NYSICA New York State Internal Control Association

Internal Control, Fraud & Risk Management
Annual Spring Conference
May 9, 2019

Fraud Risk Management and Assessment

David L. Cotton, CPA, CFE, CGFM
Cotton & Company LLP
Alexandria, VA 22314
www.cottoncpa.com
dcotton@cottoncpa.com

DAVID L. COTTON, CPA, CFE, CGFM
COTTON & COMPANY LLP CHAIRMAN

Dave Cotton is chairman of Cotton & Company LLP, Certified Public Accountants, headquartered in Alexandria, Virginia. The firm was founded in 1981 and has a practice concentration in assisting Federal and State government agencies, inspectors general, and government grantees and contractors with a variety of government program-related assurance and advisory services. Cotton & Company has performed grant and contract, indirect cost rate, financial statement, financial related, and performance audits for more than two dozen Federal inspectors general as well as numerous other Federal and State agencies and programs.

Cotton & Company's Federal agency audit clients have included the U.S. Government Accountability Office, U.S. Navy, U.S. Marine Corps, U.S. Transportation Command, U.S. House of Representatives, U.S. Capitol Police, U.S. Small Business Administration, U.S. Bureau of Prisons, Millennium Challenge Corporation, U.S. Marshals Service, and Bureau of Alcohol, Tobacco, Firearms and Explosives. Cotton & Company also assists numerous Federal agencies in preparing financial statements and improving financial management, accounting, and internal control systems.

Dave received a BS in mechanical engineering (1971) and an MBA in management science and labor relations (1972) from Lehigh University in Bethlehem, PA. He also pursued graduate studies in accounting and auditing at the University of Chicago Graduate School of Business (1977 to 1978). He is a Certified Public Accountant (CPA), Certified Fraud Examiner (CFE), and Certified Government Financial Manager (CGFM).

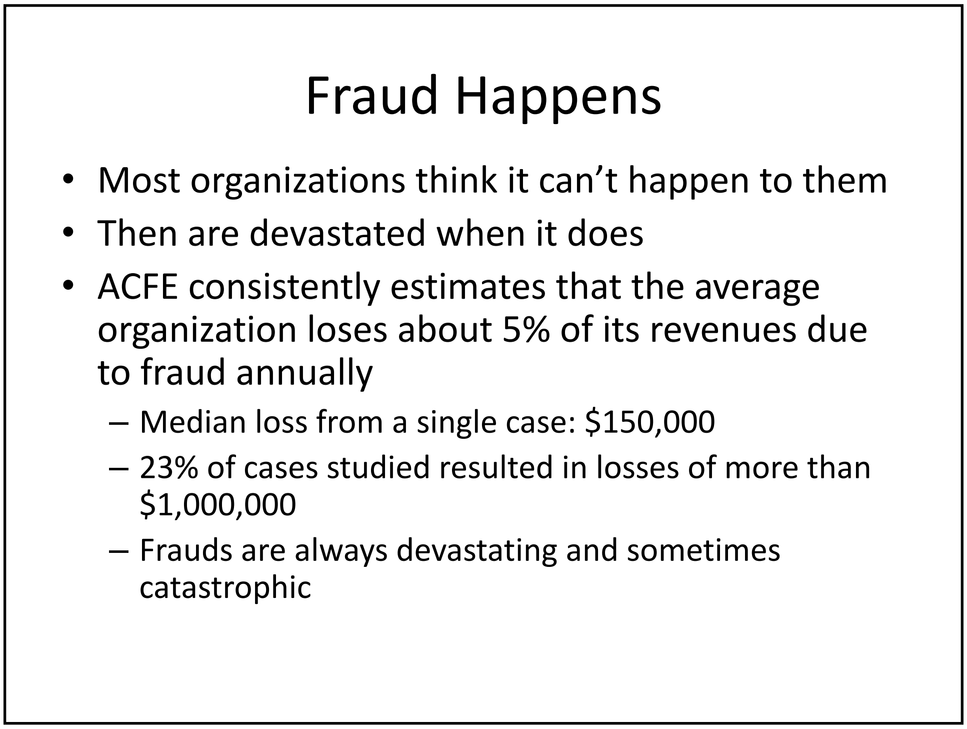
Dave served on the Advisory Council on Government Auditing Standards (the Council advises the United States Comptroller General on promulgation of ***Government Auditing Standards***—GAO's yellow book) from 2006 to 2009. He served on the Institute of Internal Auditors (IIA) Anti-Fraud Programs and Controls Task Force and co-authored ***Managing the Business Risk of Fraud: A Practical Guide***. He served on the American Institute of CPAs Anti-Fraud Task Force and co-authored ***Management Override: The Achilles Heel of Fraud Prevention***. Dave is the past-chair of the AICPA Federal Accounting and Auditing Subcommittee and has served on the AICPA Governmental Accounting and Auditing Committee and the Government Technical Standards Subcommittee of the AICPA Professional Ethics Executive Committee. Dave chaired the Fraud Risk Management Task Force, sponsored by COSO and ACFE and is a principal author of the ***COSO-ACFE Fraud Risk Management Guide***.

Dave served on the board of the Virginia Society of Certified Public Accountants (VSCPA) and on the VSCPA Litigation Services Committee, Professional Ethics Committee, Quality Review Committee, and Governmental Accounting and Auditing Committee. He is a member of the Association of Government Accountants (AGA) and past-advisory board chairman and past-president of the AGA Northern Virginia Chapter. He is also a member of the Institute of Internal Auditors and the Association of Certified Fraud Examiners.

Dave has testified as an expert in governmental accounting, auditing, and fraud issues before the United States Court of Federal Claims and other administrative and judicial bodies.

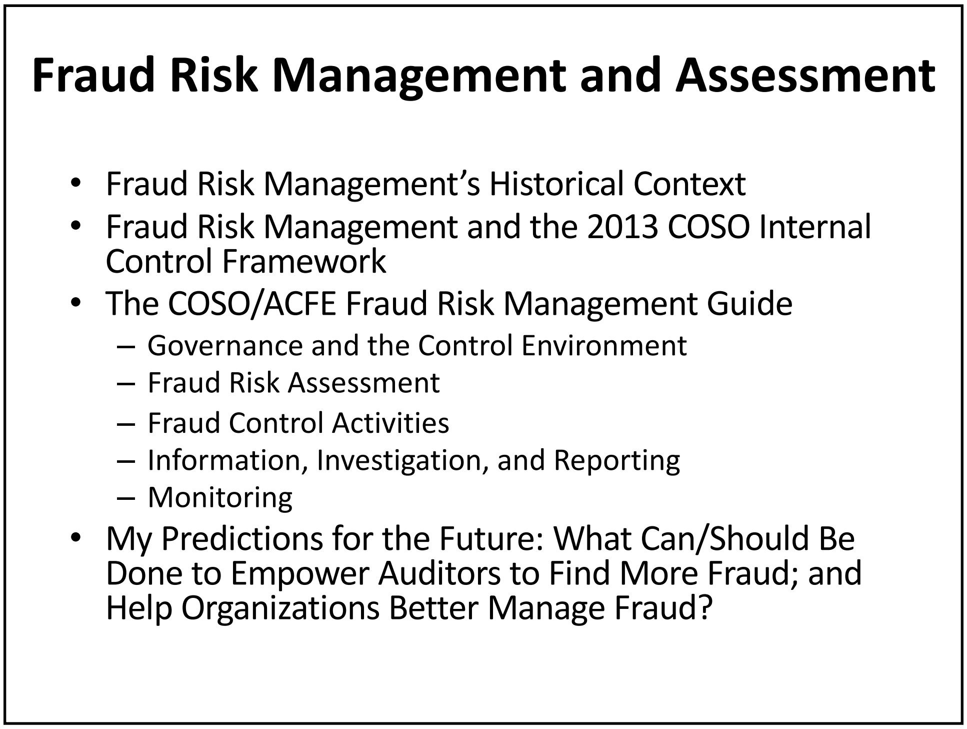
Dave has spoken frequently on cost accounting, professional ethics, and auditors' fraud detection responsibilities under SAS 99, *Consideration of Fraud in a Financial Statement Audit*. He has been an instructor for the George Washington University masters of accountancy program (***Fraud Examination and Forensic Accounting***)*,* and has instructed for the George Mason University Small Business Development Center (***Fundamentals of Accounting for Government Contracts***).

Dave was the recipient of the ACFE 2018 Certified Fraud Examiner of the Year Award ("presented to a CFE who has demonstrated outstanding achievement in the field of fraud examination … based on their contributions to the ACFE, to the profession, and to the community"); AGA's 2012 Educator Award ("to recognize individuals who have made significant contributions to the education and training of government financial managers"); and AGA's 2006 Barr Award ("to recognize the cumulative achievements of private sector individuals who throughout their careers have served as a role model for others and who have consistently exhibited the highest personal and professional standards").



Fraud Happens

- Most organizations think it can't happen to them
- Then are devastated when it does
- ACFE consistently estimates that the average organization loses about 5% of its revenues due to fraud annually
  - Median loss from a single case: $150,000
  - 23% of cases studied resulted in losses of more than $1,000,000
  - Frauds are always devastating and sometimes catastrophic

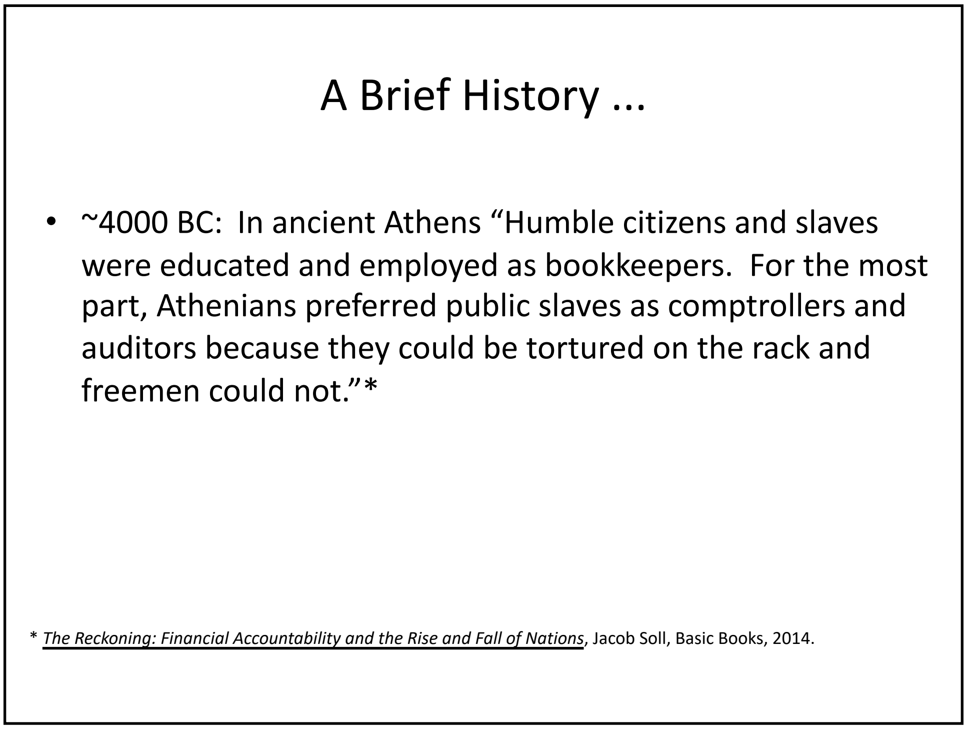


Fraud Risk Management and Assessment

- Fraud Risk Management's Historical Context
- Fraud Risk Management and the 2013 COSO Internal Control Framework
- The COSO/ACFE Fraud Risk Management Guide
  - Governance and the Control Environment
  - Fraud Risk Assessment
  - Fraud Control Activities
  - Information, Investigation, and Reporting
  - Monitoring
- My Predictions for the Future: What Can/Should Be Done to Empower Auditors to Find More Fraud; and Help Organizations Better Manage Fraud?

Historical Context

3



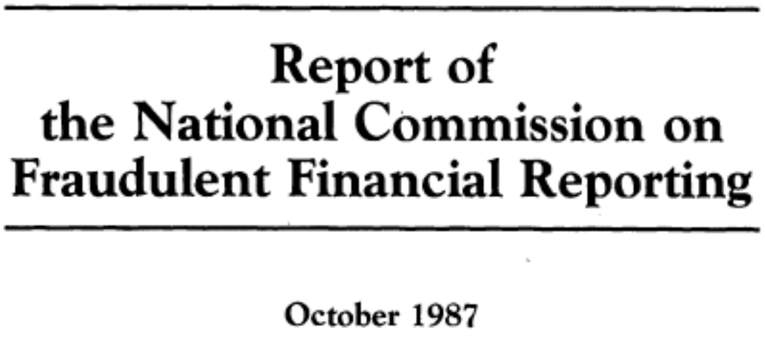
A Brief History ...

- ~4000 BC: In ancient Athens “Humble citizens and slaves were educated and employed as bookkeepers. For the most part, Athenians preferred public slaves as comptrollers and auditors because they could be tortured on the rack and freemen could not.”*

* _The Reckoning: Financial Accountability and the Rise and Fall of Nations_, Jacob Soll, Basic Books, 2014.

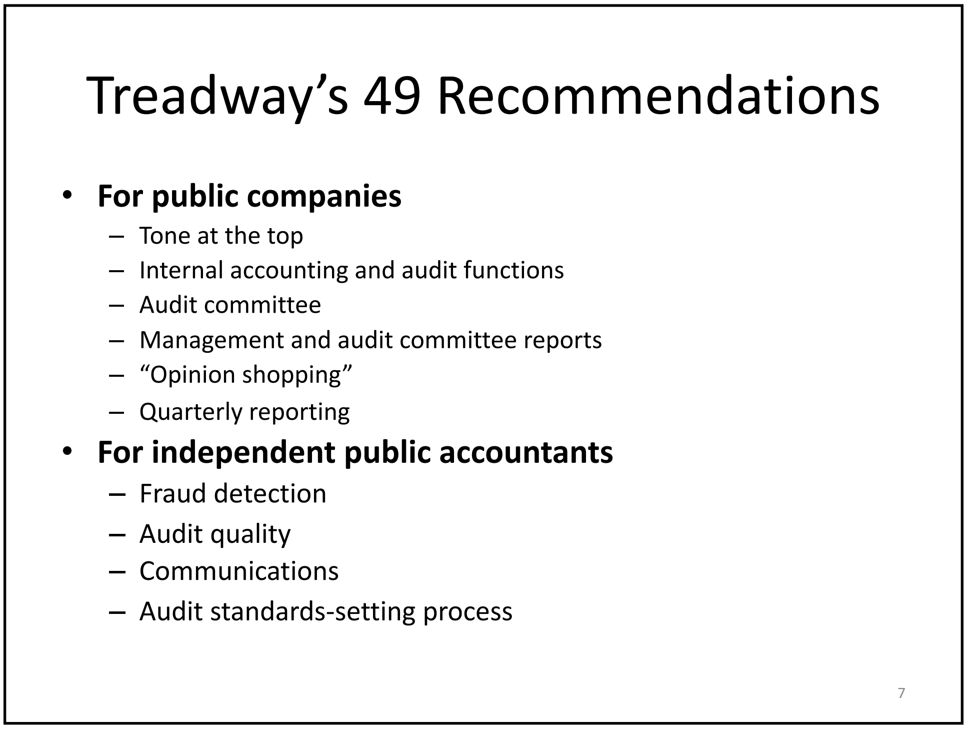
A Brief History ...

- 1985: The Committee of Sponsoring Organizations of the Treadway Commission was formed
  - American Institute of Certified Public Accountants (AICPA)
  - American Accounting Association (AAA)
  - Financial Executives Institute (FEI)
  - Institute of Internal Auditors (IIA)
  - National Association of Accountants (now the Institute of Management Accountants (IMA))



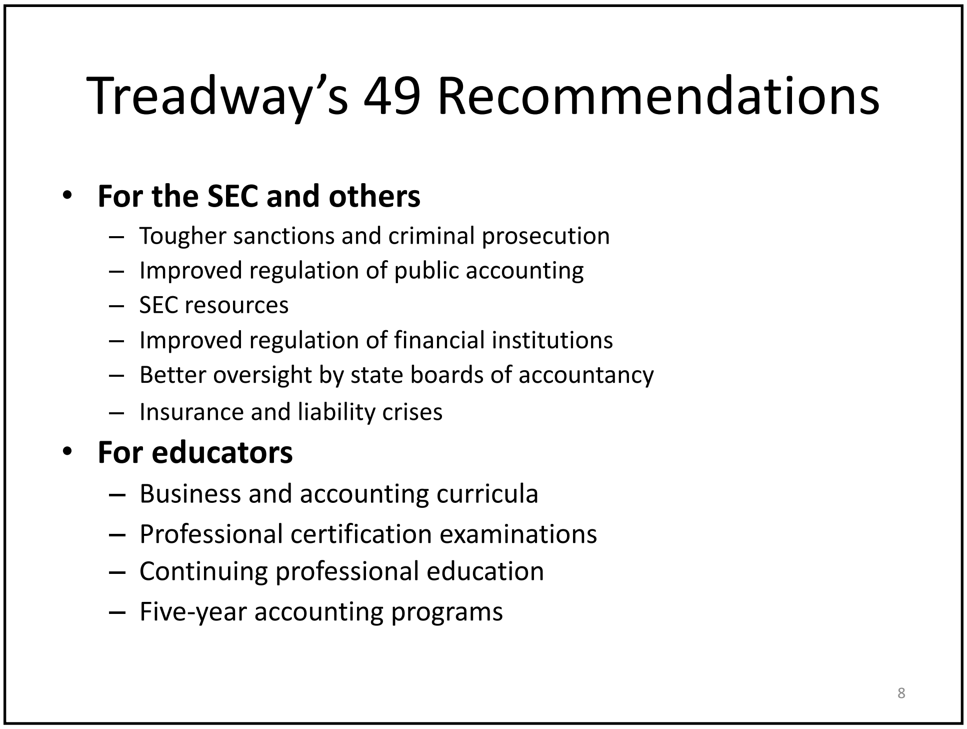
Report of
the National Commission on
Fraudulent Financial Reporting

October 1987



Treadway's 49 Recommendations

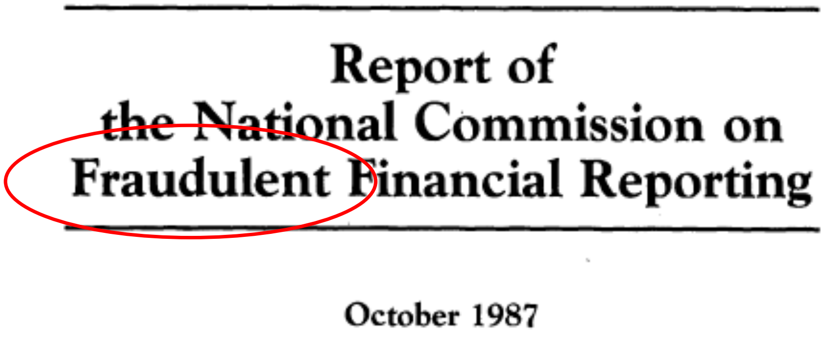
- **For public companies**
  - Tone at the top
  - Internal accounting and audit functions
  - Audit committee
  - Management and audit committee reports
  - "Opinion shopping"
  - Quarterly reporting
- **For independent public accountants**
  - Fraud detection
  - Audit quality
  - Communications
  - Audit standards-setting process



Treadway's 49 Recommendations

- **For the SEC and others**
  - Tougher sanctions and criminal prosecution
  - Improved regulation of public accounting
  - SEC resources
  - Improved regulation of financial institutions
  - Better oversight by state boards of accountancy
  - Insurance and liability crises
- **For educators**
  - Business and accounting curricula
  - Professional certification examinations
  - Continuing professional education
  - Five-year accounting programs

"Fraud" appears ***554*** times in the 183-page document.

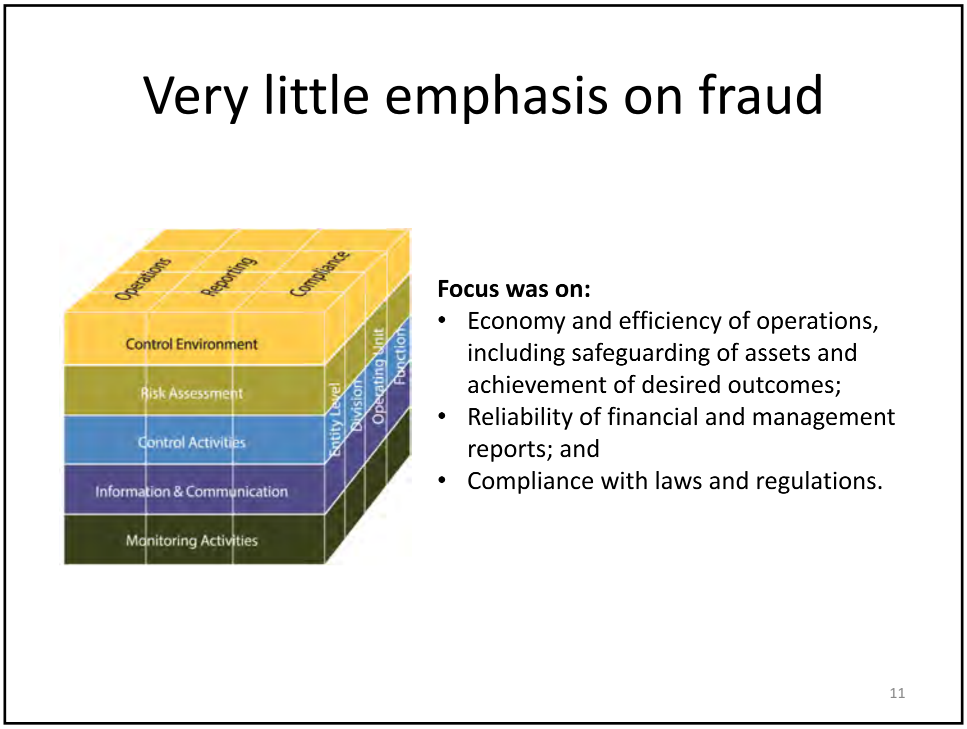


Report of
the National Commission on
Fraudulent Financial Reporting

October 1987

A Brief History ...

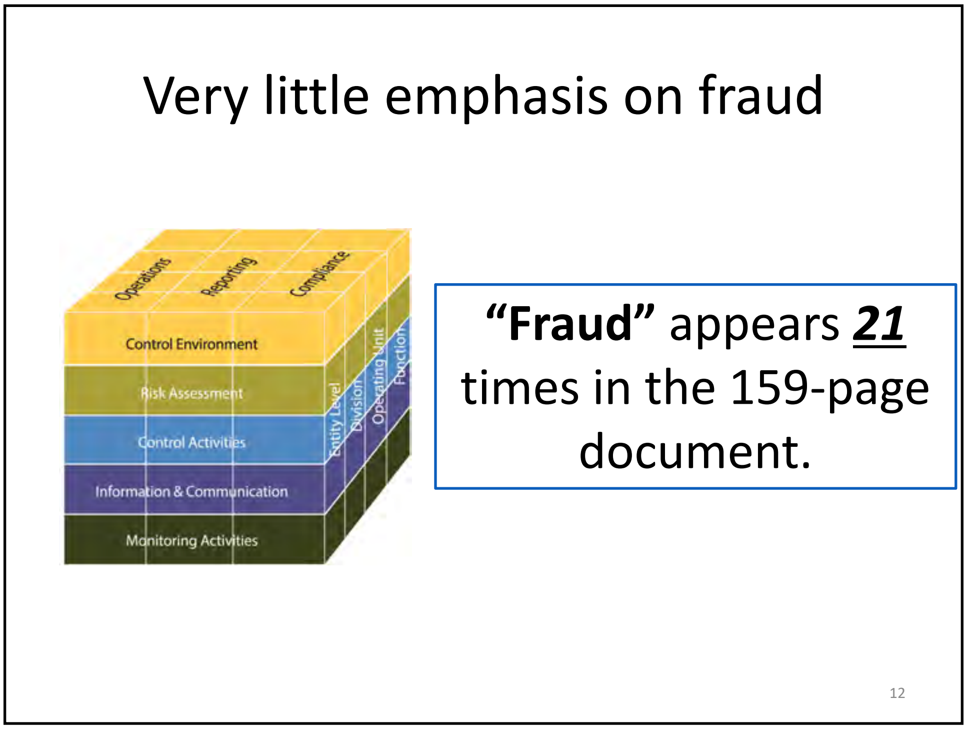
- 1987: The Treadway Commission declared victory and disbanded, but COSO carried on
- 1992: COSO issued its Internal Control—Integrated Framework



Very little emphasis on fraud

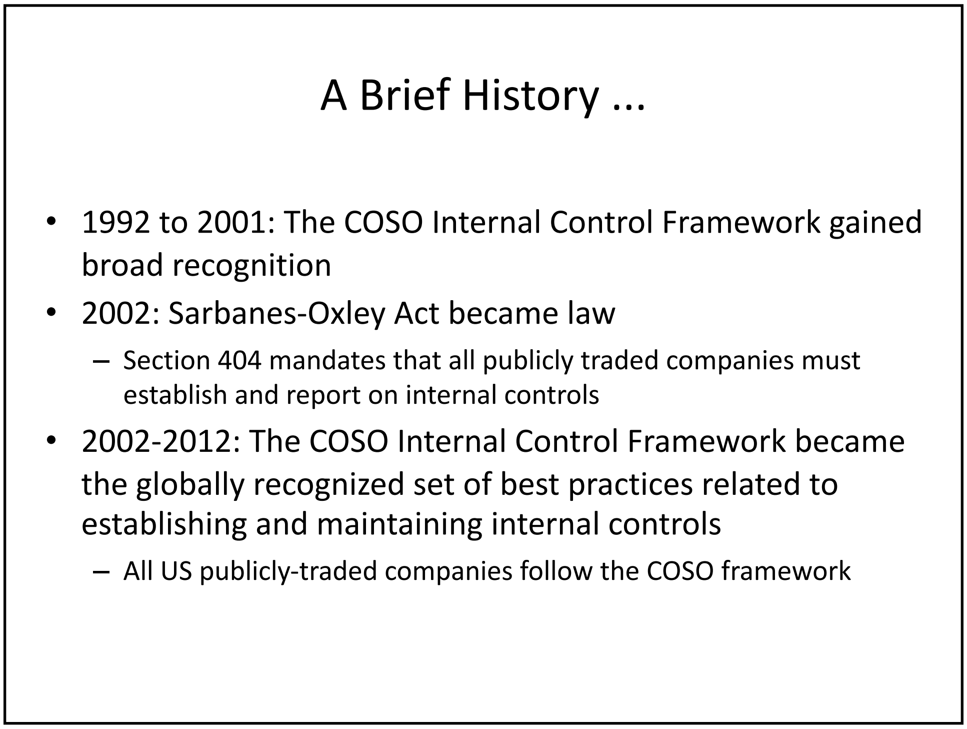
Focus was on:

- Economy and efficiency of operations, including safeguarding of assets and achievement of desired outcomes;
- Reliability of financial and management reports; and
- Compliance with laws and regulations.



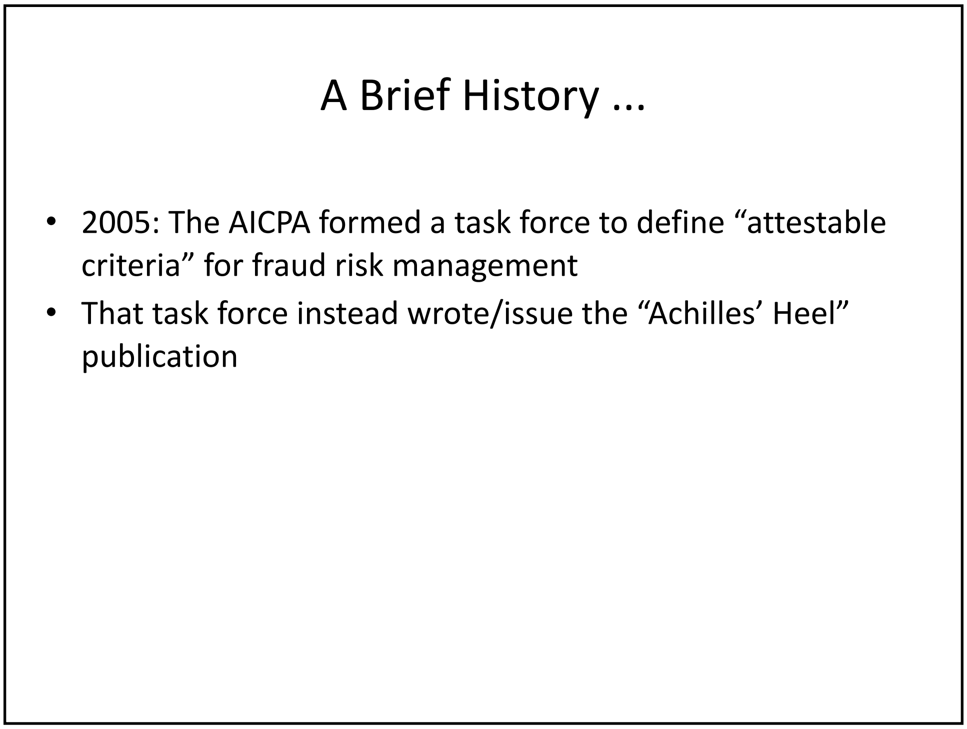
Very little emphasis on fraud

“Fraud” appears ***<u>21</u>*** times in the 159-page document.



A Brief History ...

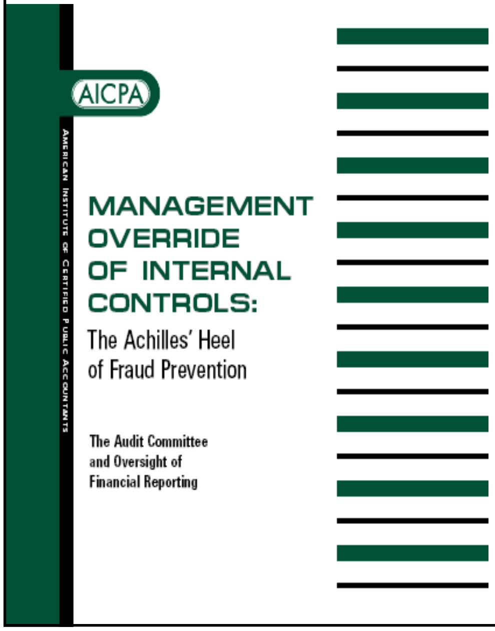
- 1992 to 2001: The COSO Internal Control Framework gained broad recognition
- 2002: Sarbanes-Oxley Act became law
  - Section 404 mandates that all publicly traded companies must establish and report on internal controls
- 2002-2012: The COSO Internal Control Framework became the globally recognized set of best practices related to establishing and maintaining internal controls
  - All US publicly-traded companies follow the COSO framework



A Brief History ...

- 2005: The AICPA formed a task force to define “attestable criteria” for fraud risk management
- That task force instead wrote/issue the “Achilles’ Heel” publication

Guidance for Audit Committees



AICPA

American Institute of Certified Public Accountants

MANAGEMENT OVERRIDE OF INTERNAL CONTROLS:

The Achilles' Heel of Fraud Prevention

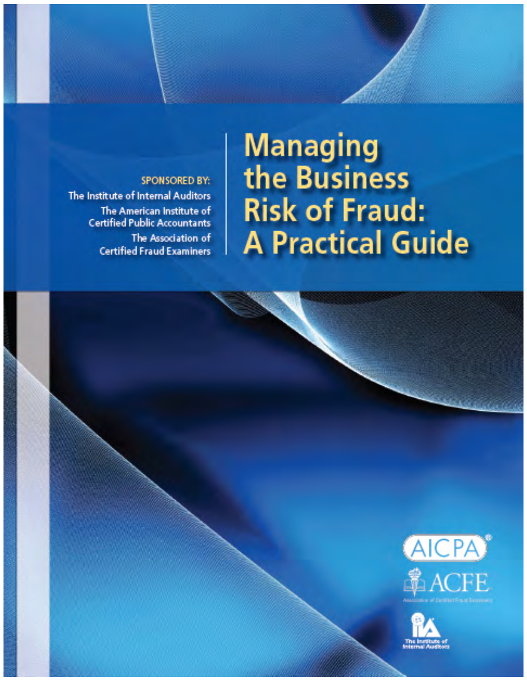
The Audit Committee and Oversight of Financial Reporting

FREE at:
http://www.cottoncpa.com/outreach/thought-leadership/

Published in 2005; updated in 2016

A Brief History ...

