SAMPLE FRAMEWORK FOR A FRAUD CONTROL POLICY

NOTE: This appendix is a sample from another entity. As such, no adjustment has been made to this material. The information may or may not agree with all the concepts noted within this paper. The material is being provided as an example that may be a used as a tool, reference, or starting point.

1. EXECUTIVE

SUMMARY Definition of

fraud
Statement of attitude to fraud
Code of conduct (relationship to)
Relationship with entity's other plans
Roles and accountabilities

2. SUMMARY OF FRAUD CONTROL

STRATEGIES Appointment of fraud control

officer
External assistance to the fraud control officer
Fraud control responsibilities
Fraud risk management (including fraud risk assessment) Fraud awareness
Fraud detection
Fraud reporting
Investigation of fraud and other improper conduct
Internal control review following discovery of fraud
Fidelity guarantee and criminal conduct insurance
Internal audit program

3. FRAUD RISK MANAGEMENT

Regular program for fraud risk assessment Ongoing review of fraud control strategies Fraud risk assessment
Implementation of proposed actions

4. PROCEDURES FOR REPORTING

FRAUD Internal reporting

Reports by members of staff
Protection of employees reporting suspected fraud
External anonymous reporting
Reports to the police
Reports to external parties
Administrative remedies
Recovery of the proceeds of fraudulent
conduct Reporting requirements

5. EMPLOYMENT CONDITIONS

Pre-employment screening
Annual leave

6. CONFLICT OF INTEREST

The impact of conflicts of interest
Register of interests
Conflict of interest policy

7. PROCEDURES FOR FRAUD

INVESTIGATION Internal investigations
External investigative resources
Documentation of the results of the investigation

8. INTERNAL AUDIT

STRATEGY Internal audit

capability
Internal audit fraud control function

9. REVIEW OF FRAUD CONTROL ARRANGEMENTS

SAMPLE FRAUD POLICY

NOTE: This appendix is a sample from another entity. As such, no adjustment has been made to this material. The information may or may not agree with all the concepts noted within this paper. The material is being provided as an example that may be a used as a tool, reference, or starting point.

BACKGROUND

The corporate fraud policy is established to facilitate the development of controls that will aid in the detection and prevention of fraud against ABC Corporation. It is the intent of ABC Corporation to promote consistent organizational behavior by providing guidelines and assigning responsibility for the development of controls and conduct of investigations.

SCOPE OF POLICY

This policy applies to any irregularity, or suspected irregularity, involving employees as well as shareholders, consultants, vendors, contractors, outside agencies doing business with employees of such agencies, and/or any other parties with a business relationship with ABC Corporation (also called the Company).

Any investigative activity required will be conducted without regard to the suspected wrongdoer's length of service, position/title, or relationship to the Company.

POLICY

Management is responsible for the detection and prevention of fraud, misappropriations, and other irregularities. *Fraud* is defined as the intentional, false representation or concealment of a material fact for the purpose of inducing another to act upon it to his or her injury. Each member of the management team will be familiar with the types of improprieties that might occur within his or her area of responsibility and be alert for any indication of irregularity.

Any irregularity that is detected or suspected must be reported immediately to the Director of_____, who coordinates all investigations with the Legal Department and other affected areas, both internal and external.

ACTIONS not CONSTITUTING FRAUD

The terms *defalcation, misappropriation,* and *other fiscal irregularities* refer to, but are limited to:

- Any dishonest or fraudulent act.
- Misappropriation of funds, securities, supplies, or other assets.
- Impropriety in the handling or reporting of money or financial transactions.
- Profiteering as a result of insider knowledge of company activities.
- Disclosing confidential and proprietary information to outside parties.
- Disclosing to other persons securities activities engaged in or contemplated by the company.
- Accepting or seeking anything of material value from contractors, vendors, or persons providing services/materials to the Company. Exception: Gifts less than US

$50 in value.

- Destruction, removal, or inappropriate use of records, furniture, fixtures, and equipment.
- Any similar or related irregularity.

OTHER IRREGULARITIES

Irregularities concerning an employee's moral, ethical, or behavioral conduct should by resolved by departmental management and the Employee Relations Unit of Human Resources rather than the _____ Unit.

If there is any question as to whether an action constitutes fraud, contact the Director of _____ for guidance.

