# FRAUD RISK MANAGEMENT SCORECARDS

These five scorecards are from the COSO/ACFE Fraud Risk Management Guide. These scorecards can be used in performing organizational self-assessments of each of the five fraud risk management principles to aid in determining how comprehensive an organization's fraud risk management program is, how well it is achieving its fraud risk management objectives, and where improvements and strengthening is needed.

**APPENDIX J1**

**FRAUD RISK GOVERNANCE SCORECARD**

# APPENDIX J1: RAUD RISK GOVERNANCE SCORECARD

To assess the strength of the organization's fraud governance, carefully assess each area below and score the area, factor, or consideration as:

**Red:** indicating that the area, factor, or consideration needs substantial strengthening and improvement to bring fraud risk down to an acceptable level

**Yellow:** indicating that the area, factor, or consideration needs some strengthening and improvement to bring fraud risk down to an acceptable level

**Green:** indicating that the area, factor, or consideration is strong and that fraud risk has been reduced — at least — to a minimally acceptable level

Each area, factor, or consideration scored either red or yellow warrants having a note associated with it that describes the action plan for bringing it to green on the next scorecard.

| Fraud Risk Governance Area, Factor, or Consideration | Score | Notes |
|---|---|---|
| **MAKING AN ORGANIZATIONAL COMMITMENT TO A FRAUD RISK MANAGEMENT PROGRAM** | | |
| **Our organization has a strong correlation between our organizational culture and fraud risk management.** | | |
| **Our organization's leadership demonstrates "tone at the top" by promoting ethical behavior and emphasizing a focus on deterring, preventing and detecting fraud.** | | |
| **Our organization's leadership leads by example to ensure that all personnel, vendors, and contractors understand that the organization is serious about promoting ethical behavior and is committed to deterring, preventing, and detecting fraud.** | | |
| **The way that our management reacts to instances of fraud sends a powerful message inside and outside the organization and acts as a strong deterrent to fraudulent behavior.** | | |
| **Our organization has a policy regarding our standards of business conduct that reflects the commitment of our organization and our board of directors, officers, executives, and other personnel to conduct business according to the highest standards of integrity and ethics.** | | |
| **Our organization creates a positive work environment for employees, hires and promotes appropriate employees, and conducts effective training programs.** | | |
| **Our organization requires employees to periodically confirm their understanding of our code of conduct.** | | |
| **Our organization disciplines employees appropriately and consistently regardless of their positions.** | | |
| **SUPPORTING FRAUD RISK GOVERNANCE** | | |

# FRAUD RISK GOVERNANCE SCORECARD

| Fraud Risk Governance Area, Factor, or Consideration | Score | Notes |
|---|---|---|
| **Our board of directors is composed of members who are independent and objective.** | | |
| **Our board of directors is responsible for ensuring that management designs effective fraud risk management policies that encourage ethical behavior and empower employees, customers, and vendors to strive for those standards every day.** | | |
| **Our board of directors has a thorough understanding of what constitutes fraud and corruption.** | | |
| **Our board sets the appropriate tone at the top through its own independent practices and through the CEO's job description, evaluation, and succession-planning process** | | |
| **Our board of directors maintains oversight of the fraud risk assessment.** | | |
| **Our board of directors evaluates management's identification of fraud risks, including overseeing the internal controls over financial reporting established by management.** | | |
| **Our board of directors assesses the risk of fraud by management, including the risk of management override of controls, and ensures that controls are designed and functioning to prevent and detect managerial fraud.** | | |
| **Our board of directors supports internal audit's approved annual plan and ensures that the internal audit department has access to all information, data and employees, taking into account applicable data privacy regulations.** | | |
| **Our board of directors ensures that the internal audit department has unrestricted access to the board or a committee of the board, namely the audit committee.** | | |
| **Our board of directors ensures that all employees have access to the board, the audit committee, and the internal audit department.** | | |
| **Our board empowers a committee of the board to focus on fraud deterrence, prevention and detection.** | | |
| **Our organization's board of directors is fully informed about occurrences of fraud within the organization, namely those involving senior-level employees and significant internal control deficiencies.** | | |
| **Our organization's board of directors documents the responsibilities of board members and communicates them throughout the organization.** | | |

# FRAUD RISK GOVERNANCE SCORECARD

| Fraud Risk Governance Area, Factor, or Consideration | Score | Notes |
|---|---|---|
| Our organization's board of directors ensures that we have sufficient resources to implement and maintain a fraud risk management program and for retaining outside advisors and counsel as necessary. | | |
| **ESTABLISHING A COMPREHENSIVE FRAUD RISK MANAGEMENT POLICY** | | |
| Our organization has established a comprehensive fraud risk management policy that includes broad policies and principles which guide personal conduct. | | |
| All employees know about and understand our fraud risk management policy. | | |
| Our fraud risk management policy emphasizes that ethics and honesty are taken very seriously, especially at the highest levels of our organization. | | |
| Our fraud risk management policy is tailored to our specific risk profile and is structured to relevant fraud risk scenarios for our organization. | | |
| Our organization's fraud risk management policy clearly defines the processes and communication channels by which violations and potential violations are to be reported. | | |
| **ESTABLISHING FRAUD RISK GOVERNANCE ROLES AND RESPONSIBILITIES THROUGHOUT THE ORGANIZATION** | | |
| We have assigned the overall responsibility for fraud risk management to a single executive-level individual who reports to the board periodically. | | |
| The individual we have assigned the primary responsibility for fraud risk management is familiar with the organization's fraud risks and process-level controls and is responsible for designing and implementing the processes by which violations are to be reported and investigated. | | |
| We have formally documented the roles and responsibilities of all personnel as part of our organization's fraud risk management program. | | |
| Our fraud risk management policy serves as a guidepost about the expectations of our board and senior management regarding fraud-related matters. | | |
| Our management retains the primary responsibility for ensuring that our fraud risk management program is carried out. | | |
| **DOCUMENTING THE FRAUD RISK MANAGEMENT PROGRAM** | | |

# FRAUD RISK GOVERNANCE SCORECARD

| Fraud Risk Governance Area, Factor, or Consideration | Score | Notes |
|---|---|---|
| **Our fraud risk management policy is documented and updated based on our organization's current risk profile and experiences.** | | |
| **The documentation concerning all aspects of our fraud risk management program is included in our fraud risk management policy and is separate from our code of conduct.** | | |
| **Our board of directors and senior management summarize their commitments to a fraud risk management program in a short document made available to all employees, vendors and customers. This document is written or endorsed by a senior executive or board member, reissued periodically, and tracked by our organization to ensure receipt and understanding.** | | |
| **Our organization augments our fraud risk management policy with an enterprise-wide fraud training course that is mandatory for all employees.** | | |
| **Our fraud risk management policy and fraud training define fraud, identify both internal and external potential perpetrators of fraud, provide hypothetical organization-based examples of fraud, and define the roles and responsibilities of those charged with oversight of fraud control.** | | |
| **All of our personnel and vendors understand their individual expectations related to our fraud risk management program.** | | |
| **COMMUNICATING FRAUD RISK MANAGEMENT AT ALL LEVELS OF THE ORGANIZATION** | | |
| **We hold our CEO and senior management responsible for establishing a system of internal controls that supports the achievement of our fraud risk management objectives at all levels of our organization. .** | | |
| **Our CEO and senior management design, implement, conduct and periodically assess the structures, authorities and responsibilities needed to establish accountability for all internal control, including fraud risk management and fraud prevention and detection.** | | |
| **Our board monitors the effectiveness of our fraud risk management program and addresses the topic periodically as an agenda item during board meetings.** | | |
| **Our board establishes mechanisms to ensure the receipt of timely and accurate information regarding potential fraud from management, employees, auditors and other stakeholders.** | | |
| **Our board assesses the degree to which relevant parties with which it communicates including management, employees, auditors and other stakeholders believe that our organization's fraud practices and policies are adequate.** | | |

