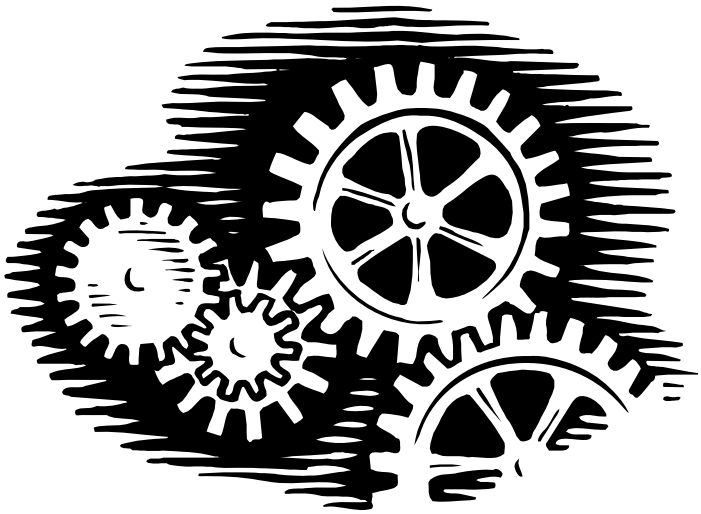
PERSEREC

Insider Risk Evaluation and Audit Tool

PP 09-03



August 2009

Defense Personnel Security Research Center
99 Pacific Street, Suite 455-E
Monterey, CA 93940-2497

This Page is Intentionally Left Blank

Contents

List of Tables

List of Figures

This Page is Intentionally Left Blank

Evaluation and Audit Tool Overview

This tool is designed to help the user gauge an organization's relative vulnerability to insider threats. Its organization into six categories of internal preventative or mitigating management activities and the selection of evaluation and audit questions in each category is based on the authors' distillation of empirical analysis from a relatively large number of insider cases, academic research, and organizational consultations on insider challenges. These research findings are discussed in a PERSEREC technical report, *Insider Risk Evaluation and Audit*, by E.D. Shaw, L.F. Fischer and A.E. Rose, TR 09-02, August 2009, Monterey CA: Defense Personnel Security Research Center. This report can be downloaded from the PERSEREC website, http://www.dhra.mil/perserec.

The six internal functional areas for risk mitigation in which organizational management can proactively play a decisive role in minimizing adverse insider behavior are:

- Policies and Practices
- Recruitment Methods
- Preemployment Screening
- Effective Training and Education
- Continuing Evaluation and Policy Implementation
- Management Intervention

In each of these areas, as seen in the tables that follow, the authors provide a set of self-audit and evaluation questions that point to specific best practices. The authors do not intend to imply that all best practices and suggested safeguards are appropriate for all organizations and situations. These are offered as an inventory of ideas and suggestions on which to draw to assess the overall risk of the organization, address specific issues confronted by management, or to develop a tailored risk mitigation strategy as determined by the nature of the organization. Also to be considered in the assessment of organizational risk are the social and regional context in which the organization functions, its mission, and its vulnerability to external threats. An organization's environment and reputation can have a significant impact on the magnitude or intensity of its insider risk.

For this reason, the risk assessment tool attempts to incorporate several rough measures of contextual risk indicators into its evaluation scheme. The first section of the tool (and the first table) focuses on organizational context—cultural, political, economic, sector-specific, and organization-specific sources of risk. These can be seen as stress factors faced by an organization that can magnify the probability of risk. For example, a sudden downturn in the national economy, in which jobs in the organization are threatened, may accentuate the need for the monitoring of online behaviors. Given a perception of the current risk level, the user of this tool may then proceed to the internal organizational evaluation questions.

One of the conclusions of this case study analysis was that an organization's ability to mitigate insider threats is synergistic across many of its personnel and technical management capabilities. Mitigating strategies can be complementary or reinforcing or, on the other hand, compensatory; in case one type of measure is not practical, another can address the risk. Organizations that employ effective recruitment, screening, and training and education methods and perform continuing evaluations of employees—especially after behaviors indicative of insider risk are observed—are better positioned to mitigate insider risk. In addition, organizations that effectively communicate, monitor, and enforce their insider-related policies also are more likely to prevent, detect, deter, and manage insider risk effectively.

Furthermore, the absence of mitigating measures diminished an organization's ability to reduce insider risk and actually exacerbated the risk when preliminary violations went unchecked. In many of the case studies, the affected organization's uninformed and/or precipitous interventions escalated insider risk. The manner in which all of these measures work together to reduce insider risk is discussed in the technical report cited above.