INVESTIGATION RESPONSIBILITIES

The _____ Unit has the primary responsibility for the investigation of all suspected fraudulent acts as defined in the policy. If the investigation substantiates that

fraudulent activities have occurred, the _____ Unit will issue reports to appropriate designated personnel and, if appropriate, to the Board of Directors through the Audit Committee.

Decisions to prosecute or refer the examination results to the appropriate law enforcement and/or regulatory agencies for independent investigation will be made in conjunction with legal counsel and senior management, as will final decisions on disposition of the case.

CONFIDENTIALITY

The _____ Unit treats all information received confidentially. Any employee who suspects dishonest or fraudulent activity will notify the _____ Unit immediately, and should not attempt to personally conduct investigations or interviews/ interrogations related to any suspected fraudulent act (see Reporting Procedures section below).

Investigation results will not be disclosed or discussed with anyone other than those who have a legitimate need to know. This is important in order to avoid damaging the reputations of persons suspected but subsequently found innocent of wrongful conduct and to protect the Company from potential civil liability.

AUTHORIZATION FOR INVESTIGATING SUSPECTED FRAUD

Members of the Investigation Unit will have:

- Free and unrestricted access to all Company records and premises, whether owned or rented.
- The authority to examine, copy, and/or remove all or any portion of the contents of files, desks, cabinets, and other storage facilities on the premises without prior knowledge or consent of any individual who might use or have custody of any such items or facilities when it is within the scope of their investigation.

REPORTING PROCEDURES

Great care must be taken in the investigation of suspected improprieties or irregularities so as to avoid mistaken accusations or alerting suspected individuals that an investigation is under way.

An employee who discovers or suspects fraudulent activity will contact the _____Unit immediately. The employee or other complainant may remain anonymous. All inquiries concerning the activity under investigation from the suspected individual, his or her attorney or representative, or any other inquirer should be directed to the Investigations Unit or the Legal Department. No information concerning the status of an investigation will be given out. The proper response to any inquiries is: "I am not at liberty to discuss this matter." Under no circumstances should any reference be made to "the allegation," "the crime," "the fraud," "the forgery," "the misappropriation," or any other specific reference.

The reporting individual should be informed of the following:

- Do not contact the suspected individual in an effort to determine facts or demand restitution.
- Do not discuss the case, facts, suspicions, or allegations with anyone unless specifically asked to do so by the Legal Department or_____Unit.

TERMINATION

If an investigation results in a recommendation to terminate an individual, the recommendation will be reviewed for approval by the designated representatives from Human Resources and the Legal Department and, if necessary, by outside counsel, before any such action is taken. The_____Unit does not have the authority to terminate an employee. The decision to terminate an employee is made by the employee's management. Should the_____Unit believe the management decision inappropriate for the facts presented, the facts will be presented to executive-level management for a decision.

ADMINISTRATION

The Director of_____is responsible for the administration, revision, interpretation, and application of this policy. The policy will be reviewed annually and revised as needed.

APPROVAL

(CEO/Senior Vice President/Executive) Date

SAMPLE FRAUD RESPONSIBILITY MATRIX

NOTE: This matrix can be used as a tool to summarize and visualize the responsibilities that have been defined for the organization. This is not a standard for "who" should have "what" responsibilities.

Action Required	Investigation Unit	Internal Auditing	Finance Acctg.	Exec Mgmt.	Line Mgmt.	Risk Mgmt.	PR	Employee Relations	Legal
1. Controls to Prevent Fraud	S	S	S	P	SR	S	S	S	S
2. Incident Reporting	P	S	S	S	S	S	S	S	S
3. Investigation of Fraud	P	S						S	S
4. Referrals to Law Enforcement	P								S
5. Recovery of Monies Due to Fraud	P								
6. Recommendations to Prevent Fraud	SR	SR	S	S	S	S	S	S	S
7. Internal Control Reviews		P							
8. Handle Cases of a Sensitive Nature	P	S		S		S		S	S
9. Publicity/Press Releases	S	S					P		
10. Civil Litigation	S	S							P
11. Corrective Action/ Recommendations to Prevent Recurrences	SR	SR		S	SR	S			S
12. Monitor Recoveries	S		P						
13. Proactive Fraud Auditing	S	P							
14. Fraud Education/ Training	P	S			S		S		
15. Risk Analysis of Areas of Vulnerability	S	S				P			
16. Case Analysis	P	S							
17. Hotline	P	S							
18. Ethics Line	S	S							P

p (primary responsibility) S (Secondary responsibility) Sr (Shared responsibility)