- 2007: An IIA, ACFE, AICPA Task Force published *Managing the Business Risk of Fraud—A Practical Guide* ("attestable criteria" for fraud risk management)



SPONSORED BY:
The Institute of Internal Auditors
The American Institute of Certified Public Accountants
The Association of Certified Fraud Examiners

Managing the Business Risk of Fraud: A Practical Guide

AICPA
ACFE
The Institute of Internal Auditors

FREE at: http://www.cottoncpa.com/wp-content/uploads/2014/08/ManagingTheBusinessRiskofFraud.pdf

Published in 2007

A Brief History ...

- May 2013: COSO updated its *Internal Control Integrated Framework* and added 17 Principles
  - Principle #8: *The organization considers the potential for fraud in assessing risks to the achievement of objectives.*

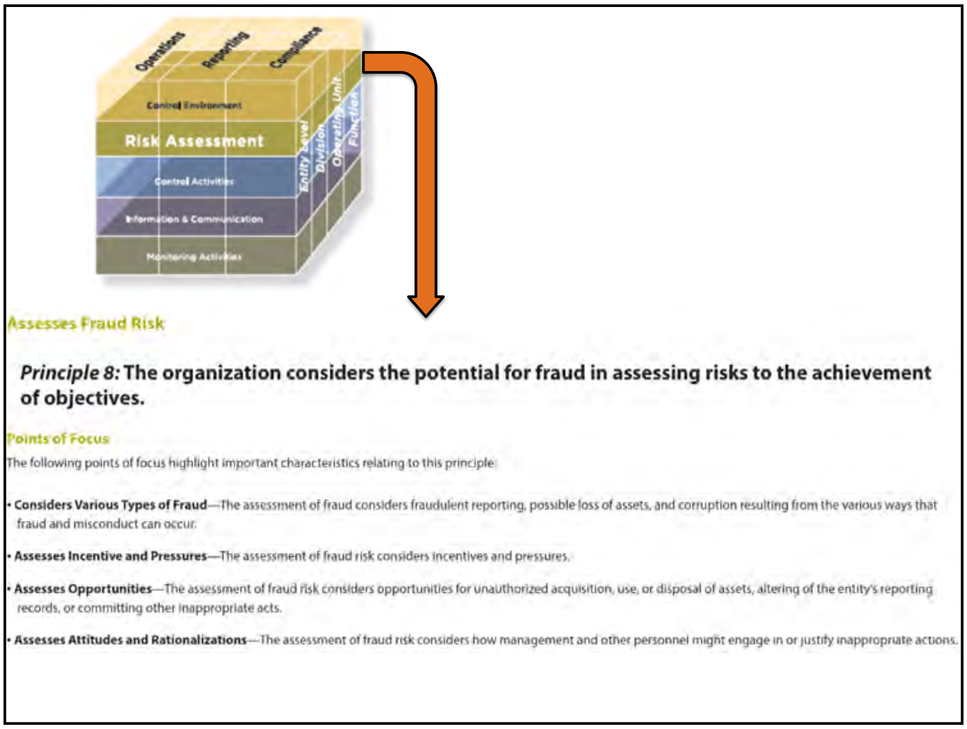
COSO

Committee of Sponsoring Organizations of the Treadway Commission

Internal Control — Integrated Framework

Executive Summary

May 2013



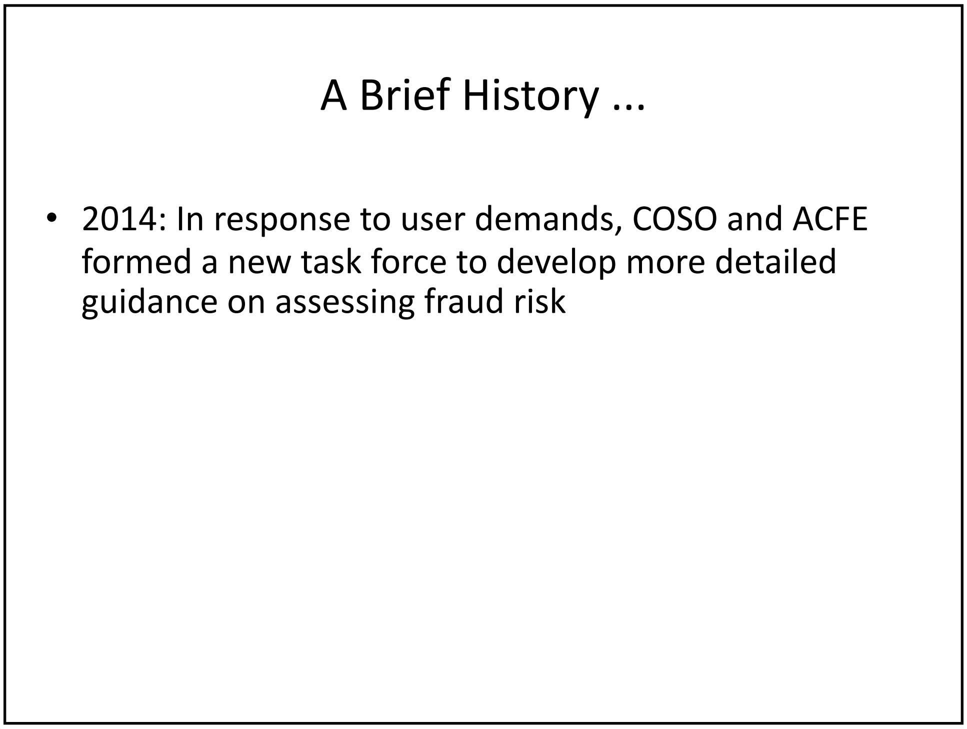
Assesses Fraud Risk

***Principle 8:* The organization considers the potential for fraud in assessing risks to the achievement of objectives.**

Points of Focus

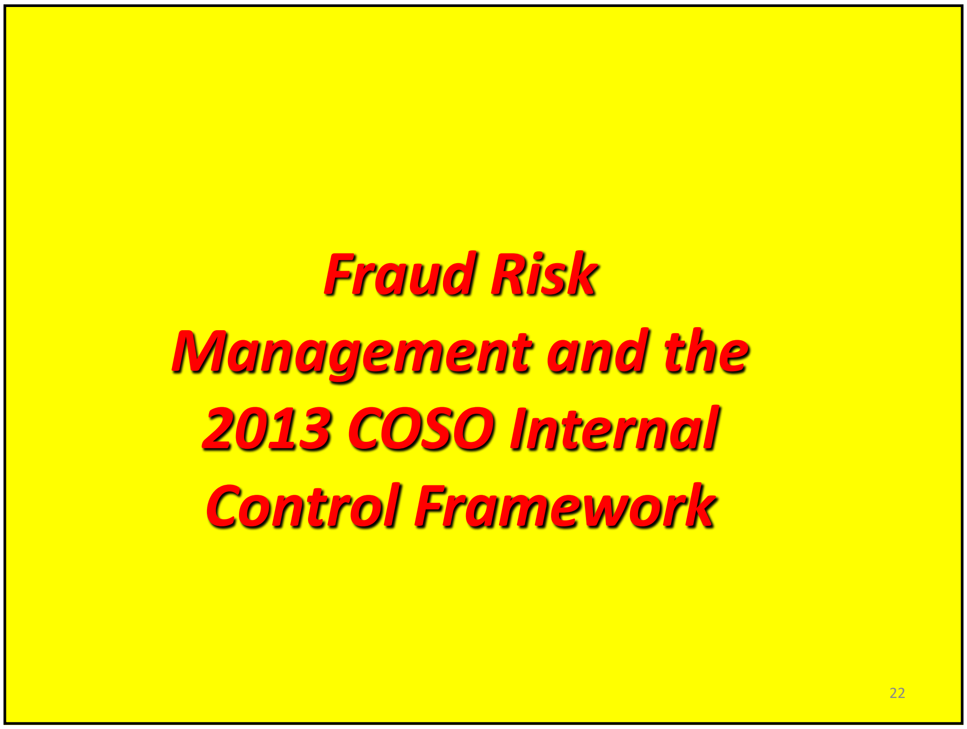
The following points of focus highlight important characteristics relating to this principle:

- **Considers Various Types of Fraud**—The assessment of fraud considers fraudulent reporting, possible loss of assets, and corruption resulting from the various ways that fraud and misconduct can occur.
- **Assesses Incentive and Pressures**—The assessment of fraud risk considers incentives and pressures.
- **Assesses Opportunities**—The assessment of fraud risk considers opportunities for unauthorized acquisition, use, or disposal of assets, altering of the entity's reporting records, or committing other inappropriate acts.
- **Assesses Attitudes and Rationalizations**—The assessment of fraud risk considers how management and other personnel might engage in or justify inappropriate actions.



A Brief History ...

- 2014: In response to user demands, COSO and ACFE formed a new task force to develop more detailed guidance on assessing fraud risk



Fraud Risk Management and the 2013 COSO Internal Control Framework

22

Joint ACFE-COSO Task Force

Barbara Andrews
AICPA

Michael Birdsall
Comcast Corporation

Toby Bishop
Formerly ACFE, Deloitte

Margot Cella
Center for Audit Quality

David Coderre
CAATS

David L. Cotton, ***Chair***
Cotton & Company LLP

James Dalkin
GAO

Ron Durkin
Durkin Forensic, Inc.

Bert Edwards
Formerly State Department

Frank Faist
Charter Communications

Eric Feldman
Affiliated Monitors, Inc.

Dan George
USAC

John D. Gill
ACFE

Leslye Givarz
Formerly AICPA, PCAOB

Cindi Hook
Comcast Corporation

Sandra K. Johnigan
Johnigan, PC

Bill Leone
Norton Rose Fulbright

Andi McNeal
ACFE

Linda Miller
GAO

Kemi Olateju
General Electric

Chris Pembroke
Crawford & Associates, PC

J. Michael Peppers
University of Texas

Kelly Richmond Pope
DePaul University

Carolyn Devine Saint
University of Virginia

Jeffrey Steinhoff
KPMG

William Titera
Formerly EY

Michael Ueltzen
Ueltzen & Company

Pamela Verick
Protiviti

Vincent Walden
EY

Bill Warren
PwC

Richard Woodford
U.S. Coast Guard
Investigative Service

Joint ACFE-COSO Advisory Panel

Dan Amiram
Columbia University Business School

Zahn Bozanic
The Ohio State University

Greg Brush
Tennessee Comptroller of Treasury

Tamia Buckingham
Massachusetts School Building Authority

Ashley L. Comer
James Madison University

Molly Dawson
Cotton & Company LLP

Eric Eisenstein
Cotton & Company LLP

Michael Justus
University of Nebraska

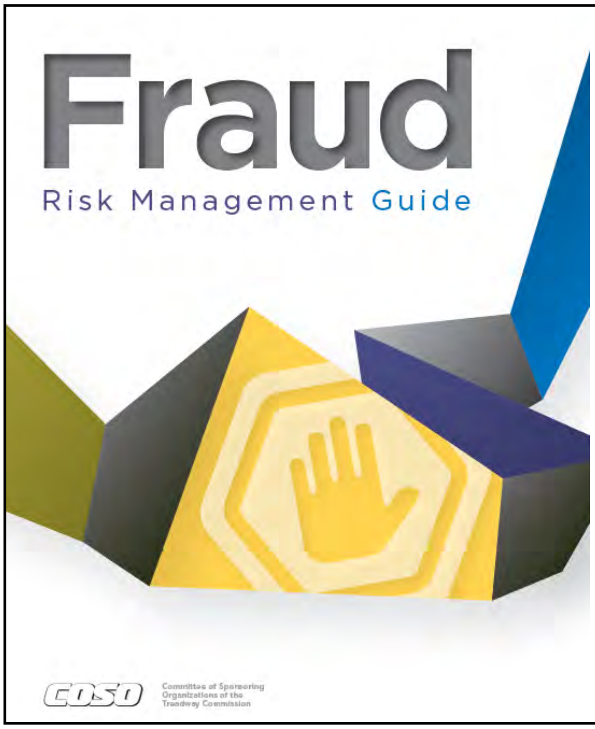
Theresa Nellis-Matson
New York Office of the State Comptroller

Jennifer Paperman
New York Office of the State Comptroller

Daniel Rossi
New York Office of the State Comptroller

Lynda Harbold Schwartz
Upland Advisory LLC

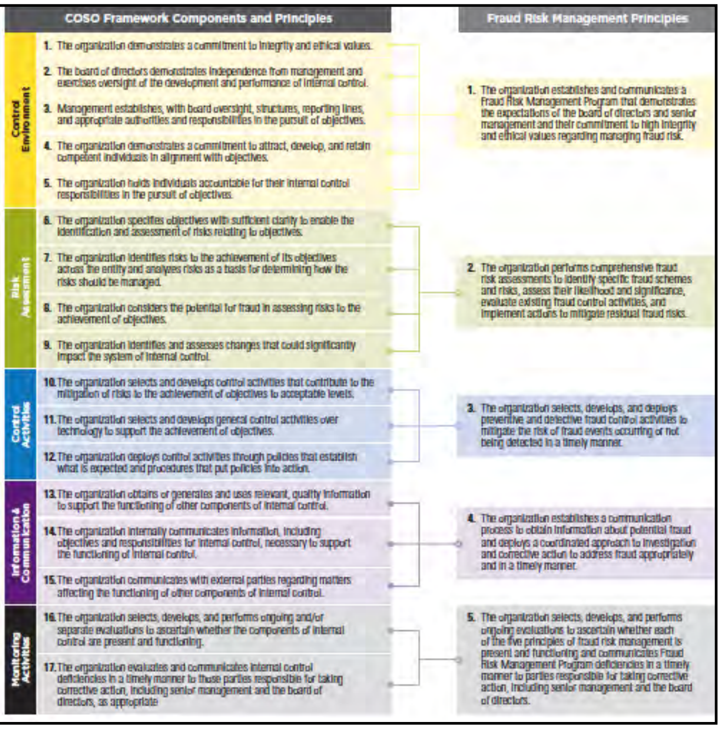
Rosie Tomforde
Regional Government


Fraud
Risk Management Guide
COSO
Committee of Sponsoring Organizations of the Treadway Commission

Buy the Guide at COSO or ACFE web sites ($69; $59 for members) Executive Summary is FREE at http://www.cottoncpa.com/outreach/thought-leadership/

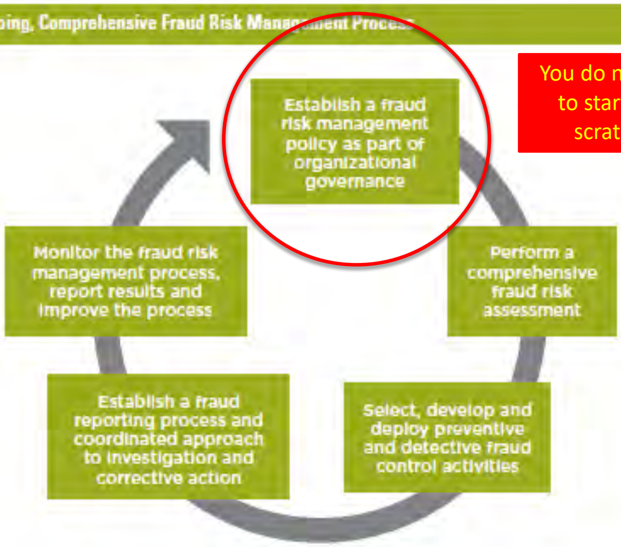
The COSO/ACFE Fraud Risk Management Guide

Mapping of COSO Components and Principles to the Fraud Risk Management Guide

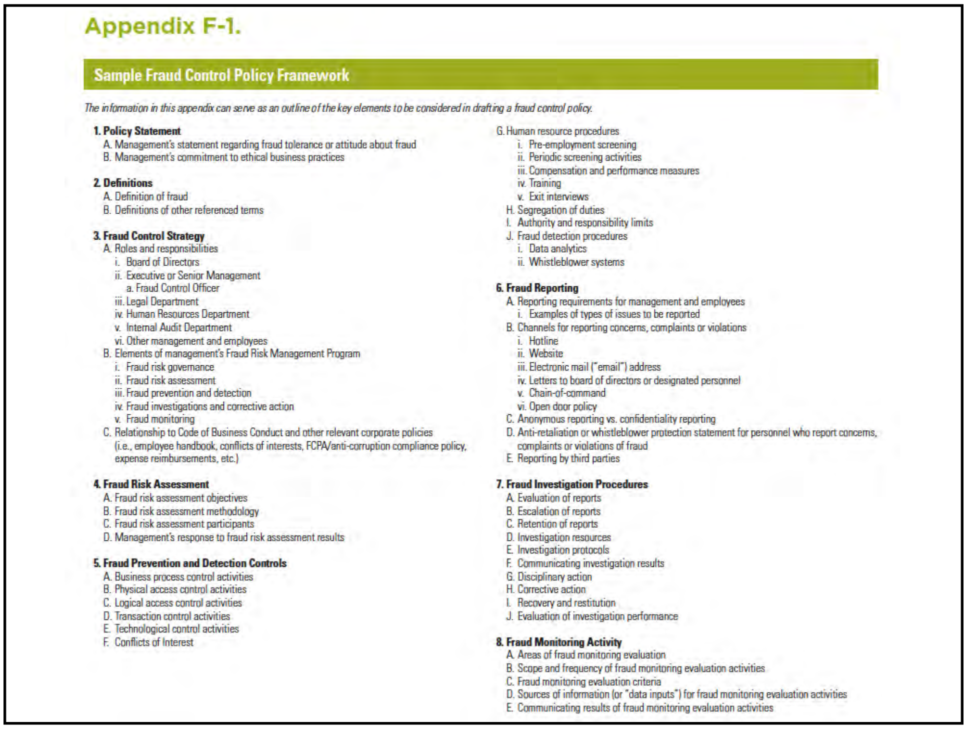


	COSO Framework Components and Principles	Fraud Risk Management Principles
Control Environment	1. The organization demonstrates a commitment to integrity and ethical values.	1. The organization establishes and communicates a Fraud Risk Management Program that demonstrates the expectations of the board of directors and senior management and their commitment to high integrity and ethical values regarding managing fraud risk.
	2. The board of directors demonstrates independence from management and exercises oversight of the development and performance of internal control.	
	3. Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives.	
	4. The organization demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.	
	5. The organization holds individuals accountable for their internal control responsibilities in the pursuit of objectives.	
Risk Assessment	6. The organization specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives.	2. The organization performs comprehensive fraud risk assessments to identify specific fraud schemes and risks, assess their likelihood and significance, evaluate existing fraud control activities, and implement actions to mitigate residual fraud risks.
	7. The organization identifies risks to the achievement of its objectives across the entity and analyzes risks as a basis for determining how the risks should be managed.	
	8. The organization considers the potential for fraud in assessing risks to the achievement of objectives.	
	9. The organization identifies and assesses changes that could significantly impact the system of internal control.	
Control Activities	10. The organization selects and develops control activities that contribute to the mitigation of risks to the achievement of objectives to acceptable levels.	3. The organization selects, develops, and deploys preventive and detective fraud control activities to mitigate the risk of fraud events occurring or not being detected in a timely manner.
	11. The organization selects and develops general control activities over technology to support the achievement of objectives.	
	12. The organization deploys control activities through policies that establish what is expected and procedures that put policies into action.	
Information & Communication	13. The organization obtains or generates and uses relevant, quality information to support the functioning of other components of internal control.	4. The organization establishes a communication process to obtain information about potential fraud and deploys a coordinated approach to investigation and corrective action to address fraud appropriately and in a timely manner.
	14. The organization internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.	
	15. The organization communicates with external parties regarding matters affecting the functioning of other components of internal control.	
Monitoring Activities	16. The organization selects, develops, and performs ongoing and/or separate evaluations to ascertain whether the components of internal control are present and functioning.	5. The organization selects, develops, and performs ongoing evaluations to ascertain whether each of the five principles of fraud risk management is present and functioning and communicates Fraud Risk Management Program deficiencies in a timely manner to parties responsible for taking corrective action, including senior management and the board of directors.
	17. The organization evaluates and communicates internal control deficiencies in a timely manner to those parties responsible for taking corrective action, including senior management and the board of directors, as appropriate	

Figure 1. Ongoing, Comprehensive Fraud Risk Management Process


Establish a fraud risk management policy as part of organizational governance
Perform a comprehensive fraud risk assessment
Select, develop and deploy preventive and detective fraud control activities
Establish a fraud reporting process and coordinated approach to investigation and corrective action
Monitor the fraud risk management process, report results and improve the process

You do not need to start from scratch …



Appendix F-1.

Sample Fraud Control Policy Framework

The information in this appendix can serve as an outline of the key elements to be considered in drafting a fraud control policy.

1. Policy Statement
- A. Management's statement regarding fraud tolerance or attitude about fraud
- B. Management's commitment to ethical business practices

2. Definitions
- A. Definition of fraud
- B. Definitions of other referenced terms

3. Fraud Control Strategy
- A. Roles and responsibilities
  - i. Board of Directors
  - ii. Executive or Senior Management
    - a. Fraud Control Officer
  - iii. Legal Department
  - iv. Human Resources Department
  - v. Internal Audit Department
  - vi. Other management and employees
- B. Elements of management's Fraud Risk Management Program
  - i. Fraud risk governance
  - ii. Fraud risk assessment
  - iii. Fraud prevention and detection
  - iv. Fraud investigations and corrective action
  - v. Fraud monitoring
- C. Relationship to Code of Business Conduct and other relevant corporate policies (i.e., employee handbook, conflicts of interests, FCPA/anti-corruption compliance policy, expense reimbursements, etc.)

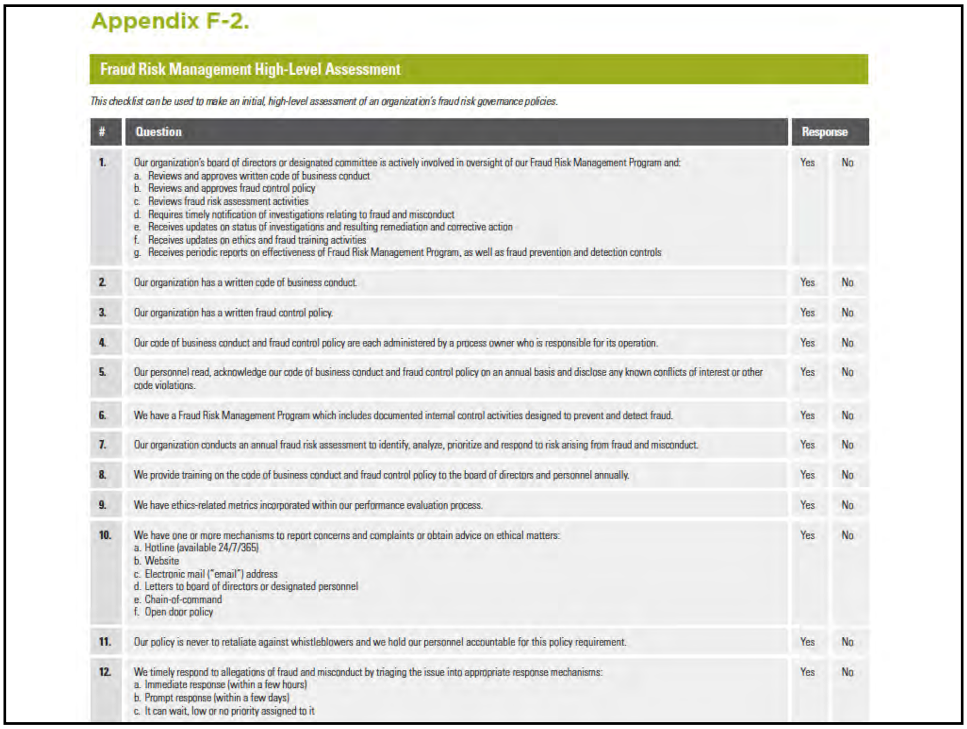
4. Fraud Risk Assessment
- A. Fraud risk assessment objectives
- B. Fraud risk assessment methodology
- C. Fraud risk assessment participants
- D. Management's response to fraud risk assessment results

5. Fraud Prevention and Detection Controls
- A. Business process control activities
- B. Physical access control activities
- C. Logical access control activities
- D. Transaction control activities
- E. Technological control activities
- F. Conflicts of Interest
- G. Human resource procedures
  - i. Pre-employment screening
  - ii. Periodic screening activities
  - iii. Compensation and performance measures
  - iv. Training
  - v. Exit interviews
- H. Segregation of duties
- I. Authority and responsibility limits
- J. Fraud detection procedures
  - i. Data analytics
  - ii. Whistleblower systems

6. Fraud Reporting
- A. Reporting requirements for management and employees
  - i. Examples of types of issues to be reported
- B. Channels for reporting concerns, complaints or violations
  - i. Hotline
  - ii. Website
  - iii. Electronic mail ("email") address
  - iv. Letters to board of directors or designated personnel
  - v. Chain-of-command
  - vi. Open door policy
- C. Anonymous reporting vs. confidentiality reporting
- D. Anti-retaliation or whistleblower protection statement for personnel who report concerns, complaints or violations of fraud
- E. Reporting by third parties

7. Fraud Investigation Procedures
- A. Evaluation of reports
- B. Escalation of reports
- C. Retention of reports
- D. Investigation resources
- E. Investigation protocols
- F. Communicating investigation results
- G. Disciplinary action
- H. Corrective action
- I. Recovery and restitution
- J. Evaluation of investigation performance

8. Fraud Monitoring Activity
- A. Areas of fraud monitoring evaluation
- B. Scope and frequency of fraud monitoring evaluation activities
- C. Fraud monitoring evaluation criteria
- D. Sources of information (or "data inputs") for fraud monitoring evaluation activities
- E. Communicating results of fraud monitoring evaluation activities

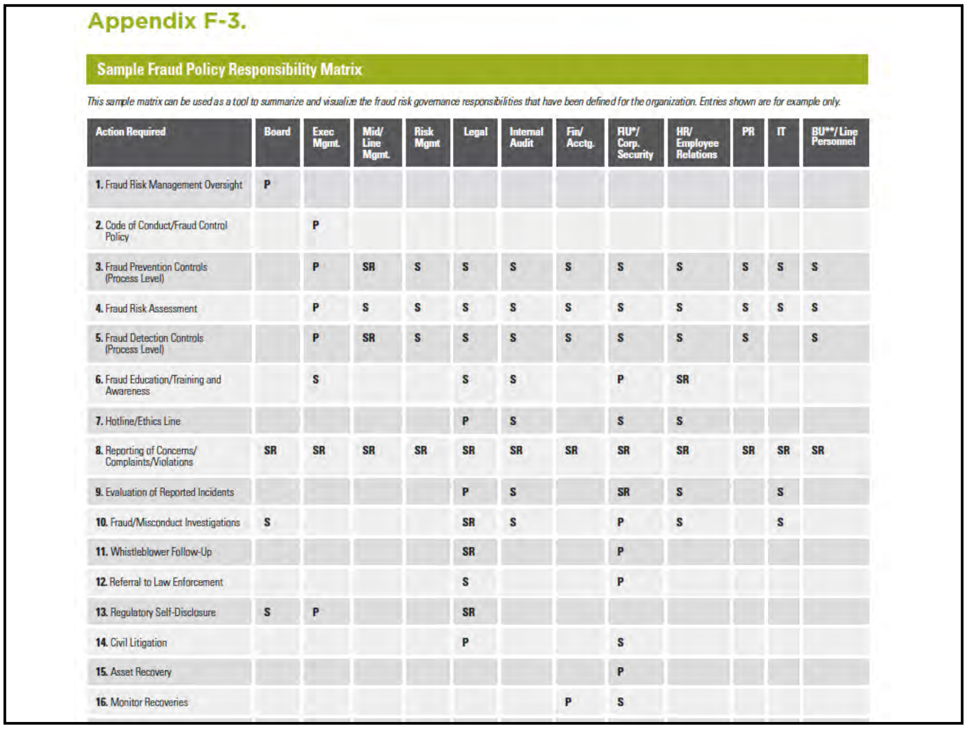


Appendix F-2.

Fraud Risk Management High-Level Assessment

This checklist can be used to make an initial, high-level assessment of an organization's fraud risk governance policies.

#	Question	Response	
1.	Our organization's board of directors or designated committee is actively involved in oversight of our Fraud Risk Management Program and: a. Reviews and approves written code of business conduct b. Reviews and approves fraud control policy c. Reviews fraud risk assessment activities d. Requires timely notification of investigations relating to fraud and misconduct e. Receives updates on status of investigations and resulting remediation and corrective action f. Receives updates on ethics and fraud training activities g. Receives periodic reports on effectiveness of Fraud Risk Management Program, as well as fraud prevention and detection controls	Yes	No
2.	Our organization has a written code of business conduct.	Yes	No
3.	Our organization has a written fraud control policy.	Yes	No
4.	Our code of business conduct and fraud control policy are each administered by a process owner who is responsible for its operation.	Yes	No
5.	Our personnel read, acknowledge our code of business conduct and fraud control policy on an annual basis and disclose any known conflicts of interest or other code violations.	Yes	No
6.	We have a Fraud Risk Management Program which includes documented internal control activities designed to prevent and detect fraud.	Yes	No
7.	Our organization conducts an annual fraud risk assessment to identify, analyze, prioritize and respond to risk arising from fraud and misconduct.	Yes	No
8.	We provide training on the code of business conduct and fraud control policy to the board of directors and personnel annually.	Yes	No
9.	We have ethics-related metrics incorporated within our performance evaluation process.	Yes	No
10.	We have one or more mechanisms to report concerns and complaints or obtain advice on ethical matters: a. Hotline (available 24/7/365) b. Website c. Electronic mail ("email") address d. Letters to board of directors or designated personnel e. Chain-of-command f. Open door policy	Yes	No
11.	Our policy is never to retaliate against whistleblowers and we hold our personnel accountable for this policy requirement.	Yes	No
12.	We timely respond to allegations of fraud and misconduct by triaging the issue into appropriate response mechanisms: a. Immediate response (within a few hours) b. Prompt response (within a few days) c. It can wait, low or no priority assigned to it	Yes	No

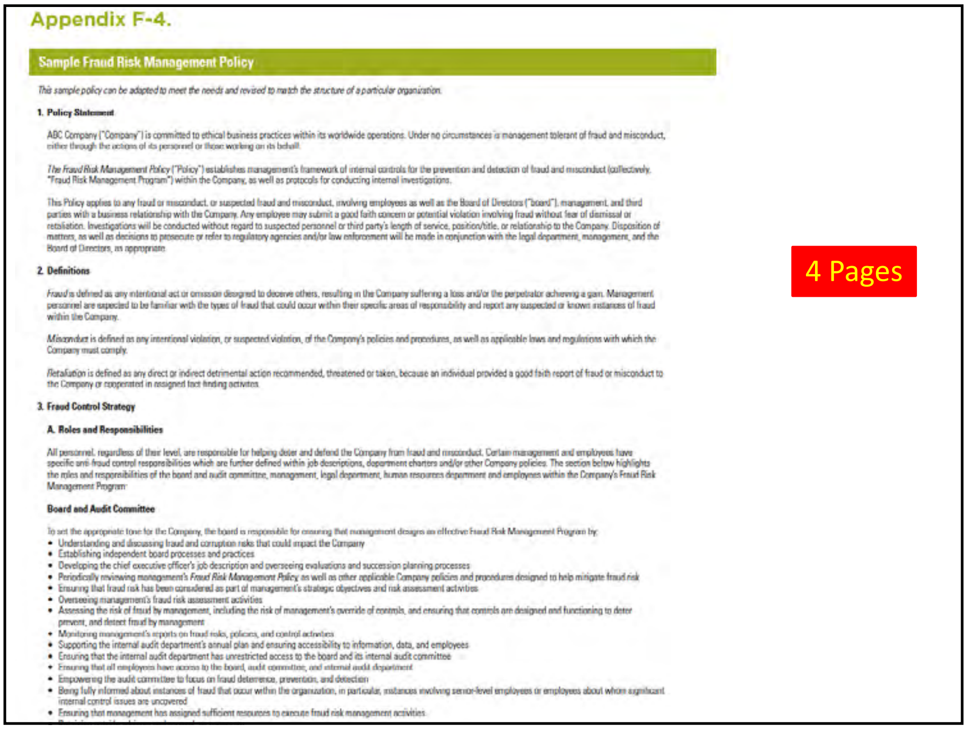


Appendix F-3.

