



PREVENTING HOLIDAY FRAUD:

Insights and Best Practices for Handlers of High-Value Assets



**LOWERS
& ASSOCIATES**

International Risk Mitigation Partners



TABLE OF CONTENTS:

When a Perfect Storm of Risk Meets the Holiday Season	3
Why Fraud Prevention (Always) Matters	4
Spotlight: 2 Startling Human Capital Risk Factors	7
Infographic: The 3 Sides of the Fraud Triangle	8
4 Culprits of Complacency	9
Spotlight: Data Analytics & Fraud Control	13
5 Principles of Fraud Risk Management	14
The Claims Investigation Process in 6 Steps	17
About Lowers & Associates	18



**LOWERS
& ASSOCIATES**
International Risk Mitigation Partners

When a **Perfect Storm** of Risk Meets the **Holiday Season**

Fraud at any time is never a welcome event. But fraud during the holidays has the concentrated potential to ruin one of the most important revenue opportunities for many businesses managing high-value assets.

The current threat environment includes pressure from inflation, supply and distribution challenges, skilled labor shortages, and skyrocketing cybercrime. It's unlike anything I've seen in my 40 years in this business. But as always, it's in these moments that prevention and detection matter most.

We've designed this eBook to provide high-value asset handlers (and the insurers that represent them) actionable insights and best practices to rise above the perfect storm of risk threatening their business this holiday season. Being proactive when employees have the opportunity and incentive to rationalize fraud stymies complacency and keeps businesses and the communities they serve moving forward.

In the following pages, we highlight several advancements in technology and data analytics, as well as how established fraud risk management principles can be applied to current threats to prevent fraud. One of the core beliefs our team has long held is that, to prevent fraud, you must always "Trust, but verify." The companion piece of advice in this eBook is that "If you stay ready, there's no need to get ready."

The team at Lowers & Associates is standing by to help with an assessment, audit, or evaluation of your business. We wish you a blessed, happy, and fraud-free holiday season.



D. Mark Lowers
CEO
Lowers Risk Group

Why Fraud Prevention (Always) Matters



Despite the prevalence of organizational fraud and its well-documented costs, businesses both large and small continue to operate without – or fail to review and test – systematic fraud prevention programs, running the risk of avoidable loss and reputational harm.

Being able to identify, avoid, and overcome social engineering, wire fraud, cyber hygiene, and physical security threats provide business owners and their teams real opportunities to scale effectively and pursue new opportunities to grow the business.

WHAT'S AT STAKE?

The process of developing a fraud prevention program is beneficial because, in addition to helping prevent future fraud, it also kick-starts discovery. Often, fraud hides in plain sight (for example, interdepartmental dependencies and shared access points can create vulnerabilities).

High Reliability Organizations – and those that work on their behalf – are not satisfied with convenience, remain inherently curious, and choose willingly to reduce the risk of fraud. This provides the business numerous tactical and competitive advantages over those organizations that don't.

Here's a quick look into what's at stake (and what to expect) when it comes to fraud prevention for those that handle cash and those who represent their insurance interests:



FOR HIGH-VALUE ASSET HANDLERS, this means:

Understanding and continually validating the Three P's of fraud prevention – [Policy](#), [Process](#), [Procedure](#) – that are designed to reduce and control the likelihood and severity of loss relating to risk.



FOR RETAILERS, this means:

Specifically controlling points of access to key assets or functions integral to the business, deploying a system of checks and balances, utilizing employment background screening, and incorporating random audits.



FOR BROKERS, this means:

Making sure clients have the correct infrastructure, training, and understanding of their policies, as well as the proper coverage to match the risk and associated collateral risks.



FOR UNDERWRITERS AND INSURERS, this means:

Confirming that the insured's risks are truly covered (with all third-party assessments adequate) and they can engage an incident response team.

OBJECTIONS

The known/unknown paradox says that, just because a business does not know its risks, does not mean the risks do not exist. Because unless the business has designed and implemented a custom fraud prevention program informed by leading best practices, it cannot actually and accurately identify where its vulnerabilities are.