FRAUD RISK ASSESSMENT FRAMEWORK SAMPLE

NOTE: This example is for illustrative purposes and focuses solely on potential revenue recognition risks within financial reporting. A full fraud risk assessment would consider fraudulent financial reporting in other areas relevant to the organization, such as accounts subject to estimation, related-party transactions, and inventory accounting. In addition, the risk of misappropriation of assets, corruption, and other misconduct would be assessed in the same manner.

identified Fraud risks and Schemes (1)	Likelihood (2)	Significance (3)	people and/or Department (4)	existing anti-fraud Controls (5)	Controls effectiveness assessment (6)	residual risks (7)	Fraud risk response (8)
Financial Reporting Revenue recognition • Backdating agreements	Reasonably possible	Material	Sales personnel	Controlled contract administration system	Tested by IA	N/A	Periodic testing by IA
• Channel stuffing	Remote	Insignificant	N/A	N/A	N/A	N/A	N/A
• Holding books open	Reasonably possible	Material	Accounting	Standard monthly close process Reconciliation of invoice register to general ledger Established procedures for shipping, invoicing, and revenue recognition Established process for consolidation	Tested by IA Tested by management Tested by IA Tested by IA	Risk of management override	Testing of late journal entries Cut off testing by IA
• Late shipments	Reasonably possible	Significant	Shipping dept.	Integrated shipping system, linked to invoicing and sales register Daily reconciliation of shipping log to invoice register Required management approval of manual invoices	Tested by IA Tested by management Tested by IA	Risk of management override	Cut off testing by IA
• Side letters/ agreements	Probable	Material	Sales personnel	Annual training of sales and finance personnel on revenue recognition practices Quarterly signed attestation of sales personnel concerning extra contractual agreements Internal audit confirming with customers that there are no other agreements, written or oral, that would modify the terms of the written agreement	Tested by management Tested by management	Risk of override	Disaggregated analysis of sales, sales returns, and adjustments by salesperson

• Inappropriate journal entries	Reasonably possible	Material	Accounting & Finance	Established process for consolidation Established, systematic access controls to the general ledger Standard monthly and quarterly journal entry log maintained. Review process in place for standard entries, and nonstandard entries subject to two levels of review	Tested by IA Tested by IA Tested by management	Risk of override N/A N/A	Data mining of journal entry population by IA for: • Unusual Dr/CR combinations • Late entries to accounts subject to estimation

identified Fraud risks and Schemes (1)	Likelihood (2)	Significance (3)	people and/or Department (4)	existing anti-fraud Controls (5)	Controls effectiveness assessment (6)	residual risks (7)	Fraud risk response (8)
• Roundtrip transactions	Remote	Insignificant	N/A	N/A	N/A	N/A	N/A
• Manipulation of bill and hold arrangements	Remote	Insignificant	N/A	N/A	N/A	N/A	N/A
• Early delivery of product	Reasonably possible	Significant	Sales and shipping	Systematic matching of sales order to shipping documentation; exception reports generated.	Tested by management	Adequately mitigated by controls	N/A
• Partial shipments	Reasonably possible	Significant	Sales and shipping	Systematic shipping documents manually checked against every shipment. Systematic matching of sales order to shipping documentation; exception reports generated. Customer approval of partial shipment required prior to revenue recognition.	Tested by management	Adequately mitigated by controls	N/A
• Additional revenue risks				Systematic shipping documents manually checked against every shipment.			

1. Identified Fraud Risks and Schemes: This column should include a full list of the potential fraud risks and schemes that may face the organization. This list will be different for different organizations and should be informed by (a) industry research, (b) interviews of employees and other stakeholders, (c) brainstorming sessions, and (d) activity on the whistleblower hotline.
2. Likelihood of Occurrence: To design an efficient fraud risk management program, it is important to assess the likelihood of the identified fraud risks so that the organization establishes proper anti-fraud controls for the risks that are deemed most likely. For purposes of the assessment, it should be adequate to evaluate the likelihood of risks as remote, reasonably possible, and probable.
3. Significance to the Organization: Quantitative and qualitative factors should be considered when assessing the significance of fraud risks to an organization. For example, certain fraud risks may only pose an immaterial direct financial risk to the organization, but could greatly impact its reputation, and therefore, would be deemed to be a more significant risk to the
organization. For purposes of the assessment, it should be adequate to evaluate the significance of risks as immaterial, significant, and material.
4. People and/or Department Subject to the Risk: As fraud risks are identified and assessed, it is important to evaluate which people inside and outside the organization are subject to the risk. This knowledge will assist the organization in tailoring its fraud risk response, including establishing appropriate segregation of duties, proper review and approval chains of

authority, and proactive fraud auditing procedures.

