GTAG 13

Fraud Detection and Prevention in an Automated World

Ken Askelson CIA, CPA, CITP

John Vadalabene CIA, CISA, CLP, PMP

December 14, 2010

The Institute of Internal Auditors

Detroit Chapter

The IIA GTAG Series

GTAG
INFORMATION TECHNOLOGY CONTROLS

GTAG
Change and Patch Management Controls: Critical for Organizational Success

GTAG
Continuous Auditing: Implications for Assurance, Monitoring, and Risk Assessment

GTAG
Management of IT Auditing

GTAG
Managing and Auditing Privacy Risks

GTAG
Managing and Auditing IT Vulnerabilities

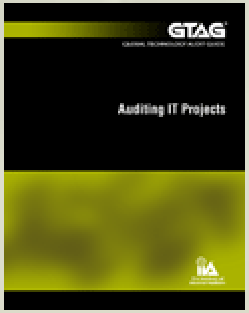
GTAG
Information Technology Outsourcing

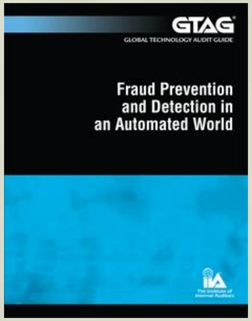
GTAG
Auditing Application Controls

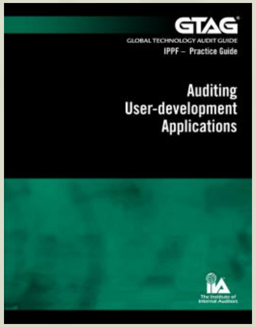
GTAG
Identity and Access Management

GTAG
Business Continuity Management

GTAG
Developing the IT Audit Plan


GTAG
Auditing IT Projects

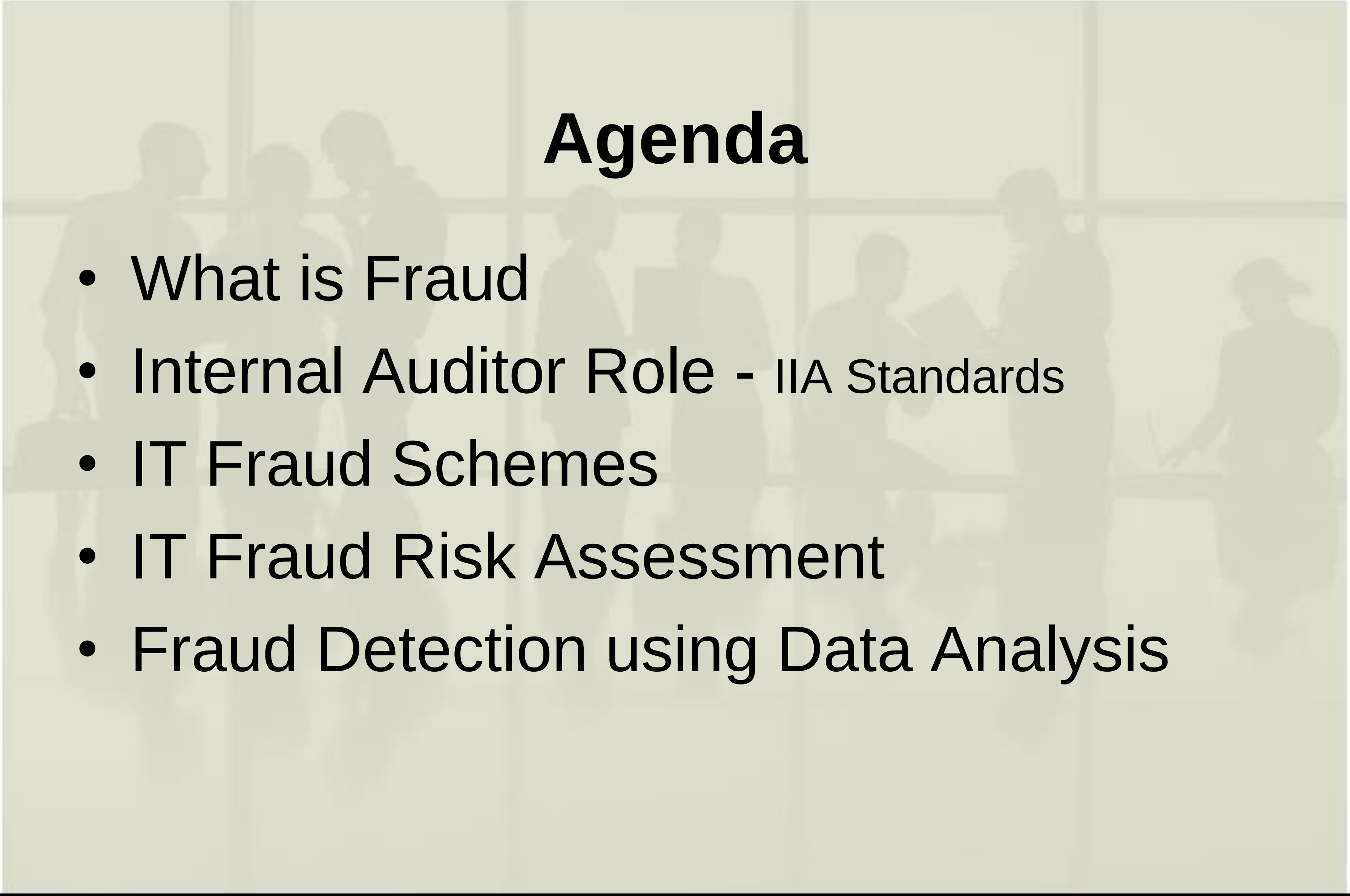

GTAG
GLOBAL TECHNOLOGY AUDIT GUIDE
Fraud Prevention and Detection in an Automated World


GTAG
GLOBAL TECHNOLOGY AUDIT GUIDE
IPPF – Practice Guide
Auditing User-development Applications

GTAG
GLOBAL TECHNOLOGY AUDIT GUIDE
IPPF – Practice Guide
Information Security Governance

The IIA GTAG Series

GTAG 1	Information Technology Controls	Mar 05
GTAG 2	Change and Patch Management Controls	Jun 05
GTAG 3	Continuous Auditing	Oct 05
GTAG 4	Management of IT Auditing	Mar 06
GTAG 5	Managing and Auditing Privacy Risks	Jul 06
GTAG 6	Managing and Auditing IT Vulnerabilities	Oct 06
GTAG 7	Information Technology Outsourcing	Mar 07
GTAG 8	Auditing Applications Controls	Jul 07
GTAG 9	Identity and Access Management	Nov 07
GTAG 10	Business Continuity Management	Jul 08
GTAG 11	Developing the IT Audit Plan	Jul 08
GTAG 12	Auditing IT Projects	Mar 09
GTAG 13	Fraud Prevention and Detection in an Automated World	Dec 09
GTAG 14	Auditing User-developed Applications	Jun 10
GTAG 15	Information Security Governance	Jun 10



Agenda

- What is Fraud
- Internal Auditor Role - IIA Standards
- IT Fraud Schemes
- IT Fraud Risk Assessment
- Fraud Detection using Data Analysis

What is Fraud

- **“** The SEC **named the CEO and/or CFO for some level of involvement in 89% of financial reporting fraud cases**.”

  COSO Fraud Study May 2010

- **“**some **59 percent of employees who leave a company are stealing company data,** …..”

  Ponemon Institute

  CSO magazine July/August 2009

- **“Insiders,** by virtue of legitimate access to information, systems, and networks, **pose a significant risk to employers”**

  Carnegie Mellon publication May 2008

What is Fraud

"… *any illegal act characterized by deceit, concealment, or violation of trust.*

Frauds are perpetrated to obtain money, property, or services; to avoid payment or loss of services; or to secure personal or business advantage."

