ONTIC

The Ultimate Guide to Building an Effective Insider Risk Program

Table of Contents

The growing need for insider risk management programs

You're likely well aware that insider risk is a growing problem — one that threatens your ability to keep people and assets safe. Because insider incidents come from people who have or had valid access to your systems, data, and facilities, it can be difficult to surface risk signals that indicate malicious intent or dangerous mistakes — and that's before we factor in cloud environments, remote work, and the increased use of AI.

If you're reading this guide, you might be among the 84% of organizations that don't consider themselves "extremely effective" in handling insider incidents. With disconnected insider risk solutions and programs, you're likely in full react mode instead of actively mitigating risks where you'd like to be.

Instead, you probably have several people working independently on managing pieces of insider risk — colleagues in HR, physical security, or cyber security. Known sources of risk, such as employee termination, may bring your HR and security teams together temporarily to revoke access. Still, it's very unlikely your security teams will get a heads-up to start tracking an employee for unusual behavior when that employee is put on a performance plan. Risk signals remain isolated, disconnected, or entirely unobserved. Preventative action comes too late.

There's also a good chance your teams use spreadsheets, emails, HR tools, access control systems, and other standalone tools to monitor and manage insider threats. You may have some sophisticated tools for identifying cyber risk, but what you lack is a system that connects all the signals, managing cyber risk alongside physical or personnel threats. You're likely operating without a program that helps build relationships across teams with the shared goal of building a risk-averse culture.

You're here because getting people to shift out of their lanes and begin collaborating is not straightforward. It's not always easy to gain support — or budget — for new technology. That's why we've put together this guide — to help walk you through how to start an insider risk management program, encourage collaboration across teams, and gain executive support. We'll cover:

- **Common mistakes that cause insider risk management programs to fail**
- **The baseline tools you should build into your insider risk management program**
- **The importance of having an Insider Risk Working Group**
- **How to foster a culture of risk aversion, not mistrust**

The current state of insider risk

Insider risk represents the potential for an insider — who has or once had authorized access to your organization's assets — to act in a way that could negatively harm the organization. While cyber incidents can have damaging financial and operational consequences, physical security incidents can also lead to catastrophic outcomes, including loss of production, infrastructure damage, and harm to personnel.

Examples of potential insiders, risk activity, and harm to your organization

INSIDERS

Current or former:

- Full-time employees
- Part-time employees
- Temporary employees
- Contractors
- Trusted business partners

ORGANIZATION'S ASSETS

- People
- Technology
- Information
- Facilities

MALICIOUS OR NON-MALICIOUS ACTIVITIES

- Fraud
- Theft of intellectual property
- Cyber sabotage
- Espionage
- Workplace violence
- Social engineering
- Data breach
- Accidental loss or disposal of equipment or documents

