KEY DIFFERENCES BETWEEN INSIDER RISK MANAGEMENT PROGRAM & FRAUD DETECTION PROGRAM

National Insider Threat Special Interest Group

www.nationalinsiderthreatsig.org

Insider Risk Management Program Training Courses

www.insiderthreatdefensegroup.com

KEY DIFFERENCES BETWWEN INSIDER RISK MANAGEMENT PROGRAM & FRAUD DETECTION PROGRAM

Core Differences & Similarities

Aspect	Insider Risk Management Program	Fraud Detection Program
Primary Focus	Protecting National Security Information (Classified, Sensitive), Business Information (Trade Secrets, Etc.), Other Assets: Facilities, Employees, Data, Computers, Networks From The Negative Impacts Caused By Employees Or Other Individuals With Authorized Access, Who Had Authorized Access, Or Gained Access Without Authorization.	Protecting Financial Assets And The Integrity Of Business Transactions From Deliberate Deception For Personal Or Organizational Gain.
Primary Objective	Prevent Any Type Of Negative Impacts That Could Effect The Mission Of The Organization.	Prevent, Detect & Investigate Financial Crimes Such As Theft, Embezzlement, Procurement & Contracting Fraud, Etc.
Typical Triggers	Behavioral Changes, Disgruntlement, Unexplained Wealth, Financial Problems, Gambling Problems, Foreign Contacts & Travel, Security Policy Violations, Access To Data Outside Scope Of Job, Alcohol Or Other Substance Abuse Problems, Mental Health Issues, Extreme, Persistent Interpersonal Difficulties, Hostile Or Vindictive Behavior, Criminal Problems, Etc., Employee Reporting (13 Adjudicative Guidelines For Security Clearance Holders) Holding 2 Jobs Violating Company Policy	Financial Anomalies, Financial Records Manipulation, Payroll Fraud, Billable Hours Fraud, Creating Ghost Employees, Overtime Fraud, Unauthorized Credit Card Use, Duplicate Payments, Shell Companies, Falsified Invoices, Paying Vendor For Services Never Performed, Inventory Discrepancies, Contracting Fraud: Bid Rigging, Accepting Bribes & Kickbacks, Employee-Vendor Collusion, Unexplained Wealth, Financial Problems, Gambling Problems Whistle-Blower Tips, Etc.
Key Data Sources	Human Resources (Disciplinary Records, Performance Evaluations, Etc.), Facility Access System Logs, Computer - Network Logs, Network Security Tools, Insider Threat Monitoring Tools, Security Incident Reports, Tips, Etc.	Financial Systems (ERP, Accounts Payable & Receivable Data), Procurement Records, Contracts, Expense Reports, Payroll Information, Reimbursement Requests, Audit Trails, Bank Statements, Vendor Payments, Etc.
Investigative Lens	Espionage (National Security, Corporate, Research, Etc.), Data Theft Or Sabotage, Computer – Network Sabotage, Theft Of Organization Assets, Workplace Violence, Criminal Actions, Etc.	Financial Crime, Deception, Asset Misappropriation, Regulatory Non-Compliance, Etc.
Governing Framework	National Insider Threat Policy, NISPOM 32 CFR Part 117 and others.	Federal Reserve, SEC, FDIC, FDIC, OCC, CFTC, FINCEN, Etc.

Is The Insider Risk Management Program Working Closely With The Fraud Detection Program Within Your Organization?

Similarities Between Both:

Trust Exploitation: Both involve an employee who abuses his position of trust and authorized access.
Proactive Stance: Both rely on proactive monitoring, detection, and prevention rather than just reactive investigation.
Multi-Disciplinary: Both require collaboration between Security, HR, Finance, Vendor Management, Legal, Etc.

Additional Information On Fraudulent Invoices - Shell Company Schemes By Employees Can Be Found In This NITSIG Report

ASSOCIATION OF CERTIFIED FRAUD EXAMINERS 2024 REPORT ON FRAUD

If you are an Insider Risk Program Manager, or support the program, you should read this report. Insider Risk Program Managers should print the infographics on the links below, and discuss them with the CEO and other key stakeholders that support the Insider Risk Management Program. If there is someone else within the organization who is responsible for fraud, the Insider Risk Program Manager should be collaborating with this person very closely.

