CyLab Carnegie Mellon University Security and Privacy Institute

Insider Risk Management Program Building: Summary of Insights from Practitioners

May 2021

Andrew P. Moore
Sarah Miller
Angela Horneman

Introduction

A survey of insider risk management practitioners illuminates the deep complexity of insider risk management and the broad range of *realized* insider threats faced by organizations across industry sectors.[1] Some decision makers may resist considering their employees as a potential threat. While it certainly makes sense to be sensitive regarding *how* to frame insider risk programs to best serve the organization, practitioner experience shows that simply ignoring insider risk is problematic. Nevertheless, the complexity and potential scope of the problem can be daunting to organizations. Practitioners recommend an incremental approach to navigate this complexity and practically deal with the insider risk scenarios that an organization considers important. In addition, a well-balanced insider risk program can become known as an *advocate* for employee well-being and a means for a more productive, engaged, connected, and committed workforce.

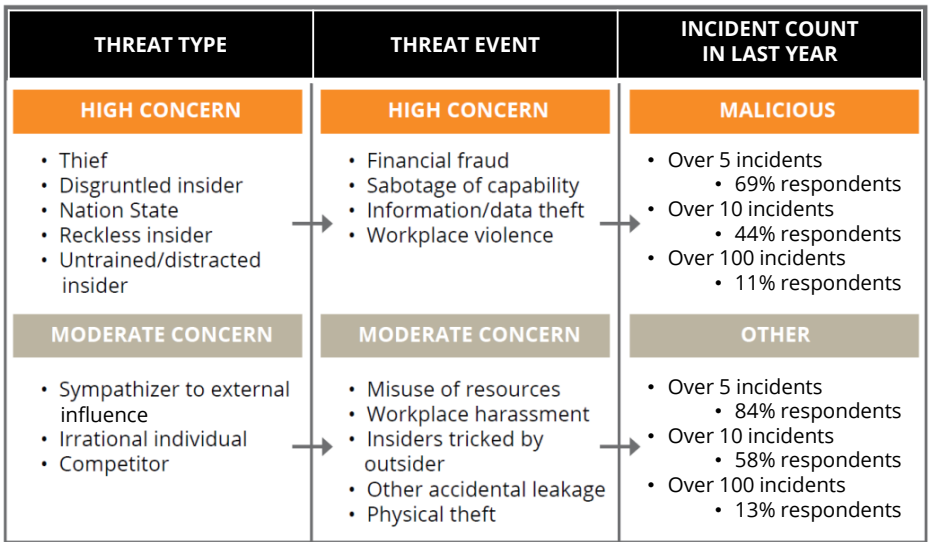
For the purposes of this study, insider risk to an organization is the potential for a person to use their authorized access to the organization's assets, either maliciously or unintentionally, in a way that negatively affects the organization. Access includes both physical and virtual (cyber) access; assets include information, processes, systems, and facilities. An insider risk program exists when an organization has staffing, policies, practices, and procedures in place to address any aspect of insider risk, such as prevention, detection, mitigation, or response. Organizations may use different terms for this, such as insider threat program or internal risk program, but for our purposes the idea is the same.

Using the collected survey data, this paper summarizes and contextualizes practitioner recommendations for organizations building their insider risk programs. We expect the results to be most useful for organizations at earlier stages of establishing or extending their insider risk management capability. This paper summarizes a longer version of the paper describing the research study's full report, "Insider Risk Management Program Building: Results from a Survey of Practitioners." [2]

1 The survey was conducted in January and February of 2021. Seventy-three individuals who responded to the survey were members of the Open Source Information Sharing Group (OSIT) and alumni of the CMU Heinz School Executive Education Program.

2 This work was funded by Carnegie Mellon University CyLab, with generous support from Microsoft. The authors gratefully thank Cylab, Microsoft, OSIT, and the Heinz alumni. For their help in survey design and paper review, the authors would also like to thank Dan Costa, Carrie Gardner, Bob Ditmore, Michael Theis, David Evans, Raman Kalyan, and Khetiwe Chitewere. The full report is available.

What Insider Threats are Practitioners Faced With?

