



52nd Annual Virginia Accounting & Auditing  
Conference

## *The ACFE/COSO Fraud Risk Management Guide: 2022 Edition*

Dave Cotton, CFE, CPA, CGFM

Cotton

A MEMBER COMPANY

333 John Carlyle Street | Alexandria, VA 22314

[www.cottoncpa.com](http://www.cottoncpa.com)

**DAVID L. COTTON, CPA, CFE, CGFM**  
**CHAIRMAN EMERITUS, COTTON & COMPANY**

Dave Cotton is founder and Chairman Emeritus of Cotton & Company, Certified Public Accountants, headquartered in Alexandria, Virginia. Cotton & Company was founded in 1981 and has a practice concentration in assisting Federal and State 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 organizations, programs, activities, and functions. In April 2022, Cotton & Company became a wholly-owned subsidiary of Sikich LLP.

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. Defense Security Cooperation Agency, 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 and an MBA in management science and labor relations from Lehigh University in Bethlehem, PA. He also pursued graduate studies in accounting and auditing at the University of Chicago Graduate School of Business. 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). 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 is currently co-chairing a task force to update the **COSO-ACFE Fraud Risk Management Guide**. In May 2022, Governor Glenn Youngkin appointed Dave to the Virginia Board of Accountancy.

Dave served on the board of the Virginia Society of Certified Public Accountants (VSCPA) and on the **VSCPA Litigation Services, Professional Ethics, Quality Review, and Governmental Accounting and Auditing Committees**. 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 and past Vice Chair of the **AGA Professional Ethics Board**. He is also a member of the IIA 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, the Armed Services Board of Contract Appeals, and other administrative and judicial bodies.

Dave has spoken and written frequently on cost accounting, professional ethics, and auditor fraud detection responsibilities. 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").

## ***The ACFE/COSO Fraud Risk Management Guide: 2022 Edition***



- A short history: COSO, internal control, enterprise risk management, and fraud risk management
- The big picture: principles, standards, and leading practices
- FRMG overview
- The 2022 Update Task Force
- What has not changed
- Major changes
- Fraud risk management tools
- Be part of the antifraud effort

Cotton  
A BDO COMPANY

## ***Disclaimer***



**The views expressed in this presentation are my views and do not necessarily align with the views of the Virginia Board of Accountancy.**

Cotton  
A BDO COMPANY

## A short history: COSO, internal control, enterprise risk management, and fraud risk management



- 1985: Committee of Sponsoring Organizations of the Treadway Commission
- 1987: Treadway Commission Report
- 1992: Internal Control—Integrated Framework

Cotton  
A BDO COMPANY

## 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.

4

Cotton  
A BDO COMPANY

## A short history: COSO, internal control, enterprise risk management, and fraud risk management



- 1985: Committee of Sponsoring Organizations of the Treadway Commission
- 1987: Treadway Commission Report
- 1992: Internal Control—Integrated Framework
- 1992-2001: COSO IC Framework gained broad recognition
- 2002: SOX section 404 mandated establishing/reporting on IC
- 2002-2012: COSO IC Framework gained global recognition


Cotton  
A BDO COMPANY

## A short history: COSO, internal control, enterprise risk management, and fraud risk management



- 2004: COSO Enterprise Risk Management Framework
- 2013: COSO Internal Control—Integrated Framework
  - Principle 8: Consider fraud when assessing risks

Cotton  
A BDO COMPANY




The COSO Cube diagram illustrates the components of internal control. The top face lists the three components: Control Environment, Risk Assessment, and Control Activities. The front face lists the five components: Control Environment, Risk Assessment, Control Activities, Information & Communication, and Monitoring Activities. The side faces represent the three levels of the organization: Entity Level, Division/Operating Unit, and Function. An orange arrow points from the 'Risk Assessment' component to the 'Assesses Fraud Risk' section below.

**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.

 **Cotton**  
A BDO COMPANY

## A short history: COSO, internal control, enterprise risk management, and fraud risk management

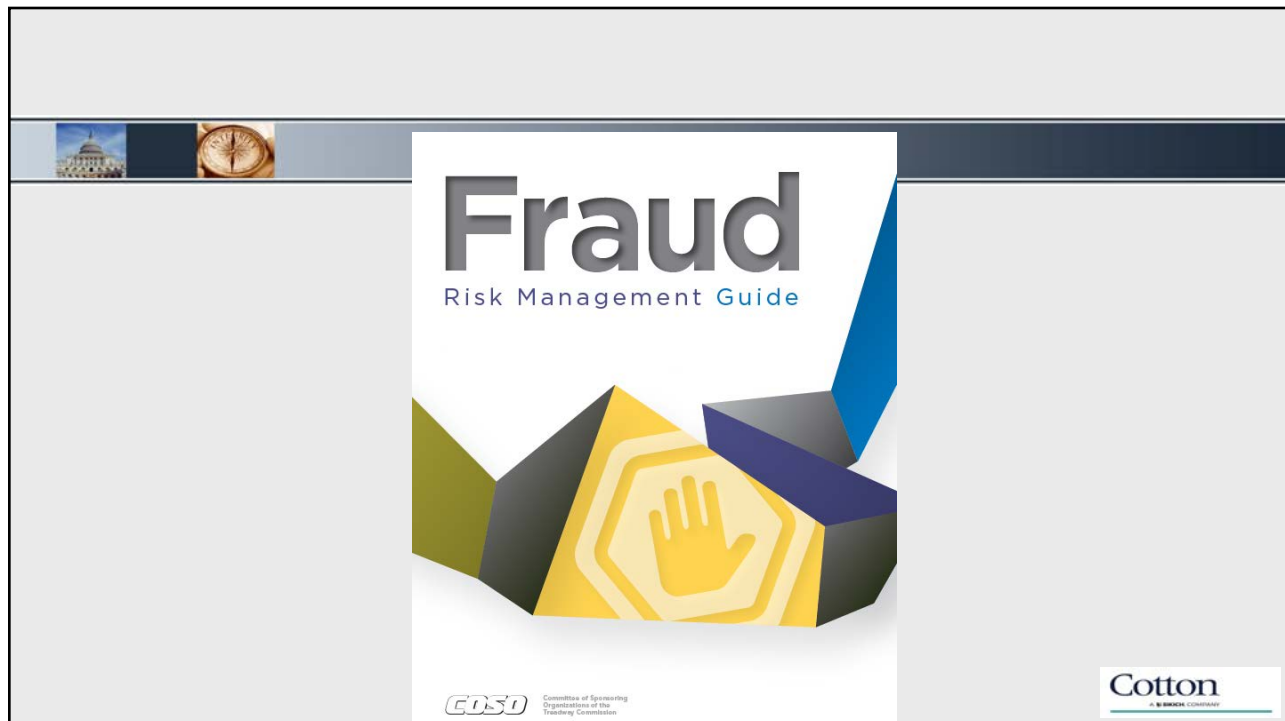


- 2004: COSO Enterprise Risk Management Framework
- 2013: COSO Internal Control—Integrated Framework
  - Principle 8: Consider fraud when assessing risks
- 2014: ACFE/COSO Fraud Risk Management task force
- 2015: GAO Fraud Risk Management Framework