# FRAUD RISK GOVERNANCE SCORECARD

| Fraud Risk Governance Area, Factor, or Consideration | Score | Notes |
|---|---|---|
| Our fraud risk management policy articulates our risk tolerance considerations and the expectation that suspected fraud will be reported immediately. | | |
| Our organization conveys that it has the right to institute civil or criminal action against perpetrators of fraud and specifies the consequences for fraudulent activity in the fraud risk management policy. | | |
| Our organization communicates the protections afforded to any individual who reports suspected fraud to encourage timely reporting of such issues. | | |
| Our organization has an effective whistleblower process in place and our fraud risk management program includes a thorough explanation of this process. | | |
| Our internal audit group reviews the gathering process and reporting for completeness, accuracy, and follow-through. | | |
| Our fraud risk management policy reflects the need to conduct a remediation analysis when fraud allegations arise or when an investigation uncovers improper behavior or transactions in order to identify the control weakness responsible. | | |
| Our senior management openly shares the details of key frauds that have occurred within the organization including the ultimate consequences to the perpetrators. | | |

**APPENDIX J2**

**FRAUD RISK ASSESSMENT SCORECARD**

# APPENDIX J2: FRAUD RISK ASSESSMENT SCORECARD

To assess the strength of the organization's fraud risk assessment process, carefully assess each area below and score the area, factor, or consideration as:

Red: indicating that the area, factor, or consideration needs substantial strengthening and improvement to bring fraud risk down to an acceptable level

Yellow: indicating that the area, factor, or consideration needs some strengthening and improvement to bring fraud risk down to an acceptable level

Green: indicating that the area, factor, or consideration is strong and that fraud risk has been reduced — at least — to a minimally acceptable level

Each area, factor, or consideration scored either red or yellow warrants having a note associated with it that describes the action plan for bringing it to green on the next scorecard.

| Fraud Risk Assessment Area, Factor, or Consideration | Score | Notes |
|---|---|---|
| **INVOLVING APPROPRIATE LEVELS OF MANAGEMENT** | | |
| **Our fraud risk assessment team includes all appropriate levels of management and internal and external sources to assess fraud throughout the organization.** | | |
| **Our risk assessment team includes resources such as:**<br>• **Accounting/finance personnel**<br>• **Non-financial business unit and operations personnel**<br>• **Information technology personnel**<br>• **Risk management personnel**<br>• **Legal and compliance personnel**<br>• **Internal audit personnel**<br>• **External consultants, if expertise is not available internally** | | |
| **Management, senior management, business unit leaders, and significant process owners participate in the risk assessment because they are ultimately accountable for the effectiveness of our organization's fraud risk management efforts.** | | |
| **Our fraud risk assessment team reviews our organization's strategic plan, process maps, and control matrices to identify the population of activities that are potentially exposed to fraud.**<br><br>**Our fraud risk assessment team engages in** | | |

# FRAUD RISK ASSESSMENT SCORECARD

| Fraud Risk Assessment Area, Factor, or Consideration | Score | Notes |
|---|---|---|
| **brainstorming sessions to identify incentives, pressures, and opportunities to commit fraud; the risk of management override of controls; and the fraud risks that are most relevant to our organization.**<br><br>**Our fraud risk assessment team shares its fraud risk identification information with the board and solicits feedback from them.** | | |
| **Our board assesses the implications of its own processes on fraud risk and considers how its policies may create incentives, pressures, and opportunities to commit fraud.** | | |
| **INCLUDING ENTITY, SUBSIDIARY, DIVISION, OPERATING UNIT, AND FUNCTIONAL LEVELS** | | |
| **Our organization identifies and assesses risk at the entity, subsidiary, division, operating unit and functional levels relevant to the achievement of our objectives.** | | |
| **We assemble multiple fraud risk teams as necessary to accommodate the size and complexity of our organization and to ensure the consideration of every possible fraud scheme and fraud risk exposure.** | | |
| **Each of our fraud risk assessment teams includes personnel with a detailed working knowledge and understanding of the organizational unit under assessment and how it interacts with other organizational units.** | | |
| **ANALYZING INTERNAL AND EXTERNAL FACTORS** | | |
| **Our identification of risks takes into account internal factors such as the processes and controls in place to process and account for everyday transactions, and organizational incentives, pressures, and opportunities to commit fraud.** | | |
| **Our identification of risks takes into account external factors, such as customers and vendors with which our organization interacts, the business environment in which we operate, and the extent to which individuals or groups are inclined to disrupt or interfere with our organization's business.** | | |
| **CONSIDERING VARIOUS TYPES OF FRAUD** | | |
| **Our fraud risk assessment team considers various types of fraud that may be committed against or by the organization, including fraudulent financial reporting, fraudulent non-financial reporting, misappropriation of** | | |

# FRAUD RISK ASSESSMENT SCORECARD

| Fraud Risk Assessment Area, Factor, or Consideration | Score | Notes |
|---|---|---|
| **assets, and illegal acts such as corruption.** | | |
| **Our fraud risk assessment team obtains information from external sources such as industry news to understand the fraud risks and subset of risks specific to our organization.** | | |
| **Our fraud risk assessment team gathers information about potential fraud from internal sources, such as interviews with personnel, brainstorming sessions, complaints received from the whistleblower hotline, and analytical procedures.** | | |
| **When assessing the risk of fraudulent financial reporting, we consider risks such as:**<br>• **Inappropriately reported revenues, expenses, and balance sheet amounts and inappropriately exaggerated or omitted disclosures**<br>• **Concealment of misappropriation of assets, including unauthorized acquisition, disposition, and use of assets**<br>• **Concealment of unauthorized receipts and expenditures, such as facilitation payments and bribes** | | |
| **We use a fraud risk assessment matrix to identify and document the specific areas of greatest risk to our organization and to help us determine how to tailor the assessment process accordingly.** | | |
| **Our fraud risk assessment team considers the following questions in addressing significant marketplace disclosures:**<br>• **What controls are in place to monitor internal gathering and reporting of these disclosures?**<br>• **Is there oversight from someone whose compensation is not directly affected by the disclosure?**<br>• **Does someone monitor the organization's disclosures in relation to other organizations and ask hard questions about whether the organization's disclosures are adequate or could be improved?** | | |
| **When assessing the risk of fraudulent non-financial reporting, we consider fraud schemes that can lead to:**<br><br>• **Manipulation of health and safety records and reports**<br>• **Intentional misreporting of productivity measures**<br>• **Falsification of quality assurance reports** | | |

