Reduce	Share	Accept
Exit activities giving rise to risk	*Reduce risk likelihood or impact, or both*	*Transfer or otherwise share risk*	*No action taken*

Fraud Schemes and the Role of IT

Develop a Response

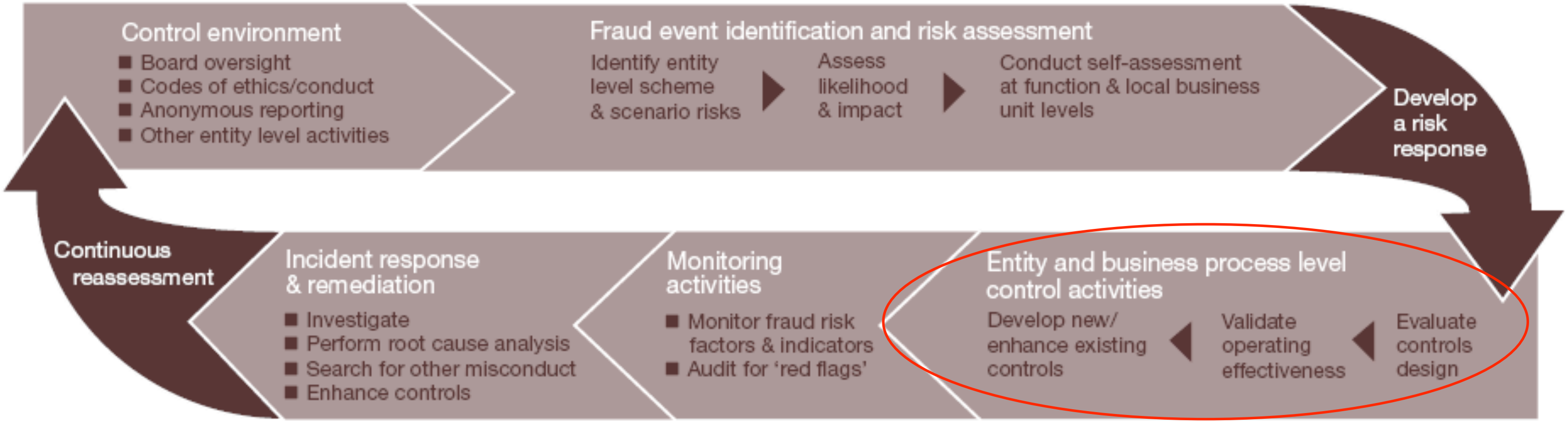
Potential Fraud & Misconduct Risk	Link & Evaluate Specific Control Activity	Periodic Fraud Auditing Detection Procedures
Red (high) (M/P, M/RP or MI/P)	Yes	Yes
Yellow (medium) (MI/RP or IM/P or RP)	Yes	Yes
Blue (guarded) (M/R)	Optional depending upon severity	Optional depending upon severity and quality of controls
Green (low) (IM/R)	No	No

Fraud Schemes and the Role of IT

Develop a Response

Financial Statement Impact	Reasonably Possible or Probable	Remote
Material * – Quantitatively > planning materiality or qualitatively material.	Red: Evaluate specific control activities and design fraud auditing procedures to attain medium to high level of assurance	Blue: Auditing standards do not require additional or specific fraud auditing detection procedures; recommended consideration of fraud auditing procedures given that the audit team assessed the risk as potentially material.
Indirectly Material – Indirect impact quantitatively or qualitatively material.	Orange: Evaluate specific control activities. If control activities are deficient consider fraud auditing procedures	Blue: Auditing standards do not require evaluation of controls or fraud auditing procedures; recommended consideration of fraud auditing procedures given that the audit team assessed the risk as potentially material.
More Than Inconsequential – Quantitatively < planning materiality but > SUD level or qualitatively more than inconsequential.	Yellow: Evaluate specific control activities. If control activities are deficient, consider need for substantive detection procedures.	Green: Auditing standards do not require additional or specific fraud auditing detection procedures. Review procedures if the engagement team expands beyond financial reporting risk.
Inconsequential – Quantitatively and qualitatively inconsequential.	Green: Auditing standards do not require additional or specific fraud auditing detection procedures.	Green: Auditing standards do not require additional or specific fraud auditing detection procedures.