IIA's International Professional Practices Framework (IPPF)

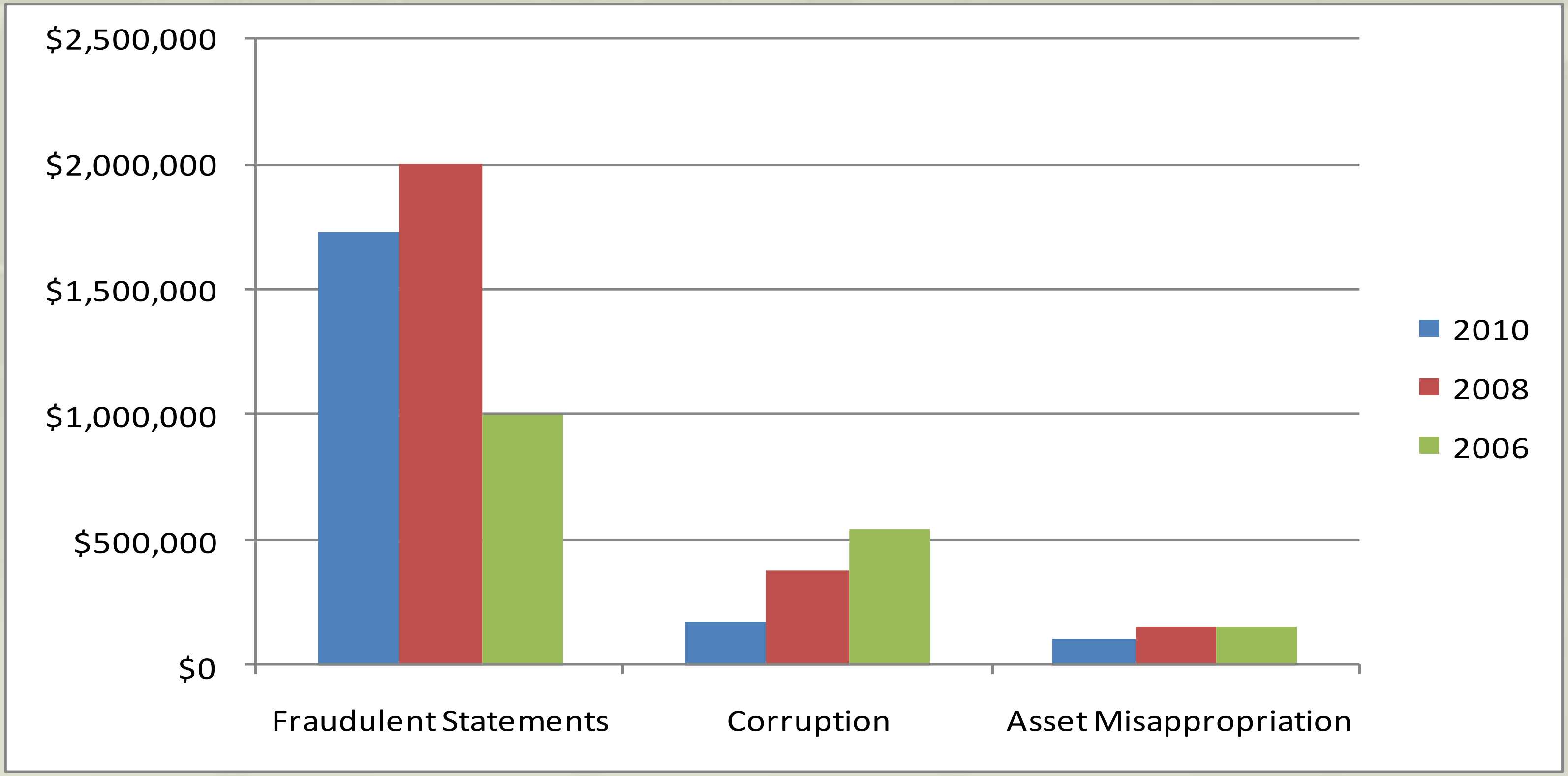
What is Fraud

Occupational fraud – “the use of one’s occupation for personal enrichment through the deliberate misuse or misapplication of the employing organization’s resources or assets.”

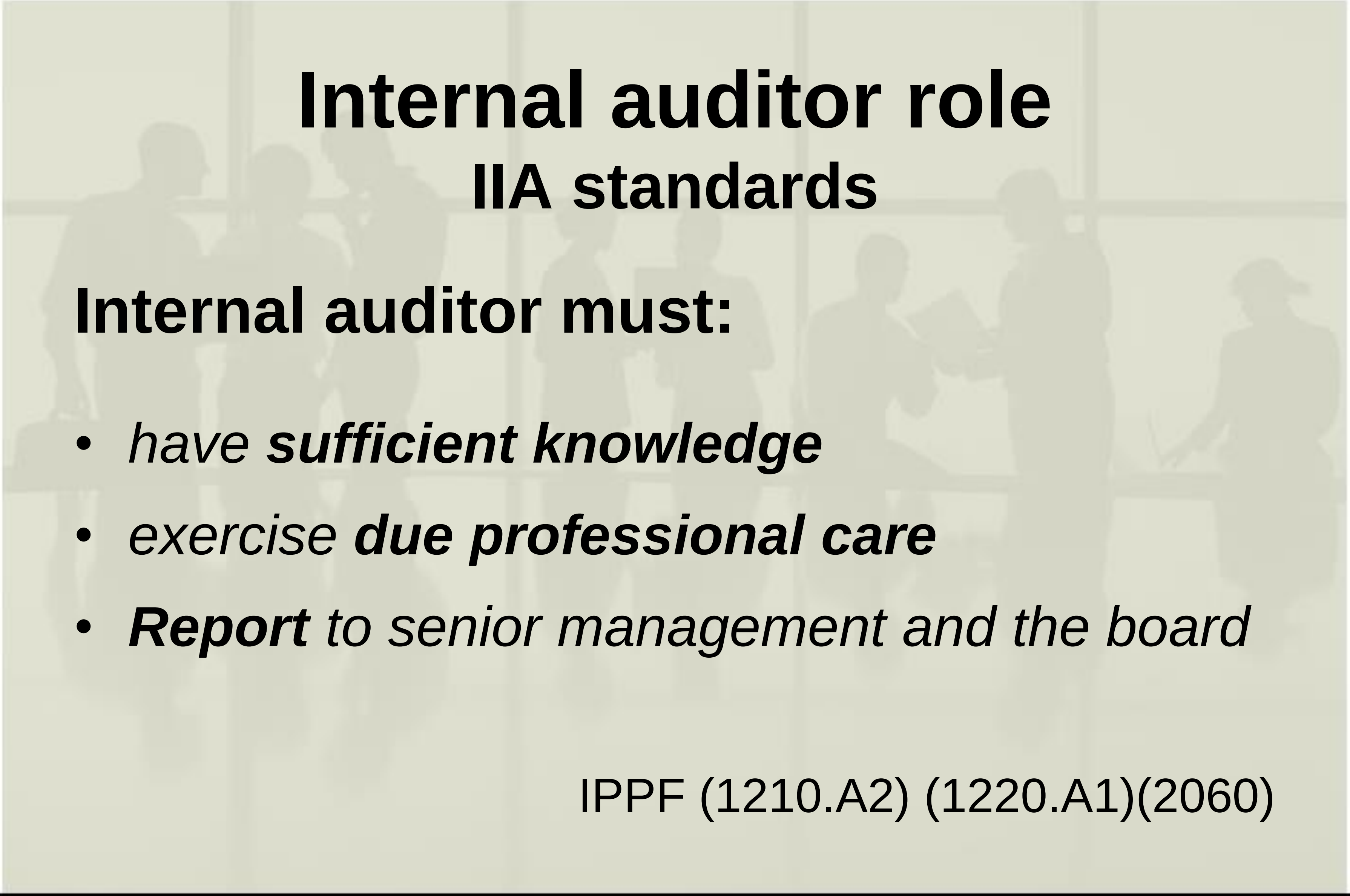
Association of Certified Fraud Examiners (ACFE)

Cost of Fraud

Occupational Fraud by Category (U.S. only) – Median Loss



Source: ACFE's "Report to the Nation on Occupational Fraud & Abuse" (2010, 2008, 2006)



Internal auditor role

IIA standards

Internal auditor must:

- *have* ***sufficient knowledge***
- *exercise* ***due professional care***
- ***Report*** *to senior management and the board*

IPPF (1210.A2) (1220.A1)(2060)

Internal auditor role
IIA standards

Internal auditor must:

- ***evaluate*** *the potential for fraud*
- ***evaluate*** *how fraud risk is managed*
- ***consider*** *the probability of significant* ***fraud****, when developing engagement objectives.*

IPPF (2120.A2) (2210.A2)