5. Existing Anti-fraud Internal Controls: Map pre-existing controls to the relevant fraud risks identified. Note that this occurs after fraud risks are identified and assessed for likelihood and significance. By progressing in this order, this framework intends for the organization to assess identified fraud risks on an inherent basis, without consideration of internal controls.
6. Assessment of Internal Controls Effectiveness: The organization should have a process in place to evaluate whether the identified controls are operating effectively and mitigating fraud risks as intended. Companies subject to the provisions of The U.S. Sarbanes- Oxley Act of 2002 Section 404 will have a process such as this in place. Organizations not subject to Sarbanes-Oxley should consider what review and monitoring procedures would be appropriate to implement to gain assurance that their internal control structure is operating as intended.
7. Residual Risks: After consideration of the internal control structure, it may be determined that certain fraud risks may not be mitigated adequately due to several factors, including (a) properly designed controls are not in place to address certain fraud risks or (b) controls identified are not operating effectively. These residual risks should be evaluated by the organization in the development of the fraud risk response.
8. Fraud Risk Response: Residual risks should be evaluated by the organization and fraud risk responses should be designed to address such remaining risk. The fraud risk response could be one or a combination of the following: (a) implementing additional controls, (b) designing proactive fraud auditing techniques, and/or (c) reducing the risk by exiting the activity.

FRAUD RISK EXPOSURES

NOTE: This appendix is a sample from another entity. As such, no adjustment has been made to this material. The information may or may not agree with all the concepts noted within this paper. The material is being provided as an example that may be a used as a tool, reference, or starting point.

The following illustrates the types of frauds an organization might encounter. This listing is not meant to be all-inclusive but to provide a starting point for an organization to identify which areas are vulnerable to fraud. More attention will be needed to identify specific industry, location, and cultural factors that can influence fraudulent behavior. Once identified, the fraud risk assessment framework shown in Appendix D could be used[43].

1) Intentional manipulation of financial statements can lead to:
    a) Inappropriately reported revenues
        (1) Fictitious revenues
        (2) Premature revenue recognition
        (3) Contract revenue and expense recognition
    b) Inappropriately reported expenses
        (1) Period recognition of expenses
    c) Inappropriately reflected balance sheet amounts, including reserves
        (1) Improper asset valuation
            (a) Inventory
            (b) Accounts receivable
            (c) Mergers and acquisitions
            (d) Capitalization of intangible items
        (2) Misclassification of assets
        (3) Inappropriate depreciation methods
        (4) Concealed liabilities and expenses
            (a) Omission
            (b) Sales returns and allowances and warranties
            (c) Capitalization of expenses
            (d) Tax liability
    d) Inappropriately improved and/or masked disclosures
        (1) Liabilities omissions
        (2) Subsequent events
        (3) Related-party transactions
        (4) Accounting changes
        (5) Management frauds uncovered
        (6) Backdating transactions
    e) Concealing misappropriation of assets
    f) Concealing unauthorized receipts and expenditures
    g) Concealing unauthorized acquisition, disposition, and use of assets

2) Misappropriation of:
    a) Tangible assets by
        (1) Cash theft
            (a) Sales register manipulation
            (b) Skimming
            (c) Collection procedures
            (d) Understated sales
            (e) Theft of checks received
            (f) Check for currency substitution
            (g) Lapping accounts
            (h) False entries to sales account
            (i) Inventory padding
            (j) Theft of cash from register
            (k) Deposit lapping
            (l) Deposits in transit
        (2) Fraudulent disbursements
            (a) False refunds
            (b) False voids
            (c) Small disbursements
            (d) Check tampering
            (e) Billing schemes
            (f) Personal purchases with company funds
            (g) Returning merchandise for cash
        (3) Payroll fraud
            (a) Ghost employees
            (b) Falsified hours and salary
            (c) Commission sales
        (4) Expense reimbursement
            (a) Mischaracterized expenses
            (b) Overstated expenses
            (c) Fictitious expenses
            (d) Multiple reimbursements
        (5) Loans
            (a) Loans to nonexistent borrowers
            (b) Double pledged collateral
            (c) False application information
            (d) Construction loans
        (6) Real estate
            (a) Appraisal value
            (b) Fraudulent appraisal
        (7) Wire transfer
            (a) System password compromise