## A short history: COSO, internal control, enterprise risk management, and fraud risk management

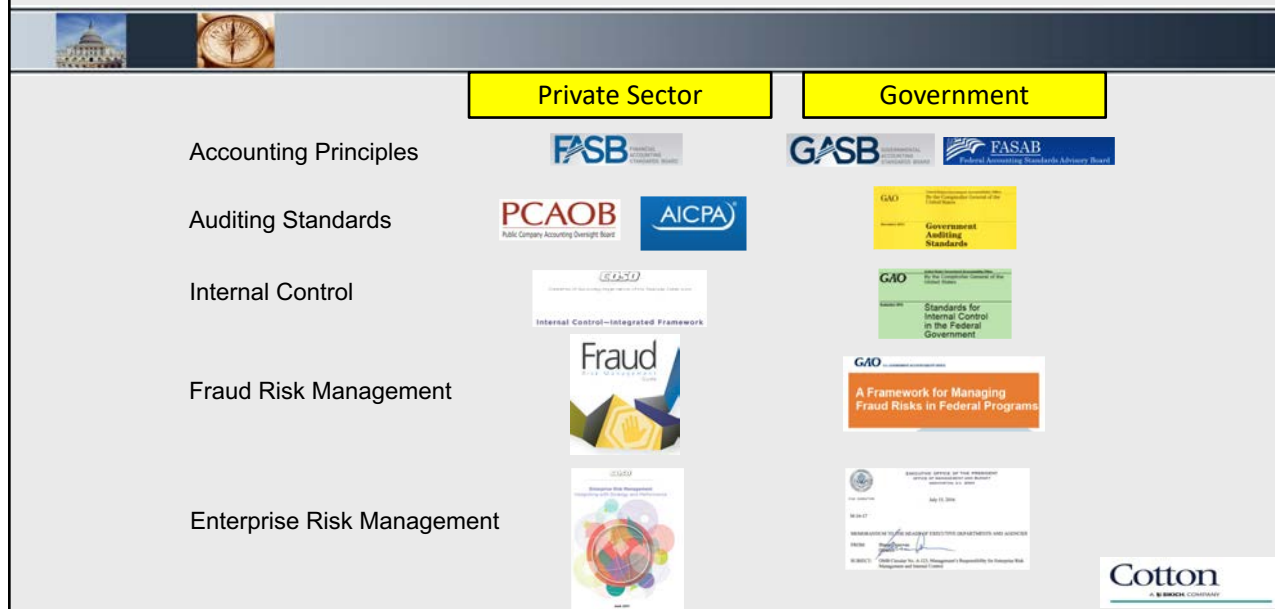
- 2004: COSO Enterprise Risk Management Framework
- 2013: COSO Internal Control—Integrated Framework
  - Principle 8: Consider fraud when assessing risks
- 2014: ACFE/COSO Fraud Risk Management task force
- 2015: GAO Fraud Risk Management Framework
- 2016: ACFE/COSO Fraud Risk Management Guide



## **A short history: COSO, internal control, enterprise risk management, and fraud risk management**

- 
- 2004: COSO Enterprise Risk Management Framework
  - 2013: COSO Internal Control—Integrated Framework
    - Principle 8: Consider fraud when assessing risks
  - 2014: ACFE/COSO Fraud Risk Management task force
  - 2015: GAO Fraud Risk Management Framework
  - 2016: ACFE/COSO Fraud Risk Management Guide
  - 2017: COSO Enterprise Risk Management Framework—Integrating with Strategy and Performance
- 

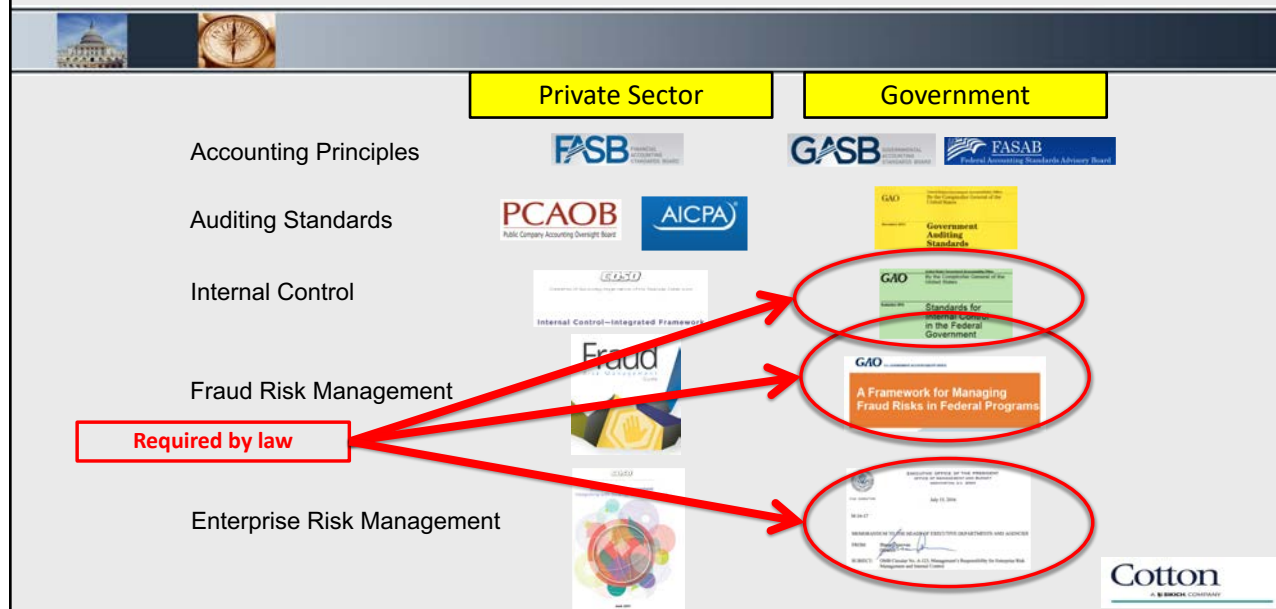
## The big picture: principles, standards, and leading practices



## The big picture: principles, standards, and leading practices



## The big picture: principles, standards, and leading practices



## 2016 FRMG overview


- Five fraud risk management principles
- Maps to COSO IC Framework
- Detailed information on performing a fraud risk assessment
- 19 Appendices