The assessment tool takes the user through the seven organizational components displayed below in Figure 1. First, users are asked to assess the insider risk their organization may face due to contextual factors. The more significant these contextual stresses, the greater the pressure on internal organizational mechanisms for risk reduction. As mentioned above, contextual factors in our assessment scheme act as force multipliers. The greater these contextual pressures, the more the insider risk.

Next the user is asked to focus on the organization's current policies and management practices and to determine the presence or absence, and in some cases the effectiveness of, mitigating factors in six internal functional areas. Figure 1 presents these areas within the context of an employment life-cycle. Following preemployment screening, an employee passes through two phases: Socialization and Continuing Evaluation, which encompass the remaining four areas of management involvement (or opportunities for management intervention) before the employee leaves the organization.

In general, the closer an organization comes to its optimal configuration of internal organizational mechanisms for risk prevention, deterrence, detection and management, the less insider risk there is to the organization. But there is no easy calculus to determine just what that optimal configuration is. It will be influenced by organizational characteristics and environmental factors, but in one way or another should cover the full range of management activities: recruitment processes, screening practices, employee socialization through training and the effective communication of policies and practices, and planning for employee intervention when required.

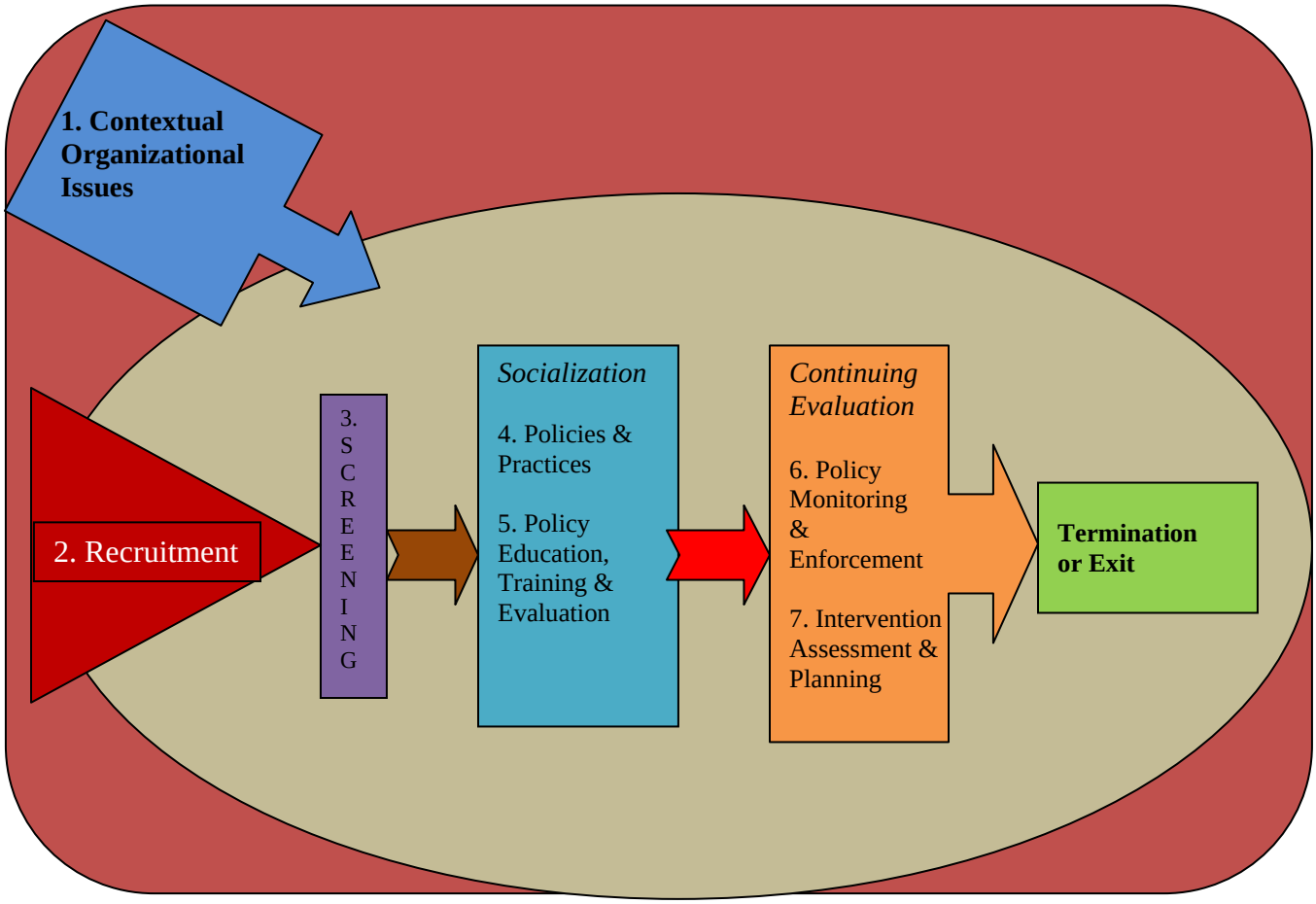


Figure 1 Overview of Assessment Tool Components

Contextual Organizational Issues

Table 1 below contains the five different contextual issues described in the report that can directly and indirectly contribute to insider risk. Any of these, to one degree or another, may apply to your organization.

For example, the two types of cultural risks identified in Table 1 concern cultural diversity within the corporate structure or even the organization's workforce that includes differences in values and beliefs among employees and how they affect (1) potential loyalty to the organization and (2) communication regarding behaviors associated with loyalty and security. Unlike in the West, in some societies, loyalty to the employer—especially an outside employer—may be secondary to loyalty to the family, nation, political party, religious or ethnic group. Conventional Western cultural expectations regarding loyalty, sacrifice and dedication to the organization above other parties may not apply in this environment. Cultural difficulties with communication on these issues may further interfere with effective insider security. In a multinational setting, it may be difficult to effectively communicate expectations for security-related behaviors, to determine whether these expectations are understood, and to gauge their acceptance and compliance. On a more basic level, cultural differences can have profound effects on the most basic communication between supervisors and employees and among coworkers. These cultural contrasts can increase the risk of disgruntlement and insider episodes.

Table 1
Contextual Organizational Risk Issues

Type of Risk	*Factors that May Magnify Insider Risk*
Cultural	Does your organization have branches, suppliers, subcontractors or other affiliates abroad where differences in cultural beliefs and values may affect loyalty to the organization versus other local groups? Does your organization have branches, suppliers, subcontractors or other affiliates abroad where differences in language, cultural beliefs and values can complicate communication and lead to conflicts?
Political	Does your organization have branches, employees, suppliers, subcontractors or other affiliates with access to your resources or information in areas where there is intensive social, political or military conflict that may result in increased insider risk?
