Please tell us what you think!

- Please scan this QR code using your mobile to access a short feedback survey →
- Also accessible via the mobile app

Fraud Detection & Investigation Techniques

Advanced Fraud Prevention Tactics: Building Resilience in Accounts Payable and Accounts Receivable
Paul Zikmund

Presented by: Paul Zikmund

IOFM Fall
CONFERENCE & EXPO

Objectives

01

Understand the current fraud landscape and identify emerging threats in accounts payable and accounts receivable.

02

Learn advanced techniques and best practices for detecting and preventing fraud.

03

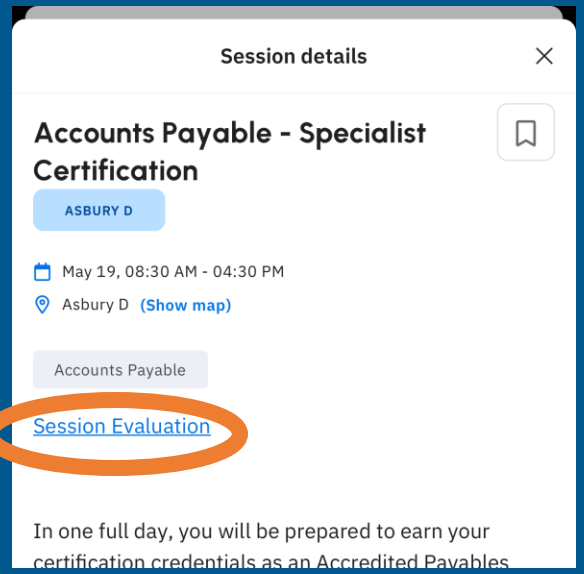
Develop strategies to enhance internal controls and improve fraud detection capabilities.

04

Explore the role of technology and data analytics in strengthening fraud prevention efforts.

Please tell us what you think!

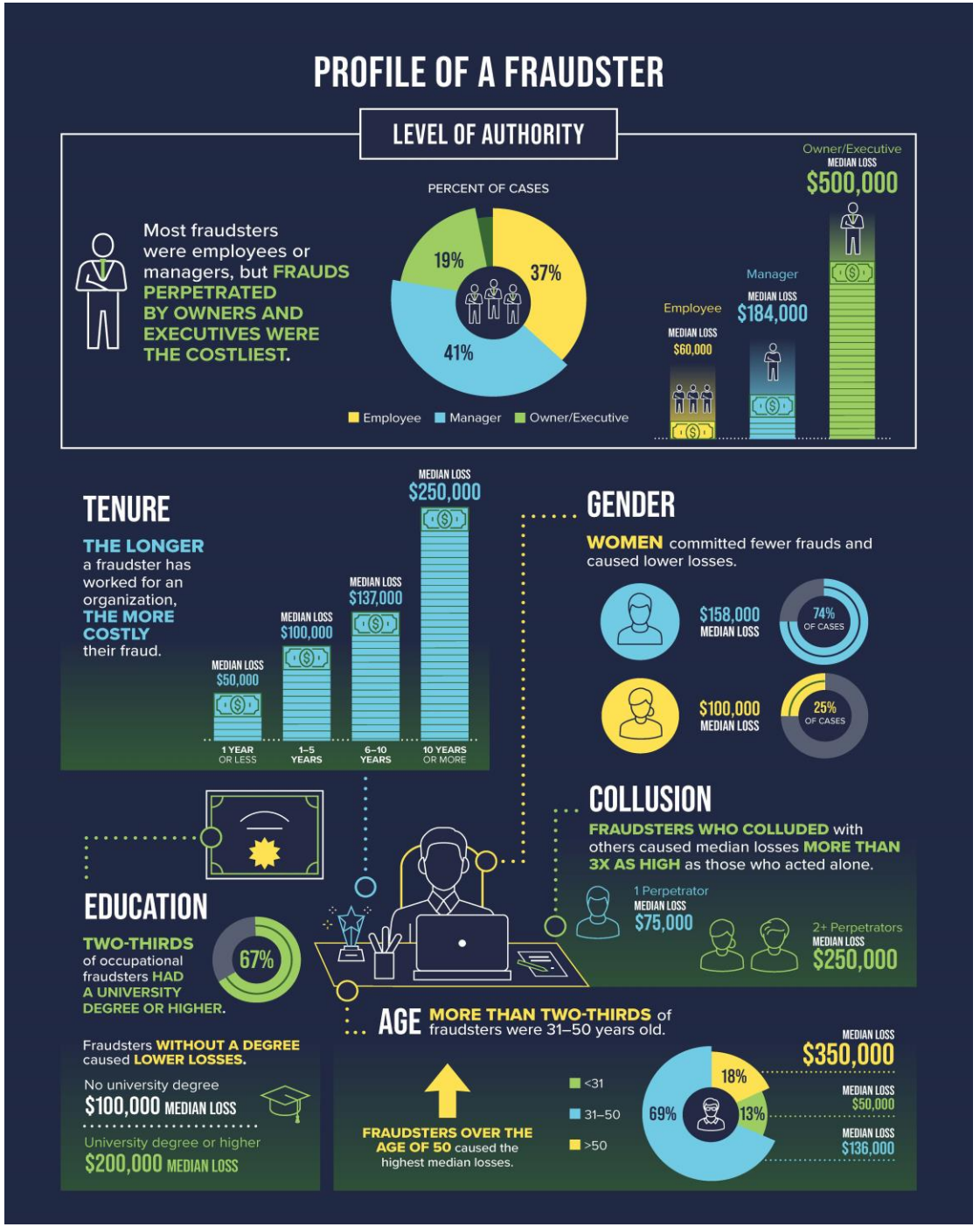
- Please scan this QR code using your mobile to access a short feedback survey →
- Also accessible via the mobile app



Advanced Fraud Prevention Tactics: Buildin g Resilience in Accounts Payable and Accou nts Receivable

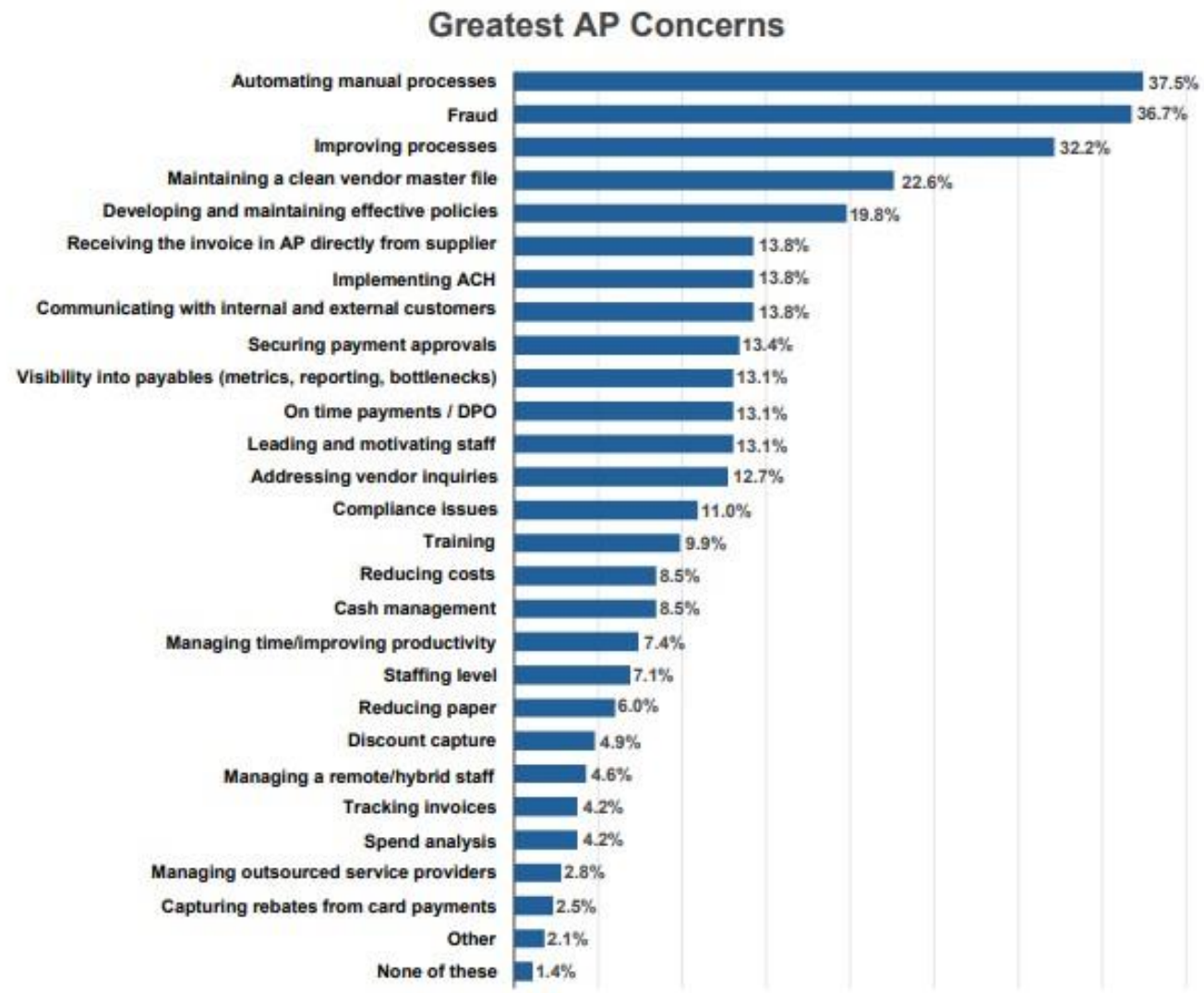
Risk Landscape

ACFE 2024 Fraud Statistics



IOFM 2024 Accounts Payable Benchmarking Report

FIGURE 1. AP'S GREATEST CONCERNS



IOFM Fall CONFERENCE & EXPO

IOFM 2024 Accounts Payable Benchmarking Report

FIGURE 10. DETECTED FRAUD ATTEMPTS

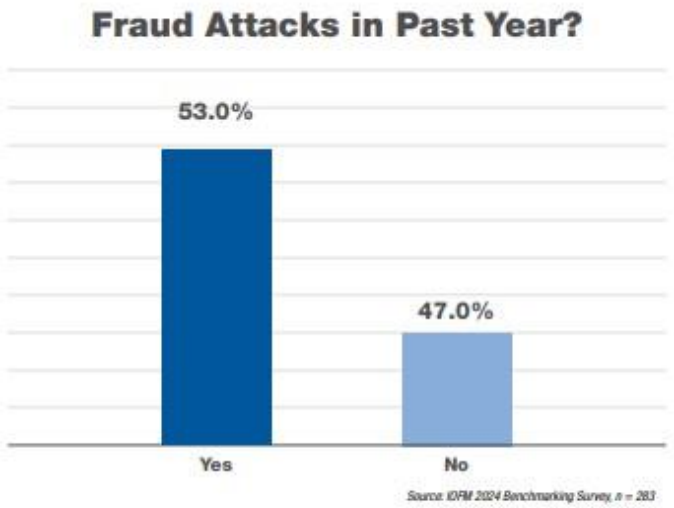
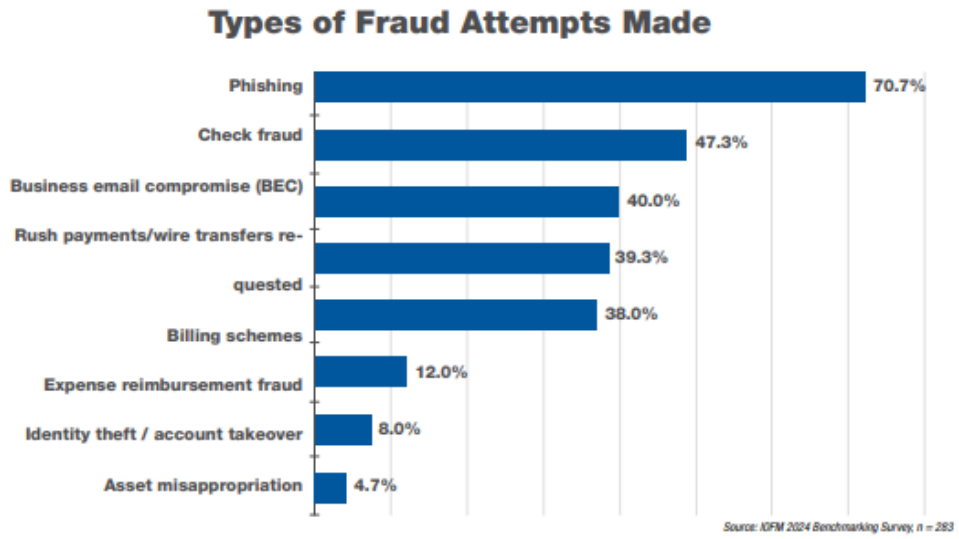


FIGURE 11. TYPES OF FRAUD ATTEMPTS

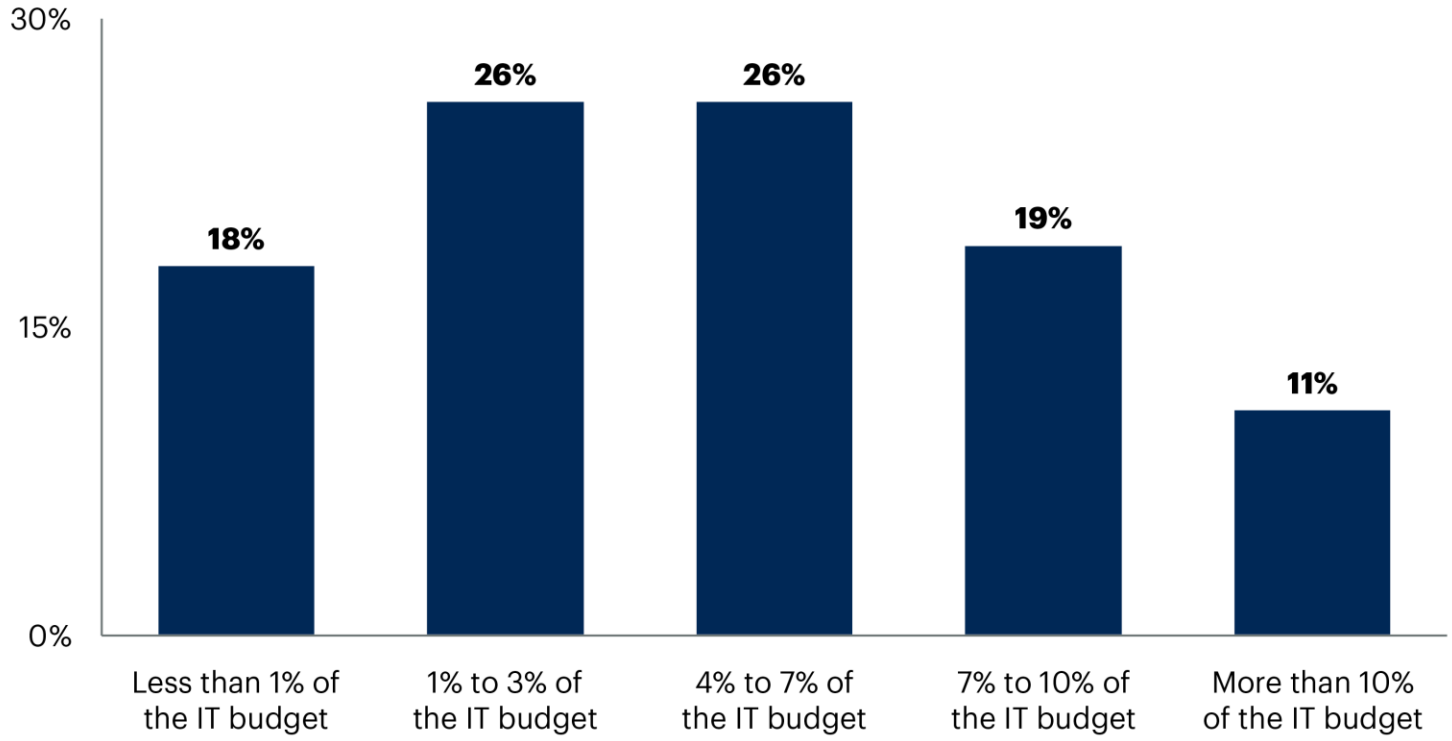


IOFM Fall CONFERENCE & EXPO

Gartner Financial Services Research Survey

IT Budget Spent on Overall Fraud Prevention at Banks

Percentage of respondents



n = 57 senior financial services executives

Q. What percentage of your organization's annual IT budget is allocated for software applications and infrastructure used to detect and prevent overall fraudulent activity by external actors (not internal employees)?