POTENTIAL HARM

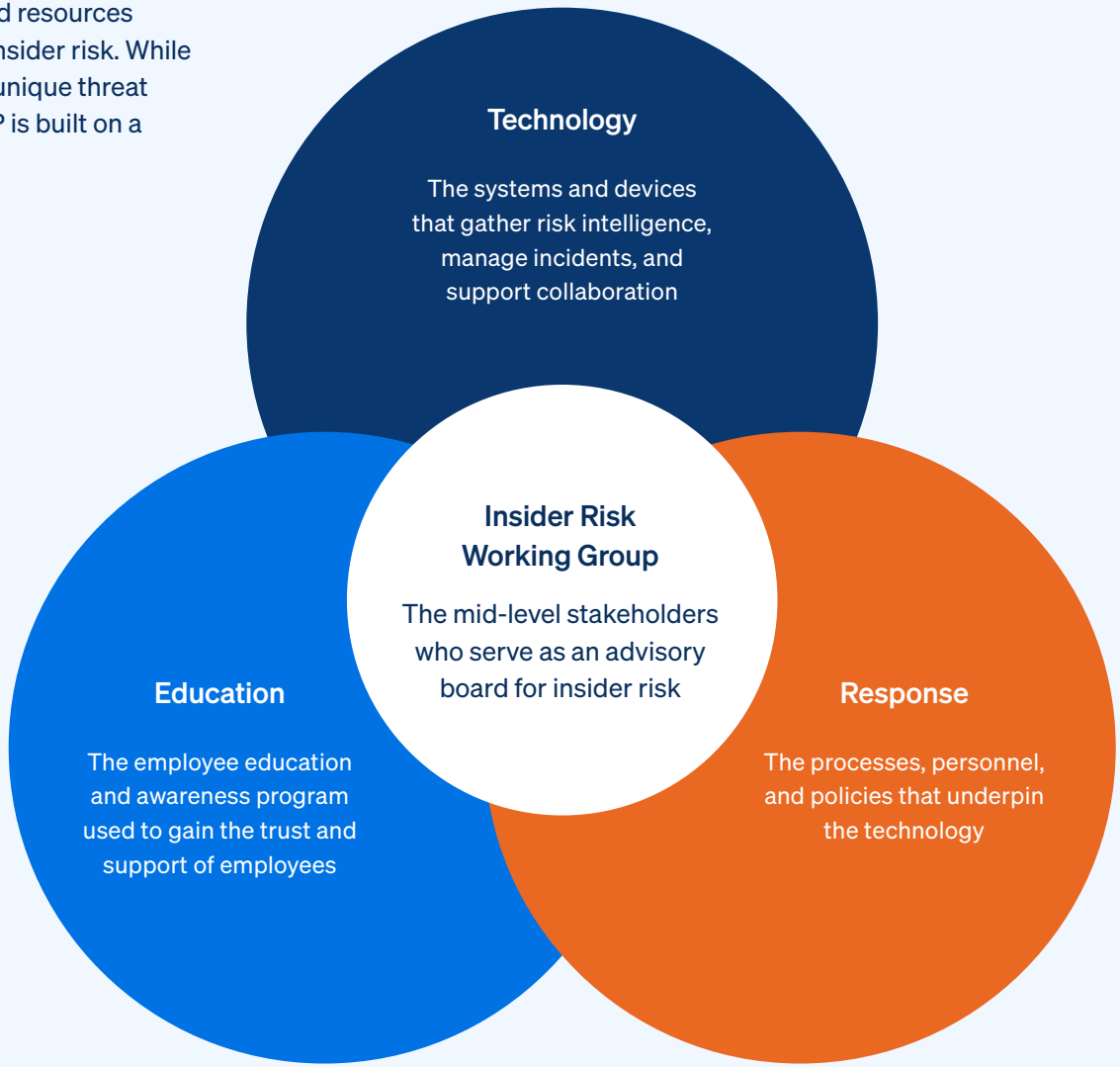
- Harm to organization's employees
- Loss of confidentiality, integrity, or availability of information and systems
- Disruption of organization's ability to meet its mission
- Damage to organization's reputation
- Harm to organization's customers
- Loss of production
- Damage to infrastructure

Insider events can often be linked with instances of concerning behavior or actions (like unusual credit card activity), but these signals are often viewed as unrelated events that might not need attention — only emerging as connected through retroactive analysis. However, if multiple signals are spotted, they can trigger further investigation and the opportunity to mitigate the threat.

If you're here, you understand the consequences of inaction and are ready to start an insider risk management program (IRMP).

The core elements of every insider risk management program

An IRMP is a designated set of people, processes, and resources designed to help monitor for, mitigate, and manage insider risk. While no two IRMPs are ever alike — reflecting a business' unique threat environment, risk appetite, and culture — every IRMP is built on a foundation of technology, education, and response.



A 9-step process to create an insider risk management program

Before you dive in, remember: **Think big, but start small.** The advice throughout this guide is comprehensive, covering each step needed to develop your program to an advanced level. However, the steps you choose to focus on will depend on your program's maturity.

If starting your program from scratch, focus on the first three steps to build the foundation. Then, revisit the remaining steps once your Insider Risk Working Group is established. Trying to tackle all the steps at once is the quickest path to losing your budget and momentum.