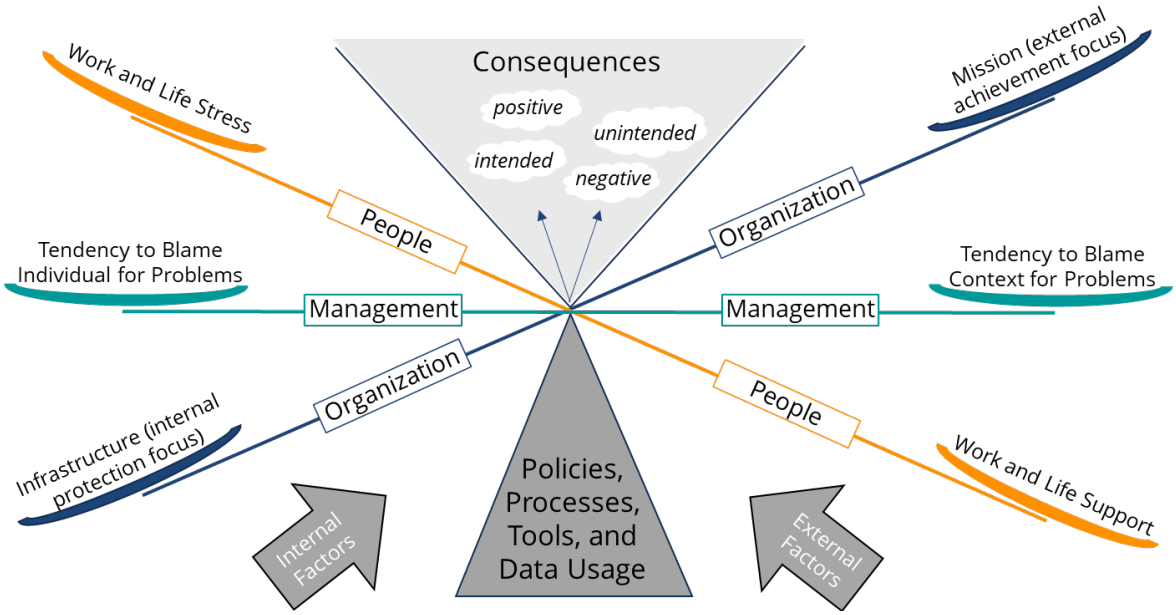


Survey respondents indicated broad consensus and high levels of concern for a wide range of different insider threats including both malicious acts involving disgruntled insiders or nation state actors, and unintentional threats involving reckless, untrained, or distracted actors. Although with less consensus among respondents, thieves and sympathizers to external influences were rated as a medium-high to high level of concern. Rated at a high level of concern were acts of insider financial fraud, sabotage, information/physical theft, and workplace violence. Less egregious and unintentional insider acts were rated of moderate concern as shown in the figure.

Respondents clearly indicated that many insider risks translate into quantifiable insider incidents. Organizational concern is justified by almost all respondents having experienced actual incidents over the last year, some in the hundreds of incidents. The detailed analysis shows that all of the event types were relevant for some organizations and all sectors were negatively affected. While it is true that larger organizations (in terms of workforce size) have a greater potential for insider incidents, it is noteworthy that some large organizations had fairly few incidents and some relatively small organizations had a large number of incidents in the last year.

Why is Insider Risk Management So Complex?

Insider risk is unique in the realm of organizational security and resilience in that the potential threat agents (the organization's trusted personnel) play fundamental roles in accomplishing the organization's mission. Insider goodwill is essential to both keeping intentional insider risk to a minimum and ensuring organizational success generally. Insider risk management activities in organizations typically focus almost exclusively on individual behaviors rather than also considering the context in which that behavior occurs. Established theory on employee-employer relationship shows that individuals reciprocate their experience of their employer's treatment of them, whether that treatment is perceived as good or bad. Fortunately, threat-conducive organizational behaviors can be prevented, detected, and responded to as a means to reduce risk, just as insider misbehaviors can. And as an organization's insider risk program becomes known as a source of advocacy for the workforce and a means for improving employee work life, organizations can expect a reduction of insider risk and the associated investigative costs.



The figure above depicts the complexity of the insider risk management problem, which involves people, management, and organizational dimensions. Employees must balance the work (professional) and life (personal) stress with the supports they have to reduce, or otherwise manage, that stress. Both personal and professional stressors are a common factor in turning otherwise committed and loyal employees into insider threats. While a well-known cognitive attribution bias documents the tendency of managers to blame workers, and for workers to blame their environment, for problems that arise, overcoming these tendencies is essential to effective program function.