Source: Gartner Financial Services Research Panel Survey, October 2023

Note: "Don't know" responses have been removed.

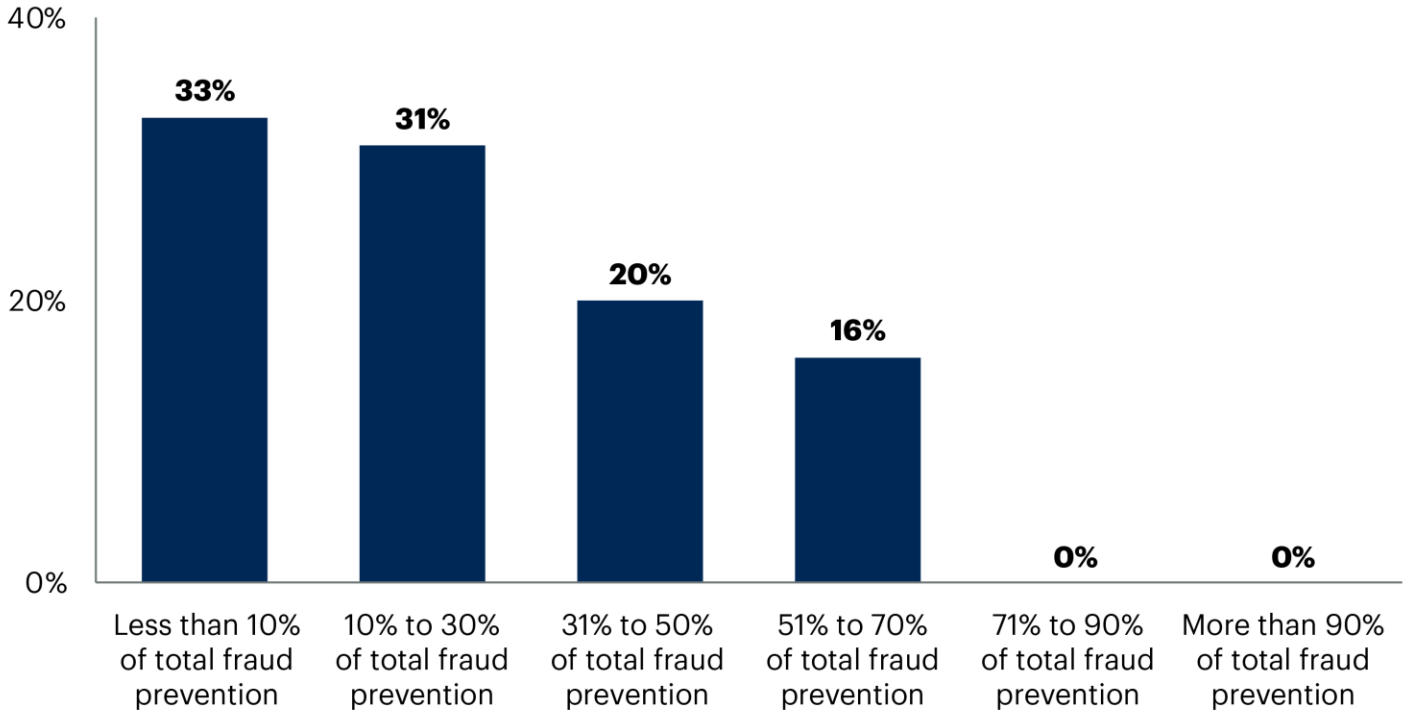
806082_C

IOFM Fall CONFERENCE & EXPO

Gartner

Gartner Financial Services Research Survey

Fraud Prevention Budget Spent on Payments Fraud
Percentage of respondents



n = 49 senior financial services executives

Q. Considering what your organization spends annually on overall fraud prevention, what is the average percentage of that total which is spent specifically on preventing payments fraud (i.e., the percentage spent on transaction monitoring for payments events)?

Source: Gartner Financial Services Research Panel Survey, October 2023

Note: "Don't know" responses have been removed.

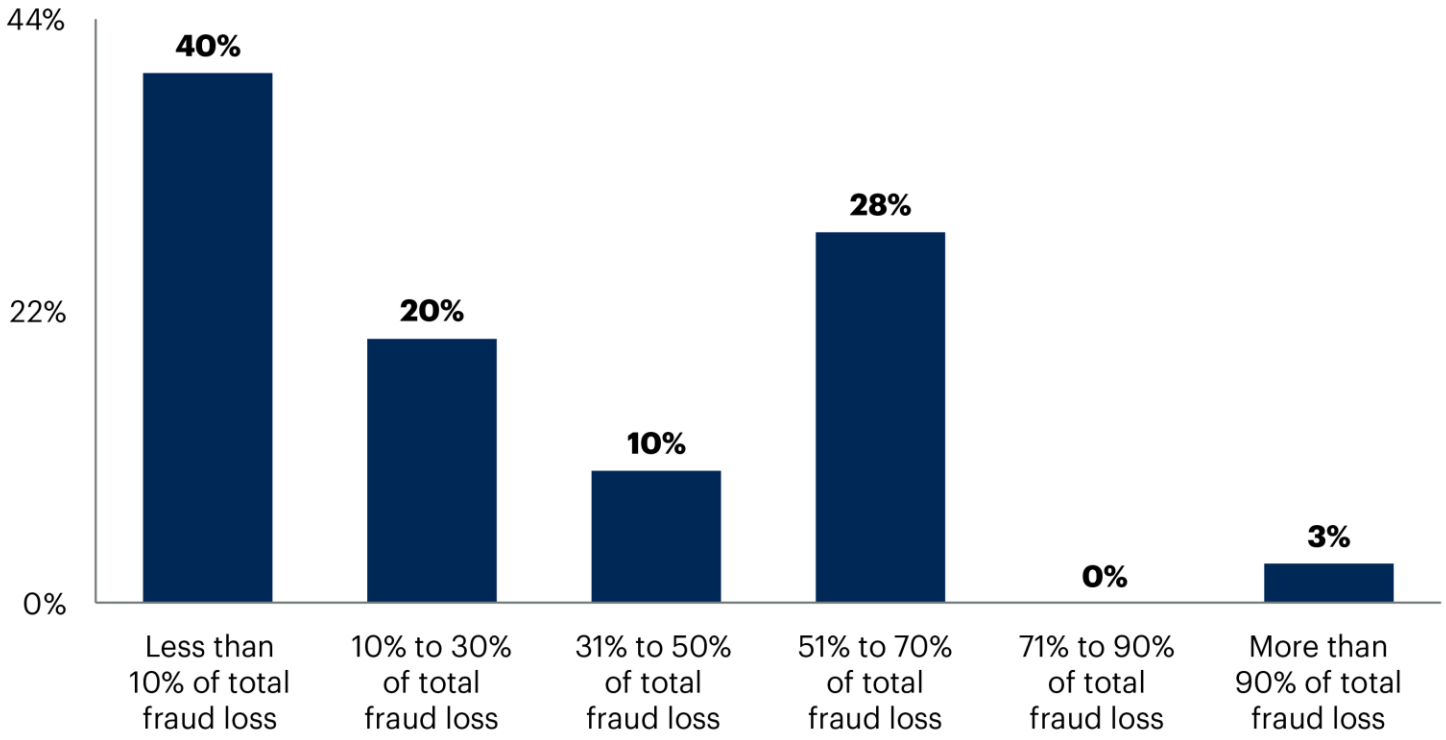
806082_C

Gartner

IOFM Fall CONFERENCE & EXPO

Gartner Financial Services Research Survey

Fraud Losses Due to Payments Fraud
Percentage of respondents



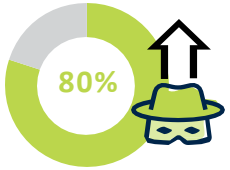
n = 40 senior financial services executives

Q. Of the total losses due to fraud that your organization experiences each year, what percentage of that is to payments fraud specifically?
Source: Gartner Financial Services Research Panel Survey, October 2023
Note: "Don't know" responses have been removed.
806082_C

IOFM Fall CONFERENCE & EXPO

Gartner

Key Findings – 2024 AFP Report

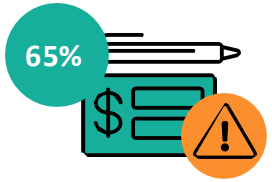


Payments Fraud Activity on the Rise

Overall, 80% of organizations were targets of either an actual or attempted payments fraud attack in 2023. This is an uptick of 15 percentage points from 2022. Organizations most impacted by fraud were those with at least $1 billion in revenue and fewer than 26 payments accounts (86%).

Discovering Fraud

Thirty percent of respondents report that after a successful fraud attempt, their organizations were unable to recover the funds lost due to fraud. At the other end of the spectrum, 29% were able to recoup up to 75% of the funds lost and 41% were successful in recouping more than 75% of the funds lost (mostly via checks).



Checks Continue to be Vulnerable to Fraud

Checks continue to be the payment method most susceptible to fraud, as reported by 65% of respondents. Seventy percent of organizations using checks have no immediate plans to discontinue their use. The primary reason for continued check use is the requirement for checks by small businesses.

Email Targets ACH Credits

This year, ACH credits have surpassed wires as the most vulnerable payment type for BEC fraud. Even as most payment methods continue to be vulnerable to BEC, payments made via ACH credits (47%), wire transfers (39%) and ACH debits (20%) were most often targeted.

Business Email Compromise (BEC) Controls Have Room for Improvement

Less than 60% of organizations have completed the documentation that includes the creation of written policies and procedures which are required to safeguard against BEC, while less than half (49%) have completed testing these policies. Although BEC has been prevalent for over a decade, findings reveal a gap in preparedness to mitigate scams via email.

Organizations Overlook the Vulnerability of Payments Sent by USPS

Over 20% of respondents report fraud due to interference with the United States Postal Service (USPS), which is 10 percentage points higher than the share reported for 2022. Despite alerts from the Financial Crimes Enforcement Network (FinCEN)[2] regarding increased fraud attempts via mail interception, over 80% of respondents indicate their organizations still deliver checks via the United States Postal Service (USPS) — without tracking.

[2] https://www.fincen.gov/reports/sar-stats

Key Findings – 2025 AFP Report

KEY FINDINGS

Fraud is down very slightly — but remains elevated.

A full 79% of respondents say that their organizations experienced actual or attempted payments fraud in 2024, down slightly from 80% in 2023. The one-percentage-point drop is not very encouraging; 65% of corporate practitioners reported payments fraud at their organizations in 2022. Clearly, fraudsters have not been deterred by any of the anti-fraud protections that organizations have put in place.

Business email compromise (BEC) continues to be a threat.

BEC once again was the number one avenue for attempted and actual payments fraud in 2024, cited by 63% of respondents. Incidence of vendor imposter fraud was also high, at 45%, a sharp increase from 34% in the previous survey. It's important to note that vendor imposter fraud is another form of BEC, as is invoice fraud which increased to 24% in 2024 from 14% in 2023. Spoof emails are still the most prevalent type of BEC, cited by 79% of respondents (up from 77% in 2023).

Check fraud remains constant.

Checks continue to be the payment method most often subjected to payments fraud, with 63% of respondents experiencing attempted or actual fraud via checks in 2024. While that percentage is down slightly from 65% in the previous survey, it is clear that checks remain easy targets for criminals. Nevertheless, more than 75% of organizations currently have no plans to reduce check usage in the next two years.

Wire transfers reclaim their BEC crown.

Wire transfers reclaimed their rank as the payment method most frequently targeted by BEC scammers in 2024, reported by 63% of respondents, up from 39% in the previous survey. Nevertheless, ACH credits — which were the prime targets for BEC in 2023 — were the source of more BEC scam activity in 2024 than in the previous year, rising to 50% from 47%. ACH debits and checks tied for third place at 26% (up from 20% and 18%, respectively).

Classic BEC scams may be falling off.

One significant change seen in this year's survey is the decline in "classic" BEC scams. These are cases in which a fraudster impersonates a senior executive and requests a transfer of funds. In 2023, this method of payments fraud was on par with vendor impersonation, cited by 57% of organizations. In 2024, however, the incidence declined to 49%. Vendor impersonation experienced a slight increase — cited by 60% of respondents — while third-party impersonation remained the most frequent type of BEC scam at 63%. This change in tactics is likely to due to organizations' growing awareness of such "classic" BEC attempts.

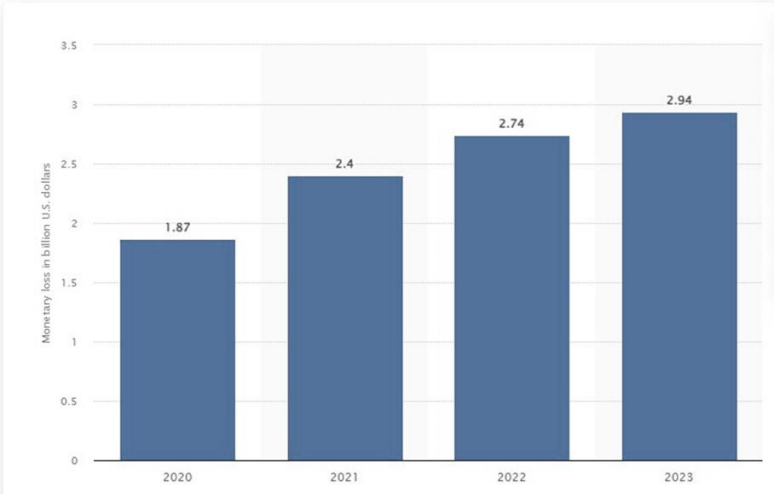
Recovering losses has mixed success.