## Joint ACFE-COSO Task Force

	<b>Barbara Andrews</b> AICPA	<b>Bert Edwards</b> Formerly State Department	<b>Bill Leone</b> Norton Rose Fulbright	<b>Jeffrey Steinhoff</b> KPMG
	<b>Michael Birdsall</b> Comcast Corporation	<b>Frank Faist</b> Charter Communications	<b>Andi McNeal</b> ACFE	<b>William Titera</b> Formerly EY
	<b>Toby Bishop</b> Formerly ACFE, Deloitte	<b>Eric Feldman</b> Affiliated Monitors, Inc.	<b>Linda Miller</b> GAO	<b>Michael Ueltzen</b> Ueltzen & Company
	<b>Margot Cella</b> Center for Audit Quality	<b>Dan George</b> USAC	<b>Kemi Olateju</b> General Electric	<b>Pamela Verick</b> Protiviti
	<b>David Coderre</b> CAATS	<b>John D. Gill</b> ACFE	<b>Chris Pembroke</b> Crawford & Associates, PC	<b>Vincent Walden</b> EY
	<b>David L. Cotton, Chair</b> Cotton & Company LLP	<b>Leslye Givarz</b> Formerly AICPA, PCAOB	<b>J. Michael Peppers</b> University of Texas	<b>Bill Warren</b> PwC
	<b>James Dalkin</b> GAO	<b>Cindi Hook</b> Comcast Corporation	<b>Kelly Richmond Pope</b> DePaul University	<b>Richard Woodford</b> U.S. Coast Guard Investigative Service
	<b>Ron Durkin</b> Durkin Forensic, Inc.	<b>Sandra K. Johnigan</b> Johnigan, PC	<b>Carolyn Devine Saint</b> University of Virginia	



## Joint ACFE-COSO Advisory Panel

	<b>Dan Amiram</b> Columbia University Business School	<b>Michael Justus</b> University of Nebraska
	<b>Zahn Bozanic</b> The Ohio State University	<b>Theresa Nellis-Matson</b> New York Office of the State Comptroller
	<b>Greg Brush</b> Tennessee Comptroller of Treasury	<b>Jennifer Paperman</b> New York Office of the State Comptroller
	<b>Tamia Buckingham</b> Massachusetts School Building Authority	<b>Daniel Rossi</b> New York Office of the State Comptroller
	<b>Ashley L. Comer</b> James Madison University	<b>Lynda Harbold Schwartz</b> Upland Advisory LLC
	<b>Molly Dawson</b> Cotton & Company LLP	<b>Rosie Tomforde</b> Regional Government
	<b>Eric Eisenstein</b> Cotton & Company LLP	



## The 2022 Update Task Force



### Fraud Risk Management Guide Update Task Force

**Tom Caulfield**  
Procurement Integrity Consulting Service

**Sandra K. Johnigan, Co-Chair**  
Johnigan, PC

**Jeffrey Steinhoff**  
Formerly KPMG and GAO

**David Coderre**  
CAATS

**Andi McNeal**  
ACFE

**Pamela Verick**  
Protiviti

**David L. Cotton, Co-Chair**  
Cotton & Company

**Linda Miller**  
Grant Thornton

**Vincent Walden**  
Kona AI

**John D. Gill**  
ACFE

**Lynda Schwartz**  
University of Massachusetts Amherst

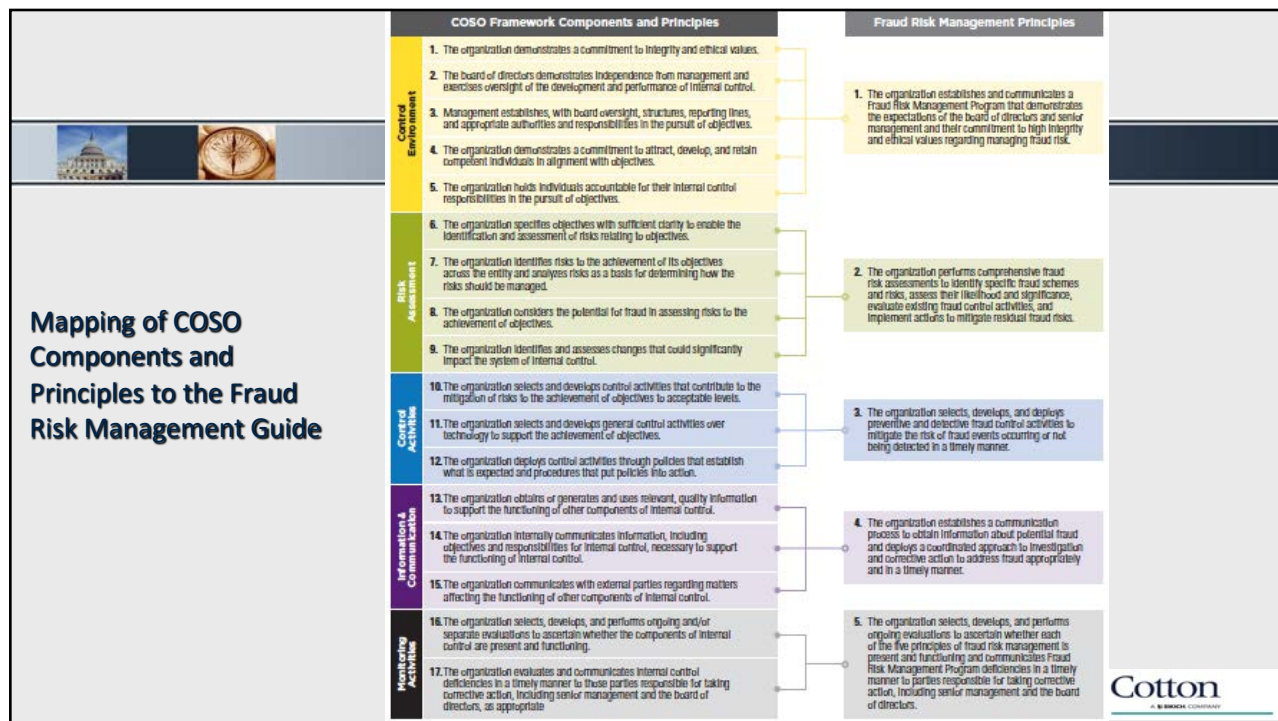
**Cotton**  
A BDO COMPANY

## What has not changed



- Mapping to COSO IC Framework

**Cotton**  
A BDO COMPANY



## What has not changed

- Mapping to COSO IC Framework
- Five fraud risk management principles and the basic process