If your program is mature, you can use these steps as a benchmark or concentrate on steps eight and nine for enhancement.

Throughout this guide, we've also defined "baseline," "better," and "best" for several steps, recognizing that many of you are approaching this with different levels of program maturity.

> Every insider risk program is in a constant state of maturation and review based on the changing threat landscape.

01 Assess available resources

02 Identify stakeholders and establish an Insider Risk Working Group

03 Identify roles and responsibilities

04 Build out your alerting process

05 Build out your triage process

06 Build out your response process

07 Establish an ongoing education and awareness program

08 Report on the program

09 Mature the program

Establishing the foundation of your program

If you're building an insider risk program from the ground up, your first objective should be establishing a solid foundation: the triad of technology, education, and response overseen by a cross-sectional working group.

By assembling the right group of stakeholders, you can better identify the insider risks you face, more efficiently mitigate those risks, and compile metrics that support the value of your program.

01 Assess available resources

02 Identify stakeholders and establish an Insider Risk Working Group

03 Identify roles and responsibilities

04 Build out your alerting process

05 Build out your triage process

06 Build out your response process

07 Establish an ongoing education and awareness program

08 Report on the program

09 Mature the program

Assess available resources

You have established that your organization needs an IRMP, so you're already ahead of the game. Before making changes or investments, take stock of the policies, processes, controls, and tools already available in your organization to gather risk intelligence and manage incidents — there's a good chance you have more than you think.

Establishing your current capabilities will help you design a preliminary IRMP that can deliver results with a minimum investment.

Assess your insider risk capabilities

The exact policies and tools you use to manage insider risk will reflect your threat environment, risk tolerance, and culture. Although these capabilities will vary, most organizations find themselves at "baseline" with similar sets of capabilities.

The following chart represents the baseline capabilities you may have or should have to set up your IRMP and highlights the kinds of actions you will take to mature your program over time.

Maturity level	Policy and educational resources	Technology
Baseline Most security policies are written, but infrequently communicated or enforced. Baseline capabilities focus on information risk (cyber threats) and containment, rather than prevention.	• Acceptable use policy • Removable media policy • Data sharing policy • Data privacy policy • General security training	**Tools are siloed and may include:** • Cyber tools (data loss prevention, endpoint management, intrusion detection) • Access controls (password policies, MFA) • HR information systems (HRIS) • Visitor management system (VMS) • Research and monitoring tools
Better Capabilities are more sophisticated and education expands to cover a wider range of use cases.	• Policies expand to new use cases • Education is regular and targeted to specific use cases and groups	• Data sources are consolidated and centralized using modern case management
Best You have created a culture of trust where employees understand their critical role as part of preventing insider risk.	• Policies are holistic, reflecting all threat types • Education is built into every response activity as a learning opportunity	**Insider risk tools are sophisticated, targeted and connected, including:** • User entity behavior analytics (UEBA) • Tactical remote monitoring & management (RMM) • Sophisticated access controls (phishing-resistant MFA, Zero Trust)