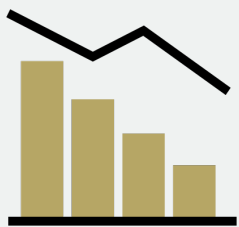
Here are a few of the standard arguments against fraud prevention programs we often hear:

- “With the probability of fraud so low, the cost outweighs the benefit of prevention.”
- “Spending time focused on prevention tactics detracts from real growth opportunities.”
- “The business is too small/ too big to not notice fraud before it happens.”
- “Trusted employees would never commit fraud against their place of work.”

KEY DATA POINTS

When it comes to handling valuable assets like cash, coin, data, and specie, understanding how to manage risk provides a boost to any businesses’ bottom-line. Controlling fraud risks is a vital component:

- According to data revealed in the Association of Certified Fraud Examiners (ACFE) [2022 Report to the Nations](#)



Certified Fraud Examiners (CFEs) estimate that organizations consistently lose 5% of their revenue each year to fraud.



now involve two or more people, a 16% increase in the last 10 years.

2,110 cases of occupational fraud were investigated by CFEs in 133 countries



The typical fraud lasted 12 months before detection, causing a median loss of \$8,300 per month.



- In September 2022, a U.S. Labor Department report estimated that \$45.7 billion in federal unemployment insurance funds were [stolen by fraudsters](#) taking advantage of the COVID-19 pandemic.
- In our connected world, digital [fraud risks like BEC](#) (business email compromise) have multiplied alongside ransomware, jumping from \$1.8 billion to \$2.4 billion (as [many large companies](#) have learned).

WHO BENEFITS?

In our research, we've found that most businesses we work with typically only consider the threats external entities pose (the flipside being that these external entities are, in turn, viewing the business as a risk). Clients often don't consider this, ignoring their own internal threats.

When a business develops and regularly pressure-tests a strong fraud prevention program, it gains the ability to control its own fate. Those are qualities that give board members, investors, vendors, partners, and compliance auditors confidence.

During Fraud Week 2021, L&A President and expert witness Jon Groussman talked about preventing fraud:



BOTTOM-LINE

Whether during the holidays, peak summer, or any time in-between, the fall-out of reputational, operational, or financial fraud can be a gut punch to the integrity of any business. And while it may not always seem like an immediate catastrophe, the cumulative effects always are.

The truth is, as long as businesses compete fiercely on price in markets where consumers can purchase with the click of a button, tight margin conditions and the cost management of fighting fraud can – and often does – mean the difference between profit and loss.



2 Startling Human Capital Risk Factors

In its recently released 2022 Report to the Nations, the Association of Certified Fraud Examiners (ACFE) detailed several notable trends in global fraud. For high-value asset handlers and small-to-medium size business owners attempting to prevent or identify fraud this holiday season, two data points stand out:

#1

50% of fraudsters exhibit at least ONE red flag to the **HUMAN RESOURCES** department

Human Resources plays an integral role in identifying – and preventing – potential fraud. In their 2022 Report to the Nations, data collected by the ACFE showed that in half of all fraud cases, Human Resources observed at least one red flag prior to or during the fraud. The three most common were fear of job loss, poor performance evaluations, and having been denied a raise or promotion.

#2

Check and payment tampering, as well as skimming, impact small businesses more than others – and they typically take

16-18 months to discover.

With an average median loss per month of \$8,700 combined, these two types of fraud can cause any cash-centric business to fail. According to a [2020 PwC Global Economic Crime and Fraud Survey](#), 60% of companies ended up better-off after conducting an investigation, but only 50% actually complete that step.



Infographic: The 3 Sides of the Fraud Triangle

In 1973, criminologist Donald R. Cressey first published his theory about fraud, highlighting the now famous “fraud triangle”, which says fraud occurs when the fraudster feels financial pressure, his or her organization presents an opportunity, and the person can rationalize the theft.