Twenty-two percent of organizations were able to recover 75% or more of the funds lost due to payments fraud in 2024. That is a sharp decrease from results reported for 2023, during which 41% of companies recouped the same amount. However, it is encouraging that the percentage of organizations that were unable to recover anything at all in 2024 was 20%, down from 30% in 2023, and 58% were able to recoup up to 75% of their funds in 2024 (up from 29% in 2023).

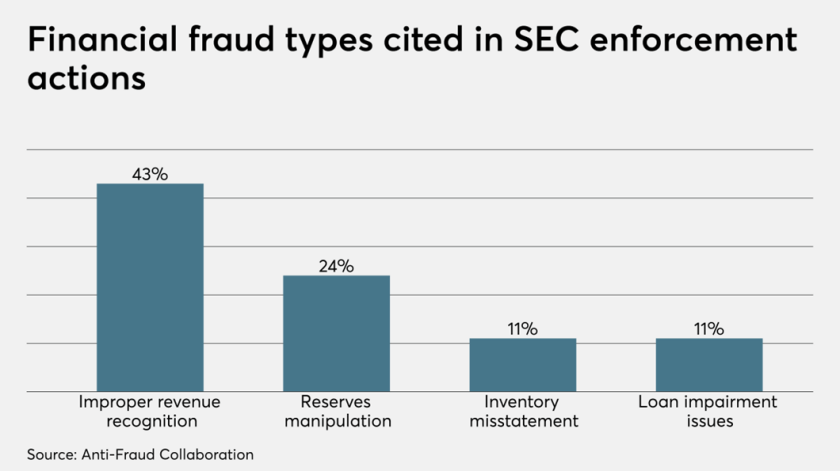
IOFM Fall CONFERENCE & EXPO

Accounts Payable/Accounts Receivable Fraud Risk

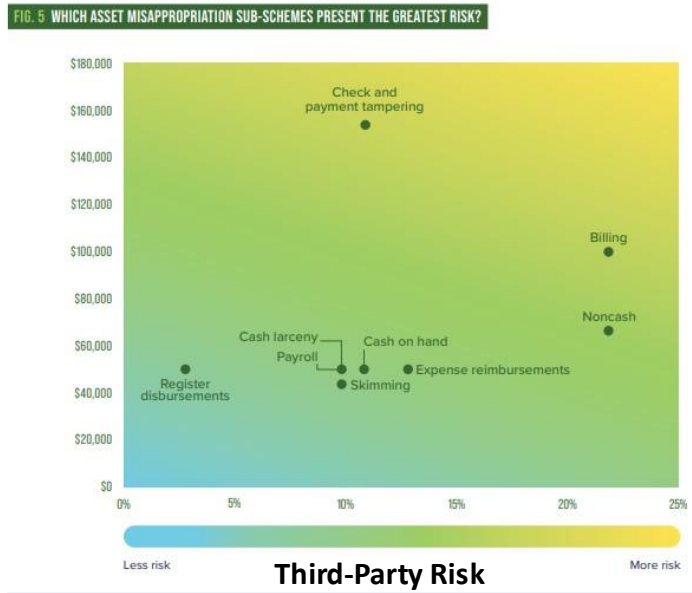
Loss attributed to BEC fraud schemes



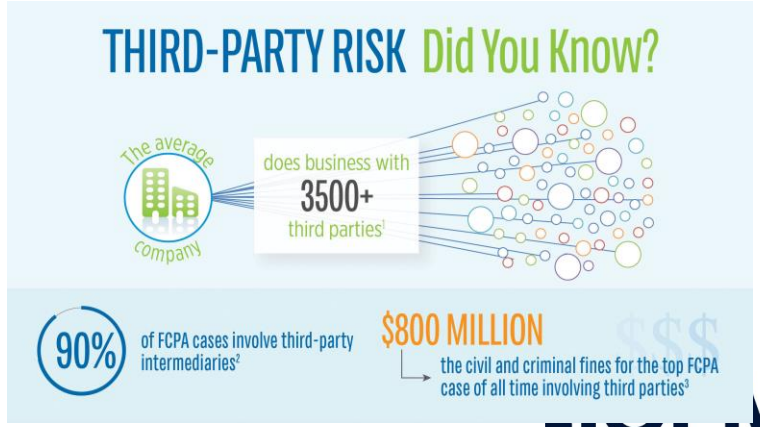
SEC Enforcement Actions



2024 ACFE Asset Misappropriation fraud schemes



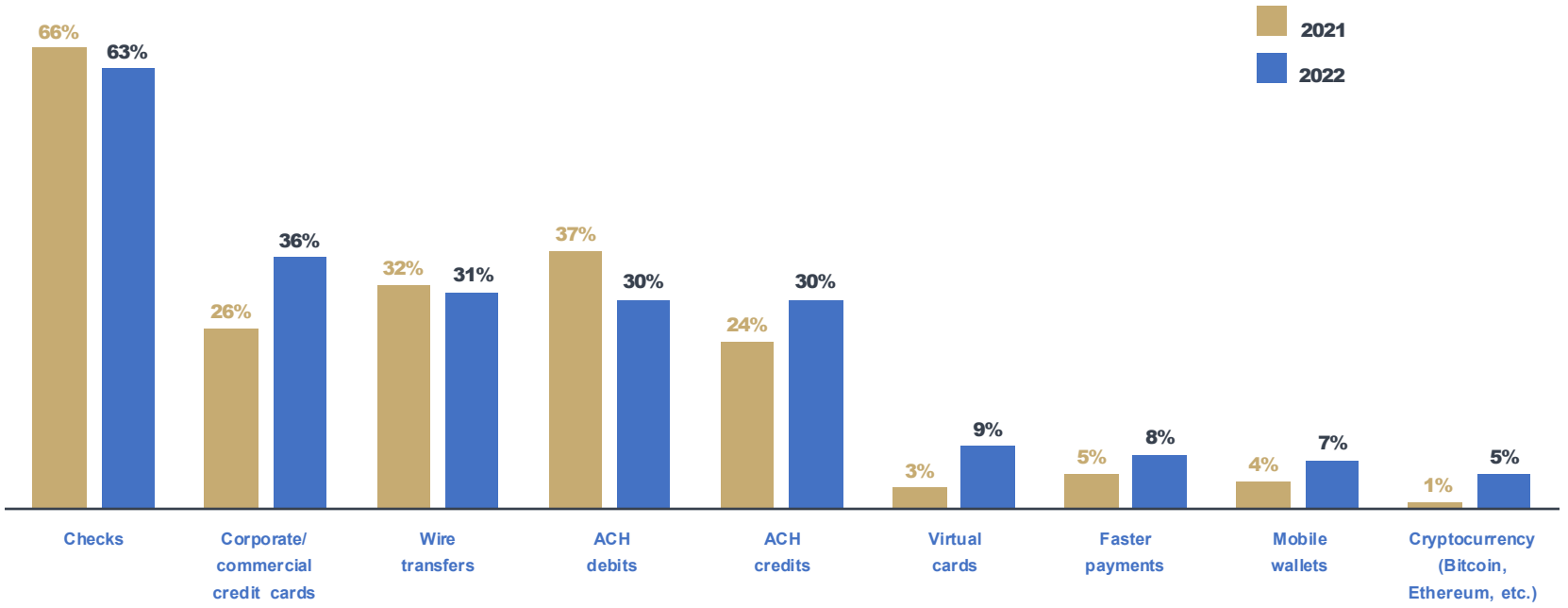
Third-Party Risk



Reduce AP Payment Fraud by Moving to Electronic Payments

Check fraud is prevalent in **63%** of organizations experiencing fraud.

Checks are **7X** more likely to be involved in fraud than virtual cards.



Source: 2023 AFP Payments Fraud and Control Survey. Percent of surveyed organizations where payment methods were subject to attempted/actual payments fraud.

IOFM Fall CONFERENCE & EXPO

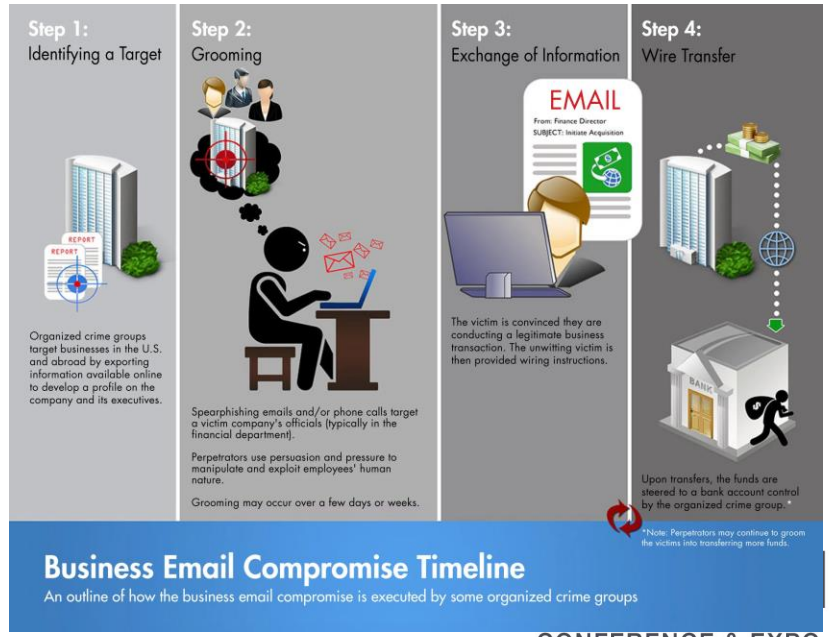
Payment Methods Subjected to Fraud – 2025 AFP Report

Payment Methods Subject to Attempted/Actual Payments Fraud
(Percent of Organizations)

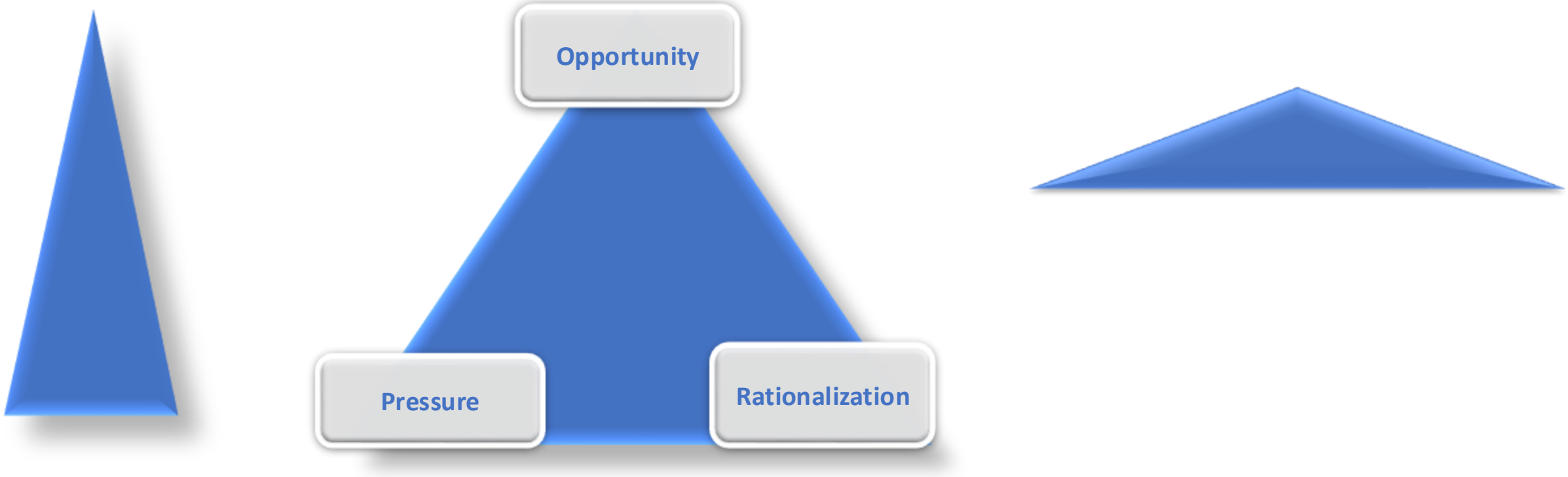
	2024	ANNUAL REVENUE LESS THAN $1 BILLION	ANNUAL REVENUE AT LEAST $1 BILLION	ANNUAL REVENUE AT LEAST $1 BILLION AND FEWER THAN 26 PAYMENT ACCOUNTS	ANNUAL REVENUE AT LEAST $1 BILLION AND MORE THAN 100 PAYMENT ACCOUNTS	2023
Checks	63%	55%	70%	73%	66%	65%
ACH debits	38%	32%	42%	42%	43%	33%
Wire transfers	30%	25%	34%	23%	46%	24%
Corporate/commercial credit cards (e.g., purchasing, T&E, fleet)	21%	25%	18%	16%	21%	20%
ACH credits	20%	17%	22%	20%	22%	19%
Cash	5%	4%	6%	4%	9%	4%
Virtual cards	5%	6%	4%	5%	5%	3%
Mobile Wallets (Venmo, PayPal®, etc.)	3%	3%	4%	2%	7%	1%
Faster payments (RTP®, FedNow®, etc.)	2%	1%	2%	--	6%	1%
Cryptocurrency (Bitcoin, Ethereum, etc.)	1%	1%	1%	1%	2%	--

Evolution of Fraud Schemes

Accounts payable (AP) fraud is a type of illegal and dishonest activity that involves misappropriating money from a company's payment system. It can be perpetrated by employees, vendors, or outside parties, and can take many forms.

