Monday, October 20
4:30 pm-6:00 pm

308 Fraud Planning & Prevention for In-house Counsel

Martin T. Biegelman
Director, Financial Integrity Unit
Microsoft Corporation

Nidhi Gupta
Director
BDO Consulting

Miriam Smolen
Associate General Counsel
Fannie Mae

Faculty Biographies

Martin T. Biegelman

Martin T. Biegelman is director of the financial integrity unit at Microsoft Corporation in Redmond, WA. He was brought to Microsoft in order to create and lead a worldwide fraud detection, investigation and prevention program based within internal audit. In addition to focusing on preventing financial fraud and abuse, Mr. Biegelman's group also promotes financial integrity and fiscal responsibility through a committee of sponsoring organization framework of improved business ethics, effective internal controls, and greater corporate governance. Mr. Biegelman also works closely with Microsoft's executive leadership in protecting Microsoft from financial and reputational risk.

Prior to joining Microsoft, Mr. Biegelman was a director of litigation and investigative services in the fraud investigation practice at BDO Seidman LLP. He is also a former federal law enforcement professional having served as a United States Postal Inspector in a variety of investigative and management assignments. As a federal agent, Mr. Biegelman was a subject matter expert in fraud detection and prevention.

Mr. Biegelman currently serves on the board of directors for the Association of Certified Fraud Examiners Foundation, the board of advisors for the Economic Crime Institute at Utica College, and the accounting advisory board for the Department of Accounting and Law at the SUNY Albany School of Business.

Mr. Biegelman received a BA from Cornell University and MA in Public Administration from Golden Gate University.

Nidhi Gupta

Nidhi Gupta is a director at BDO Consulting, a division of BDO Seidman LLP, in New York. Ms. Gupta assists clients with corporate investigations as well as fraud prevention programs through BDO Consulting's Critical Anti-Fraud Program. Ms. Gupta's fraud prevention work involves conducting fraud risk assessments, fraud education, and monitoring anti-fraud programs and controls. In addition to shadow investigations, Ms. Gupta has investigated numerous matters involving issues related to sub-prime mortgages, earnings management, and frauds committed against organizations by employees and management.

Ms. Gupta received a BBA from the University of Texas at Arlington.

Miriam Smolen

Miriam Smolen serves as associate general counsel in the litigation department for Fannie Mae in Washington, DC. She directs the legal support of the company's anti-fraud activities, including preventing mortgage fraud and oversight of the internal fraud controls. Prior to joining the litigation department, Ms. Smolen served in Fannie Mae's office of corporate compliance where she assessed legal and regulatory risk for business operations, created and implemented business specific compliance plans, and implemented the code of business conduct to prevent conflict of interest and other violations. Ms. Smolen's current responsibilities also include conducting internal investigations and responding to government investigations. Her expertise also includes electronic evidence retention and production.

Prior to joining Fannie Mae, Ms. Smolen was an assistant US attorney with the US Attorney's Office in Washington, DC where she served a detail with the Department of Justice Computer Crime and Intellectual Property Section. Ms. Smolen has investigated and tried dozens of violent crime, narcotics, and financial fraud cases, including multi-million dollar embezzlements from government agencies and labor unions, health care fraud, and computer crime. She specialized in health care fraud and intellectual property and computer crime cases, serving as the health care fraud coordinator and chair of the Health Care Fraud Task Force, and as the Computer and Telecommunications Coordinator for the DC US Attorney's Office.

Ms. Smolen is a graduate of the Boalt Hall School of Law at the University of California, Berkeley.

Agenda

- Fraud Statistics and Regulatory Requirements
- Components of Anti-Fraud Program
- Fraud Risk Assessment Methodology
- Q&A

Did You Know… Fraud Statistics

- Fraud and abuse costs U.S. organizations more than **$994 billion** annually
- The average organization loses about **7%** of its total annual revenue to fraud and abuse
- The median loss caused by occupational fraud was **$175,000**, more than 60% of schemes caused a loss of at least a **$100,000**
- Median length of a time a fraud scheme went undetected was **24 months**
- Nearly **40%** of the victim organizations were privately owned companies

Source: Association of Certified Fraud Examiners – 2008 Report to the Nation

Fraud Statistics and Regulatory Requirements

Did You Know… Fraud Statistics

Median Loss Based on Presence of Anti-Fraud Controls

Control	% of Cases Implemented	Yes	No	% Reduction
Surprise Audits	25.5%	$ 70,000	$ 207,000	66.2%
Job Rotation / Mandatory Vacation	12.3%	$ 64,000	$ 164,000	61.0%
Hotline	**43.5%**	**$ 100,000**	**$ 250,000**	**60.0%**
Employee Support Programs	**52.9%**	**$ 110,000**	**$ 250,000**	**56.0%**
Fraud Training for Managers / Executives	**41.3%**	**$ 100,000**	**$ 227,000**	**55.9%**
Internal Audit / Fraud Examination Department	55.8%	$ 118,000	$ 250,000	52.8%
Fraud Training for Employees	**38.6%**	**$ 100,000**	**$ 208,000**	**51.9%**
Anti-Fraud Policy	**36.2%**	**$ 100,000**	**$ 197,000**	**49.2%**
External Audit of ICOFR	53.6%	$ 121,000	$ 232,000	47.8%
Code of Conduct	**61.5%**	**$ 126,000**	**$ 232,000**	**45.7%**
Management Review of Internal Control	41.4%	$ 110,000	$ 200,000	45.0%
External Audit of Financial Statements	69.6%	$ 150,000	$ 250,000	40.0%
Independent Audit Committee	49.9%	$ 137,000	$ 200,000	31.5%
Management Certification of Financial Statements	51.6%	$ 141,000	$ 200,000	29.5%
Rewards for Whistleblowers	5.4%	$ 107,000	$ 150,000	28.7%

Source: Association of Certified Fraud Examiners – 2008 Report to the Nation

Consequences of Fraud

- Loss of Reputation
- Higher Cost of Capital
- Loss of Assets
- Inability to Attract the Most Qualified Workforce
- Reduced Value of Investment to Stakeholders
- Criminal and Civil Proceedings Against the Organization

Conditions Where Fraud May Occur

All three conditions must be present for fraud to occur!