## Basic fraud risk management process has not changed

Figure 1. Ongoing, Comprehensive Fraud Risk Management Process



otton  
A RISK-ORIENTED COMPANY

## What has not changed

- Mapping to COSO IC Framework
- Five fraud risk management principles and the basic process
- The fraud risk assessment process

Cotton  
A RISK-ORIENTED COMPANY

## Risk assessment process has not changed



## Major changes

- Fraud risk management and deterrence *linkage*
- COSO's two frameworks and fraud risk management *linkage*
- *Expanded* information on data analytics
- Internal control and fraud risk management: *how they differ*
- *Assessing the effectiveness* of existing control procedures
- Changes in the legal and regulatory environment
- Fraud reporting systems (hotlines)
- Changes in the external environment and fraud landscape
- Appendices changes
- Fraud risk management tools

## Fraud risk management and deterrence



- COSO's mission is to help organizations improve performance by developing thought leadership that enhances internal control, risk management, governance and **fraud deterrence**.
- According to the National Institute of Justice:
  - The *certainty* of being caught is a vastly more powerful deterrent than the punishment.
  - Police deter crime by increasing the perception that criminals will be caught and punished.



## Fraud risk management and deterrence



Fraud deterrence is the combined result of prevention and detection:



## Fraud risk management and deterrence



- Deterrence is also supported and enhanced by the knowledge throughout the organization that:
  - Those charged with governance have made a commitment to comprehensive fraud risk management.
  - Periodic fraud risk assessments are being conducted.
  - Overt *and* covert fraud control activities are in place.
  - Suspected frauds are investigated quickly.
  - Fraud reporting mechanisms are in place.
  - Discovered frauds are remediated thoroughly.
  - The entire Fraud Risk Management Program is being monitored on an ongoing basis.

Cotton  
A BDO COMPANY

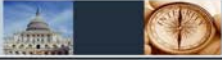
## COSO's two frameworks and fraud risk management



- COSO Internal Control—Integrated Framework: 1992, 2013
- COSO Enterprise Risk Management Framework: 2004
- Enterprise Risk Management — Integrating with Strategy and Performance: 2017
- Fraud Risk management Guide: 2016, 2022

Cotton  
A BDO COMPANY

## COSO's two frameworks and fraud risk management



Cotton  
A BDO COMPANY

## Expanded information on data analytics



- Added a data analytics Point of Focus under each of the five fraud risk management Principles:
  1. **Uses Data Analytics to Support Fraud Risk Governance**
  2. **Uses Data Analytics Techniques for Fraud Risk Assessment and Fraud Risk Responses**
  3. **Uses Proactive Data Analytics Procedures**
  4. **Performs Data Analytics**
  5. **Uses Data Analytics to Continuously Monitor and Improve**

Cotton  
A BDO COMPANY

## Expanded information on data analytics



### Expanded Data Analytics Appendices

- **Appendix D-1** explains how to build a sustainable data analytics capability, develop a data analytics plan, attract, and develop a team of skilled professionals, acquire the right technological solutions, and implement processes and procedures.
- **Appendix D-2** provides both guidance and practical examples of the application of data analytics techniques and approaches as part of a fraud risk assessment.
- **Appendix D-3** explains how data analytics techniques can enhance fraud control activities to mitigate residual risks that were identified during the fraud risk assessment.



## Internal control and fraud risk management



- Internal control and fraud risk management are related and support each other, but are different in some important respects.
- Controls that may assure accuracy in accounting and financial reporting may not be sufficient to protect against fraud.





## Internal control and fraud risk management

- Internal control and fraud risk management are related and support each other, but are different in some important respects.
- Controls that may assure accuracy in accounting and financial reporting may not be sufficient to protect against fraud.
- *Let's look at some examples ...*

## Internal control and fraud risk management



- Segregation of Duties.
- Approved Vendor Lists.
- Higher Transaction Approval Authorities.
- Asset Verification Physical Counts.

Cotton  
A BDO COMPANY

## Segregation of Duties



- ***Do not let one person control all transaction phases***
- Good for accuracy in accounting and financial reporting
- BUT, in assessing fraud risk, we need to consider how that control can be circumvented or rendered ineffective
  - Collusion among the people across whom duties are segregated
  - Password-sharing
  - I.e., residual fraud risk
- Let's apply additional controls to mitigate the residual risk
  - Frequently rotate the duties
  - Monitor password use and attendance



Cotton  
A BDO COMPANY

## Approved Vendor List

Overt Control Activity



- ***We only do business with reputable companies that have been thoroughly vetted***
- Good for accuracy in accounting and financial reporting
- BUT, in assessing fraud risk, we need to consider how that control can be circumvented or rendered ineffective
  - Employee gains access to vendor database and adds bogus company
  - Corrupt vendor offers bribes or kickbacks
  - I.e., residual fraud risk
- Let's apply additional controls to mitigate the residual risk
  - Match fields in employee and vendor databases
  - Apply data analytics to track unusual buying and pricing patterns

Covert Control Activities

Cotton  
A BDO COMPANY

39

## Approved Vendor List



- ***Wait: what if your organization includes employees in the vendor database in order to process travel expense reimbursement transactions?***

40

Cotton  
A BDO COMPANY

## Higher Level Approvals Required for Large Transactions



- ***Any purchase of more than \$50,000 requires regional manager approval***
- Good for accuracy in accounting and financial reporting
- BUT, in assessing fraud risk, we need to consider how that control can be circumvented or rendered ineffective
  - Purchase-splitting
  - Regional manager becomes corrupt
  - I.e., residual fraud risk
- Let's apply additional controls to mitigate the residual risk
  - Apply Benford's Law to the purchasing database
  - Apply data analytics to track unusual buying and pricing patterns

Overt Control Activity

Covert Control Activities

Cotton  
A BIRMINGHAM COMPANY

## Physical Counts of Assets/Inventory



- ***We periodically take physical counts of assets and inventory***
- Good for accuracy in accounting and financial reporting
- BUT, in assessing fraud risk, we need to consider how that control can be circumvented or rendered ineffective
  - Actual inventory is moved from location to location
  - Empty boxes are disguised to appear to have contents
  - I.e., residual fraud risk
- Let's apply additional controls to mitigate the residual risk
  - Vary the inventory counting process to conduct surprise counts or simultaneous location counts
  - Vary the counting process (weigh boxes; open boxes; etc.)

Overt Control Activity

Covert Control Activities

42

Cotton  
A BIRMINGHAM COMPANY

## More examples ...



- Two signatures required for checks above a certain amount.
- Thresholds for procurements:
  - Up to \$50,000 requires 3 or more quotes/bids
  - Above \$50,000 requires full/open competition
- CFO approval of all journal entries above \$100,000
- ?
- ?
- ?