# FRAUD RISK ASSESSMENT SCORECARD

| Fraud Risk Assessment Area, Factor, or Consideration | Score | Notes |
|---|---|---|
| • **Falsifications of customer metrics or other operational metrics**<br>• **Falsification of educational or professional credentials** | | |
| **We have developed our own protocols and controls over the processing of non-financial data relevant to our operations.** | | |
| **When assessing the risk of fraudulent non-financial reporting, we consider the following questions:**<br>• **What are key reports on which the organization relies on to operate effectively?**<br>• **What are the key reports or certifications the organization is required to provide by law, rule, regulation, or contractual requirements?**<br>• **Is the data contained within those reports from controlled sources, or is it subject to manual intervention and bias?**<br>• **Are there non-financial metrics that are important to the organization's stakeholders, including regulators?**<br>• **Are there non-financial reports or metrics that can have a direct or indirect impact on personnel compensation and bonuses?**<br>• **Are there industry-specific issues the organization needs to consider?** | | |
| **Our fraud risk assessment team has an understanding of what assets are subject to misappropriation, the locations of the related assets, and which personnel have control over or access to tangible and intangible assets.** | | |
| **Our fraud risk assessment team considers the risk of illegal acts such as:**<br><br>• **Bribery and gratuities made to companies, private individuals, and public officials**<br>• **Receipt of bribes, kickbacks, and gratuities**<br>• **Aiding and abetting fraud by other parties**<br>• **Violation of the False Claims Act or other relevant federal, state, or local laws and regulations** | | |
| **We have considered all applicable anti-corruption laws that may affect our overseas operations in establishing our fraud risk management program.** | | |

# FRAUD RISK ASSESSMENT SCORECARD

| Fraud Risk Assessment Area, Factor, or Consideration | Score | Notes |
|---|---|---|
| Our board evaluates its performance regularly with respect to reputation risk and ensures that our organization's risk assessment process includes the consideration of reputation risk. | | |
| We incorporate information technology risk and the ongoing threat of cyber fraud into our overall fraud risk assessment. | | |
| **SPECIFICALLY CONSIDERING THE RISK OF MANAGEMENT OVERRIDE OF CONTROLS** | | |
| During the risk identification process, our fraud risk assessment team specifically considers the potential for management override of controls, including the controls designed to prevent or detect fraud. | | |
| We keep the risk of management's override of controls in mind when evaluating the effectiveness of controls. | | |
| **ESTIMATING THE LIKELIHOOD AND SIGNIFICANCE OF RISKS IDENTFIIED** | | |
| Our risk assessment team evaluates the likelihood and significance of identified fraud risks based on historical information, known fraud schemes, and interviews with business process owners. | | |
| Our management assesses the likelihood of a fraud risk's occurrence by determining instances in which the particular fraud has occurred in our organization in the past, the prevalence of the particular fraud risk in our organization's industry, and other factors. | | |
| Our organization categorizes the likelihood of a particular fraud risk as remote, reasonably possible, or probable | | |
| Our management assesses the significance of a fraud risk by taking into account financial and monetary significance as well as significance to our organization's operations, brand value, reputation, and criminal, civil, and regulatory liability. | | |
| Our organization categorizes the significance of a fraud risk as inconsequential, more than inconsequential, or material. | | |

# FRAUD RISK ASSESSMENT SCORECARD

| Fraud Risk Assessment Area, Factor, or Consideration | Score | Notes |
|---|---|---|
| **ASSESSING PERSONNEL OR DEPARTMENTS INVOLVED IN ALL ASPECTS OF THE FRAUD TRIANGLE** | | |
| **We evaluate the incentives and pressures on individuals and departments and use that information to determine who is most likely to commit fraud and the means by which the fradulent activity will most likely be committed so that we can formulate appropriate risk responses.** | | |
| **Our fraud risk assessment team focuses on the elements of the fraud triangle, namely:**<br><br>• **Incentives and pressures that motivate an individual to commit a fraudulent act**<br>• **Opportunities or perceived opportunities that provide an individual with some assurance that a fraudulent act can be committed without being detected**<br>• **Attitudes or rationalizations that enable an individual to internally justify the performance of a fraudulent act** | | |
| **Our board evaluates incentive programs for senior executives and management evaluates these programs for others in the organization.** | | |
| **Our fraud risk assessment team considers incentives to commit fraud, such as compensation or maintaining the status quo, as well as pressures to commit fraud, such as a desire to achieve performance or other targets.** | | |
| **Our fraud risk assessment team considers how our organization may affect attitudes and rationalizations through our hiring and evaluation process and in the tone established by leadership and management.** | | |
| **Our fraud risk assessment team considers opportunities for unauthorized acquisition, use or disposal of assets and for altering of our entity's reporting records.** | | |
| **We examine areas in which opportunities to commit fraud are the greatest, namely, where internal controls are weak and there is a lack of segregation of duties.** | | |
| **IDENTIFYING EXISTING FRAUD CONTROL ACTIVITIES AND ASSESSING THEIR EFFECTIVENESS** | | |
| **Our fraud risk assessment team examines each** | | |

# FRAUD RISK ASSESSMENT SCORECARD

| Fraud Risk Assessment Area, Factor, or Consideration | Score | Notes |
|---|---|---|
| specific fraud scheme or risk, identifies the control activities in place to mitigate these risks, and determines the effectiveness of these existing controls. | | |
| Our management evaluates the potential of any residual risks and determines what controls and procedures should be implemented to address such risks. | | |
| We prioritize the fraud risks that are deemed to be highly likely and highly significant.<br><br>Our risk assessment team evaluates control optimization and notes any instances of unnecessary or redundant control activities. | | |
| **DETERMINING HOW TO RESPOND TO RISKS** | | |
| Our board determines our organization's risk tolerance, taking into consideration our responsibilities to all shareholders, citizens, capital providers, and other stakeholders. | | |
| Our board ensures that management has selectively and efficiently implemented the right level of controls based on our established risk tolerance. | | |
| Management's documentation of fraud control activities includes a description of what the control is designed to do, who is to operate the control, who is to monitor and assess the effectiveness of the control, and the related segregation of duties. | | |
| **USING DATA ANALYTICS TECHNIQUES FOR FRAUD RISK ASSESSMENT AND FRAUD RISK RESPONSES** | | |
| We perform disaggregated analytics on revenue as part of the fraud risk assessment process. | | |
| We use data analytics to compile, display, and analyze the results of employee surveys, facilitated sessions, and other data-gathering techniques. | | |
| We utilize any of the following data analytics techniques to gather fraud risk evidence:<br><br>• Data stratification<br>• Risk scoring<br>• Trend analysis<br>• Fluctuation analysis<br>• Data visualization<br>• Statistical and predictive modeling<br>• Using information from external sources in | | |