Motive

What drives employees or management to commit fraud, such as greed, pressure or recognition.

Opportunity

Culture or environment that enables fraud to occur, such as complex organizations or transactions that can be used to hide fraud and lack of strong controls or values to prevent it.

Means

How an individual commits fraud – such as typical fraud schemes, tools or technology that can be used.

Impacts of Fraud - Not Just Financial

- **Direct Financial Loss** - loss of monetary assets
- **Customer** - relationship damage and lost business opportunity
- **Regulatory** – review or action by regulator, law enforcement, or other government agency
- **Business Disruption** – business interruption including lost time or productivity, delayed or missed transactions, and decrease in employee morale
- **Reputation** - reputation damage to Company due to misconduct by employees or external parties
- **Financial Reporting** – incorrect financial reporting and disclosures, internally or externally

Current Regulatory Requirements

- Sarbanes-Oxley Act of 2002
- PCAOB Auditing Standard No. 5
- Statement on Auditing Standards (SAS) 99
- SEC Regulations and Enforcement Policy
- Amended US Federal Sentencing Guidelines
- US Foreign Corrupt Practices Act
- OECD Anti-Bribery Convention
- National Exchange Listing Rules

Increased organizational responsibility to deter, prevent and detect fraud

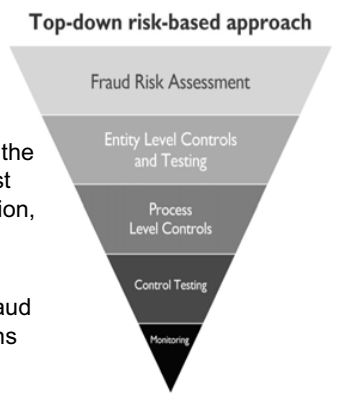
Components of an Anti-Fraud Program

Critical Elements of an Anti-Fraud Program

- Fraud Risk Assessment
- Background Investigations and Employment Practices
- Mechanisms for Reporting, Investigating, and Remediating Fraud
- Ethics Awareness and Education
- Fraud Awareness Education

Fraud Risk Assessment (FRA)

- FRA expands on traditional risk assessments
- Should be a top-down risk based approach
- Focuses management's efforts on the fraud risks that present the greatest threat to the organization's reputation, assets or financial reports
- Should involve fraud expert or individuals who are familiar with fraud schemes and/or fraud investigations



Fraud Risk Assessment - Step #1

- Identify fraud risks in the organization by:
  - Researching historical occurrences of fraud within the organization and the industry
  - Interviews of key management personnel
  - Inquiries of employees
  - Inquiries of the audit committee/board of directors
  - Inquiries of internal and external auditors
  - Risk Assessment surveys
  - Analytical procedures
  - Review of other risk assessment results such as risk assessments conducted for SOX and Enterprise Risk Management exercises

Fraud Risk Assessment - Step #2

- Prioritize the identified fraud risks for the organization, i.e. fraud risks that present the greatest threat to the organization's reputation, assets or financial reports.
  - Consider the likelihood and impact of the fraud risks
  - Prioritize the fraud risks by:
    - Geographic Location
    - Division
    - Department
    - Process

Fraud Risk Assessment - Step #3

- Organize the fraud brainstorming session for selected processes and/or departments.
  - Identify a facilitator for the fraud brainstorming session
    - Can be done internally using employees trained in conducting and overseeing these sessions and/or using external consultants
    - Should include a fraud expert
  - Consider who should attend
    - Employees who have a significant control over the controls and procedures
    - Internal Audit
  - Identify fraud risks using fraud scenarios in process without controls
  - Prioritize the fraud risks identified in the fraud scenarios

Fraud Risk Assessment - Step #4

- Consider Likelihood and Impact to the organization during the prioritization process
  - Likelihood – probability of the fraud scheme being perpetrated
    - Schemes that are easy to perpetrate without being detected
    - Number of schemes associated with a fraud risk
  - Impact – damage that could be caused by the fraud scheme
    - Potential Dollar value of the loss
    - Potential reputational damage to the organization
    - Frequency of the fraud being perpetrated
    - Possible involvement of Senior Manager in the fraud scheme

Fraud Risk Assessment - Step #5

- After prioritization of the fraud risks identified in the fraud scenarios
  - Determine what controls are in place to reduce the risk of these frauds
  - Identify ways that these controls can be circumvented (consider the possibility of management over-ride)
  - Identify control gaps

Evaluating Control Effectiveness

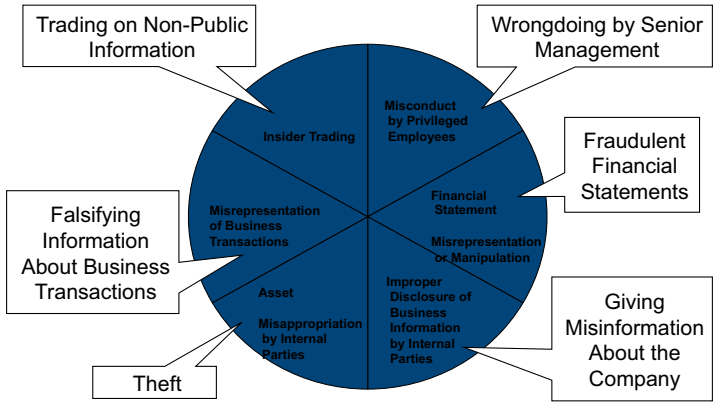
- Evaluate the vulnerability of identified controls to circumvention, collusion, and override.
- The best evidence of control effectiveness will generally come from traditional testing (i.e., selecting a sample and re-performing the control).
- For purposes of the RCSA, participants are recommended to leverage previous SOX findings in order to assess the effectiveness of controls.