43

 Cotton  
A BDO COMPANY

## Library of Internal Controls



- If your organization is following the COSO framework, you probably have a list (“library”) of all controls
- Apply this “how could fraud happen despite this control” analysis to every control

44

 Cotton  
A BDO COMPANY

## Assessing the effectiveness of existing control procedures



Clarification that assessing the effectiveness of existing controls is a two step process.

- First, a determination will be made as to whether the control is *in place and functioning as designed*.
- Once that determination is made, the control will be *re-assessed in terms of its effectiveness for preventing and detecting fraud*.



## Changes in the legal and regulatory environment



- Includes updated information with respect to recent legal and regulatory developments pertaining to fraud and fraud risk management, including:
  - The Department of Justice's *Evaluation of Corporate Compliance Programs*.
  - The Government Accountability Office's *A Framework for Managing Fraud Risks in Federal Programs*.
  - U.S. Securities and Exchange Commission Climate and ESG Task Force





## THE WALL STREET JOURNAL.

By [Dave Michaels](#) [Follow](#)

June 10, 2022 5:18 pm ET

### SEC Is Investigating Goldman Sachs Over ESG Funds

Regulator's civil probe focuses on bank's mutual-funds business, according to people familiar with the matter

47

**Cotton**  
A BDO COMPANY

## Fraud reporting systems (hotlines)



- ACFE research consistently reveals the importance of having fraud hotlines or whistleblower reporting systems in place.

**Cotton**  
A BDO COMPANY

## 2022 Report to the Nations



Cotton  
A BDO COMPANY

## 2022 Report to the Nations



FIG. 10 HOW IS OCCUPATIONAL FRAUD INITIALLY DETECTED?

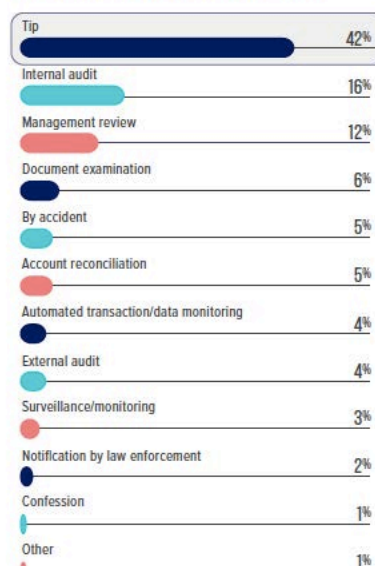
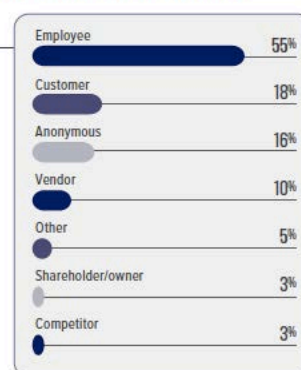


FIG. 11 WHO REPORTS OCCUPATIONAL FRAUD?



Cotton  
A BDO COMPANY

## 2022 Report to the Nations



Cotton  
A BDO COMPANY

## 2022 Report to the Nations



Cotton  
A BDO COMPANY

## Fraud reporting systems (hotlines)



- ACFE research consistently reveals the importance of having fraud hotlines or whistleblower reporting systems in place.
- Expanded information on the importance of hotlines as part of Principle 1 (Control Environment) and Principle 4 (Information and Communication)



## Changes in the external environment and fraud landscape



The fraud landscape is changing rapidly. The 2022 FRMG edition includes information on this changing environment, including:

- Environmental, social and governance (ESG) initiatives and reporting
- Cyberfraud
- Blockchain, cryptocurrency, and digital assets
- Ransomware
- COVID-19 response efforts, the CARES Act, and related programs
- Remote working and hybrid working environments
- Innovative and virtual management tools and accounting procedures



## Appendices changes



- 2016 edition had 19 appendices
- 2022 edition has 7 appendices

Cotton  
A BAKER COMPANY

## Appendices changes



2016 Appendices	2022 Edition Changes
A. Glossary	Updated and retained.
B. FRM Roles/Responsibilities	Updated and retained.
C. FRM Considerations for Smaller Entities	Updated and retained.
D. Reference Materials	Eliminated.
E. Data Analytics and FRM	Revised and expanded. New Appendices D-1, D-2, D-3.
F-1. Sample Fraud Control Policy	Updated but moved to the ACFE Tools site.
F-2. Fraud Risk Management High-Level Assessment	Updated but moved to the ACFE Tools site.
F-3. Sample Fraud Policy Responsibility Matrix	Updated but moved to the ACFE Tools site.
F-4. Sample Fraud Risk Management Policy	Updated but moved to the ACFE Tools site.
F-5. Sample Fraud Risk Management Survey	Updated but moved to the ACFE Tools site.
G. Fraud Risk Exposures	Eliminated but replaced with an expended list on the ACFE Tools site.
H. Fraud Risk Assessment Example	Updated and retained. New Appendix E.
I-1 thru I-5 Scorecards	Updated but moved to the ACFE Tools site.
J. Hyperlinks to Additional Tools	Updated and retained. New Appendix F.
K. Managing the Risk of Fraud, Waste, and Abuse in the Governmental Environment	Updated and retained. New Appendix G.

Cotton  
A BAKER COMPANY

## Fraud risk management tools at ACFE



<https://www.acfe.com/fraud-resources/fraud-risk-tools---coso/tools>

- Antifraud Playbook
- Library of Antifraud Data Analytic Tests
- Fraud Risk Management Interactive Scorecards
- Risk Assessment and Follow-Up Action Templates
- Points of Focus Documentation Templates

Cotton  
A BDO COMPANY

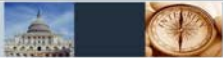
## Fraud risk management tools at ACFE



- Sample Fraud Control Policy
- Fraud Risk Management High-Level Assessment
- Sample Fraud Policy Responsibility Matrix
- Sample Fraud Risk Management Policy
- Sample Fraud Risk Management Survey
- Expanded list of fraud exposures, hyperlinked to underlying descriptions
  - Generic schemes
  - Industry-specific schemes

Cotton  
A BDO COMPANY

## Fraud risk management tools at ACFE



Coming soon:

- PowerPoint Deck to use to explain Fraud Risk Management and its importance to senior management and those charged with governance.
- Fraud Risk Management Implementation Program: an audit-program-like set of step-by-step procedures for implementing a robust FRM program.

**Cotton**  
A KPMG COMPANY

### 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 fraud risk has been reduced — at least — to a minimally acceptable level.