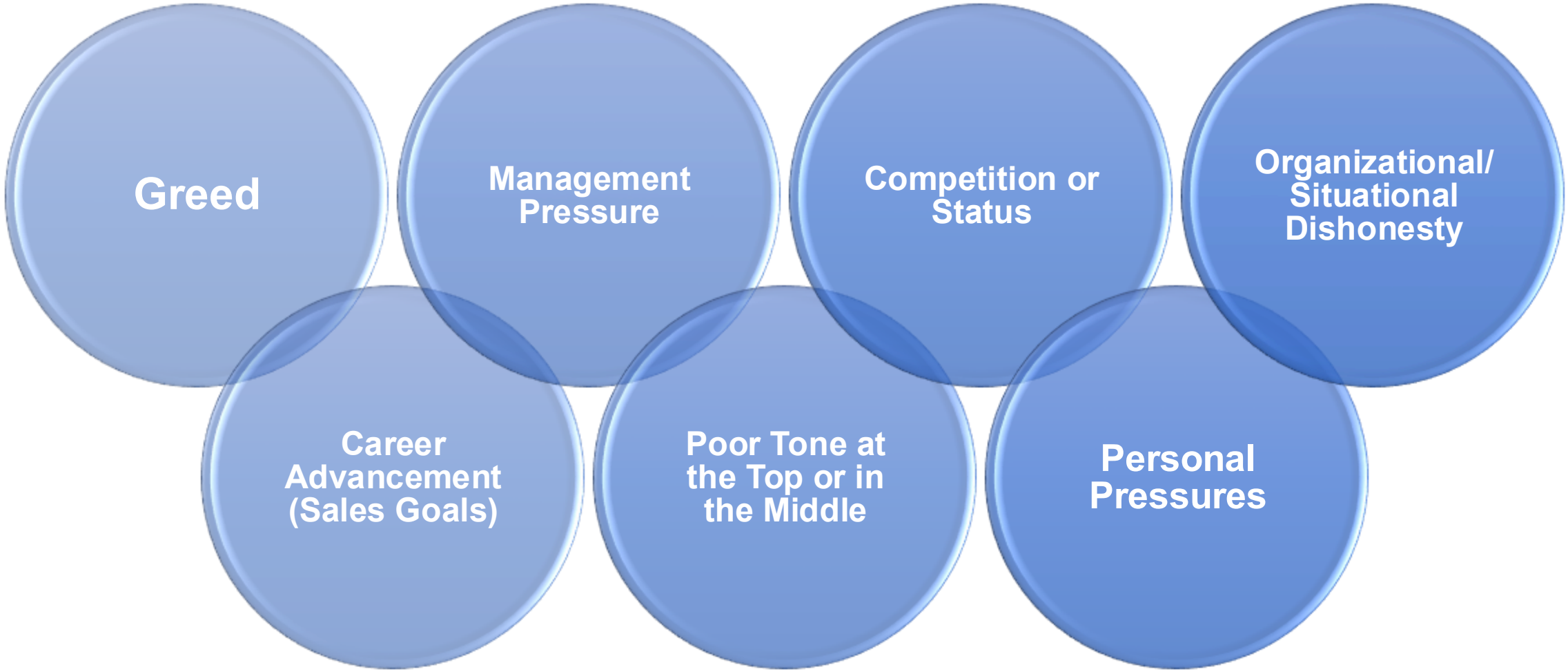


Why People Commit Fraud – Human Factors



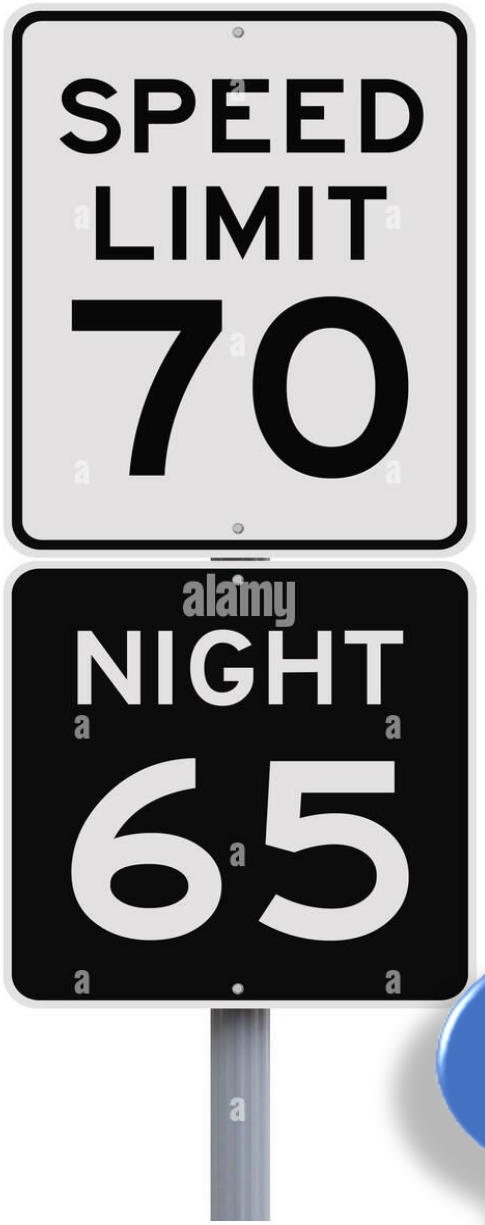
Grievance or ideation → Preparation → Exploration → Experimentation → Execution → Escape

What Motivates Unethical Behavior



What Sign

The Law



Guidance

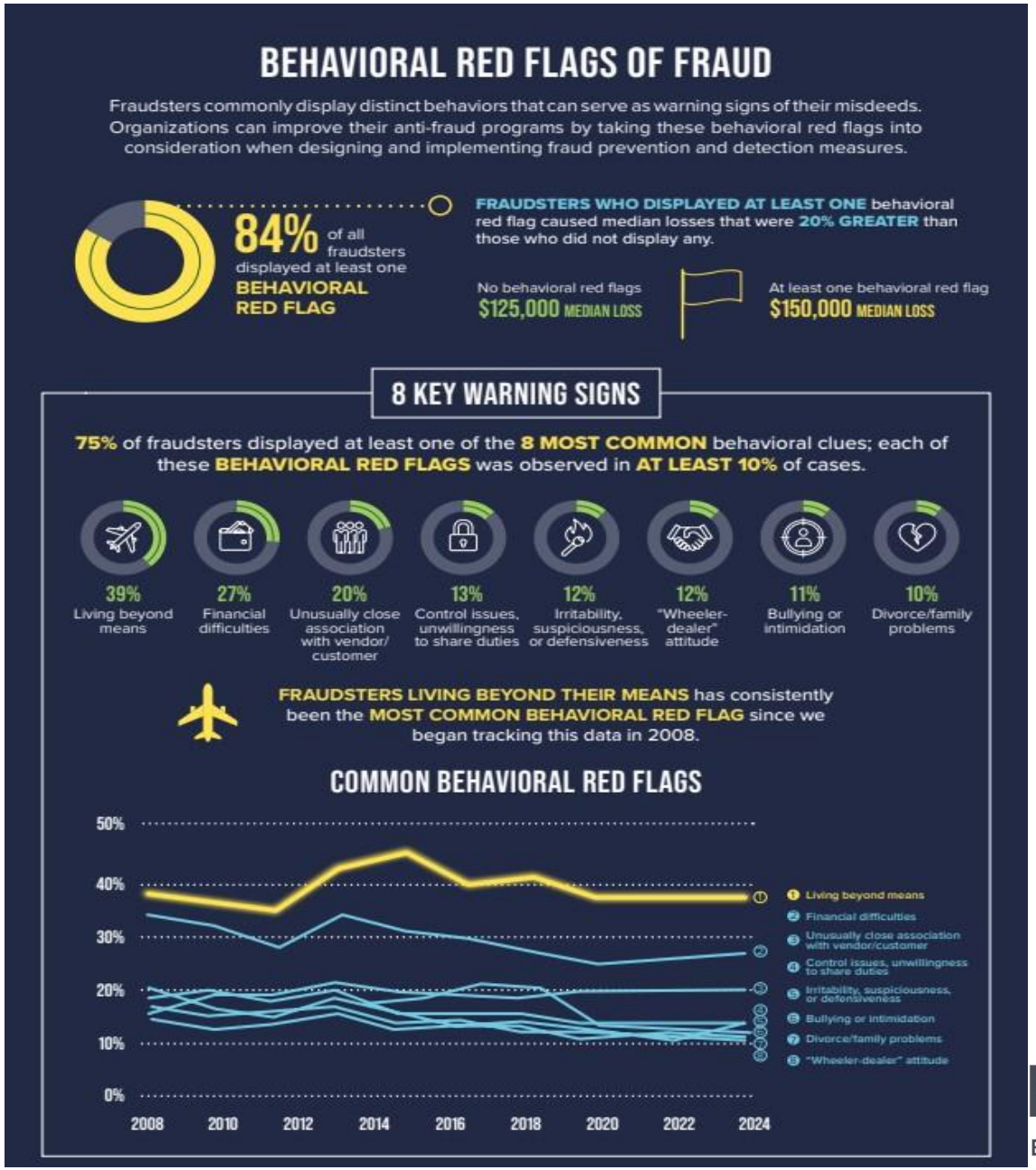
Tolerable Limit

Suggestion

ACFE 2024 Annual Fraud Report to the Nation

Behavioral Red Flags

- *Is there consistent dialogue among departments and functions?*
- *Does ERM track and elevate awareness of risk?*
- *What proactive steps are you taking to manage risk?*
- *How effective is your organization at managing human capital risk?*

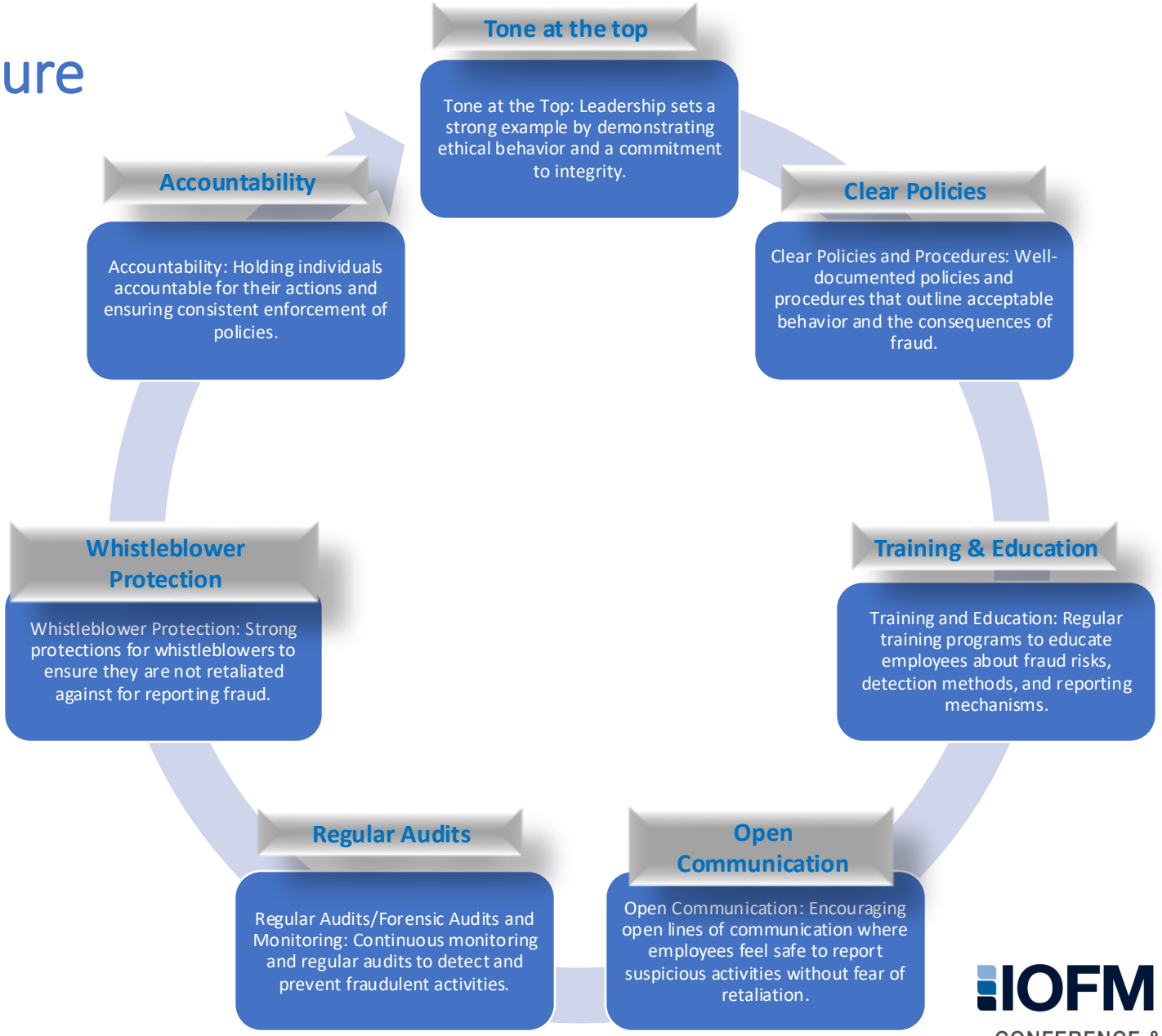


Fall EXPO

Importance of Training & Awareness Programs

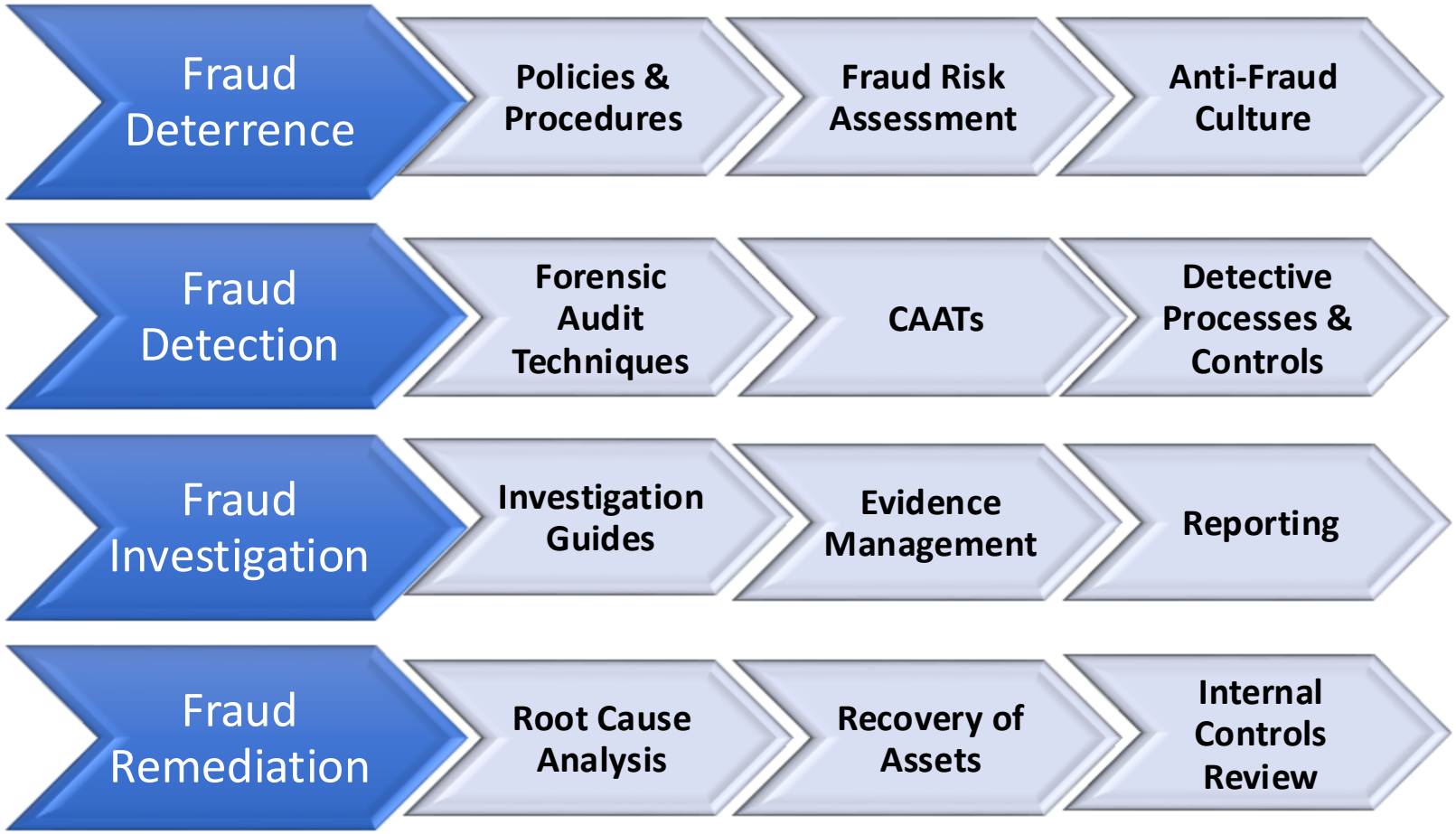
ACFE 2024 Annual Fraud Report to the Nation

