STRIDER

How Your Organization's Insider Threat Program Compares

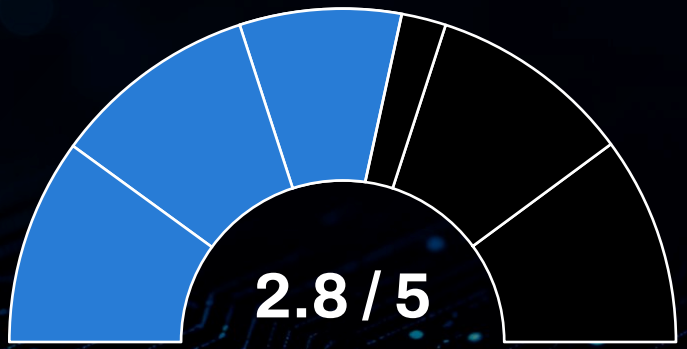
Benchmarking Against Strider's Insider Threat Program Maturity Assessment

SEPTEMBER 2026

Executive Summary

Between 2025 and 2026, Strider's insider risk experts on the Client Services team conducted proprietary Program Maturity Assessments (PMAs) for 41 insider risk and economic security programs across a range of global organizations. Each assessment evaluated a program against 13 categories spanning governance, policy, training, technical controls, and risk intelligence, benchmarking maturity on a 1-to-5 scale from ad hoc practices to optimized. This study offers a comprehensive view of how insider risk and economic security programs perform once measured against a consistent standard.

Overall Insider Threat Maturity Score



Across all categories and all 41 assessments, the overall maturity score averaged 2.8 out of 5. That places most organizations at a stage where processes are documented but not yet consistently monitored or measured. Eight of the 13 categories tracked carried an average score of 3.0, suggesting that this level of baseline maturity now looks standard across the field. Employee management, however, is an exception. Where other categories cluster tightly around that average, employee management showed the widest spread of scores in the dataset and the lowest average of any category, at 2.1, pointing to a persistent gap between security and human resources functions.

The most common challenges among organizations included:

- Training that stops at general cybersecurity awareness instead of recurring, role-specific instruction
- Weak coordination between HR and security across employee lifecycle events, most visible at offboarding
- Risk detection and risk intelligence functions that tend toward one extreme or the other: either largely absent or fully embedded in governance, with little middle ground

Organizations that excelled shared a few traits:

- Executive sponsorship paired with active, cross-functional governance
- Technical and detection systems that are monitored, measured, and mapped to specific risk indicators
- A dedicated risk intelligence function that extends well beyond cyber-only threat feeds

The sections below introduce and summarize the trends identified across the 41 completed assessments on file since 2025. Strider will continue tracking these trends as the assessment practice grows, working with organizations across sectors to benchmark maturity and close the gaps this study identifies.

Introduction

Insider threats are a persistent challenge for organizations around the world. They serve as a critical reminder for government, industry, and academia that some of the most harmful risks to an organization come from within.

An insider threat is a security risk posed by someone who already has some level of trusted access to company systems, data, intellectual property, or facilities. That person could be a full-time employee, a contractor, or a business partner. The common denominator is access that makes individuals capable of bypassing traditional perimeter defenses built to catch intruders.

The motivations behind that misuse vary widely. Some insiders act with clear intent, driven by financial gain, revenge, or loyalty to a competing organization or nation-state. In January 2026, for example, a federal jury convicted a former Google software engineer on seven counts of economic espionage and seven counts of trade secret theft after he transferred proprietary AI chip technology to outside parties while secretly working with PRC-based companies.

Others, however, can cause just as much damage unintentionally through a careless mistake that exposes information. But a growing share of insider threat cases involves neither malice nor negligence on the part of the insider, but rather manipulation: a foreign government or intelligence service identifying an employee with valuable access and building a relationship with the intent to exploit it.