In addition, although the organization has a mission to accomplish, exclusive focus on the mission while sacrificing necessary infrastructure is counterproductive in the longer term. One essential piece of the organizational infrastructure is a well-oriented insider risk program, but remediation of insider incidents can be more complex than for outsider incidents. The way that the organization handles insider risk and responds to employee concerns may be deeply engrained in its culture. However, an insider risk program can mitigate potential cultural issues by striking the right balance of policies, practices, and resources to support employees through work/life stressors, minimize attribution bias, and reasonably invest in organization infrastructure.

Insider risk management program policies, processes, tools, and data used to manage insider risk form the fulcrum by which balance can be promoted or undermined within an organization. Consequences arise as a result of the way an organization decides to manage its workforce. Consequences can be positive or negative, intended or unintended. Positive consequences are of course always desirable whether they are intended or not. Negative intended consequences can be thought of as realized risks that were understood and accepted as a part of doing business. Negative unintended consequences, on the other hand, are those that are most undesired, perhaps not understood or even identified, and thus possibly a surprise to the organization.

In addition, a diverse set of internal factors (such as an organizational culture that can promote insider disaffection) and external factors (such as industry competition that can promote insider theft) varies greatly from organization to organization. While this variation makes it impossible to find a one-size-fits-all solution to these complexities, there are principles that apply to organizations in general.

What Should the Focus be for Organizations Building their Program?

Institutionalization of insider risk programs within organizations is central to the program's success. Institutionalization, as commonly defined in organizational maturity models, requires following ingrained business practices routinely as part of its corporate culture. For insider risk programs, as shown in the center of the figure to the right, predominant advice includes ensuring that the executive support for the program is consistent and communicated, funding for the program is sufficient, benefits of and commitment to the insider risk program are understood across the organization through workforce training and awareness, and collaboration among the departments to share data takes place.

Respondents emphasized the need for incremental implementation, resisting "boiling the ocean" and promoting "start small, and build as you go" - an issue that will be explored in more depth later. In addition, many advise new organizations to leverage existing processes and resources where possible, presumably from other risk management and cybersecurity related activities. Respondents also commonly advised establishing risk tolerances of what the organization is willing to accept or not, and identifying and protecting the organization's "crown jewels."

Other advice by experienced insider risk practitioners is shown in the figure to the right, identified as a result of an open-ended question on the subject. *Predominant* advice includes those recommendations that were most commonly cited by respondents. *Frequent* advice includes recommendations cited by at least five different respondents. While advice identified as *Key* was cited less commonly by respondents, organizations establishing an insider risk program should consider that advice carefully. For example, a continuous improvement perspective suggests a culture of learning, whereby an organization learns and adapts to what works best for the organization and its employees based on experience gained through incremental advances.

PREDOMINANT ADVICE

- Obtain executive sponsorship and adequate funding*
- Stakeholder support, collaboration, data sharing*
- Workforce education to instill effective culture*

FREQUENT ADVICE

- Promote trust and transparency
- Choose good analytics with tool support
- Ensure access to quality data*
- Develop business case for program, tools, data
- Leverage existing processes/resources
- Build program incrementally
- Hire, retain, and train experienced program staff*
- Plan/scope program establishing insider risk tolerance*

KEY ADVICE

- Engage in continuous improvement activities
- Incorporate controls for trusted business partners
- Work within budget
- Ensure employee accountability
- Reference best practices and research
- Comply with applicable legal requirements*
- Understand privacy/legal risks and concerns*

* Advice that is also deemed by respondents as particularly challenging.

How Can I Incrementally Roll Out my Program?

The survey included a few questions to determine in what insider risk program implementation phase specific analytical tools, processes, and data sources would best be deployed. The phase options are *initial launch* - the first year of the program - and *full rollout* - about two to three years after program launch.

A majority felt that the focus of initial launch should include pre-employment screening, and monitoring and analysis of select user activity. While not the most common response, over a third of respondents indicated that analysis of employee complaints and grievances should also come at initial launch.

Of course, monitoring insider behaviors is an essential aspect of any insider risk program. Organizational data sources provide insight into insider behaviors but their integration into insider threat analytics can be complex. The variety of available data sources adds to this complexity. As shown in the figure below, respondents did distinguish among those data sources that would best be delayed until full rollout.