Sample Fraud Policy Responsibility Matrix

This sample matrix can be used as a tool to summarize and visualize the fraud risk governance responsibilities that have been defined for the organization. Entries shown are for example only.

Action Required	Board	Exec Mgmt.	Mid/ Line Mgmt.	Risk Mgmt	Legal	Internal Audit	Fin/ Acctg.	FIU*/ Corp. Security	HR/ Employee Relations	PR	IT	BU**/ Line Personnel
1. Fraud Risk Management Oversight	P											
2. Code of Conduct/Fraud Control Policy		P										
3. Fraud Prevention Controls (Process Level)		P	SR	S	S	S	S	S	S	S	S	S
4. Fraud Risk Assessment		P	S	S	S	S	S	S	S	S	S	S
5. Fraud Detection Controls (Process Level)		P	SR	S	S	S	S	S	S	S		S
6. Fraud Education/Training and Awareness		S			S	S		P	SR			
7. Hotline/Ethics Line					P	S		S	S			
8. Reporting of Concerns/ Complaints/Violations	SR	SR	SR	SR	SR	SR	SR	SR	SR	SR	SR	SR
9. Evaluation of Reported Incidents					P	S		SR	S		S	
10. Fraud/Misconduct Investigations	S				SR	S		P	S		S	
11. Whistleblower Follow-Up					SR			P				
12. Referral to Law Enforcement					S			P				
13. Regulatory Self-Disclosure	S	P			SR							
14. Civil Litigation					P			S				
15. Asset Recovery								P				
16. Monitor Recoveries							P	S				



Appendix F-4.

Sample Fraud Risk Management Policy

This sample policy can be adapted to meet the needs and revised to match the structure of a particular organization.

1. Policy Statement

ABC Company ("Company") is committed to ethical business practices within its worldwide operations. Under no circumstances is management tolerant of fraud and misconduct, either through the actions of its personnel or those working on its behalf.

The Fraud Risk Management Policy ("Policy") establishes management's framework of internal controls for the prevention and detection of fraud and misconduct (collectively, "Fraud Risk Management Program") within the Company, as well as protocols for conducting internal investigations.

This Policy applies to any fraud or misconduct, or suspected fraud and misconduct, involving employees as well as the Board of Directors ("board"), management, and third parties with a business relationship with the Company. Any employee may submit a good faith concern or potential violation involving fraud without fear of dismissal or retaliation. Investigations will be conducted without regard to suspected personnel or third party's length of service, position/title, or relationship to the Company. Disposition of matters, as well as decisions to prosecute or refer to regulatory agencies and/or law enforcement will be made in conjunction with the legal department, management, and the Board of Directors, as appropriate.

2. Definitions

Fraud is defined as any intentional act or omission designed to deceive others, resulting in the Company suffering a loss and/or the perpetrator achieving a gain. Management personnel are expected to be familiar with the types of fraud that could occur within their specific areas of responsibility and report any suspected or known instances of fraud within the Company.

Misconduct is defined as any intentional violation, or suspected violation, of the Company's policies and procedures, as well as applicable laws and regulations with which the Company must comply.

Retaliation is defined as any direct or indirect detrimental action recommended, threatened or taken, because an individual provided a good faith report of fraud or misconduct to the Company or cooperated in assigned fact finding activites.

3. Fraud Control Strategy

A. Roles and Responsibilities

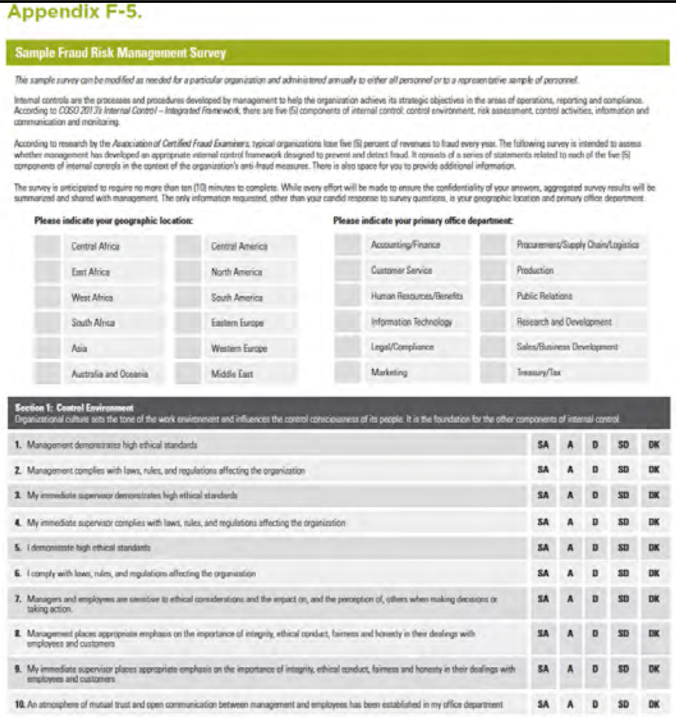
All personnel, regardless of their level, are responsible for helping deter and defend the Company from fraud and misconduct. Certain management and employees have specific anti-fraud control responsibilities which are further defined within job descriptions, department charters and/or other Company policies. The section below highlights the roles and responsibilities of the board and audit committee, management, legal department, human resources department and employees within the Company's Fraud Risk Management Program:

Board and Audit Committee

To set the appropriate tone for the Company, the board is responsible for ensuring that management designs an effective Fraud Risk Management Program by:

- Understanding and discussing fraud and corruption risks that could impact the Company
- Establishing independent board processes and practices
- Developing the chief executive officer's job description and overseeing evaluations and succession planning processes
- Periodically reviewing management's *Fraud Risk Management Policy*, as well as other applicable Company policies and procedures designed to help mitigate fraud risk
- Ensuring that fraud risk has been considered as part of management's strategic objectives and risk assessment activities
- Overseeing management's fraud risk assessment activities
- Assessing the risk of fraud by management, including the risk of management's override of controls, and ensuring that controls are designed and functioning to deter prevent, and detect fraud by management
- Monitoring management's reports on fraud risks, policies, and control activities
- Supporting the internal audit department's annual plan and ensuring accessibility to information, data, and employees
- Ensuring that the internal audit department has unrestricted access to the board and its internal audit committee
- Ensuring that all employees have access to the board, audit committee, and internal audit department
- Empowering the audit committee to focus on fraud deterrence, prevention, and detection
- Being fully informed about instances of fraud that occur within the organization, in particular, instances involving senior-level employees or employees about whom significant internal control issues are uncovered
- Ensuring that management has assigned sufficient resources to execute fraud risk management activities

4 Pages



Appendix F-5.

Sample Fraud Risk Management Survey

This sample survey can be modified as needed for a particular organization and administered annually to either all personnel or to a representative sample of personnel.

Internal controls are the processes and procedures developed by management to help the organization achieve its strategic objectives in the areas of operations, reporting and compliance. According to *COSO 2013's Internal Control – Integrated Framework*, there are five (5) components of internal control: control environment, risk assessment, control activities, information and communication and monitoring.

According to research by the *Association of Certified Fraud Examiners*, typical organizations lose five (5) percent of revenues to fraud every year. The following survey is intended to assess whether management has developed an appropriate internal control framework designed to prevent and detect fraud. It consists of a series of statements related to each of the five (5) components of internal controls in the context of the organization's anti-fraud measures. There is also space for you to provide additional information.

The survey is anticipated to require no more than ten (10) minutes to complete. While every effort will be made to ensure the confidentiality of your answers, aggregated survey results will be summarized and shared with management. The only information requested, other than your candid response to survey questions, is your geographic location and primary office department.

Please indicate your geographic location:

□	Central Africa	□	Central America
□	East Africa	□	North America
□	West Africa	□	South America
□	South Africa	□	Eastern Europe
□	Asia	□	Western Europe
□	Australia and Oceania	□	Middle East

Please indicate your primary office department:

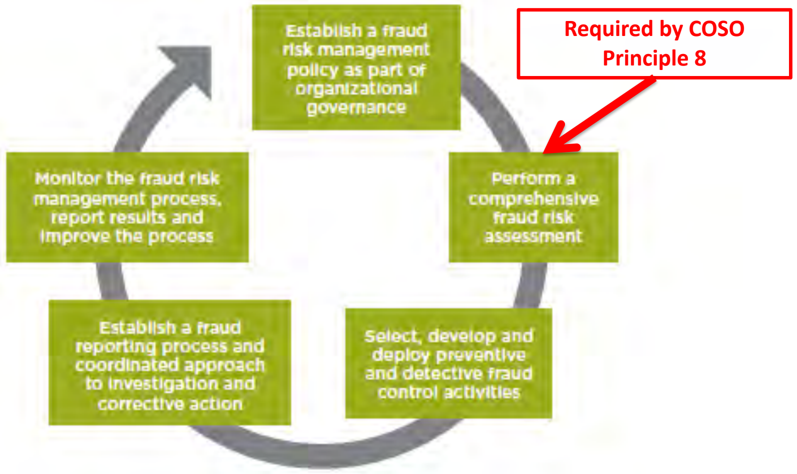
□	Accounting/Finance	□	Procurement/Supply Chain/Logistics
□	Customer Service	□	Production
□	Human Resources/Benefits	□	Public Relations
□	Information Technology	□	Research and Development
□	Legal/Compliance	□	Sales/Business Development
□	Marketing	□	Treasury/Tax

Section 1: Control Environment
Organizational culture sets the tone of the work environment and influences the control consciousness of its people. It is the foundation for the other components of internal control.

1. Management demonstrates high ethical standards	SA	A	D	SD	DK
2. Management complies with laws, rules, and regulations affecting the organization	SA	A	D	SD	DK
3. My immediate supervisor demonstrates high ethical standards	SA	A	D	SD	DK
4. My immediate supervisor complies with laws, rules, and regulations affecting the organization	SA	A	D	SD	DK
5. I demonstrate high ethical standards	SA	A	D	SD	DK
6. I comply with laws, rules, and regulations affecting the organization	SA	A	D	SD	DK
7. Managers and employees are sensitive to ethical considerations and the impact on, and the perception of, others when making decisions or taking action.	SA	A	D	SD	DK
8. Management places appropriate emphasis on the importance of integrity, ethical conduct, fairness and honesty in their dealings with employees and customers	SA	A	D	SD	DK
9. My immediate supervisor places appropriate emphasis on the importance of integrity, ethical conduct, fairness and honesty in their dealings with employees and customers	SA	A	D	SD	DK
10. An atmosphere of mutual trust and open communication between management and employees has been established in my office department	SA	A	D	SD	DK

4 Pages

Figure 1. Ongoing, Comprehensive Fraud Risk Management Process


Establish a fraud risk management policy as part of organizational governance
Perform a comprehensive fraud risk assessment
Select, develop and deploy preventive and detective fraud control activities
Establish a fraud reporting process and coordinated approach to investigation and corrective action
Monitor the fraud risk management process, report results and improve the process

Required by COSO Principle 8

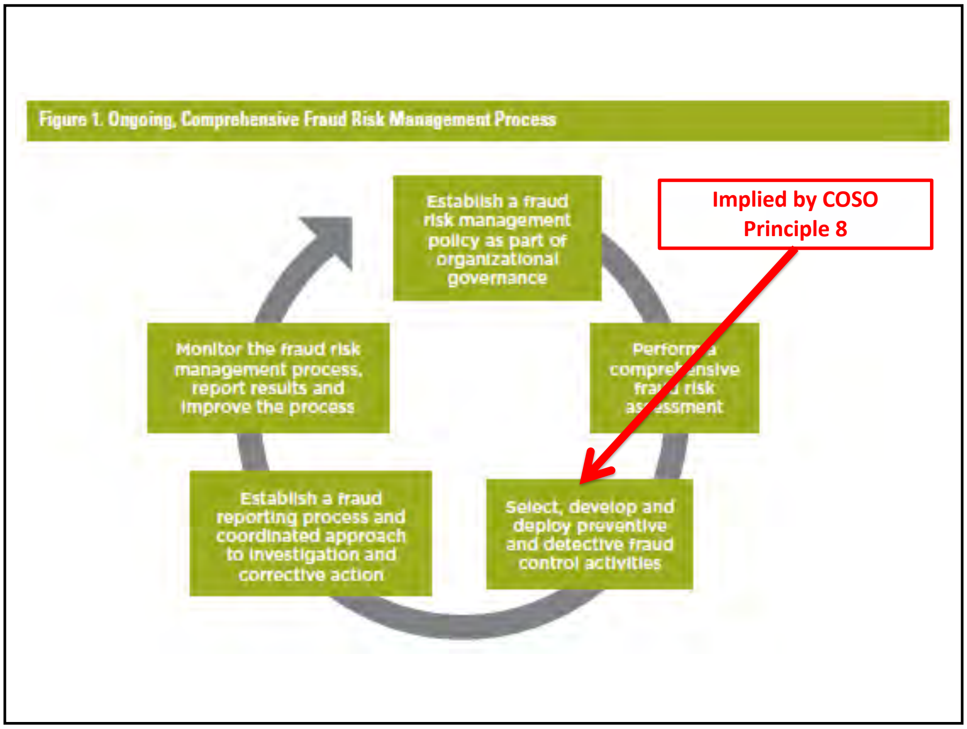


Figure 1. Ongoing, Comprehensive Fraud Risk Management Process

Establish a fraud risk management policy as part of organizational governance
Perform a comprehensive fraud risk assessment
Select, develop and deploy preventive and detective fraud control activities
Establish a fraud reporting process and coordinated approach to investigation and corrective action
Monitor the fraud risk management process, report results and improve the process

Implied by COSO Principle 8

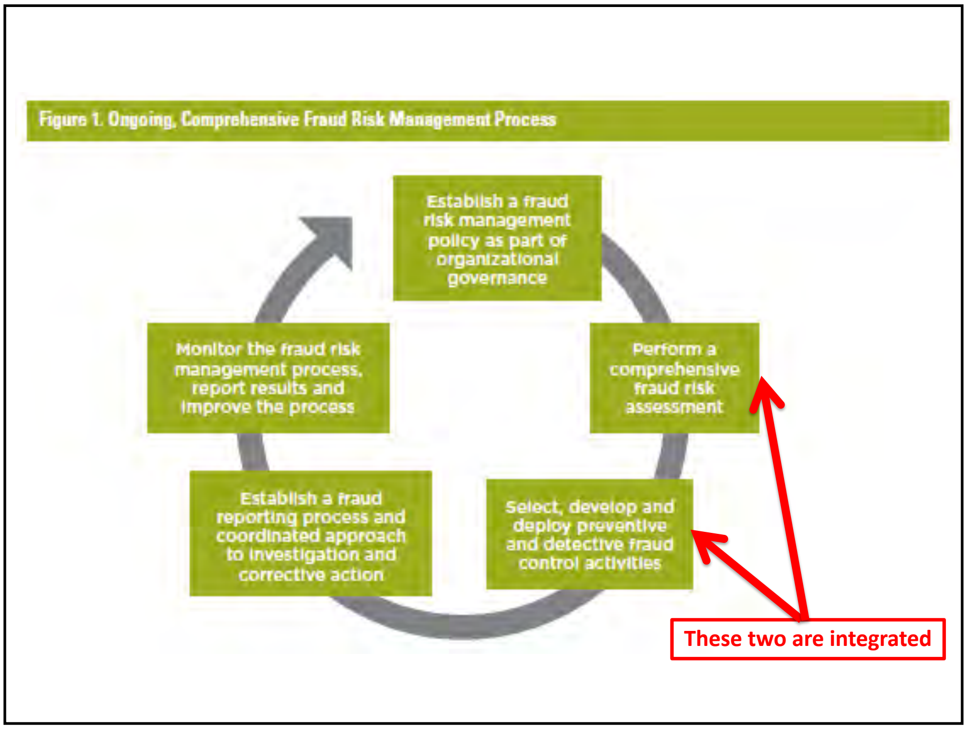


Figure 1. Ongoing, Comprehensive Fraud Risk Management Process

Establish a fraud risk management policy as part of organizational governance
Perform a comprehensive fraud risk assessment
Select, develop and deploy preventive and detective fraud control activities
Establish a fraud reporting process and coordinated approach to investigation and corrective action
Monitor the fraud risk management process, report results and improve the process

These two are integrated

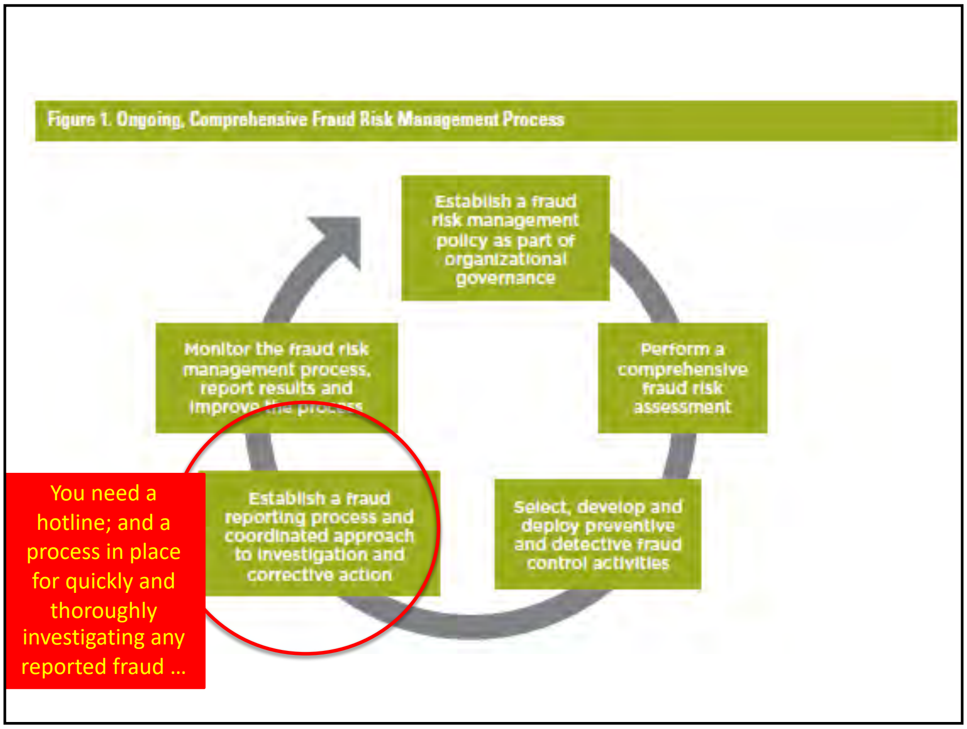


Figure 1. Ongoing, Comprehensive Fraud Risk Management Process

Establish a fraud risk management policy as part of organizational governance

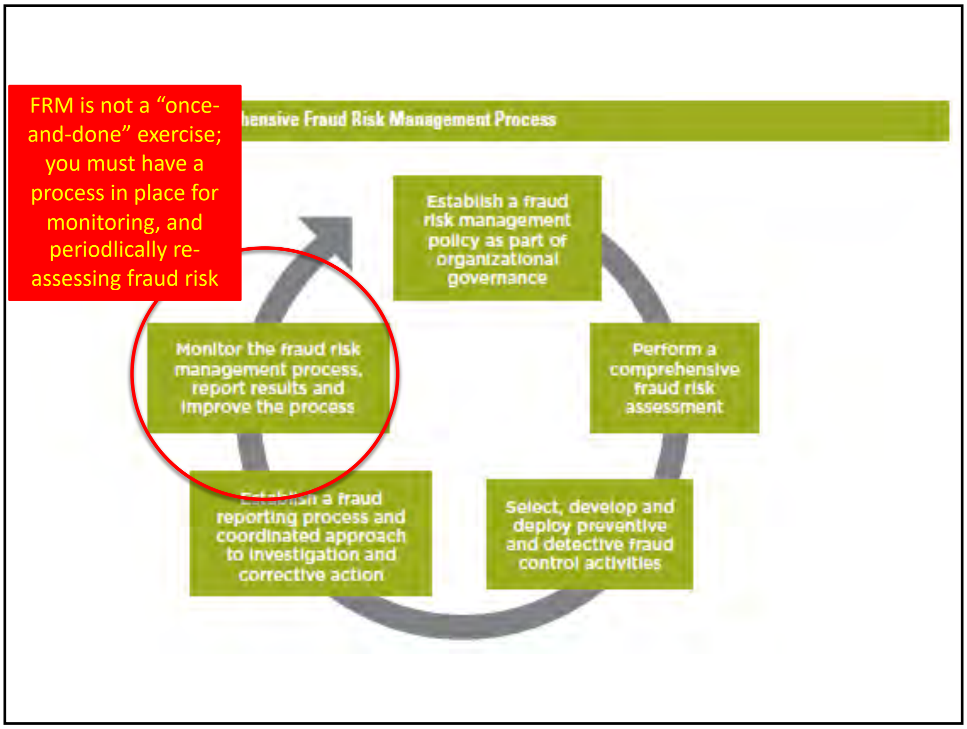
Perform a comprehensive fraud risk assessment

Select, develop and deploy preventive and detective fraud control activities

Establish a fraud reporting process and coordinated approach to investigation and corrective action

Monitor the fraud risk management process, report results and improve the process

You need a hotline; and a process in place for quickly and thoroughly investigating any reported fraud …



hensive Fraud Risk Management Process

FRM is not a “once-and-done” exercise; you must have a process in place for monitoring, and periodlically re-assessing fraud risk

Establish a fraud risk management policy as part of organizational governance

Perform a comprehensive fraud risk assessment

Select, develop and deploy preventive and detective fraud control activities

Establish a fraud reporting process and coordinated approach to investigation and corrective action

Monitor the fraud risk management process, report results and improve the process

Updated Guide Can Be Used:

- Just for complying with Principle #8—performing a fraud risk assessment, or
- For developing and implementing a comprehensive fraud risk management program

So, ….

You get to work one Monday morning and your boss says,

"Hey, we need to do a fraud risk assessment in order to comply with the new COSO Principle about fraud risk, and we want you to head up the effort to do that for us. Get started right away and report back when you are done."

So, ….

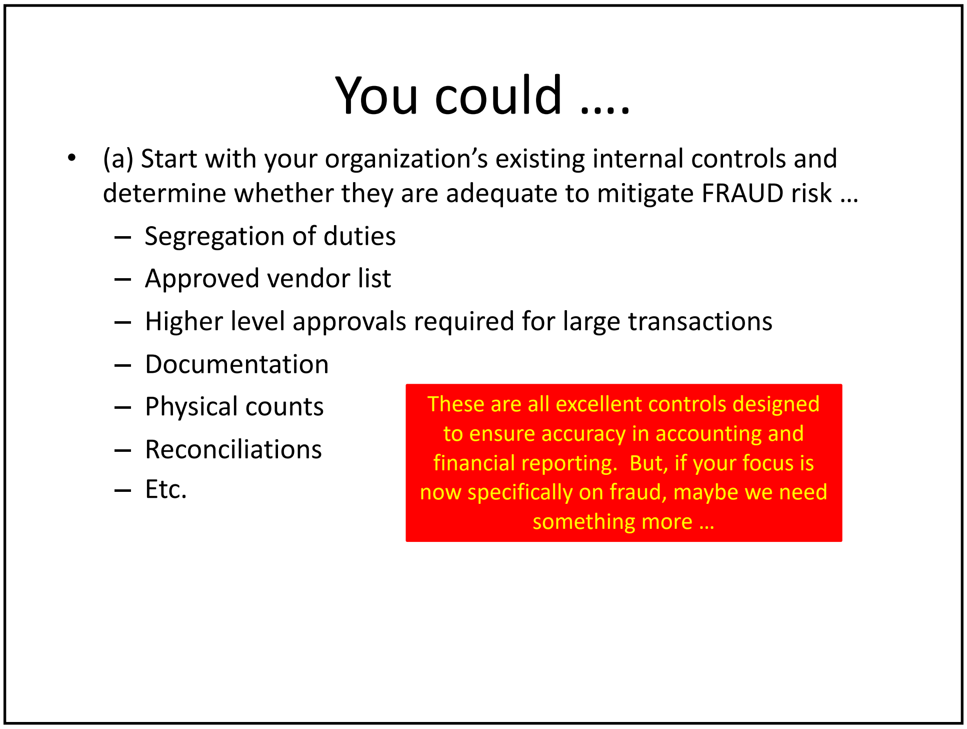
You get to work one Monday morning and your boss says,

"Hey, we need to do a fraud risk assessment in order to comply with the new COSO Principle about fraud risk, and we want you to head up the effort to do that for us. Get started right away and report back when you are done."

What would you do?

You could ….

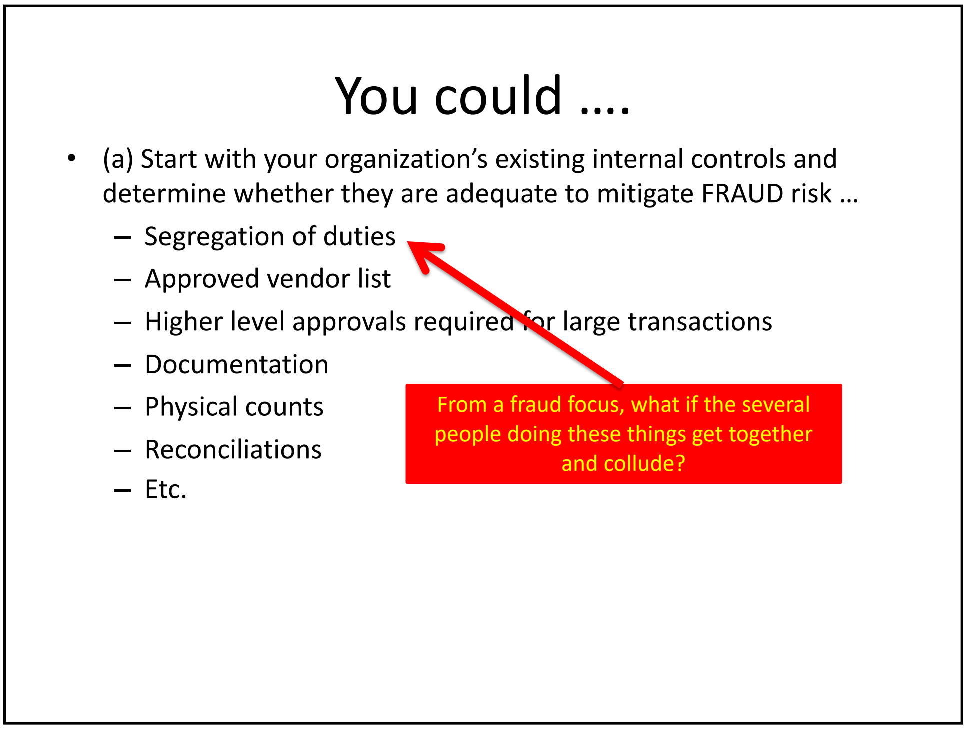
- (a) Start with your organization's existing internal controls and determine whether they are adequate to mitigate FRAUD risk …
  - Segregation of duties
  - Approved vendor list
  - Higher level approvals required for large transactions
  - Documentation
  - Physical counts
  - Reconciliations
  - Etc.



You could ….

- (a) Start with your organization’s existing internal controls and determine whether they are adequate to mitigate FRAUD risk …
  - Segregation of duties
  - Approved vendor list
  - Higher level approvals required for large transactions
  - Documentation
  - Physical counts
  - Reconciliations
  - Etc.

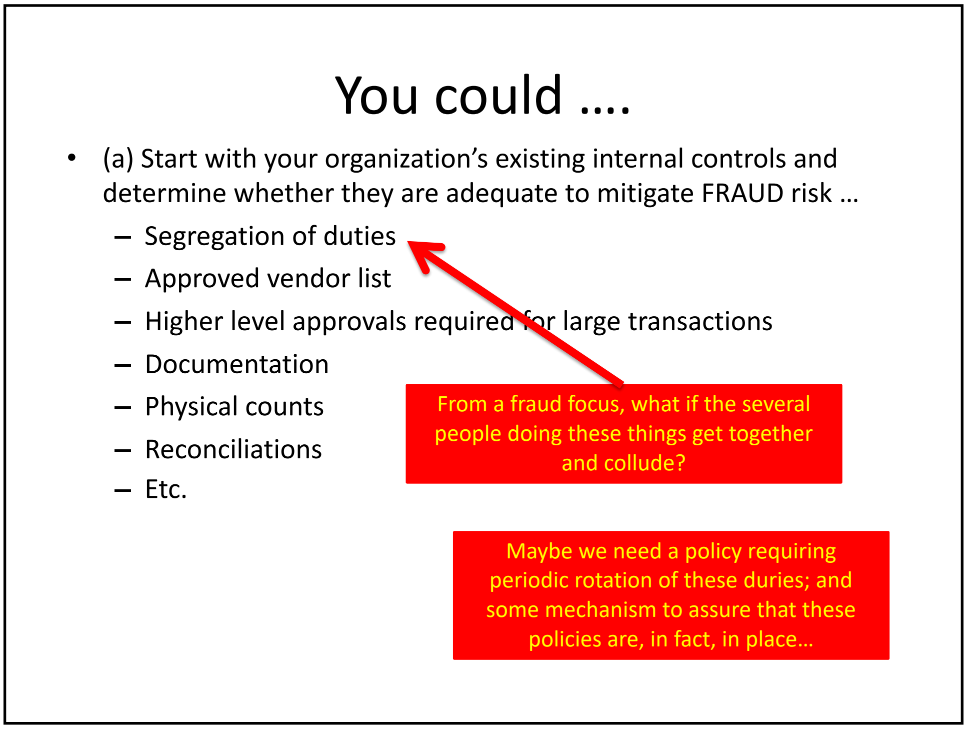
These are all excellent controls designed to ensure accuracy in accounting and financial reporting. But, if your focus is now specifically on fraud, maybe we need something more …



You could ….

- (a) Start with your organization’s existing internal controls and determine whether they are adequate to mitigate FRAUD risk …
  - Segregation of duties
  - Approved vendor list
  - Higher level approvals required for large transactions
  - Documentation
  - Physical counts
  - Reconciliations
  - Etc.

From a fraud focus, what if the several people doing these things get together and collude?

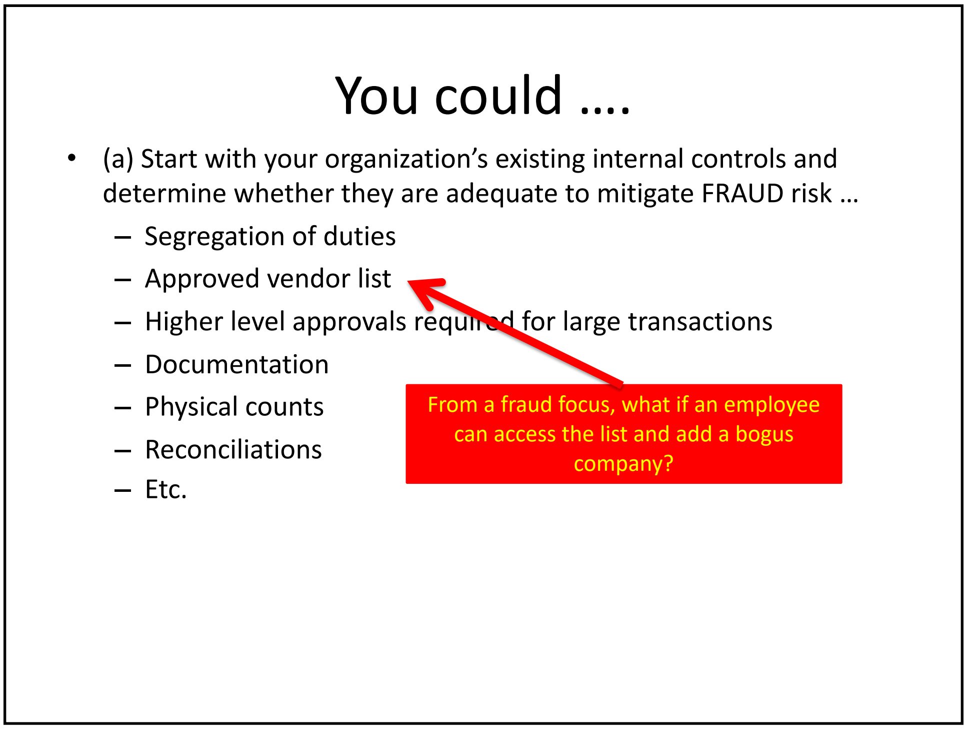


You could ….