Identify stakeholders and establish an insider risk working group

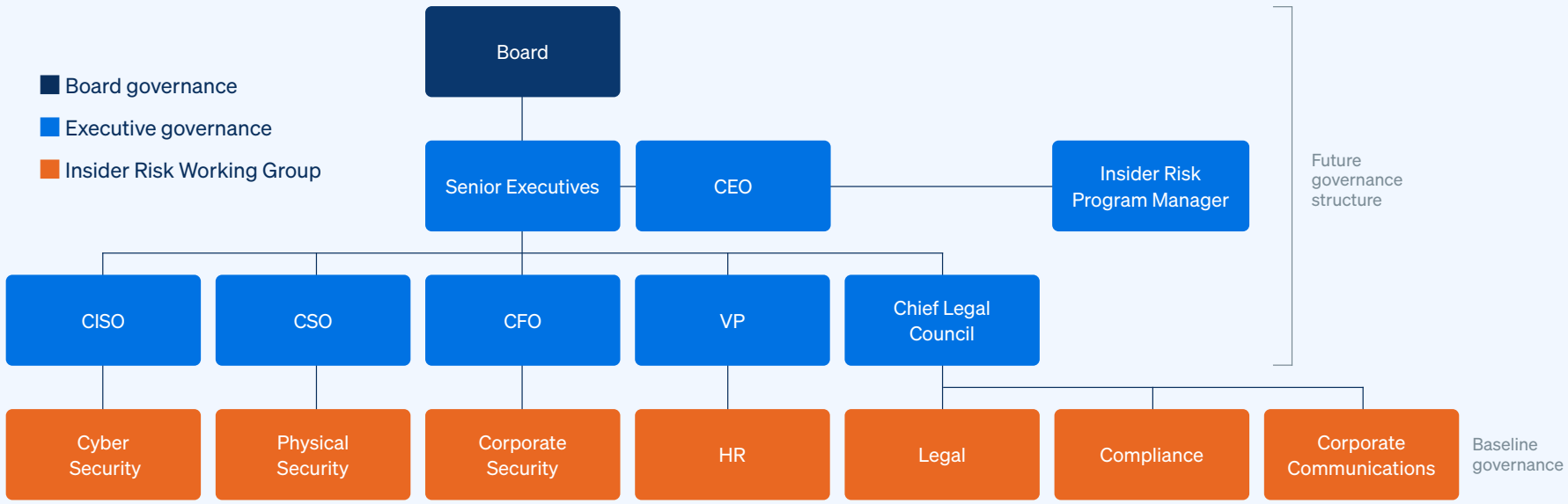
Once you've assessed your current resources and capabilities, connect with a senior executive, whether that's your CSO or your CISO, to ensure that your program aligns with their strategic vision for managing risk and security.

This senior executive will be your sponsor and champion for the program but will not be part of the day-to-day working group you'll establish to operate the IRMP.

With executive support, your next job is identifying stakeholders from across the organization who are already managing insider risk, usually at the director level. If you have a global organization, this should include stakeholders at the working level for each geographic region. These stakeholders will form your Insider Risk Working Group.

The most effective insider risk management programs bring together people from across the organization who work together to monitor for and manage insider risk.

Example governance structure for an Insider Risk Working Group



The insider risk program manager is responsible for the overall program strategy, with input from the Insider Risk Working Group. While the insider risk program manager is responsible for the program's day-to-day operations, issues are escalated to the Insider Risk Working Group when needed. Ideally, your group convenes regularly (like monthly) throughout the year to review and update the strategy, report on initiatives, review cases, and weigh in on the next steps.

While at this stage, it's not yet time to establish higher levels of governance (first, you have to demonstrate the value of your program), your IRMP will eventually incorporate regular presentations to executives and the board.

Build cross-departmental relationships

While the Insider Risk Working Group plays a critical role in overseeing the IRMP, the day-to-day management of risk falls to security teams. However, capturing the full picture of insider risk requires close alliances with HR, IT, legal, and other departments. Fostering these cross-departmental relationships can feel like an uphill battle, with teams laser-focused on their own goals.

But keep in mind that it's not that your cross-functional colleagues don't want to collaborate — in fact, most teams outside of security share your concern for insider risk — but their different objectives and priorities often make it difficult to come together and focus on the bigger picture.

Tip for success

While connecting with executive stakeholders is crucial, building relationships with operational stakeholders is just as important. Find and connect with the people who are going to do the work with you.

Breaking down those silos starts with something as simple as a face-to-face meeting to align on your shared objectives and risk concerns. It's important to attend these interactions with an open mind and willingness to understand each team's mandates and perspectives on risk. It's also important to take stock of what technology each team leverages on a day-to-day basis to get an understanding of where critical data might live.

Unlike other teams within the organization, you possess the training and knowledge necessary to understand the bigger picture of what information is required to prevent or investigate insider incidents effectively. Beyond establishing shared goals and information-sharing or reporting policies, you play a critical role in connecting people and teams to support ongoing communication.