Example of Fraud Risk Assessment

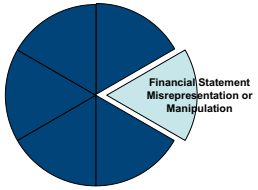
Evaluating Control Effectiveness

- In addition, RCSA participants should take into consideration the following in order to help them with their assessment:
  - Are people in the business unit generally aware of this control?
  - Do the persons performing the control possess the necessary authority, skill and qualifications to perform the control effectively?
  - Have exceptions been noted in the past through performance of the control? If yes, were exceptions appropriately followed up on?
  - What is the degree of oversight of these controls?

Internal Fraud Risk Categories



Risk of Misrepresentation of Liabilities and Expenses

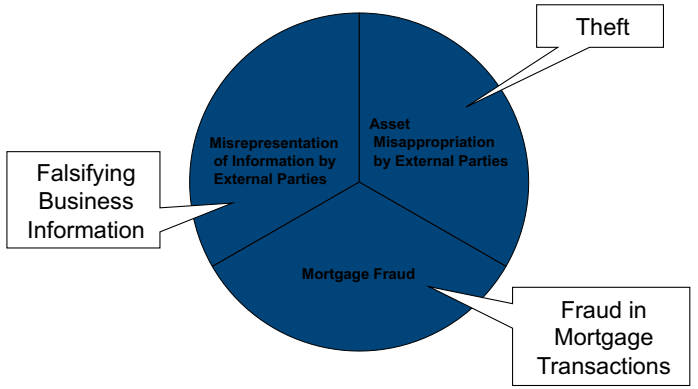


Intentional misrepresentation of liabilities and expenses in the Company's financial statements. This could include improper capitalization of expenses, inflating balance sheet or misstating reserves.

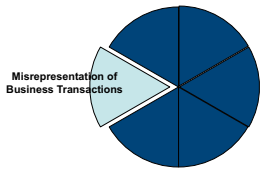
Examples include: Misstating accounting estimates or payables; Improperly recording expenses as prepaid expenses thereby improving entity's income statement and inflating balance sheet or understating reserves; Improper use of foreign currency rates; Delaying the recording of expenses made near the closing period until the next accounting period; Misrepresentation or misuse of the reserves.

Example: Misrepresentation or Misuse of Reserves	
Conditions	
Motive	Pressure to meet financial targets and/or improve financial position
Means	Access to calculate and/or book reserve amount to the G/L
Opportunity	Domination of management by a single person or a small group; High volume of transactions
Considerations	
Impacts	Financial Reporting; Regulatory
Sample Controls to Mitigate	Segregation of duties between employee who calculates reserve and employee who reviews it; Effective access controls to the G/L; Conduct regular and rigorous reviews of aged receivable trends, gross margins, expense comparisons, etc.; Perform periodic reconciliations and retrospective reviews

External Fraud Risk Categories



Risk of Improper Receipts and Expenditures

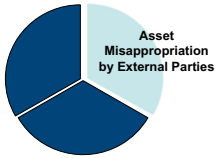


Revenue, assets, costs or expenses are manipulated or presented in a manner that does not reflect their fair values, for purposes of improper gain.

Examples include: Illegal marketing; Improper loan acquisitions; Improper trading arrangements; Overbilling customers; Tax evasion; Fraudulent avoidance of brokerage fees or contractual obligatory payments.

Example: Property Tax Evasion by Understating Value of Physical Assets	
Conditions	
Motive	Greed – Avoidance of expenses
Means	Use understated asset values to determine tax liability
Opportunity	Access to high volume of appraisers; No independent verification
Considerations	
Impacts	Regulatory; Reputation
Sample Controls to Mitigate	Segregation of duties; Proper assignment of authority; Confirmation with counterparties

Risk of Asset Misappropriation by External Parties

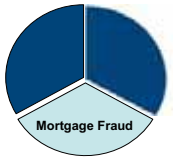


Theft of Company or external party physical, information or intellectual assets by external parties for improper gain.

Examples include: Illegal acquisition of trade secrets or company confidential information; Improper disposal or safeguarding of Company proprietary or confidential data in order to facilitate third party or personal gain (e.g. stealing consumer information, social security numbers, etc.); Theft of laptop.

Example: Consultant Steals Company Proprietary Economic Forecasting Applications	
Conditions	
Motive	Greed – cash, if information can be sold or knowledge, if information used by competitors or customers, Recognition – new employment prospects
Means	Access to information that can be easily transferred using modern technology
Opportunity	High number of consultants with access to confidential information; High turnover of consultants
Considerations	
Impacts	Business Disruption
Sample Controls to Mitigate	Limit or log access to proprietary information by consultants; Signed confirmation of contractor code of conduct; Limit transferability of data to consultants computers

Risk of Counterparty Misrepresentation or Duplicate Sales of Loans



Counterparty misrepresents key information to gain loan approval or sells a duplicative loan to Company or to multiple investors.