Each area, factor, or consideration scored either red or yellow should have 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
<b>MAKING AN ORGANIZATIONAL COMMITMENT TO A FRAUD RISK MANAGEMENT PROGRAM</b>		
Our organization has a strong correlation between our organizational culture and fraud risk management.	● ● ●	<input type="text"/>
Our organization's leadership demonstrates "tone at the top" by promoting ethical behavior and emphasizing a focus on deterring, preventing and detecting fraud.	● ● ●	<input type="text"/>
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.	● ● ●	<input type="text"/>
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.	● ● ●	<input type="text"/>
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.	● ● ●	<input type="text"/>

**Cotton**  
A KPMG COMPANY

[Download Report](#)

### 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.

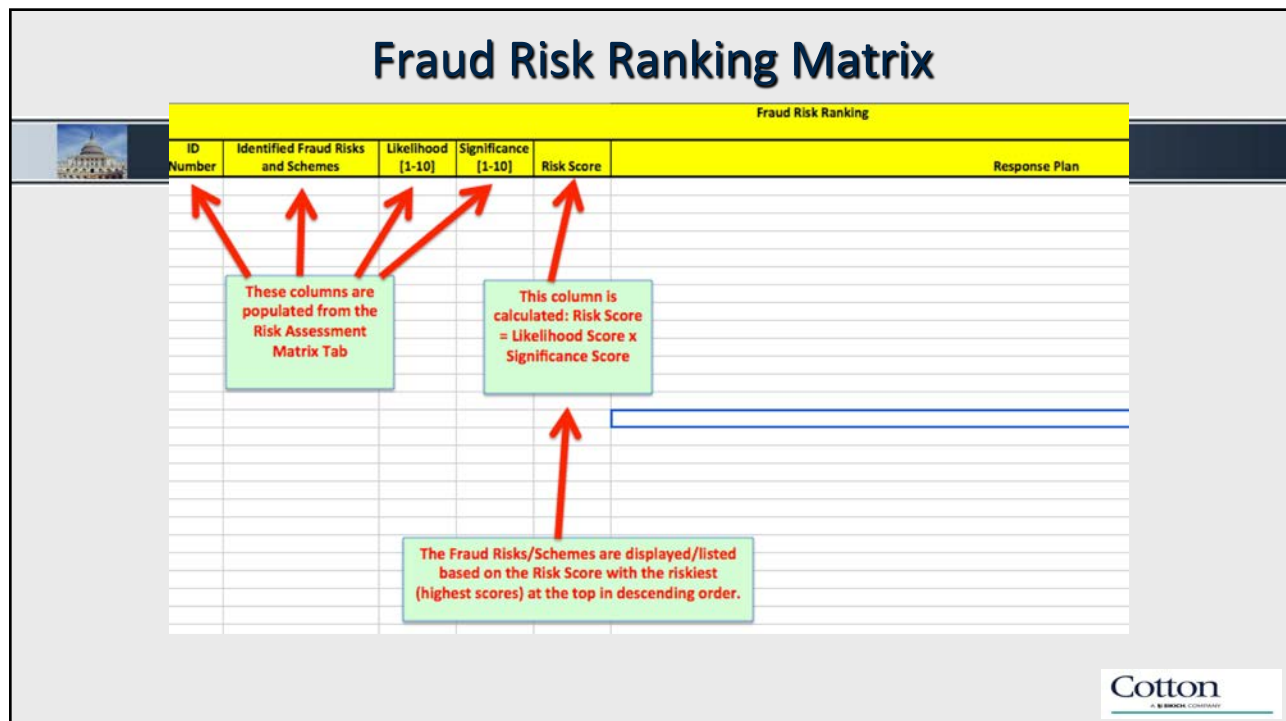
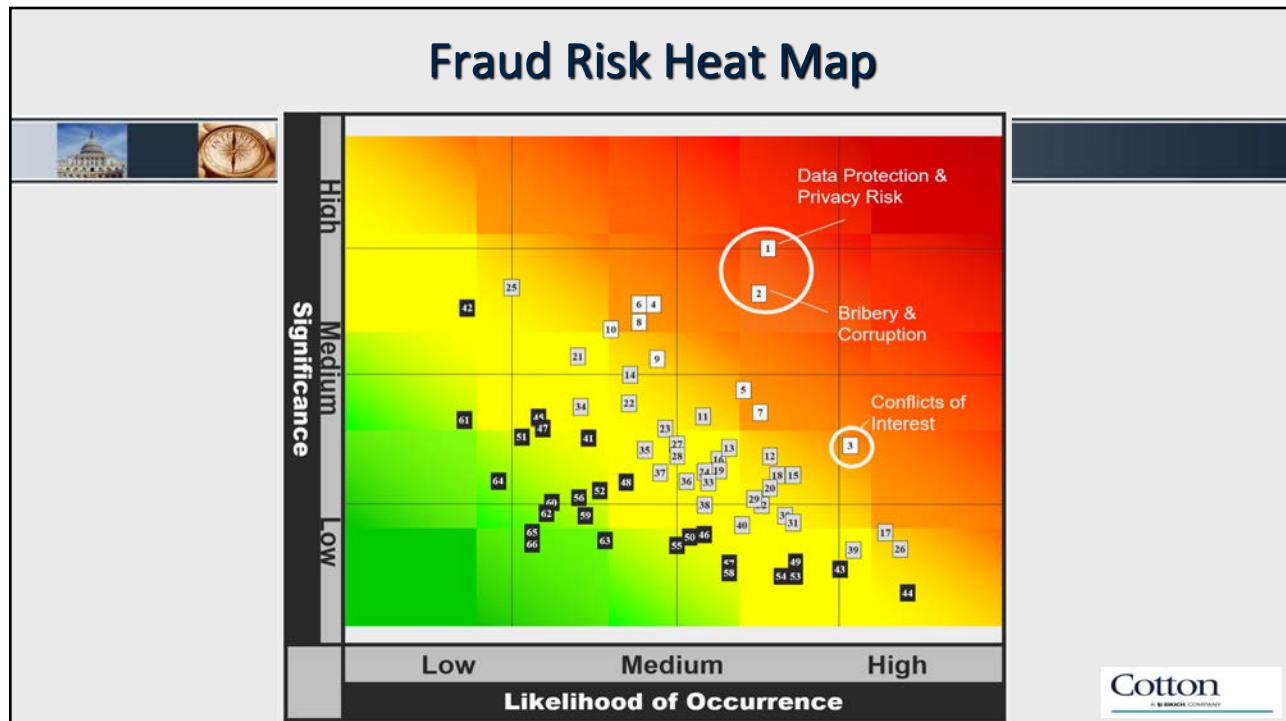
#### CONSIDERING FACTORS FOR SETTING THE SCOPE AND FREQUENCY OF EVALUATIONS

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.