- (a) Start with your organization’s existing internal controls and determine whether they are adequate to mitigate FRAUD risk …
  - Segregation of duties
  - Approved vendor list
  - Higher level approvals required for large transactions
  - Documentation
  - Physical counts
  - Reconciliations
  - Etc.

From a fraud focus, what if the several people doing these things get together and collude?

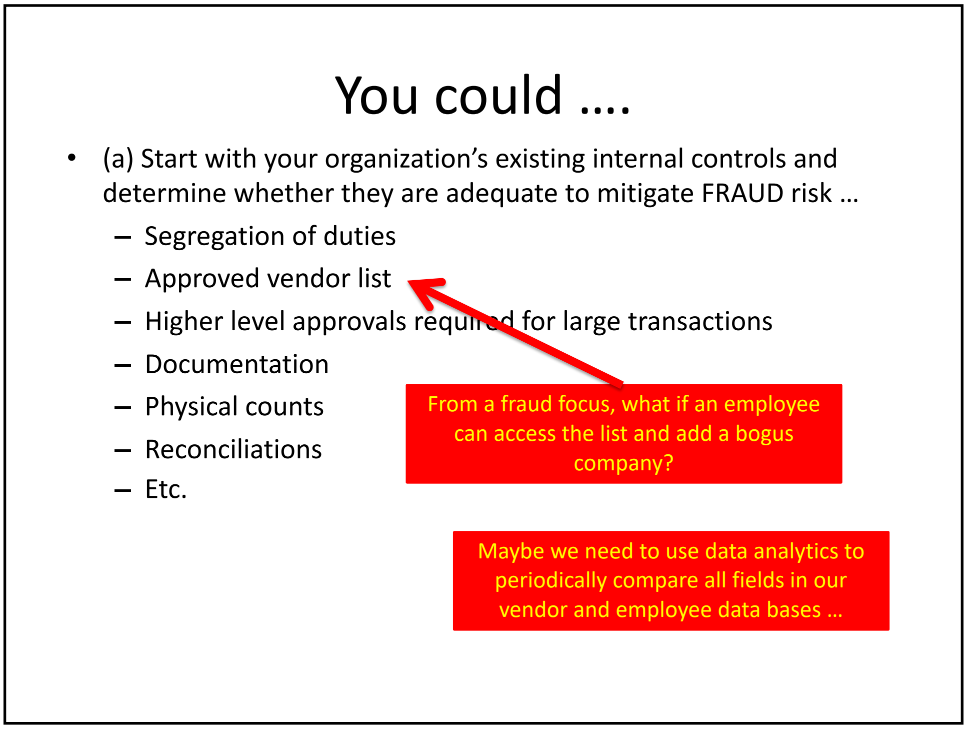
Maybe we need a policy requiring periodic rotation of these duries; and some mechanism to assure that these policies are, in fact, in place…



You could ….

- (a) Start with your organization’s existing internal controls and determine whether they are adequate to mitigate FRAUD risk …
  - Segregation of duties
  - Approved vendor list
  - Higher level approvals required for large transactions
  - Documentation
  - Physical counts
  - Reconciliations
  - Etc.

From a fraud focus, what if an employee can access the list and add a bogus company?

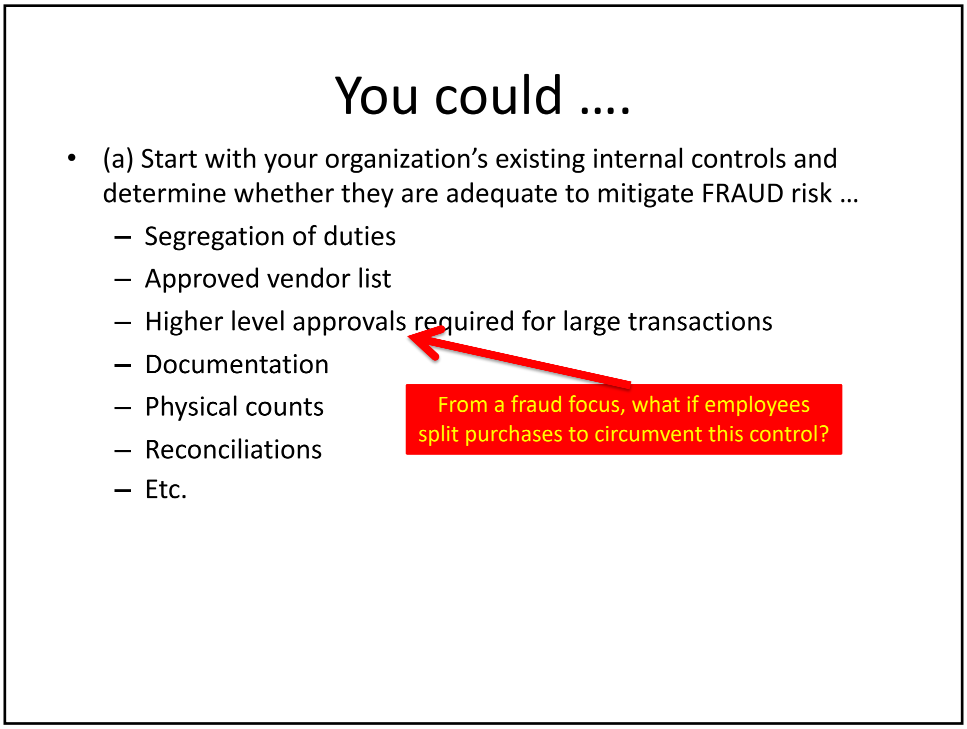


You could ….

- (a) Start with your organization's existing internal controls and determine whether they are adequate to mitigate FRAUD risk …
  - Segregation of duties
  - Approved vendor list
  - Higher level approvals required for large transactions
  - Documentation
  - Physical counts
  - Reconciliations
  - Etc.

From a fraud focus, what if an employee can access the list and add a bogus company?

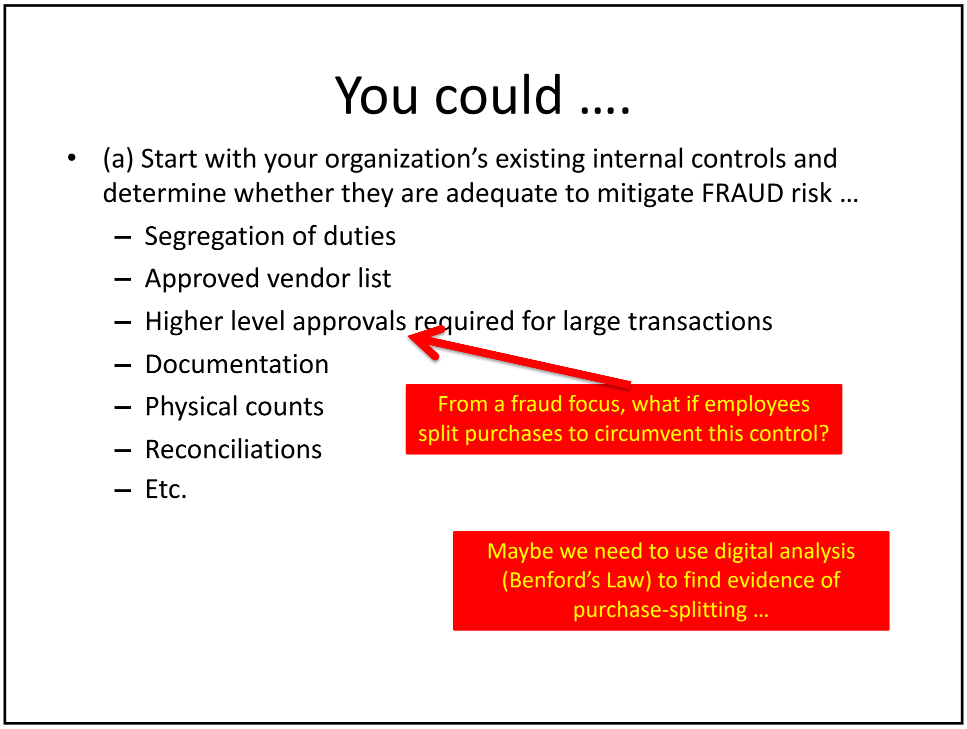
Maybe we need to use data analytics to periodically compare all fields in our vendor and employee data bases …



You could ….

- (a) Start with your organization's existing internal controls and determine whether they are adequate to mitigate FRAUD risk …
  - Segregation of duties
  - Approved vendor list
  - Higher level approvals required for large transactions
  - Documentation
  - Physical counts
  - Reconciliations
  - Etc.

From a fraud focus, what if employees split purchases to circumvent this control?

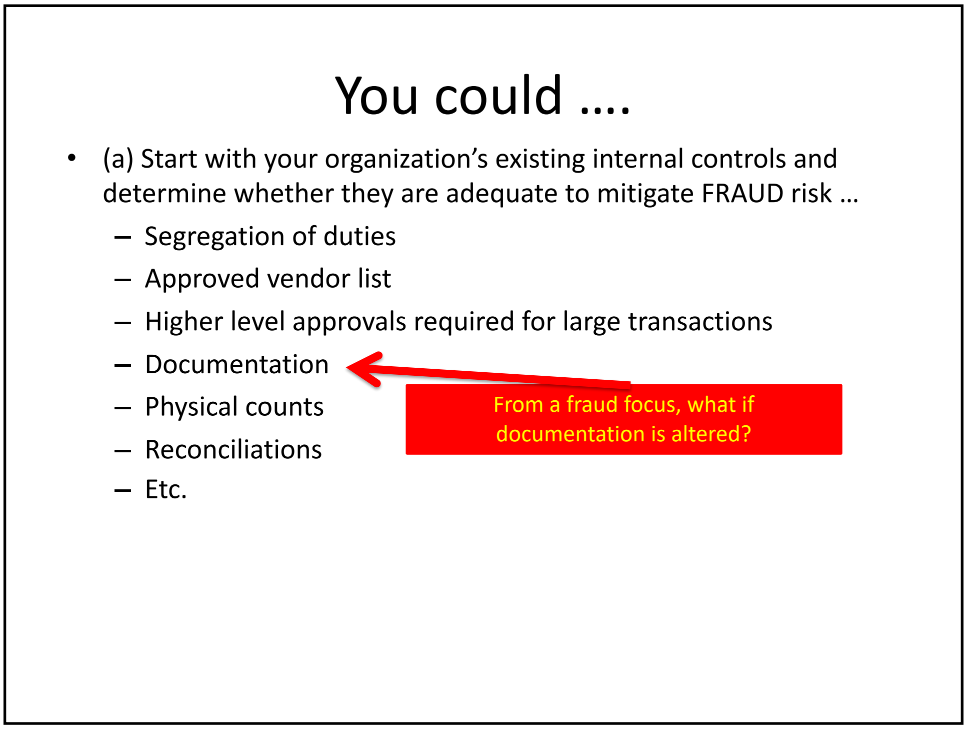


You could ….

- (a) Start with your organization's existing internal controls and determine whether they are adequate to mitigate FRAUD risk …
  - Segregation of duties
  - Approved vendor list
  - Higher level approvals required for large transactions
  - Documentation
  - Physical counts
  - Reconciliations
  - Etc.

From a fraud focus, what if employees split purchases to circumvent this control?

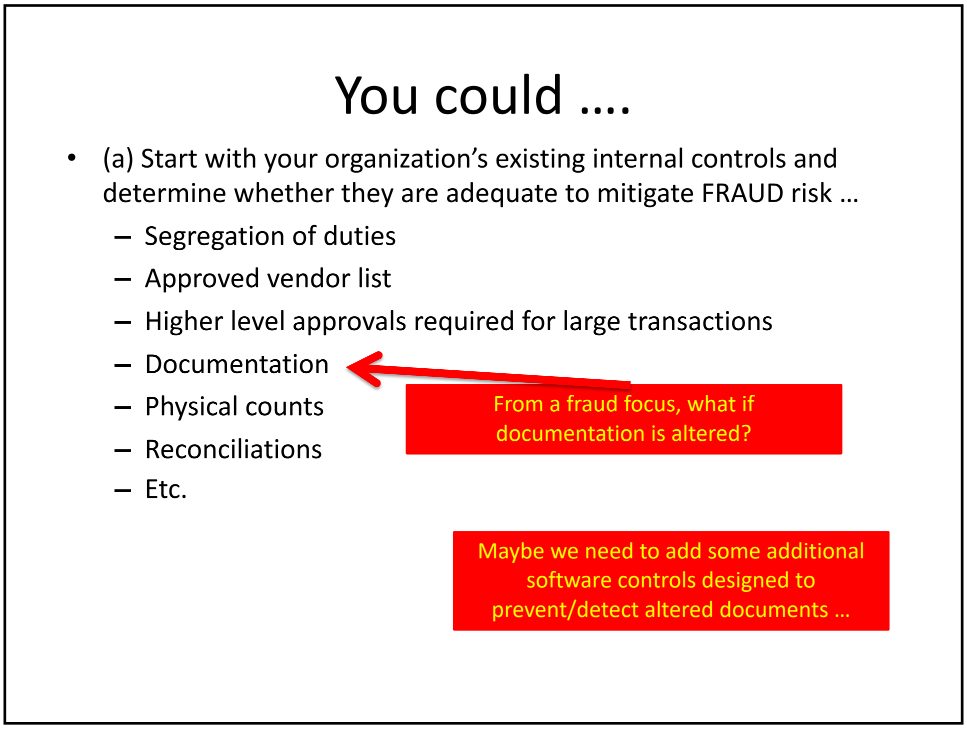
Maybe we need to use digital analysis (Benford's Law) to find evidence of purchase-splitting …



You could ….

- (a) Start with your organization's existing internal controls and determine whether they are adequate to mitigate FRAUD risk …
  - Segregation of duties
  - Approved vendor list
  - Higher level approvals required for large transactions
  - Documentation
  - Physical counts
  - Reconciliations
  - Etc.

From a fraud focus, what if documentation is altered?

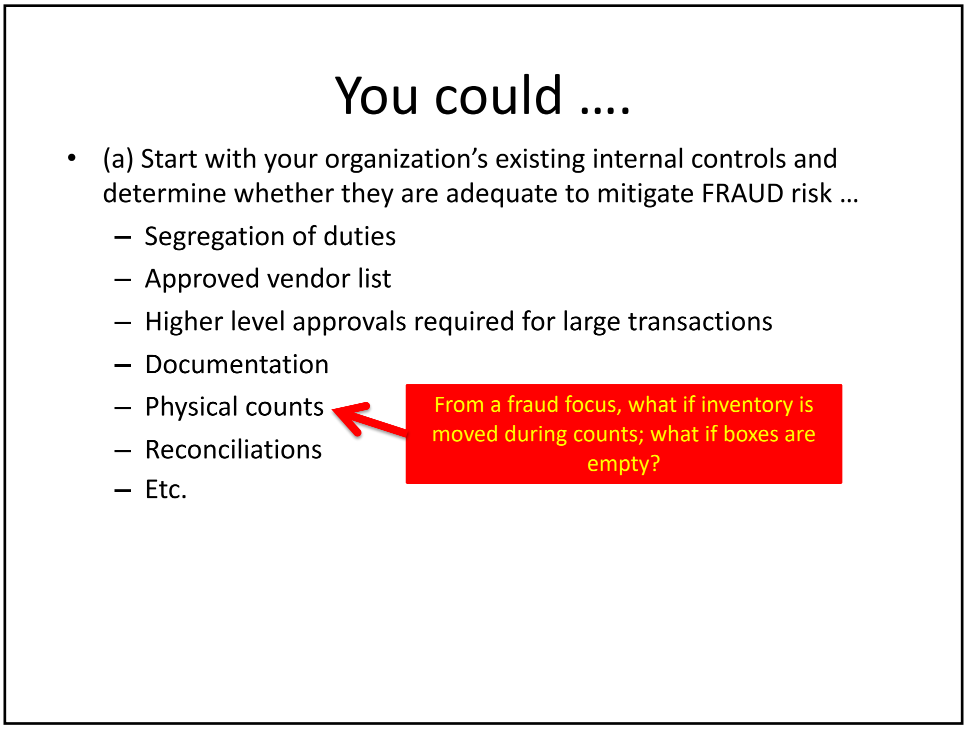


You could ….

- (a) Start with your organization’s existing internal controls and determine whether they are adequate to mitigate FRAUD risk …
  - Segregation of duties
  - Approved vendor list
  - Higher level approvals required for large transactions
  - Documentation
  - Physical counts
  - Reconciliations
  - Etc.

From a fraud focus, what if documentation is altered?

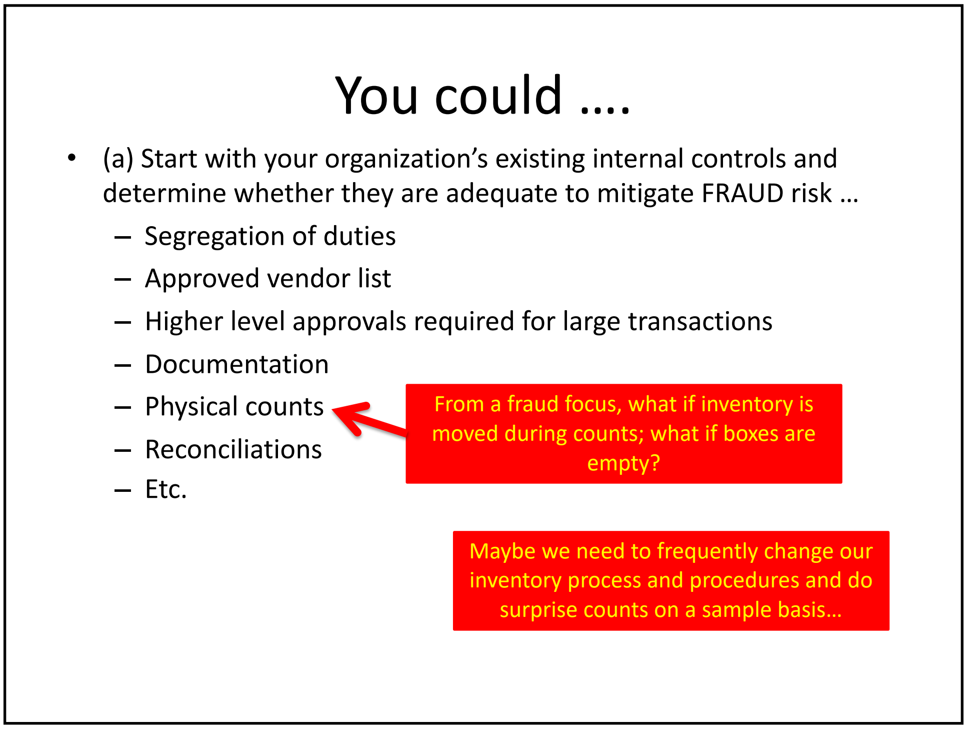
Maybe we need to add some additional software controls designed to prevent/detect altered documents …



You could ….

- (a) Start with your organization’s existing internal controls and determine whether they are adequate to mitigate FRAUD risk …
  - Segregation of duties
  - Approved vendor list
  - Higher level approvals required for large transactions
  - Documentation
  - Physical counts
  - Reconciliations
  - Etc.

From a fraud focus, what if inventory is moved during counts; what if boxes are empty?

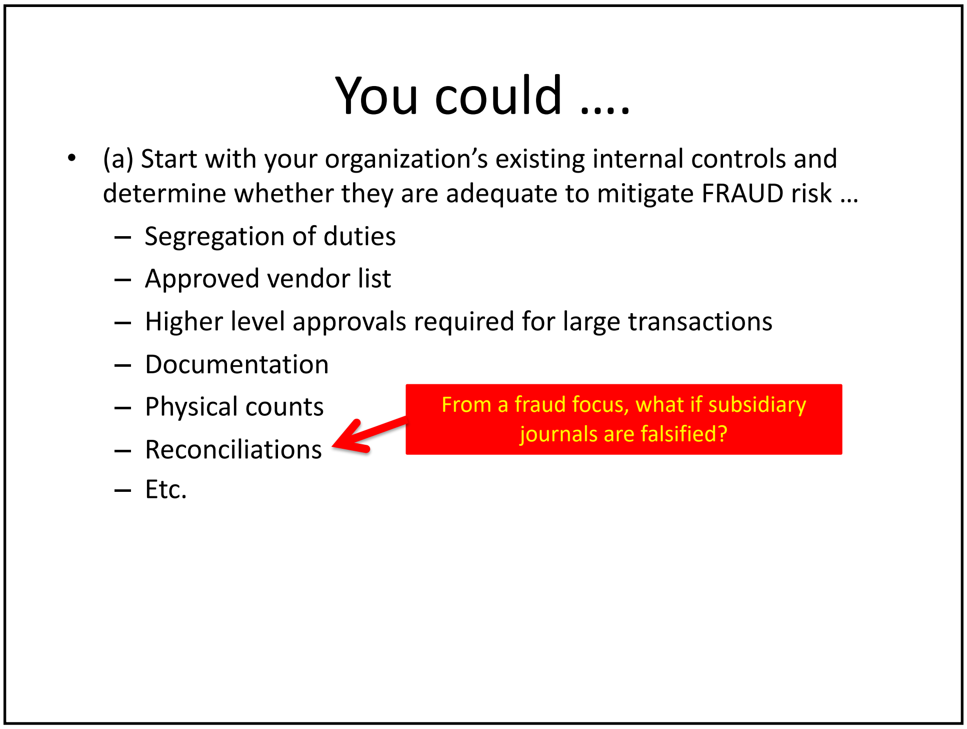


You could ….

- (a) Start with your organization's existing internal controls and determine whether they are adequate to mitigate FRAUD risk …
  – Segregation of duties
  – Approved vendor list
  – Higher level approvals required for large transactions
  – Documentation
  – Physical counts
  – Reconciliations
  – Etc.

From a fraud focus, what if inventory is moved during counts; what if boxes are empty?

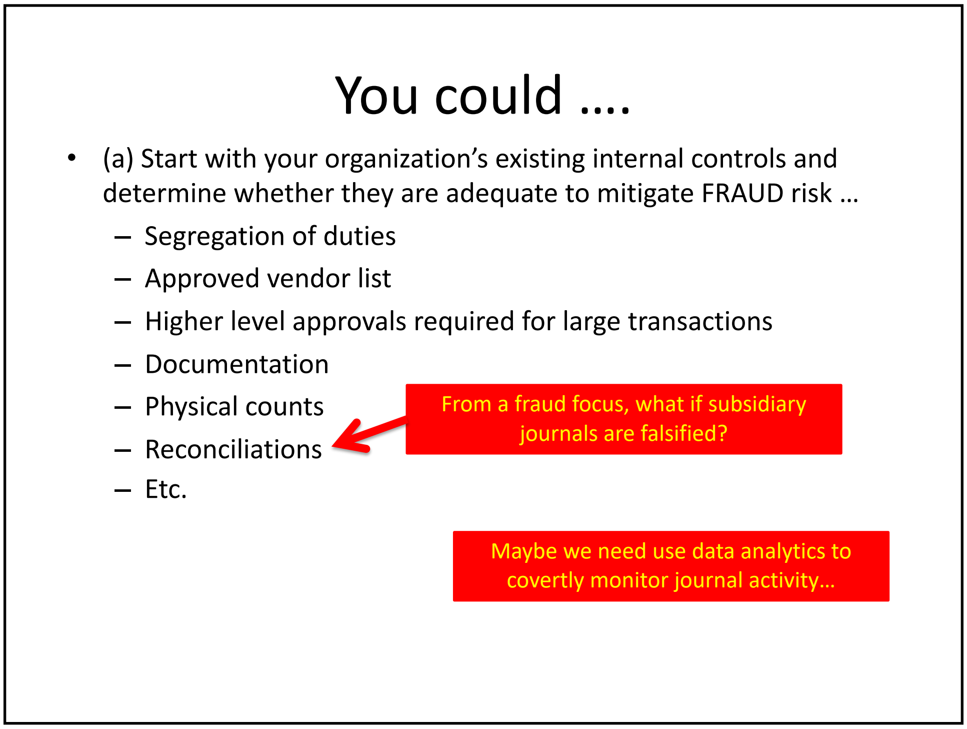
Maybe we need to frequently change our inventory process and procedures and do surprise counts on a sample basis…



You could ….

- (a) Start with your organization's existing internal controls and determine whether they are adequate to mitigate FRAUD risk …
  – Segregation of duties
  – Approved vendor list
  – Higher level approvals required for large transactions
  – Documentation
  – Physical counts
  – Reconciliations
  – Etc.

From a fraud focus, what if subsidiary journals are falsified?

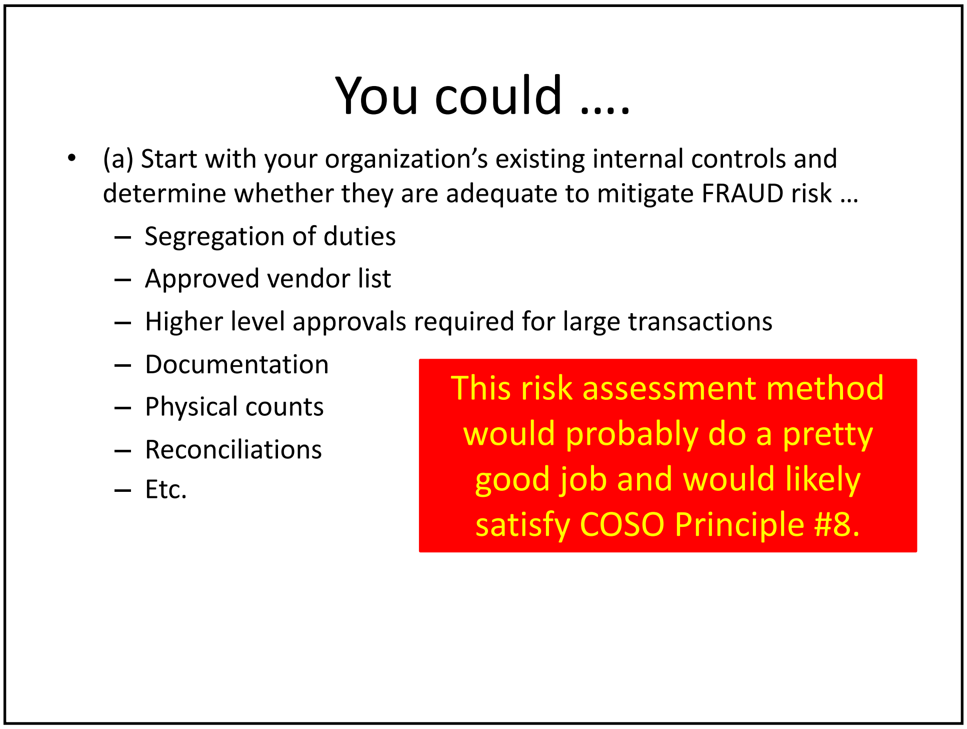


You could ….

- (a) Start with your organization’s existing internal controls and determine whether they are adequate to mitigate FRAUD risk …
  - Segregation of duties
  - Approved vendor list
  - Higher level approvals required for large transactions
  - Documentation
  - Physical counts
  - Reconciliations
  - Etc.

From a fraud focus, what if subsidiary journals are falsified?

Maybe we need use data analytics to covertly monitor journal activity…



You could ….

- (a) Start with your organization’s existing internal controls and determine whether they are adequate to mitigate FRAUD risk …
  - Segregation of duties
  - Approved vendor list
  - Higher level approvals required for large transactions
  - Documentation
  - Physical counts
  - Reconciliations
  - Etc.

This risk assessment method would probably do a pretty good job and would likely satisfy COSO Principle #8.

You could ….

- (a) Start with your organization's existing internal controls and determine whether they are adequate to mitigate FRAUD risk …
  - Segregation of duties
  - Approved vendor list
  - Higher level approvals required for large transactions
  - Documentation
  - Physical counts
  - Reconciliations
  - Etc.

This risk assessment method would probably do a pretty good job and would likely satisfy COSO Principle #8.

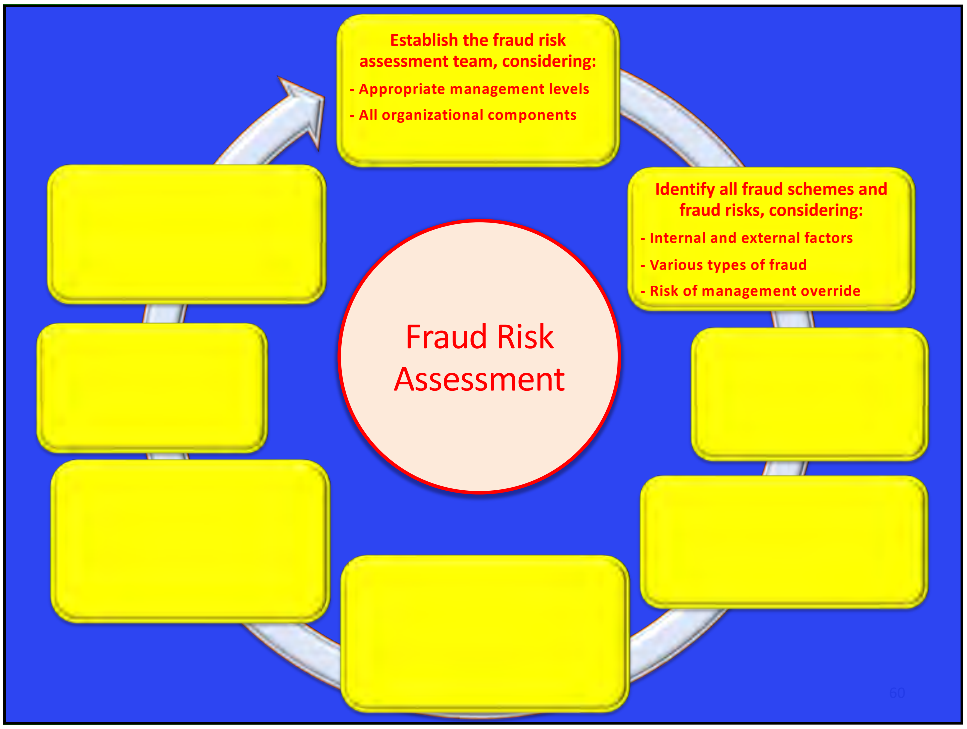
On the other hand, these controls are all focused on accounting and financial reporting; and we know that many frauds can occur elsewhere …

So, perhaps you should ….