Notes from the field

Let's say your corporate security team has been monitoring an employee ever since a formal complaint was logged about unusual and threatening behavior. When the corporate security team also noticed a concerning social media post by the employee, they notified the cyber security team to monitor network activity. This is already too late. Since the employee was on the corporate team's radar for a while, they should have also been on the cyber team's radar so that both teams could work in tandem to monitor behavior.

The importance of modern case management software

Although our goal at this time is to primarily rely on existing capabilities, innovative companies are investing early in modern case management software. End-to-end case management software can help your working group and security teams minimize data silos by connecting technology and people across functions with a central system of record. Just as importantly, this backbone will help produce the metrics you need to report on and grow your program.

Want to dive deeper?

Download *The Guide to Evaluating Case Management Solutions*

Download

Identify roles and responsibilities

For cross-functional collaboration to be effective, you must create joint policies and processes that help transform insider risk mitigation into an organization-wide responsibility — not just a security initiative. Establish guidelines for what risk signals to look for, how to report them, and to whom, and create boundaries that ensure employee privacy.

While communication and relationship-building are critical, the best programs leverage centralized case management systems everyone can access and contribute to. Centralized documentation leads to fewer blind spots, faster case resolution, better reporting, and effective litigation support.

Each of your IRMP stakeholders has existing day-to-day responsibilities, so it's vital to clearly define their specific roles in insider risk management. Clearly defined roles ensure that each stakeholder's contributions are aligned with their expertise, promoting a more unified approach to mitigating risks.

While the Insider Risk Working Group plays a critical role in helping proactively plan for and manage risk, true success is only possible when everyone in the organization embraces their role in mitigating insider risk.

Example roles and responsibilities

IRMP Leader

- Run meetings
- Know the status of all programs
- Ensure plans adhere to the long-term strategy
- Oversee insider risk education campaigns
- Report to executives and the board

Legal

- Ensure policies and technologies abide by state and federal regulations
- Determine if incidents are a legal matter or require outside experts
- Ensure proper handling and use of data

HR

- Incorporate insider risk into onboarding and offboarding
- Monitor for behavioral indicators
- Ensure investigations are compliant with HR policies
- Establish onboarding and offboarding procedures

Security Teams (Physical, Cyber)

- Establish systems and processes
- Monitor for threats
- Action investigations
- Keep logs of insider threat activity
- Contribute to case reviews

Building your program

Now that you have an IRMP in place, you can begin collaborating as a working group to connect the dots and respond to that risk activity. This will require you to establish processes for alerting, triage, and response — which we will cover in the next three steps.

01 Assess available resources

02 Identify stakeholders and establish an Insider Risk Working Group

03 Identify roles and responsibilities

04 Build out your alerting process

05 Build out your triage process

06 Build out your response process

07 Establish an ongoing education and awareness program

08 Report on the program

09 Mature the program

Build out your alerting process

Unsurprisingly, a key element of any IRMP is identifying and prioritizing which assets need protection (like protected data, intellectual property, credentials, systems, facilities, and people) and establishing situational awareness over those assets.

The Insider Risk Working Group should establish a set of pre-incident risk indicators: those early warning signs that an individual is behaving unusually. Security teams then play a critical role in codifying these risk indicators into cross-departmental policies and processes to enable teams to identify and take action on potential threats. Mature security teams that connect and integrate their data from various security functions — intelligence, investigations, security operations, executive protection — will likely be faster and more effective at identifying and substantiating threats.

★★★
BASELINE
Cybersecurity team receives alerts and sends to the insider risk team management

★★★★
BETTER
Alerts are sent to central triage location and risk scored prior to investigation

★★★★★
BEST
All available data sources are integrated into one technology to manage continual risk score and anomaly detection management

Not all signals indicate that an insider is a threat, but when you can see the bigger picture and connect the dots to identify a threat, it should quickly move to triage so that, when warranted, you can take action to prevent incidents from occurring altogether or mitigating their impact.