Anti-Fraud Framework – The Role of IT


Control environment
Board oversight
Codes of ethics/conduct
Anonymous reporting
Other entity level activities
Fraud event identification and risk assessment
Identify entity level scheme & scenario risks
Assess likelihood & impact
Conduct self-assessment at function & local business unit levels
Develop a risk response
Entity and business process level control activities
Evaluate controls design
Validate operating effectiveness
Develop new/ enhance existing controls
Monitoring activities
Monitor fraud risk factors & indicators
Audit for 'red flags'
Incident response & remediation
Investigate
Perform root cause analysis
Search for other misconduct
Enhance controls
Continuous reassessment

IT Entity & Process Level Control Activities:

- ***Identify the IT and Business Process Controls***
- ***Validate control design***
- ***Develop the testing approach with regard to IT and Business Controls***
- ***Review systems changes on a pre-implementation basis***

Anti-Fraud Framework – The Role of IT

Leverage the Fraud Triangle

- Opportunity: Seal the gaps and cracks
- Incentives & pressures: Protect good people from committing bad acts
- Rationalization: What would their mothers say?

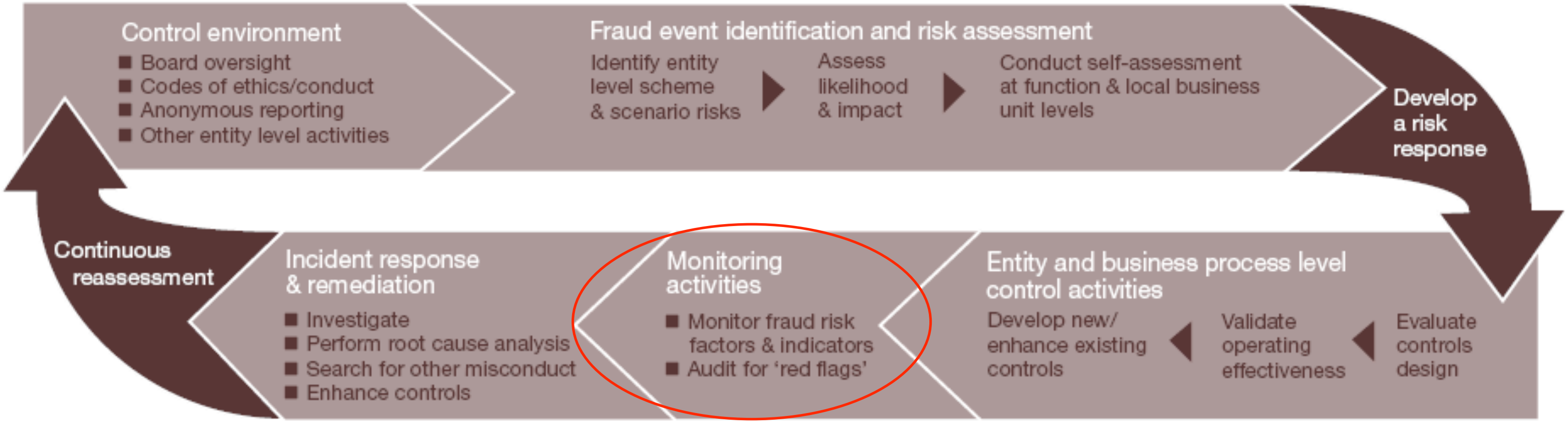
Evaluate design

- Address potential collusion and management override
- Consider practicality of segregation of duties

Validate operating effectiveness

- Test like any other control activity with observations, walkthroughs, interviews, document review and/or reperformance

Anti-Fraud Framework – The Role of IT


Control environment
Board oversight
Codes of ethics/conduct
Anonymous reporting
Other entity level activities
Fraud event identification and risk assessment
Identify entity level scheme & scenario risks
Assess likelihood & impact
Conduct self-assessment at function & local business unit levels
Develop a risk response
Entity and business process level control activities
Evaluate controls design
Validate operating effectiveness
Develop new/ enhance existing controls
Monitoring activities
Monitor fraud risk factors & indicators
Audit for 'red flags'
Incident response & remediation
Investigate
Perform root cause analysis
Search for other misconduct
Enhance controls
Continuous reassessment

IT Monitoring Activities

- ***Automated controls used to monitor real time***
- ***Direct Access to Data monitoring***
- ***Security compliance monitoring***
- ***Internal Audit functions***

Anti-Fraud Framework – The Role of IT

Fraud Risk Factors and Indicators

Fraud risk factors -- increased *likelihood* that fraud will be committed

- Analogy: dry and hot conditions increase the likelihood of fire

Fraud risk indicators -- indicia that fraud *might* have occurred or is occurring

- Analogy: smoke might indicate that there is a fire

Anti-Fraud Framework – The Role of IT

Fraud Risk Factors and Indicators

Example: Trade loading / channel stuffing

Fraud risk factors

- **Common/accepted industry practice that can be easily abused to manipulate sales revenues**
- **Company does not enforce standard policies and procedures for negotiating, approving, executing and documenting sales agreements**
- **Sales commission structure weighted heavily toward period-end revenue goals**