(b) Forged authorizations
(c) Unauthorized transfer account
(d) ATM

(8) Check and credit card fraud
(a) Counterfeiting checks
(b) Check theft
(c) Stop payment orders
(d) Unauthorized or lost credit cards
(e) Counterfeit credit cards
(f) Mail theft

(9) Insurance fraud
(a) Dividend checks
(b) Settlement checks
(c) Premium
(d) Fictitious payee
(e) Fictitious death claim
(f) Underwriting misrepresentation
(g) Vehicle insurance — staged accidents
(h) Inflated damages
(i) Rental car fraud

(10) Inventory
(a) Misuse of inventory
(b) Theft of inventory
(c) Purchasing and receiving falsification
(d) False shipments
(e) Concealing inventory shrinkage

b) Intangible assets
(1) Theft of intellectual property
(a) Espionage
(b) Loss of information
(c) Spying
(d) Infiltration
(e) Informants
(f) Trash and waste disposal
(g) Surveillance
(2) Customers
(3) Vendors
c) Proprietary business opportunities

3) Corruption including:
a) Bribery and gratuities to
(1) Companies
(2) Private individuals
(3) Public officials

b) Embezzlement
    (1) False accounting entries
    (2) Unauthorized withdrawals
    (3) Unauthorized disbursements
    (4) Paying personal expenses from bank funds
    (5) Unrecorded cash payments
    (6) Theft of physical property
    (7) Moving money from dormant accounts
c) Receipt of bribes, kickbacks, and gratuities
    (1) Bid rigging
    (2) Kickbacks
        (a) Diverted business to vendors
        (b) Over billing
    (3) Illegal payments
        (a) Gifts
        (b) Travel
        (c) Entertainment
        (d) Loans
        (e) Credit card payments for personal items
        (f) Transfers for other than fair value
        (g) Favorable treatment
    (4) Conflicts of interest
        (a) Purchases
        (b) Sales
        (c) Business diversion
        (d) Resourcing
        (e) Financial disclosure of interest in vendors
        (f) Ownership interest in suppliers
d) FCPA violations
    (1) Anti-bribery provisions
    (2) Books and records violations
    (3) Internal control weaknesses
e) Money laundering
f) Aiding and abetting fraud by other parties (customers, vendors)

The *Fraud Risk Manual* issued by the ACFE, 2007.

For a sample list of fraud schemes and potential controls to be installed to combat the fraud, see Appendix 8 of *Managing the Risk of Fraud: A Guide for Managers* by HM Treasury, in Appendix A of this paper.

FRAUD PREVENTION SCORECARD

To assess the strength of the organization's fraud prevention system, 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 fraud risk has been reduced — at least — to a minimally acceptable level.

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

Fraud Prevention Area, Factor, or Consideration	Score	Notes
Our organizational culture — tone at the top — is as strong as it can possibly be and establishes a zero-tolerance environment with respect to fraud.		
Our organization's top management consistently displays the appropriate attitude regarding fraud prevention and encourages free and open communication regarding ethical behavior.		
Our Code of Organizational Conduct has specific provisions that address and prohibit inappropriate relationships whereby members of our board or members of management could use their positions for personal gain or other inappropriate purposes.		
We have done a rigorous fraud risk assessment using the COSO *Enterprise Risk Management–Integrated Framework* and have taken specific actions to strengthen our prevention mechanisms as necessary.		
We have assessed fraud risk for our organization adequately based on evaluations of similar organizations in our industry, known frauds that have occurred in similar organizations, in-house fraud brainstorming, and periodic reassessments of risk.		
We have addressed the strengths and weaknesses of our internal control environment adequately and have taken specific steps to strengthen the internal control structure to help prevent the occurrences of fraud.		