The first few words of his hypothesis capture the essence of this crime, and why it is difficult to confront: “Trusted persons become trust violators...” In other words, there is an internal conversion that turns an employee (at any level) into a thief.

During the holidays, all three sides of the fraud triangle can be in play, but the value of the fraud triangle is that it helps us to look at the objective factors that have to be present for fraud to occur. Recognizing these helps to define actions high-value asset handlers can take to help prevent fraud, partly through organizational policy controls and partly through managing employee relationships to encourage openness and trust.

As your business navigates this upcoming holiday season and the external economic threats, use this infographic to recognize the factors that must be present for fraud to occur and how to combat them.

THE FRAUD TRIANGLE

OPPORTUNITIES STEM FROM:

- ▶ Weak Internal Controls
- ▶ Poor Security
- ▶ Unchecked Management Access
- ▶ Low Likelihood of Detection
- ▶ Lack of Policy Enforcement
- ▶ Uncontrolled Vendor Relationships



OPPORTUNITY

Potential fraudsters identify an opportunity to use/abuse a position of trust for personal gain and believe they have a low risk of getting caught in the act.

Opportunity can sway the otherwise honest.

INCENTIVE

Need and greed are common incentives for committing fraud. When coupled with opportunity, the temptation can be all too great.



A model for understanding why people commit fraud

RATIONALIZATION

Some individuals possess an attitude or set of ethical values that allows them to knowingly and intentionally commit a dishonest act. Others may be able to rationalize a fraudulent act as being consistent with their personal code of ethics.



COMMON PRESSURES:

- ▶ Financial Difficulties
- ▶ Living Beyond Means
- ▶ Control Issues
- ▶ Divorce/Family Problems
- ▶ Wheeler-Dealer Attitude
- ▶ Unusually Close Association with Vendors

COMMON RATIONALIZATIONS:

- ▶ “I was only borrowing the money.”
- ▶ “I was entitled to the money.”
- ▶ “I had to steal to provide for my family.”
- ▶ “I was underpaid; my employer cheated me.”
- ▶ “My employer is dishonest and deserved to be fleeced.”

6 WAYS TO COMBAT FRAUD

- ▶ Form internal audit programs
- ▶ Establish a code of conduct
- ▶ Conduct pre-employment screening
- ▶ Perform management reviews
- ▶ Screen suppliers and third parties
- ▶ Watch for “red flag” fraud indicators

For more information, explore our [fraud investigation](#) and [loss prevention services](#), or contact us for a [fraud prevention consultation](#).



4 Ways Complacency and Fraud Work Together

Complacency is a cold-blooded killer. Dreams, goals, strategy. Personal or professional. None of it stands a chance when complacency finds a home. With its warm blanket of delusion, complacency is guaranteed to leave you (and your business) behind the times, below your potential, and exposed to threats.

In its 2022 Report to the Nations, the Association of Certified Fraud Examiners (ACFE) observed that businesses lose 5% of their revenue every year to fraud. In our line of work, we have found that, whenever complacency takes root, fraud is never far behind.

KEY DATA POINTS

Since 2019, the pandemic has accelerated cybercrime by 1600%. In the last year, inflation has soared above 8%. Food prices are up 10%, 5 million skilled laborers have exited the market, and most economists believe a recession is looming in 2023. With all these external pressures, finding stability for your business will be essential to survival.

There are four ways complacency and fraud typically work together. Businesses that proactively identify and avoid these culprits of complacency are “[whole brands](#)” – or organizations that believe everyone is responsible for the success of the business – and position themselves for growth in most environments.

Set your business up for success by learning how complacency and fraud work together.

1

Aha Moments:

Sudden insights can provide a roadmap to take action.

What Complacency Says:

“This crisis is not imminent, there’s other things to do.”

Some organizations take action proactively, in response to a security assessment, compliance audit, or business continuity evaluation. Others, however, are forced into it by responding to an event (wide-area damage, a cyber hack, or premises liability ruling).