Examples include: Counterparty retains credit guarantee income due Company; Lack of collateral where loans sold in duplicate; Loan payoffs not reported; Foreclosures not reported; Multiple active first liens on a single property; Misuse of custodial funds; Loan proceeds not forwarded to Company; Lack of information regarding key parties/details to the transaction; Number of property liens misstated.

Example: Multiple Active First Liens Not Reported	
Conditions	
Motive	Greed – mortgage loans received without proper payoff of first lien
Means	Closing agent hides existence of first lien or does not use proceeds to pay off lien
Opportunity	Secondary market relies on information from loan originator; No front end verification
Considerations	
Impacts	Direct Financial Loss; Financial Reporting
Sample Controls to Mitigate	Requirement for repurchase clause in contract; Approval standards for lenders and continued review of lender qualifications including on site visits; After the fact data checks – check for charter compliance, duplicate loan checks, same borrower/same property check

Other Components of an Anti-Fraud Program

Next Steps After Fraud Risk Assessment

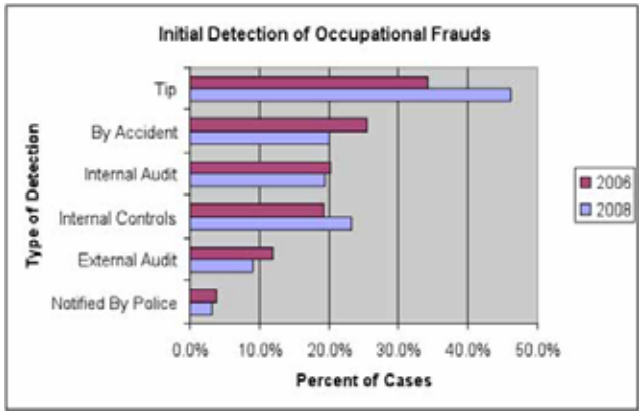
- Identify and develop a remediation plan to address the control gaps identified through the fraud risk assessment process
- Identify areas for increased internal audit or management scrutiny
- Assign a Senior Manager to oversee the remediation process
- Identify areas for increased employee training
- Determine the need for re-perform the fraud risk assessment

Background Investigations and Employment Practices

Effective employment practices include:

- conducting comprehensive background investigations of individuals being considered for employment or for promotion to a position of trust;
- thoroughly checking a candidate's education, employment history, and personal references
- periodic training of all employees about the entity's values and code of conduct
- regular performance review process
- providing appropriate incentives to perform in accordance with the organization's compliance and ethics programs

Mechanisms for Reporting, Investigating & Remediating Fraud



Source: Association of Certified Fraud examiners – 2008 Report to the Nation

Fraud Awareness Training

- An effective fraud awareness training program:
  - Prepares employees and business partners to identify the preconditions and characteristics of fraud
  - Provides guidance on how to recognize and report fraud
  - Helps employees understand their specific roles and responsibilities in fighting fraud

Ethics Awareness and Education

- Establishing Ethics awareness and education within an organization includes:
  - Drafting a clear and understandable code of ethics and business conduct
  - Conducting ethics assessments through the use of questionnaires, survey tools, employee interviews
  - Developing in-house ethics education programs for the organization's board members, management, and employees
  - Drafting internal newsletters, columns on ethics and values for the organization on an as needed basis

Enterprise Anti-Fraud Program

1. Governance
- Maintain and update Fraud Risk Management Policy
- Chair cross-functional Anti-fraud Working Group

2. Assessment
- RCSA – both high level and "evolution"
- Targeted Deep Dive reviews
- Third party assessments

3. Monitoring
- Monitoring Plans for Businesses with Significant Risks
- Monthly Monitoring of operational incidents, fraud investigations and Audit findings
- Quarterly Certification of fraud risk position including potential events within businesses
- Review of fraud related litigation activity

4. Testing
- Operational Effectiveness Testing
- SOX testing
- Targeted testing in high risk areas

5. Reporting and Communication
- Board Reporting – Compliance and Audit Committees
- Quarterly Fraud Review provided to Chief Compliance Officer and Division Risk Officer/SVP Operational Risk Oversight
- Annual Fraud Risk Aggregation Report
- Deploy all-employee fraud awareness training

Robust Framework Ensures Comprehensive Management of Fraud Risk

Emerging Markets

Emerging Markets Due Diligence

Key findings of 2007 D&T survey on developing business in emerging markets:

- Just 67% of companies always conduct background investigations before M&A activity
- Integrity checks are not always thorough especially in AML, terrorist financing, and FCPA
- 70% pulled out of deals as a result of uncovering negative information
- Larger companies conduct more thorough background investigations

The World is Flat

- 85% of companies plan to expand operations in emerging markets
- 52% of future revenue growth & 59% of sourcing opportunities will come from Asia Pacific
- BRIC countries have potential to become among the four most dominant economies by the year 2050
  - Forecasted to be 39% of world's population and combined GDP of $15.4 *Trillion* Dollars
  - By 2025, it is estimated that over 200 million people in BRIC nations will earn over $15,000 per year, creating a large middle-class
- Goldman Sach's N-11

Greatest Risk in Emerging Markets

Key Finding:
Consider fraud risks in light of your industry and market

Source: E&Y 9th Global Fraud Survey, June 2006

Foreign Corrupt Practices Act (FCPA)

Foreign Corrupt Practices Act

- FCPA prohibits U.S. companies, their subsidiaries, employees, and agents from paying or offering to pay anything of value:
  - To a foreign official, political party, or candidate in his or her official capacity, or;
  - To any person, directly or indirectly, knowing that any part of the payment is destined for a foreign official;
  - In order to corruptly influence the recipient to act, fail to act, or to secure an improper advantage, or;
  - In order to cause the recipient to use his or her influence to assist the company in obtaining, retaining, or directing business, or;
  - In order to cause the recipient to do or omit to do any act in violation of his or her lawful duty