Fraud risk indicators

- **Large, numerous or unusual sales transactions occurring shortly before the end of the period**
- **Increase in volume of customer returns**
- **Significant increase or excess levels of inventory in the distribution channel**
- **Build up of aged accounts receivable balances**

Anti-Fraud Framework – The Role of IT

Fraud Auditing

Applies auditing techniques to search for fraud indicators

Techniques include:

- Inquiry & interview
- Analytics
- Targeted testing of transactions
- Electronic data fraud detection tools (CAATs)

Design “real time” detection / monitoring procedures

Anti-Fraud Framework – The Role of IT

Example: Trade loading / channel stuffing

Inquiry & interview

Inquire of accounting personnel as to sales activity recorded close to reporting period ends

Analytics / CAATs

Analyze the ratio of sales in the last week or month of the period to total sales for the period

Compare gross margin, overall and by product line and major vendor, to previous periods and to budget considering industry trends

Compare the number of weeks of inventory in distribution channels with prior periods

Targeted testing of transactions / CAATs

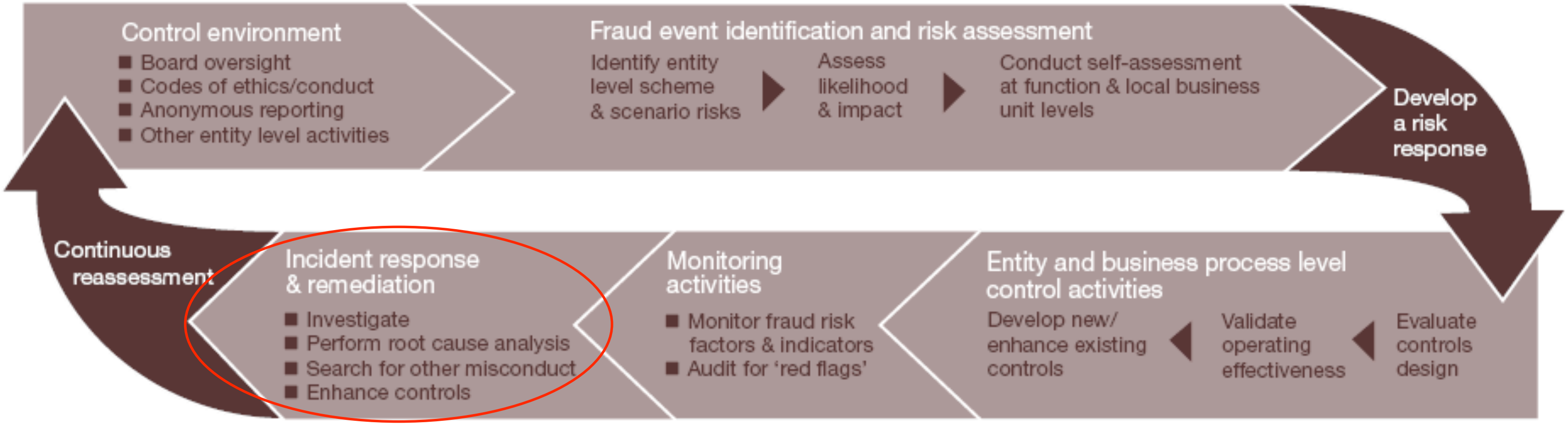
Compare daily recorded revenues for periods shortly before and after period end

Compare sales credits for returns subsequent to period end with sales credits during the period

Compare weekly and daily sales for selected periods near quarter or year end by location, product line and major vendor with sales of the preceding and prior year periods

Compare revenue trends by salesperson for indications of potential revenue overstatement

Anti-Fraud Framework – The Role of IT


Control environment
■ Board oversight
■ Codes of ethics/conduct
■ Anonymous reporting
■ Other entity level activities
Fraud event identification and risk assessment
Identify entity level scheme & scenario risks
Assess likelihood & impact
Conduct self-assessment at function & local business unit levels
Develop a risk response
Entity and business process level control activities
Evaluate controls design
Validate operating effectiveness
Develop new/ enhance existing controls
Monitoring activities
■ Monitor fraud risk factors & indicators
■ Audit for 'red flags'
Incident response & remediation
■ Investigate
■ Perform root cause analysis
■ Search for other misconduct
■ Enhance controls
Continuous reassessment

IT Incident Response and Remediation

- ***Investigate instances of fraud***
- ***Leverage system based resources where available***
- ***Enhance controls based upon a root analysis***

Anti-Fraud Framework – The Role of IT

Forensic Investigation

Whether to investigate

Assembling the investigative team

Legal, audit & business implications

Key Take-Aways

Fraud Risks – IT Controls

Questions???

Today's Presenter

David Eikel – Senior Manager

Armanino McKenna

(925) 790-2600 x7097

(650) 740-3868 (cell)