- (b) spend $59 to buy the FRMG, start from scratch, and perform a ***more comprehensive*** fraud risk assessment

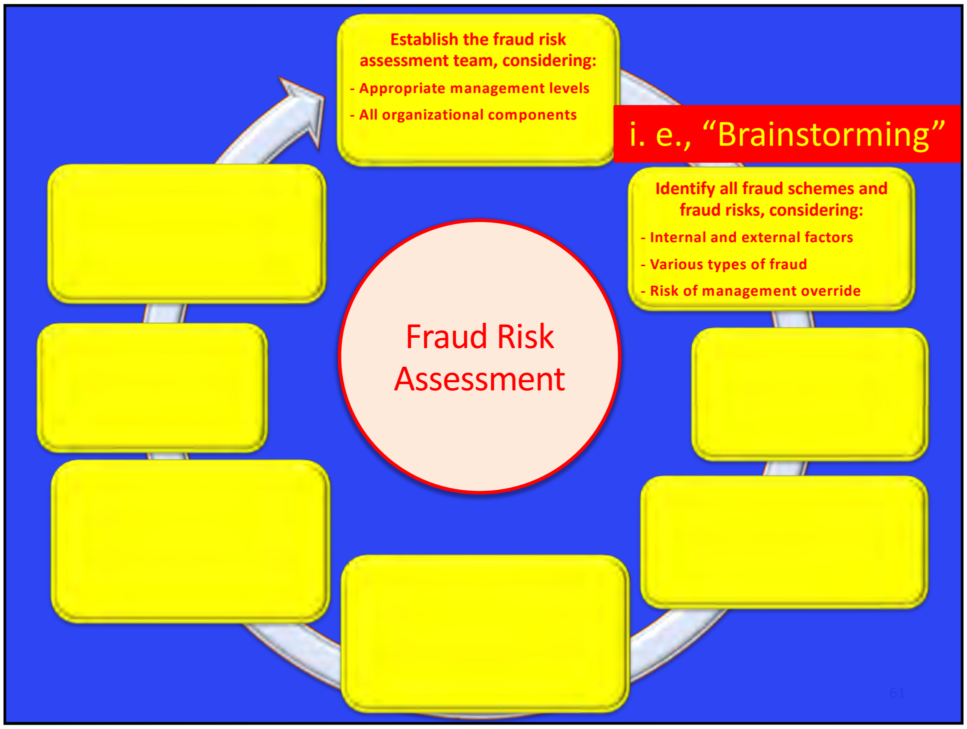
The Fraud Risk Assessment Process

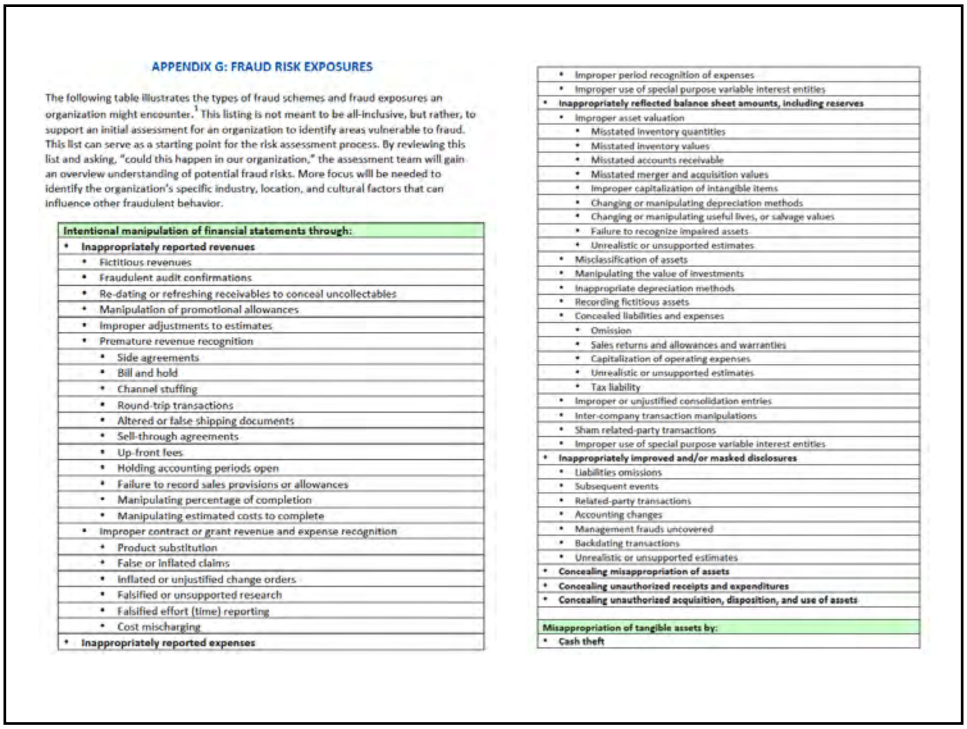
Fraud Risk Assessment
59



Establish the fraud risk assessment team, considering:
- Appropriate management levels
- All organizational components

Identify all fraud schemes and fraud risks, considering:
- Internal and external factors
- Various types of fraud
- Risk of management override


Establish the fraud risk assessment team, considering:
- Appropriate management levels
- All organizational components
i. e., “Brainstorming”
Identify all fraud schemes and fraud risks, considering:
- Internal and external factors
- Various types of fraud
- Risk of management override
Fraud Risk Assessment



APPENDIX G: FRAUD RISK EXPOSURES

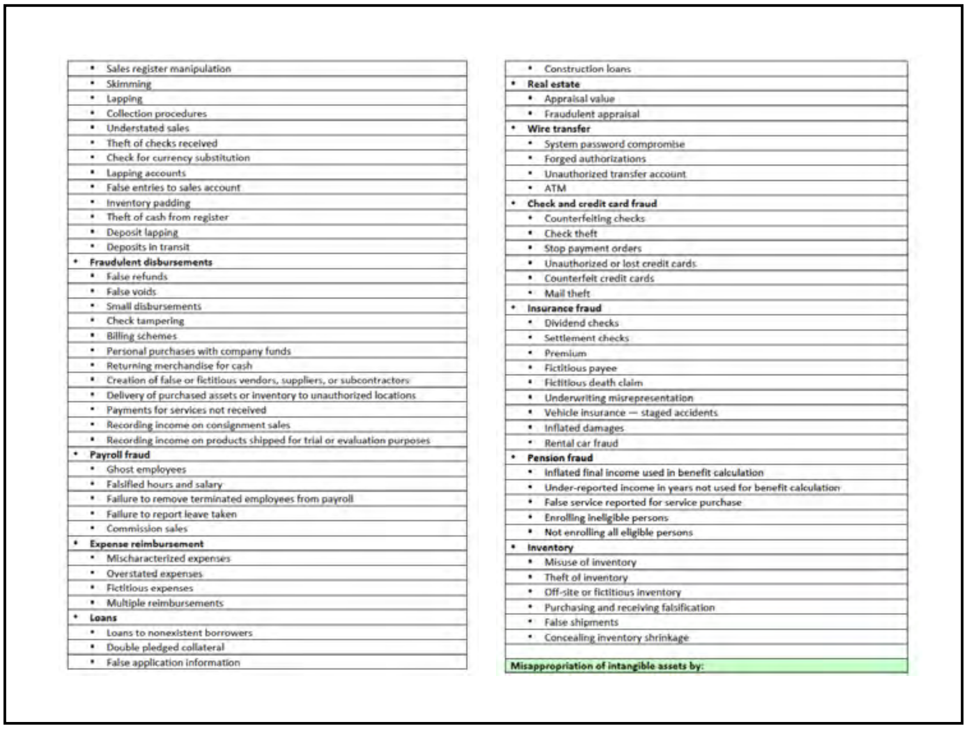
The following table illustrates the types of fraud schemes and fraud exposures an organization might encounter.[1] This listing is not meant to be all-inclusive, but rather, to support an initial assessment for an organization to identify areas vulnerable to fraud. This list can serve as a starting point for the risk assessment process. By reviewing this list and asking, "could this happen in our organization," the assessment team will gain an overview understanding of potential fraud risks. More focus will be needed to identify the organization's specific industry, location, and cultural factors that can influence other fraudulent behavior.

Intentional manipulation of financial statements through:

- **Inappropriately reported revenues**
  - Fictitious revenues
  - Fraudulent audit confirmations
  - Re-dating or refreshing receivables to conceal uncollectables
  - Manipulation of promotional allowances
  - Improper adjustments to estimates
  - Premature revenue recognition
    - Side agreements
    - Bill and hold
    - Channel stuffing
    - Round-trip transactions
    - Altered or false shipping documents
    - Sell-through agreements
    - Up-front fees
    - Holding accounting periods open
    - Failure to record sales provisions or allowances
    - Manipulating percentage of completion
    - Manipulating estimated costs to complete
  - Improper contract or grant revenue and expense recognition
    - Product substitution
    - False or inflated claims
    - Inflated or unjustified change orders
    - Falsified or unsupported research
    - Falsified effort (time) reporting
    - Cost mischarging
- **Inappropriately reported expenses**
  - Improper period recognition of expenses
  - Improper use of special purpose variable interest entities
- **Inappropriately reflected balance sheet amounts, including reserves**
  - Improper asset valuation
    - Misstated inventory quantities
    - Misstated inventory values
    - Misstated accounts receivable
    - Misstated merger and acquisition values
    - Improper capitalization of intangible items
    - Changing or manipulating depreciation methods
    - Changing or manipulating useful lives, or salvage values
    - Failure to recognize impaired assets
    - Unrealistic or unsupported estimates
  - Misclassification of assets
  - Manipulating the value of investments
  - Inappropriate depreciation methods
  - Recording fictitious assets
  - Concealed liabilities and expenses
    - Omission
    - Sales returns and allowances and warranties
    - Capitalization of operating expenses
    - Unrealistic or unsupported estimates
    - Tax liability
  - Improper or unjustified consolidation entries
  - Inter-company transaction manipulations
  - Sham related-party transactions
  - Improper use of special purpose variable interest entities
- **Inappropriately improved and/or masked disclosures**
  - Liabilities omissions
  - Subsequent events
  - Related-party transactions
  - Accounting changes
  - Management frauds uncovered
  - Backdating transactions
  - Unrealistic or unsupported estimates
- **Concealing misappropriation of assets**
- **Concealing unauthorized receipts and expenditures**
- **Concealing unauthorized acquisition, disposition, and use of assets**

Misappropriation of tangible assets by:

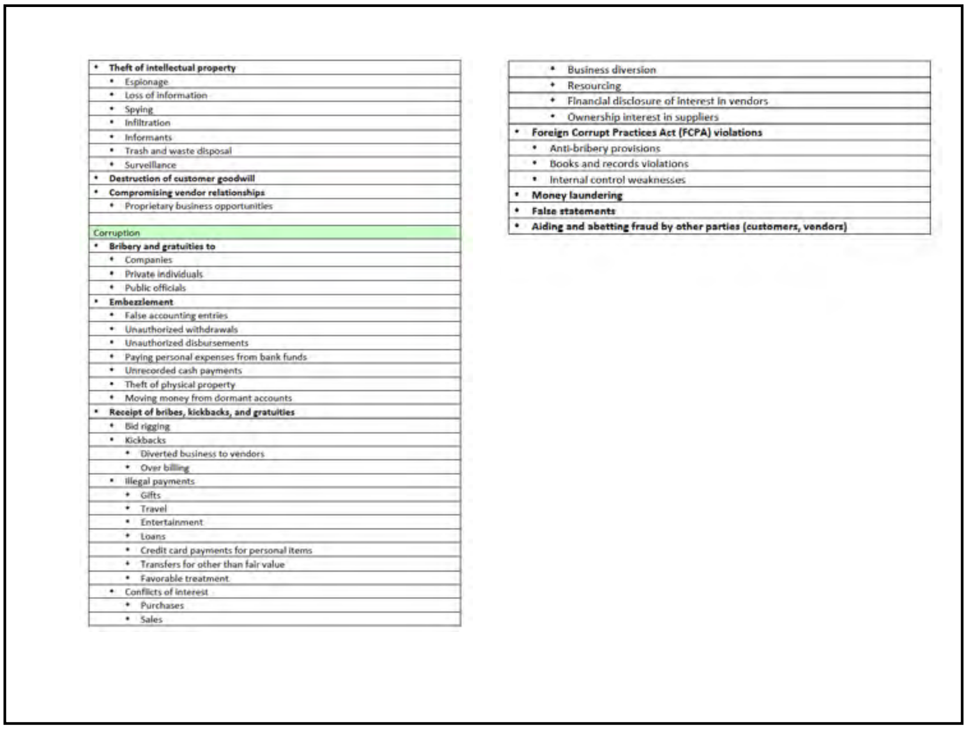
- **Cash theft**



- Sales register manipulation
- Skimming
- Lapping
- Collection procedures
- Understated sales
- Theft of checks received
- Check for currency substitution
- Lapping accounts
- False entries to sales account
- Inventory padding
- Theft of cash from register
- Deposit lapping
- Deposits in transit

- **Fraudulent disbursements**
  - False refunds
  - False voids
  - Small disbursements
  - Check tampering
  - Billing schemes
  - Personal purchases with company funds
  - Returning merchandise for cash
  - Creation of false or fictitious vendors, suppliers, or subcontractors
  - Delivery of purchased assets or inventory to unauthorized locations
  - Payments for services not received
  - Recording income on consignment sales
  - Recording income on products shipped for trial or evaluation purposes
- **Payroll fraud**
  - Ghost employees
  - Falsified hours and salary
  - Failure to remove terminated employees from payroll
  - Failure to report leave taken
  - Commission sales
- **Expense reimbursement**
  - Mischaracterized expenses
  - Overstated expenses
  - Fictitious expenses
  - Multiple reimbursements
- **Loans**
  - Loans to nonexistent borrowers
  - Double pledged collateral
  - False application information
  - Construction loans
- **Real estate**
  - Appraisal value
  - Fraudulent appraisal
- **Wire transfer**
  - System password compromise
  - Forged authorizations
  - Unauthorized transfer account
  - ATM
- **Check and credit card fraud**
  - Counterfeiting checks
  - Check theft
  - Stop payment orders
  - Unauthorized or lost credit cards
  - Counterfeit credit cards
  - Mail theft
- **Insurance fraud**
  - Dividend checks
  - Settlement checks
  - Premium
  - Fictitious payee
  - Fictitious death claim
  - Underwriting misrepresentation
  - Vehicle insurance — staged accidents
  - Inflated damages
  - Rental car fraud
- **Pension fraud**
  - Inflated final income used in benefit calculation
  - Under-reported income in years not used for benefit calculation
  - False service reported for service purchase
  - Enrolling ineligible persons
  - Not enrolling all eligible persons
- **Inventory**
  - Misuse of inventory
  - Theft of inventory
  - Off-site or fictitious inventory
  - Purchasing and receiving falsification
  - False shipments
  - Concealing inventory shrinkage

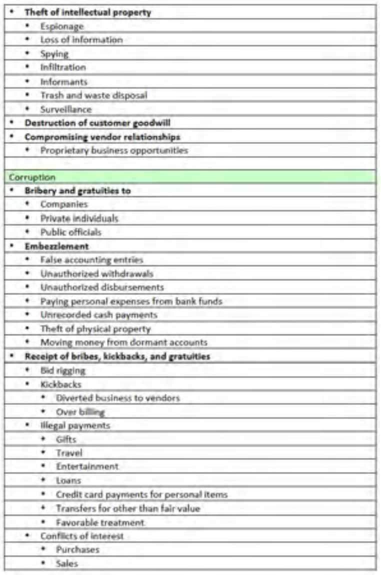
Misappropriation of intangible assets by:



- **Theft of intellectual property**
  - Espionage
  - Loss of information
  - Spying
  - Infiltration
  - Informants
  - Trash and waste disposal
  - Surveillance
- **Destruction of customer goodwill**
- **Compromising vendor relationships**
  - Proprietary business opportunities

Corruption

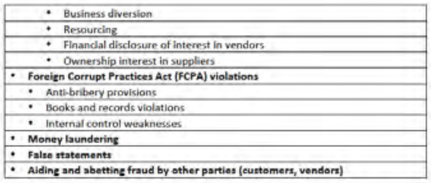
- **Bribery and gratuities to**
  - Companies
  - Private individuals
  - Public officials
- **Embezzlement**
  - False accounting entries
  - Unauthorized withdrawals
  - Unauthorized disbursements
  - Paying personal expenses from bank funds
  - Unrecorded cash payments
  - Theft of physical property
  - Moving money from dormant accounts
- **Receipt of bribes, kickbacks, and gratuities**
  - Bid rigging
  - Kickbacks
    - Diverted business to vendors
    - Over billing
  - Illegal payments
    - Gifts
    - Travel
    - Entertainment
    - Loans
    - Credit card payments for personal items
    - Transfers for other than fair value
    - Favorable treatment
  - Conflicts of interest
    - Purchases
    - Sales
    - Business diversion
    - Resourcing
    - Financial disclosure of interest in vendors
    - Ownership interest in suppliers
- **Foreign Corrupt Practices Act (FCPA) violations**
  - Anti-bribery provisions
  - Books and records violations
  - Internal control weaknesses
- **Money laundering**
- **False statements**
- **Aiding and abetting fraud by other parties (customers, vendors)**



- **Theft of intellectual property**
  - Espionage
  - Loss of information
  - Spying
  - Infiltration
  - Informants
  - Trash and waste disposal
  - Surveillance
- **Destruction of customer goodwill**
- **Compromising vendor relationships**
  - Proprietary business opportunities

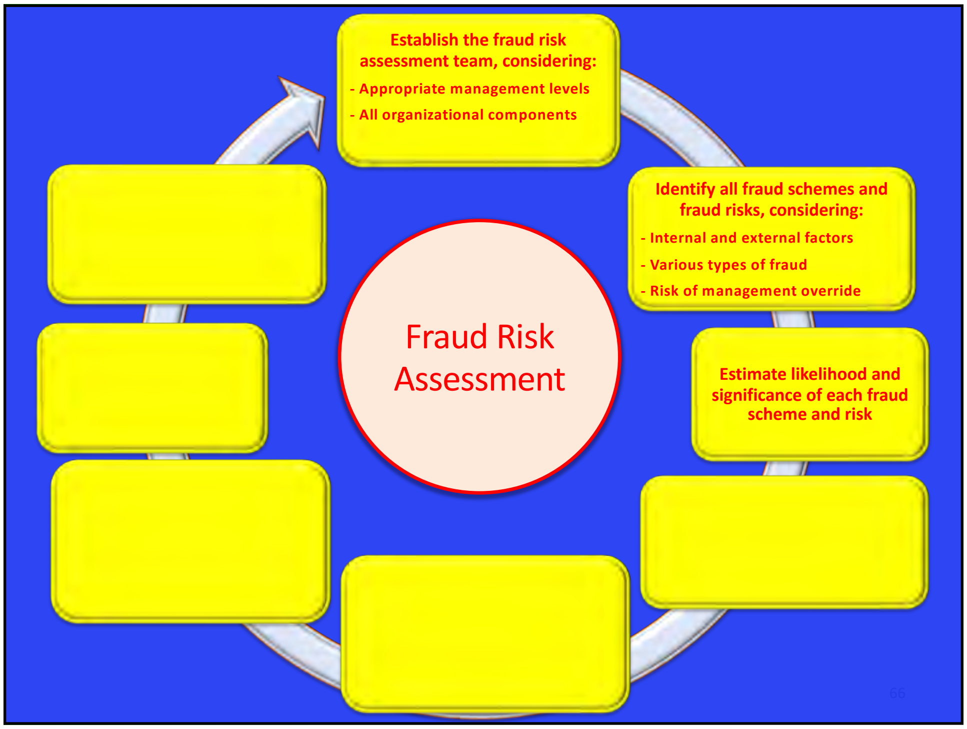
Corruption

- **Bribery and gratuities to**
  - Companies
  - Private individuals
  - Public officials
- **Embezzlement**
  - False accounting entries
  - Unauthorized withdrawals
  - Unauthorized disbursements
  - Paying personal expenses from bank funds
  - Unrecorded cash payments
  - Theft of physical property
  - Moving money from dormant accounts
- **Receipt of bribes, kickbacks, and gratuities**
  - Bid rigging
  - Kickbacks
    - Diverted business to vendors
    - Over billing
  - Illegal payments
    - Gifts
    - Travel
    - Entertainment
    - Loans
    - Credit card payments for personal items
    - Transfers for other than fair value
    - Favorable treatment
  - Conflicts of interest
    - Purchases
    - Sales



    - Business diversion
    - Resourcing
    - Financial disclosure of interest in vendors
    - Ownership interest in suppliers
- **Foreign Corrupt Practices Act (FCPA) violations**
  - Anti-bribery provisions
  - Books and records violations
  - Internal control weaknesses
- **Money laundering**
- **False statements**
- **Aiding and abetting fraud by other parties (customers, vendors)**

ACFE is in the process of moving this list to their "Fraud Risk Management Tools" page and adding hyperlinked definitions/descriptions



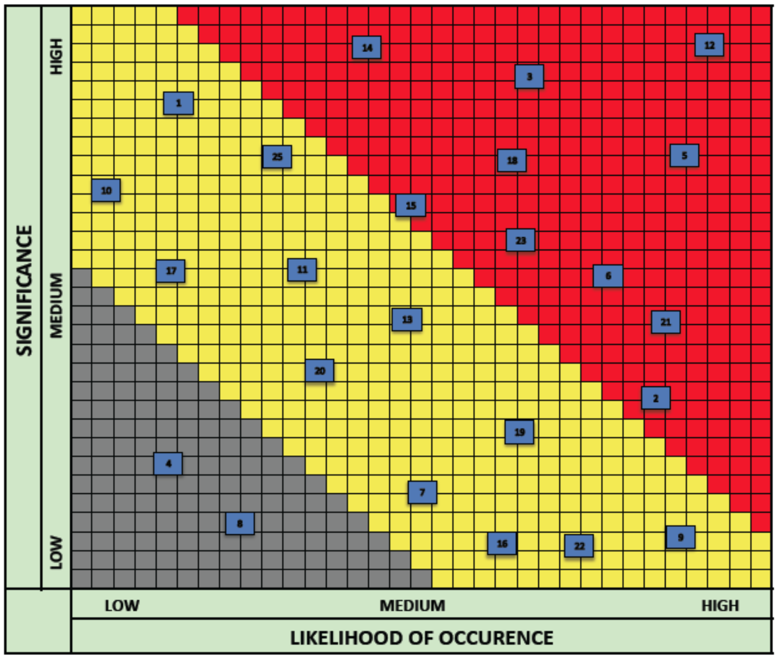
Establish the fraud risk assessment team, considering:
- Appropriate management levels
- All organizational components

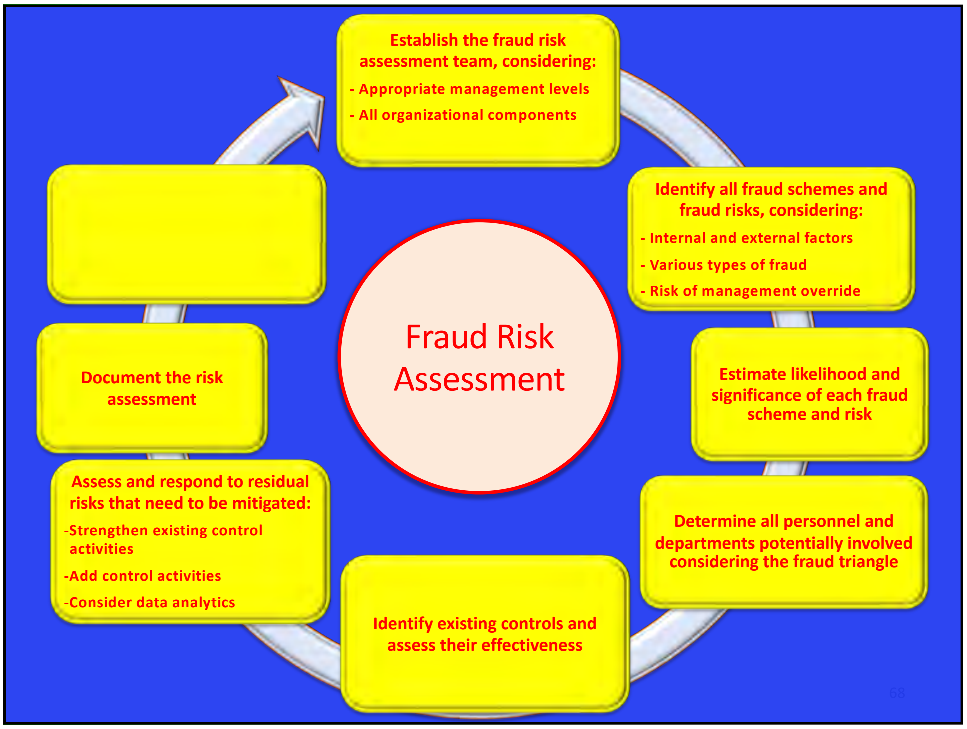
Identify all fraud schemes and fraud risks, considering:
- Internal and external factors
- Various types of fraud
- Risk of management override

Estimate likelihood and significance of each fraud scheme and risk

Fraud Risk Assessment

FRAUD RISK ASSESSMENT HEAT MAP





Fraud Risk Assessment

Establish the fraud risk assessment team, considering:
- Appropriate management levels
- All organizational components

Identify all fraud schemes and fraud risks, considering:
- Internal and external factors
- Various types of fraud
- Risk of management override

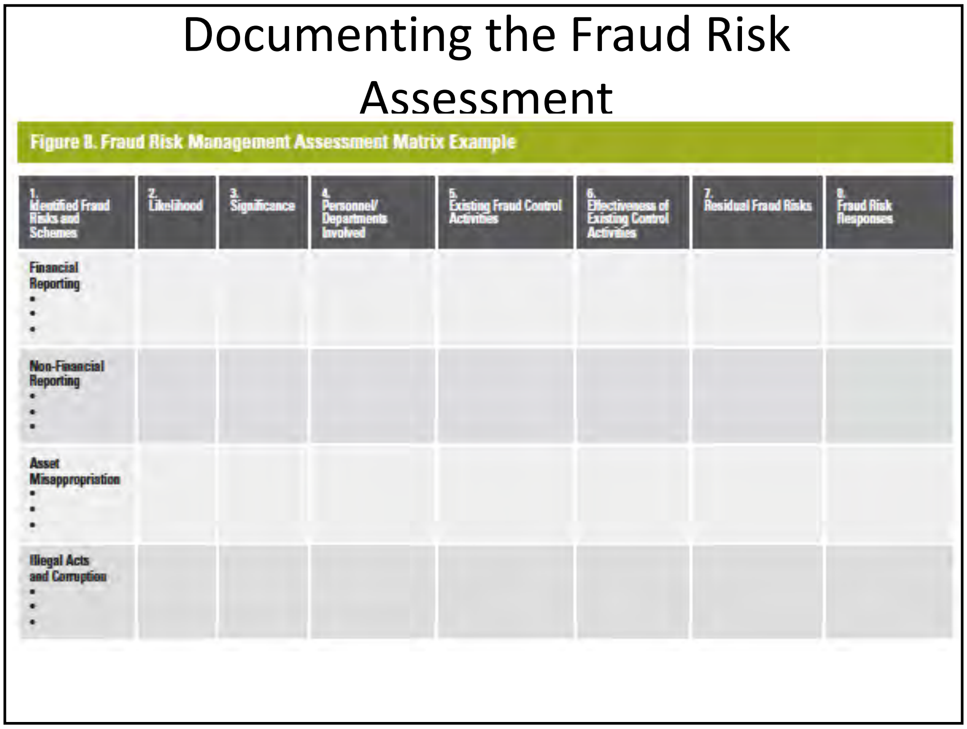
Estimate likelihood and significance of each fraud scheme and risk

Determine all personnel and departments potentially involved considering the fraud triangle

Identify existing controls and assess their effectiveness

Assess and respond to residual risks that need to be mitigated:
-Strengthen existing control activities
-Add control activities
-Consider data analytics

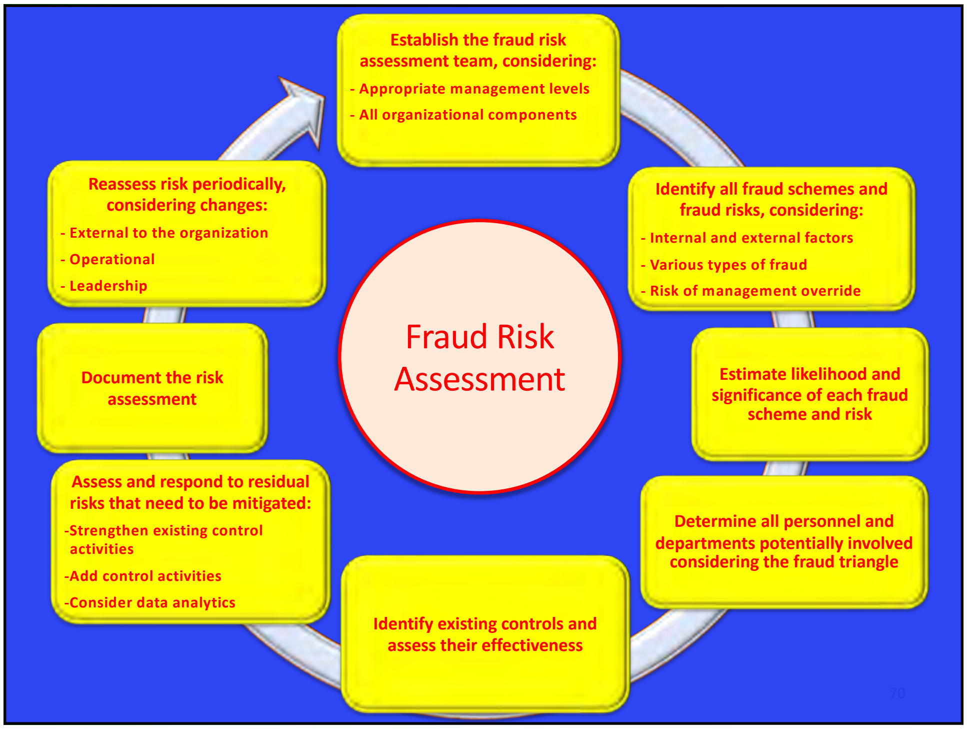
Document the risk assessment



Documenting the Fraud Risk Assessment

Figure 8. Fraud Risk Management Assessment Matrix Example

1. Identified Fraud Risks and Schemes	2. Likelihood	3. Significance	4. Personnel/ Departments Involved	5. Existing Fraud Control Activities	6. Effectiveness of Existing Control Activities	7. Residual Fraud Risks	8. Fraud Risk Responses
Financial Reporting • • •							
Non-Financial Reporting • • •							
Asset Misappropriation • • •							
Illegal Acts and Corruption • • •							



Fraud Risk Assessment

Establish the fraud risk assessment team, considering:
- Appropriate management levels
- All organizational components

Identify all fraud schemes and fraud risks, considering:
- Internal and external factors
- Various types of fraud
- Risk of management override

Estimate likelihood and significance of each fraud scheme and risk

Determine all personnel and departments potentially involved considering the fraud triangle

Identify existing controls and assess their effectiveness

Assess and respond to residual risks that need to be mitigated:
-Strengthen existing control activities
-Add control activities
-Consider data analytics

Document the risk assessment

Reassess risk periodically, considering changes:
- External to the organization
- Operational
- Leadership

FRMG Appendices

A: GLOSSARY

B: ROLES AND RESPONSIBILITIES

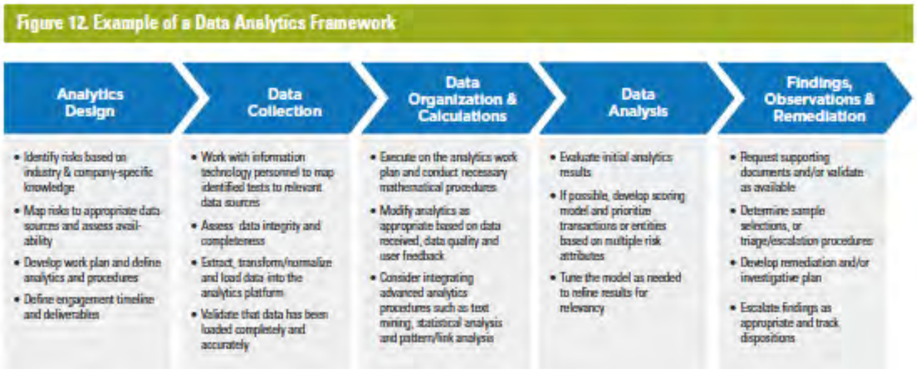
C: CONSIDERATIONS FOR SMALLER ENTITIES

D: REFERENCE MATERIAL

E: DATA ANALYTICS

Data Analytics

Figure 12. Example of a Data Analytics Framework



Analytics Design

- Identify risks based on industry & company-specific knowledge
- Map risks to appropriate data sources and assess availability
- Develop work plan and define analytics and procedures
- Define engagement timeline and deliverables

