

Antifraud program and controls assessment grid*

Fraud risks & controls
February 2008

*connectedthinking

Antifraud program and controls assessment grid

		Assessment ranking		
Element	Criteria	Best practice	Generally in compliance	Deficient
Control environment				
Management accountability	<p>Management should</p> <ol style="list-style-type: none"> Effectively implement the company's antifraud programs and controls, and Take appropriate actions involving circumvention of internal controls over financial reporting. 	<p>Management:</p> <ol style="list-style-type: none"> Demonstrates that internal controls, including fraud, are important, Implements antifraud programs and controls including codes of ethics and conduct, and Takes appropriate, consistent remediation action in instances of violations. 	<p>Management takes sufficient actions with respect to prevention, detection, investigation, remediation, and monitoring of fraud and fraud controls.</p>	<p>Management fails to conduct oversight of antifraud programs and controls. Remediation, including disciplinary action, is inconsistent.</p>
Board of directors and audit committee oversight	<p>The board and audit committee should provide oversight over:</p> <ol style="list-style-type: none"> Management's antifraud programs and controls, Assessment of fraud risk, Control activities over fraud risks identified by the assessment, Monitoring and auditing for fraud, Investigation of alleged or suspected fraud, and Remediation. 	<p>The board and the audit committee</p> <ol style="list-style-type: none"> Conduct oversight of management's antifraud program, Seeks the views of internal audit, the independent auditor, and others regarding the topic of fraud. The charter expressly addresses fraud oversight as an essential function of the audit committee. 	<p>Board and Audit Committee provide oversight.</p>	<p>Audit Committee fails to provide oversight; and does not sufficiently consider fraud.</p>
Codes of ethics and conduct	<p>Written standards that are reasonably designed to deter wrongdoing and to promote honest and ethical conduct. Operating effectiveness evidenced through communication plan, annual confirmation process, training, management and audit committee involvement and oversight.</p>	<p>Documented and effective codes of conduct should include and be effectively communicated to all employees. Code should address</p> <ol style="list-style-type: none"> Conflicts of interest, Related party transactions, Accuracy of accounting records, Illegal acts, and Compliance with laws and regulations. 	<p>Documented and effective code of conduct with only minor deficiencies. Applies to all individuals in an accounting or financial reporting oversight role.</p>	<p>Code omits topics specified in SEC's Final Rules or is not operating effectively. Ineffective communication to all covered persons.</p>
Ethics Hotline/ Whistleblower program	<p>Documented procedures for the receipt, retention and treatment of complaints and confidential, anonymous submission of concerns by employees or external third parties.</p>	<p>Ethics hotline with a documented process and proven effectiveness as evidenced by employee and external third-party awareness, encouragement of use, and appropriate and timely response. Program operates independently of management and with audit committee oversight.</p>	<p>Ethics hotline that appears to be of proper design and effectiveness but potentially with perceived low volume of use.</p>	<p>Ethics hotline or whistleblower program omits elements (design or operating) in SEC rules.</p>

Antifraud program and controls assessment grid

		Assessment ranking		
Element	Criteria	Best practice	Generally in compliance	Deficient
Hiring and promotion procedures	Established standards for hiring and promotion including background investigations and maintenance of all information in the personnel files for all positions of trust in an organization.	For new and promotions of personnel in positions of trust, conduct full-scope background investigations, including interviews with independent references. Similar investigations conducted for strategic third parties such as vendors, joint venture partners, consultants, and customers. All results documented. Background investigations should include educational background, employment history, and criminal record.	Performs public record background investigations on personnel hired or promoted into positions of trust.	Fails to perform substantive background investigations for individuals being considered for employment to a position of trust.
Investigative process	Standardized procedure for tracking, responding to, investigating and assessing allegations of fraud, whether or not material, potentially including a 10A investigation by independent counsel.	Written plan and process for tracking and responding to allegations of misconduct. Where appropriate, investigative process allows for investigation independent of management. Audit committee and external auditors advised of all significant deficiencies in internal controls and of any fraud involving management or other employees who have significant role in internal controls.	In the absence of a written process, company demonstrates that a process exists for tracking and responding to allegations, notwithstanding a lack of a written plan.	Inadequate process for responding to allegations for suspicions of fraud.
Remediation	Documented process of assessing and improving relevant internal controls, taking appropriate action against violators and communicating results both internally as well as to the necessary external parties.	Improves relevant internal controls, takes appropriate action against violators and communicates results both internally as well as to the necessary external parties. Evidence and documentation of audit committee involvement.	Takes appropriate disciplinary action and considers need for additional action to prevent recurrence.	Fails to take consistent remedial action with regard to identified significant deficiencies, material weaknesses, actual fraud or suspected fraud.
Risk assessment				
Process for assessing risk	Systematic rather than haphazard; considers fraud schemes and circumvention of existing controls; active oversight by Audit Committee.	Fully documents fraud risk assessment process; process includes interviews of personnel at various levels of organization, occurs periodically throughout organization and in response to significant events, e.g., acquisitions, entry into new markets/ products; active oversight by audit committee.	Assesses fraud risk on systematic basis; Audit Committee review.	Fails to assess fraud risk on systematic basis; haphazard or informal process for fraud risk assessment; inadequate evidence of Audit Committee involvement and review.
Frauds considered	Consideration of fraudulent financial reporting, misappropriation of assets, unauthorized or improper receipts and expenditures, and fraud by senior management should all be demonstrated.	Assesses exposure from each of the categories of fraud risks considered.	Address all fraud risks that have a more than remote likelihood of having material impact upon the financial statements.	Absence of adequate documentary evidence of management's risk assessment process and the Audit Committee's involvement and review.