General economic	Is your organization currently suffering from general economic forces that place unusual financial stress on employees? Is your organization currently impacted by economic or financial stresses that impact its treatment of employees in a manner that could increase insider risk such as, reduced benefits, stock options, retirement contributions or other incentives for loyalty?
Sector-specific	Is your organization affected by specific sector stresses that place economic or competitive pressures on employees?
Organization-specific	Is there anything about your organization's function, affiliation, reputation, competitive environment, adversaries or other characteristics that would increase pressures on employees, resulting in greater insider risk?

Policies and Practices to Mitigate Insider Risk

Table 2 moves from external contextual factors to a checklist of specific internal policy and practice areas that should be covered within an organization's basic governance structure. Not all policy areas may apply to an organization. However, it is not enough to have excellent policies on the books; employees must be informed of their meaning and how they may affect their working relationships and behaviors. Policy and practice guidelines must be clearly documented and easily accessible to employees and be the subject of education and training programs.

Table 2
Policy and Practice

Audit Questions
Does your organization have policies facilitating preemployment screening?
• Information gathered to evaluate suitability of job candidates
Does your organization have policies that protect the security of organizational information and IT resources in the following areas?
• Job descriptions and employee contracts include descriptions of information security responsibilities including implementing and maintaining policies, and protecting organizational assets scaled for each employee position • Email, network, website and databases • Incident management recovery • Access controls and change management, configuration control, logging, auditing, monitoring • Routine probationary monitoring of new users • Specialized monitoring of system administrators and other "super users" • Addressing the risks and consequences of inadvertent damage or losses, including records of these losses
Does your organization have policies that allow for an employment probationary period with increased monitoring for new hires?
• New hires are monitored closely for insider security risks during an initial period of performance ▪ Closely examine technical and interpersonal behaviors for a probationary period
Does your organization have policies protecting the physical security of facilities?
• Facility access and egress of persons, information and property
Does your organization have policies that limit employee use of property for nonwork reasons and establish boundaries between personal and professional activities that utilize work time and resources?
• Rules governing employee and others access to, use, distribution of organization assets and personal activities on work time (surfing the web, personal appointments, etc.).
Does your organization have clearly defined policies regarding the ownership and sharing of organization intellectual property?
• Rules describing organization and employee rights to intellectual property • Procedures for answering questions regarding ownership and benefits from IP • Contingencies for rule violations
Does your organization have policies and practices for disaster recovery that may deter insider actions?
Does your organization have policies regarding outside business involvements and contacts and the reporting of these contacts?
• Rules governing permissible employee business or consulting relationships and information sharing • Procedures for reporting relationships, resolving ambiguities, and contingencies for rule violations • Agreements covering disclosure of information, competition after leaving the organization, operation of