Internal auditor role
Other fraud guidance

- **Internal Auditing and Fraud**

  IPPF Practice Guide - December 2009

- **GTAG 13 – Fraud Prevention and Detection in an Automated World**

  IPPF Practice Guide - December 2009

- **Managing the Business Risk of Fraud: A Practical Guide**

  The IIA, ACFE, and AICPA - 2008

Internal auditor role
Other fraud guidance

- **Report to the Nations: 2010 Global Fraud Study**

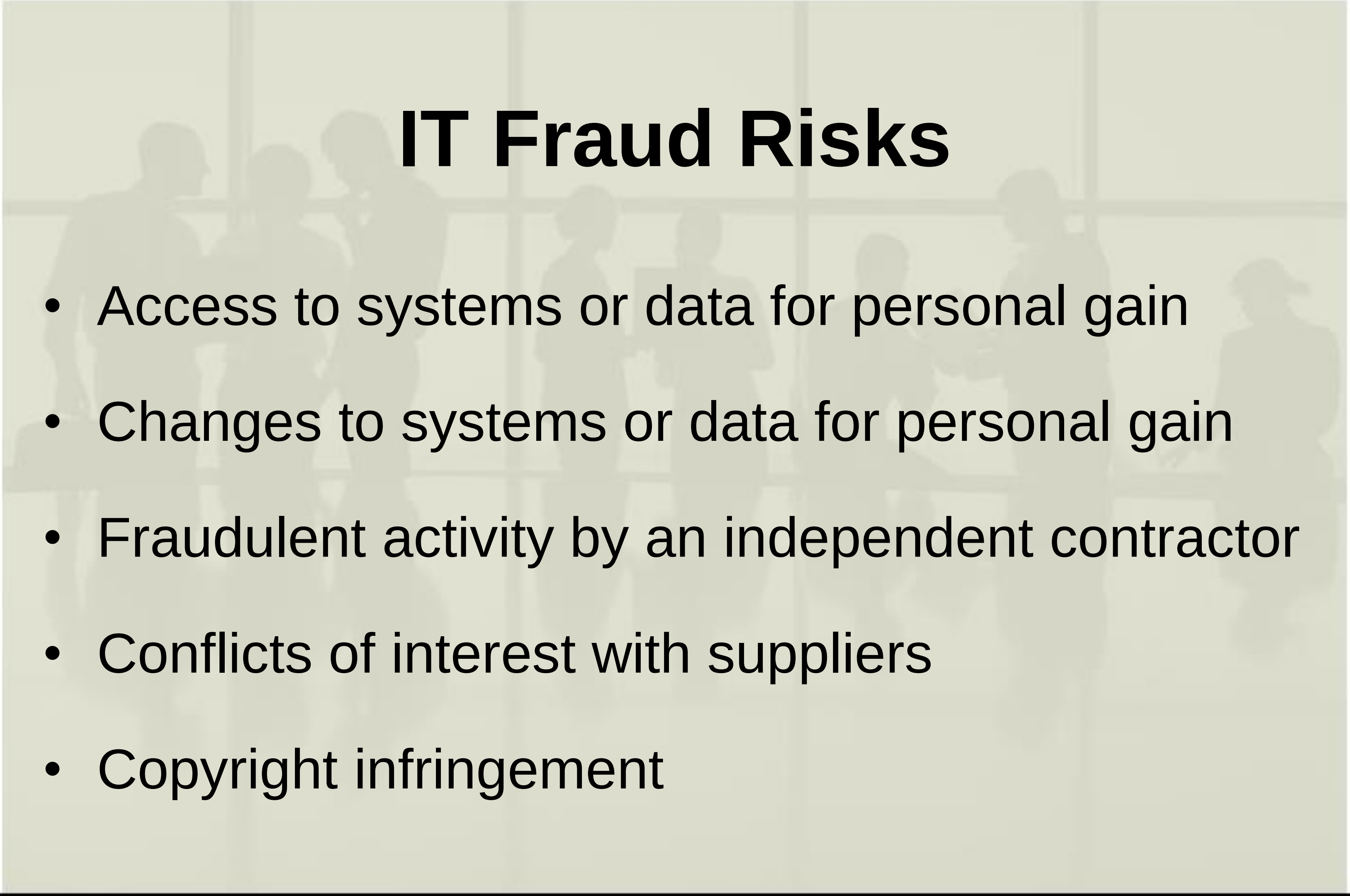
  ACFE - 2010

- **Fraudulent Financial Reporting: 1998 - 2007**

  COSO – May 2010

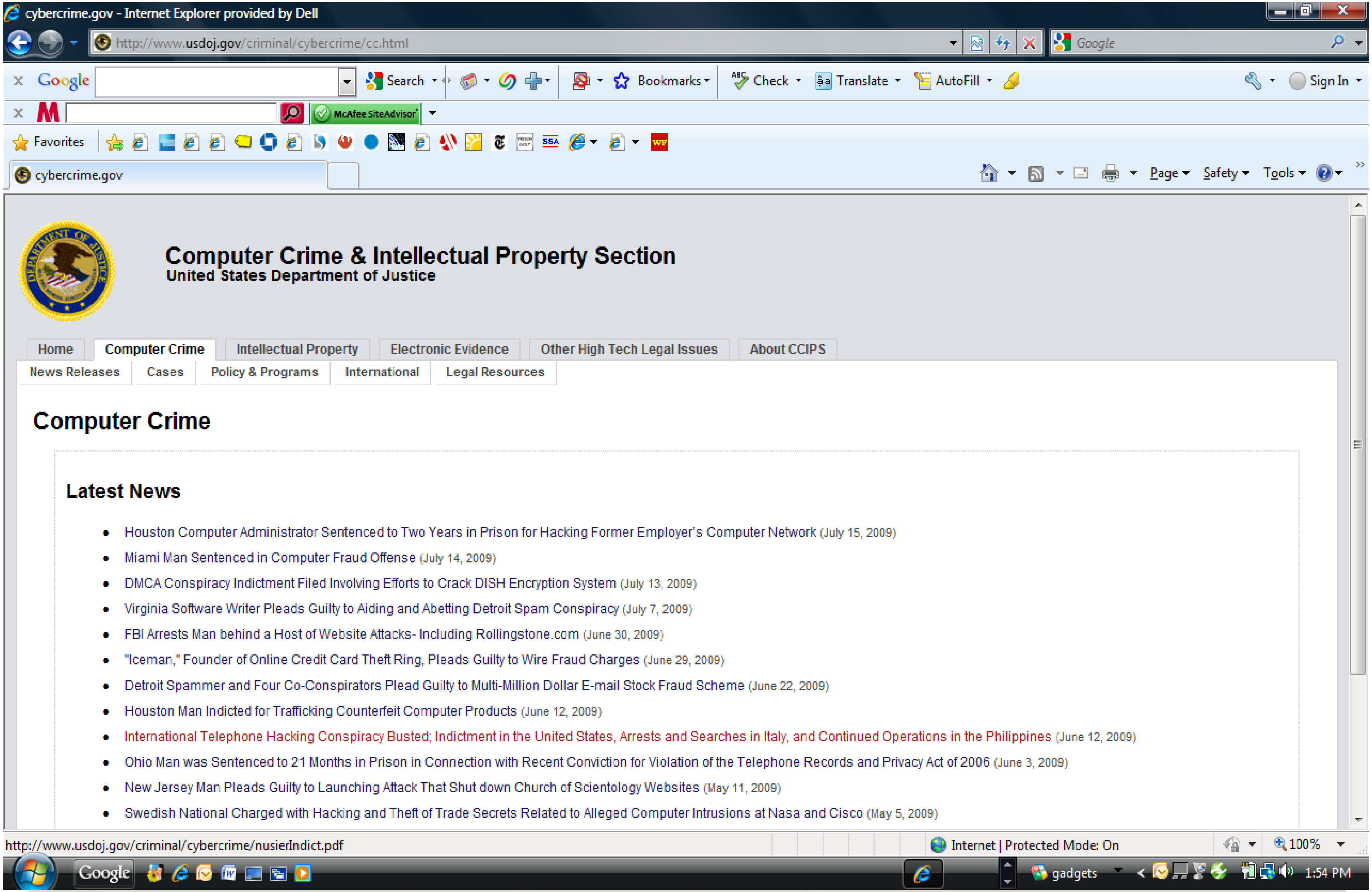
Fraud Risks

Examples	
Asset misappropriation	Information misrepresentation
Skimming	Corruption
Disbursements	Bribery
Expense reimbursement	Conflict of interest
Payroll	Related parties
Financial statements	Tax evasion