This is what makes insider risk different from an external attack, and so much harder to build a defense against. A firewall is designed to notice something foreign showing up where it shouldn't. Insider risk asks an organization to notice something familiar behaving differently over time, making it much easier to miss.

Strider's insider risk experts created a proprietary Program Maturity Assessment (PMA) to help organizational leaders see where their own programs stand against this challenge. The findings below draw on the results of that work, tracing the patterns Strider's experts have observed across dozens of organizations navigating the same pressures, category by category, along with the practices that tend to separate strong programs from struggling ones.

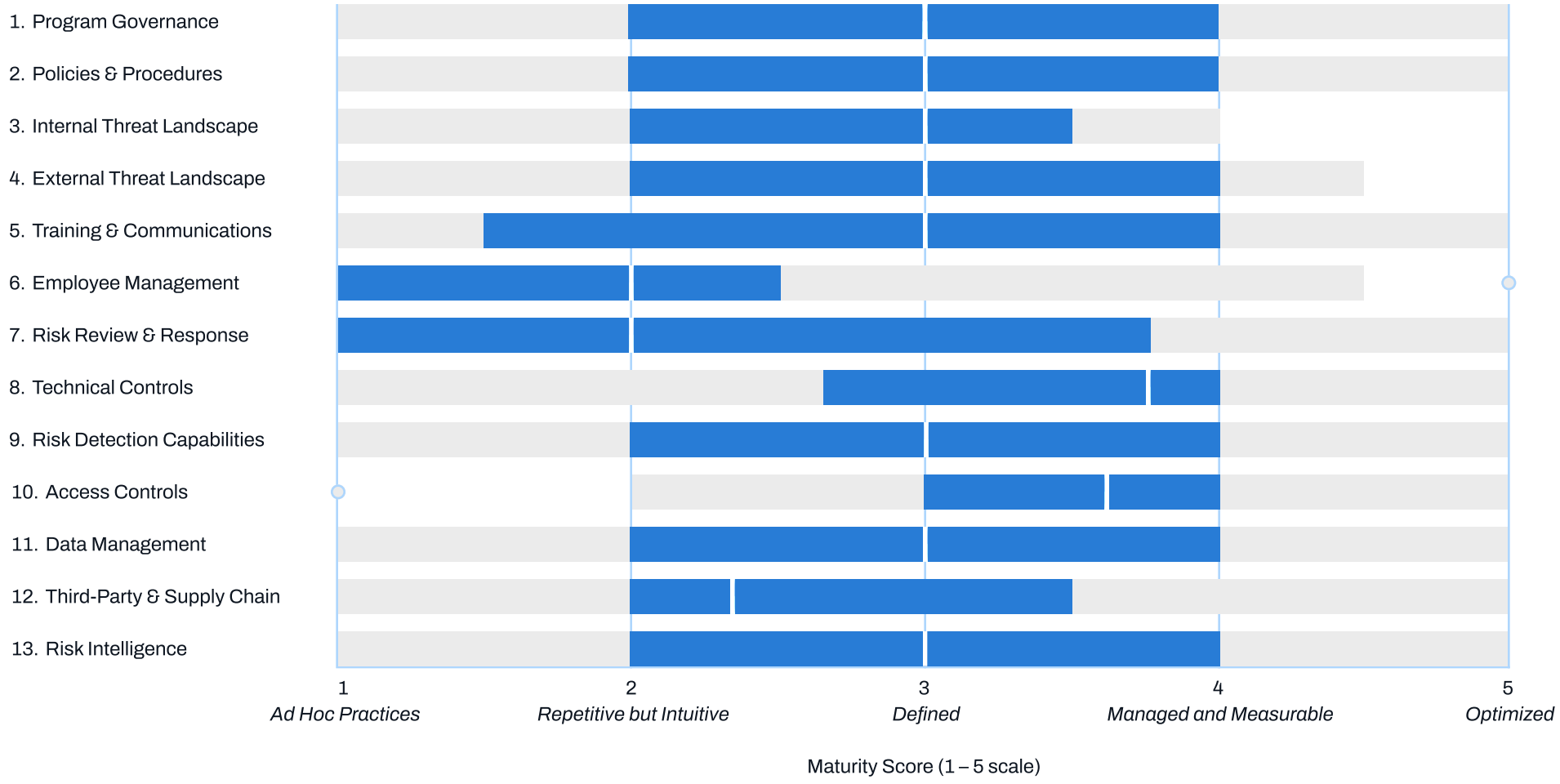
Strider Findings

Strider's insider risk experts conducted PMAs for 41 insider risk and economic security programs across a range of global organizations from 2025-2026.