Pre-incident threat indicators and/or behaviors of concern may include:

Technical (automated alerts)

- Unusual network or data access
- Requesting access not required for role
- Accessing facilities at strange hours
- Accessing controlled areas
- Negative online commentary
- License plate recognition
- Fraud / intrusion / cyber threat alert
- High volume printing or data downloads
- Use of privileged credentials from remote locations or unusual workstations
- Unapproved changes to computer systems
- Unusual visitor requests or check-ins

Non-technical

- Employee grievances
- Negative feedback from review cycles
- Decreasing performance
- Employee put on a performance improvement plan (PIP)
- Lawsuits or law enforcement reports
- Pending termination or contract end
- Major life event or stressor
- Aggressive behavior
- Control issues
- Misuse of travel and expense funds
- Unexcused lateness or absences

Build out your triage process

With an alerting process in place, the next step is to build out your triage process, which is the steps you take to evaluate an incident and determine how to respond to it.

The process should include quickly capturing concerns, gathering data to substantiate the threat, setting a priority level based on your assessment, and notifying appropriate stakeholders for further inquiry and investigation. Assessment during this process is critical as it is where you get the necessary data to properly prioritize the matter.

Some alerts require immediate containment actions if the threat represents an immediate danger to people, facilities, systems, or data. However, the working group can leverage a threat assessment to assign a priority for non-urgent threats.

When a high-risk insider investigation is substantiated, the Insider Risk Working Group should be convened, briefed, and consulted regarding potential impact and actions.

Notes from the field

In many organizations, security teams (physical and cyber) are notified when an employee is terminated in order to revoke employee access to systems and facilities. This may already be too late if the employee was on a performance improvement plan (PIP). With connected systems or shared data integrations, security teams can be automatically notified if employees are on a PIP, allowing teams to keep an eye out for additional threat indicators.

The ideal path of a confirmed incident

Capture threat or incident

Assess the threat

Set priority

Notify Insider Risk Working Group or appropriate stakeholders

Build out your response process

When further inquiry or investigation is required, building out a standardized response process (appropriate to the threat level) is critical to scope, document, and resolve the incident. Your response process should include the tools you use to document, investigate, and collaborate on an incident as well as the steps of a response, including:

- Processes for gathering research on a person of interest (POI)
- Interview templates to ensure each touchpoint with a POI, witness, or manager is an opportunity for learning
- Triggers for when it's appropriate to notify internal and external stakeholders (like media) or law enforcement
- Processes that respect roles and responsibilities, ideally creating and assigning tasks to specific individuals
- Cross-departmental collaboration, including data-sharing protocols and shared visibility over common tasks (like behavioral monitoring)
- Templated interview strategies

While your IRMP aims to protect your organization, its assets, and its people from risk, how you manage insider risk is equally important. Everyone in the organization must realize that the goal of an insider risk program is not punitive action but to identify and resolve risk for the benefit of the person of interest, the organization, and every other individual in the organization.

To avoid interactions that feel punitive or judgmental, it is critical to establish a templated interview strategy for your response process that views the interview as a learning opportunity. This is a critical chance to provide corrective guidance, gain program supporters, and increase your pool of employee reporters — accelerating the maturity of your IRMP.

The goal of any interaction with a person of interest, witness, or manager is to leave the interviewee feeling valued, understanding that mistakes happen, and armed with information on how to do better.

"Even the best employees, when under stress, can make bad decisions or accidentally create a risk. Either way, our goal is to help them successfully resolve the issue so they can go back to what they do best — generating company revenue."

— **Tim Kirkham**, Senior Director and Global Head of Investigations and Insider Risk Management at Dell Technologies

How to Run Effective Insider Risk Investigations Checklist

For more detailed steps on what to do pre-incident, during incident intake, and throughout the investigation download our *How to Run Effective Insider Risk Investigations* checklist.