Building Fraud Aware Culture



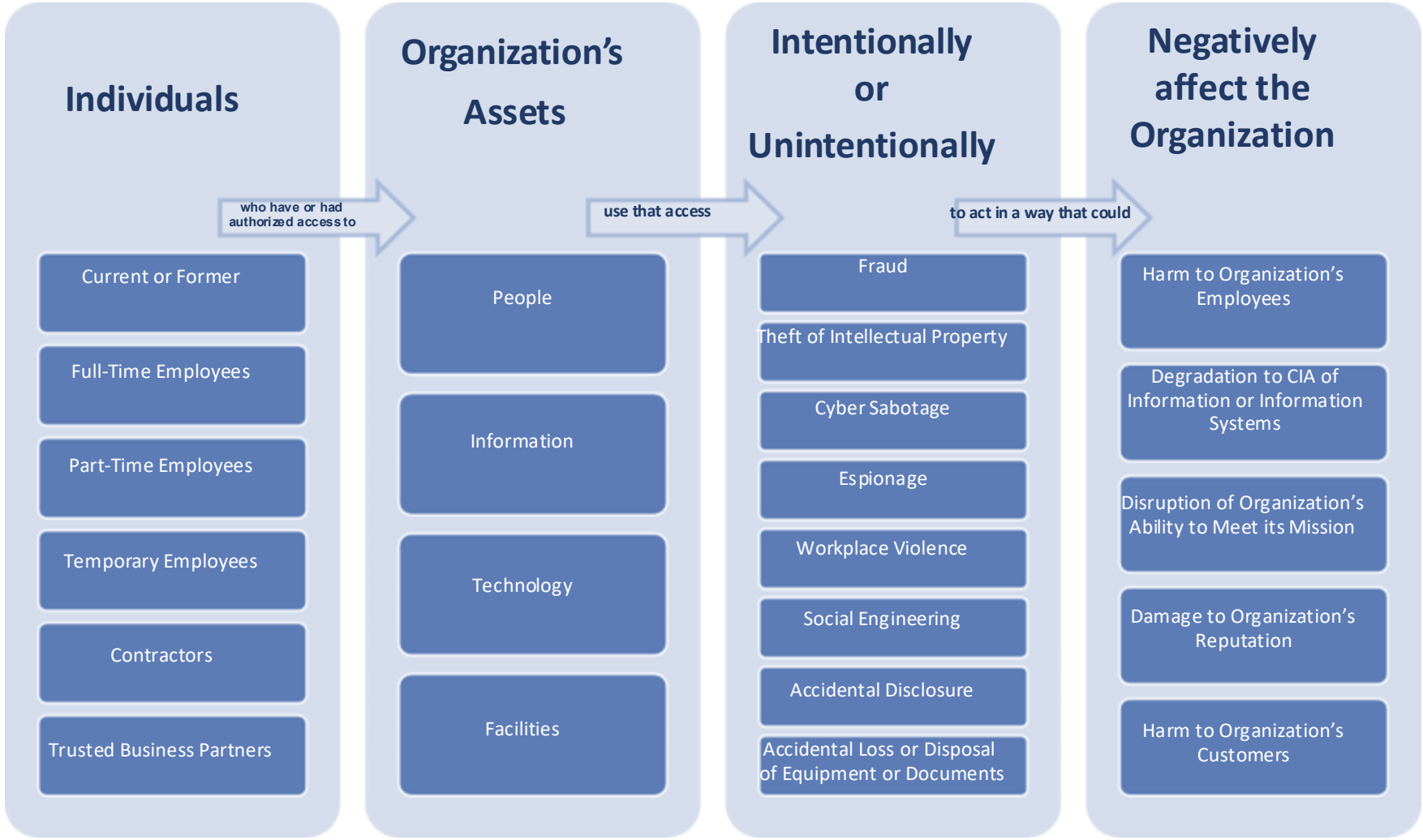
IOFM Fall CONFERENCE & EXPO

Fraud Risk Management Programs & Controls



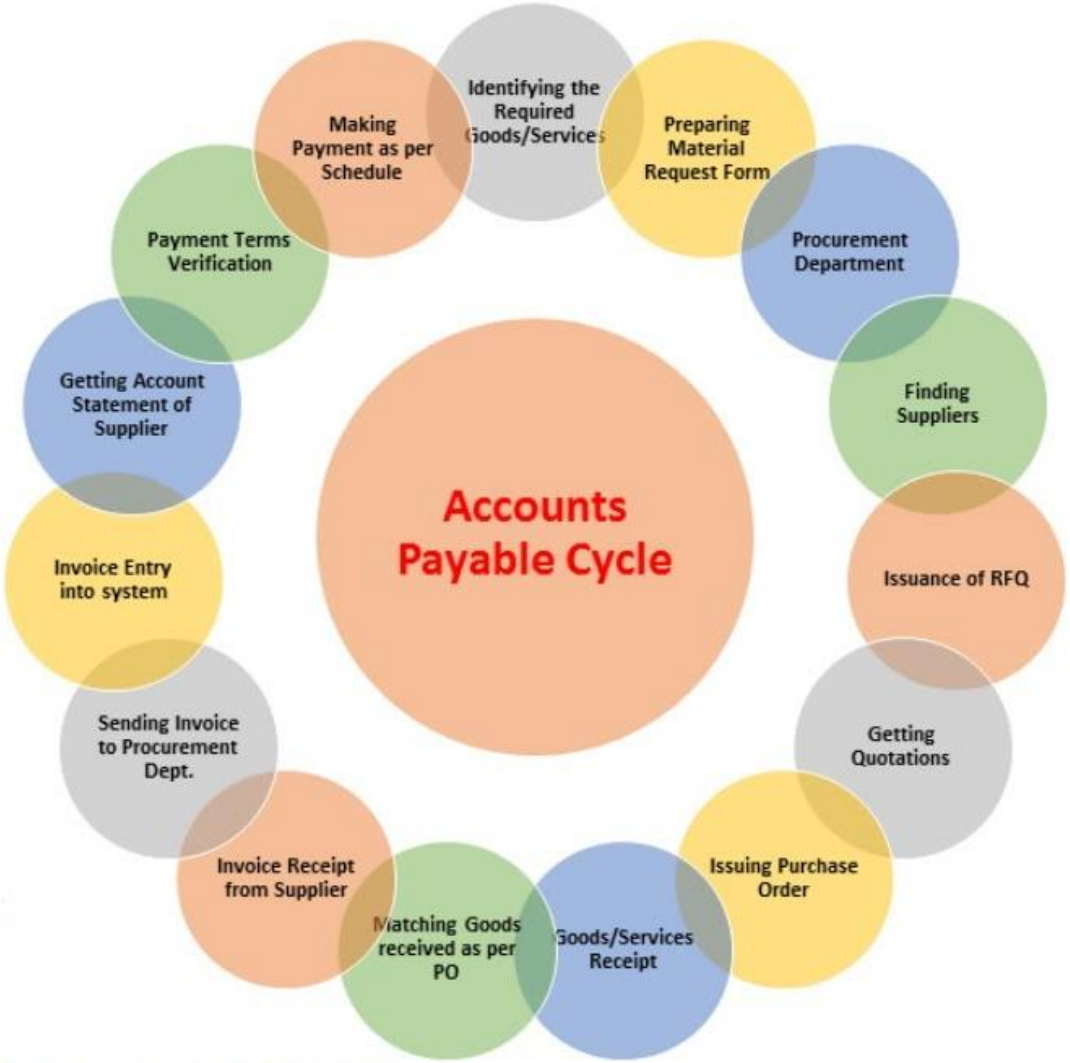
Insider Threat

75% to 80% fraud risk attributed to insider



Accounts Payable Risk Landscape

Account Payable Lifecycle

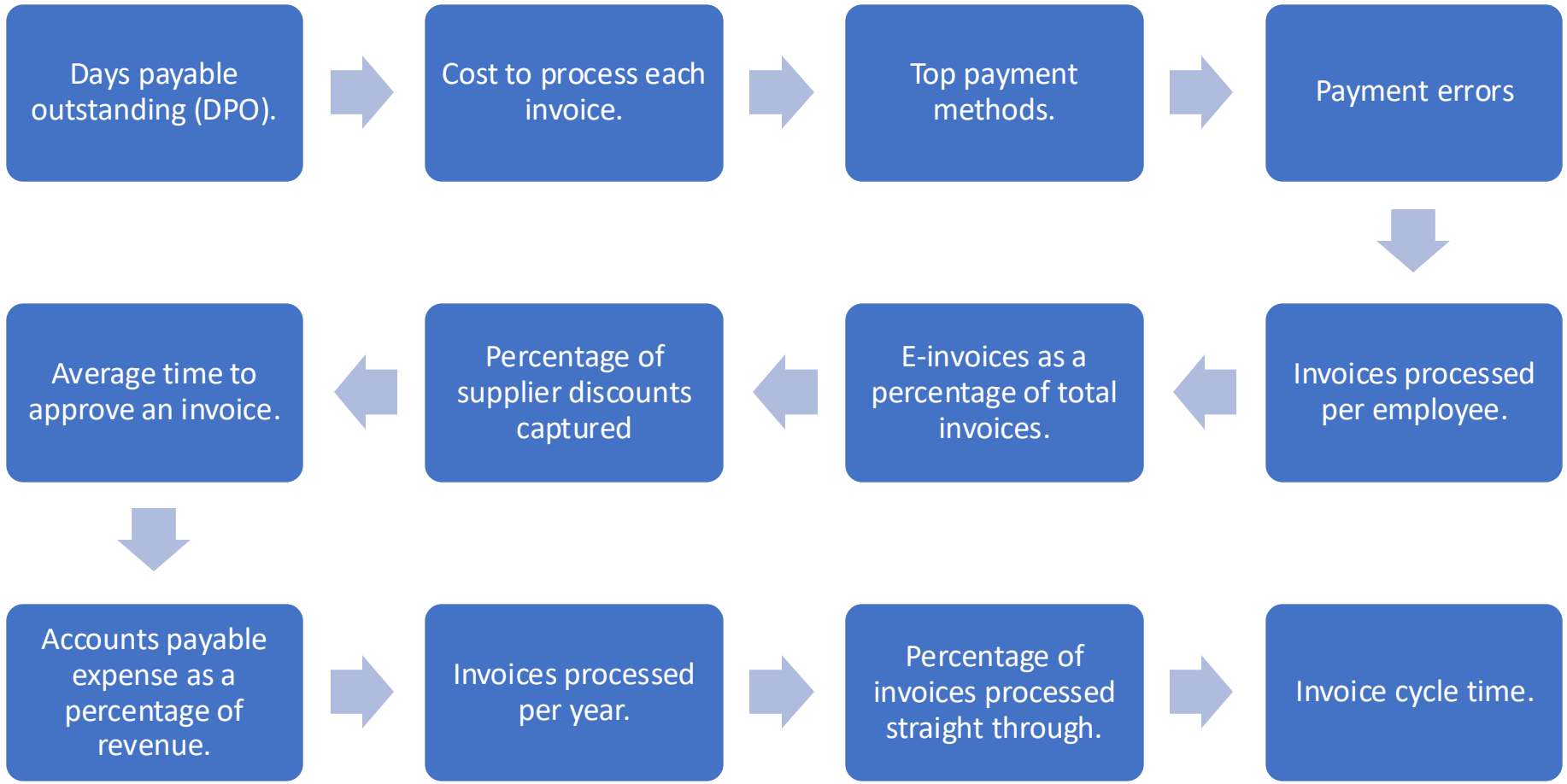


Risk = Vulnerability X Threat

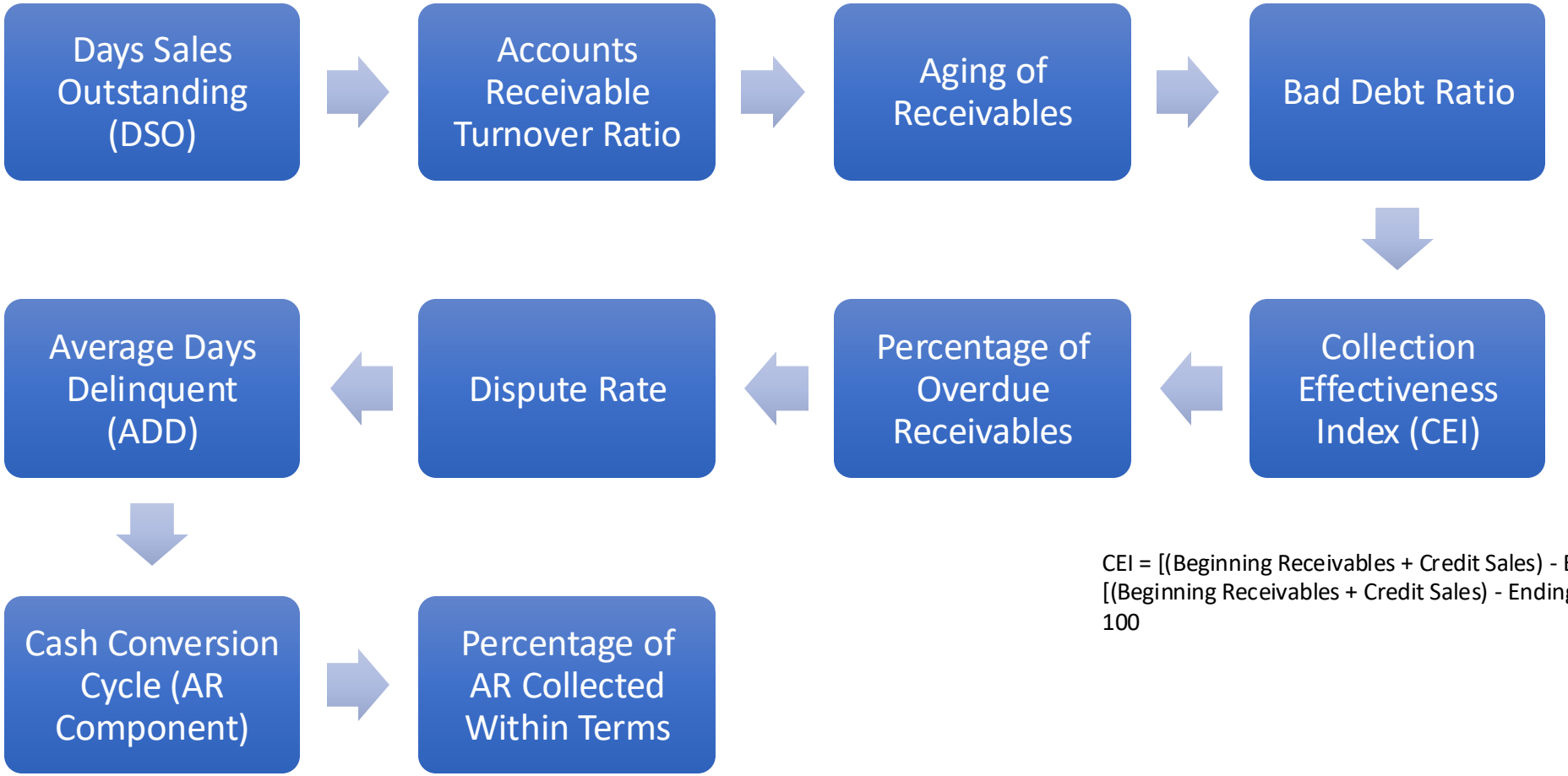
Invoice Receipt → Invoice Verification → Payment Processing → Payment Reconciliation