Each assessment evaluated a program against 13 categories, benchmarking maturity on a 1-to-5 scale from ad hoc practices (1) to optimized ones (5). A score of 3 signifies that the category is defined, while a 2 is repetitive but intuitive, and a 4 signals the category is managed and measurable. Across all categories and all 41 assessments, the overall maturity score for an insider risk/economic security program averaged 2.8 out of 5.

Maturity Score Distribution by Category (2025 – 2026)

Blue bars show the middle 50% of scores, with the white line inside marking the median; the surrounding gray bars show the full range, and circles mark outliers.



Strider Findings Expanded by Category

1. Program Governance: 3.0 (Defined)

Scores in this category ranged from 1.0 to 5.0, with an average score of 3.0. Most organizations have identified a program owner and a governance structure, but formal charters and working-group cadence vary widely.

The highest-scoring organizations reflect an established, cross-functional governance structure with regular interdepartmental engagement. The lowest-scoring organizations have no formally rolled-out charter or governance cadence. Leadership transitions have also disrupted continuity in several programs, such as program ownership transitioning from the legal department to a newly hired Chief Security Officer.

2. Policies and Procedures: 3.0 (Defined)

Scores in this category ranged from 1.0 to 5.0, with an average score of 3.0. Policy frameworks exist in most organizations but are frequently borrowed from adjacent functions—such as cybersecurity or HR—rather than purpose-built for insider risk. Enforcement consistency across business units remains uneven.

The highest-scoring organizations reflect a dedicated, actively maintained policy set. The lowest-scoring organizations have no formal insider-risk policy in place. For example, one low-scoring organization has identified formalizing dedicated policy as a stated action item for its program manager.

3. Internal Threat Landscape: 2.8 (Defined)

Scores in this category ranged from 1.0 to 5.0, with an average score of 2.8. Awareness of internal risk is typically strongest among security leadership and staff with relevant backgrounds but rarely extends to the employees who directly handle sensitive data or technology.

The highest-scoring organizations show internal threat awareness reaching operational staff, not just leadership. The lowest-scoring organizations show awareness concentrated in a small security or leadership group. For example, one organization studied had former federal intelligence staff in senior leadership roles, but line employees handling at-risk data and technology had limited awareness.

4. External Threat Landscape: 2.8 (Defined)

Scores in this category ranged from 1.0 to 4.5, with an average score of 2.8. Recognition of geopolitical and nation-state threats is generally strong among security leadership but inconsistently shared with functions like Legal and HR that intersect with insider-risk decisions.

The highest-scoring organizations maintain structured external threat awareness through government or intelligence-community briefings. The lowest-scoring organizations show minimal external threat analysis outside the cyber domain. One organization (with a score of 2.0) illustrates this gap: Legal does not share leadership's understanding of the threat landscape and has resisted information-sharing tied to employee departures, even as the organization pursues partnerships with firms that have existing ties to the PRC.

2.7 / 5

5. Training and Communications: 2.7 (Repetitive but Intuitive – Defined)

Scores in this category ranged from 1.0 to 5.0, with an average score of 2.7. Training remains a practice-wide gap. Most programs deliver general onboarding coverage rather than recurring, role-based modules tied to insider-risk indicators.

The highest-scoring organizations deliver structured, recurring training distinct from general cybersecurity awareness. The lowest-scoring organizations show no measurable training cadence. For example, a low-scoring organization only delivers security training through HR onboarding.