IT Fraud Risks

- Access to systems or data for personal gain
- Changes to systems or data for personal gain
- Fraudulent activity by an independent contractor
- Conflicts of interest with suppliers
- Copyright infringement


cybercrime.gov - Internet Explorer provided by Dell
http://www.usdoj.gov/criminal/cybercrime/cc.html
Google
Search
Bookmarks
Check
Translate
AutoFill
Sign In
McAfee SiteAdvisor
Favorites
cybercrime.gov
Page
Safety
Tools
http://www.usdoj.gov/criminal/cybercrime/nusierIndict.pdf
Internet | Protected Mode: On
100%
gadgets
1:54 PM

Computer Crime & Intellectual Property Section

United States Department of Justice

Home | Computer Crime | Intellectual Property | Electronic Evidence | Other High Tech Legal Issues | About CCIPS

News Releases | Cases | Policy & Programs | International | Legal Resources

Computer Crime

Latest News

- Houston Computer Administrator Sentenced to Two Years in Prison for Hacking Former Employer's Computer Network (July 15, 2009)
- Miami Man Sentenced in Computer Fraud Offense (July 14, 2009)
- DMCA Conspiracy Indictment Filed Involving Efforts to Crack DISH Encryption System (July 13, 2009)
- Virginia Software Writer Pleads Guilty to Aiding and Abetting Detroit Spam Conspiracy (July 7, 2009)
- FBI Arrests Man behind a Host of Website Attacks- Including Rollingstone.com (June 30, 2009)
- "Iceman," Founder of Online Credit Card Theft Ring, Pleads Guilty to Wire Fraud Charges (June 29, 2009)
- Detroit Spammer and Four Co-Conspirators Plead Guilty to Multi-Million Dollar E-mail Stock Fraud Scheme (June 22, 2009)
- Houston Man Indicted for Trafficking Counterfeit Computer Products (June 12, 2009)
- International Telephone Hacking Conspiracy Busted; Indictment in the United States, Arrests and Searches in Italy, and Continued Operations in the Philippines (June 12, 2009)
- Ohio Man was Sentenced to 21 Months in Prison in Connection with Recent Conviction for Violation of the Telephone Records and Privacy Act of 2006 (June 3, 2009)
- New Jersey Man Pleads Guilty to Launching Attack That Shut down Church of Scientology Websites (May 11, 2009)
- Swedish National Charged with Hacking and Theft of Trade Secrets Related to Alleged Computer Intrusions at Nasa and Cisco (May 5, 2009)

Access to systems or data for personal gain

Scenario	Fraud
An employee in the payroll department **moved to a new position**. Upon switching positions, the employee's **access rights were left unchanged**. Source: 2008 Insider Threat Study, US Secret Service and CERT/SEI	Using the retained privileged access rights, the employee **provided an associate with confidential information** for 1,500 of the firm's employees, including 401k account numbers, credit card account numbers, and social security numbers, which was then used to commit over **100 cases of identity theft**. The insider's actions caused over $1 million in damage to the company and its employees.

Changes to system programs or data for personal gain

Phase	Fraud	Oversights
Requirements Definition	**195 illegitimate drivers' licenses were created and sold** by a police communications officer who accidentally discovers she can create them.	Ill-defined authentication and role-based access control requirements. Ill-defined security requirements for automated business processes. Lack of segregation of duties.

Source: 2008 Insider Threat Study, US Secret Service and CERT/SEI

Changes to system programs or data for personal gain

Phase	Fraud	Oversights
System Design	An employee realizes there **is** no oversight in his company's system and business processes, so he works with organized crime to enter and profit from $20 million in **fake health insurance claims**.	Insufficient attention to security details in automated workflow processes. Lack of consideration for security vulnerabilities posed by authorized system overrides.

Source: 2008 Insider Threat Study, US Secret Service and CERT/SEI

Changes to system programs or data for personal gain

Phase	Fraud	Oversights
System Maintenance	A foreign currency trader covers up losses of $691 million over a five-year period by making **unauthorized changes to the source code**.	Lack of code reviews. End-user access to source code.

Source: 2008 Insider Threat Study, US Secret Service and CERT/SEI

Fraudulent activity by an independent contractor

Scenario	Fraud
A disgruntled independent contractor was fired from his current employer. Source: U.S. Department of Justice	An independent contractor, a UNIX engineer, was fired and told to turn in all client equipment including laptop. On the day of termination, the **contractor imbedded malicious code designed to propagate throughout the network and destroy all financial, securities and mortgage information**. A senior engineer discovered the malicious script before it executed. The contractor faces up to 10 years in prison.

IT Fraud Risk Assessment Key Elements

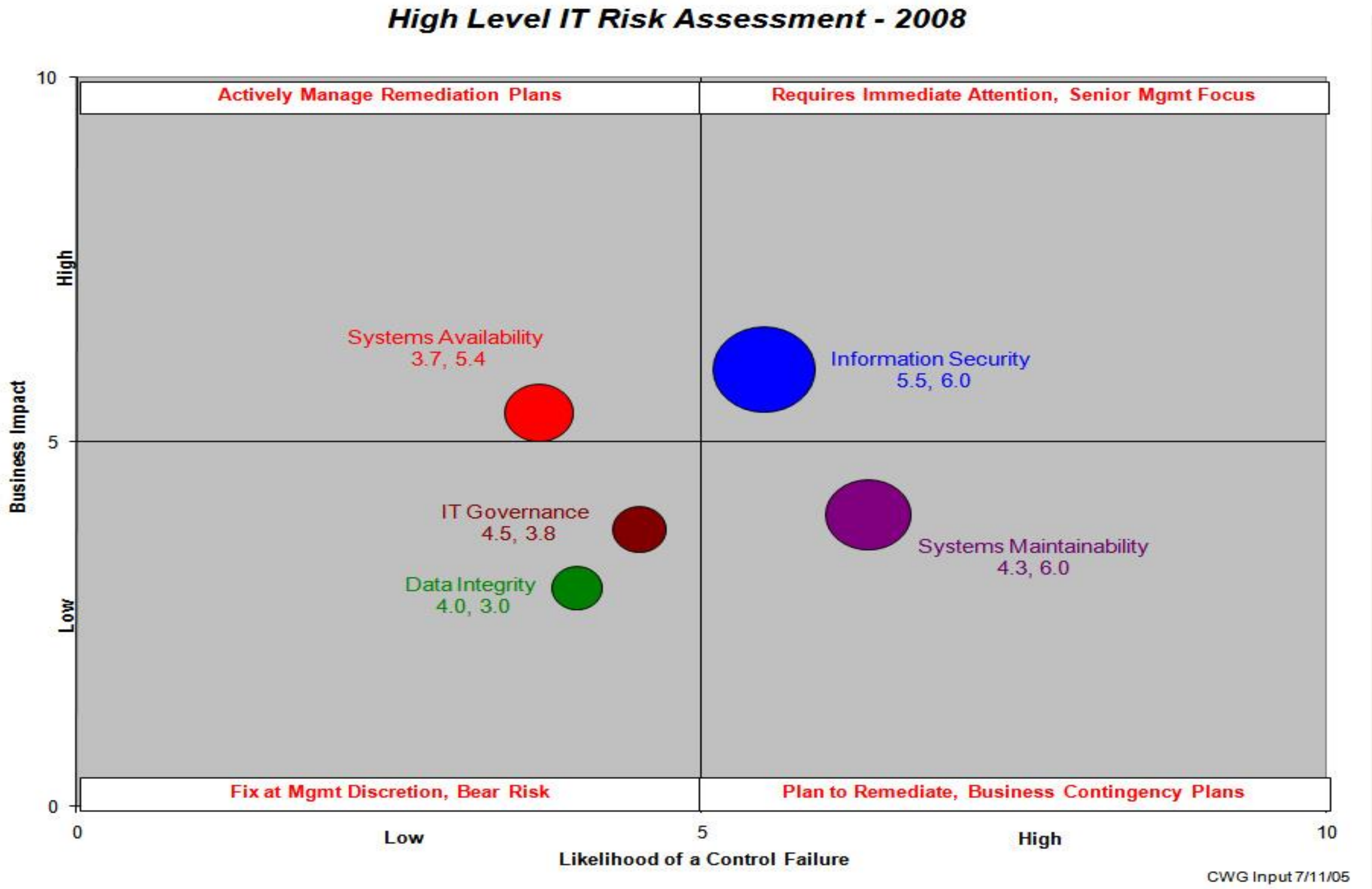
- Types of frauds
- Inherent risk of fraud
- Existing controls
- Control gaps
- Likelihood
- Business impact