Fraud Prevention Area, Factor, or Consideration	Score	Notes
Our organizational structure contains no unnecessary entities that might be used for inappropriate purposes or that might enable less-than-arms-length transactions or relationships.		
We have assessed all overseas and decentralized operations carefully and have taken proactive steps to ensure that they have fraud preventive controls in place to conform with the strictest legal standards and highest ethical principles.		
We have divested our organization of all unnecessary third-party and related-party relationships.		
For any remaining third-party and related-party relationships, we have taken positive measures to ensure that such relationships do not allow opportunities for frauds to occur without detection.		
We have assessed the alignment of authorities and responsibilities at all levels of organization management and are not aware of any misalignments that might represent vulnerabilities to fraud.		
Our audit committee has taken a very proactive posture with respect to fraud prevention.		
Our audit committee is composed only of independent directors and includes persons with financial accounting and reporting expertise.		
Our audit committee meets at least quarterly and devotes substantial time to assessing fraud risk and proactively implementing fraud preventive mechanisms.		
We have a strong internal audit department (if applicable) that functions independently of management. The charter of our internal audit department expressly states that the internal audit team will help prevent and detect fraud and misconduct.		
We have designated an individual with the authority and responsibility for overseeing and maintaining our fraud prevention programs, and have given this individual the resources needed to manage our fraud prevention programs effectively. This individual has direct access to the audit committee.		

Fraud Prevention Area, Factor, or Consideration	Score	Notes
Our human resources department conducts background investigations with the specific objective of assuring that persons with inappropriate records or characters inconsistent with our corporate culture and ethics are identified and eliminated from the hiring process.		
Our human resources department conducts background investigations with respect to promotions or transfers into positions of responsibility.		
Personnel involved in the financial reporting process have been assessed with regard to their competencies and integrity and have been found to be of the highest caliber.		
All of our employees, vendors, contractors, and business partners have been made aware of our zero-tolerance policies related to fraud and are aware of the appropriate steps to take in the event that any evidence of possible fraud comes to their attention.		
We have a rigorous program for communicating our fraud prevention policies and procedures to all employees, vendors, contractors, and business partners.		
We have policies and procedures in place for authorization and approvals of certain types of transactions and for certain values of transactions to help prevent and detect the occurrences of fraud.		
Our performance measurement and evaluation process includes an element specifically addressing ethics and integrity as well as adherence to the Code of Organizational Conduct.		
All new hires must undergo rigorous ethics and fraud awareness and fraud prevention training.		
All employees must attend periodic (at least annual) ethics and fraud awareness and fraud prevention training, and the effectiveness of this training is affirmed through testing.		
Terminated, resigning, or retiring employees participate in an exit interview process designed to identify potential fraud and vulnerabilities to fraud that may be taking place in our organization. A specific focus of these interviews is an assessment of management's integrity and adherence to the Code of Organizational Conduct. All concerns resulting from these interviews are communicated to our audit committee.		

Fraud Prevention Area, Factor, or Consideration	Score	Notes
We have an effective whistleblower protection program and fraud hotline in place, and its existence and procedures are known to all employees, vendors, contractors, and business partners.		
We review the above fraud preventive mechanisms on an ongoing basis and document these reviews as well as the communication with the audit committee regarding areas that need improvement.		
We have a fraud response plan in place and know how to respond if a fraud allegation is made. The fraud response plan considers: • Who should perform the investigation. • How the investigation should be performed. • When a voluntary disclosure to the government should be made. • How to determine the remedial action. • How to remedy control deficiencies identified. • How to administer disciplinary action.		

FRAUD DETECTION SCORECARD

To assess the strength of the organization's fraud detection system, 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 fraud risk has been reduced — at least — to a minimally acceptable level.

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

Fraud Prevention Area, Factor, or Consideration	Score	Notes
We have integrated our fraud detection system with our fraud prevention system in a cost-effective manner.		
Our fraud detection processes and techniques pervade all levels of responsibility within our organization, from the board of directors and audit committee, to managers at all levels, to employees in all areas of operation.		
Our fraud detection policies include communicating to employees, vendors, and stakeholders that a strong fraud detection system is in place, but certain critical aspects of these systems are not disclosed to maintain the effectiveness of hidden controls.		
We use mandatory vacation periods or job rotation assignments for employees in key finance and accounting control positions.		
We periodically reassess our risk assessment criteria as our organization grows and changes to make sure we are aware of all possible types of fraud that may occur.		
Our fraud detection mechanisms place increased focus on areas in which we have concluded that preventive controls are weak or are not cost-effective.		