Audit Questions
side businesses, etc.
Does your organization have policies that define the privacy of employee, customer, client and other sensitive personal information?
• Rules governing the protection and permissible release of employee, customer, client information, especially sensitive personal information • Organizational rules for the implementation of relevant state and federal privacy mandates such as HIPAA, Sarbannes-Oxley (Sox), other regulations regarding possible violations of privacy protections
Does your organization have guidelines describing the organization's right to monitor and audit employee activity on proprietary systems as well as their online interpersonal behavior?
• Rules and procedures are established, described and acknowledged by employees as a condition of employment or access to resources such that there are no legal impediments to monitoring or resulting consequences • Intensified monitoring of individuals when violations or other risky actions indicate the need for more effective monitoring • Means available to collect and record adversary efforts to recruit or compromise employees • Intensified monitoring of individuals with mental health, alcohol, substance abuse or other personal problems who are and are not in treatment for these concerns
Does your organization have policies describing how employees report grievances and their own and others' risk behaviors?
• For employees to report grievances, problems and concerns about themselves and others and for investigating and reacting to these reports in a manner that promotes social justice within the organization ▪ Protections against false reports, retaliation for reports, penalties for nonreporting of serious security issues
Does your organization have policies describing unacceptable workplace interpersonal behaviors?
• Guidelines exist covering illegal and disruptive interpersonal behaviors, reporting these behaviors and resulting contingencies for investigating and reacting to these reports covering: ▪ Violence and threats ▪ Sexual harassment ▪ Online behavior ▪ Equal Employment Opportunity rules ▪ Attendance ▪ Vacation and leave ▪ Drug and alcohol use ▪ Weapons ▪ Dress and hygiene ▪ Fraternization and relationships at work ▪ Interpersonal respect ▪ Conflict resolution, etc.
Does your organization have policies describing how to identify and respond to employees specifically at-risk for insider acts?
• Guidelines for recognizing and addressing signs or symptoms that an employee is: ▪ Experiencing stress ▪ Engaged in interpersonal conflict ▪ Guilty of technical violations ▪ Susceptible to social engineering or involved with dangerous outsiders ▪ Other signs that he may be at risk for insider violations
Does your organization have policies and practices designed to improve loyalty and reduce the risk of insider activity?
• Stock options • Rewards for periods without security violations • Rewards for ideas to improve security

Audit Questions
Does your organization have clear policies describing how employee benefits and compensation are obtained and changed?
• For benefits and pay • Criteria and procedures for changes in pay and benefits are fair and clear and uniformly followed
Does your organization have clear policies describing how employee evaluation and advancement are accomplished?
• The manner in which employee performance is evaluated and related to pay, promotion, privileges, benefits, and consequences, etc. are clearly described
Does your organization have clear procedures describing access to and benefits of employee assistance programs and other employee support services?
• Services, policies and procedures to assist employees and their families with personal, psychological, financial, legal and other stressors which have been related to insider risk are in place and accessible to employees, including provisions for privacy, voluntary and involuntary referral and referrals by others
Does your organization have a good conduct policy?
• Employees may be terminated for legal violations or behavior that damages the reputation of the organization
Do your organizational policies and practices extend to trusted partners?
• These important policies and practices related to insider risk are applied in appropriate or parallel form to all personnel working with the organization, including contractors, subcontractors, temporary employees, clients and customers who utilize shared resources, etc.
Does your organization have policies and practices mandating security awareness training?
• Training tailored for the specific risks and adversaries faced by your organization