IT Fraud Risk Assessment Template - Example

Business Owner-	Fraud Risks	Controls	Preventive or Detective	Monitoring	Likelihood	Impact
IT - CIO	Access to systems or data for personal gain. (Logical Access) Access to customers' or employees' personal information (e.g., credit card information, payroll information) Access to confidential company information (e.g., financial reporting, supplier data, strategic plans) Copying and use of software or data for distribution	Identity management (e.g. individual user IDs, automated password complexity rules, password rotation) Access controls Authentication controls Authorization controls Access control lists Network controls Anti-virus and patch management Restricted access to software code	Both	Information security System administrators Business owners Internal auditing	Medium	High

IT Risk Assessment Tool

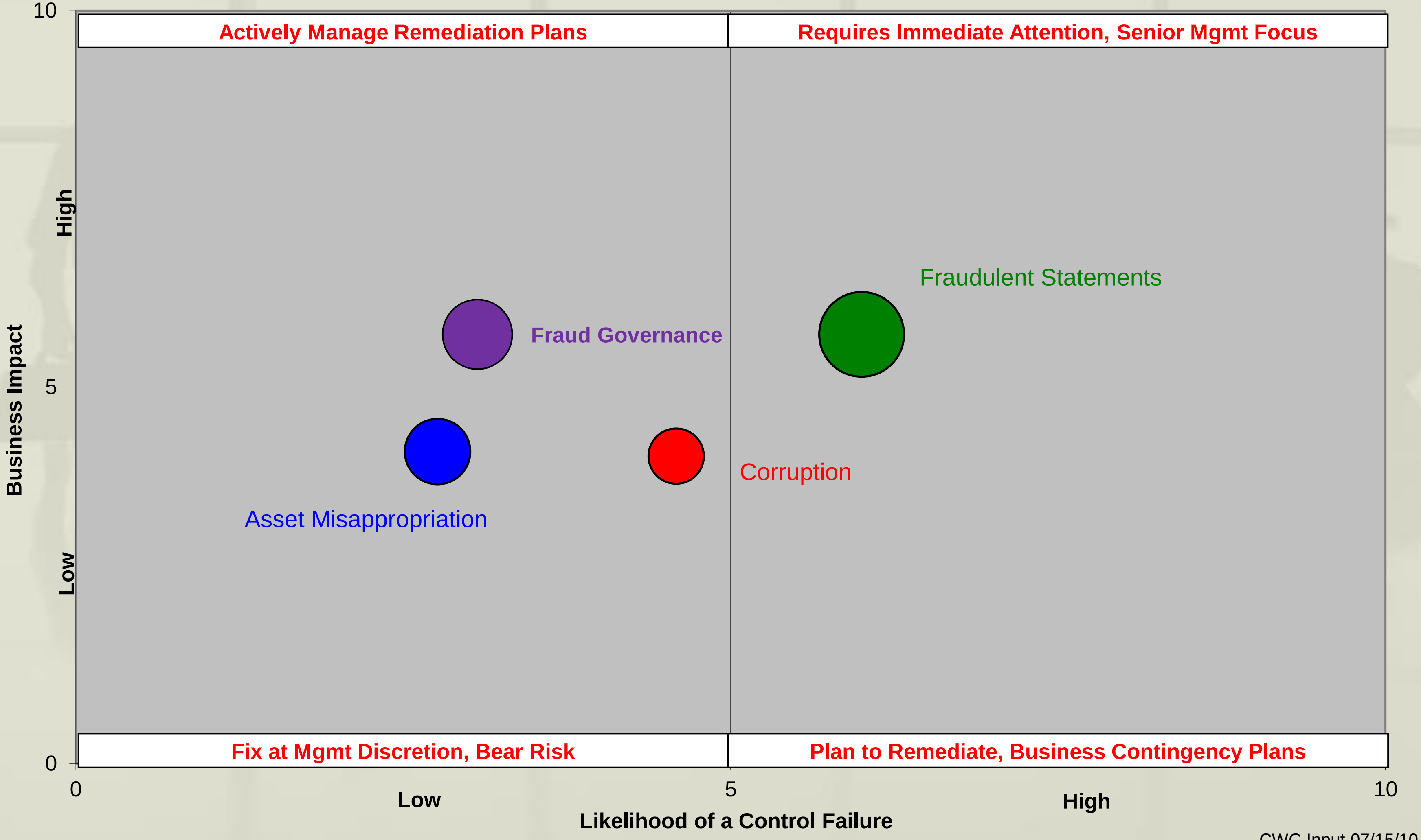
IT Risk Assessment Criteria	Criteria Description	Likelihood of a Control Failure	Business Impact	Effort/Cost to Mitigate
System Availability (SA)	**Risk: Inefficient use of computing resources resulting in lost sales, profits and associate productivity.**	**3.2**	**6.0**	**4.0**
SA - Service Level Agreements	**Service level agreements are defined and met for critical systems availability and response time.**			
IT Auditor 1		5	5	5
IT Auditor 2		2	5	5
IT Auditor 3		5	8	5
IT Manager 1		2	8	5
IT Manager 2		5	5	5
IT Manager 3		5	5	5
	Scoring Average	4.0	6.0	5.0
SA - Responsibility Assigned	**Responsibility and accountability for systems availability are assigned in job descriptions and appropriately aligned within the organization.**			
IT Auditor 1		2	5	2
IT Auditor 2		5	5	2
IT Auditor 3		2	5	2
IT Manager 1		5	5	2
IT Manager 2		5	5	5
IT Manager 3		5	5	5
	Scoring Average	4.0	5.0	3.0


High Level IT Risk Assessment - 2008
10
5
0
High
Low
Business Impact
Actively Manage Remediation Plans
Requires Immediate Attention, Senior Mgmt Focus
Fix at Mgmt Discretion, Bear Risk
Plan to Remediate, Business Contingency Plans
Systems Availability
3.7, 5.4
Information Security
5.5, 6.0
IT Governance
4.5, 3.8
Systems Maintainability
4.3, 6.0
Data Integrity
4.0, 3.0
0
5
10
Low
High
Likelihood of a Control Failure
CWG Input 7/11/05