# Cotton

## Risk Assessment and Follow-up Actions Template

The diagram illustrates the Fraud Risk Assessment process flow. It begins with a 'Brainstorming' phase, which leads to the 'Identified Fraud Risks and Schemes' column. This column is populated based on the results of the fraud brainstorming process. The 'Identified Fraud Risks and Schemes' column then feeds into the 'Likelihood [1-10]' and 'Significance [1-10]' columns. These two columns, along with the 'People and/or Department' column, automatically generate the 'heat map' that graphs likelihood versus significance. The 'Likelihood [1-10]' and 'Significance [1-10]' columns also feed into the 'Existing Anti-Fraud Controls' column. The 'Existing Anti-Fraud Controls' column, along with the 'Preventive [C] or Detective [D]' column, automatically generates the 'Control Activities' tab columns. Finally, the 'Existing Anti-Fraud Controls' and 'Preventive [C] or Detective [D]' columns feed into the 'Controls Effectiveness Assessment [1-10]' column, which then feeds into the 'Residual Risks' column. The 'Residual Risks' column feeds into the 'Fraud Risk Response' column.



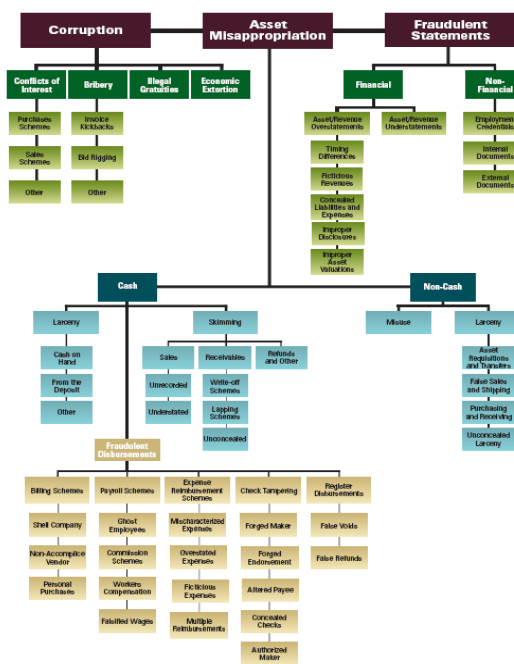
## Points of Focus Documentation

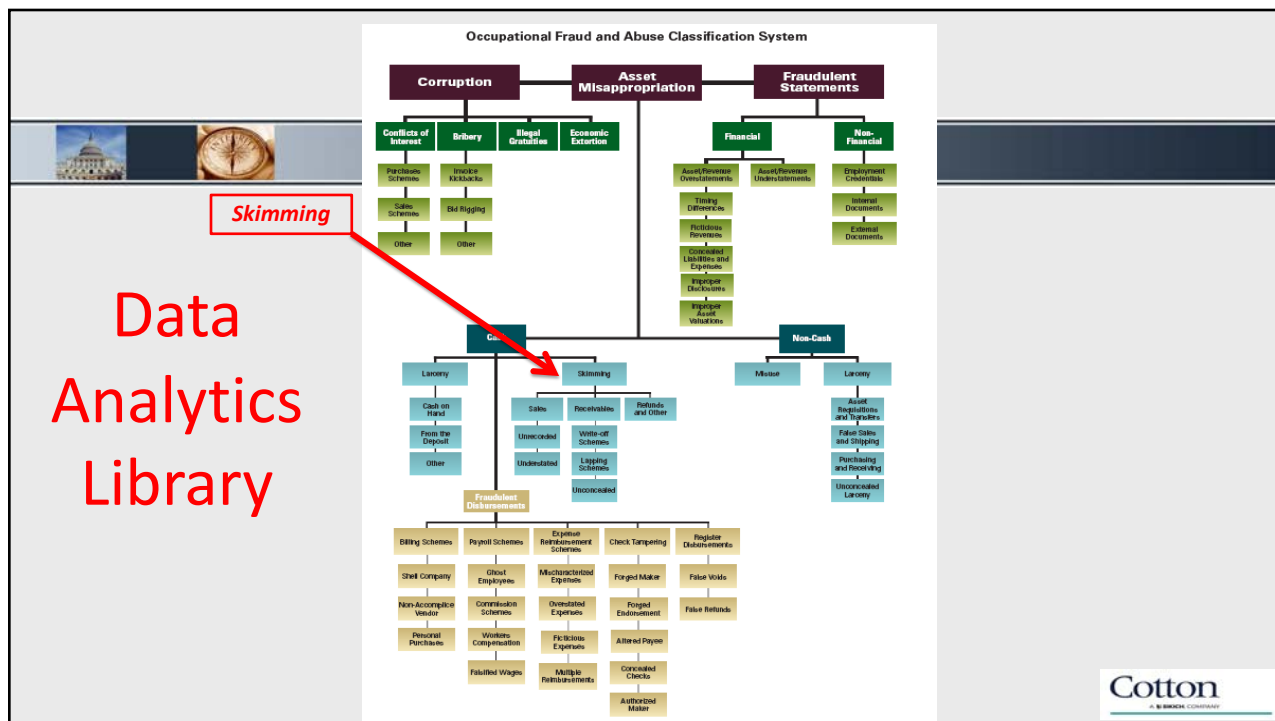
### Fraud Risk Control Activities Points of Focus and Our Organization's Response

Points of Focus	Our Organization's Response Including Cross-References to Other Material and Documentation
<b>Promotes Fraud Deterrence through Preventive and Detective Control Activities</b> — The organization addresses its fraud deterrence as a process of eliminating factors that may cause fraud to occur and understands that deterrence results from having effective preventive and detective fraud control activities in place.	
<b>Integrates with the Fraud Risk Assessment</b> — The organization ensures that the design and implementation of fraud control activities link directly to the fraud risk assessment.	
<b>Considers Organization-Specific Factors and Relevant Business Processes</b> — The organization ensures that the design and implementation of fraud control activities consider a range of factors, including factors unique to the organization, its industry, and its operating environment.	
<b>Considers the Application of Control Activities to Different Levels of the Organization</b> — The organization ensures that fraud control activities exist throughout the organization at all appropriate organizational levels.	
<b>Utilizes a Combination of Fraud Control Activities</b> — The organization ensures that fraud control activities include a range, variety, and mix of preventive and detective controls.	
<b>Considers Management Override of Controls</b> — The organization includes fraud control activities that consider and address the ability of senior management personnel to circumvent or override internal control activities, including fraud control activities.	
<b>Uses Proactive Data Analytics Procedures</b> — The organization implements a well-designed, rigorous system of data analytic processes and procedures that can identify anomalous transactions or events for further investigation.	
<b>Deploys Control Activities through Policies and Procedures</b> — The organization ensures that fraud control activities are thoroughly documented and implemented through organizational policies.	