Download

Education, reporting, and growth

Your Insider Risk Working Group is established, and processes are in place. Now, it's time to focus on educating the rest of your organization about their critical role in mitigating insider risk. It's also essential to implement a reporting process for tracking the results of your efforts and to develop plans for continuously improving your program over time.

01 Assess available resources

02 Identify stakeholders and establish an Insider Risk Working Group

03 Identify roles and responsibilities

04 Build out your alerting process

05 Build out your triage process

06 Build out your response process

07 Establish an ongoing education and awareness program

08 Report on the program

09 Mature the program

Establish an ongoing education and awareness program

Chances are, your organization already has some form of HR and/or IT security which likely includes some insider risk training, like how to spot phishing attacks. This represents only a small slice of insider risk. Furthermore, it's not uncommon to see insider behaviors painted negatively, such as "you must not" or "if you do this, you will get fired," the result of which seeds distrust instead of awareness. Feeling untrusted or unvalued will only hinder employee reporting.

The people in your organization serve as the most effective guard against insider risks. When employees are trained to recognize potential indicators of insider threat behavior and are aware of the damage insiders can cause, they are more likely to modify their own risky behaviors and increase reporting to defend the company from a malicious act. However, there is a big jump between awareness of risk and ownership over managing risk.

Instead, to cultivate employees to understand their critical role in managing insider risk, employees must feel trusted, valued, and heard. Your executive leadership sets the tone, but up-leveling your HR and IT education and awareness programs can help employees believe in and support your program. To do so, programs should be targeted, interesting, adjustable across units, and infused with empathy, using language such as:

"We see the value of your hard work, and as fellow employees, understand your work is critical to the organization. OUR employment depends on that hard work."

"The goal of our program is to ensure the safekeeping of your work, keeping it out of the hands of those who would use it to undermine our success."

"For us to be effective, we need your expertise — nobody knows your work like you do, and nobody knows the daily operation of the business like you do."

"We can educate you regarding the risk to our people, property, and information, but without your insight and the benefit of what you see and do each day, our ability to be successful is limited."

"We are counting on you to help us understand what to protect, what areas of risk to focus on, and to educate us regarding events and actions that put your work or employees at risk."

"We know our company goes to great lengths to hire good people, but even good people make bad decisions under stress. Our goal is to prevent employees in that situation from damaging their careers or our organization. We can ensure our peers make good choices if we work together."

If you succeed in helping employees feel like valuable members of your insider risk program, you will see increased reporting, referrals, and service offering requests.

The employees you train will be a force multiplier who feel empowered to correct unsafe behavior, educate peers, and report suspicious activity — reducing the volume of unintentional insider activity and increasing reporting.

Finally, seek feedback on all aspects of your program — specifically, your employee awareness training. Continual evaluation, modernization, and change are a must. Fit your training to the business unit. Understand that training length, delivery, content, and tone must reflect the unit you're working with.

Tip for success

To foster trust in the program, we recommend being transparent with employees about the tools used to collect data or monitor behavior and establishing clearly defined policies for expected behavior. These policies will be incorporated into future education and awareness initiatives.

⚠ While we've listed this as "Step 7," establishing and executing an education and awareness program should be happening concurrently with the previous steps.

Report on the program

At this point, you have launched your IRMP and have been running it for several months. During this time, you've refined your processes, responses, and training to better meet the program's initial goals. However, the true lifeblood of your IRMP's long-term success lies in the metrics you track to demonstrate the impact of your efforts.

If you come from a government or law enforcement background, you might not immediately see the value of investing time and effort into tracking metrics. But in the corporate world, metrics are the only way to ensure continued investment in your program and team.

> The true lifeblood of your IRMP's long-term success lies in the metrics you track to demonstrate the impact of your efforts.

Where should you start? While you may be inclined to track metrics that reflect the volume of work, such as the number of investigations, these types of metrics have limited value in demonstrating your program's overall impact. Instead, consider what's most important to your business — what is being lost and how — to help guide what you measure and act upon. This alignment also shows leadership how security investments contribute to overall business success, fostering greater buy-in and resource allocation.