Why do some companies act when others do not? Because their culture permits – and encourages – it. These organizations balance to-dos like operations, process, budgets, communication, competition, and innovation with a vision for the future of the business. They create intentional urgency.

WHY CULTURE MATTERS:

In its 2022 State of the Whole Brand report, creative idea agency Barkley noted that “Culture is the sweet spot when what you do and say on the inside matches on the outside (and vice versa).”

Their findings revealed that businesses with engaged employees who believe in and act on a brand’s idea grew their odds of success more than 50%.

When it comes to risk management in an unstable market, your people are your most valuable – and volatile – asset.

2

Overconfidence:

What once inspired growth can also lead to [financial ruin](#).

What Complacency Says:

"Nothing bad has happened before, the odds are so slim."

Teams typically take cues from management and in this top-down problem, small behavior patterns can snowball into bigger issues: **the door is propped open** while employees run an errand; crisis **communication plans become outdated**; when an employee leaves the company, **passwords are not decommissioned**.

Whether it is a statistical calculation, the illusion of preparedness, or outright arrogance, operating with this mindset invites problems where there need none be. [High Reliability Organizations](#) constantly push to be better – and those efforts further distance the business from the complacency and potential fraud.



3

Delusion:

When big dreams of success grow into fantasies of invincibility.

What Complacency Says:

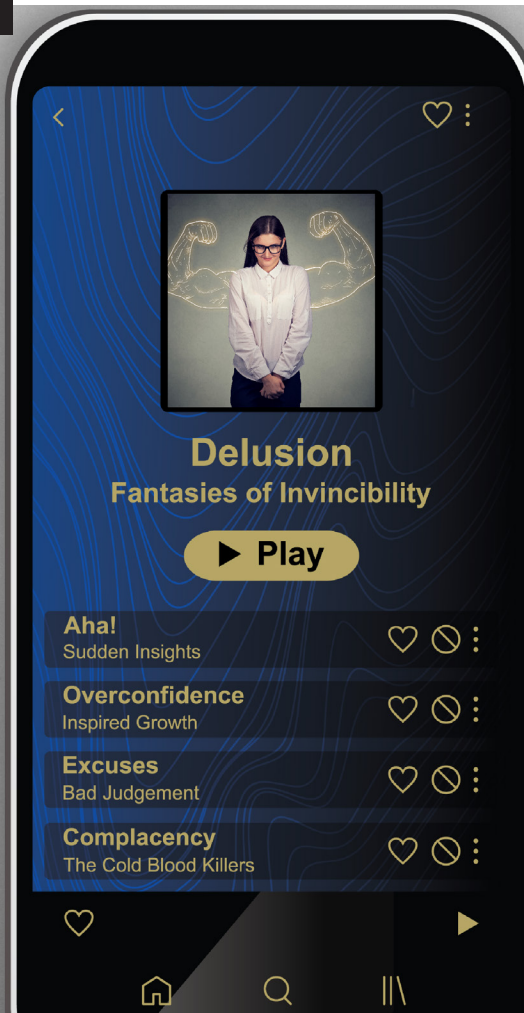
"You already know the answers because you've seen it all."

When executive leadership, risk managers, and yes – asset handlers – believe they know everything, their creative ability to seek out, anticipate, and proactively plan for potential threats stagnates. This false sense of reality can be crippling if fraudsters attack the business.

In 2006, renowned psychologist Carol Dweck introduced the growth mindset concept. For business owners dreaming big, a growth mindset requires action. According to London-based leadership coach Toye Oshunbiyi, [a learner mindset](#) is also advantageous when change – and success – both come fast.

APPLIED MINDSET:

In 2007, Apple applied a learner mindset when they launched the iPhone, Oshunbiyi says. Released at the peak of iPod sales, the iPhone killed the iPod, making way for something bigger and better. They changed the way they learned to anticipate a different future for their products.






4

Excuses:

Justifying bad judgement.

What Complacency Says:

"We've been successful so far, so we must be doing something right."