Data Collection

- Work with information technology personnel to map identified tests to relevant data sources
- Assess data integrity and completeness
- Extract, transform/normalize and load data into the analytics platform
- Validate that data has been loaded completely and accurately

Data Organization & Calculations

- Execute on the analytics work plan and conduct necessary mathematical procedures
- Modify analytics as appropriate based on data received, data quality and user feedback
- Consider integrating advanced analytics procedures such as text mining, statistical analysis and pattern/link analysis

Data Analysis

- Evaluate initial analytics results
- If possible, develop scoring model and prioritize transactions or entities based on multiple risk attributes
- Tune the model as needed to refine results for relevancy

Findings, Observations & Remediation

- Request supporting documents and/or validate as available
- Determine sample selections, or triage/escalation procedures
- Develop remediation and/or investigative plan
- Escalate findings as appropriate and track dispositions

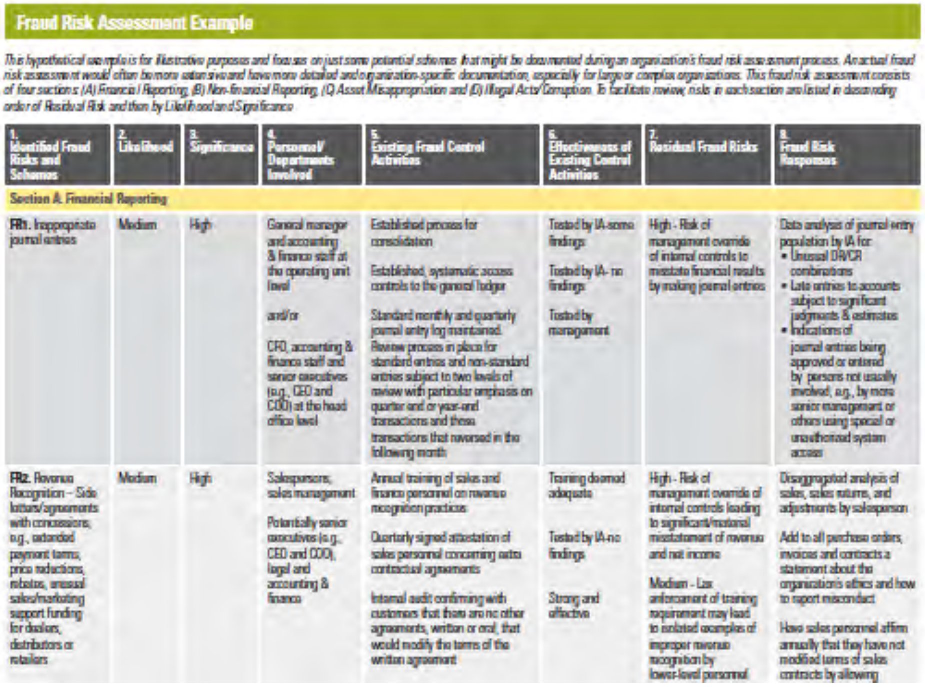
FRMG Appendices

F: SAMPLE GOVERNANCE MATERIALS

- F1: FRAUD CONTROL POLICY FRAMEWORK
- F2: FRAUD RISK HIGH-LEVEL ASSESSMENT
- F3: FRAUD POLICY RESPONSIBILITY MATRIX
- F4: FRAUD RISK MANAGEMENT POLICY
- F5: FRAUD RISK MANAGEMENT SURVEY

G: LIST OF FRAUD RISK EXPOSURES

H: SAMPLE FRAUD RISK ASSESSMENT



Fraud Risk Assessment Example

This hypothetical example is for illustrative purposes and focuses on just some potential schemes that might be documented during an organization's fraud risk assessment process. An actual fraud risk assessment would often be more extensive and have more detailed and organization-specific documentation, especially for large or complex organizations. This fraud risk assessment consists of four sections: (A) Financial Reporting, (B) Non-financial Reporting, (C) Asset Misappropriation and (D) Illegal Acts/Corruption. To facilitate review, risks in each section are listed in descending order of Residual Risk and then by Likelihood and Significance

1. Identified Fraud Risks and Schemes	2. Likelihood	3. Significance	4. Personnel/ Departments Involved	5. Existing Fraud Control Activities	6. Effectiveness of Existing Control Activities	7. Residual Fraud Risks	8. Fraud Risk Responses
Section A. Financial Reporting							
FR1. Inappropriate journal entries	Medium	High	General manager and accounting & finance staff at the operating unit level and/or CFO, accounting & finance staff and senior executives (e.g., CEO and COO) at the head office level	Established process for consolidation Established, systematic access controls to the general ledger Standard monthly and quarterly journal entry log maintained. Review process in place for standard entries and non-standard entries subject to two levels of review with particular emphasis on quarter and or year-end transactions and those transactions that reversed in the following month	Tested by IA-some findings Tested by IA- no findings Tested by management	High - Risk of management override of internal controls to misstate financial results by making journal entries	Data analysis of journal entry population by IA for: • Unusual DR/CR combinations • Late entries to accounts subject to significant judgments & estimates • Indications of journal entries being approved or entered by persons not usually involved, e.g., by more senior management or others using special or unauthorized system access
FR2. Revenue Recognition – Side letters/agreements with concessions, e.g., extended payment terms, price reductions, rebates, unusual sales/marketing support funding for dealers, distributors or retailers	Medium	High	Salespersons; sales management Potentially senior executives (e.g., CEO and COO), legal and accounting & finance	Annual training of sales and finance personnel on revenue recognition practices Quarterly signed attestation of sales personnel concerning extra contractual agreements Internal audit confirming with customers that there are no other agreements, written or oral, that would modify the terms of the written agreement	Training deemed adequate Tested by IA-no findings Strong and effective	High - Risk of management override of internal controls leading to significant/material misstatement of revenue and net income Medium - Lax enforcement of training requirement may lead to isolated examples of improper revenue recognition by lower-level personnel	Disaggregated analysis of sales, sales returns, and adjustments by salesperson Add to all purchase orders, invoices and contracts a statement about the organization's ethics and how to report misconduct Have sales personnel affirm annually that they have not modified terms of sales contracts by allowing

FRMG Appendices

I: FRAUD RISK MANAGEMENT ASSESSMENT SCORECARDS

I1: FRAUD RISK GOVERNANCE

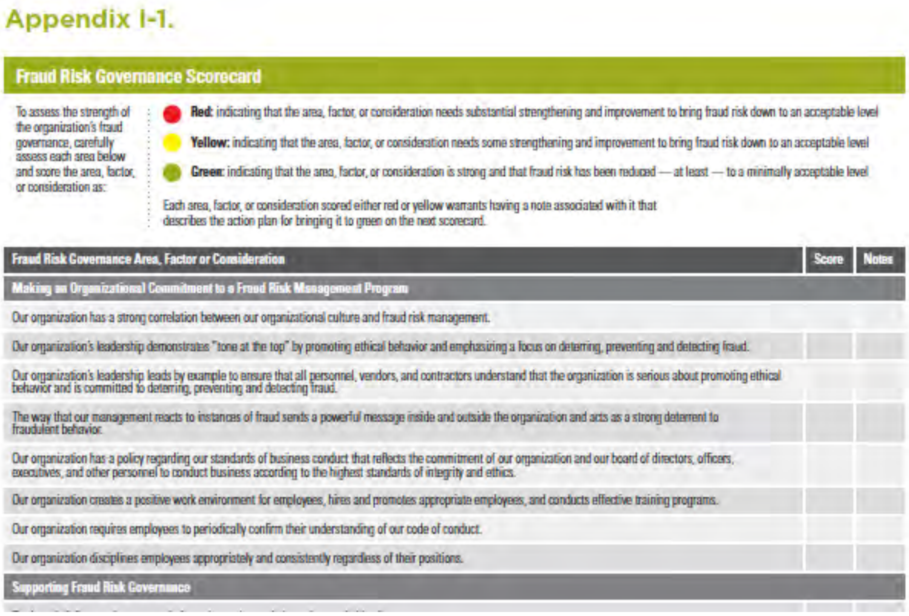
I2: FRAUD RISK ASSESSMENT

I3: FRAUD CONTROL ACTIVITIES

I4: FRAUD INVESTIGATION AND FOLLOWUP

I5: FRAUD RISK MANAGEMENT MONITORING

Automated versions of these scorecards reside at the ACFE "Fraud Risk Management Tools" page



Appendix I-1.

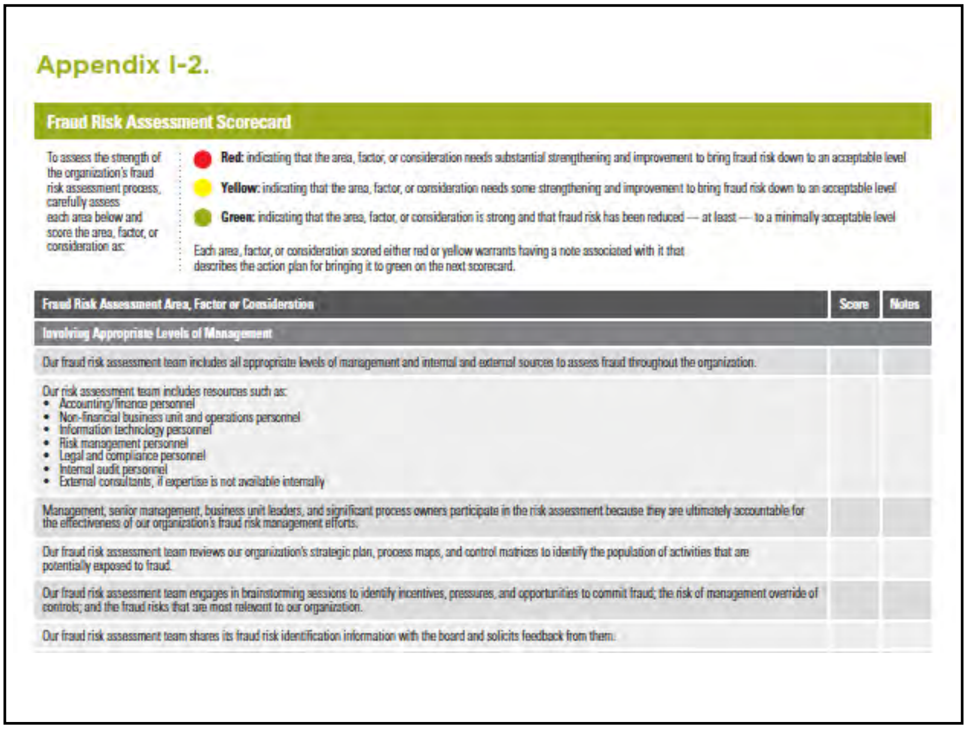
Fraud Risk Governance Scorecard

To assess the strength of the organization's fraud governance, carefully assess each area below and score the area, factor, or consideration as:

- 🔴 **Red:** indicating that the area, factor, or consideration needs substantial strengthening and improvement to bring fraud risk down to an acceptable level
- 🟡 **Yellow:** indicating that the area, factor, or consideration needs some strengthening and improvement to bring fraud risk down to an acceptable level
- 🟢 **Green:** indicating that the area, factor, or consideration is strong and that fraud risk has been reduced — at least — to a minimally acceptable level

Each area, factor, or consideration scored either red or yellow warrants having a note associated with it that describes the action plan for bringing it to green on the next scorecard.

Fraud Risk Governance Area, Factor or Consideration	Score	Notes
Making an Organizational Commitment to a Fraud Risk Management Program		
Our organization has a strong correlation between our organizational culture and fraud risk management.		
Our organization's leadership demonstrates "tone at the top" by promoting ethical behavior and emphasizing a focus on deterring, preventing and detecting fraud.		
Our organization's leadership leads by example to ensure that all personnel, vendors, and contractors understand that the organization is serious about promoting ethical behavior and is committed to deterring, preventing and detecting fraud.		
The way that our management reacts to instances of fraud sends a powerful message inside and outside the organization and acts as a strong deterrent to fraudulent behavior.		
Our organization has a policy regarding our standards of business conduct that reflects the commitment of our organization and our board of directors, officers, executives, and other personnel to conduct business according to the highest standards of integrity and ethics.		
Our organization creates a positive work environment for employees, hires and promotes appropriate employees, and conducts effective training programs.		
Our organization requires employees to periodically confirm their understanding of our code of conduct.		
Our organization disciplines employees appropriately and consistently regardless of their positions.		
Supporting Fraud Risk Governance		



Appendix I-2.

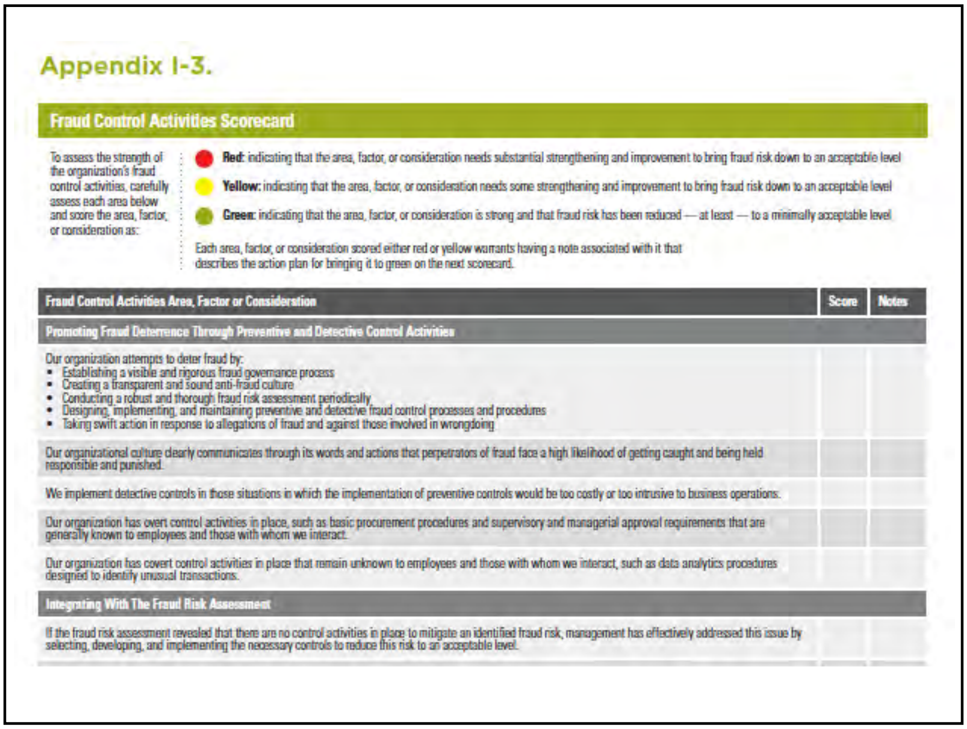
Fraud Risk Assessment Scorecard

To assess the strength of the organization's fraud risk assessment process, carefully assess each area below and score the area, factor, or consideration as:

- 🔴 **Red:** indicating that the area, factor, or consideration needs substantial strengthening and improvement to bring fraud risk down to an acceptable level
- 🟡 **Yellow:** indicating that the area, factor, or consideration needs some strengthening and improvement to bring fraud risk down to an acceptable level
- 🟢 **Green:** indicating that the area, factor, or consideration is strong and that fraud risk has been reduced — at least — to a minimally acceptable level

Each area, factor, or consideration scored either red or yellow warrants having a note associated with it that describes the action plan for bringing it to green on the next scorecard.

Fraud Risk Assessment Area, Factor or Consideration	Score	Notes
Involving Appropriate Levels of Management		
Our fraud risk assessment team includes all appropriate levels of management and internal and external sources to assess fraud throughout the organization.		
Our risk assessment team includes resources such as: • Accounting/finance personnel • Non-financial business unit and operations personnel • Information technology personnel • Risk management personnel • Legal and compliance personnel • Internal audit personnel • External consultants, if expertise is not available internally		
Management, senior management, business unit leaders, and significant process owners participate in the risk assessment because they are ultimately accountable for the effectiveness of our organization's fraud risk management efforts.		
Our fraud risk assessment team reviews our organization's strategic plan, process maps, and control matrices to identify the population of activities that are potentially exposed to fraud.		
Our fraud risk assessment team engages in brainstorming sessions to identify incentives, pressures, and opportunities to commit fraud; the risk of management override of controls; and the fraud risks that are most relevant to our organization.		
Our fraud risk assessment team shares its fraud risk identification information with the board and solicits feedback from them.		



Appendix I-3.

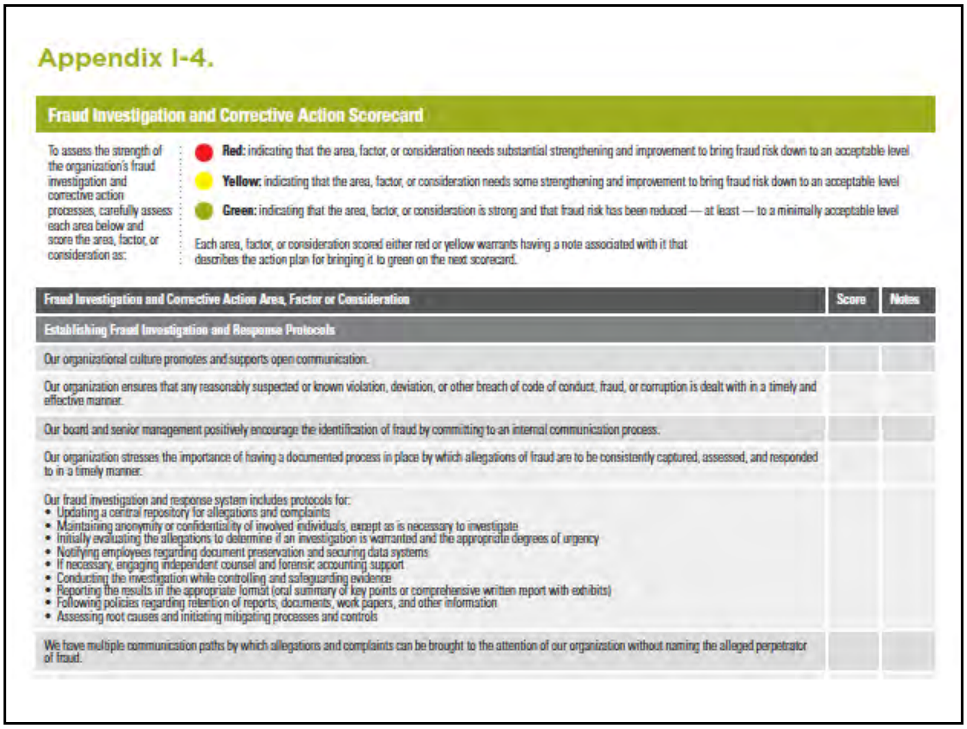
Fraud Control Activities Scorecard

To assess the strength of the organization's fraud control activities, carefully assess each area below and score the area, factor, or consideration as:

- 🔴 **Red:** indicating that the area, factor, or consideration needs substantial strengthening and improvement to bring fraud risk down to an acceptable level
- 🟡 **Yellow:** indicating that the area, factor, or consideration needs some strengthening and improvement to bring fraud risk down to an acceptable level
- 🟢 **Green:** indicating that the area, factor, or consideration is strong and that fraud risk has been reduced — at least — to a minimally acceptable level

Each area, factor, or consideration scored either red or yellow warrants having a note associated with it that describes the action plan for bringing it to green on the next scorecard.

Fraud Control Activities Area, Factor or Consideration	Score	Notes
Promoting Fraud Deterrence Through Preventive and Detective Control Activities		
Our organization attempts to deter fraud by: • Establishing a visible and rigorous fraud governance process • Creating a transparent and sound anti-fraud culture • Conducting a robust and thorough fraud risk assessment periodically • Designing, implementing, and maintaining preventive and detective fraud control processes and procedures • Taking swift action in response to allegations of fraud and against those involved in wrongdoing		
Our organizational culture clearly communicates through its words and actions that perpetrators of fraud face a high likelihood of getting caught and being held responsible and punished.		
We implement detective controls in those situations in which the implementation of preventive controls would be too costly or too intrusive to business operations.		
Our organization has overt control activities in place, such as basic procurement procedures and supervisory and managerial approval requirements that are generally known to employees and those with whom we interact.		
Our organization has covert control activities in place that remain unknown to employees and those with whom we interact, such as data analytics procedures designed to identify unusual transactions.		
Integrating With The Fraud Risk Assessment		
If the fraud risk assessment revealed that there are no control activities in place to mitigate an identified fraud risk, management has effectively addressed this issue by selecting, developing, and implementing the necessary controls to reduce this risk to an acceptable level.		



Appendix I-4.

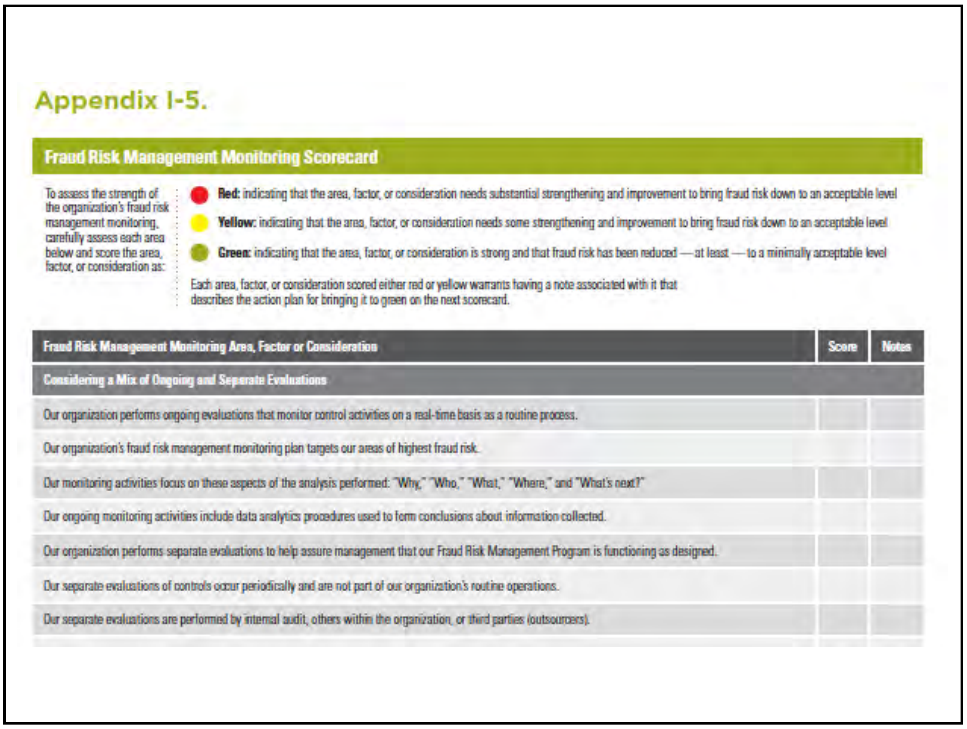
Fraud Investigation and Corrective Action Scorecard

To assess the strength of the organization's fraud investigation and corrective action processes, carefully assess each area below and score the area, factor, or consideration as:

- ● **Red:** indicating that the area, factor, or consideration needs substantial strengthening and improvement to bring fraud risk down to an acceptable level
- ● **Yellow:** indicating that the area, factor, or consideration needs some strengthening and improvement to bring fraud risk down to an acceptable level
- ● **Green:** indicating that the area, factor, or consideration is strong and that fraud risk has been reduced — at least — to a minimally acceptable level

Each area, factor, or consideration scored either red or yellow warrants having a note associated with it that describes the action plan for bringing it to green on the next scorecard.

Fraud Investigation and Corrective Action Area, Factor or Consideration	Score	Notes
Establishing Fraud Investigation and Response Protocols		
Our organizational culture promotes and supports open communication.		
Our organization ensures that any reasonably suspected or known violation, deviation, or other breach of code of conduct, fraud, or corruption is dealt with in a timely and effective manner.		
Our board and senior management positively encourage the identification of fraud by committing to an internal communication process.		
Our organization stresses the importance of having a documented process in place by which allegations of fraud are to be consistently captured, assessed, and responded to in a timely manner.		
Our fraud investigation and response system includes protocols for: • Updating a central repository for allegations and complaints • Maintaining anonymity or confidentiality of involved individuals, except as is necessary to investigate • Initially evaluating the allegations to determine if an investigation is warranted and the appropriate degrees of urgency • Notifying employees regarding document preservation and securing data systems • If necessary, engaging independent counsel and forensic accounting support • Conducting the investigation while controlling and safeguarding evidence • Reporting the results in the appropriate format (oral summary of key points or comprehensive written report with exhibits) • Following policies regarding retention of reports, documents, work papers, and other information • Assessing root causes and initiating mitigating processes and controls		
We have multiple communication paths by which allegations and complaints can be brought to the attention of our organization without naming the alleged perpetrator of fraud.		



Appendix I-5.

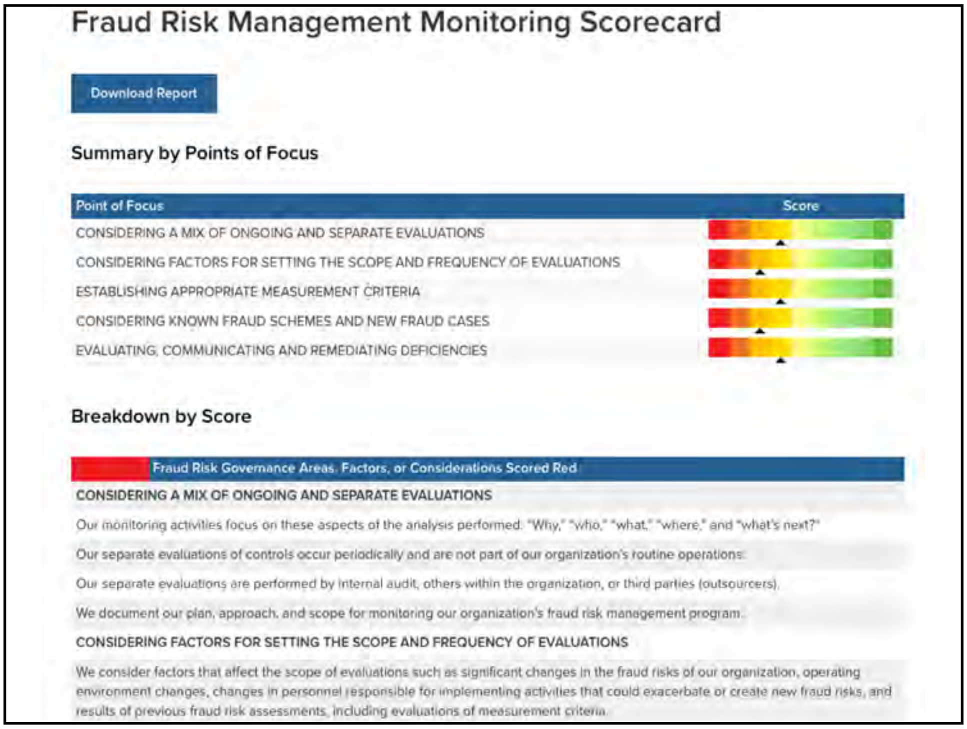
Fraud Risk Management Monitoring Scorecard

To assess the strength of the organization's fraud risk management monitoring, carefully assess each area below and score the area, factor, or consideration as:

- ● **Red:** indicating that the area, factor, or consideration needs substantial strengthening and improvement to bring fraud risk down to an acceptable level
- ● **Yellow:** indicating that the area, factor, or consideration needs some strengthening and improvement to bring fraud risk down to an acceptable level
- ● **Green:** indicating that the area, factor, or consideration is strong and that fraud risk has been reduced — at least — to a minimally acceptable level

Each area, factor, or consideration scored either red or yellow warrants having a note associated with it that describes the action plan for bringing it to green on the next scorecard.

Fraud Risk Management Monitoring Area, Factor or Consideration	Score	Notes
Considering a Mix of Ongoing and Separate Evaluations		
Our organization performs ongoing evaluations that monitor control activities on a real-time basis as a routine process.		
Our organization's fraud risk management monitoring plan targets our areas of highest fraud risk.		
Our monitoring activities focus on these aspects of the analysis performed: "Why," "Who," "What," "Where," and "What's next?"		
Our ongoing monitoring activities include data analytics procedures used to form conclusions about information collected.		
Our organization performs separate evaluations to help assure management that our Fraud Risk Management Program is functioning as designed.		
Our separate evaluations of controls occur periodically and are not part of our organization's routine operations.		
Our separate evaluations are performed by internal audit, others within the organization, or third parties (outsourcers).		



Fraud Risk Management Monitoring Scorecard

Summary by Points of Focus

Point of Focus	Score
CONSIDERING A MIX OF ONGOING AND SEPARATE EVALUATIONS	
CONSIDERING FACTORS FOR SETTING THE SCOPE AND FREQUENCY OF EVALUATIONS	
ESTABLISHING APPROPRIATE MEASUREMENT CRITERIA	
CONSIDERING KNOWN FRAUD SCHEMES AND NEW FRAUD CASES	
EVALUATING, COMMUNICATING AND REMEDIATING DEFICIENCIES	

Breakdown by Score

🟥 Fraud Risk Governance Areas, Factors, or Considerations Scored Red

CONSIDERING A MIX OF ONGOING AND SEPARATE EVALUATIONS

Our monitoring activities focus on these aspects of the analysis performed: "Why," "who," "what," "where," and "what's next?"

Our separate evaluations of controls occur periodically and are not part of our organization's routine operations.

Our separate evaluations are performed by internal audit, others within the organization, or third parties (outsourcers).

We document our plan, approach, and scope for monitoring our organization's fraud risk management program.

CONSIDERING FACTORS FOR SETTING THE SCOPE AND FREQUENCY OF EVALUATIONS

We consider factors that affect the scope of evaluations such as significant changes in the fraud risks of our organization, operating environment changes, changes in personnel responsible for implementing activities that could exacerbate or create new fraud risks, and results of previous fraud risk assessments, including evaluations of measurement criteria.

FRMG Appendices

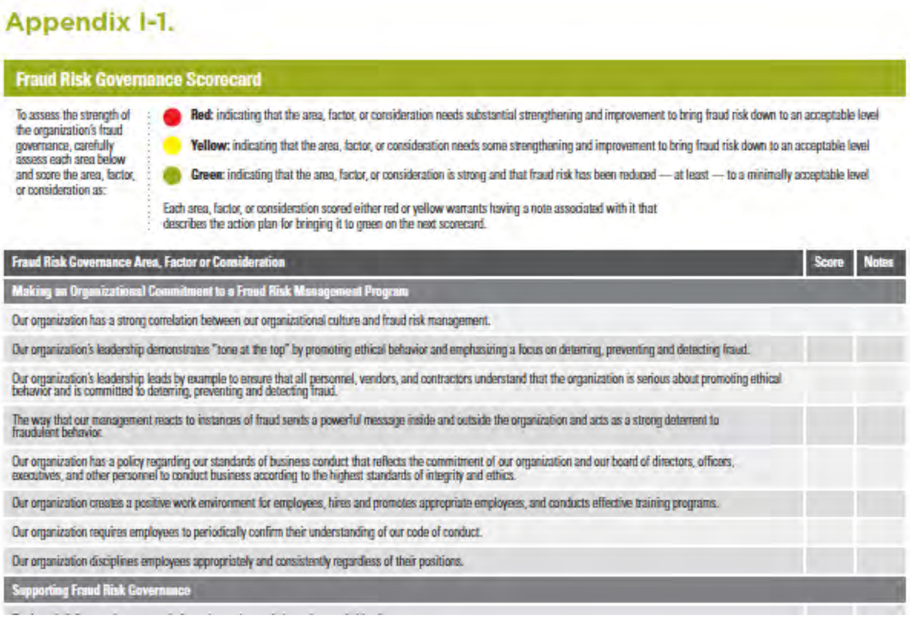
I: FRAUD RISK MANAGEMENT ASSESSMENT SCORECARDS

- I1: FRAUD RISK GOVERNANCE
- I2: FRAUD RISK ASSESSMENT
- I3: FRAUD CONTROL ACTIVITIES
- I4: FRAUD INVESTIGATION AND FOLLOWUP
- I5: FRAUD RISK MANAGEMENT MONITORING

J: HYPERLINKS TO ADDITIONAL TOOLS

HYPERLINKS TO ADDITIONAL TOOLS

- Interactive Scorecards



Appendix I-1.

