ISSUES TO DEVELOP A FRAUD PREVENTION AND INCIDENT MANAGEMENT PROGRAM

Developed by Sikich for illustrative and discussion purposes only and should not be construed as legal advice in any manner. Every plan will be customized to the unique circumstances of the individual entity.

PREVENTION PLAN

1. Establish the tone at the top: Clear policies which are frequently and formally communicated to employees, management, Board and vendors:
   - Will not tolerate fraud or embezzlement and entity is fully and lawfully ready to terminate employment, prosecute, pursue civil remedies rescind a contract and obtain restitution.
   - That no one has a reasonable expectation of privacy related to any tangible or electronic assets used during normal business; computers, phone records, PDAs, etc. and desk/file area may be searched and monitored at will.
   - All employees will take regular vacations and will be cross trained in duties.
   - All measures will be taken to provide for separation of duties in all operational areas.
   - Internal audits will be frequent and often by surprise.
   - All vendors will be subject to audit on demand.
2. Establish a whistleblower system that is confidential and where the reporting person can be safe from reprisals and know that their tip will be considered and, if credible, will be pursued.
3. Establish a fraud prevention team who will conduct a thorough risk assessment of the organization.
4. Construct a system to separate business duties to every extent possible and institute compensating controls responsibility where necessary.
5. Review all sensitive areas where fraud may occur – consider rotation of staff, fidelity bonding, surprise audit, movement of part time employees etc. Do thorough background checks when hiring.
6. Review, update and upgrade insurance coverage to cover incidents of fraud and embezzlement.
7. Retain the best lawyer available with an employment law specialty who is knowledgeable in issues of wrongful termination, administrative leave, invasion of privacy, reasonableness issues related to searches in the workplace, false imprisonment, and /contractual issues.
8. Devise a policy on how to handle communication with the media and the public in the event of a fraud. Interview and retain a public relations firm.
9. Review and create clean desk policy and security of assets from blank check stock to donor' information to cash registers to loading docks. Purchase and install locks, smart key card systems and video surveillance.
10. Review the technological sophistication of the IT system with emphasis on issues of security and fraud prevention. Hire a forensic consultant to perform a vulnerability test on the system.
11. Devise a regular internal audit schedule. Do not invest one person with this function but rotate it as possible. Review the reviewer regularly.
12. Establish a regular training program for employees, Board and vendors in issues and expectations surrounding fraud prevention.
13. Add policies and procedures to employee/program handbook and secure signatures from each employee and vendor. Include right to audit in vendor contacts.

INCIDENT MANAGEMENT PROTOCOL (IMP)

1. Establish an IMP Team, who are "need to know" decision makers to receive a tip, evaluate the credibility of the tip as well as its materiality and put this process in motion if necessary. This team should at least consist of a member of Senior Management and Department Head where issue resides. Note that the immediate supervisor of a targeted individual should not be included. Do not include any one who appears to have a conflict of interest or who may be part of the problem. This Team remains in complete control of this process from start to resolution. Immediately shut down all outside communication on the matter and this group must not speak to any outside party with the following exceptions on an as needed basis to plan the next steps in the investigative process:
   - Insurance broker/agent/risk pool representative
   - Forensic investigator
   - External auditor (informed but will not be integral in this process by policy)
   - Computer forensics specialist
   - General counsel
   - Employment attorney
2. Establish a sense of urgency and continuous communication among the IMP Team. Decide early on who and how the matter will be investigated.
3. Review public relations policy. Keep incident in complete secrecy until properly investigated.
4. In consultation with attorney, devise a system to preserve the legal confidentiality and privilege of the process.
5. In consultation with the employment attorney, establish a plan to place the suspected employee on administrative leave if necessary. Do this in such a way as to maximize the ability of the investigators to locate and preserve relevant and material evidence. Limit employee access to building and work area, secure workstation and files, change computer access, and secure all electronic devices. Notify IT to preserve possible evidence banks including email. Do this in a way that is not demeaning, showy, or otherwise unprofessional.
6. In consultation with legal counsel, establish a plan to deal with specific incident of vendor fraud including the suspension of purchasing or payment of invoices and the securing of evidence, paper and electronic, related to the vendor, sales representation and any employee who may be supplying assistance in the matter.
7. Secure the electronic and paper evidence. Engage the services of a forensic computer specialist if needed to image electronic devices and establish a chain of custody. Image and secure the evidence. Make copies available to investigators to complete their analysis. Secure all paper files.
8. Do not allow unplanned or random investigation, especially interviews, by personnel untrained in these matters. Be particularly cognizant of issues of false imprisonment, defamation of character, invasion of privacy, and incrimination. Best practice to engage forensic investigator.
9. Be sure that investigators follow best practices related to chain of custody and proper handling of original documents. Establish a clear filing system by witness or transaction, create a key document file and database early in the process. Consult with forensic investigator for proper procedure.
10. Develop a brief written plan to investigate the matter including a timeframe for completion. Limit the investigation to the matters indicated by the evidence. Investigation procedures are dictated by the specific matter and will include use of data mining, financial analysis, joining of computer files, and other machine and paper-based techniques. It may or may not include interviews or surveillance.
11. IMP Team is continuously informed of the progress of the investigation and determines the point at which there is sufficient evidence to pursue corrective action or end the investigation. However, the Team should not cross the fine line between supervision/responsibility for the process and driving the investigation in a way that clouds the results.
12. Based on the results of the investigation, take corrective action or restore the person/vendor in question to normal status.
13. Hold a formal debriefing meeting of the Team which reviews the process and the results of the investigation. Immediately, take all corrective actions to improve the Protocol and the flaws in the operational systems that created the problem.
14. Devise a policy on how to communicate with the Board, management and staff. Who, what, when, where, how and what provides the outline for this policy. Devise a method to effectively deal with leaks. Employ public relations firm to assist with these communications and with the press.

For more information or to engage the forensic team, please contact:

MARY O'CONNOR
ASA, CFE
PRINCIPAL,
FORENSICS AND VALUATION SERVICES
E: mary.oconnor@sikich.com