Metrics to support your insider risk management program

High value metrics Focused on specific threat types and mitigation efforts, ideal for reporting	Low value metrics Focused on performance, more useful within the Insider Risk Working Group
% of cases generated by technology alerts vs. employee reports	Number of signals captured
% of employees or executives who resign to a competitor and take assets or data with them	BOLO reports disseminate
# of substantiated investigations per business unit	Number of cases by type of insider risk (open, closed, all)
When data is moved, how is it moved? (USB? Cloud? Physical copies?) Note: These metrics are then used to drive more controls. Future iterations of the metrics will show how you reduced those numbers and types.	Number of insider risk cases before vs. after countermeasure

While the high-value metrics mentioned above are critical to your program and can certainly help illustrate risk, money talks. Great insider risk teams take it a step further by calculating the ROI of their program. How you do this will depend on your business goals, but it's essential to create a metric that assigns assumed dollar values to insider risk scenarios. Some examples include:

- **Direct cost savings:** Reduction of risk events that might directly lead to losses
- **Indirect cost savings:** Reduced insurance premiums, demonstrated diligence in the event of litigation, employee productivity
- **Ancillary benefits:** Customer loyalty and talent attraction and retention

Mature the program

After successfully reporting key results to executives, you will begin the cycle of maturing your program. Your Insider Risk Working Group will establish a new yearly plan, expanding to new use cases or geographic regions and filling gaps in detection and deterrence with new technology, policy, or education improvements.

Over the course of several years, you can expect to grow your program to maturity, a state in which you have the tools, people, processes, and policies in place to continue effectively reducing insider risks in your organization.

Insider risk management program maturity

The maturity of your IRMP can be visualized across three maturity levels, each of which looks at the three core pillars of an IRMP: technology, response, and education. Today, organizations spend 91.2% of their insider risk management budget on post-incident activities, putting most organizations at the baseline level.

Earlier in this guide, we established the capabilities you should have in place at baseline and during the evolution of your IRMP. Expressed another way, you can expect that as you evolve your capabilities, processes, and education programs, your IRMP will transform your organizational culture to become risk-aware, incrementally moving from reactive to proactive insider risk management activities.

Client spotlight

By integrating key data from their employee management system into Ontic, a leading healthcare company can now identify and address potential insider risk by monitoring signs of employee disengagement.

Before the integration, the security team had limited awareness of disengaged employees, relying on word-of-mouth and one-off emails from the human resources department. Without a reliable process in place, the counterintelligence team lacked information to detect early risk signals.

After working with partners in employee relations and legal to ensure privacy protections were in place for employees and build trust with the security team, the counterintelligence team gained access to employee information to monitor for threats, manage investigations and mitigate risks to the organization.

This healthcare organization now receives alerts when employees submit resignations or are placed on a PIP, allowing the security team to monitor for risk signals. With this integration, the team was alerted when a disengaged employee sent valuable information to a personal email, providing security with the opportunity to work with the employee to reclaim the information and prevent monetary harm to the organization.

Ontic: An end-to-end solution to manage insider risk

Ontic's Insider Risk solution helps organizations minimize data silos and connect technology and people across functions, including security, HR, and legal, for an effective insider risk program and central system of record.

With Ontic, teams can address the complex insider risk landscape using:

Integrated incident intake and triage

Access intake forms for internal tips, observations, complaints, and whistleblowers. Specific incident types reported via intake forms can automatically be escalated to an investigation.

Configurable investigation workflows

Leverage integrations with HR or IT systems to automatically trigger an investigation workflow assigned to the Insider Risk team when incidents occur.

Dynamic collaboration and activity timeline

Share investigations with partners in HR, cybersecurity, or other teams. Use activity timelines to allow multiple investigators to work an ongoing investigation.

Comprehensive analysis and reporting

Analyze and report on metrics like loss mitigation and policy violation. Build a database of all insider risk investigation results.

ONTIC

Request a demo to see Ontic in action

Schedule Now