FCPA's Two Provisions

- Anti-bribery
  - Giving or offering anything of value to a foreign official
  - With the intention of obtaining or retaining business, or
  - Obtaining an improper business advantage
  - In connection with a business transaction
- Internal Accounting Controls & Recordkeeping
  - All employees must abide by this provision
  - Maintenance of books and records that accurately reflect each transaction
  - Maintenance of a system of internal accounting controls

Facilitating Payments

- For "routine governmental action"
  - Obtaining permits, licenses, or official documents to facilitate business in a foreign country
  - Processing governmental papers
  - Providing police protection, official inspections related to transit of goods, scheduling of inspections, or mail delivery
  - Telephone, power, water or other utilities service, unloading cargo, or protecting perishable products
  - Other services not related to the decision to award new business or continue business

USDOJ's FCPA Red Flags

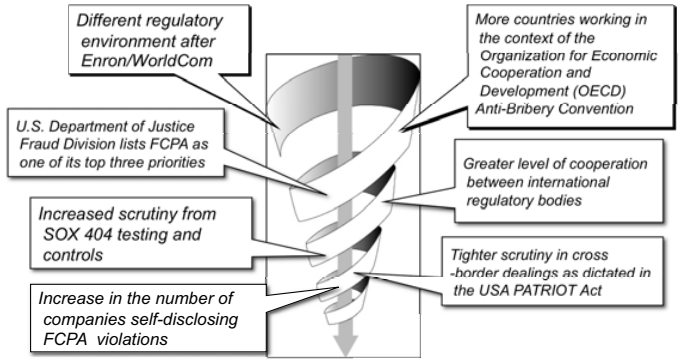
- Unusual payment patterns or financial arrangements
- A history of corruption in the country
- Refusal by the foreign joint venture partner or representative to provide a certification that it will not take any action in furtherance of an unlawful offer, promise, or payment to a foreign public official in violation of the FCPA
- Unusually high commissions
- Lack of transparency in expenses and accounting records
- Apparent lack of qualifications or resources on the part of the JVP or representative to perform the services offered
- Whether the JVP or representative has been recommended by an official of the potential governmental customer

Source: http://www.justice.gov/criminal/fraud/docs/dojdocb.html

FCPA Compliance Standards

- Clear FCPA policy establishing compliance standards and practices to be followed by employees, consultants, and agents.
- Creating and maintaining a committee to review the hiring of agents, consultants, or other representatives to do business in a foreign country, and the related contracts as well as prospective joint venture partners.
- Clear corporate procedures to assure that the necessary precautions are taken to make sure the company only does business with reputable and qualified individuals.
- Communicating FCPA policies, standards, and procedures to employees, agents, and consultants; requiring regular training on the FCPA and other applicable foreign bribery laws to officers and employees involved in foreign projects.

An Increase in FCPA Enforcement



The trend of increasing numbers of enforcement actions and voluntary reporting will continue

FCPA Compliance Standards

- Including in all foreign business contracts provisions banning foreign bribery.
- Periodic review, at least once every five years, of corporate policies and FCPA compliance program, to be conducted by independent legal and auditing firms retained for such purpose.
- Prompt investigation and/or reporting of any alleged violations of the FCPA or other applicable foreign bribery laws.
- The company must determine the regions or countries in which it does business that pose higher risks of corruption, and then on a periodic basis, conduct rigorous FCPA audits of its operations in such areas.

Assessing FCPA Risk

- Ask – is personal information form foreign consumers collected? What do foreign privacy and data security laws require?
- Identify customers ("Know Your Customer") – where are they, who are they, what will they do with your goods or technology?
- Identify suppliers – where are they, who are they, where did the goods come from, who made them?
- Learn where you can and cannot travel to, who you can sell to, what products or services you can sell, what prohibitions are their on foreign nationals for work or visitation?

The Value of an Anti-Fraud Program

Assessing FCPA Risk

- Understanding the inherent risks
  - Varies from country to country, business to business
  - Who can assist with assessment – local business management (finance, HR, legal) and headquarters (audit, legal, other subject matter experts)
  - Local affiliate should have significant input in risk assessment but with guidance from headquarters

An Interview with

Martin Biegelman,

CFE, ACFE Fellow, director of Microsoft's Financial Integrity Unit

BUILDING A ROBUST FRAUD PREVENTION PROGRAM

The diverse members of Microsoft's five-year-old Financial Integrity Unit tackle internal cases but also prevent and deter fraud through intensive training for management and employees. Their aim? Squash fraud long before it shows up on the radar and help create a "culture of compliance."

Microsoft, of course, is huge. That computer on your desk probably contains at least one Microsoft product. The firm has almost 80,000 full-time employees with offices in more than 100 countries and thousands of vendors. Like many burgeoning global corporations, it has to seek staffers with integrity. But even with the best hiring practices, no entity can ignore the possibility of fraud in its ranks.

Five years ago, Microsoft began its Financial Integrity Unit with Martin Biegelman, CFE, ACFE Fellow, at its helm. Biegelman initially sent members of his Washington-state team around the globe to conduct investigations. But soon he realized that he needed to hire nationals who would understand the specific cultures, social mores, and country laws.

The approach is paying off. With 11 team members (and growing) throughout the world, the FIU has been able to tackle cases that have helped protect Microsoft's assets and reputation while providing anti-fraud education for management and employees. "By creating this 'perception of detection,' we are able to proactively reduce the risk of potential opportunities to commit fraud," Biegelman says.