Fraud Prevention Area, Factor, or Consideration	Score	Notes
We focus our data analysis and continuous auditing efforts based on our assessment of the types of fraud schemes to which organizations like ours (in our industry, or with our lines of business) are susceptible.		
We take steps to ensure that our detection processes, procedures, and techniques remain confidential so that ordinary employees — and potential fraud perpetrators — do not become aware of their existence.		
We have comprehensive documentation of our fraud detection processes, procedures, and techniques so that we maintain our fraud detection vigilance over time and as our fraud detection team changes.		
Our detective controls include a well-publicized and well-managed fraud hotline.		
Our fraud hotline program provides anonymity to individuals who report suspected wrongdoing.		
Our fraud hotline program includes assurances that employees who report suspected wrongdoing will not face retaliation. We monitor for retaliation after an issue has been reported.		
Our fraud hotline has a multilingual capability and provides access to a trained interviewer 24 hours a day, 365 days a year.		
Our fraud hotline uses a case management system to log all calls and their follow-up to resolution, is tested periodically by our internal auditors, and is overseen by the audit committee.		
Our fraud hotline program analyzes data received and compares results to norms for similar organizations.		
Our fraud hotline program is independently evaluated periodically for effectiveness and compliance with established protocols.		
We use a rigorous system of data analysis and continuous auditing to detect fraudulent activity.		
Our information systems/IT process controls include controls specifically designed to detect fraudulent activity, as well as errors, and include reconciliations, independent reviews, physical inspections/counts, analyses, audits, and investigations.		

Fraud Prevention Area, Factor, or Consideration	Score	Notes
Our internal audit department's charter includes emphasis on conducting activities designed to detect fraud.		
Our internal auditors participate in the fraud risk assessment process and plan fraud detection activities based on the results of this risk assessment.		
Our internal auditors report to the audit committee and focus appropriate resources on assessing management's commitment to fraud detection.		
Our internal audit department is adequately funded, staffed, and trained to follow professional standards, and our internal audit personnel possess the appropriate competencies to support the group's objectives.		
Our internal audit department performs risk-based assessments to understand motivation and where potential manipulation may take place.		
Our internal audit personnel are aware of, and are trained in, the tools and techniques of fraud detection, response, and investigation as part of their continuing education program.		
Our data analysis programs focus on journal entries and unusual transactions, and transactions occurring at the end of a period or those that were made in one period and reversed in the next period.		
Our data analysis programs identify journal entries posted to revenue or expense accounts that improve net income or otherwise serve to meet analysts' expectations or incentive compensation targets.		
We have systems designed to monitor journal entries for evidence of possible management override efforts intended to misstate financial information.		
We use data analysis, data mining, and digital analysis tools to: (a) identify hidden relationships among people, organizations, and events; (b) identify suspicious transactions; (c) assess the effectiveness of internal controls; (d) monitor fraud threats and vulnerabilities; and (e) consider and analyze large volumes of transactions on a real-time basis.		

Fraud Prevention Area, Factor, or Consideration	Score	Notes
We use continuous auditing techniques to identify and report fraudulent activity more rapidly, including Benford's Law analysis to examine expense reports, general ledger accounts, and payroll accounts for unusual transactions, amounts, or patterns of activity that may require further analysis.		
We have systems in place to monitor employee e-mail for evidence of potential fraud.		
Our fraud detection documentation identifies the individuals and departments responsible for: • Designing and planning the overall fraud detection process. • Designing specific fraud detective controls. • Implementing specific fraud detective controls. • Monitoring specific fraud detective controls and the overall system of these controls for realization of the process objectives. • Receiving and responding to complaints related to possible fraudulent activity. • Investigating reports of fraudulent activity. • Communicating information about suspected and confirmed fraud to appropriate parties. • Periodically assessing and updating the plan for changes in technology, processes, and organization.		
We have established measurement criteria to monitor and improve compliance with fraud detective controls, including: • Number of, and loss amounts from, known fraud schemes committed against the organization. • Number and status of fraud allegations received by the organization that required investigation. • Number of fraud investigations resolved. • Number of employees who have signed the corporate ethics statement. • Number of employees who have completed ethics training sponsored by the organization. • Number of whistleblower allegations received via the organization's hotline. • Number of messages supporting ethical behavior delivered to employees by executives. • Number of vendors who have signed the organization's ethical		

We periodically assess the effectiveness of our fraud detection processes, procedures, and techniques; document these assessments; and revise our processes, procedures, and techniques as appropriate.		