The figure shows the most common response regarding the best phase for use of the data source in the insider risk program. The data sources where at least three-quarters of the respondents identified the phase are indicated by an exclamation point ("!"). The data sources where at least one-third of the respondents identified the *other* phase are indicated by a tilde ("~"). Program managers can use the extent of agreement or lack thereof in making their own decisions regarding when to use particular data sources in their program rollout.

The following data source categories were considered in this survey:

- **Administrative:** Administrative data sources have to do with system privilege, account, asset, permission, and configuration data, which can give insight into abuses of insider access that may take place.
- **Communication:** Communication data sources involve insiders' communication with other individuals, printing/copying information, or other transfer of information between domains that may be unauthorized and/or part of insider compromise.
- **Network:** Network data sources involve the insider's use of computer system networks to access data, including data outside the organizational domain.
- **Personnel:** Personnel data sources include human resources records including background investigations, performance evaluations, and physical access.
- **Security:** Security data sources involve data related to system security or other organizational security issues such as conflict of interest or clearance investigation.
- **Violation Reporting:** Violation reporting data sources involve records associated with organizational violations or disciplinary actions, including anonymous reporting of such violations.

The majority of the data sources that were recommended for full rollout are those that would have a greater complexity of implementation than those identified for initial launch. The administrative data sources identified are those that are potentially more verbose in their output, or that might have a greater degree of latency. With the exception of the administrative data chosen for full rollout, the data sources identified are those that do not necessarily generate standardized logs or events for input to a tool; a greater degree of human interaction and manipulation is required to make the resulting data more suited to aggregation and correlation at scale. Taken together with behavioral science methods/tools being recommended for full rollout, it would seem that complexity of implementation is a deciding factor for respondent's recommendation to delay.

INITIAL LAUNCH

Administrative Data Sources

- Account creation data
- Active directory data!
- Asset management data~
- Authentication data~

Communication Data Sources

- Chat data~
- Data Loss Prevention (DLP) data!
- Email data!
- Printer / copier / scanner / fax data

Network Data Sources

- DNS data~
- Firewall data
- HTTP/SSL proxy data
- Network monitoring data
- VPN data

Personnel Records and Data Sources

- Background investigations
- Physical access records~

Security Data Sources

- Antivirus data~
- File access data~
- Intrusion detection / prevention data~
- Removal media manager data!
- User Activity Monitoring (UAM) data~
- Security clearance records~

Violation Reporting Data Sources

- Anonymous Reporting
- Acceptable Use Policy Violation Records~
- Intellectual Property Policy Violation Records~
- Physical Security Violation Records~

FULL ROLLOUT

Administrative Data Sources

- Configuration change data~
- Mobile Device Manager (MDM) data~
- Permission change monitor data~

Communication Data Sources

- Help Desk Ticket System data~
- Telephone records / data

Network Data Sources

- Network packet tags
- Wireless spectrum monitor data

Personnel Records and Data Sources

- Corporate credit card records
- Performance evaluations
- Personnel records~

Security Data Sources

- Application data
- Conflict of Interest (COI) reports~
- Foreign contacts reports~
- Travel reports~

Violation Reporting Data Sources

- Disciplinary Records~

! At least 3/4 of respondents so indicated.
~ At least 1/3 of respondents indicated otherwise.

What about More Advanced Processes?

The most common response for most of the processes asked about in the survey was to wait until full rollout, including the following:

- Applying behavioral science methods to identify indicators
- Applying multi-source data integration methods / advanced analytics
- Analyzing employee complaints/grievances~
- Analyzing threat intelligence from external sources
- Periodically re-investigating employees to assess risk over time
- Continuously evaluating employee behaviors to assess ongoing threat
- Regularly evaluating employee perception of working conditions

At least one-third of the respondents indicated that analysis of employee complaints/grievances should be done at initial launch (as indicated by the tilde).
The most common response for improvement processes, including the following, was to wait until full rollout:

- Conducting audits of the insider risk program
- Conducting operational exercises to evaluate defenses
- Testing the workforce's vulnerability to unintentional insider risk~
- Periodically analyzing privacy/regulatory requirements to ensure compliance~
- Analyzing performance metrics over time

At least one-third of the respondents thought that testing vulnerability to unintentional insider risk and periodically analyzing compliance to privacy/regulatory requirements should be done at initial launch. Again, program decision-makers can use this level of agreement in making their own decisions.