Recruitment Issues Influencing Insider Risk

Table 3 examines the potential for insider risk from recruitment policies that encourage the use of placement groups and employee bounties and encourage referrals from the family and social networks of current employees. Many organizations utilize some or all of these recruitment channels and (with the exception of the use of unscreened or poorly screened employees recruited through placement groups or bounties) can argue for their utility. In fact, many personnel and security officers prefer employees recruited from personal referrals, including social networking sites. However, in our case data involving insider incidents, the personal or family connection between the employees often biased the manner in which a hired employee was managed and often led to at-risk behaviors being ignored, underreported or inadequately sanctioned. In general, there was a risk of such employees being granted exceptions to policies and practices to the detriment of the organization. In addition, difficulties in managing these employees when they did display at-risk behaviors were exacerbated by their personal relationships with more senior employees. In several cases where there was significant family or social network hiring, the resulting subgroup of employees actually conspired against management with significant negative results for the company.

Table 3
Recruitment Methods

Audit Questions
Does your organization utilize the services of head hunters, recruitment firms or other placement groups?
• To what extent do you rely on these service providers to screen candidates for risk factors associated with insider violations?
• To what extent do you validate or supplement screening conducted by these providers?
• What is the attrition of employees recruited in this manner compared to those recruited by other means?
• Have employees recruited in this manner been implicated in policy or legal violations or other insider acts?
Does your organization encourage employees to facilitate recruitment and hiring through the payment of a bounty?
• Are there any restrictions on the eligibility of bounty candidates according to their social or family relationship with the employee?
• Are there any restrictions on the eligibility of candidates based on the history of behaviors of concern or risk presented by the person referring the candidate?
• Are there any restrictions on where the recruited employee may serve within the organization in relation to the recruiting employee's position?
• What is the attrition of bounty-recruited employees versus employees recruited by other means?
• Have employees recruited in this manner been associated with insider violations or risks?
Does your organization allow the hiring of candidates related to current or former employees?
• Are there any restrictions on the positions in which these employees may serve in relation to their employee relatives?
• Are there any restrictions on such hiring when the internal referral comes from someone with a history of behaviors of concern or other risk factors?
• What is the attrition of recruited family members compared to nonfamily employees?
• Have any employees, who are family members, been implicated in insider violations or risk-related

Audit Questions
behavior?
Does your organization allow the hiring of candidates with close personal relationships with current or former employees?
• Are there any restrictions on the positions in which these employees may serve in relation to their employee friends? • Are there any restrictions on such hiring when the internal referral comes from someone with a history of behaviors of concern or other risk factors? • What is the attrition of recruited social contacts compared to non-family employees? • Have any friends been implicated in insider violations or risk-related behavior?

Preemployment Screening

Table 4 assumes that without effective screening the odds of employing an individual with a predisposition for insider activities, such as predisposing personal characteristics, previous legal or rule violations, and potentially dangerous personal or social connections, is increased. Organizations have found a range of means to reduce this risk through different levels of candidate screening. Preemployment screening methods range from routine background checks with previous employers and personal interviews to more advanced procedures for honesty and psychological testing that are now more readily available as online or web-based products. This table also provides information on specific types of risks mitigated by each screening measure.

Table 4
Preemployment Screening

Screening Measures and Targeted Information	*Mitigated Risks*
Does your organization review employment applications for completeness?	
• Current name and address, phone and email • Alias • Address history (previous 7 to 10 years) • Social Security number • Citizenship • Date of birth • Driver's license number and state of issuance • Criminal history, to include type, level and date of offense • Employment history • Education • License or certification information • Applicant signature authorizing release of information • Applicant signature attesting to the truthfulness of responses	• Misconduct[1] • Inability to perform job duties
Does your organization conduct personal interviews?	
• Topics of discussion: ▪ Level of education ▪ Previous work experience ▪ Skills • Use the interview to evaluate: ▪ Interpersonal skills ▪ Reactions to personal and professional stress ▪ Negative work experiences or references ▪ Ethical decision-making patterns ▪ Information provided in the employment application	• Hiring employees using fraudulent identities • Inability to perform job duties • Potentially problematic interpersonal skills
Does your organization verify authenticity of government issued documents	
• Applicant's government issued documents (i.e., Social Security card, passport, driver's license, etc.) are inspected for evidence of counterfeiting or tampering.	• Hiring an employee with a fraudulent identity

[1] Within a court of law, misconduct typically requires "some act of wanton or willful disregard of the employer's interest, a deliberate violation of the employer's rules, or a disregard of the standard of behavior the employer has a right to expect of its employees." Baker v. Director, 39 Ark. App. 5, 6, 832 S.W.2d 864, 865 (1992).