Fraud Risk Governance Scorecard

To assess the strength of the organization's fraud governance, carefully assess each area below and score the area, factor, or consideration as:

- 🔴 **Red:** indicating that the area, factor, or consideration needs substantial strengthening and improvement to bring fraud risk down to an acceptable level
- 🟡 **Yellow:** indicating that the area, factor, or consideration needs some strengthening and improvement to bring fraud risk down to an acceptable level
- 🟢 **Green:** indicating that the area, factor, or consideration is strong and that fraud risk has been reduced — at least — to a minimally acceptable level

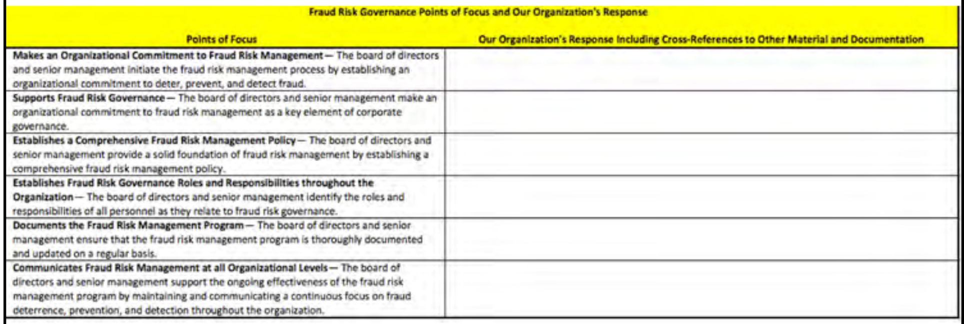
Each area, factor, or consideration scored either red or yellow warrants having a note associated with it that describes the action plan for bringing it to green on the next scorecard.

Fraud Risk Governance Area, Factor or Consideration	Score	Notes
Making an Organizational Commitment to a Fraud Risk Management Program		
Our organization has a strong correlation between our organizational culture and fraud risk management.		
Our organization's leadership demonstrates "tone at the top" by promoting ethical behavior and emphasizing a focus on deterring, preventing and detecting fraud.		
Our organization's leadership leads by example to ensure that all personnel, vendors, and contractors understand that the organization is serious about promoting ethical behavior and is committed to deterring, preventing and detecting fraud.		
The way that our management reacts to instances of fraud sends a powerful message inside and outside the organization and acts as a strong deterrent to fraudulent behavior.		
Our organization has a policy regarding our standards of business conduct that reflects the commitment of our organization and our board of directors, officers, executives, and other personnel to conduct business according to the highest standards of integrity and ethics.		
Our organization creates a positive work environment for employees, hires and promotes appropriate employees, and conducts effective training programs.		
Our organization requires employees to periodically confirm their understanding of our code of conduct.		
Our organization disciplines employees appropriately and consistently regardless of their positions.		
Supporting Fraud Risk Governance		

HYPERLINKS TO ADDITIONAL TOOLS

- Interactive Scorecards
- **Points of Focus Documentation Templates**

Points of Focus Documentation Templates



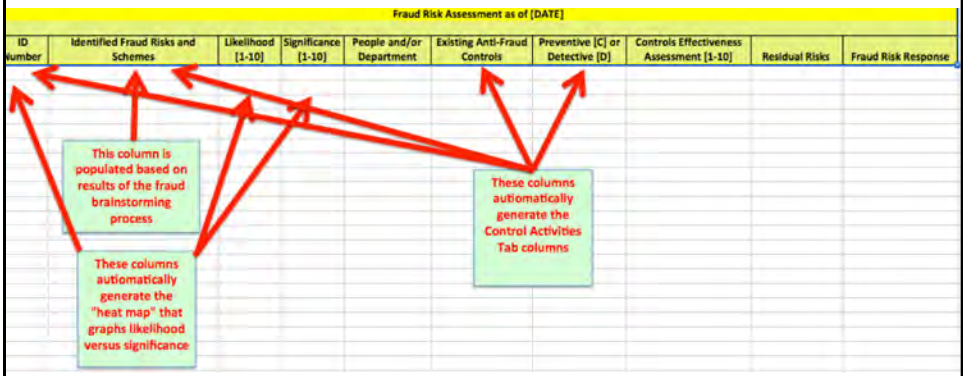
Fraud Risk Governance Points of Focus and Our Organization's Response

Points of Focus	Our Organization's Response Including Cross-References to Other Material and Documentation
Makes an Organizational Commitment to Fraud Risk Management— The board of directors and senior management initiate the fraud risk management process by establishing an organizational commitment to deter, prevent, and detect fraud.	
Supports Fraud Risk Governance— The board of directors and senior management make an organizational commitment to fraud risk management as a key element of corporate governance.	
Establishes a Comprehensive Fraud Risk Management Policy— The board of directors and senior management provide a solid foundation of fraud risk management by establishing a comprehensive fraud risk management policy.	
Establishes Fraud Risk Governance Roles and Responsibilities throughout the Organization— The board of directors and senior management identify the roles and responsibilities of all personnel as they relate to fraud risk governance.	
Documents the Fraud Risk Management Program— The board of directors and senior management ensure that the fraud risk management program is thoroughly documented and updated on a regular basis.	
Communicates Fraud Risk Management at all Organizational Levels— The board of directors and senior management support the ongoing effectiveness of the fraud risk management program by maintaining and communicating a continuous focus on fraud deterrence, prevention, and detection throughout the organization.	

HYPERLINKS TO ADDITIONAL TOOLS

- Interactive Scorecards
- Points of Focus Documentation Templates
- **Risk Assessment and Follow-up Actions Template**

Risk Assessment and Follow-up Actions Template



Fraud Risk Assessment as of [DATE]

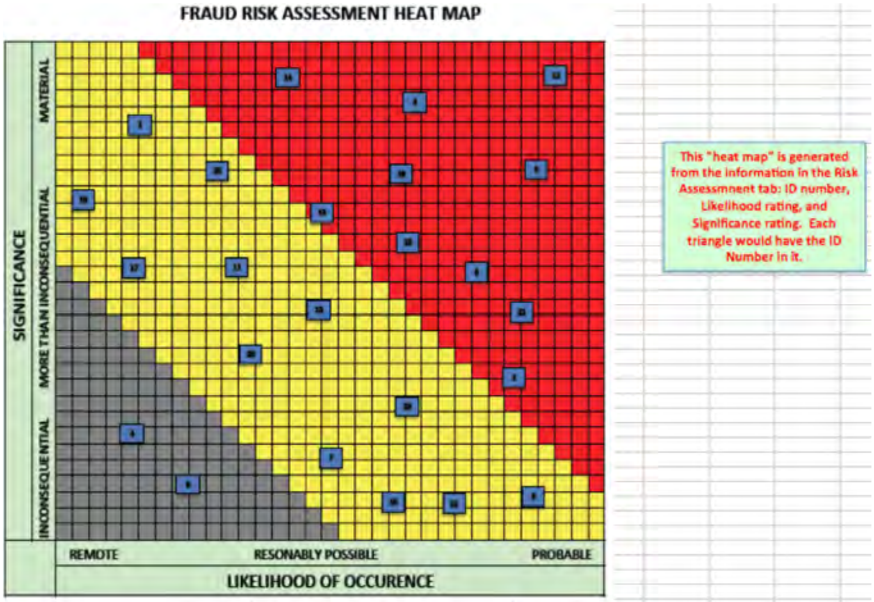
ID Number	Identified Fraud Risks and Schemes	Likelihood [1-10]	Significance [1-10]	People and/or Department	Existing Anti-Fraud Controls	Preventive [C] or Detective [D]	Controls Effectiveness Assessment [1-10]	Residual Risks	Fraud Risk Response

This column is populated based on results of the fraud brainstorming process

These columns autiomatically generate the "heat map" that graphs likelihood versus significance

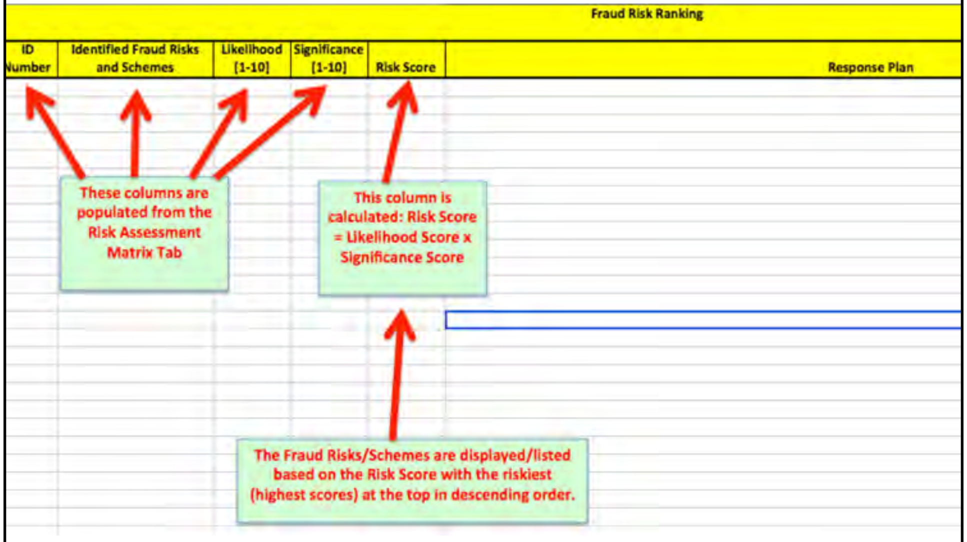
These columns autiomatically generate the Control Activities Tab columns

Fraud Risk Heat Map



This "heat map" is generated from the information in the Risk Assessmnent tab: ID number, Likelihood rating, and Significance rating. Each triangle would have the ID Number in it.

Fraud Risk Ranking Matrix



Fraud Risk Ranking

ID Number	Identified Fraud Risks and Schemes	Likelihood [1-10]	Significance [1-10]	Risk Score	Response Plan

These columns are populated from the Risk Assessment Matrix Tab

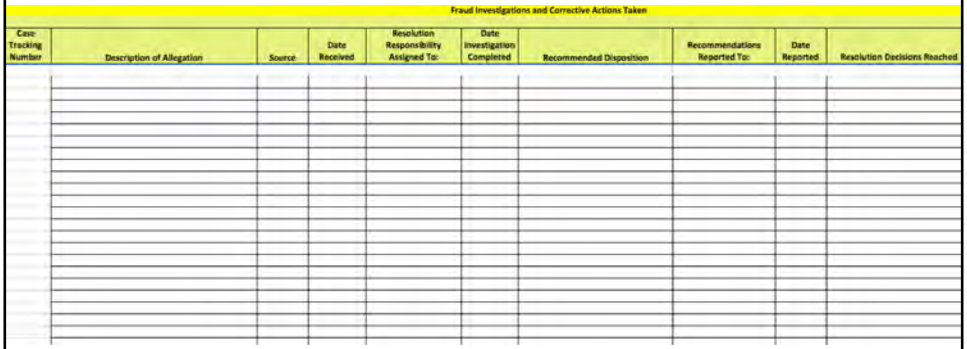
This column is calculated: Risk Score = Likelihood Score x Significance Score

The Fraud Risks/Schemes are displayed/listed based on the Risk Score with the riskiest (highest scores) at the top in descending order.

HYPERLINKS TO ADDITIONAL TOOLS

- Interactive Scorecards
- Points of Focus Documentation Templates
- Risk Assessment and Follow-up Actions Template
- **Log for allegations of fraud and investigation results**

Log for allegations of fraud and investigation results

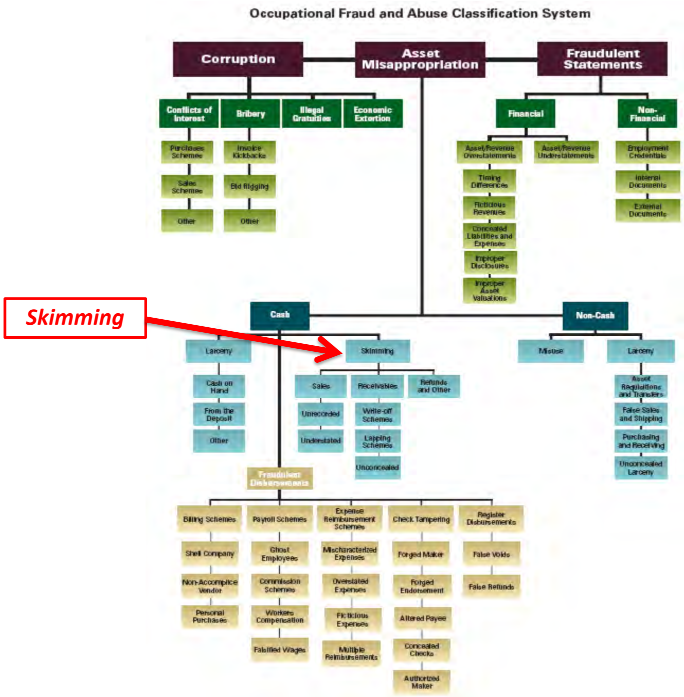


Fraud Investigations and Corrective Actions Taken

Case Tracking Number	Description of Allegation	Source	Date Received	Resolution Responsibility Assigned To:	Date Investigation Completed	Recommended Disposition	Recommendations Reported To:	Date Reported	Resolution Decisions Reached

HYPERLINKS TO ADDITIONAL TOOLS

- Interactive Scorecards
- Points of Focus Documentation Templates
- Risk Assessment and Follow-up Actions Template
- Log for allegations of fraud and investigation results
- Interactive Scorecards
- **Library of Data Analytics Tests**

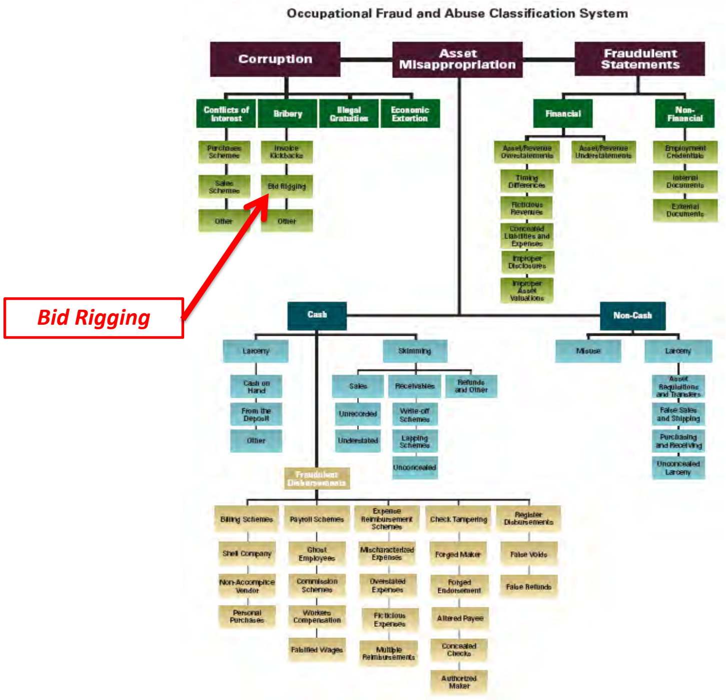

Occupational Fraud and Abuse Classification System

Skimming

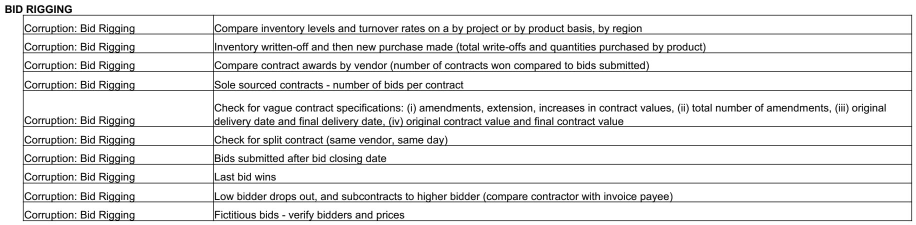
Library of Data Analytics Tests

CASH - SKIMMING

Cash Receipts Analysis	Review sequential numbering of cash receipts journal to ensure no out-of-sequence numbers
Vertical Analysis	Vertical analysis of sales accounts, (i.e., cash as a percentage of total assets over time, etc. can be used to detect skimming at a high level)
Horizontal Analysis	Horizontal analysis of sales accounts, (i.e., cash percent change over time, can be used to detect skimming at a high level)
Current Ratio Analysis	Track current assets to current liabilities over time
Quick Ratio Analysis	(Cash+Securities+Receivables) over Current Liabilities percent change over time
Inventory Analysis	Track inventory shrinkage due to unrecorded sales. Inventory detection may include statistical sampling, trend analysis, reviews of receiving reports and inventory records and verification for material requisition and shipping documentation as well as actual physical inventory counts
Red Flags	Bank employee questions the validity of a check
Red Flags	Inspect for a forged endorsement on a check
Red Flags	Inspect for an employee bank account with a name similar to the company name
Red Flags	Inspect for alteration of the check payee or endorsement
Journal Entry Review	Analysis of journal entries made to the cash and inventory accounts to identify: (1) False credits to inventory to conceal unrecorded or understated sales, (2) Write-offs related to lost, stolen or obsolete product, (3) Write-offs to accounts receivable, (4) Irregular entries to cash accounts
Journal Entry Review	Analysis of journal entries to review suspicous or inaccurate journal entries.
Journal Entry Review	Identify larger entries split into smaller entries to avoid exceeding their approval limit. To ensure authorization and validity of the Journal Entry based on the approval limits

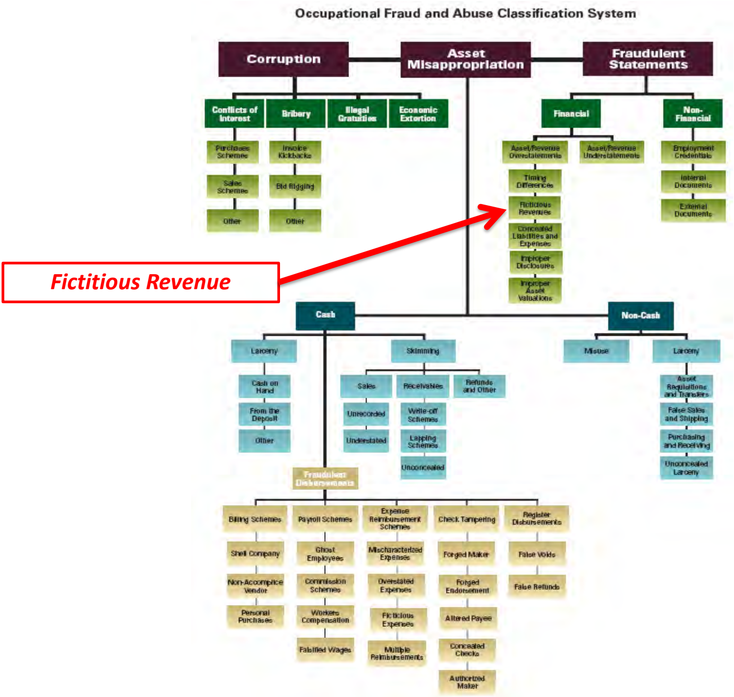


Library of Data Analytics Tests



BID RIGGING

Corruption: Bid Rigging	Compare inventory levels and turnover rates on a by project or by product basis, by region
Corruption: Bid Rigging	Inventory written-off and then new purchase made (total write-offs and quantities purchased by product)
Corruption: Bid Rigging	Compare contract awards by vendor (number of contracts won compared to bids submitted)
Corruption: Bid Rigging	Sole sourced contracts - number of bids per contract
Corruption: Bid Rigging	Check for vague contract specifications: (i) amendments, extension, increases in contract values, (ii) total number of amendments, (iii) original delivery date and final delivery date, (iv) original contract value and final contract value
Corruption: Bid Rigging	Check for split contract (same vendor, same day)
Corruption: Bid Rigging	Bids submitted after bid closing date
Corruption: Bid Rigging	Last bid wins
Corruption: Bid Rigging	Low bidder drops out, and subcontracts to higher bidder (compare contractor with invoice payee)
Corruption: Bid Rigging	Fictitious bids - verify bidders and prices



Occupational Fraud and Abuse Classification System

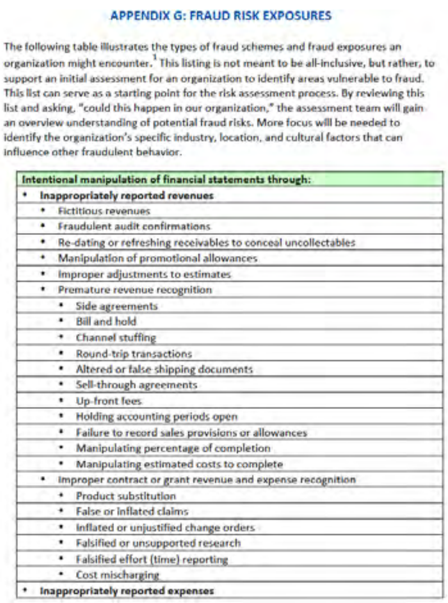
Fictitious Revenue

Library of Data Analytics Tests

REVENUE RECOGNITION

Bill & Hold	Analysis of inventory that has been "segregated" or shipped to a third party intermediary where the customer has not taken title and assumed the risks, yet the company has booked this isolated inventory as revenue
Bill & Hold	Identify revenue and receivables recorded prior to shipment
Channel Stuffing	Compare discounts or incentives on a monthly basis to identify unusual spikes at the end of the quarter or year.
Channel Stuffing	Compare sales and corresponding returns on a per customer basis
Debt Swap	Identification of Journal Entries with Net Debit to Liability and Credit to Revenue
Debt Swap	Identification of Journal Entries with Net Debit to Liability and Credit to Expenses
Fake Invoices	Analysis of sequentially numbered invoices
Fake Invoices	Benford's analysis of the first two digits to identify anomalies such as a disproportionate number of invoices starting with 7, 8 or 9
Fake Invoices	Analysis of company names that "sound like" known vendors
Fake Invoices	Examine inventory records to identify locations or items that require specific attention during or after the physical inventory count
Revenue Recognition	Analysis and anomaly detection of the sequence of transactions to identify missing checks, invoices
Revenue Recognition	Compare A/R credit memos to A/P invoices
Revenue Recognition	Compare revenue reported by month and by product line during the current period with comparable prior periods
Revenue Recognition	Confirm with selected, high risk customers relevant contract terms or question company staff regarding shipments near the end of the period
Revenue Recognition	Identification of revenue recognized at period end and subsequently reversed or partially reversed
Fraud Triangle Analytics	E-mail analysis of selected employees (accounting or sales) for "Rev Rec" related key words around incentive/pressure, opportunity and rationalization

NEW TOOL—COMING SOON



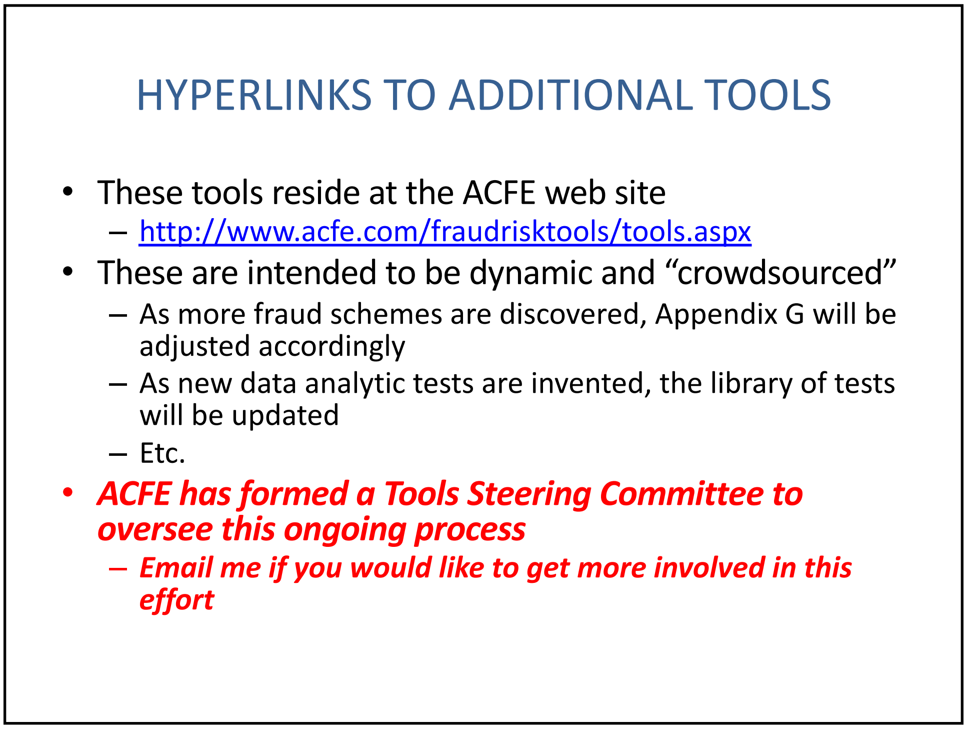
APPENDIX G: FRAUD RISK EXPOSURES

The following table illustrates the types of fraud schemes and fraud exposures an organization might encounter.[1] This listing is not meant to be all-inclusive, but rather, to support an initial assessment for an organization to identify areas vulnerable to fraud. This list can serve as a starting point for the risk assessment process. By reviewing this list and asking, "could this happen in our organization," the assessment team will gain an overview understanding of potential fraud risks. More focus will be needed to identify the organization's specific industry, location, and cultural factors that can influence other fraudulent behavior.

Intentional manipulation of financial statements through:
• **Inappropriately reported revenues**
• Fictitious revenues
• Fraudulent audit confirmations
• Re-dating or refreshing receivables to conceal uncollectables
• Manipulation of promotional allowances
• Improper adjustments to estimates
• Premature revenue recognition
• Side agreements
• Bill and hold
• Channel stuffing
• Round-trip transactions
• Altered or false shipping documents
• Sell-through agreements
• Up-front fees
• Holding accounting periods open
• Failure to record sales provisions or allowances
• Manipulating percentage of completion
• Manipulating estimated costs to complete
• Improper contract or grant revenue and expense recognition
• Product substitution
• False or inflated claims
• Inflated or unjustified change orders
• Falsified or unsupported research
• Falsified effort (time) reporting
• Cost mischarging
• **Inappropriately reported expenses**

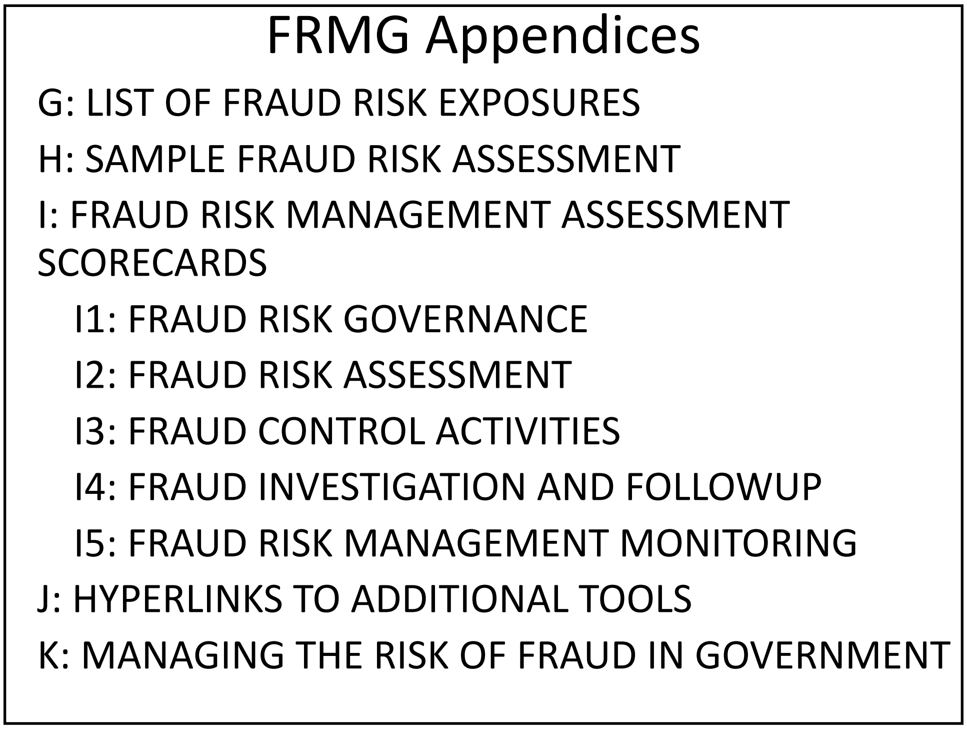
List of fraud schemes, hyperlinked to underlying definitions and descriptions.

To be expanded through crowdsourcing.



HYPERLINKS TO ADDITIONAL TOOLS

- These tools reside at the ACFE web site
  - http://www.acfe.com/fraudrisktools/tools.aspx
- These are intended to be dynamic and "crowdsourced"
  - As more fraud schemes are discovered, Appendix G will be adjusted accordingly
  - As new data analytic tests are invented, the library of tests will be updated
  - Etc.
- ***ACFE has formed a Tools Steering Committee to oversee this ongoing process***
  - ***Email me if you would like to get more involved in this effort***



FRMG Appendices

G: LIST OF FRAUD RISK EXPOSURES

H: SAMPLE FRAUD RISK ASSESSMENT

I: FRAUD RISK MANAGEMENT ASSESSMENT SCORECARDS

I1: FRAUD RISK GOVERNANCE

I2: FRAUD RISK ASSESSMENT

I3: FRAUD CONTROL ACTIVITIES

I4: FRAUD INVESTIGATION AND FOLLOWUP

I5: FRAUD RISK MANAGEMENT MONITORING

J: HYPERLINKS TO ADDITIONAL TOOLS

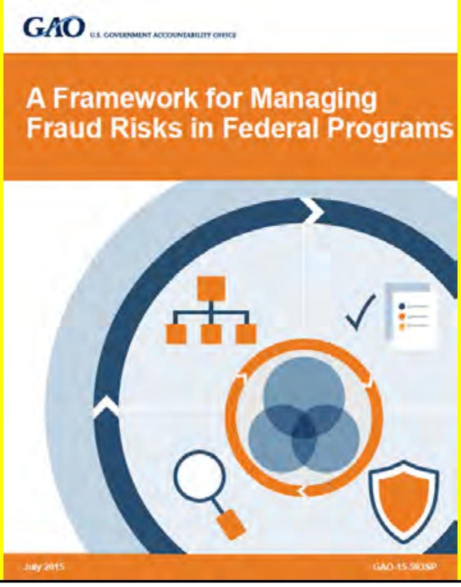
K: MANAGING THE RISK OF FRAUD IN GOVERNMENT

Still not convinced that you need Fraud Risk Management?

- Go to http://www.cottoncpa.com/outreach/thought-leadership/ and download and print the five scorecards
- Go to Staples and buy some red, yellow, and green dots
- At your next board retreat or senior staff meeting, use the scorecards to self assess
- Tape those scorecards on the wall and step back
- If you see a lot of RED, you definitely need to implement fraud risk management

For those of us who work in or for government

GAO's Fraud Risk Management Framework: Not Just for Federal Agencies



GAO U.S. GOVERNMENT ACCOUNTABILITY OFFICE

A Framework for Managing Fraud Risks in Federal Programs

July 2015

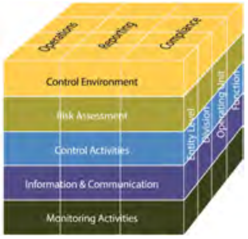
GAO-15-593SP

GAO's Fraud Risk Management Framework

"While the primary target audience of this study is managers in the U.S. federal government, the practices and concepts described in the Framework may also be applicable to state, local, and foreign government agencies, as well as nonprofit entities that are responsible for fraud risk management."