# FRAUD RISK ASSESSMENT SCORECARD

| Fraud Risk Assessment Area, Factor, or Consideration | Score | Notes |
|---|---|---|
| analytics | | |
| **PERFORMING PERIODIC REASSESSMENTS AND ASSESSING CHANGES TO FRAUD RISK** | | |
| **We perform an initial risk assessment and then re-perform periodically.** | | |
| **Our risk assessment team recognizes that both external and internal changes result in the need for a new and updated fraud risk assessment related to areas affected by the change.** | | |
| **We consider how external changes, such as those in the regulatory or economic environment, can affect items with which regulators are most concerned and the financial incentives and pressures facing our organization.** | | |
| **We consider how organizational changes, such as the introduction of new product lines or services, can lead to new incentives and pressures on employees and new activites to assess for fraud risks.** | | |
| **We consider the impact of outsourcing initiatives on current employee morale and whether the outsource provider has adequate controls to address the fraud risks inherent in the services they provide.** | | |
| **We consider how changes in organizational leadership may change the tone at the top and therfore affect the culture of compliance within our organization.** | | |
| **We consider how changes in organizational leadership can change who executes and approves transactions, who oversees the fraud risk management program, and whether these new leaders fully understand the processes, controls and monitoring activities that are in place.** | | |
| **DOCUMENTING THE RISK ASSESSMENT** | | |
| **We document our fraud risk assessment in a matrix that includes the following columns, from left to right:**<br>• **1. Identified fraud risks and schemes**<br>• **2.  Likelihood of occurrence**<br>• **3. Significance of occurrence**<br>• **4. Personnel/Departments involved**<br>• **5. Exisiting fraud control activities**<br>• **6. Effectiveness of existing control activities**<br>• **7. Residual fraud risks**<br>• **8. Fraud risk reponses** | | |

**APPENDIX J3**

**FRAUD CONTROL ACTIVITIES SCORECARD**

# APPENDIX J3: FRAUD CONTROL ACTIVITIES SCORECARD

To assess the strength of the organization's fraud control activities, carefully assess each area below and score the area, factor, or consideration as:

Red: indicating that the area, factor, or consideration needs substantial strengthening and improvement to bring fraud risk down to an acceptable level

Yellow: indicating that the area, factor, or consideration needs some strengthening and improvement to bring fraud risk down to an acceptable level

Green: indicating that the area, factor, or consideration is strong and that fraud risk has been reduced — at least — to a minimally acceptable level

Each area, factor, or consideration scored either red or yellow warrants having a note associated with it that describes the action plan for bringing it to green on the next scorecard.

| Fraud Control Activities Area, Factor, or Consideration | Score | Notes |
|---|---|---|
| **PROMOTING FRAUD DETERRENCE THROUGH PREVENTIVE AND DETECTIVE CONTROL ACTIVITIES** | | |
| **Our organization attempts to deter fraud by:**<br>• **Establishing a visible and rigorous fraud governance process**<br>• **Creating a transparent and sound anti-fraud culture**<br>• **Conducting a robust and thorough fraud risk assessment periodically**<br>• **Designing, implementing, and maintaining preventive and detective fraud control processes and procedures**<br>• **Taking swift action in response to allegations of fraud and against those involved in wrongdoing** | | |
| **Our organizational culture clearly communicates through its words and actions that perpetrators of fraud face a high likelihood of getting caught and being held responsible and punished.** | | |
| **We implement detective controls in those situations in which the implementation of preventive controls would be too costly or too intrusive to business operations.** | | |
| **Our organization has overt control activities in place, such as basic procurement procedures and supervisory and managerial approval requirements that are generally known to employees and those with whom we interact.** | | |

# FRAUD CONTROL ACTIVITIES SCORECARD

| Fraud Control Activities Area, Factor, or Consideration | Score | Notes |
|---|---|---|
| Our organization has covert control activities in place that remain unknown to employees and those with whom we interact, such as data analytics procedures designed to identify unusual transactions. | | |
| **INTEGRATING WITH THE FRAUD RISK ASSESSMENT** | | |
| If the fraud risk assessment revealed that there are no control activities in place to mitigate an identified fraud risk, management has effectively addressed this issue by selecting, developing, and implementing the necessary controls to reduce this risk to an acceptable level. | | |
| If the fraud risk assessment revealed that there are existing control activities that are not sufficient to reduce fraud risk to an acceptable level, management has effectively addressed this issue by selecting, developing, and implementing *additional* controls to supplement or replace the existing controls. | | |
| We have categorized our control activities in our fraud risk assessment matrix as either:<br>• **A-Type: Existing fraud control activities that are identified and linked to identified fraud risks and schemes (column 5), or**<br>• **B-Type: Additional fraud control activities developed as a response to residual fraud risk (column 8)** | | |
| In documenting control activities, the first column lists fraud risks taken directly from column 1 of the risk assessment matrix. The second column lists all controls related to each risk (A-Type and B-Type). The third column identifies the person or persons responsible for ensuring that the control activity is performed and remains effective. | | |
| **CONSIDERING ORGANIZATION-SPECIFIC FACTORS AND RELEVANT BUSINESS PROCESSES** | | |
| We select our fraud control activities in response to organization-specific factors and relevant business processes. | | |
| **CONSIDERING THE APPLICATION OF CONTROL ACTIVITIES TO DIFFERENT LEVELS OF THE ORGANIZATION** | | |

# FRAUD CONTROL ACTIVITIES SCORECARD

| Fraud Control Activities Area, Factor, or Consideration | Score | Notes |
|---|---|---|
| **We implement our preventive controls at lower organizational levels and early in business processes in order to be more effective.** | | |
| **We implement our detective controls at various organizational and operational levels.** | | |
| **We pay special attention to preventive control activities surrounding senior management activities and transactions initiated by senior managers.** | | |
| **UTILIZING A COMBINATION OF FRAUD CONTROL ACTIVITIES** | | |
| **The design and implementation of our fraud control activities represent a coordinated effort by senior management and the support of personnel representing all significant business processes across the organization.** | | |
| **Our control activities adequately mitigate the risk of fraud in accordance with our organization's specific risk tolerance.** | | |
| **We have multiple (sometimes redundant and overlapping) control activities in place to manage risks with a high likelihood or significant potential impact, and those that are rapidly-evolving, such as cybersecurity risks.** | | |
| **We have considered all costs of implementing controls, including the direct cost of the control and the potential costs of the control's effect on or interference with operations, in arriving at the optimum mix of preventive and detective controls.** | | |
| **Our organization stresses the existence of a fraud prevention program internally and externally through a wide variety of media such as emails, webcasts, posters, flyers, electronic messages, and articles.** | | |
| **We have business process control activities in place that structure and manage operations, delegate authority and responsibility, centralize and decentralize processes, define whether to outsource or keep production in-house, and define whether to subcontract.** | | |
| **We have physical access controls in place related to facilities, assets, and information systems.** | | |
| **We have logical access controls in place to restrict access to our organization's technology and** | | |

# FRAUD CONTROL ACTIVITIES SCORECARD

| Fraud Control Activities Area, Factor, or Consideration | Score | Notes |
|---|---|---|
| information systems environments. | | |
| We have transaction controls in place that mitigate transaction processing risks in our organization's business processes by testing for completeness, accuracy, and validity. | | |
| We have technological controls in place such as third-party due diligence checks against known credit, sanctions, criminal or watch list databases, use of software-based fraud risk awareness training, and automated business rules or risk-scoring mechanisms that restrict certain business activities from occurring. | | |
| Our organization stresses its human resources procedures, authority limits, transaction-level control procedures, and oversight designed to prevent management override of controls as the most important elements supporting fraud prevention. | | |
| Our organization assesses and continuously monitors detective controls to determine that our fraud detection techniques are present and functioning to ensure that fraud that is occurring or has occurred is detected in a timely manner. | | |
| We carefully control who has access to the knowledge regarding the exact nature and specific design of detective controls. | | |
| Our detective controls occur in the ordinary course of business, draw on external information to corroborate internally generated information, routinely and automatically communicate identified deficiencies and exceptions to appropriate leadership, and use results to enhance or modify other controls. | | |
| We have data analytic procedures in place to trigger follow-up investigations of anomalous trends when preventive controls designed to prevent every fraudulent transaction would have been too costly or intrusive to implement. | | |
| We know our employees well enough to evaluate their credentials and competence, match their skills to job requirements, and be aware of any issues of personal integrity that may affect their suitability for a position. | | |
| Our human resources department uses job applications, resumes and follow-up communications | | |