Biegelman says that the FIU exists not just to conduct fraud examinations but to foster a "culture of compliance," enhance the company's internal controls, and build a robust fraud prevention program. Prevention and deterrence aren't just clichés, Biegelman says; they're the lifeblood of the FIU.

Biegelman spoke to *Fraud Magazine* from his office in Redmond, Wash.

What is Microsoft's Financial Integrity Unit?

The global business environment is continuously changing and demanding more from us as a company and as employees. Not only does the world expect us to deliver the best products and services, it expects us also to conduct ourselves ethically and responsibly.

Consequently, in September 2002, Microsoft formed its Financial Integrity Unit [FIU], an internal corporate investigation resource based within the Internal Audit Department. The FIU is designed to address internal and external integrity matters including financial frauds and reported concerns related to possible violations of Microsoft's Standards of Business Conduct. The FIU also plays a role in enhancing the integrity of the internal control environment through recommended process and policy improvements. It has a global charter with people in Microsoft offices in the United States (Redmond, Wash.) in Asia (Singapore, China, and India) and in Europe (France and Russia). These offices are staffed with FIU members who are Certified Fraud Examiners, former law enforcement professionals, CPAs, forensic accountants, and other fraud-detection professionals. The FIU works closely with Microsoft's executive leadership, the Office of Legal Compliance, the Internal Audit Department, and others in protecting Microsoft from financial and reputational risk.

How was Microsoft's Financial Integrity Unit formed?

Microsoft has long made corporate compliance and proactive fraud prevention a top priority. In 2001, prior to Enron, WorldCom, Adelphia and other corporate scandals, our then-CFO, in consultation with the Internal Audit Department and the Office of Legal Compliance, determined that Microsoft needed increased protection from potential financial fraud and abuse issues. The company decided to construct a dedicated unit staffed with professional investigators focused on both a proactive and reactive approach.

After an in-depth analysis, Microsoft determined the key elements needed for an effective fraud prevention unit. Some of those are: a clear charter or mission, a comprehensive fraud risk management strategy, written policies and procedures, sufficiently experienced personnel, sound internal organizational structure, executive sponsorship, investigative priorities aligned with fraud risk and Microsoft business objectives and strategy, effective and timely response, essential array of technology tools, case management system, and key performance measurements.

Microsoft then needed to find a leader for this new unit. They wanted someone with significant experience conducting financial fraud investigations in both the government and private sectors. They wanted a person with management experience along with other leadership qualifications. Microsoft understood the value of the Certified Fraud Examiner certification and made this a qualification requirement for the position.

In March 2002, I was asked to be a speaker at the ACFE Middle Tennessee Chapter's Annual Fraud Conference. I have been involved with the ACFE and a CFE since 1995. I have had many roles at the ACFE including adjunct instructor, Regent Emeritus, and Fellow. At the conference I met Odell Guyton, Microsoft's director of compliance, who was also a speaker. Odell was a former federal prosecutor and I was a former federal agent and we shared our experiences and stories. He mentioned that Microsoft was about to start a newly created fraud prevention unit and they were looking for someone to lead it. He asked if I was interested in this challenge. I was excited about this unique opportunity and, of course, I said yes. As a result, he recommended me for the role and the rest is history.

Why label it an FIU rather than the more common name, Special Investigation Unit?

Given the company's focus on preserving integrity, process improvements and prevention rather than just reactive investigations, Financial Integrity Unit was a natural name reflecting our team's important focus beyond just an investigative response. We place less emphasis on the word fraud because our focus on compliance is all about integrity and the expected behaviors from employees and others.

Financial stewardship, responsibility, and integrity are key tenets of Microsoft's Standards of Business Conduct. We wanted to emphasize to our employees, our shareholders, our partners, and our customers that preserving the financial integrity of our company was paramount. Creating and enhancing shareholder value is absolutely critical for our company's performance now and in the future. Fraud and issue resolution, reduction, prevention and recovery of defrauded assets add to the bottom line. We also wanted to reemphasize to our employees that the FIU was there to protect them by mitigating their financial and reputational risk and working with management and the legal and human resources departments.

How does your FIU differ from a traditional SIU?

I think the traditional SIU has undergone many changes so more and more of them are looking like our FIU. From the beginning, we built fraud detection and prevention along with recovery of defrauded assets into the FIU program. We hired people with strong financial analysis skills and data-mining expertise, CPAs, forensic accountants, and, of course, CFEs. We hired former federal agents such as Postal Inspectors and FBI Special Agents just as traditional SIUs do. Removing the profit motive from those who commit fraud through civil and criminal restitution has been part of our program from the beginning. In addition, being based in the Internal Audit Department has provided us with a great interaction with and sharing of audit findings and red flags for further investigation. At times, our investigators have participated in audits to gain a greater understanding of the audit process and identify areas of risk. As a result, our investigators have greater and more productive interactions with the internal auditors. This cross-group collaboration has been critical to the success of the FIU.

What was your strategy when constructing the FIU?

Our goal from the beginning was to build a world-class fraud prevention program at Microsoft. We employed a number of strategies to accomplish this and we're not done yet. It began and continues with the power of people. I learned early in my career that anything is possible when you have passionate, motivated, and dedicated people on your team. Our company's success springs from identifying, hiring, and retaining the best possible people.

So, in addition to hiring the best fraud detection and pre-

By Dick Carozza • Photos by Ron Wurzer

FIU TEAM EXPANDS GLOBALLY

The Microsoft FIU continues to expand throughout the world. Jerry Bamel, CFE, based in Singapore, is group manager of the APAC Team, and Kimberly Phoon, based in Beijing, China, is investigations senior manager for the APAC Team.

vention professionals, our strategy has been a combination of integration of the fraud prevention program into the company, developing policies and procedures, creating a case management system, building a global coverage model, developing employee and management fraud awareness and training programs, implementing fraud detection tools and technology to detect and prevent fraud, and sharing red flags of fraud and improvements in internal controls to reduce fraud and abuse.