IOFM Fall CONFERENCE & EXPO

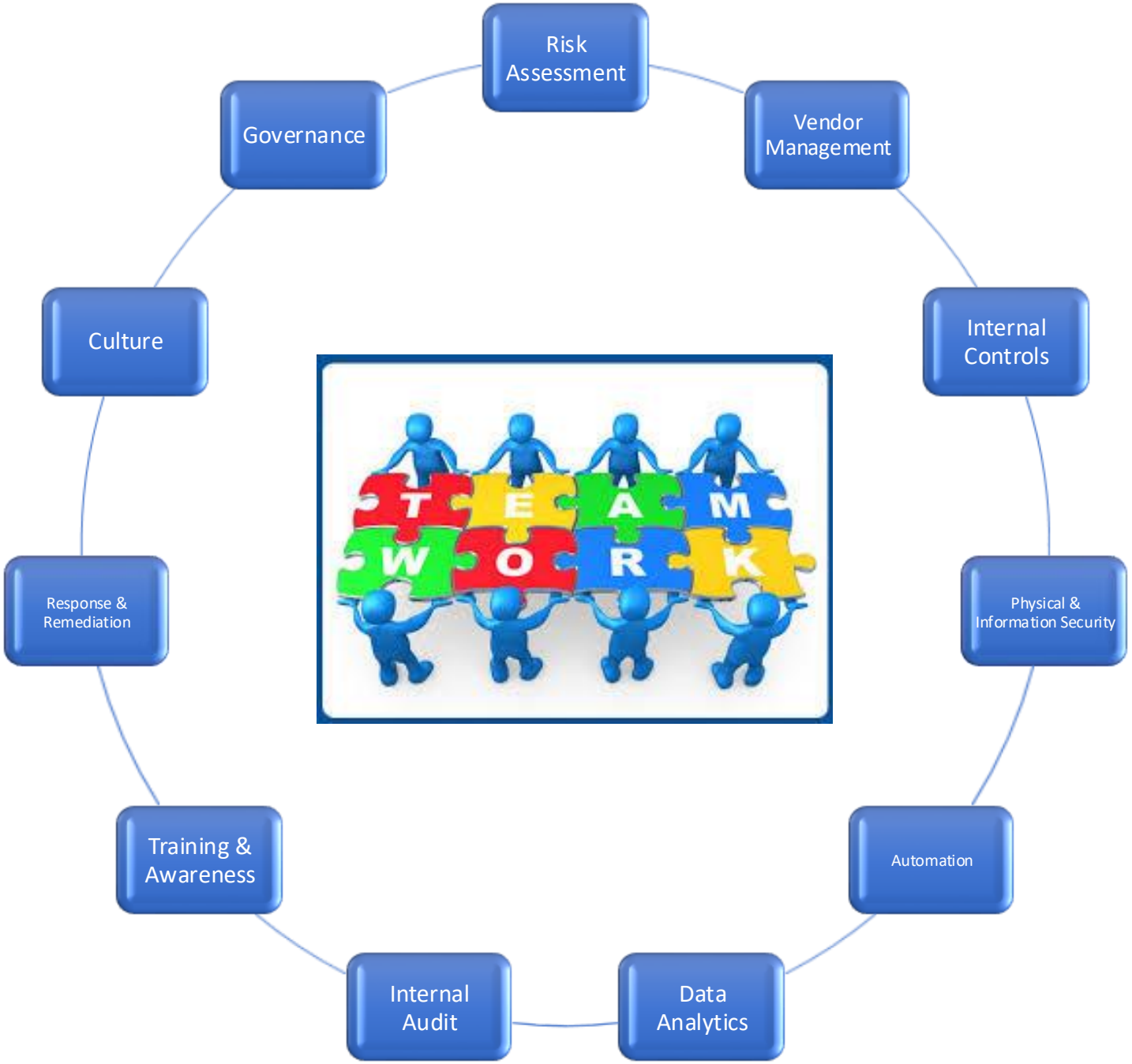
Top Accounts Payable KPIs



Top Accounts Receivable KPIs

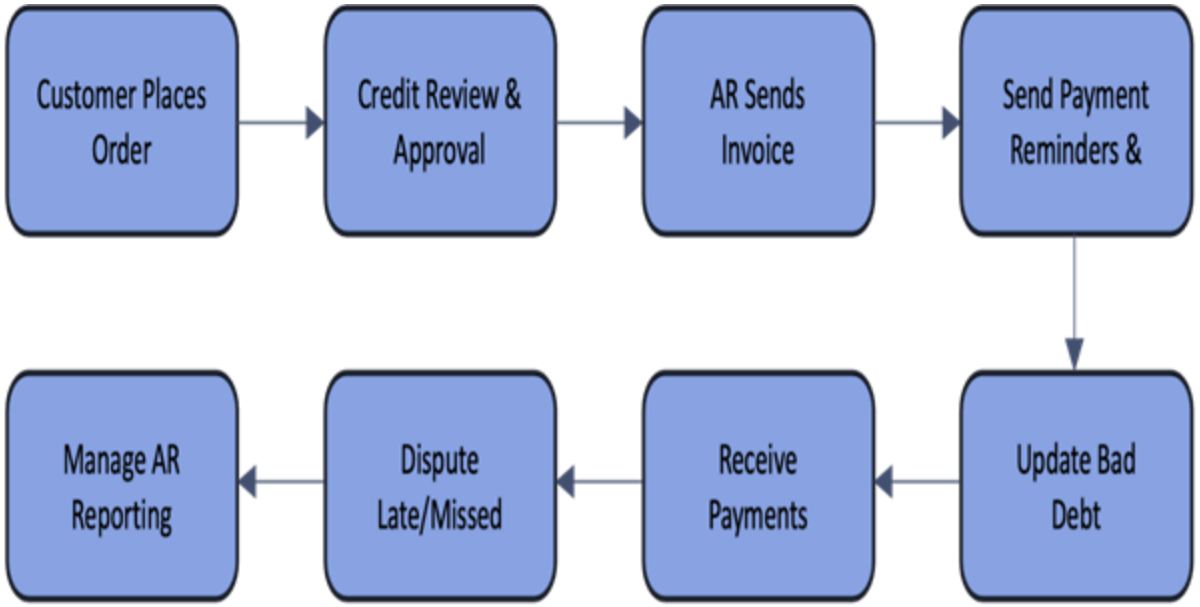


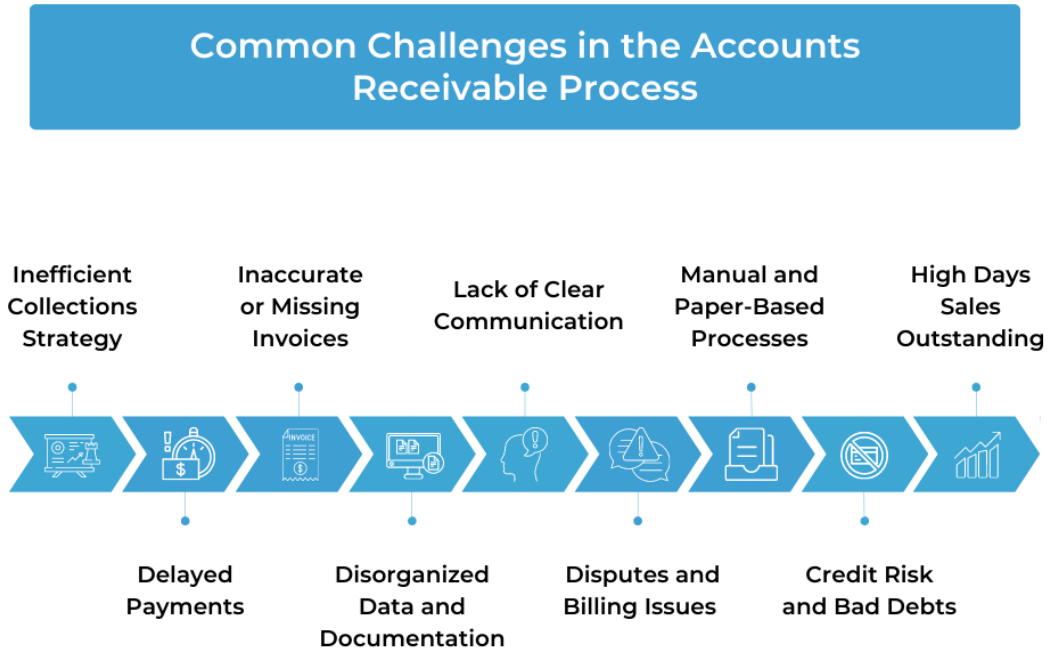
CEI = [(Beginning Receivables + Credit Sales) - Ending Total Receivables] / [(Beginning Receivables + Credit Sales) - Ending Current Receivables] * 100