The traditional norm or mindset that malicious Insiders just steal classified information, an organizations data, trade secrets or other sensitive information, is no longer the case. There continues to be a drastic increase in financial fraud and embezzlement committed by employees'.

Could your organization rebound / recover from the severe impacts that an Insider Threat incident can cause?

Has the Insider Risk Program Manager conducted a gap analysis, to analyze the capabilities of your organizations existing Network Security / Insider Threat Detection Tools to detect fraud?

Can your organizations Insider Threat Detection Tools detect an employee creating a shell company, and then billing the organization with an invoice for services that are never performed?

This report states that more than half of frauds occurred due to lack of internal controls or an override of existing internal controls.

This report is based on **1,921** real cases of occupational fraud, includes data from **138** countries and territories, covers **22** major industries and explores the costs, schemes, victims and perpetrators of fraud. These fraud cases caused losses of more than **$3.1 BILLION**. (Download Report)

Key Findings From Report / Infographic
Fraud Scheme Types, How Fraud Is Detected, Types Of Victim Organizations, Actions Organizations Took Against Employees, Etc. (Source)

Behavioral Red Flags / Infographic
Fraudsters commonly display distinct behaviors that can serve as warning signs of their misdeeds. Organizations can improve their anti-fraud programs by taking these behavioral red flags into consideration when designing and implementing fraud prevention and detection measures. (Source)

Profile Of Fraudsters / Infographic
Most fraudsters were employees or managers, but **FRAUDS PERPETRATED BY OWNERS AND EXECUTIVES WERE THE COSTLIEST**. (Source)

Fraud In Government Organization's / Infographic

How Are Organization Responding To Employee Fraud / Infographic
Outcomes in fraud cases can vary based on the role of the perpetrator, the type of scheme, the losses incurred, and how the victim organization chooses to pursue the matter. Whether they handle the fraud internally or through external legal actions, organizations must decide on the best course of action. (Source)

Providing Fraud Awareness Training To The Workforce / Info Graphic
Providing fraud awareness training to staff at all levels of an organization is a vital part of a comprehensive anti-fraud program. Our study shows that training employees, managers, and executives about the risks and costs of fraud can help reduce fraud losses and ensure frauds are caught more quickly. **43% of frauds were detected by a tip**. (Source)