A culture that, at worst, accepts excuses or at best, turns a blind eye at opportunities to learn, nonetheless embraces a false sense of reality. Common excuses that lead to inaction could be anything from the failure to conduct quarterly safety trainings or the absence of consistent background checks to overlooking [due diligence](#) with a new business partner.



Jamey Waters, CFE
VP of Operations at
Lowers & Associates:

"The holidays create an increase in opportunity. This is an important part of the fraud triangle because it's usually not a lack of policy that leads to fraud, but rather not following policy that creates the opportunity. For example, staffing in 2022 is a concern – it doesn't do any good to have a dual-control cash register policy if only one person is tasked with the job. While policies may be relaxed in an effort to "get the job done" this time of year, a countermeasure could be as simple as continuing to enforce security policy through awareness initiatives and a diligent purposeful check and balance. For our team at L&A, that means trust – but verify."

How Cash Handlers Can Overcome Complacency – And Fraud

Strong leadership is essential to any business, but when it comes to overcoming complacency, it all starts from the culture at the top. Threat assessments, security reviews, [fortifying corporate IT](#) and cybersecurity, building rock-solid controls, quarterly training – none of your security or BCP plans matter if leadership is complacent.



1. Be clear on your vision.

Ensuring sustainable growth means balancing long-term vision (no more than two years out) with any and ALL short-term goals required to execute and make that vision a reality.



2. Trust, but verify.

Having confidence and trust in your managers, co-workers, advisors, and vendors is good, but it is always wise to verify. Due diligence should be thought of as applicable in all cases.



3. Have a specific plan for each day.

This includes specific time each week (about 1 hour) to think strategically and evaluate where the business is and if it's heading in the right direction.



4. Be aware of your surroundings at all times.

In both work and personal life, staying situationally aware keeps you safe and reduces the risk of fraud. When controls are circumvented, risk ALWAYS increases.

“I will not allow yesterday’s success to lull me into today’s complacency, for this is the great foundation of failure.”

- Augustine “Og” Mandino II, author
“The Greatest Salesman in the World”

The below list of insights for high-value asset handlers are drawn from our team of experts and organizations we’ve either worked with or [admire about](#) how to [overcome](#) complacency. Learning to deploy these strategies effectively can mean the difference between meeting your goals or closing your doors.



5. Create a formal process to learn from mistakes.

Risk mitigation, fraud training, business continuity plans, and control audits are both time (and money) well spent to improve skills and build a growth (and learner) mindset within your team.



6. Challenge your team to think.

Encourage and reward innovation by creating platforms for teams to better communicate. Breaking down silos can help create more unified, less vulnerable processes, too.



7. Budgets help you meet goals.

Having cash reserves is obvious, but cashflow must also account for reinvestment, cost control, debt management, and catastrophe planning.



8. Whatever you do, don’t sit still.

“We’ve Always Done It This Way” is a death knell for progress. Attachments to legacy ideas and software, blind loyalty, and a stay-in-your-lane culture do not create greatness – or prevent fraud.

Spotlight: Data as a Fraud Control

As ecommerce, Software as a Service (SaaS), Internet of Things (IoT), automation, and other digital innovations continue to evolve, data – and the ability to analyze that data – has become essential to controlling fraud. Certified fraud examiners, forensic accountants, law enforcement, insurance professionals, and more are **using data to help their high-value asset handling clients** identify trends, backstop vulnerabilities, and create new opportunities to fight fraud.

Two specific innovations Lowers & Associates has embraced are continuous monitoring and open-source global data. Taking advantage of greater accessibility, these software platforms now allow for real-time access to monitor court records data, as well as business information, financial connections, and recoverable assets. Used in combination, it provides a potent one-two punch in fighting fraud.

#1 Background Screening

Businesses screen employees prior to hiring, but continuous monitoring provides the ability to keep eyes on a population that may be deemed higher-risk, those employees that work in dangerous, high-compliance environments, or those that are in situations where pressure, opportunity, and rationalization can often lead to poor decision-making.