Screening Measures and Targeted Information	*Mitigated Risks*
▪ Social Security numbers (SSN) can be verified at www.ssa.gov	
Does your organization verify employment eligibility?	
• Identity vetting via the Department of Homeland Security's E-Verify program will confirm U.S. Alien Registration numbers, naturalization certificate numbers, or passport numbers	• Hiring an employee with a fraudulent identity • Hiring an employee with fraudulent immigration documents
Does your organization review credit reports?	
• Credit reports reveal: ▪ Aliases - identity vetting ▪ Unlisted residences ▪ Identify foreign bank accounts and foreign relationships ▪ Bankruptcy ▪ Tax records ▪ Foreclosures ▪ Judgment ▪ Liens ▪ Lawsuits ▪ Unexplained affluence (i.e., rapid pay-down of mortgage) ▪ Amount and types of credit consistent with age of subject	• Hiring an employee with a fraudulent identity • Personal misconduct • Financial misconduct
Does your organization contact personal references?	
• Personal reference checks can confirm or reveal: ▪ Identity ▪ Current residence ▪ Current occupation and employer ▪ Personal misconduct	• Hiring an employee with a fraudulent identity
Does your organization conduct neighborhood interviews?	
• Neighborhood interviews can confirm or reveal: ▪ Identity ▪ Current residence ▪ Personal misconduct	• Hiring someone with a fraudulent identity • Personal misconduct
Does your organization contact professional references?	
• Professional references can confirm or reveal: ▪ Identity ▪ Employment history ▪ Misconduct ▪ Terminations	• Hiring someone with fraudulent identity • Hiring unqualified person • Hiring potentially disruptive person
Does your organization verify education records?	
• Education records can confirm or reveal: ▪ Identity ▪ Level of education and training, including licensing and certification ▪ Authenticity of institution and degree	• Hiring someone with a fraudulent identity • Inability to perform job duties
Does your organization check civil records?	
• Civil records will reveal: ▪ Aliases - identity vetting ▪ Bankruptcy ▪ Tax records ▪ Foreclosures ▪ Judgment ▪ Liens ▪ Lawsuits	• Hiring someone with a fraudulent identity • Personal misconduct • Financial misconduct

Screening Measures and Targeted Information	*Mitigated Risks*
▪ Protection orders ▪ Unexplained affluence	
Does your organization check criminal records?	
• Criminal records will reveal: ▪ Arrests, charges and convictions ▪ History of violent behavior ▪ Substance abuse	• Espionage • Sabotage • Personal and professional • Misconduct • Workplace violence
• Criminal records can be obtained from local police departments, local, state and federal courts and state central repositories of criminal history information (CHRI). ▪ Police departments may not release records, even when presented with a release signed by the employment candidate ▪ Only "open record states" will provide access to the state's repository of CHRI for noncriminal justice purposes.	
• Free and fee-based online resources for conducting checks of law enforcement agencies and courts:· ▪ National Court Check: Public Access to Court Electronic Records, AKA PACER. Access to case and docket information from the Federal Appellate, District and Bankruptcy court, and the U.S. Party/Case Index ▪ Trial Courts (not all states provide this resource) ▪ Appellate Courts (not all states provide this resource) ▪ State Supreme Court Online Docket (not all states provide this resource) ▪ Department of Public Safety or State Police criminal records checks (not all states provide this resource) ▪ Online Driver Records (not all states provide this resource) ▪ Sex Offender Registry: www.nsopr.gov ▪ Inmate Information (not all states provide this resource) ▪ Federal Bureau of Prisons for prisoner information ▪ Interpol: www.interpol.int	
• Commercial vendors providing criminal background checks ▪ LexisNexis ▪ ChoicePoint	
Does your organization conduct fingerprints checks?	
• FBI's Criminal Justice Information System (CJIS) ▪ Each fingerprint submission is checked against the Integrated Automated Fingerprint Identification System, and name checks of the National Crime Information Center ▪ Fingerprints can be submitted via Livescan, an electronic fingerprinting service or via rolled ink prints on finger and palm print cards	• Fraud • Espionage • Sabotage • Workplace misconduct • Workplace violence • Hiring someone with a criminal record
• FBI Civil fingerprint file ▪ Fingerprints are collected on federal employees and contractors, military service members, resident aliens and naturalized citizens	• Hiring someone with a fraudulent identity • Fraud • Workplace misconduct
• FBI Violent Gangs and Terrorist Organization File (VGTOF) ▪ Regularly updated by the Terrorist Screening Center ▪ GOTF conducted on all submissions to the FBI's CJIS	• Fraud • Espionage • Sabotage • Workplace misconduct • Workplace violence