# FRAUD CONTROL ACTIVITIES SCORECARD

| Fraud Control Activities Area, Factor, or Consideration | Score | Notes |
|---|---|---|
| with references provided by candidates to uncover any false or embellished information or an undesirable history or reputation that may represent risk to our organization. | | |
| We perform background checks on prospective employees as part of the initial hiring process. | | |
| We take into account applicable laws and regulations when requesting background information from prospective and existing employees and seek legal counsel regarding what information can and cannot be obtained and the appropriate procedures to follow. | | |
| We perform additional periodic updated background checks on key individuals to identify any changed circumstances that may indicate heightened fraud risk. We also use this procedure for existing employees whenever behavioral red flags are noted. | | |
| We perform background checks on prospective and existing suppliers, customers, and business partners to help us identify any issues of financial health, ownership, reputation, and integrity that represent a risk to our organization. | | |
| All employees at all levels of our organization receive an initial orientation and ongoing education on our fraud risk management program. | | |
| Our fraud training reflects the specific fraud risks, operations, and circumstances of our organization. | | |
| Attendance is mandatory for all employees for fraud-related training sessions, including periodic updates and refresher sessions. | | |
| We obtain signed affirmations from every employee on an annual basis that he or she is aware of our organizational code of conduct, will continue to comply with the code of conduct, and is aware of our fraud risk management program. | | |
| We perform regular and robust assessments of employee performance and provide timely and constructive feedback. | | |
| Our human resources department conducts compensation surveys and local market analysis to determine whether employees are compensated properly. It evaluates the structure of our compensation system to ensure that desired behavior is being incentivized properly. | | |
| We conduct annual employee surveys that seek feedback in various areas, such as our organization's strategy, customer experience, products and services, leadership, work environment, work life integration, | | |

# FRAUD CONTROL ACTIVITIES SCORECARD

| Fraud Control Activities Area, Factor, or Consideration | Score | Notes |
|---|---|---|
| opportunity and development, and transparency and distribution of information. | | |
| Our annual employee surveys include a section related to integrity within the organization in order to assess employees' knowledge of our fraud risk management program. | | |
| Our annual employee surveys assess the following attributes: <br>• Employee ability to report unethical behavior without fear of retaliation <br>• The effectiveness of our organization's responses to verified or proven unethical behavior <br>• Any observed misconduct in the past year and whether or not it was reported <br>• Employee knowledge of how to report ethical concerns or observed misconduct | | |
| We conduct exit interviews to gather information regarding the integrity of management and whether any conditions exist within the organization that may be conducive to fraud. | | |
| Our human resources managers scan resignation letters for any information regarding possible fraud and misconduct existing within our organization. | | |
| Our exit interviews include questions as to whether the former employee has witnessed any dishonest, unethical, or fraudulent conduct within our organization. | | |
| We implement segregation of duties to as great an extent as possible when selecting control activities to ensure that individuals do not have responsibility or authority for all steps in a business process. | | |
| We complement duty segregation control activities with regular rotation of duties among personnel and mandatory leave policies to deter collusion among employees. | | |
| We use data analytics procedures to isolate unusual transactions that may indicate collusion and identify employees who rarely take leave. | | |
| We ensure that an employee's level of authority is commensurate with his or her level of responsibility. | | |
| We re-evaluate authority and responsibility authorizations periodically as they may become outdated due to changes in employment status, promotions, reassignments, and terminations. | | |

# FRAUD CONTROL ACTIVITIES SCORECARD

| Fraud Control Activities Area, Factor, or Consideration | Score | Notes |
|---|---|---|
| **We implement transaction-level control procedures, including data entry edit tests, segregation of transaction-processing duties, authorization approvals, and requirements for higher-level reviews and approvals for potentially problematic transactions, such as third-party and related-party transactions and journal entries.** | | |
| **We have thorough authorization and approval controls that prevent the exploitation of third-party relationships to perpetrate fraud.** | | |
| **We examine adjustments occurring just before and just after important closing dates to determine whether they are valid and appropriate.** | | |
| **We particularly scrutinize journal entries initiated by senior managers and officials to ensure that they are not indicative of management override of controls.** | | |
| **We have adequate preventive controls in place for all transactions that can be influenced by board members and senior executives or controlled by employees with authority who have an interest in an outside organization with whom we conduct business.** | | |
| **We have a whistleblower system in place to allow for reporting of suspicions of fraud.** | | |
| **We publicize and promote our organization's whistleblower system to make our employees, management, and others well aware of its existence and effectiveness.** | | |
| **Our whistleblower system includes a multilingual capability and provides access to a trained interviewer 24 hours a day.** | | |
| **Our whistleblower system provides anonymity to any individual who comes forward to report suspicions of fraud and provides assurance to employees that they will not experience retaliation for reporting.** | | |
| **We demonstrate that reporting fraud through our whistleblower hotline results in timely action being taken.** | | |
| **To protect the integrity of the whistleblower process, we ensure that suspicions of fraud reach the appropriate level in the organization.** | | |
| **We utilize a single case management system for logging all whistleblower reports and their follow-up to facilitate management of the resolution process, testing by internal auditors, and oversight by the board or audit committee.** | | |
| **Our organization's board disseminates fraud-related reports to the appropriate parties in their respective** | | |

# FRAUD CONTROL ACTIVITIES SCORECARD

| Fraud Control Activities Area, Factor, or Consideration | Score | Notes |
|---|---|---|
| areas of responsibility to ensure that no single person or functional area controls highly sensitive information and to increase accountability. | | |
| We analyze data gathered from our whistleblower program to identify any trends, increases, or decreases in activity that may require us to restructure our fraud risk management program in order to address evolving risk. | | |
| We evaluate our whistleblower process independently and periodically for effectiveness and for compliance with privacy and information security protocols. | | |
| **CONSIDERING MANAGEMENT OVERRIDE OF CONTROLS** | | |
| Our governing board recognizes a priority to have oversight controls in place designed to hold senior management accountable and prevent instances of management override of controls. | | |
| We have adequate control activities in place to prevent improper transactions through top-side adjustments to accounting information, because journal entries present one of the easiest ways for management to circumvent controls over financial reporting. | | |
| We check for evidence of management override of controls in the application of inappropriate bias in assumptions underlying accounting estimates, unusual and fraudulent transactions occurring near period-end to meet objectives, and pressures on subordinates to initiate or participate in improper transactions or activities. | | |
| **USING PROACTIVE DATA ANALYTICS PROCEDURES** | | |
| We use data analytics procedures to examine journal entries for suspicious transactions, such as those occurring outside normal operating hours, those made in one period and reversed in the next, and those that fraudulently credit expense accounts to improve net income. | | |
| We use data analytics procedures to identify anomalous relationships among people, organizations, and events. | | |
| We proactively consider how certain fraud schemes may result in identifiable types of transactions or trends so that we can design and implement our data analytics procedures accordingly. | | |
| **DEPLOYING CONTROL ACTIVITIES THROUGH POLICIES AND PROCEDURES** | | |