Lowers Risk Group's proprietary software analyzes over 2.3 billion corporate documents from 70,000+ global sources in 120 different countries.

Source: Lowers & Associates

#2 Due Diligence Investigations

When the threat of financial, reputational, or personal risk is high, new technology platforms can aggregate open-source global data to provide investigators and researchers instant access to structured business information, offering a more complete picture of new potential vendors, employees, investors, partners, and other business participants.

5 Modern Applications of Effective Fraud Risk Management

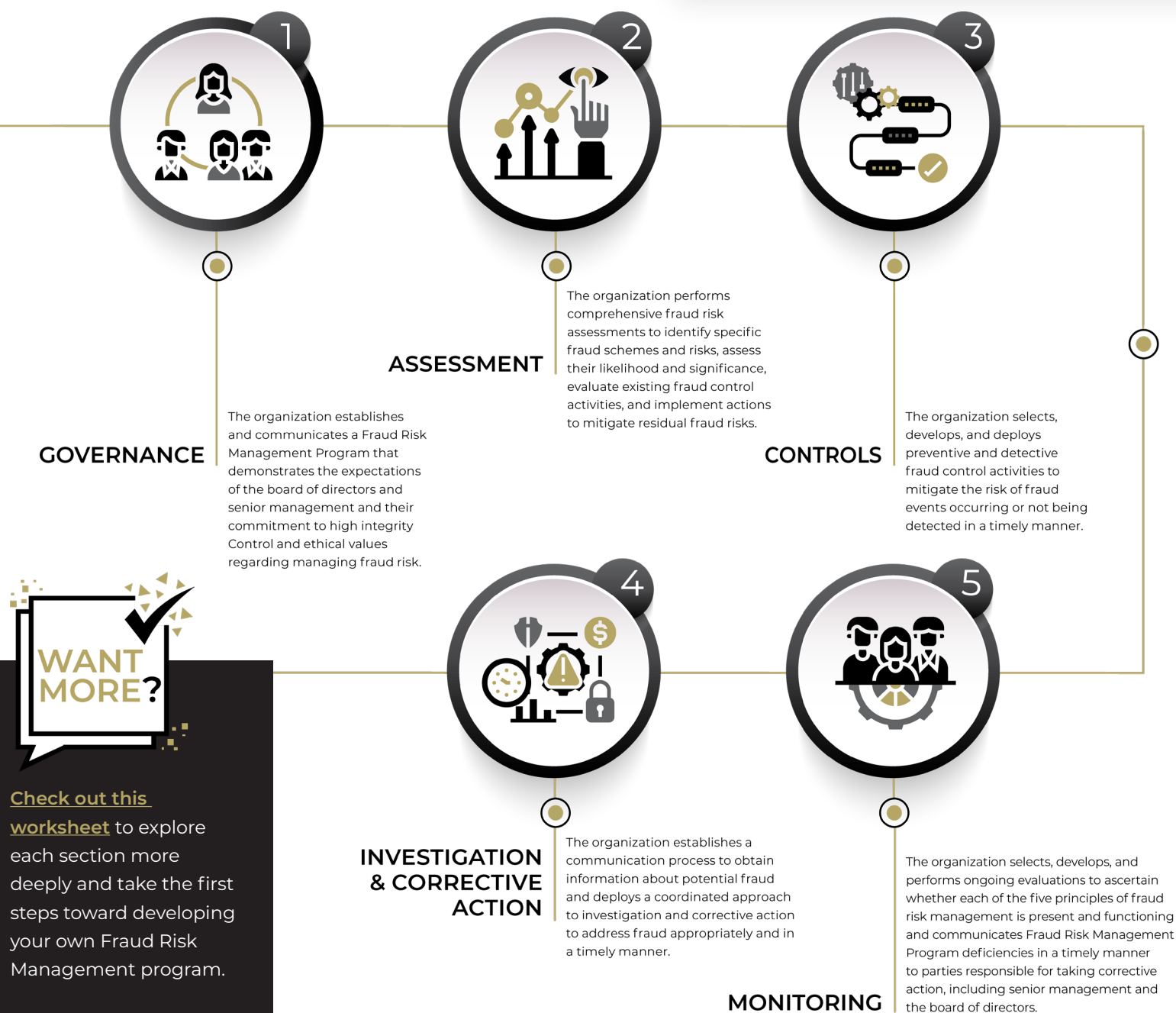
In 2016, the Committee of Sponsoring Organizations of the Treadway Commission (COSO) published the "[Fraud Risk Management Guide](#)" in collaboration with the ACFE. Quickly becoming the gold standard for how to understand, assess, detect, prevent, and monitor fraud, even [the Executive Summary](#) provides a thorough enough overview that any business in any industry can use it as a quick reference for fraud-related questions.