Screening Measures and Targeted Information	*Mitigated Risks*
Does your organization conduct Department of Motor Vehicle (DMV) and National Driver Register (NDR) record checks?	
• DMV and NDR record checks will reveal: ▪ Aliases - identity vetting ▪ Drug and alcohol-related convictions ▪ Current and previous addresses ▪ Physical description of driver	• Workplace misconduct • Workplace violence • Personal misconduct • Drug and alcohol problems
Does your organization conduct a homeland security search?	
• OFAC Specially Designated Nationals and Blocked Persons • DTC Debarred Parties • Bureau of Industry and Security (formerly BXA)	• Terrorism • Espionage • Sabotage • Workplace misconduct
Does your organization conduct additional watch-list checks?	
• FBI Most Wanted • Interpol Most Wanted • United Nations Consolidated Terrorist List • European Union Terrorist List	• Terrorism • Espionage • Sabotage
Does your organization search overseas records?	
• Overseas records can confirm or reveal: ▪ Identity ▪ Interactions with foreign governments ▪ Interactions with U.S. embassies ▪ Foreign criminal history	• Terrorism • Espionage • Sabotage • Workplace misconduct
Does your organization test for illegal drug use?	
• Drug testing will reveal: ▪ Use of illicit drugs ▪ Illegal use of prescription drugs	• Workplace misconduct • Policy violations • Security violations • Disgruntled employee • Workplace violence • Workplace harassment • Inability to perform job duties • Criminal connections
Does your organization conduct informal online searches?	
• Google • Facebook • MySpace • Peoplesearch.com	• Hiring someone with a fraudulent identity • Hiring someone with a fraudulent work or education history • Hiring someone with a criminal record • Hiring someone at risk for misconduct or poor judgment
Does your organization evaluate risk-related personal associations?	
• Personal or professional connections to persons or groups with known risk factors • Social networking search engines • ERIK, NORA, ANNA	• Security violations • Workplace misconduct • Workplace violence • Possible criminal or dangerous associates
Does your organization conduct honesty testing?	

Screening Measures and Targeted Information	*Mitigated Risks*
• Purposes of honesty testing: ▪ Honesty ▪ Integrity ▪ Reliability	• Workplace misconduct • Policy violations • Security violations
Does your organization conduct mental health and personality testing?	
• Purposes of psychological testing: ▪ Psychological disorders ▪ Personality disorders ▪ Likely organizational aptitude, behavior and "fit"	• Disgruntled employee • Workplace violence • Workplace harassment • Inability to perform job duties • Impaired judgment, reliability and trustworthiness
Does your organization conduct polygraph exams?	
• In specialized, legal settings involving high risk. • A polygraph exam can: ▪ Deception detection regarding personal history or intentions ▪ Identify those who may be more likely to engage in counterproductive behavior	• Espionage • Sabotage • Workplace misconduct • Policy violations • Security violations • Inability to perform job duties

Training, Education and Program Effectiveness

Policies and practices that are not recognized, understood, and adhered to may be of marginal effectiveness without training and education. Table 5 addresses whether an organization has deployed training and/or educational resources to increase the likelihood of policy compliance in areas related to insider risk. Critical to the success of training and education programs is the regular evaluation of these programs for effectiveness in communicating policy requirements and for their impact on the targeted behaviors related to insider risk.

Table 5
Training, Education and Program Effectiveness

Audit Questions
Do specific training and education programs addressing policy and practice areas relevant to insider risk exist, and include:
• Job descriptions and employment contracts describe employee responsibilities for information security and protection of sensitive information and resources. Also included are consequences for failing to protect these assets • Rules for a probationary period with increased monitoring for new hires • Information and personnel security in the workplace • Physical security of facilities • Employee use of organizational property outside of work • Boundaries between personal and professional activities that utilize work time and resources • Ownership and sharing of organization intellectual property • Handling and management of sensitive, proprietary or classified information • Outside business involvements and contacts and the reporting of these contacts • Privacy of employee, customer, client and other sensitive personal information • The organizations right to monitor and audit employee activity on proprietary systems • Description on how employees report grievances and their own and others' risk behaviors • Defining unacceptable workplace interpersonal behaviors • Guidelines for reporting and addressing unacceptable workplace behaviors • Employee benefits and compensation • Employees evaluation and advancement • Describing access to and benefits of employee assistance programs and other support services • Describing the good conduct policy • Applying policies and practices to trusted partners • Adversary awareness training describing possible observable insider risk behaviors, pre-attack planning, recruitment or other suspicious behaviors • Adversary awareness training describing the collection methods of adversary groups that may be targeting the organization and its employees, including through the use of insiders • Adversary awareness training appropriate to international organizational sites, employees and travel • Guidelines on recognizing, reporting, intervening with and following-up on employees identified as at risk for insider acts
Are these training and education efforts appropriately structured for the needs of different employee groups such as managers, systems administrators, human resource personnel, persons in different geographic areas or risk environments, etc?
Are these training and education programs updated according to new information regarding these issues,