FRAUD RESOURCES

ASSOCIATION OF CERTIFIED FRAUD EXAMINERS

Fraud Risk Schemes Assessment Guide

Fraud Risk Management Scorecards

Other Tools

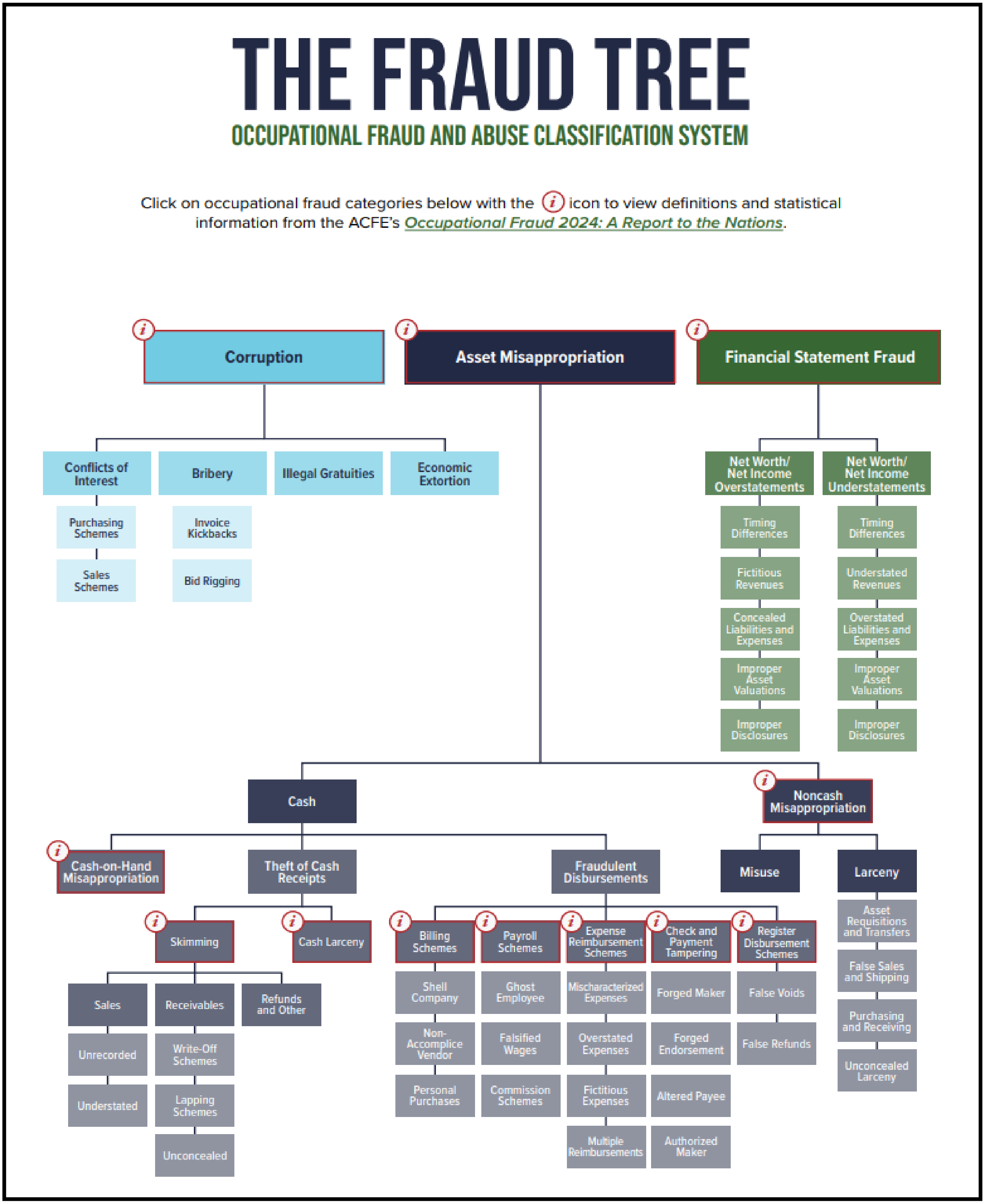
DEPARTMENT OF DEFENSE FRAUD DETECTION RESOURCES

General Fraud Indicators & Management Related Fraud Indicators

Fraud Red Flags & Indicators

Comprehensive List Of Fraud Indicators

ASSOCIATION OF CERTIFIED FRAUD EXAMINERS FRAUD TREE



THE FRAUD TREE

OCCUPATIONAL FRAUD AND ABUSE CLASSIFICATION SYSTEM

Click on occupational fraud categories below with the *i* icon to view definitions and statistical information from the ACFE's *Occupational Fraud 2024: A Report to the Nations*.

- Corruption
  - Conflicts of Interest
    - Purchasing Schemes
    - Sales Schemes
  - Bribery
    - Invoice Kickbacks
    - Bid Rigging
  - Illegal Gratuities
  - Economic Extortion
- Asset Misappropriation
  - Cash
    - Cash-on-Hand Misappropriation
    - Theft of Cash Receipts
      - Skimming
        - Sales
          - Unrecorded
          - Understated
        - Receivables
          - Write-Off Schemes
          - Lapping Schemes
          - Unconcealed
        - Refunds and Other
      - Cash Larceny
    - Fraudulent Disbursements
      - Billing Schemes
        - Shell Company
        - Non-Accomplice Vendor
        - Personal Purchases
      - Payroll Schemes
        - Ghost Employee
        - Falsified Wages
        - Commission Schemes
      - Expense Reimbursement Schemes
        - Mischaracterized Expenses
        - Overstated Expenses
        - Fictitious Expenses
        - Multiple Reimbursements
      - Check and Payment Tampering
        - Forged Maker
        - Forged Endorsement
        - Altered Payee
        - Authorized Maker
      - Register Disbursement Schemes
        - False Voids
        - False Refunds
  - Noncash Misappropriation
    - Misuse
    - Larceny
      - Asset Requisitions and Transfers
      - False Sales and Shipping
      - Purchasing and Receiving
      - Unconcealed Larceny
- Financial Statement Fraud
  - Net Worth/ Net Income Overstatements
    - Timing Differences
    - Fictitious Revenues
    - Concealed Liabilities and Expenses
    - Improper Asset Valuations
    - Improper Disclosures
  - Net Worth/ Net Income Understatements
    - Timing Differences
    - Understated Revenues
    - Overstated Liabilities and Expenses
    - Improper Asset Valuations
    - Improper Disclosures

Source