Alignment with COSO

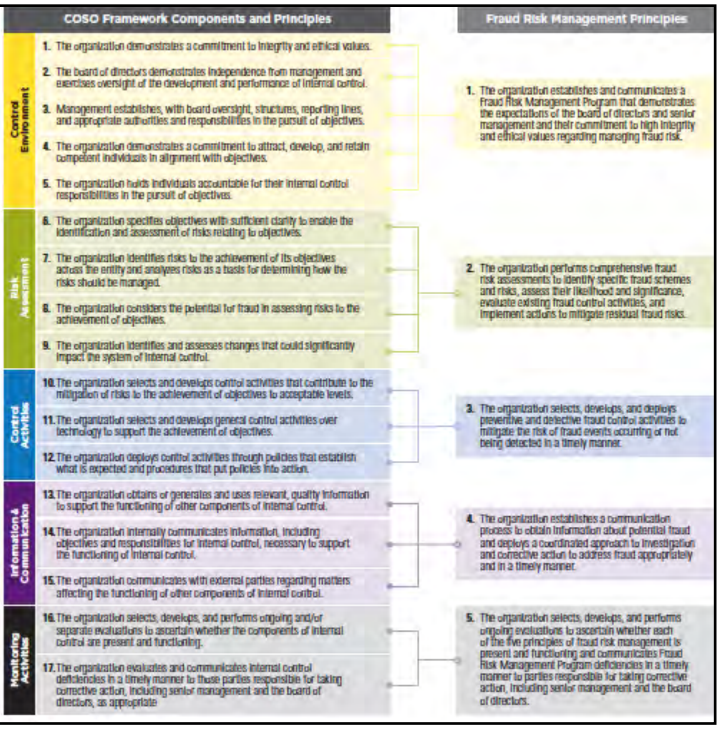
- **The COSO Internal Control—Integrated Framework has 5 components**
  - Control Environment
  - Risk Assessment
  - Has Control Activities
  - Information & Communication
  - Monitoring Activities



- **The GAO Green Book (Standards for Internal Control in the Federal Government) has the same 5 components**
- **The COSO ACFE Fraud Risk Management Guide maps to both the COSO internal Control Framework and the Green Book**

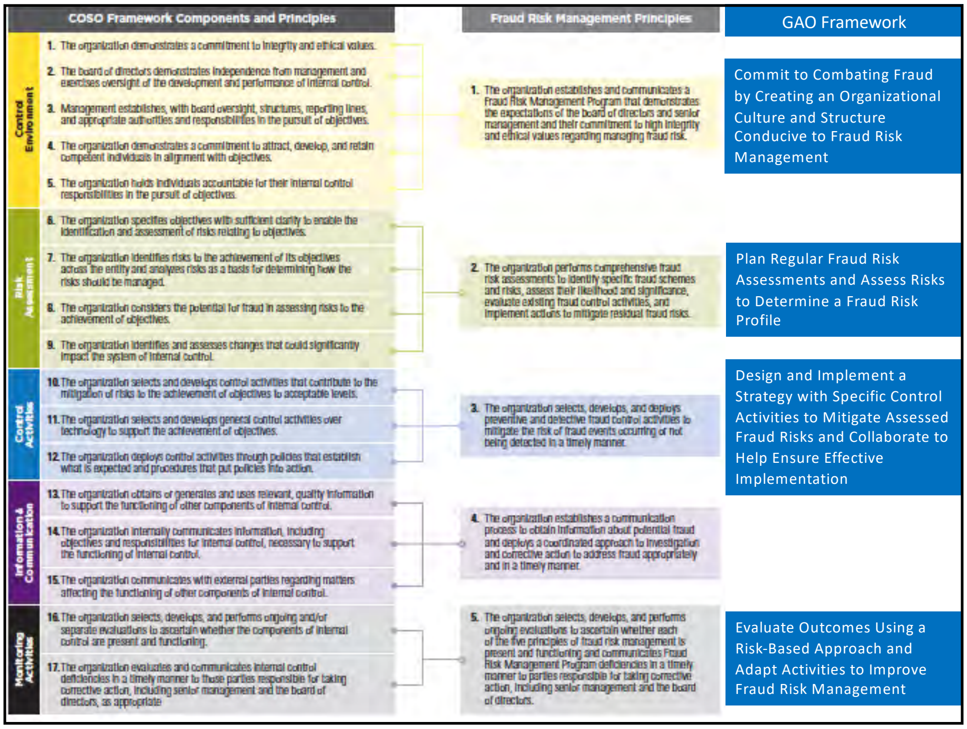
Cotton& Company

Mapping of COSO Components and Principles to the Fraud Risk Management Guide



	COSO Framework Components and Principles	Fraud Risk Management Principles
Control Environment	1. The organization demonstrates a commitment to integrity and ethical values.	1. The organization establishes and communicates a Fraud Risk Management Program that demonstrates the expectations of the board of directors and senior management and their commitment to high integrity and ethical values regarding managing fraud risk.
	2. The board of directors demonstrates independence from management and exercises oversight of the development and performance of internal control.	
	3. Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives.	
	4. The organization demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.	
	5. The organization holds individuals accountable for their internal control responsibilities in the pursuit of objectives.	
Risk Assessment	6. The organization specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives.	2. The organization performs comprehensive fraud risk assessments to identify specific fraud schemes and risks, assess their likelihood and significance, evaluate existing fraud control activities, and implement actions to mitigate residual fraud risks.
	7. The organization identifies risks to the achievement of its objectives across the entity and analyzes risks as a basis for determining how the risks should be managed.	
	8. The organization considers the potential for fraud in assessing risks to the achievement of objectives.	
	9. The organization identifies and assesses changes that could significantly impact the system of internal control.	
Control Activities	10. The organization selects and develops control activities that contribute to the mitigation of risks to the achievement of objectives to acceptable levels.	3. The organization selects, develops, and deploys preventive and detective fraud control activities to mitigate the risk of fraud events occurring or not being detected in a timely manner.
	11. The organization selects and develops general control activities over technology to support the achievement of objectives.	
	12. The organization deploys control activities through policies that establish what is expected and procedures that put policies into action.	
Information & Communication	13. The organization obtains or generates and uses relevant, quality information to support the functioning of other components of internal control.	4. The organization establishes a communication process to obtain information about potential fraud and deploys a coordinated approach to investigation and corrective action to address fraud appropriately and in a timely manner.
	14. The organization internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.	
	15. The organization communicates with external parties regarding matters affecting the functioning of other components of internal control.	
Monitoring Activities	16. The organization selects, develops, and performs ongoing and/or separate evaluations to ascertain whether the components of internal control are present and functioning.	5. The organization selects, develops, and performs ongoing evaluations to ascertain whether each of the five principles of fraud risk management is present and functioning and communicates Fraud Risk Management Program deficiencies in a timely manner to parties responsible for taking corrective action, including senior management and the board of directors.
	17. The organization evaluates and communicates internal control deficiencies in a timely manner to those parties responsible for taking corrective action, including senior management and the board of directors, as appropriate	

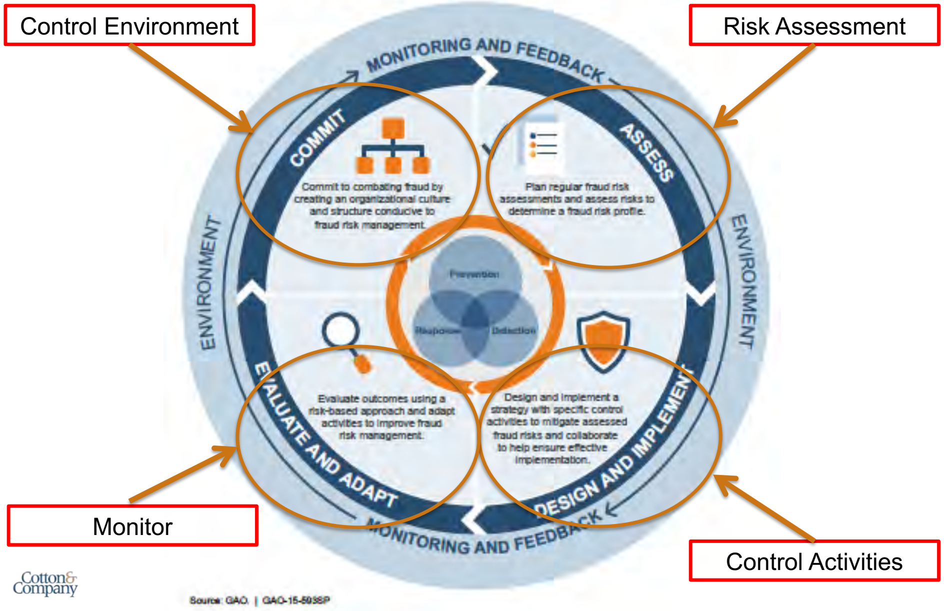
Cotton& Company



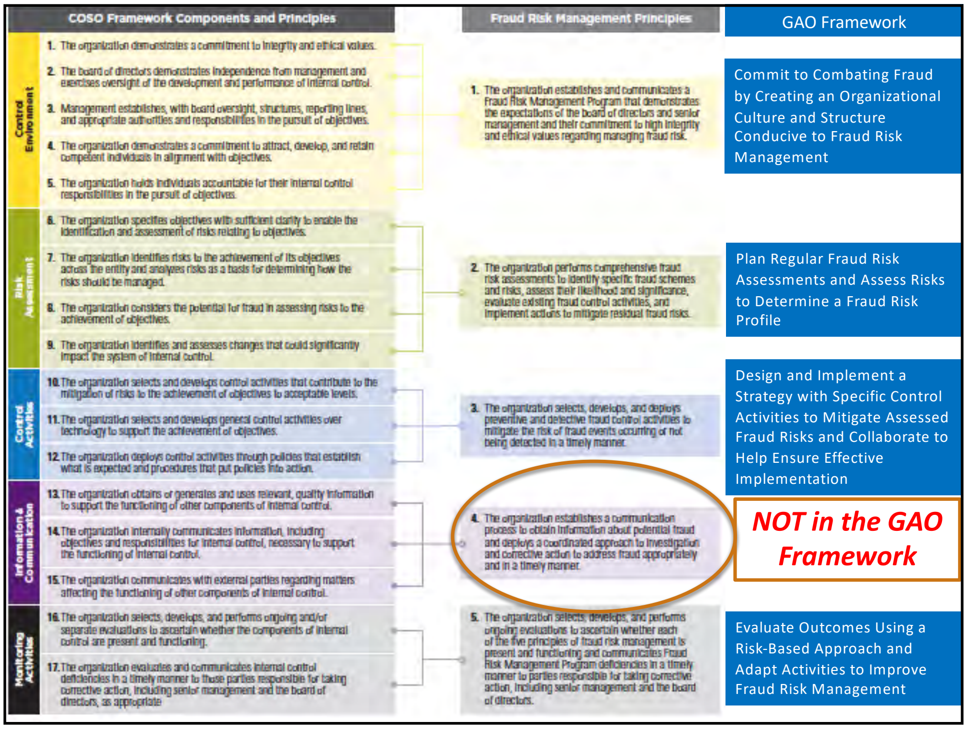
COSO Framework Components and Principles		Fraud Risk Management Principles	GAO Framework
Control Environment	1. The organization demonstrates a commitment to integrity and ethical values. 2. The board of directors demonstrates independence from management and exercises oversight of the development and performance of internal control. 3. Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives. 4. The organization demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives. 5. The organization holds individuals accountable for their internal control responsibilities in the pursuit of objectives.	1. The organization establishes and communicates a Fraud Risk Management Program that demonstrates the expectations of the board of directors and senior management and their commitment to high integrity and ethical values regarding managing fraud risk.	Commit to Combating Fraud by Creating an Organizational Culture and Structure Conducive to Fraud Risk Management
Risk Assessment	6. The organization specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives. 7. The organization identifies risks to the achievement of its objectives across the entity and analyzes risks as a basis for determining how the risks should be managed. 8. The organization considers the potential for fraud in assessing risks to the achievement of objectives. 9. The organization identifies and assesses changes that could significantly impact the system of internal control.	2. The organization performs comprehensive fraud risk assessments to identify specific fraud schemes and risks, assess their likelihood and significance, evaluate existing fraud control activities, and implement actions to mitigate residual fraud risks.	Plan Regular Fraud Risk Assessments and Assess Risks to Determine a Fraud Risk Profile
Control Activities	10. The organization selects and develops control activities that contribute to the mitigation of risks to the achievement of objectives to acceptable levels. 11. The organization selects and develops general control activities over technology to support the achievement of objectives. 12. The organization deploys control activities through policies that establish what is expected and procedures that put policies into action.	3. The organization selects, develops, and deploys preventive and detective fraud control activities to mitigate the risk of fraud events occurring or not being detected in a timely manner.	Design and Implement a Strategy with Specific Control Activities to Mitigate Assessed Fraud Risks and Collaborate to Help Ensure Effective Implementation
Information & Communication	13. The organization obtains or generates and uses relevant, quality information to support the functioning of other components of internal control. 14. The organization internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control. 15. The organization communicates with external parties regarding matters affecting the functioning of other components of internal control.	4. The organization establishes a communication process to obtain information about potential fraud and deploys a coordinated approach to investigation and corrective action to address fraud appropriately and in a timely manner.	
Monitoring Activities	16. The organization selects, develops, and performs ongoing and/or separate evaluations to ascertain whether the components of internal control are present and functioning. 17. The organization evaluates and communicates internal control deficiencies in a timely manner to those parties responsible for taking corrective action, including senior management and the board of directors, as appropriate	5. The organization selects, develops, and performs ongoing evaluations to ascertain whether each of the five principles of fraud risk management is present and functioning and communicates Fraud Risk Management Program deficiencies in a timely manner to parties responsible for taking corrective action, including senior management and the board of directors.	Evaluate Outcomes Using a Risk-Based Approach and Adapt Activities to Improve Fraud Risk Management

Nutshell View—Alignment with COSO

Figure 2: The Fraud Risk Management Framework


Control Environment
Risk Assessment
MONITORING AND FEEDBACK
COMMIT
Commit to combating fraud by creating an organizational culture and structure conducive to fraud risk management.
ASSESS
Plan regular fraud risk assessments and assess risks to determine a fraud risk profile.
ENVIRONMENT
ENVIRONMENT
Prevention
Response
Detection
Evaluate outcomes using a risk-based approach and adapt activities to improve fraud risk management.
EVALUATE AND ADAPT
Design and implement a strategy with specific control activities to mitigate assessed fraud risks and collaborate to help ensure effective implementation.
DESIGN AND IMPLEMENT
MONITORING AND FEEDBACK
Monitor
Control Activities

Source: GAO. | GAO-15-593SP



COSO Framework Components and Principles

Control Environment

1. The organization demonstrates a commitment to integrity and ethical values.
2. The board of directors demonstrates independence from management and exercises oversight of the development and performance of internal control.
3. Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives.
4. The organization demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.
5. The organization holds individuals accountable for their internal control responsibilities in the pursuit of objectives.

Risk Assessment

6. The organization specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives.
7. The organization identifies risks to the achievement of its objectives across the entity and analyzes risks as a basis for determining how the risks should be managed.
8. The organization considers the potential for fraud in assessing risks to the achievement of objectives.
9. The organization identifies and assesses changes that could significantly impact the system of internal control.

Control Activities

10. The organization selects and develops control activities that contribute to the mitigation of risks to the achievement of objectives to acceptable levels.
11. The organization selects and develops general control activities over technology to support the achievement of objectives.
12. The organization deploys control activities through policies that establish what is expected and procedures that put policies into action.

Information & Communication

13. The organization obtains or generates and uses relevant, quality information to support the functioning of other components of internal control.
14. The organization internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.
15. The organization communicates with external parties regarding matters affecting the functioning of other components of internal control.

Monitoring Activities

16. The organization selects, develops, and performs ongoing and/or separate evaluations to ascertain whether the components of internal control are present and functioning.
17. The organization evaluates and communicates internal control deficiencies in a timely manner to those parties responsible for taking corrective action, including senior management and the board of directors, as appropriate

Fraud Risk Management Principles

1. The organization establishes and communicates a Fraud Risk Management Program that demonstrates the expectations of the board of directors and senior management and their commitment to high integrity and ethical values regarding managing fraud risk.
2. The organization performs comprehensive fraud risk assessments to identify specific fraud schemes and risks, assess their likelihood and significance, evaluate existing fraud control activities, and implement actions to mitigate residual fraud risks.
3. The organization selects, develops, and deploys preventive and detective fraud control activities to mitigate the risk of fraud events occurring or not being detected in a timely manner.
4. The organization establishes a communication process to obtain information about potential fraud and deploys a coordinated approach to investigation and corrective action to address fraud appropriately and in a timely manner.
5. The organization selects, develops, and performs ongoing evaluations to ascertain whether each of the five principles of fraud risk management is present and functioning and communicates Fraud Risk Management Program deficiencies in a timely manner to parties responsible for taking corrective action, including senior management and the board of directors.

GAO Framework

Commit to Combating Fraud by Creating an Organizational Culture and Structure Conducive to Fraud Risk Management

Plan Regular Fraud Risk Assessments and Assess Risks to Determine a Fraud Risk Profile

Design and Implement a Strategy with Specific Control Activities to Mitigate Assessed Fraud Risks and Collaborate to Help Ensure Effective Implementation

NOT in the GAO Framework

Evaluate Outcomes Using a Risk-Based Approach and Adapt Activities to Improve Fraud Risk Management

Nutshell View—Alignment with COSO

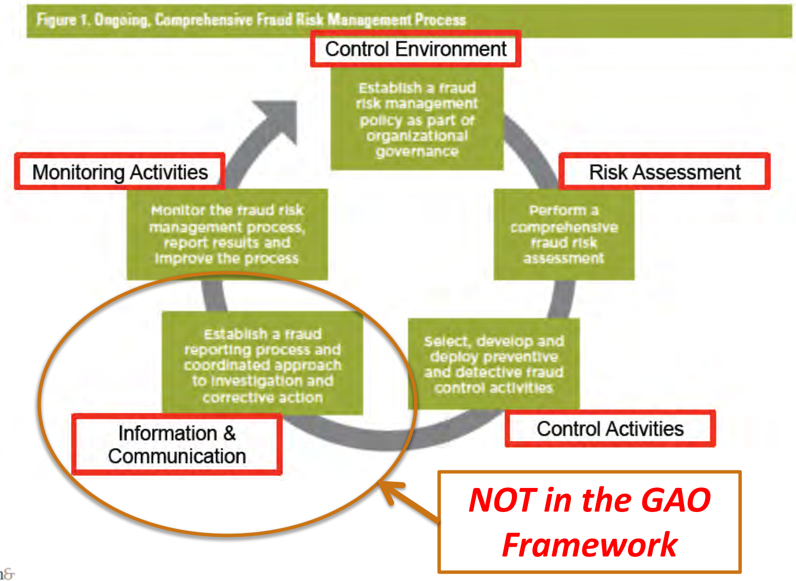


Figure 1. Ongoing, Comprehensive Fraud Risk Management Process
Control Environment
Establish a fraud risk management policy as part of organizational governance
Risk Assessment
Perform a comprehensive fraud risk assessment
Select, develop and deploy preventive and detective fraud control activities
Control Activities
Establish a fraud reporting process and coordinated approach to investigation and corrective action
Information & Communication
Monitoring Activities
Monitor the fraud risk management process, report results and improve the process
NOT in the GAO Framework

Nutshell View—Alignment with COSO

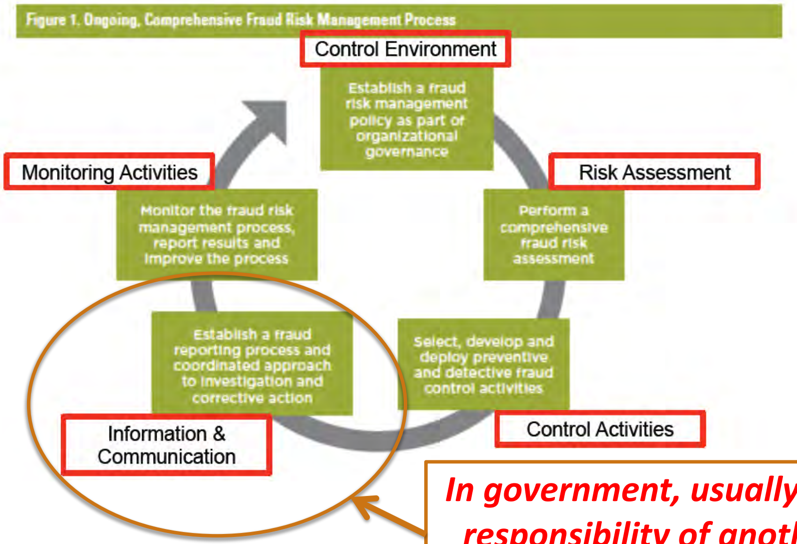


Figure 1. Ongoing, Comprehensive Fraud Risk Management Process

Control Environment

Establish a fraud risk management policy as part of organizational governance

Risk Assessment

Perform a comprehensive fraud risk assessment

Select, develop and deploy preventive and detective fraud control activities

Control Activities

Establish a fraud reporting process and coordinated approach to investigation and corrective action

Information & Communication

Monitoring Activities

Monitor the fraud risk management process, report results and improve the process

In government, usually the responsibility of another office—e.g., OIG

Cotton& Company

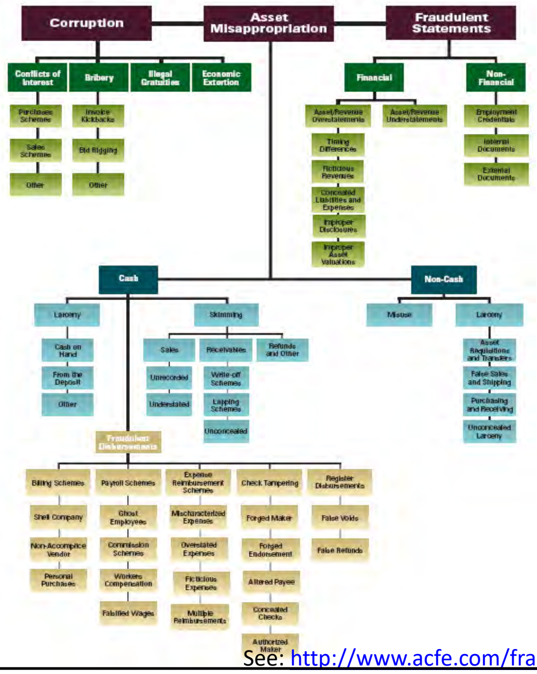
My Predictions for the Future: What Can/Should Be Done to Empower Auditors to Find More Fraud; and Help Organizations Better Manage Fraud?

114

What Can We Expect to See in the Future?

- Data analytics will be where most of the focus will be

Occupational Fraud and Abuse Classification System



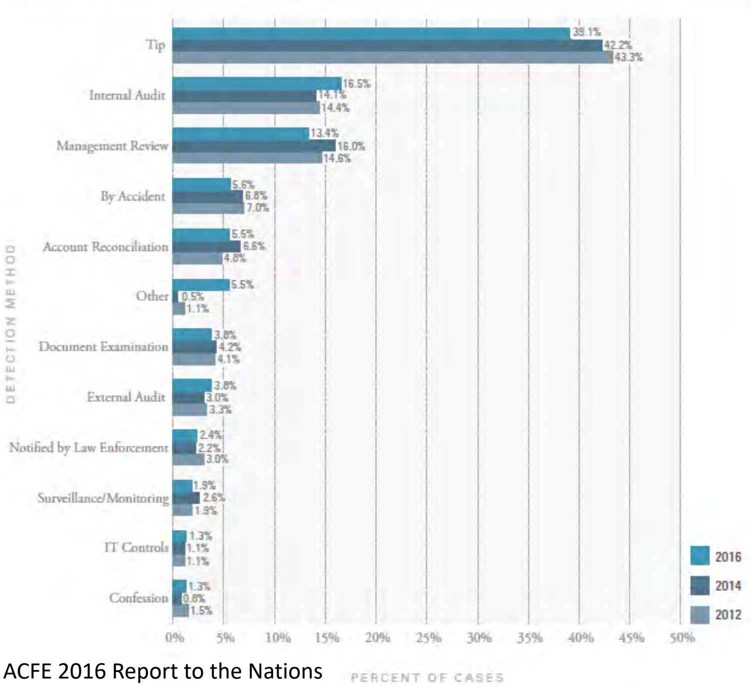
See: http://www.acfe.com/fraudrisktools/tools.aspx

What Can We Expect to See in the Future?

- Data analytics will be where most of the focus will be
- More emphasis on “hotline” employee reporting

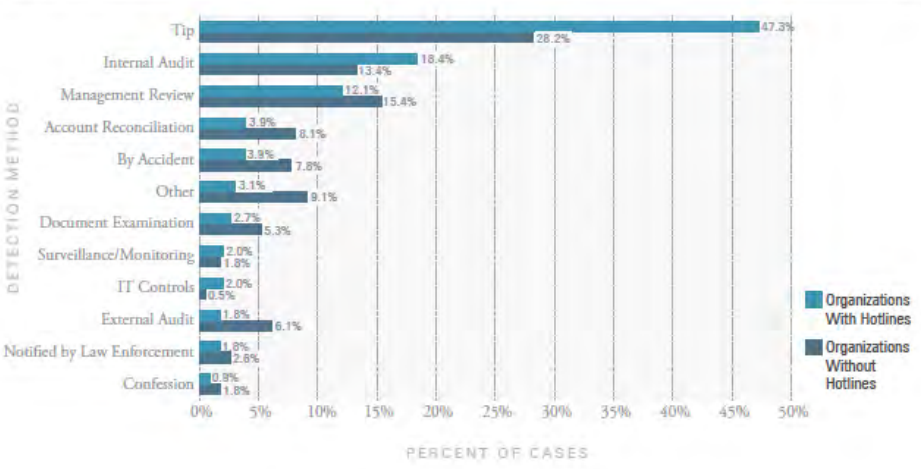
117

Figure 21: Initial Detection of Occupational Frauds



Source: ACFE 2016 Report to the Nations

Figure 34: Impact of Hotlines



Source: ACFE 2016 Report to the Nations

What Can We Expect to See in the Future?

- Data analytics will be where most of the focus will be
- More emphasis on “hotline” employee reporting
- More auditor focus on fraud risk management (FRM)

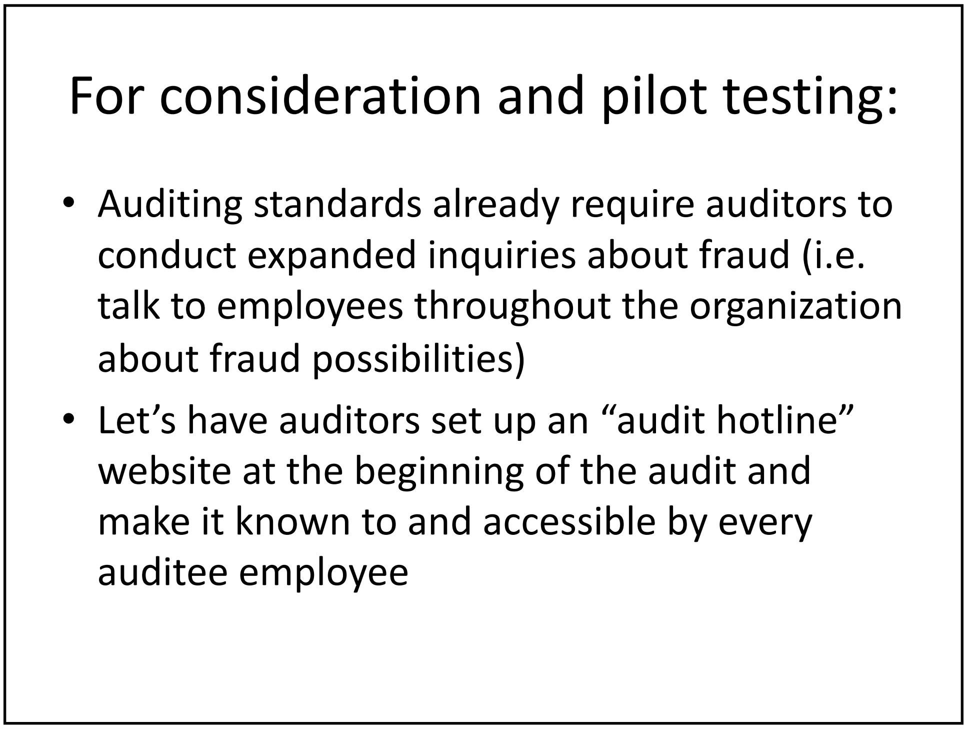
120

What Does FRM Mean for External Auditors?

- External auditors are required to assess fraud risk
- Audits are risk-based: higher risk = more audit work needed = higher audit fees
- If you tell your auditors that you have implemented rigorous fraud risk management processes, their assessment of fraud risk should go down …

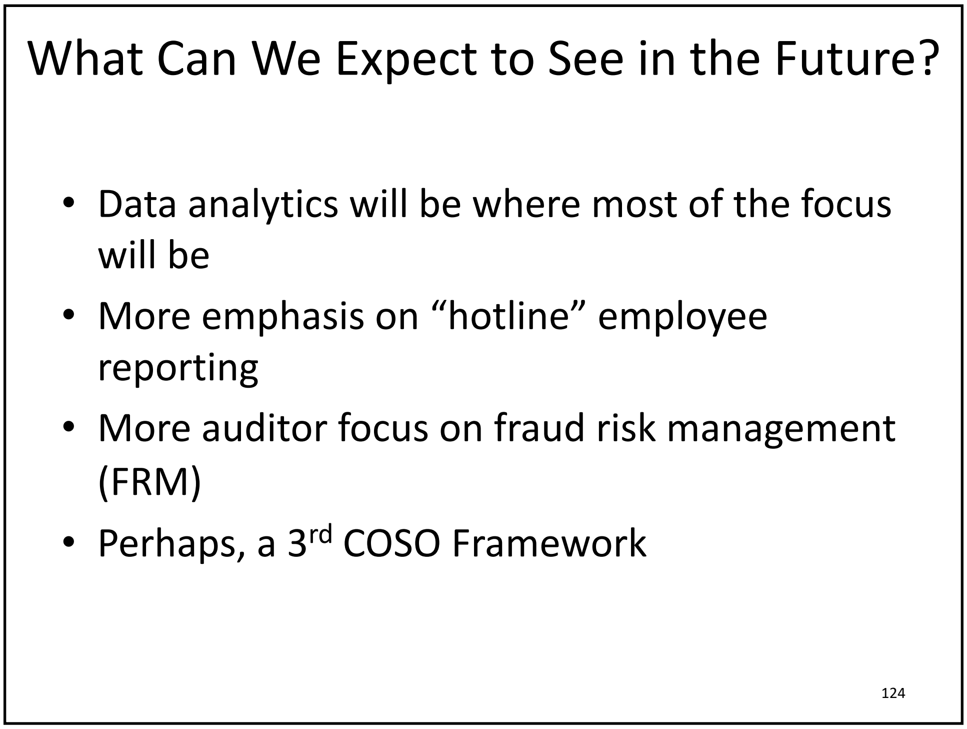
Prediction:

- Auditing standards will be revised to *REQUIRE* auditors to evaluate and test management's fraud risk management system and processes
- Similar to the existing requirement that auditors must evaluate and test management's system of internal control



For consideration and pilot testing:

- Auditing standards already require auditors to conduct expanded inquiries about fraud (i.e. talk to employees throughout the organization about fraud possibilities)
- Let’s have auditors set up an “audit hotline” website at the beginning of the audit and make it known to and accessible by every auditee employee



What Can We Expect to See in the Future?

- Data analytics will be where most of the focus will be
- More emphasis on “hotline” employee reporting
- More auditor focus on fraud risk management (FRM)
- Perhaps, a 3rd COSO Framework

COSO Frameworks

[81]

COSO
Committee of Sponsoring Organizations of the Treadway Commission
Internal Control — Integrated Framework
Executive Summary

[4]

COSO
Enterprise Risk Management
Aligning Risk with Strategy and Performance

[2,862]

Coming soon ...

Fraud
Risk Management
Guide

New York State Internal Control Association

Internal Control, Fraud & Risk Management
May 9, 2019
Annual Spring Conference

Fraud Risk Management and Assessment

David L. Cotton, CPA, CFE, CGFM
Cotton & Company LLP
Alexandria, VA 22314
www.cottoncpa.com
dcotton@cottoncpa.com