# FRAUD CONTROL ACTIVITIES SCORECARD

| Fraud Control Activities Area, Factor, or Consideration | Score | Notes |
|---|---|---|
| **We formally document our fraud risk management policies and procedures, such as the control activities in place to prevent and detect fraud.** | | |
| **Our fraud documentation includes the processes used to monitor the performance of fraud control activities and indicates when these controls do not sufficiently reduced risk to an acceptable level.** | | |
| **We document the testing procedures and the results of such procedures conducted to determine that controls are present and functioning as designed.** | | |
| **The board approves a specific list of individuals who are permitted access to information and defines its own level of information access for the aspects of our fraud detection techniques we wish to keep confidential.** | | |
| **We designate and document the individuals and departments responsible for:**<br>• **Designing and planning the overall fraud prevention and detection processes**<br>• **Designing and implementing specific fraud preventive and detective controls**<br>• **Monitoring specific fraud preventive and detective controls and the overall system of these controls for realization of the process and program objectives**<br>• **Receiving and responding to all complaints related to possible fraudulent activity in a timely manner**<br>• **Investigating all reports of fraudulent activity in a timely manner**<br>• **Communicating information about suspected and confirmed fraud to appropriate parties in a timely manner**<br>• **Periodically assessing and updating the plan for changes in technology, processes and organization** | | |
| **We ensure that only personnel who are competent and have sufficient authority our fraud control activities are performed.** | | |
| **We periodically reassess our fraud control activities on a scheduled basis and with every significant organizational or operational change.** | | |
| **Our periodic reassessment of fraud control activities includes:**<br>• **Ensuring that existing fraud control activities are working as designed** | | |

# FRAUD CONTROL ACTIVITIES SCORECARD

| Fraud Control Activities Area, Factor, or Consideration | Score | Notes |
|---|---|---|
| • **Refreshing and updating the fraud risk assessment and the design of control activities**<br>• **Seeking efficiencies and filling gaps** | | |

**APPENDIX J4**

**FRAUD INVESTIGATION AND CORRECTIVE ACTION SCORECARD**

# APPENDIX J4: FRAUD INVESTIGATION AND CORRECTIVE ACTION SCORECARD

To assess the strength of the organization's fraud investigation and corrective action processes, carefully assess each area below and score the area, factor, or consideration as:

Red: indicating that the area, factor, or consideration needs substantial strengthening and improvement to bring fraud risk down to an acceptable level

Yellow: indicating that the area, factor, or consideration needs some strengthening and improvement to bring fraud risk down to an acceptable level

Green: indicating that the area, factor, or consideration is strong and that fraud risk has been reduced — at least — to a minimally acceptable level

Each area, factor, or consideration scored either red or yellow warrants having a note associated with it that describes the action plan for bringing it to green on the next scorecard.

| Fraud Investigation and Corrective Action Area, Factor, or Consideration | Score | Notes |
|---|---|---|
| **ESTABLISHING FRAUD INVESTIGATION AND RESPONSE PROTOCOLS** | | |
| **Our organizational culture promotes and supports open communication.** | | |
| **Our organization ensures that any reasonably suspected or known violation, deviation, or other breach of code of conduct, fraud, or corruption is dealt with in a timely and effective manner.** | | |
| **Our board and senior management positively encourage the identification of fraud by committing to an internal communication process.** | | |
| **Our organization stresses the importance of having a documented process in place by which allegations of fraud are to be consistently captured, assessed, and responded to in a timely manner.** | | |
| **Our fraud investigation and response system includes protocols for:**<br>• **Updating a central repository for allegations and complaints**<br>• **Maintaining anonymity or confidentiality of involved individuals, except as is necessary to investigate**<br>• **Initially evaluating the allegations to determine if an investigation is warranted and the appropriate degrees of urgency**<br>• **Notifying employees regarding document preservation and securing data systems** | | |

# FRAUD INVESTIGATION AND CORRECTIVE ACTION SCORECARD

| Fraud Investigation and Corrective Action Area, Factor, or Consideration | Score | Notes |
|---|---|---|
| • **If necessary, engaging independent counsel and forensic accounting support**<br>• **Conducting the investigation while controlling and safeguarding evidence**<br>• **Reporting the results in the appropriate format (oral summary of key points or comprehensive written report with exhibits)**<br>• **Following policies regarding retention of reports, documents, work papers, and other information**<br>• **Assessing root causes and initiating mitigating processes and controls** | | |
| **We have multiple communication paths by which allegations and complaints can be brought to the attention of our organization without naming the alleged perpetrator of fraud.** | | |
| **Our organization communicates appreciation to an employee reporting fraud, periodically updates the employee on the status of efforts to address the allegations and complaints, notifies the employee when the matter has been resolved, and thanks him or her for her input.** | | |
| **Our board ensures that our organization develops a system for prompt, competent, and confidential evaluation, investigation, and resolution of allegations and complaints involving potential fraud or misconduct.** | | |
| **The process approved by our board to follow up on allegations or complaints includes a tracking or case management system.** | | |
| **We have taken all foreign privacy laws and regulations into account when implementing international fraud reporting mechanisms for our overseas operations.** | | |
| **We designate or retain an individual or individuals with the necessary authority and skills to conduct an initial evaluation of an allegation when it is received and determine the appropriate course of action to take to resolve it.** | | |
| **We consider whether allegations of fraud involve a potential violation of laws, regulations, or company policy, and whether the allegation implicates one or more employees.** | | |
| **We advise our external auditor at the appropriate time of any alleged fraud that could affect our organization's financial statements.** | | |
| **We perform fraud investigations in accordance with protocols approved and documented by the board, which we refer to as our fraud response plan.** | | |

# FRAUD INVESTIGATION AND CORRECTIVE ACTION SCORECARD

| Fraud Investigation and Corrective Action Area, Factor, or Consideration | Score | Notes |
|---|---|---|
| Our fraud response plan is formally documented by those in charge with our organization's overall fraud management program and outlines how we receive, investigate, document, and report on fraudulent activity. | | |
| Our fraud response plan outlines our board's authority to conduct investigations independently of our organization as well as the type of allegations that senior management refers to the board. | | |
| Our fraud response plan outlines the authority of those responsible for conducting internal investigations within the organization and grants those individuals unrestricted access to all company employees and records. | | |
| Our independent investigation team evaluates each allegation and develops an appropriate investigative work plan accordingly. | | |
| Each investigation is led by an individual with sufficient authority who has been assigned the overall responsibility for the investigation. | | |
| We ensure that the responsibility for overseeing a fraud investigation resides with an individual with a level of authority at least one level higher than anyone potentially involved in the matter, or with a department that is inherently independent within the organization. | | |
| Any investigation of matters involving senior management is overseen by our board, a designated committee of our board, of an independent member of senior management designated by and reporting to the board. | | |
| The individual who is assigned overall responsibility for an investigation coordinates the investigation, interfaces with management as necessary, and clearly communicates the roles and responsibilities of each team member. | | |
| Individuals who perform investigations are competent in the subject matter of the allegation and have sufficient expertise, such as investigation skills, subject matter knowledge, industry expertise, cultural and language fluency, information systems knowledge, and data analytical skills. | | |
| Individuals who perform investigations follow applicable professional standards and are free from any conflicts of interest. | | |
| Our organization considers retaining outside expertise when our internal resources are not adequate to conduct an investigation. | | |