When Should I Integrate Available Tools?

Despite the slower rollout of many of the more complex processes and data sources, the most common responses indicated that four out of five of the tools questioned about be used in the initial launch: User Activity Monitoring (UAM), Data Loss Prevention (DLP), Security and Information Event Management (SIEM), and Incident Case Management (IM).[3] Although we cannot know the exact reason for this, presumably respondents consider these tools essential to program development and think that beginning to gain experience with them from the start is important. Available tools are usually built by different vendors and their integration can be quite challenging. It makes sense to start the journey of integration of tools with business processes and other technology early during initial launch when simpler insider risk management processes and data sources are the focus.

3 The format of the table used in this section is typical of the results tables in the full report, "Insider Risk Management Program Building: Results from a Survey of Practitioners," available by request to CyLab at Carnegie Mellon University.

Most respondents indicated that the deployment of User and Entity Behavioral Analysis (UBA/UEBA) tools should be delayed until full rollout. This is consistent with the previous process advice of leaving until full rollout the integration of behavioral science methods for identifying insider risk indicators. However, a third of the respondents thought UAM should be delayed until full rollout, and a third thought that UBA/UEBA be part of the initial launch, so there is not full agreement on the best approach. Interestingly, for the DLP and SIEM tools, respondents with extensive experience were twice as likely as less experienced respondents to indicate delaying deployment.

TOOL	INITIAL LAUNCH	FULL ROLLOUT
User Activity Monitoring (UAM)	✓	*
User and Entity Behavioral Analysis (UBA/UEBA)	*	✓
Data Loss Prevention (DLP)	✓	
Security and Information Event Management (SIEM)	✓	
Incident Case Management (IM)	✓	

Legend:	
✓	Most common rating
	At least 50% respondents
	At least 75% respondents
*	At least one-third (33.3%) respondents

What Can Go Wrong and How do I Adapt?

As mentioned, an imbalance of organizational policies and practices can add stress to employees' lives, both professionally and personally. The survey questioned the extent of concern associated with potential negative unintended consequences selected from previous research.[4] While there was not broad agreement about the extent of concern in the various categories of negative consequences, respondents most commonly rated negative consequences of insider risk controls as high for infringement of employee rights and civil liberties, as medium-high for inhibiting productivity, and medium for undermining trust in the workforce and reducing retention of good employees.

Recommendations for mitigating negative consequences included training and awareness, communication of program goals to employees, clear policies, alignment of and collaboration across stakeholders (e.g., Legal, HR, Privacy, Security, and Physical Security), privacy-informed governance and controls, business-informed access controls, program audit and oversight, evidence-based and confidential investigations, and

4 "Effective Insider Threat Programs: Understanding and Avoiding Potential Pitfalls," In SEI Digital Library, Pittsburgh, PA: Software Engineering Institute, 2015.

program performance management. The table below associates identified mitigations to the negative unintended consequences and identifies those mitigations with an asterisk that were most commonly identified.

NEGATIVE UNINTENDED CONSEQUENCES (prioritized ordering)	POTENTIAL MITIGATIONS (most common recommendations are starred)
Infringing on employee privacy rights and civil liberties	Evidence-based and confidential investigations* Privacy-informed governance and controls
Insider risk controls inhibiting productivity	Business-informed access controls
Undermining trust among employees and between employees and management	Training and awareness* Communication of program goals to employees* Clear policies*
Undermining goodwill of good employees	Training and awareness* Program audit and oversight Communication of program goals to employees*
Reducing retention of good employees	Program performance management
Investigations unfairly affecting employee careers	Evidence-based and confidential investigations*
Workplace becoming more confrontational	Communication of program goals to employees*

Contextualizing the Results

Public and private organizations building insider risk programs face a daunting array of people, organizational, and technological challenges that need to be met in order to position the organization to satisfy its mission with acceptable risk. Previous research found that workforce management practices that *damage* employees' Perceived Organizational Support (POS) correlate with *increased* intentional insider misbehaviors.[5] POS involves employee perceptions that their employer values their contributions, cares about their well-being, and treats them fairly. POS-based practices generally fall into the areas of organizational justice, rewards and recognition, organizational communication, and direct supervisor support. These practices promote the insider goodwill essential to both keeping insider risk to a minimum and ensuring organizational success generally.