Last year, as the world was emerging from the worst of the COVID-19 pandemic, COSO and the ACFE put out a call on behalf of a "refresh taskforce" to [update the guide](#). New frauds, technology advancements, and regulatory developments are forcing effective fraud management to evolve.

Basic Principles of Fraud Management

As stated in the current version of the guide, "An organization should strive for a structured as opposed to a haphazard approach" when it comes to developing a fraud prevention and detection program. This means ensuring fraud prevention is part of the business' overall risk management efforts.

With that in mind, here's a quick look at the five principles:



Applying Fraud Management Principles to Modern Challenges

For high-value asset handlers, modern fraud schemes blend emerging technology and classic social engineering techniques, placing ransomware, Distributed denial of service (DDoS), and data breaches on par with white-collar crime, felony robbery, and other potential fraud-related intrusion methods as major risks to be managed.

We've compiled a list of how the current set of fraud principles can help organizations address modern challenges that require organizations to keep one foot in each world in order to address their unique risk.

PRINCIPLE

CHALLENGE

OPPORTUNITY

1 GOVERNANCE



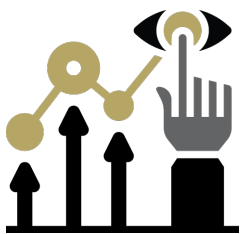
EMPLOYEE SCREENING

Continuous monitoring gives Human Resource professionals [real-time court records data](#), helping them make smarter hiring and personnel decisions while leaning on established governance and policy should the data reveal a dismissible offense.

DATA ANALYTICS

For High-Value Asset Handlers: In a 20-week study, researchers monitored 9,045 subjects, identifying 78 felony offenses and 177 non-felony jailable offenses. They were also alerted to 506 non-jailable offenses that would NOT have been reportable without continuous monitoring (but may have required attention by Human Resources per Governance policies).

2 ASSESSMENT



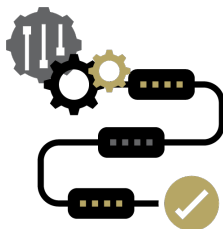
NETWORK SECURITY

From penetration tests and cloud back-ups to badge-only access and SOPs, a network and cybersecurity assessment will take into account, for example, all points of ingress and egress.

CYBERSECURITY

For High-Value Asset Handlers: Social engineering hacks often lead to fraud and are designed to put your first line of defense on its back foot. Whether executed by email, text, in-person, or via third party, the access points of your network – and all its Personal Identifiable Information – is a prime target.

3 CONTROLS



POLICY & PROCEDURE

While crypto is a digital asset, its storage and the owner's ability to transact the currency remains tied to the physical world (and therefore requires effective [operational controls](#)).

CRYPTOCURRENCY

For High-Value Asset Handlers: For businesses that offer courier services or that work in some capacity with crypto traders and custodians, any hot or cold storage, seed phrases, ledgers, and wallets should be treated like a high-value asset. Operational security is never convenient, but neither is losing a billion-dollar USB drive.