# FRAUD INVESTIGATION AND CORRECTIVE ACTION SCORECARD

| Fraud Investigation and Corrective Action Area, Factor, or Consideration | Score | Notes |
|---|---|---|
| **Our investigation team considers the following factors in developing each investigative work plan:**<br>• **Defined engagement scope—The scope is sufficient to develop a full understanding of the facts surrounding the allegation and provides reasonable assurance that there are no other similar instances of fraud.**<br>• **Time-sensitivity—Investigations may need to be conducted in a timely manner due to legal requirements.**<br>• **Notification—Certain events may require timely notification to regulators, law enforcement, external auditors, insurers, or legislative oversight committees.**<br>• **Confidentiality—Information gathered is kept confidential and distribution is limited to those with an established need to know.**<br>• **Legal privileges—Involving legal counsel helps safeguard work product and attorney-client communications.**<br>• **Compliance—The investigation team complies with all applicable laws and rules regarding gathering information and interviewing witnesses**<br>• **Secure evidence—The team protects the chain of custody of evidence.**<br>• **Goals—Specific issues or concerns appropriately influence the focus, scope and timing of the investigation.** | | |
| **For international investigations, our investigation team considers the laws and regulations of the country, customary business practices, the native language and potential communication barriers, transportation, and other logistics.** | | |
| **We engage independent outside counsel as advised who then engage other experts as necessary, either from within or outside our company.** | | |
| **CONDUCTING INVESTIGATIONS** | | |
| **We conduct investigations with integrity and objectivity and in accordance with all applicable professional standards.** | | |
| **The investigation team establishes investigation tasks as outlined in the investigation work plan and assigns each task to the appropriate team members.** | | |
| **The investigation work plan prioritizes the performance of tasks to provide an interim report of findings, if necessary, and to revise or plan next steps.** | | |
| **The investigation team considers legal issues and constraints in dealing with employees and third parties,** | | |

# FRAUD INVESTIGATION AND CORRECTIVE ACTION SCORECARD

| Fraud Investigation and Corrective Action Area, Factor, or Consideration | Score | Notes |
|---|---|---|
| obtains relevant information, and develops related documentation, which requires seeking assistance from the courts and monitoring integrity of investigation results. | | |
| The investigation team modifies the investigation work plan as necessary to increase, decrease, or modify the investigation's scope and tasks based on facts as they are uncovered. | | |
| Our investigations generally include many of the following procedures:<br><br>• Gathering evidence and performing analysis, including<br>   o Reviewing and categorizing information collected<br>   o Performing computer-assisted data analysis<br>   o Developing and testing hypotheses<br>• Gathering external records from public records, customers, vendors, and others, including media reports<br>• Examining computer forensics to collect evidence from internal sources consisting of hard copy and electronically stored information residing in servers, computers, personal and company phones, printers and other devices, building access logs and physical security cameras, and IT system records<br>• Interviewing peripheral witnesses and proceeding to the target or subject of the investigation | | |
| The investigation team documents and tracks information related to steps of the investigation, including:<br>• Privileged or confidential items<br>• Requests for documents, electronic data, and other information<br>• Memoranda of interviews conducted<br>• Analyses of documents, data, and interviews and conclusions drawn | | |
| The investigation team evaluates the root cause of issues in the event that an allegation is substantiated during an investigation. | | |
| **COMMUNICATING INVESTIGATION RESULTS** | | |
| If a third-party is engaged to conduct the investigation, the investigation report prepared by the third-party is delivered to the employee within our organization that engaged the services of the third-party. | | |

# FRAUD INVESTIGATION AND CORRECTIVE ACTION SCORECARD

| Fraud Investigation and Corrective Action Area, Factor, or Consideration | Score | Notes |
| --- | --- | --- |
| **If the investigation report is generated internally, it is delivered to the individuals charged with oversight of the investigation.** | | |
| **Our investigation reports are accurate, clear, and impartial, present only relevant facts, and are timely in their preparation and delivery.** | | |
| **Our investigation reports generally include the following elements:**<br><br>• **Executive summary**<br>• **Background investigation on the matter under investigation**<br>• **Investigation procedures performed**<br>• **Findings and recommendations, which may include remediation**<br>• **Appendices or exhibits** | | |
| **We obtain the advice of legal counsel prior to making public statements or other communications regarding an investigation.** | | |
| **We determine whether investigation results will be discussed with individuals who provided information to our organization on a case-by-case basis and continue to reinforce the confidential nature of such information.** | | |
| **The investigation team seeks feedback from individuals who provided our organization with information on whether the matter was dealt with reasonably, objectively, and appropriately.** | | |
| **TAKING CORRECTIVE ACTION** | | |
| **The investigation team reports any significant findings of actual or potential material impact to the board, the audit committee, and to both the internal and external auditor.** | | |
| **We determine if it is necessary to notify the public, law enforcement, regulatory agencies, legislative oversight committees, and our organization's insurers of significant findings after the completion of an investigation.** | | |
| **Upon completing an investigation, any action we take is appropriate in the circumstances, applied consistently to all levels of employees, and taken only after consultation with individuals responsible for such decisions.** | | |
| **Our board is notified of the nature, timing, and status of any remediation plans.** | | |
| **The investigation team makes a report to the board about the achievement of remediation of issues related to training,** | | |

# FRAUD INVESTIGATION AND CORRECTIVE ACTION SCORECARD

| Fraud Investigation and Corrective Action Area, Factor, or Consideration | Score | Notes |
|---|---|---|
| business processes, and internal control deficiencies. | | |
| Management consults with legal counsel before taking any disciplinary, civil, or criminal action. | | |
| We choose amongst the following courses of corrective action:<br><br>• **Internal control remediation**—Our organization may enhance certain internal controls to reduce the risk of similar frauds going undetected in the future<br>• **Business process remediation**—We may be able to re-engineer business processes cost-effectively to reduce or remove the opportunity for similar frauds in the future<br>• **Disciplinary action**—We may choose to terminate, suspend, demote, or warn perpetrators of fraud<br>• **Training**—We may need to provide education about our policies and procedures to enhance awareness of ethical business practices and requirements<br>• **Insurance claim**—We may be able to pursue a claim for some or all of our losses<br>• **Extended investigation**—We may conduct a root cause analysis and perform an extended investigation to help identify similar misconduct occurring elsewhere in our organization<br>• **Civil action**—We may pursue our own civil action against perpetrators to recover lost assets and investigation expenses<br>• **Criminal action**—We may choose to refer the case to law enforcement or be required to do so | | |
| We ensure that our response to an investigation is strong, clear and consistent and that it embodies the values of our organization and good corporate conduct. | | |
| **EVALUATING INVESTIGATION PERFORMANCE** | | |
| The performance metrics used to evaluate the efficiency and effectiveness of our investigation process are tailored to the scope, scale, and complexity of the fraud investigation at hand. | | |
| We consider applying the following performance metrics to evaluate the efficiency and effectiveness with which we conduct our investigations:<br>• **Resolution time**—Average number of days to resolve an issue<br>• **Investigation cost**—Resource hours and external spending | | |