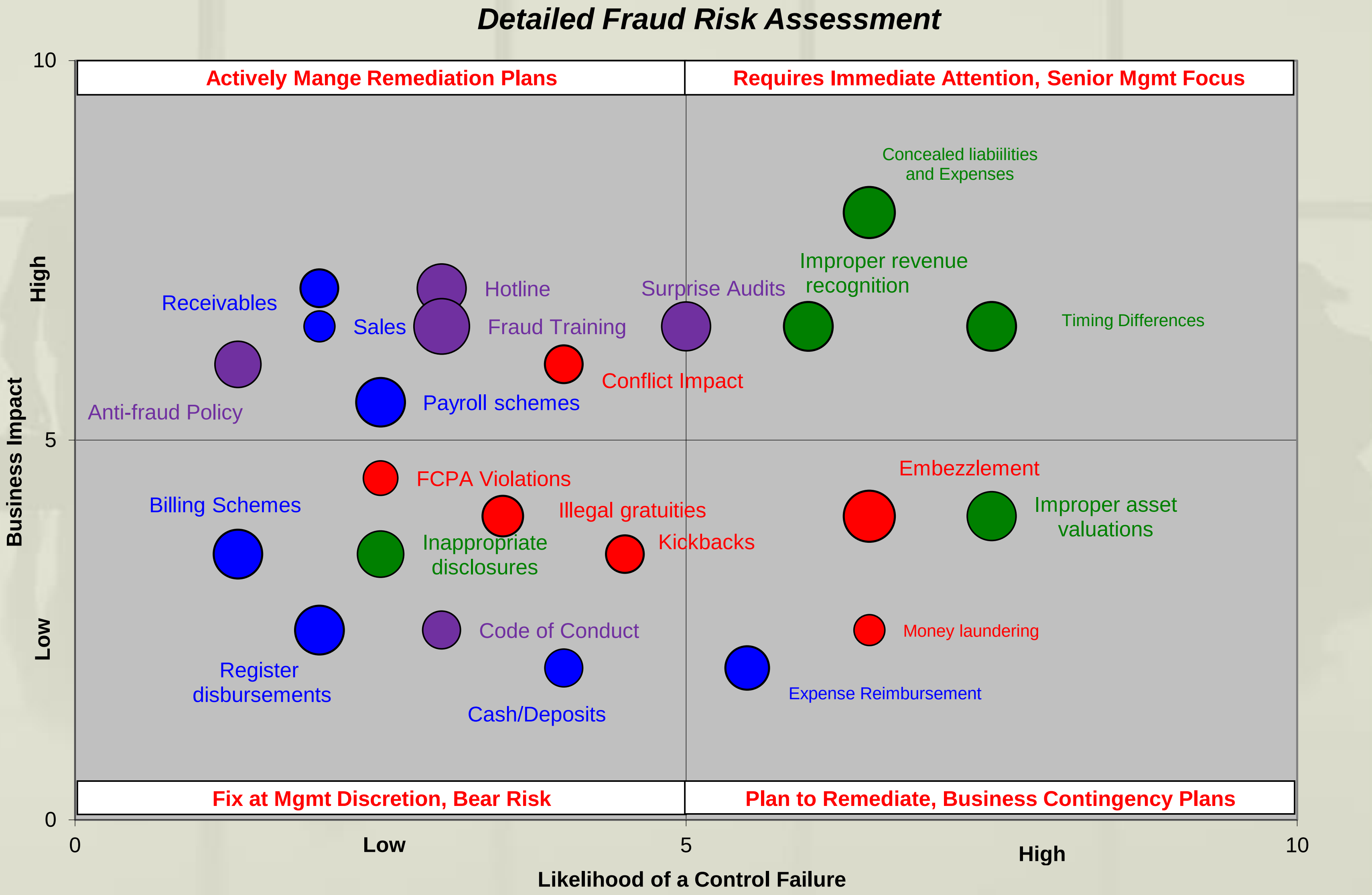
Fraud Risk Assessment Tool

		Scoring Scale: Low = 2	Medium = 5	High = 8
Fraud Risk Assessment Criteria	Criteria Description	Likelihood of Fraud	Business Impact	Effort/Cost to Mitigate
Corruption	**Fraud schemes that involve employee's use of influence in business transactions that violates duty to employer for personal gain.**	**4.6**	**4.1**	**3.3**
Conflicts of interest	**Employee diverts sales to a supplier where the employee has an ownership interest.**			
Auditor 1		2	5	2
Auditor 2		2	5	2
Auditor 3		5	5	2
Manager 1		5	5	2
Manager 2		5	8	5
Manager 3		5	8	5
	Scoring Average	4.0	6.0	3.0
Kickbacks	**Employee receives money from supplier based upon purchase volumes or supplier provides unauthorized travel and entertainment benefits based upon purchase volumes.**			
Auditor 1		5	2	2
Auditor 2		5	2	2
Auditor 3		2	2	2
Manager 1		5	5	2
Manager 2		5	5	5
Manager 3		5	5	5
	Scoring Average	4.5	3.5	3.0

High Level Fraud Risk Assessment



CWG Input 07/15/10



CWG Input 07/15/10

Risk Assessment Tool

Demonstrate Tool

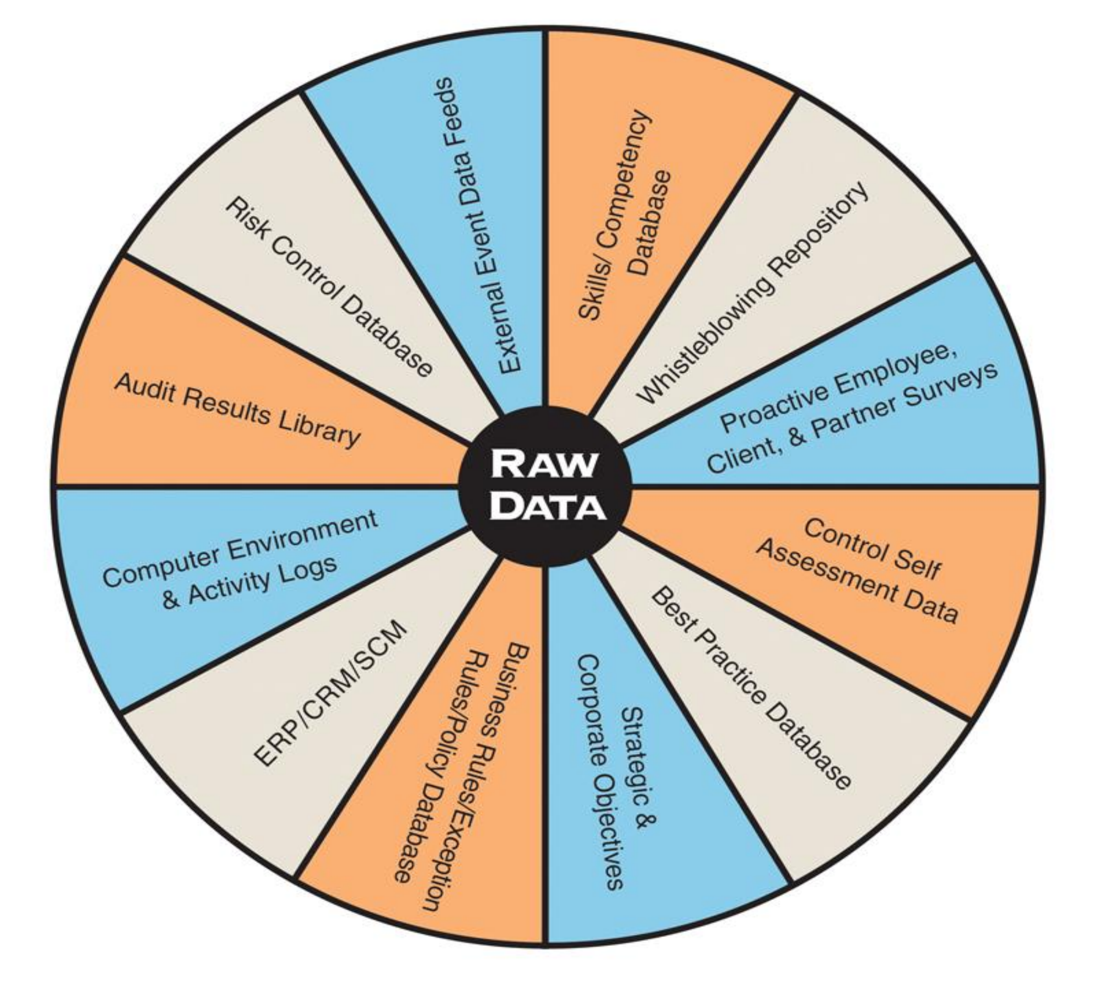
Data Analytics And Its Use at General Motors

John Vadalabene, Manager, Data Analysis Group, General Motors Company

Why Data Analytics?