Accounts Payable Fraud Resiliency Lifecycle

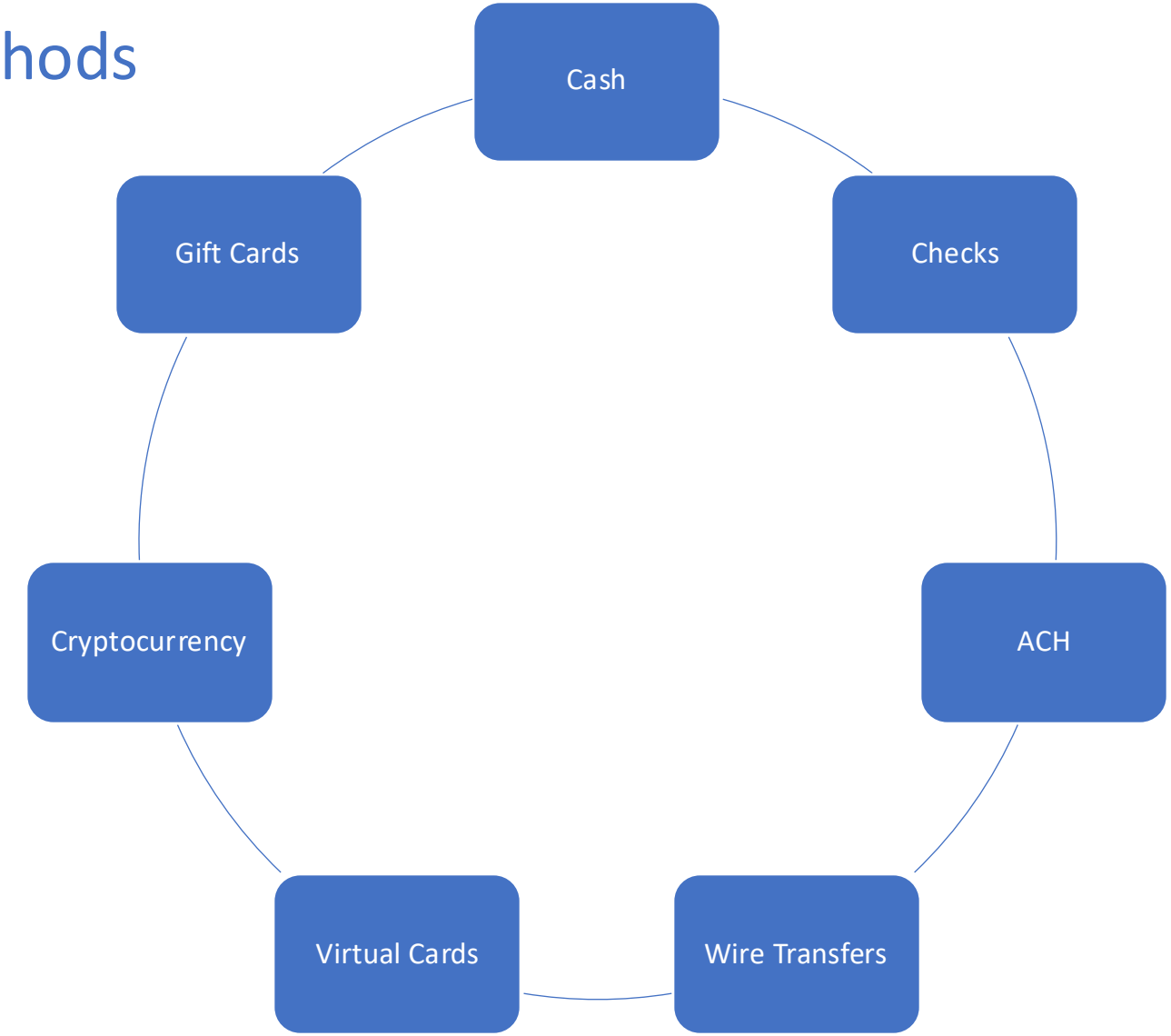
Accounts Receivable Risk Landscape



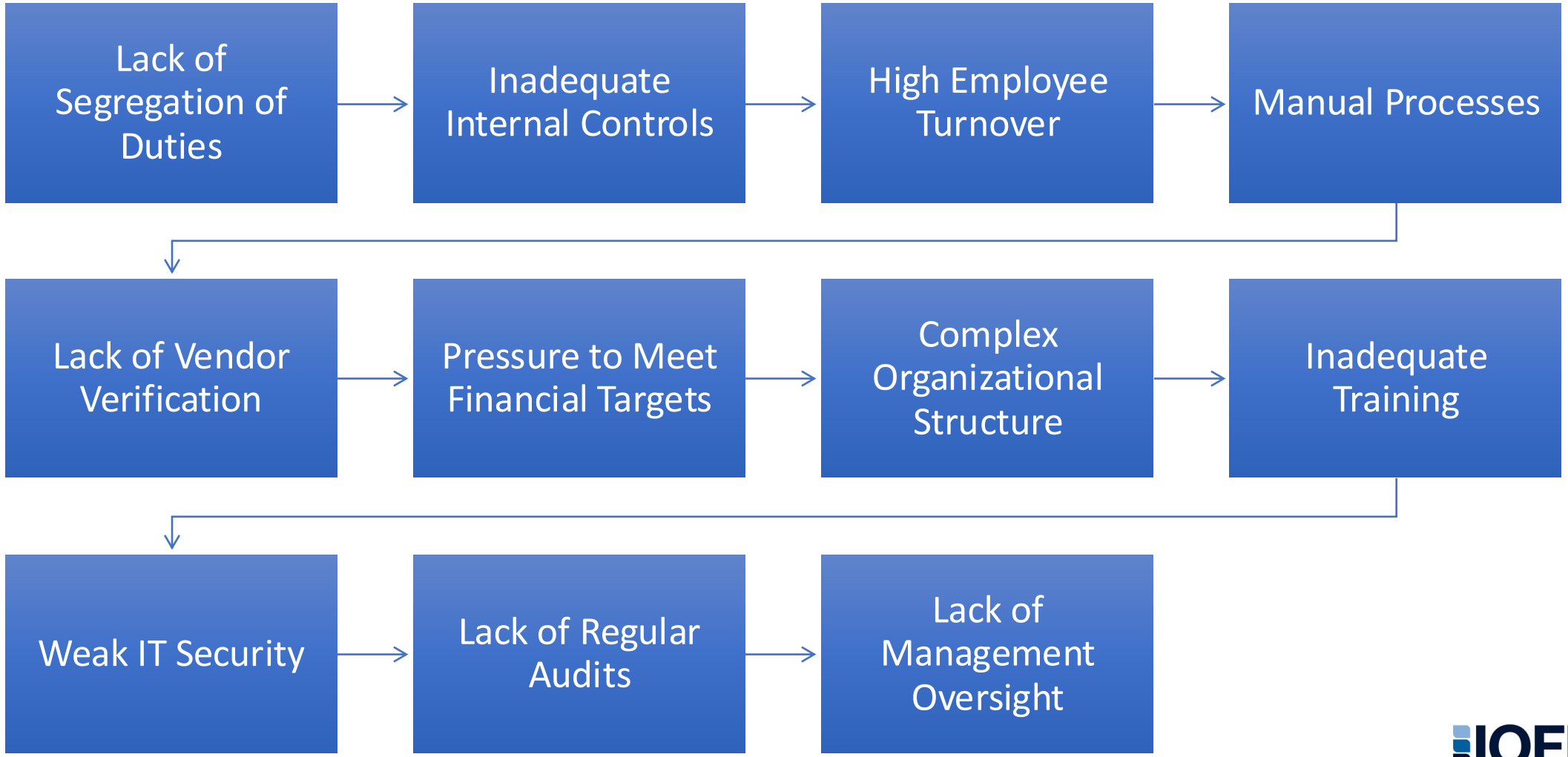


IOFM Fall CONFERENCE & EXPO

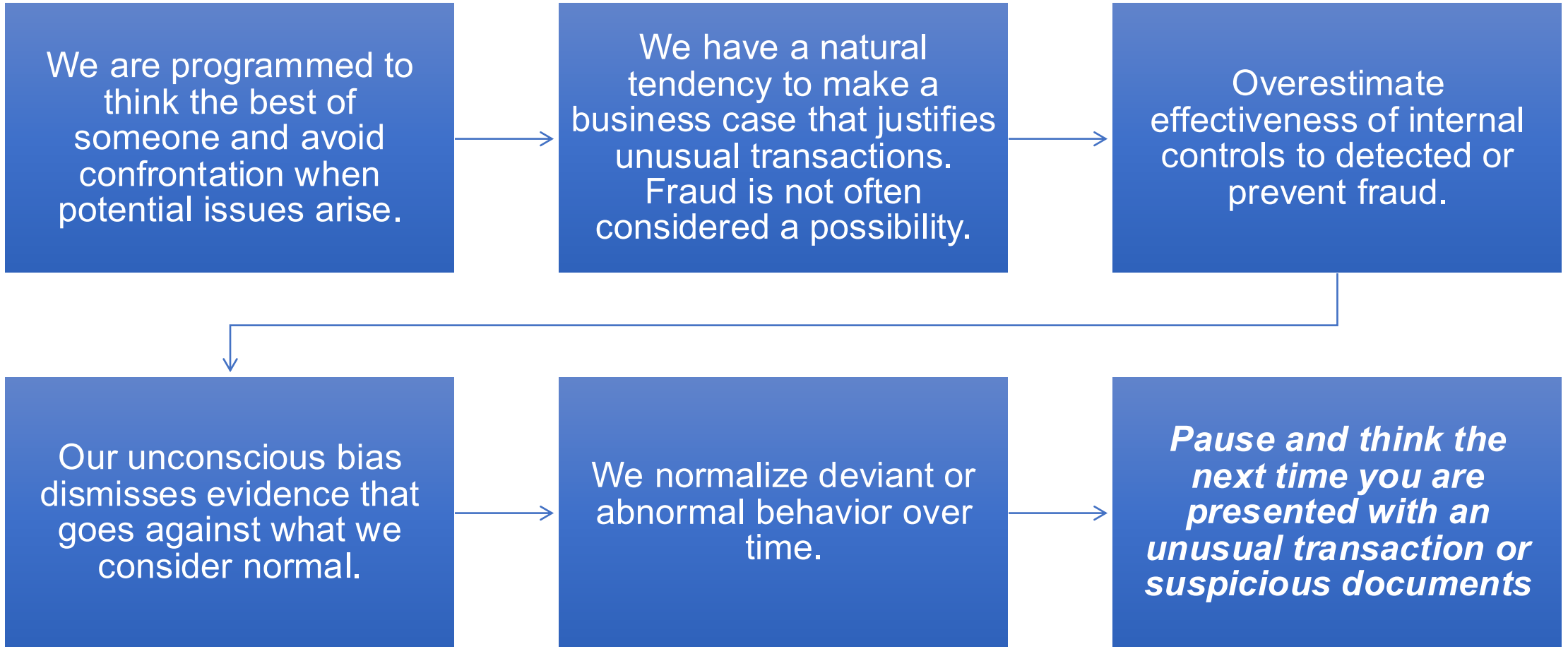
Payment Methods



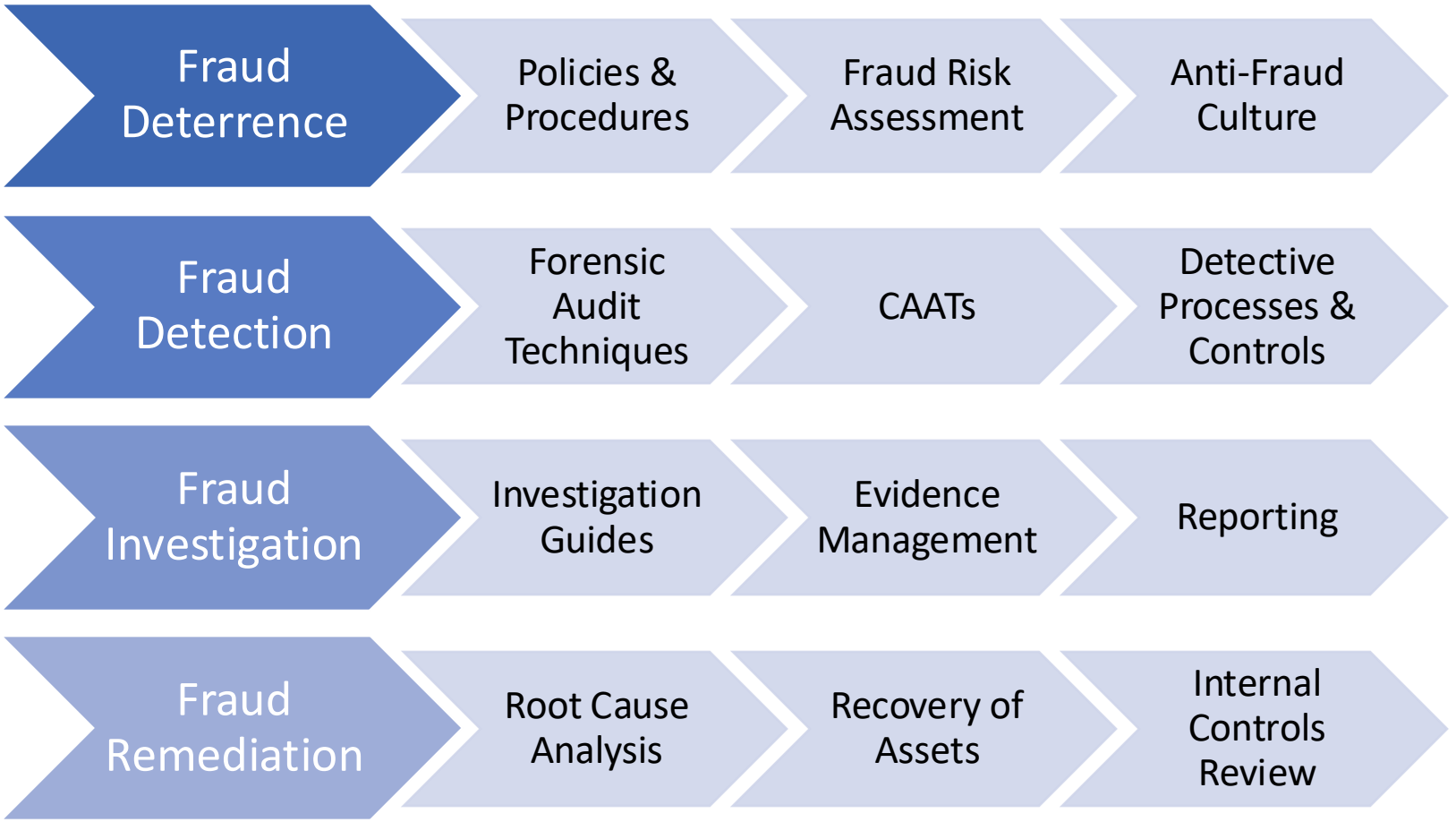
Key Risk Factors



Fraud Awareness and Mindset



Fraud Risk Management Process



Fraud Schemes

IOFM Fall
CONFERENCE & EXPO

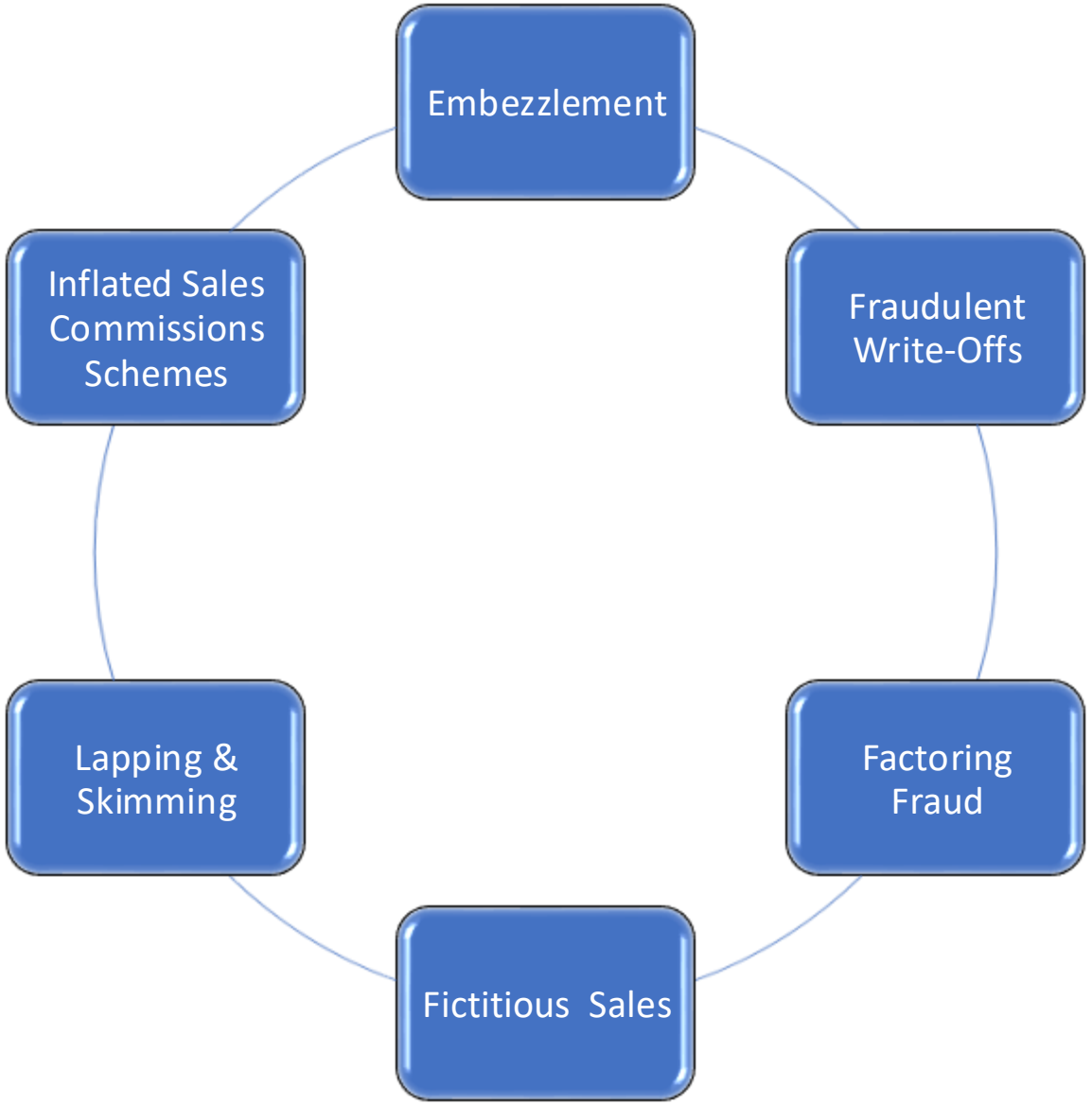
Accounts Payable Fraud

Internal	External
Overbilling or duplicate payments	Vendor fraud
Paying for goods/services not received	Corruption schemes
Fictitious vendors	Cyber fraud
Personal or disguised purchases	BEC schemes
Financial statement fraud	Conflicts of interest
Kickbacks	Incomplete/inferior goods or services

Accounts Payable Fraud Red Flags

- Unexplained variances (increase in payables to existing or new vendors/budget variances)
- Vendor complaints of non or insufficient payment
- Unusual payment requests
- Unfamiliar vendors
- Missing or falsified documentation
- Inconsistent invoices
- Unusual employee behavior
- Unexpected or increasing write-offs
- Large one-time payment

Accounts Receivable Fraud



Accounts Receivable Fraud Red Flags

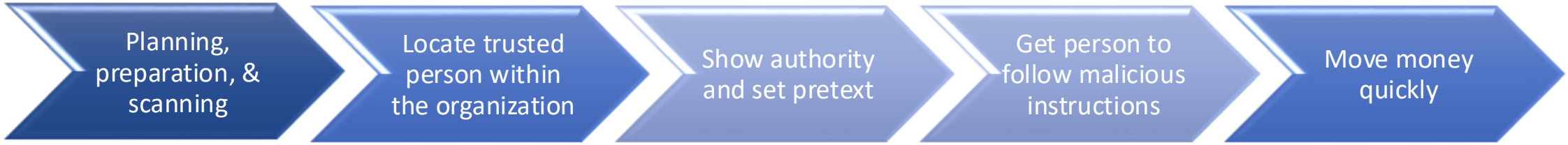
Financial Statement Fraud

- Slow turnover
- Excessive write-offs and errors
- Customer complaints
- Employees who refuse to train new staff, share responsibilities or won't take PTO.
- Unusual increase in bad debt/aged account balances
- Abnormal amount of credits and rebilling
- Increase in sales with declining cash flow (aging AR)
- Increase in AR as percentage of total revenue

Asset Misappropriation

- Increased activity with dormant customers
- Unusual increase in sales to new customers
- Increase in cash receipts applied to incorrect customer accounts
- Incomplete or altered supporting documentation
- Sudden changes in customer information
- Diversion of payments from old or written-off accounts
- Sudden decline in refunds (per store, region, or employee)

BEC – Phishing Attacks



Email

Phone Calls

Text Messages

Malicious Websites

- Business email compromise (BEC) - work email account is compromised and previous emails are compromised. Hacker exploits position of trust.
- Business email fraud (BEF) – attacker undertakes some form of fraud other than gathering additional intelligence.
- Vendor email compromise (VEC) – targeted account is a supplier to the organization.
- Financial supply chain compromise (FSCC) – hacker targets victim organization to make payment to fraudulent bank account.
- Account hijack – credentials are known by hacker but no changes are made but email rules can be altered
- Account takeover – more aggressive as changes are made to the account (change password or other info)

BEC Internal Control Methods

2024 AFP Payments
Fraud and Control Report

Common Types of AP Fraud

Billing Schemes

Most common type of fraud perpetrated by the accounting department in ACFE's 2024 study. Billing schemes can take on a few different forms, including:

Setting up a shell company for which the employee can generate false invoices and cut checks. Fraudulent invoices for services companies are most common because there is no physical inventory to account for.