Workforce management practices that bolster POS serve to improve employees' organizational commitment in a way that complements traditional security practices to provide a more holistic risk management balance. In general, we view supportive practices as creating positive attitudes in the workforce resulting in *positive deterrence* of insider threat. This contrasts with Deterrence Theory and criminology generally which is usually focused on what we would call *negative deterrence*, attempting to force rather than attract individuals to proper behavior. Supportive practices that align the workforce values and attitudes with the organization's objectives form a foundation on which to build security practices that rely on forcing functions. Of course, negative deterrence is always going to be needed since some insiders will act out no matter how supportive

5 "Balancing Organizational Incentives to Counter Insider Threat," IEEE WRIT, 2018.

the environment due to other factors, but a combination of positive and negative deterrence can improve the effectiveness and efficiency of the insider threat defense over negative deterrence alone.

Sustainable mission accomplishment is the primary objective of most organizations. Insider incidents have the often-realized potential to negatively affect an organization's mission. Most organizations' focus on reducing insider risk through a negative deterrence approach to harden systems, and detect and respond to suspicious behaviors. While such efforts are necessary, they should not significantly detract from positive deterrence efforts. The vast majority of insider incidents are perpetrated by individuals who started out in their organizations as committed and loyal employees. But as professional and/or personal stressors intervened, they found themselves motivated to act counter to their employer's interests.[6] Positive deterrence helps to align the organization and employee perspectives in a way that can reduce work and life stressors, and disincentivize insider misbehaviors.

A combination of positive and negative deterrence determines the balance of organizational policies and practices. Balance does not necessarily mean equal weighting of the two approaches. An appropriate balance depends on the nature of the subject organization. Organizations accustomed to top-down command and control (as in the military) may be perfectly fine with insider threat defense focused primarily on negative deterrence. Organizations that rely on highly skilled workers that are in short supply in a competitive domain may require a balance more weighted on the positive deterrence side.

Many of the negative unintended consequences of high concern to survey respondents arise from negative deterrence approaches. This is where POS can pay big dividends; managers who express positive value for their employees' contributions, demonstrate care for their well-being, and treat them fairly will help employees manage their work and life stress. Empathic managers that support employees through difficult times, both personally and professional, can help. Within the insider risk program, investigators that look for both confirming and disconfirming evidence of wrongdoing can reduce the negative impacts of false positives identified using available technology. Attribution bias can be difficult to overcome, but organizational training and supportive policies and practices can help to achieve a good balance and sustain the mission in the long term.

6 "Application of the Critical-Path Method to Evaluate Insider Risks," Studies in Intelligence, Vol. 59, No. 2, June 2015.

Conclusion

Public and private organizations building insider risk programs face a daunting array of people, organizational, and technological challenges that need to be met in order to position the organization to satisfy its mission sustainably. The results from the survey described in this report illustrate the broad range of realized insider threats that organizations face. Core challenges that an organization must overcome have primarily to do with institutionalization of the program – gaining executive support, sufficient funding, and collaboration across the organization for key insider threat detection and risk mitigation activities, especially cross-departmental data sharing. Management needs to find the right balance of holding people accountable for their actions while recognizing when the workplace context (including culture, policies, and practices) have the potential to exacerbate the threat. The survey results identified negative unintended consequences of high concern to program managers and ways of mitigating those consequences operationally.

The survey results should help organizations understand and overcome challenges associated with building insider risk programs in part through incremental rollout of the program. Survey respondents emphasized initial focus on 1) pre-employment screening to ensure congruence of individual and organizational expectations and values and 2) monitoring and analysis of select user activity. They recommended waiting until two to three years after launch to consider more advanced behavioral science and analytics, as well as process improvement activities overall. Recommendations on the inclusion of data sources in program rollout reflects this incremental approach leaving those data sources that have greater implementation complexity for after program launch. A gradual rollout of insider risk management policies, practices, and technologies helps to give time for the organization to gain the experience necessary to fine-tune its approach going forward. With a balance of positive and negative deterrence that is right for the organization, the insider risk program can become known as an advocate of employee well-being and a means for improving employee productivity, engagement, connection, and commitment for the benefit of both the employee and the organization overall.