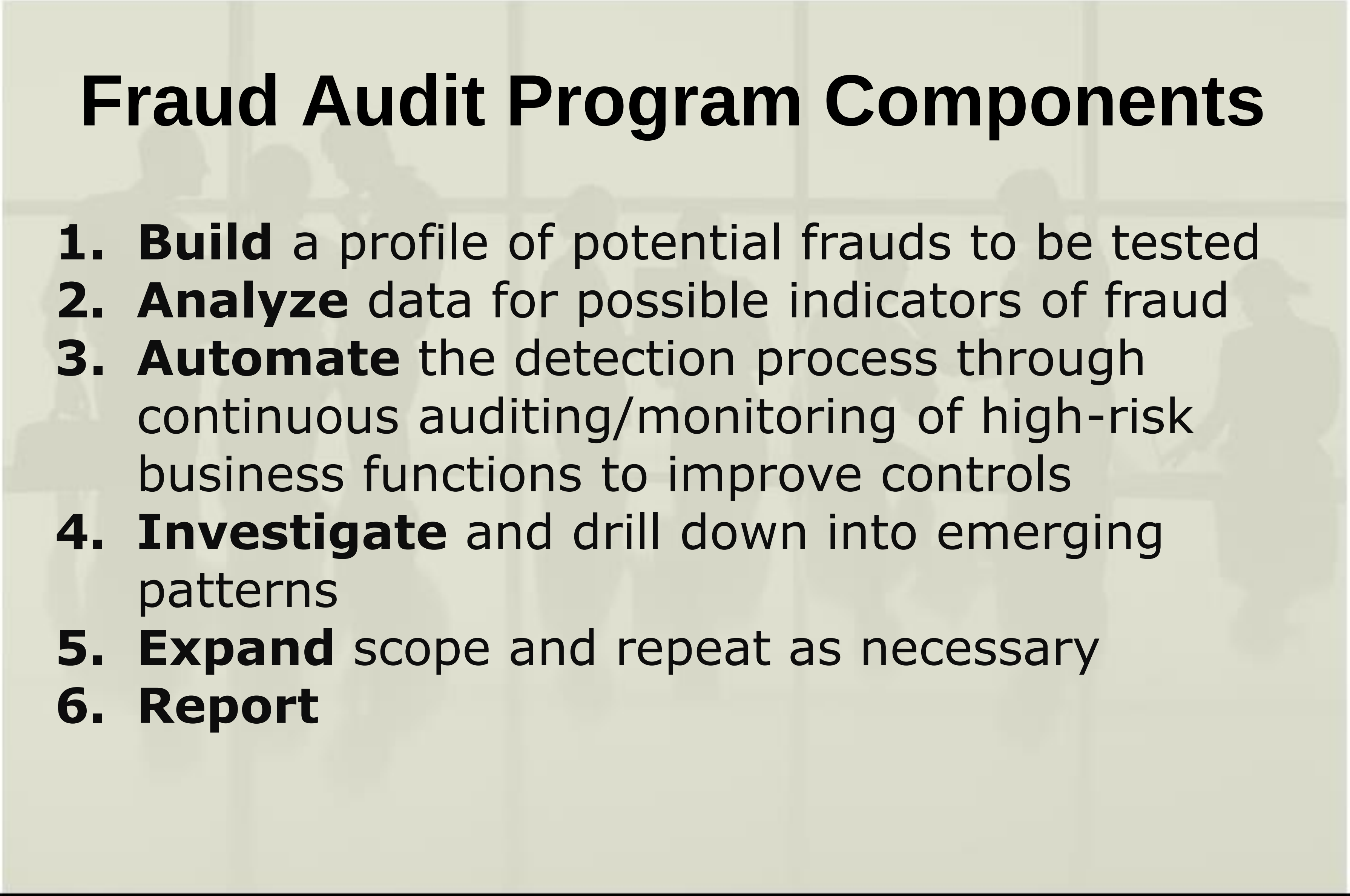
- Internal control system weaknesses
- Examine 100% of transactions
- Compare data from different applications
- Perform tests designed for fraud detection and control verification
- Automate tests in high-risk areas
- Maintain logs of analytics performed

Diversified Data Sources



RAW DATA
External Event Data Feeds
Skills/ Competency Database
Whistleblowing Repository
Proactive Employee, Client, & Partner Surveys
Control Self Assessment Data
Best Practice Database
Strategic & Corporate Objectives
Business Rules/Exception Rules/Policy Database
ERP/CRM/SCM
Computer Environment & Activity Logs
Audit Results Library
Risk Control Database

Fraud Audit Program Components



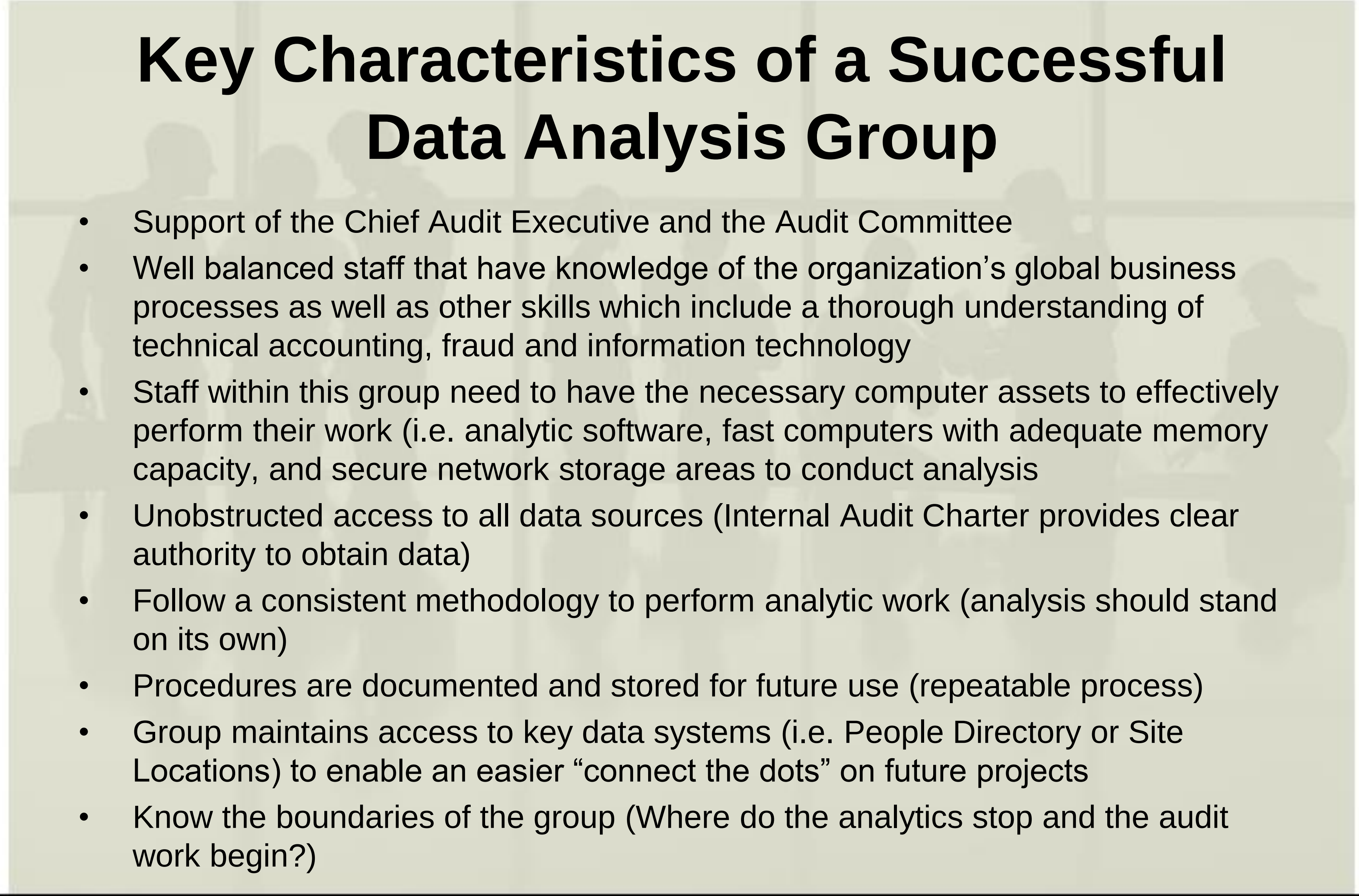
1. **Build** a profile of potential frauds to be tested
2. **Analyze** data for possible indicators of fraud
3. **Automate** the detection process through continuous auditing/monitoring of high-risk business functions to improve controls
4. **Investigate** and drill down into emerging patterns
5. **Expand** scope and repeat as necessary
6. **Report**

Analytical techniques

- Calculate **statistical parameters**
- **Classify** to find patterns
- **Stratify** to identify unusual values
- **Digital analysis**, to identify unlikely occurrences
- Joining or **matching data** between systems
- **Duplicates** testing
- **Gaps** testing to identify missing data
- Summing and totaling to check **control totals** that may be falsified
- **Graphing** to provide visual identification of anomalous transactions

Fraud Test Examples

Type	Tests used
Fictitious vendors	Run checks to uncover post office boxes used as addresses and to find any matches between vendor and employee addresses and/or phone numbers.
Altered invoices	Search for duplicates. Check for invoice amounts not matching contracts or purchase order amounts.
Duplicate invoices	Review for duplicate invoice numbers, duplicate dates, and duplicate invoice amounts.
Duplicate payments	Search for identical invoice numbers and payment amounts.
Payroll fraud	Check whether a terminated employee is still on payroll by comparing the date of termination with the pay period covered by the paycheck, and extract all pay transactions for departure date less than the date of the current pay period.