Pass-through schemes, in which an employee who approves invoices and authorizes payments sets up a shell company that orders things the company legitimately gets from another supplier. These items are then marked up and sold to the business through the shell company, and the employee keeps the profit.

Generating invoices from inactive suppliers in the vendor master file and writing checks to vendors the company no longer does business with.

Check Fraud - Prevention

Positive Pay:	• Implement a positive pay system where the company provides the bank with a list of checks issued. The bank then matches the checks presented for payment against this list.
Segregation of Duties:	• Ensure that different employees are responsible for issuing checks, reconciling bank statements, and authorizing payments to prevent any single person from having too much control.
Check Security Features:	• Use checks with advanced security features such as watermarks, microprinting, and holograms to make them harder to counterfeit.
Controlled Check Stock:	• Store blank check stock in a secure location and limit access to authorized personnel only.
Dual Signatures:	• Require dual signatures for checks above a certain amount to add an extra layer of authorization.
Regular Audits:	• Conduct regular internal and external audits to review check issuance and reconciliation processes.
Vendor Verification:	• Verify the authenticity of vendors and their banking details before issuing checks to prevent payments to fraudulent entities.
Electronic Payments:	• Encourage the use of electronic payment methods such as ACH transfers, which are generally more secure than paper checks.

Check Fraud - Detection

Bank Reconciliation:	• Perform timely and regular bank reconciliations to identify discrepancies between the company's records and the bank's records.
Check Monitoring:	• Use automated systems to monitor check activity and flag unusual transactions, such as checks issued out of sequence or to unfamiliar payees.
Fraud Detection Software:	• Implement fraud detection software that uses algorithms to identify patterns indicative of check fraud.
Employee Training:	• Train employees to recognize signs of check fraud and encourage them to report suspicious activities.
Review Check Endorsements:	• Regularly review check endorsements to ensure they match the intended payee.
Bank Alerts:	• Set up alerts with your bank for any large or unusual check transactions.
Duplicate Check Numbers:	• Monitor for duplicate check numbers, which can indicate that checks are being reused fraudulently.
Physical Inspection:	• Periodically inspect physical checks for signs of tampering, such as alterations in the payee name or amount.

ACH Fraud - Prevention

Dual Authorization:	Require dual authorization for initiating and approving ACH transactions, ensuring that no single individual has complete control over the process.
Segregation of Duties:	Separate responsibilities among different employees for initiating, approving, and reconciling ACH transactions to reduce the risk of internal fraud.
Vendor Verification:	Verify the authenticity of vendors and their banking details before setting up ACH payments to prevent payments to fraudulent entities.
ACH Blocks and Filters:	Use ACH blocks and filters to control which transactions are allowed to debit your accounts. Blocks can prevent all ACH debits, while filters allow only pre-approved transactions.
Secure Banking Platforms:	Use secure, encrypted banking platforms for initiating ACH transactions to protect against cyber threats.
Employee Training:	Train employees on the risks of ACH fraud and best practices for secure transaction processing, including recognizing phishing attempts and other social engineering tactics.
Strong Password Policies:	Implement strong password policies and multi-factor authentication (MFA) for accessing banking systems to prevent unauthorized access.
Regular Audits:	Conduct regular internal and external audits of ACH processes and transactions to identify and address vulnerabilities.

ACH Fraud - Detection

Transaction Monitoring:

- Use automated systems to monitor ACH transactions in real-time and flag unusual or suspicious activities, such as transactions to new or unrecognized accounts.

Daily Reconciliation:

- Perform daily reconciliations of ACH transactions to quickly identify and investigate discrepancies between the company's records and bank statements.

Bank Alerts:

- Set up alerts with your bank for any large or unusual ACH transactions, including notifications for transactions above a certain threshold.

Fraud Detection Software:

- Implement fraud detection software that uses algorithms to identify patterns indicative of ACH fraud.

Review ACH Reports:

- Regularly review ACH transaction reports provided by your bank to ensure all transactions are legitimate and authorized.

Account Activity Review:

- Periodically review account activity for any unauthorized or unusual transactions, especially those involving new or infrequent payees.

Positive Pay for ACH:

- Use ACH positive pay services where the company provides the bank with a list of authorized ACH transactions, and the bank matches incoming transactions against this list.

Vendor and Employee Education:

- Educate vendors and employees about ACH fraud risks and encourage them to report any suspicious activities or requests for banking information.

Kickback Schemes - Prevention

Segregation of Duties:	Vendor Due Diligence:	Vendor Rotation:	Code of Conduct:
• Ensure that different employees are responsible for vendor selection, purchase order approval, invoice processing, and payment authorization to prevent collusion.	• Conduct thorough background checks and due diligence on all vendors before establishing a business relationship. This includes verifying ownership, financial stability, and reputation.	• Rotate vendors periodically to prevent long-term relationships that could lead to kickbacks. Avoid reliance on a single vendor for critical supplies or services.	• Implement a comprehensive code of conduct that explicitly prohibits kickbacks and outlines the consequences of engaging in such activities. Ensure all employees and vendors are aware of and adhere to this code.

Kickback Schemes Prevention

Training and Awareness:	Whistleblower Program:	Approval Hierarchies:	Contract Clauses:
• Provide regular training to employees on recognizing and preventing kickback schemes. Emphasize the importance of ethical behavior and the potential legal and financial consequences of fraud.	• Establish a confidential whistleblower program that allows employees and vendors to report suspicious activities without fear of retaliation.	• Implement multi-level approval processes for high-value transactions and vendor contracts to ensure that no single individual has undue influence over the decision-making process.	• Include anti-kickback clauses in vendor contracts, specifying that any form of kickback is prohibited and will result in contract termination and potential legal action.

Kickback Schemes - Detection

Data Analytics:	• Use data analytics to identify patterns and anomalies in accounts payable transactions. • Look for red flags such as repeated use of the same vendor, unusual payment amounts, or payments made outside normal business hours.
Vendor Audits:	• Conduct regular audits of vendor transactions and relationships. • Review vendor invoices, contracts, and payment records for any signs of irregularities or suspicious activities.
Employee Lifestyle Monitoring:	• Monitor for significant changes in employee lifestyles that may indicate involvement in kickback schemes, such as sudden wealth or extravagant spending.
Cross-Referencing:	• Cross-reference vendor addresses and contact information with employee addresses and contact information to identify potential conflicts of interest.

Kickback Schemes - Detection

Anonymous Surveys:	• Conduct anonymous surveys among employees and vendors to gather insights on potential unethical practices and areas of concern.
Review of High-Risk Vendors:	• Focus on high-risk vendors, such as those with a history of irregularities or those providing non-tangible services, for more frequent and detailed reviews.
Transaction Reviews:	• Regularly review and reconcile accounts payable transactions, especially those involving high-value or high-frequency payments, sudden increases in vendor spend, to ensure they are legitimate and properly authorized.
Internal Audits:	• Conduct periodic internal audits of the accounts payable process to identify weaknesses in controls and areas susceptible to kickback schemes.

Fraud Prevention & Detection

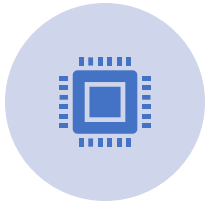
IOFM Fall
CONFERENCE & EXPO

Fraud Detection with AI

Anomaly detection: AI can analyze large volumes of transaction data to identify unusual patterns or anomalies that may indicate fraudulent activity such as duplicate payments, payments to unknown vendors, or transactions that deviate from the norm

Predictive analytics: machine learning algorithms can predict potential fraud by learning from historical data and identifying risk factors.

Automated invoice processing: AI can automate the verification of invoices against purchase orders and receiving reports, reducing the risk of human error and fraud.

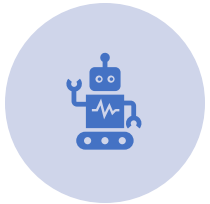


Real-time monitoring: AI systems can provide real-time monitoring and alerts for suspicious transactions or changes to vendor details, enabling immediate investigation and response.

Behavioral analysis: AI can track and analyze user behavior to detect deviations from normal activity, which may signal fraudulent intent such as unusual access to financial systems or irregularities in transaction approvals

Natural language processing (NLP): NLP can be used to analyze email communications and detect phishing attempts or fraudulent requests.

Fraud scoring: AI can assign fraud risk scores to transactions based on various factors, helping prioritize investigations.



Continuous learning: AI systems can continuously learn and adapt to new fraud tactics, improving their detection capabilities over time.

Detecting Accounts Receivable Fraud

Identify anomalies in payment schedules, delayed remittances, and unauthorized write-offs	Cross-check payment patterns against customer history and contract terms	Detect manipulation of aging reports and unauthorized credit extensions	Predict payment risks based on customer behavior	Flag unusual adjustments, sudden credit notes, and invoice reversals
Identify customers receiving unauthorized discounts or extensions	Analyze customer payment behavior and service usage trends	Identify suspicious cancellations, reversed invoices, or sudden billing changes	Monitor credit limits, payment history, and subscription patterns	Score customers based on payment reliability and behavioral risks
	Track invoice-to-payment timelines	Detect patterns of repetitive overdue accounts tied to specific sales reps	Identify inconsistencies in AR records and cash application	

Behavioral Clustering

Clustering "Normal" Behavior

- AI models analyze historical data (e.g., customer payment habits, invoice frequency, transaction size, timing).
- The model groups entities—like vendors, customers, or employees—into clusters of similar behavior.
- Example: Customers who usually pay within 30 days.
- Example: Vendors who issue 2–3 invoices per month for predictable amounts.

Detecting Anomalies

- New data points are compared against these clusters.
- Any data point that doesn't fit into any cluster well (i.e., behaves very differently from peers) is flagged for potential fraud.
- Example: A vendor who suddenly submits invoices twice as often for double the usual amount.
- Example: A customer who reverses payments frequently or applies large discounts not seen in their cluster.

Benefits in Fraud Detection

- No need to define fraud rules upfront—it adapts as behavior changes.
- Unsupervised: Doesn't require labeled fraud data, which is often scarce.
- Scalable: Can handle thousands or millions of transactions to find hidden patterns.

Detecting Accounts Payable Fraud

Invoices submitted just below approval thresholds	Repeated invoice numbers or vendor account reuse	Mismatched payment terms and vendor history	Payments to blacklisted vendors
Transactions outside normal business hours	Conflicts of interest from internal employee-vendor connections	Computer vision to read invoices and compare them with purchase orders	Models trained on historical invoice and vendor data

Detecting Accounts Payable Fraud

Anomalies such as invoice cloning, approval threshold manipulation, and vendor impersonation

- Model used fuzzy matching to compare invoice metadata (amount, vendor, line items) and detect duplicates or near-duplicates.
- Historical data trained the algorithm to understand normal vs. suspicious submission patterns.
- Invoices from the same vendor with nearly identical line items but different invoice numbers.
- Invoices submitted at irregular times (e.g., weekends or holidays).
- Same invoice amounts appearing across different business units.

Approval threshold manipulation

- Models trained to understand standard invoice patterns and detect repeated sub-threshold amounts submitted within a short time frame.
- Time-series analysis applied to track when multiple low-value invoices were submitted from the same vendor.
- Multiple invoices just below a key threshold (e.g., $9,950 when approval is needed for $10,000+).
- Several low-value invoices submitted within days of each other for the same project or purchase order.
- Invoices approved by the same employee without escalating to a second approver.

Vendor Behavior Analysis

Profile vendor behavior (e.g., frequency of invoicing, invoice size, delivery timing)	Detect anomalies like abrupt cost increases, duplicate charges, or invoice splitting	Assign dynamic fraud risk scores to each vendor	Vendor invoice trends and compare them to historical norms	Changes in vendor data like bank accounts or service types
Patterns in timing (e.g., end-of-quarter invoice spikes)	Monitor vendor behavioral shifts (new banking info, abrupt cost changes)	Detect deviations in invoice frequency and category	Build vendor risk profiles based on historical behavior and contract delivery patterns	Flag suspicious activities like repeated change orders, billing above market rates, and vendor clustering
	Monitor for deviations from expected invoice timing, pricing, and volume	Detect relationships between vendors and internal staff (conflict of interest)	Alert finance teams to high-risk vendor behavior in real time	

Preventing Fraud

Segregation of Duties: Ensure that different employees handle invoice approval, payment processing, and account reconciliation.

Vendor Management: Maintain a vetted and approved vendor list, and regularly review and update vendor information. **Authentication, Validation and Management**

Invoice Verification: Implement a three-way match process to verify that purchase orders, receiving reports, and vendor invoices align before payment.

Approval Workflows: Establish clear approval hierarchies and require multiple levels of authorization for large or unusual transactions.

Regular Audits: Conduct periodic internal and external audits to identify and address discrepancies or irregularities.

Automated Systems: Use accounts payable automation software to enhance accuracy, track transactions, and flag suspicious activities.

Employee Training: Educate employees on fraud risks and detection techniques, and encourage them to report suspicious activities.

Fraud Detection Tools: Implement data analytics and monitoring tools to detect patterns indicative of fraud.

Whistleblower Hotline: Provide a confidential reporting mechanism for employees to report suspected fraud without fear of retaliation.

Policy Enforcement: Develop and enforce comprehensive policies and procedures for accounts payable processes.

Accounts Payable Controls

Accounts Receivable Controls

- Segregation of Duties (SoD)
- Lockbox Banking Services or Direct Deposits
- Daily Bank Reconciliation
- Approval Controls for Write-Offs and Credit Memos
- Customer Statements and Confirmations
- Real-Time AR Aging and Exception Reports
- Automated Cash Application with Dual Review for Exceptions
- Restricted Access to AR Systems and Audit Trails
- Monitoring of Employee Activity and KPIs
- Fraud Awareness Training and Whistleblower Channel

Please tell us what you think!

- Please scan this QR code using your mobile to access a short feedback survey →
- Also accessible via the mobile app