## Data Analytics Library

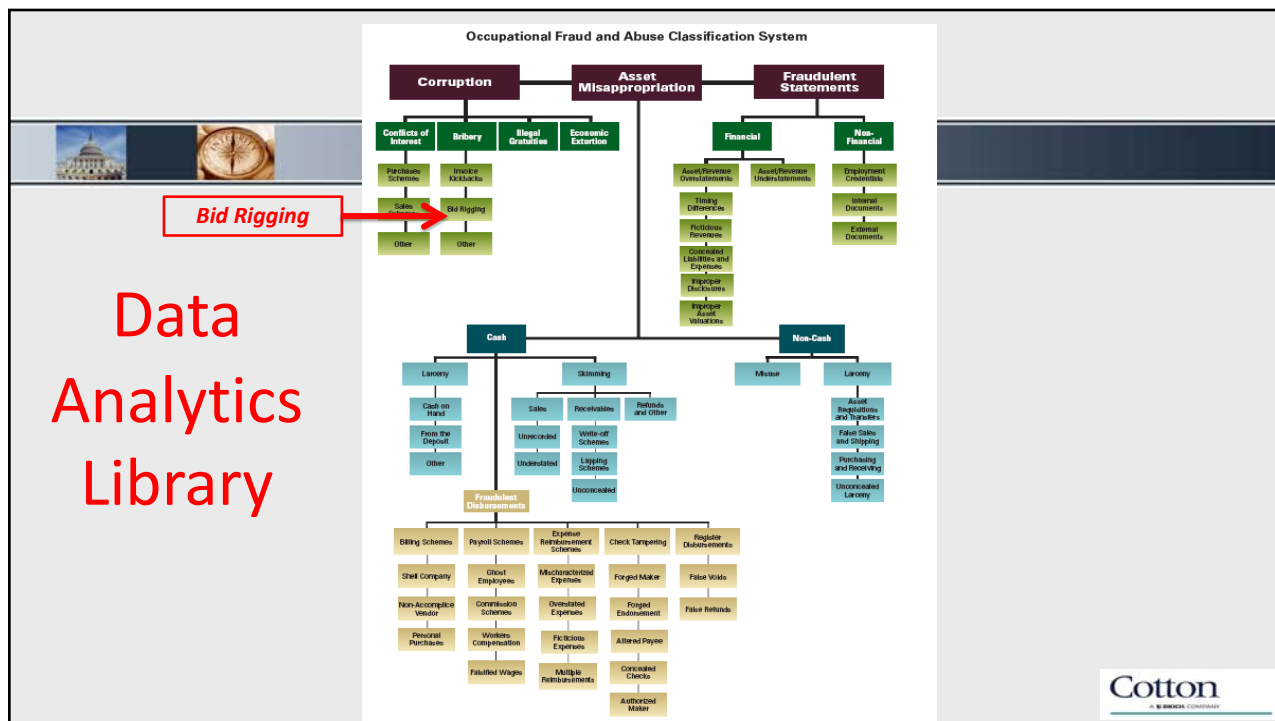
### Occupational Fraud and Abuse Classification System





Library of Data Analytics Tests	
<b>CASH - SKIMMING</b>	
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 suspicious 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

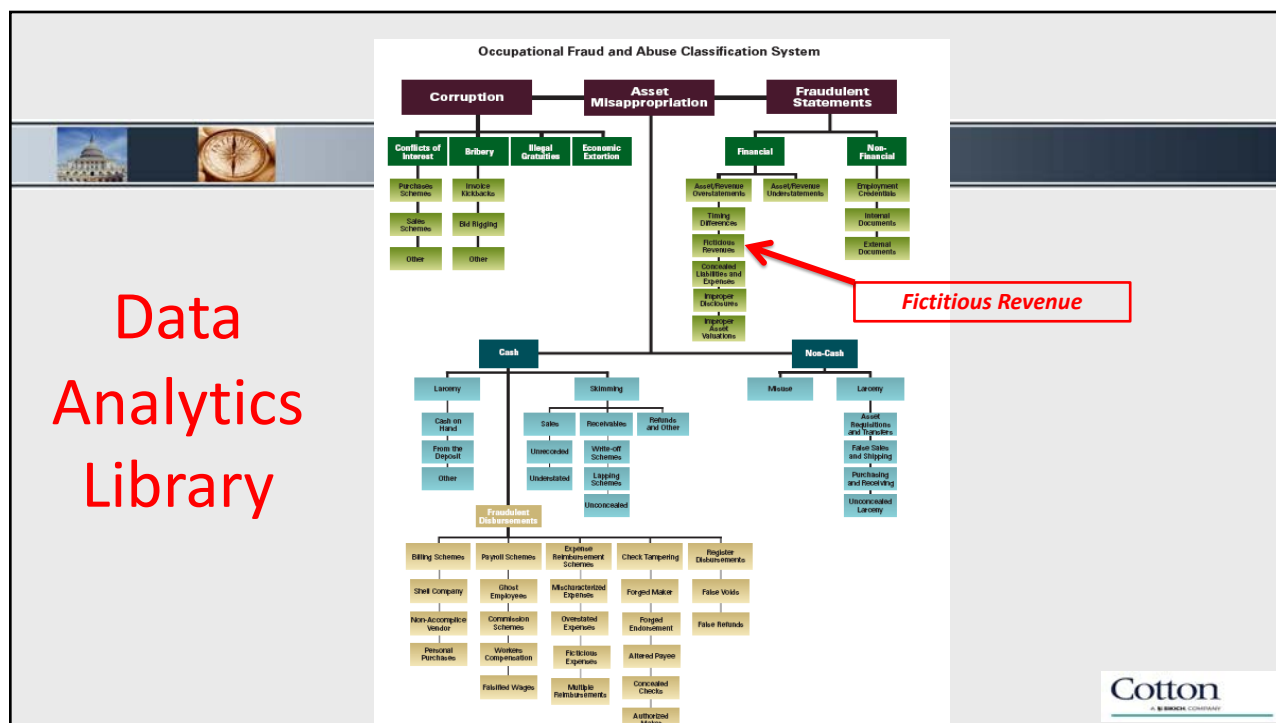
**Cotton**  
A WEIDEN COMPANY



**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

**Cotton**  
A WEISSER COMPANY



## 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

## Be part of the antifraud effort



- The tools at ACFE are intended to be crowd-sourced.
  - If you have:
    - Suggestions for modifications to existing tools
    - Ideas for additional tools
    - Additional fraud exposures to add to the list
    - Other comments or recommendations....
- Contact us.

Cotton  
A BDO COMPANY

## Yes, Yes, Yes...It's Hard Work



Just remember

- The perps hope you are lazy
- If the perps discover that you are not lazy and have thoroughly implemented fraud risk management processes, they will move on to find easier targets

74

Cotton  
A BDO COMPANY