Antifraud program and controls assessment grid

		Assessment ranking		
Element	Criteria	Best practice	Generally in compliance	Deficient
Likelihood and significance of fraud	Consideration of the likelihood of each fraud risk as probable, reasonably possible, or remote; consideration of significance of fraud as insignificant, significant or material should be demonstrated.	Evaluates comprehensively the likelihood and significance of each identified fraud risk.	Substantially evaluates likelihood and significance of each fraud risk. Management provides sufficient explanation where risk assessment process does not consider risks that are more than remote and more than inconsequential.	Management's risk assessment process does not identify the level or likelihood and significance considered. Management fails to provide an explanation where risk assessment process does not consider risks that are more than remote and more than inconsequential.
Consideration of organizational levels	Consideration of fraud at the company-wide business unit and significant account levels should all be demonstrated.	Assesses fraud risk at all levels of the organization.	Assesses fraud risk at all significant levels, accounts and locations of the organization.	Fails to consider significant business units or significant processes in the fraud risk assessment.
Circumvention of controls and management override	Effectively designed internal controls should be in place to respond to the assessment of risk of management override.	Audit Committee specifically considers vulnerability of existing controls and risk of management override.	Fraud risk assessment process addresses circumvention of existing controls and potential for management override.	Fails to adequately consider risk of 1. Circumvention of controls, and 2. Management override.
Control activities				
Linkage with risk assessment	Effective control activities should be designed and implemented to mitigate identified fraud risks.	Company links control activities to all identified fraud risks. Active oversight by Audit Committee to ensure design and operating effectiveness.	Company can link control activities to identified fraud risks and evaluates for design and operating effectiveness in compliance.	Fails to link control activities to identified fraud risks; control activities deficient in design or operating effectiveness.
Information and communication				
Training	Demonstrated frequency and sufficiency of proper training courses provided to all employees on fraud risk and antifraud programs and controls.	Provides comprehensive and frequent relevant training to all employees. Maintains records documenting types of training and employees trained.	Provides adequate training to employees regarding fraud related issues.	Fails to provide adequate or effective training regarding code of ethics and other fraud areas.
Knowledge management	Demonstrated capabilities in place to collect and share information regarding identified fraud risks, strengths and weaknesses of antifraud control activities, allegations of fraud, and remediation efforts.	Clear communication of antifraud policies and procedures flows down, up, and across the organization. Employees fully understand relevant aspects of the antifraud program and understand what behavior is acceptable and unacceptable. Strong knowledge sharing regarding fraud risks, control activities, allegations of fraud, and remediation efforts.	Shares some but not all fraud-related information.	Fails to collect or share information regarding fraud risks, control activities and remediation of identified misconduct.

Antifraud program and controls assessment grid

		Assessment ranking		
Element	Criteria	Best practice	Generally in compliance	Deficient
Information systems and technology	Elements that should be addressed are inclusion of technology in management's fraud risk assessment, effective IT security and controls, adequacy of fraud detection and monitoring tools, and ability to investigate computer misuse.	Information systems and technology addresses: <ol style="list-style-type: none"> 1. Consideration of technologically enabled fraud in management's fraud risk assessment, 2. IT security controls, 3. Inappropriate modification to computer programs, 4. System override, 5. Segregation of duties, 6. Adequacy of fraud detection and monitoring tools, and 7. Ability to investigate computer misuse. 	Information systems and technology addresses some, but not all of elements 1 through 7.	Fails to either: <ol style="list-style-type: none"> 1. Consider information technology in fraud risk assessment, 2. Maintain security and assess controls, 3. Employ information technology to prevent and detect fraud, or 4. Have an ability to investigate computer misuse.
Monitoring				
Monitoring by management	Management should have a process of assessing the quality of the antifraud programs and controls over time through ongoing monitoring activities as well as separate periodic evaluations.	Monitors antifraud controls, programs and policies on an ongoing and periodic basis; management considers possibility of fraud in day-to-day operations; management uses results of fraud assessment and IT system to monitor for fraud.	In absence of written process, company can demonstrate that management monitors for indicia of fraud as part of day-to-day operations.	Management fails to include possibility of fraud in its monitoring of day-to-day operations.
Internal audit evaluations	The internal audit function in an organization should conduct separate fraud evaluations with a documented plan, approach, scope, and results of review with knowledgeable and experienced staff.	Internal audit actively considers fraud risk in developing audit cycle. Internal audit builds fraud auditing modules into routine audits and special projects. Internal audit includes fraud experienced internal auditors.	In absence of written process, company can demonstrate that <ol style="list-style-type: none"> 1. Internal audit considers fraud in developing and executing internal audit cycle, and 2. Department includes internal auditors with training and experience in fraud auditing. 	Fails to either <ol style="list-style-type: none"> 1. Consider fraud in planning internal audit cycle, 2. Conduct fraud auditing procedures, or 3. Include routine fraud auditing in the scope of the internal audit function's annual audit cycle. Failure to include knowledgeable and experienced fraud professionals in the internal audit function.