2.1 / 5

6. Employee Management: 2.1 (Repetitive but Intuitive)

Nearly every score in this category ranged from 1.0 to 4.5, with an average score of 2.1. This is the lowest average score of any category and the one with the widest dispersion of scores across the full 41-assessment record. Pre-employment screening and behavioral monitoring vary by program, but the most consistent gap is offboarding: there is often no formal departure-communication protocol, and organizations frequently depend on self-reporting rather than dedicated insider-risk indicators.

The highest-scoring organizations show tight integration between HR and security across the full employee lifecycle. The lowest-scoring organizations have no formal offboarding process. In one example, a security team flagged a multi-day lag between an employee's departure and removal of their access.

2.5 / 5

7. Risk Review and Response Process: 2.5 (Repetitive but Intuitive – Defined)

Scores in this category ranged from 1.0 to 5.0, with an average score of 2.5. The most mature programs have shifted from reactive to proactive risk review, with documented thresholds and escalation paths. Other programs still respond only after an incident.

The highest-scoring organization (5.0) operates a custom case-management system supporting continuous, proactive review, while several others (scoring 4.5) maintain similarly formalized escalation paths. The lowest-scoring organizations have no risk review process in place at all. In each case where the organization scored a 1.0, the organization is waiting for a governance working group to convene before a review process can be defined.

3 / 5

9. Risk Detection Capabilities: 3.0 (Defined)

Scores in this category ranged from 1.0 to 5.0, with an average score of 3.0. Detection maturity tracks closely with technical controls maturity. Proactive, cross-functional detection combining multiple data streams is rare outside the most mature programs.

The highest-scoring organizations combine multiple detection streams with human review. The lowest-scoring organization has no insider-specific detection capability beyond existing cyber tooling. Other low-scoring programs, while in a similar position, are in the process of onboarding Strider data as a first step toward a dedicated capability.

3.3 / 5

8. Technical Controls: 3.3 (Defined – Managed and Measurable)

Scores in this category ranged from 1.0 to 5.0, with an average score of 3.3. Most organizations maintain a capable general cybersecurity stack, but tooling is frequently not tuned or correlated for insider-specific detection.

The highest-scoring organizations show technology investments explicitly aligned to insider-risk indicators. The lowest-scoring organizations lack meaningful technical tooling for insider risk specifically, while other low-scoring organizations rely on general cyber monitoring with no dedicated insider-focused correlation layer.

3.6 / 5

10. Access Controls: 3.6 (Defined – Managed and Measurable)

Nearly every score in this category ranged from 2.0 to 5.0, with an average score of 3.6. This is the highest average score of any category and the clearest evidence that physical and role-based access investments generalize across industries and company sizes.

The highest-scoring organizations apply least-privilege and badge-based controls consistently. The lowest-scoring organization reflects largely manual access processes and a lag between employee offboarding and access removal. Another low-scoring organization studied (2.0) is a case of active regression: badging and video systems at its new headquarters were disabled after failing to meet new government-contract security requirements, dropping the program from a prior Stage 3 to Stage 2 while a vendor reinstalls them.

2.9 / 5

11. Data Management: 2.9 (Defined)

Scores in this category ranged from 1.0 to 5.0, with an average score of 2.9. Mature organizations apply classification and labeling protocols with active enforcement, while others rely on informal, manager-driven discretion.

The highest-scoring organizations pair automated, content-aware labeling with consistent enforcement. The lowest-scoring organizations illustrate a common failure mode: document and email labeling exists but is optional and inconsistently used. In one case (scoring 1.5), recipients frequently cannot open labeled messages, which has driven employee pushback against the practice. Several organizations scoring 1.0 show the same underlying pattern.