Key Characteristics of a Successful Data Analysis Group

- Support of the Chief Audit Executive and the Audit Committee
- Well balanced staff that have knowledge of the organization’s global business processes as well as other skills which include a thorough understanding of technical accounting, fraud and information technology
- Staff within this group need to have the necessary computer assets to effectively perform their work (i.e. analytic software, fast computers with adequate memory capacity, and secure network storage areas to conduct analysis
- Unobstructed access to all data sources (Internal Audit Charter provides clear authority to obtain data)
- Follow a consistent methodology to perform analytic work (analysis should stand on its own)
- Procedures are documented and stored for future use (repeatable process)
- Group maintains access to key data systems (i.e. People Directory or Site Locations) to enable an easier “connect the dots” on future projects
- Know the boundaries of the group (Where do the analytics stop and the audit work begin?)

What Do We Hope to Accomplish (Data Analysis Group at GM)?

- Support evolution from traditional cyclical approach to one which continually assesses areas of greatest risk and performs in-depth analysis in specific areas (Audit process support)
- Maintain robust test / procedures library for CAAT and other control tests
- Collaborate with Audit group and Management to identify “High Risk” projects with high data analytic ROI
- Proactively maintain data access to major systems
- Work with system developers to ensure that the audit role is included with selected high risk new systems
- Maintain an effective training framework and promote data analytic skills within the audit team

Vision / Mission Example (General Motors Audit Services)

Vision

Lead GM and GMAS in the strategic use of data analytics to reduce risk exposure and enable the company to combine data intelligently to provide meaningful information to management.

Mission

Ensure that data analytics is embedded into the audit process and is used to effectively drive efficiencies, identify truly high risk areas, target strategic reviews, and allow management to derive useful information from the data contained within the many siloed organizations (Mining data that can provide indicators of the health of risk management and related controls).

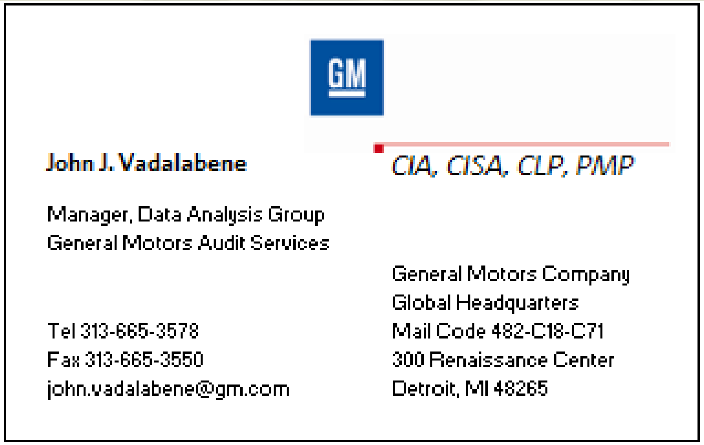
Objectives

1. ***Maintain robust test / procedures library for CAAT and other control tests (Routine repository, repeatable efficient processes)***
2. ***Audit process support (From planning through audit completion)***
3. ***Strategic Analytics (Special Projects)***
4. ***Continuous Auditing (key high risk activities derived from data analytic work performed through special projects or audits that require intensive monitoring and review)***
5. ***Obtain / Maintain Access to Key Data Sources (Over 50 key systems identified)***
6. ***Professional Development / Training (Conduct training of GMAS team in the use of various technical tools such as ACL, Excel, Access, SQL, SAS, etc. as well as new tools)***

Data Analysis Project Examples

- **Manual Journal Entries (Continuous Auditing)**
- **Expense Reporting (Continuous Auditing) - In Process**
- **Worldwide Real Estate** - testing for duplicates, changes in leases, payment outside of terms, high / negative payments from or to business
- **IT Asset Management Audit** - Performed comparison between leasing and asset management systems
- **Indirect Purchasing** - Connect to regional SAP servers to extract purchasing data and combine them using data analytic routines to conduct comprehensive analytic tests
- **IT Security Management** - Databases - Assist business team by validating data and performing initial analytics on Service Continuity Management (SCM) and Application Tracking System (ATS) databases to determine if there are any data integrity issues.
- **Network Security Audit (Firewall Rules)** - Broke rule extract into a fully exploded view of rules down to the IP Address / Service protocol level

Thank You For Joining Us!



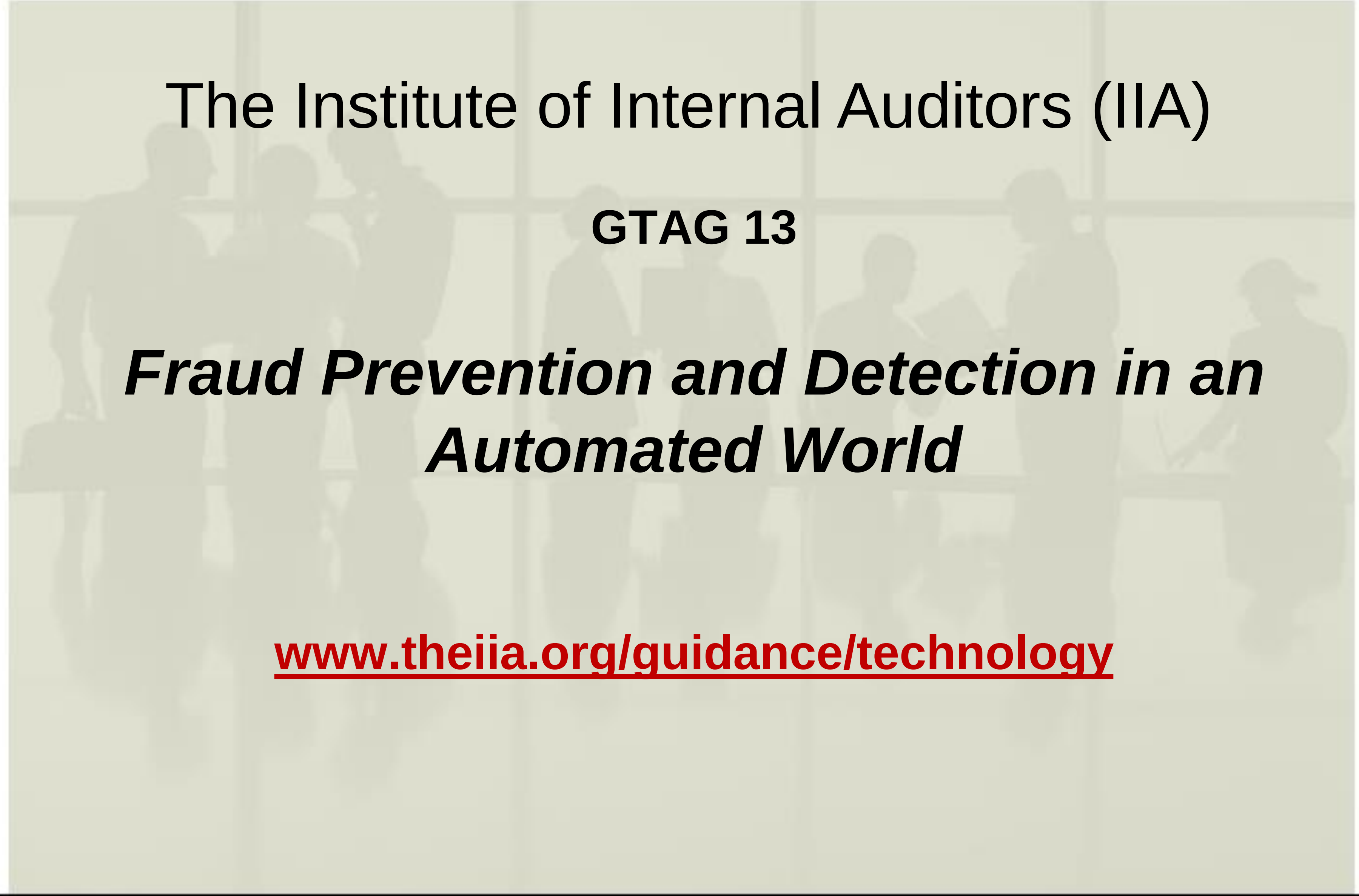
John J. Vadalabene

CIA, CISA, CLP, PMP

Manager, Data Analysis Group
General Motors Audit Services

General Motors Company
Global Headquarters
Mail Code 482-C18-C71
300 Renaissance Center
Detroit, MI 48265

Tel 313-665-3578
Fax 313-665-3550
john.vadalabene@gm.com



The Institute of Internal Auditors (IIA)

GTAG 13

Fraud Prevention and Detection in an Automated World

www.theiia.org/guidance/technology

Q & A

Thank You