Audit Questions
changes relevant to organizational risks?
Do these training and education programs require attendees to demonstrate their knowledge/competence in these areas as a condition of program completion and access to organization resources?
Are employees asked to demonstrate their competence in these areas through other means such as exercises or red team programs?
Are training and education programs modified based on their impact on target issues?
Are training and education programs modified based on employee feedback regarding their effectiveness?

Continuing Evaluation and Policy Implementation

Once effective insider risk management policies are established and communicated, they must be monitored for employee compliance and enforcement guidelines established in the event of noncompliance. Without effective continuing evaluation in the form of employee monitoring and enforcement, compliance will lapse and insider risk will escalate. Table 6 below displays nine indicators (stated as self-audit questions) of policy monitoring and enforcement with the assumption that the potential for adverse insider behavior will be minimized by the optimal number and mix of monitoring and enforcement measures employed by an organization.

Table 6
Continuing Evaluation and Policy Implementation

Audit Questions
Does your organization track the frequency and effectiveness of employee reporting of at-risk behaviors through its designated programs and channels?
Do you actively investigate these reports in a manner that does not deter future reporting?
Does your organization utilize specialized, trained, multidisciplinary staff outside the at-risk employee's reporting structure to investigate risk reports?
Do these specialized staffers follow standardized investigative and reporting procedures when looking in to these reports of risk, including guidelines for evaluating risk in multiple categories including insider espionage and sabotage, violence and theft of intellectual property (IP)?
Are the results of these investigations stored and recorded regardless of outcome, and accessible, so that future reports regarding personnel may be evaluated in context?
Are there clear options for management intervention—sanctions, referrals, further monitoring, or other steps that should be taken as a result of investigative findings?
Are the processes, rationale and justification for management intervention documented to ensure that these steps and their possible outcomes are considered carefully?
Are actual management actions enforced without discrimination, recorded, and subsequently evaluated for effectiveness?
Are records of employee at-risk behaviors, investigations, and management actions maintained and analyzed as input to new policies, practices, or interventions?
Does your organization perform periodic or follow-up database checks or other investigative actions normally associated with pre-screening to ensure that continuing employees remain reliable and are not subject to compromising factors?
Does your organization maintain and advertise the availability of an Employee Assistance Program to which employees can turn for confidential short term treatment and referral?

Management Intervention: Assessment and Planning

Research on insider events consistently indicates that many organizational interventions after employees have displayed concerning behaviors escalate rather than mitigate the problem. As noted in the background report, this was particularly the case when an employee was rapidly terminated without sufficient evaluation and assessment of risks of retaliation against the organization. Organizations that have the capability to assess insider risk prior to management intervention and that use the assessment process to design risk mitigation plans for potentially dangerous employees will be better able to minimize insider risk. Table 7 describes six recommendations (stated as self-audit questions) that represent a coordinated strategy for effective employee evaluation and management intervention.

Table 7
Management Intervention

Audit Questions
Do policies and procedures exist for early identification of employees at-risk before interventions that may cause negative employee reactions and increase insider risk?
Do policies and procedures exist for referring at-risk employees facing negative personnel actions to appropriate teams for evaluation?
Does a specialized team, including HR, legal, employee assistance programs, physical and IT security, and behavioral science members, exist to evaluate the risk of insider espionage, sabotage, theft as well as traditional risks of violence, harassment, etc. prior to interventions?
Are procedures in place to guide team members on assessment procedures? Is the team trained, exercised and prepared to execute such assessments?
Do Team members have established relationships and liaison with law enforcement, judicial, specialized medical, social service and other community personnel whose assistance and collaboration may be important for case management?
Do policies and practices exist to facilitate implementation of team recommendations designed to reduce identified risks?