2.7 / 5

12. Third-Party and Supply Chain Risk: 2.7 (Repetitive but Intuitive – Defined)

Scores in this category ranged from 1.0 to 5.0, with an average score of 2.7. This category remains a significant maturity gap across the organizations studied. Fourth-party visibility—the external vendors, cloud services, and subcontractors that an organization's third-party vendors rely on to operate—is a common shortfall, and most programs have not yet wired state-sponsored intelligence into their third-party risk workflows.

The highest-scoring organizations maintain dedicated supply-chain risk teams with active procurement and security collaboration. The lowest-scoring organizations have no defined third-party risk program yet. One program scoring 1.5 is representative of an obstacle facing defense-sector organizations: it is pursuing DoD contracts that require full supply-chain visibility but has no defined third-party risk program in place.

3.2 / 5

13. Risk Intelligence: 3.2 (Defined)

Scores in this category ranged from 1.0 to 5.0, with an average score of 3.2. This category is the starkest divide in the dataset. Mature organizations embed a dedicated intelligence function into governance and prioritization, while others have no formal capability at all.

The highest-scoring organizations each maintain structured, recurring intelligence products. One organization's product includes an annual strategic-intelligence report on external threats even though its broader program still lacks a formal risk-review process. The lowest-scoring organizations have no dedicated risk-intelligence capability. In one case, this responsibility currently falls to a single program owner with no formal program established.

13 Categories. One Clear Picture.

The foundations are there. The challenge is turning them into a connected, proactive program.

Recommendations

The findings above suggest that awareness of insider risk has become the norm across the field. Turning that awareness into a program built to catch these threats before they cause damage, however, is a separate task that many organizations still have ahead of them.

Closing the gap comes down to sustained attention across five areas that, together, define a resilient program: people and trust, education and awareness, technology and tools, evaluation and feedback, and proactive processes.

People and Trust

People are the heart of every company, and every insider risk program depends on a culture of trust built around them. Employees are the first line of defense, but only when they feel valued, supported, and responsible for the mission.

First, that means open communication, consistent leadership engagement, and strong ethics that empower employees to speak up. Second, it means reducing fear of retaliation and treating security as a shared goal. And third, it means creating an awareness loop in which employees with targeted subject matter expertise receive regular briefings about the tactics, techniques, and procedures used by nation-state actors.

These briefings could be derived from actual company examples, as well as events occurring across the industry, to both raise awareness and strengthen trust.

Education and Awareness

Education has to be continuous, relevant, and tailored to the roles and responsibilities of the workforce for awareness to be achieved. Strider recommends scenario-based training built around real-world cases, including insider activity linked to foreign adversaries, that surfaces behavioral red flags, potential coercion tactics, and ethical dilemmas before they escalate.

Training should also emphasize positive reinforcement, giving employees ownership of the outcome instead of a checklist to clear. Equipping employees to recognize and navigate potentially compromising relationships helps prevent state-sponsored actors from developing the access and leverage that can lead to insider risk.

Technology and Tools

Technology plays a critical role in preventing insider risk, but the findings above show most organizations run a general cybersecurity stack with little tuned for insider behavior. Modern programs need user activity monitoring, behavioral analytics, and anomaly detection, deployed transparently and in ways that respect privacy while enabling visibility into risk. It's the human-centric indicators, such as anomalous patterns, policy violations, foreign travel, or changes in behavior, that supply the context a tool alone can't.

Done right, these systems augment human judgment without eroding trust. A formal risk review process can bring the two together, giving the Insider Threat Working Group (ITWG) a consistent way to assess signals from existing tools and turn them into a comprehensive, repeatable, and defensible workflow.

Evaluation and Feedback

Threats evolve, and an insider risk or economic security program built and left alone can fall behind quickly. The findings above show which programs treat evaluation as ongoing: regular red teaming, structured risk assessments, and post-incident reviews that keep controls relevant.

Anonymous reporting tools, feedback surveys, and after-action debriefs give employees a voice at every level, helping organizations uncover potential blind spots. Annual PMAs and written after-action reporting provide a structured way to capture those lessons, identify areas for improvement, and strengthen the program over time.