The FIU has built a predictable response to allegations of fraud to provide thorough and timely results for management, business, and employment decisions as well as possible referral for criminal prosecution and restitution. There is also a focus on driving continuous improvement in policies, procedures, internal controls, customer satisfaction, and compliance with Sarbanes-Oxley Act certifications and whistle-blower provisions. Priority is given to high-risk/high-profile matters affecting the company.

Our strategy also involves a close interaction and cross-group collaboration with the various other investigative groups at Microsoft that have different but interrelated roles and charters. These groups include corporate security, the employee relations investigation team (within HR), network security, anti-piracy, and Internet safety.

What is the FIU organizational structure?

The FIU, based in the Internal Audit Department, reports to Alain Peracca, the corporate vice president of internal audit, who reports to Chris Liddell, our CFO. Strong executive support has been a hallmark of the compliance program at Microsoft and a critical factor for the FIU's success. Mr. Liddell has told me that Microsoft recognizes that a culture of compliance anchored by a world-class fraud detection, investigation, and prevention program significantly contributes to shareholder value.

The FIU has a strong dotted line to the Office of Legal Compliance (OLC) which is part of the Office of the General Counsel. The OLC's mission is to provide supervision and oversight in the establishment, implementation and maintenance of effective and collaborative compliance and governance programs. The OLC closely oversees and counsels the FIU in all its investigations.

Why do you find the FIU system better than other departmental anti-fraud solutions?

First, let me say that in the last few years I have seen a huge improvement in the anti-fraud programs of organizations everywhere. There is greater attention to fraud risk than at any time I have seen in my career in fraud examination. Just look at the huge growth that the ACFE has experienced worldwide. As for the FIU program, the strength of our program is that we have tried to incorporate the best practices of other great companies as well as coming up with many of our own. We want to be cutting-edge and innovate while incorporating the best that Microsoft technology and software has to offer.

We have seen great progress in building robust fraud prevention programs at companies worldwide especially since the enactment of Sarbanes-Oxley. Cross-group collaboration and benchmarking with a number of other great companies from technology and other industries have helped us in sharing and adopting best practices. For example, we hold benchmarking sessions with our counterparts from technology, financial services, manufacturing, and other industries in group sessions and one-on-one meetings. A number of companies both from the United States and Europe have wanted to learn how we built and continue to grow our program. We learn just as much from them as they do from us.

How do you emphasize the need for FIU employees to "think globally"?

Being a global organization, it is critical that the FIU build a highly diverse team with different backgrounds, cultures, and viewpoints. Microsoft does business in almost 200 countries. Everyone in the FIU has traveled internationally on investigations and for conducting fraud awareness presentations to employees, and many members of the team speak at least two languages. In fact, collectively our team members speak 11 different languages, which is extremely helpful when dealing with complex issues in our international subsidiary offices.

For regional FIU locations, the team's goal is to identify highly qualified candidates from that area in the world. Their experiences, knowledge of culture, contacts and qualifications, are an invaluable asset in conducting fraud investigations. These regional investigators, along with those from the United States, commonly provide proactive fraud awareness presentations via "road shows" to subsidiaries. This allows the team to meet management, and potential stakeholders in future investigations, in a positive setting that allows for building of close relationships outside the parameters of an investigation.

MICROSOFT FIU CONCENTRATES ON DIVERSITY IN HIRING

Diversity is a popular business buzzword, but Martin Biegelman sees it as a method, not a rule, in developing the Financial Integrity Unit. "Our team's diversity permits us to leverage our experiences and skills to enhance our creativity and innovation, and ultimately, to produce better overall results," Biegelman says.

"When people of different backgrounds and experiences work together as a team, they become more effective at achieving our goals," he says. "We become better individuals and thinkers, communicators, and problem solvers." The FIU's team members are from China, India, Singapore, the United States, and soon Russia. The team has former Postal Inspectors and FBI agents, CPAs, lawyers, forensic accountants, and financial analysts. All are, or are studying to become, Certified Fraud Examiners.

The FIU's Americas Team, based in Redmond, Wash., covers the United States, Canada, and Latin America. The Asia Pacific team, APAC, has FIU members in Singapore, Beijing, and Delhi. EMEA, or the Europe, Middle East, and Africa team, has a member in Paris and another soon in Moscow.

"The physical presence of our team members in non-U.S. locations provides a valuable resource to our international colleagues, which we believe contributes to higher levels of accountability and compliance all over the world," Biegelman says.

The Microsoft FIU team is comprised of: Martin Biegelman, CFE, ACFE Fellow, director of the FIU, Redmond; Bob Morgan, CFE, group manager, Americas Team; Shannon Grayer, CFE, CBM, investigations senior manager, Americas Team; Brock Phillips, CFE, CPA, forensic accounting senior manager, Americas Team; Heather Yu, CPA, senior investigative analyst, Americas Team; Susan Pai, J.D., investigations senior manager, Americas Team; Cindy Prudnick, paralegal, Americas Team; Jerry Bamel, CFE, group manager, APAC Team, Singapore; Kimberly Phoon, investigations senior manager, APAC Team, Beijing, China; Gaurav Ajmani, LLB, CFE, investigations manager, APAC Team, Delhi, India; and Stuart Sturm, CFE, CPA, investigations senior manager, EMEA Team, Paris, France.

You've said that the FIU is both reactive and proactive. Can you explain that?