# FRAUD INVESTIGATION AND CORRECTIVE ACTION SCORECARD

| Fraud Investigation and Corrective Action Area, Factor, or Consideration | Score | Notes |
|---|---|---|
| • **Repeat incidents—Number of current-period incidents that are similar in nature to incidents in earlier periods**<br>• **Incident location—Number of incidents in a specific business unit, operational area, or geography**<br>• **Value of losses recovered and future losses prevented**<br>• **Corrective actions—Type of remedial action taken and implementation date** | | |

**APPENDIX J5**

**FRAUD RISK MANAGEMENT MONITORING SCORECARD**

# APPENDIX J5: FRAUD RISK MANAGEMENT MONITORING SCORECARD

To assess the strength of the organization's fraud risk management monitoring, carefully assess each area below and score the area, factor, or consideration as:

Red: indicating that the area, factor, or consideration needs substantial strengthening and improvement to bring fraud risk down to an acceptable level

Yellow: indicating that the area, factor, or consideration needs some strengthening and improvement to bring fraud risk down to an acceptable level

Green: indicating that the area, factor, or consideration is strong and that fraud risk has been reduced — at least — to a minimally acceptable level

Each area, factor, or consideration scored either red or yellow warrants a note associated with it that describes the action plan for bringing it to green on the next scorecard.

| Fraud Risk Management Monitoring Area, Factor, or Consideration | Score | Notes |
|---|---|---|
| **CONSIDERING A MIX OF ONGOING AND SEPARATE EVALUATIONS** | | |
| **Our organization performs ongoing evaluations that monitor control activities on a real-time basis as a routine process.** | | |
| **Our organization's fraud risk management monitoring plan targets our areas of highest fraud risk.** | | |
| **Our monitoring activities focus on these aspects of the analysis performed: "Why," "Who," "What," "Where," and "What's next?"** | | |
| **Our ongoing monitoring activities include data analytics procedures used to form conclusions about information collected.** | | |
| **Our organization performs separate evaluations to help assure management that our fraud risk management program is functioning as designed.** | | |
| **Our separate evaluations of controls occur periodically and are not part of our organization's routine operations.** | | |
| **Our separate evaluations are performed by internal audit, others within the organization, or third parties (outsourcers).** | | |

# FRAUD RISK MANAGEMENT MONITORING SCORECARD

| Fraud Risk Management Monitoring Area, Factor, or Consideration | Score | Notes |
|---|---|---|
| **We document our plan, approach, and scope for monitoring our organization's fraud risk management program.** | | |
| **Our organization's plan for monitoring our fraud risk management program includes a balance of ongoing and separate evaluations deemed appropriate to assist management in its evaluation of whether each of the five principles of fraud risk management is present and functioning in its fraud risk management program.** | | |
| **We modify our overall fraud risk management program as necessary to account for significant changes in our organization or our operating environment that increase or change the risk of fraud.** | | |
| **CONSIDERING FACTORS FOR SETTING THE SCOPE AND FREQUENCY OF EVALUATIONS** | | |
| **Our management considers the factors affecting the scope of ongoing and separate evaluations prior to performing each evaluation, or periodically, and alters the scope of the evaluations as necessary based on the assessment.** | | |
| **We consider factors that affect the scope of evaluations, such as significant changes in the fraud risks of our organization, operating environment changes, changes in personnel responsible for implementing activities that could exacerbate or create new fraud risks, and results of previous fraud risk assessments, including evaluations of measurement criteria.** | | |
| **ESTABLISHING APPROPRIATE MEASUREMENT CRITERIA** | | |
| **We have established measurement criteria to monitor and improve fraud prevention and detection, such as:**<br>• **Number of fraud schemes, known fraud schemes committed against the organization, fraud allegations received requiring investigation, and fraud investigations resolved**<br>• **Number of fraud allegations received via our organization's fraud hotline or by other means**<br>• **Number of employees who have not signed our corporate ethics policy or completed our corporate-sponsored ethics training**<br>• **Number of interactions between employees and stakeholders concerning ethics and organizational culture** | | |

# FRAUD RISK MANAGEMENT MONITORING SCORECARD

| Fraud Risk Management Monitoring Area, Factor, or Consideration | Score | Notes |
|---|---|---|
| • **Number of vendors and customers who have not agreed to our organization's ethical terms and requirements**<br>• **Number of background checks performed and number of problems identified in background checks** | | |
| **We provide the measurement criteria established to monitor and improve fraud prevention and detection to our organization's leadership on an ongoing basis.** | | |
| **We consider using benchmarks from global fraud surveys and resources dedicated by our organization to fraud risk management as metrics to assist us in determining appropriate measurement criteria to monitor and improve fraud prevention and detection.** | | |
| **We consider using our established measurement criteria to perform the following analyses:**<br>• **Comparison of number of frauds identified versus the complaints, grievances, etc., received via hotline calls**<br>• **Comparison of frauds identified versus types of frauds previously uncovered**<br>• **Comparison of the number of frauds discovered versus the number of fraud examinations performed**<br>• **Ratios of problems revealed in background checks versus the number of checks performed** | | |
| **CONSIDERING KNOWN FRAUD SCHEMES AND NEW FRAUD CASES** | | |
| **Our organization takes into consideration known fraud schemes and new frauds discovered and reported in other industries and in other organizations in the same industry.** | | |
| **We closely monitor emerging fraud cases and determine whether our organization is protected against such frauds to ensure that our fraud risk management program remains current in the face of evolving fraud risks.** | | |
| **We study industry information and benchmarks that may provide us with sufficient information to assist management in assessing the likelihood that existing fraud schemes perpetrated against other organizations in the same industry will occur.** | | |
| **EVALUATING, COMMUNICATING, AND REMEDIATING DEFICIENCIES** | | |

# FRAUD RISK MANAGEMENT MONITORING SCORECARD

| Fraud Risk Management Monitoring Area, Factor, or Consideration | Score | Notes |
|---|---|---|
| **Our senior management and board of directors assess the results of ongoing and separate evaluations.** | | |
| **Communications about identified deficiencies in the fraud risk management program are received by those responsible for taking corrective action, senior management, and the board of directors.** | | |
| **Our management tracks whether deficiencies identified in our fraud risk management program are remediated on a timely basis and takes further action if necessary.** | | |
| **The overall responsibility for our fraud risk management program resides with a senior member of management.** | | |
| **We assign the fraud risk management principles and related fraud control activities individually to other senior members of management.** | | |
| **We ensure that each person responsible for fraud risk management principles and related fraud control activities:**<br>• **Evaluates regularly whether the fraud risk management principles and their related fraud control activities are present and functioning**<br>• **Modifies fraud risk management principles and their related fraud control activities as required and documents any necessary modifications**<br>• **Reports immediately, through the appropriate channels, details of any modifications necessary or any fraud risk management principles or related control activities that no longer exist in reducing residual fraud risk to an acceptable level in accordance with our organization's risk tolerance** | | |
| **Each of our evaluations includes evidence that our management is actively retaining responsibility for oversight of our fraud risk management program, taking timely and sufficient corrective action with respect to any identified fraud control deficiencies or weaknesses, and ensuring that the plan for monitoring our fraud risk management program continues to be adequate for ongoing success.** | | |