Proactive Process

Being proactive is a common but rarely achieved goal of all insider risk programs. To be successful, an organization’s program must develop a deep understanding of both internal and external threat environments, so leaders can identify risks before they develop into established external relationships between employees and state actors. Understanding who is likely to be targeted by these actors allows for early detection and, more importantly, early engagement.

Strider Use Case

In early 2026, Strider conducted a Program Maturity Assessment (PMA) for a company whose security program was considered average for its tenure.

In response to the PMA findings, and in addition to an internal drive to become more proactive, the company identified a business unit responsible for a new development expected to provide the company with a strategic market advantage over the next decade.

Utilizing Strider's Insights product, the company's security team detected 400 business unit engineers who either had access to the relevant research or possessed expertise sought by the People's Republic of China (PRC). Strider advisors subsequently provided a series of awareness briefings to those engineers, alongside company executives.

To demonstrate the threat, the briefings addressed patents filed by a Chinese competitor that contained elements of the company's existing research. In doing so, the briefings increased awareness about state-sponsored interest in the engineers' work and the specific tactics, techniques, and procedures commonly used to approach them.

During the briefings, several employees shared experiences like those discussed—including being contacted while traveling in China and while attending professional conferences in the U.S.

As a result of Strider's PMA and the recommended awareness campaign:

- Multiple cases were identified in which employees had been invited to attend events that were funded by the PRC for the sole purpose of developing relationships that could later be leveraged to gain access to information. For those who attended, the security team conducted risk inquiries using Strider's People Search product and discovered they had been approached by known PRC talent recruiters.
- The HR department updated its travel policies to prevent employees from traveling to overseas conferences with company-issued cellphones or laptops.
- The business unit created a process in which employees interested in attending professional conferences or joining professional organizations could request a security team screening to ensure the organization or conference is safe and trustworthy.
- The Security Operations Center (SOC) developed additional protocols for monitoring data loss prevention (DLP) activity for the business unit and mitigated unauthorized efforts to exfiltrate sensitive data.
- Additional processes were developed by the company's procurement team to address third-party and supply chain risk management utilizing Strider's Organizations Search product. Specifically, they mapped a sector of their supply chain and discovered that a long-term partner had significant ties to the PRC. This relationship was significantly modified to reduce information sharing and the partner's access to sensitive materials.

> **Strider helped identify targeted expertise, employees at risk, and organizations with unforeseen ties to the PRC, empowering the company to develop enhanced security capabilities and maturity.**

Conclusion

Industry reports indicate that 60 to 80 percent of organizations experienced an insider threat in the past year. Meanwhile, nation-state actors continue to target aerospace, defense, biopharmaceutical, and semiconductor manufacturing with no sign of slowing down. And unlike an external hacker who must force their way in, insiders already have the advantage. They know the systems, the programs, and the weaknesses. A culture of vigilance and trust, backed by consistent training and the right tools, is how organizations take control.

Insider Threat Checklist

- ☑ Established, cross-functional governance structure with regular interdepartmental engagement.
- ☑ Maintains a dedicated, active insider risk policy framework.
- ☑ Internal threat awareness reaches operational staff, not just leadership.
- ☑ Maintains structured external threat awareness through government or intelligence-community briefings.
- ☑ Delivers structured, recurring training distinct from general cybersecurity awareness.
- ☑ Demonstrates tight integration between HR and security across the full employee lifecycle.
- ☑ Operates a custom insider risk case-management system supporting continuous, proactive review.
- ☑ Shows technology investments explicitly aligned to insider-risk indicators.
- ☑ Combines multiple insider risk detection streams with human review.
- ☑ Applies least-privilege and badge-based controls consistently.
- ☑ Pairs automated, content-aware labeling with consistent enforcement.
- ☑ Maintains dedicated supply-chain risk teams with active procurement and security collaboration.
- ☑ Produces structured, recurring insider risk intelligence products.


STRIDER
Thank You
striderintel.com