PRINCIPLE

CHALLENGE

OPPORTUNITY

4 INVESTIGATION & CORRECTIVE ACTION



COVID-19

For High-Value Asset Handlers: The pandemic saw [consumers using less cash](#) but holding onto it as a high-value asset. As such, financial institutions kept more on-hand. As all companies continue adjusting post-pandemic, now is a welcome time to expand the scope of SOPs and BCPs to include fraud as the result of biological or other global health emergency-related events.

INCIDENT RESPONSE MANAGEMENT

Businesses that survived the pandemic leaned into their SOPs and BCPs to manage contact tracing, lockdowns, and insurance-related issues like business interruption (and fraud).

5 MONITORING



REMOTE WORK

For High-Value Asset Handlers: Any business managing high-value assets that has a digital infrastructure [can train their remote workers](#) against ALL of the Top Four attack methods that can lead to fraud: phishing, spear phishing, executive whaling, and social engineering.

AWARENESS TRAINING

From CEO Fraud to ransomware to premises liability, awareness training gives remote workers the confidence to identify potential fraud and the business the ability to monitor their efficacy.



Brad Moody, CFI, CFE
EVP of Operations at
Lowers & Associates:

“Asset handlers can’t afford to be complacent or deviate from basic risk and fraud management principles. For every incident we’ve seen where an armed courier may have left a gun in a bathroom at a school or a bag of cash on the truck bumper, there’s an equal number of ‘trusted advisors’ that walk into a highly secure vault and empty it out to celebrate their 15th work anniversary. Knowing and understanding your employees, how to build effective controls and policies, and actively training to prevent and monitor fraud requires diligence born from experience and a willingness to admit you don’t know what you don’t know.”

BONUS: What to Expect - The Claims Investigation Process in 6 Steps (video)

Let's suppose the worst: your business read this eBook. It did everything it could to minimize fraud. Yet somehow, a bad actor managed to test and best your meticulous governance, assessed vulnerabilities, security controls, and BCPs. You recently filed a claim, and the insurance company is going to launch a claims investigation.

The emotions at play here will range from frustration and anger to uncertainty, exasperation and beyond. But while the specific nature of the investigation – and its emotional impact – will depend on the exact nature of the claim, investigators do tend to follow a predictable series of steps that your business can prepare for.

Watch the video below for a quick summary of the claim investigation process. Even on your worst day, you'll still be one step ahead.

PRO TIP

One thing to remember is that the insurance claim investigation process is an essential part of the insurance company's own unique risk management process. It's designed to prevent fraudulent or invalid claim payments. The best thing to do is be helpful, cooperative, and don't take it personal.

What to Expect:

The claims investigation process

In 6 Steps



0:08 / 1:59

ABOUT LOWERS & ASSOCIATES

Having a single point of contact – either in the form of a managed services agreement or simply knowing the right person to go to – creates efficiency and builds trust across the fraud prevention lifecycle.

As a global risk management consulting firm, Lowers & Associates provides a full range of solutions from assessment to mitigation to recovery. We design, implement, and provide ongoing support to businesses across a wide array of industries, both long- and/or short-term programs, that are created to address the organization's unique needs.

From fraudulent-claims investigations, regulatory compliance audits, and BCP evaluations to cybersecurity policy development, litigation support, and due diligence, our experts draw upon decades of experience and expertise to provide tailored solutions that reduce risk and improve the bottom line.

To quickly help mitigate fraud during the holidays, we offer the following services that can be scheduled, executed, and a report provided – on average – **within 7 business days to help your organization reduce its risk of fraud immediately:**

- 1. Schedule a Risk Assessment:** understand the risks to your business (externally and internally) and how much it could cost.
- 2. Arrange a Compliance Audit:** get deep insight into the behaviors and operational processes that keep you in compliance with your insurance policy.
- 3. Set up a Business Continuity Plan Evaluation:** build and maintain a foundation that keeps your business moving in the event of fraud, a cyber breach, natural disaster, and more.



**LOWERS
& ASSOCIATES**
International Risk Mitigation Partners

125 East Hirst Road, Suite 3C
Purcellville, VA 20132
tel: 540.338.7151