The FIU not only conducts highly sensitive fraud investigations but it exists to ensure a culture of compliance and enhance the company's internal controls. Once an investigation is completed, we conduct numerous steps to help mitigate the risk in other organizations by meeting with key business stakeholders, including the Finance Department and Internal Audit Department.

The FIU helps reduce fraud risk by conducting internal and external fraud awareness presentations. By creating this "perception of detection," we are able to proactively reduce the risk of potential opportunities to commit fraud. Additionally, we have invested significant resources in Technology Enabled Continuous Auditing (TECA), which allows us to strategically identify occurrences of fraud, waste or abuse.

TECA is a blend of technology and statistical evaluation techniques that combine disparate sets of data with targeted queries set to detect outliers that are "red flags" of fraud or violations of policy. TECA seeks to leverage technology to expand the scope and coverage of audit and investigative activities over larger and sometimes seemingly disparate data sets. The system is flexible, with new queries regularly being added to the queue. This helps the team proactively identify additional situations of abuse in a short period of time based upon recent cases. Investigators then review these cases for follow-up. The use of TECA ensures that matters such as expense reporting and claims management, purchase orders, contracts, and other activities are in compliance with the corporate guidelines worldwide. Considering the diversity and complexity in the nature of operations across geographical barriers, TECA is a FIU tool that will play a key role in further reducing fraud risk to the company.

The FIU has also prepared in-depth white papers on various issues such as expense reporting and business funding with an eye on recommended improvements to policies. We have prepared case studies based on our investigations that are used as scenarios in our annual Standards of Business Conduct training for all employees. This year, the team worked with our procurement department to develop a training video on purchasing best practices.

How have the FIU and Microsoft benefited from its relationship with the ACFE?

From the beginning of the FIU, I made it a requirement that my team members would be CFEs. I have seen the growth of the ACFE worldwide and how the CFE certification has become the gold standard for fraud detection and prevention professionals. CFEs are now known the world over as fraud-fighting experts. CFEs, through their education, training, and experience, provide an added value to any organization, public or private, large or small, foreign or domestic. It just makes good business sense to have as many CFEs on my team as possible.

We support everyone on the team becoming a member of the ACFE and actively participating in the organization. We currently have a worldwide team of 11 and seven of us are CFEs. Three are in the process of studying for their CFE certification. We are recruiting for a new position in Russia and that team member will also be a CFE. The goal is for everyone on the team to be a CFE.

How do you encourage your staff to develop professionally through the ACFE and other continuing education sources?

Ongoing training and education is the foundation of professionalism. That's especially true for fraud investigators. No one but the ACFE provides the depth and breadth of anti-fraud training. The ACFE courses focus on the type of work that we do. Just as importantly, ACFE professional training gives us a window into the future for fraud. The FIU has a requirement of a minimum of 40 CPE hours a year and ACFE training helps us accomplish that. I normally send several team members to the Annual ACFE Fraud Conference. I have had team members attend every conference since the formation of the FIU. This year, seven team members attended the conference in Orlando.

We also encourage the professional development of our team by speaking at ACFE events including chapter conferences, the annual fraud conference, and international conferences. In the past year, four team members spoke at various ACFE training events including a joint ACFE/Institute of Internal Auditors conference in Vancouver, B.C., the Dallas Chapter Annual Conference, the Spokane Chapter Annual Conference, and the annual fraud conference.

I also encourage leadership roles in the ACFE for further professional development. For example, our investigations senior manager based in Paris is the secretary/treasurer and a founding member of the new ACFE France Chapter. And I serve on the ACFE Foundation Board of Directors.

How do internal fraud cases come to the FIU?
Employees and others concerned about questionable accounting or auditing matter can submit their concerns confidentially or anonymously by using the Web Allegation Tool at **www.MicrosoftIntegrity.com**, sending a letter or fax to the director of compliance, or by calling our hot line, the Business Conduct Line. The Business Conduct Line is a dedicated, toll-free phone line that is available to employees 24 hours a day, 7 days a week, 365 days a year. It is operated by an external third-party vendor that has trained professionals to take calls, in confidence, and report concerns to the Microsoft director of compliance for appropriate action. Issues come to us from employees, managers, HR, legal, exit interviews when employees leave the company, through internal audits, as well as through our hot line.

What kinds of investigative approaches do you use for different types of cases?
Microsoft is a unique company, with offices in more than 100 countries, doing business in almost 200 countries, with about 80,000 full-time employees and a substantial number of contract and vendor employees. Additionally, there are always new technologies being "dogfooded" – employees are beta testing our new products. Teams might have employees located all around the world, which means the majority of conversations among employees is handled via e-mail. These dynamics influence the investigative techniques each team uses. Each country has a different set of laws and regulations governing corporate investigations. What is legal and allowable in one country might be a criminal violation in another.

The FIU recognizes these issues during the preparation of the investigative plan. The team seeks guidance from the legal department, and possibly outside counsel, to determine the steps that would be appropriate in a given situation in a particular country. In fact, as I've said, all our investigations are conducted under the guidance of legal counsel. When a matter is identified as high-risk, or complex, a second team member will often be called in to assist regardless of the issue's geographical location. We employ both Microsoft technologies and other fraud-detection tools. After conducting the core investigative techniques, each case necessitates a different approach. Often times, after reviewing the data, the team will identify subject matter experts within the business and learn the standard process for an organization. Investigators obtain guidance on all of these techniques from the legal department prior to deployment.

The interview is the culmination of the investigative process. Typically, the investigator will interview witnesses and the potential subject after developing a good understanding of the process and evidence. The FIU team members conduct interviews in a professional and courteous manner. An independent human resources person is always in the interview, and when possible, a second FIU team member is present to assist.

We require investigators to respect all interviewees and be objective and fair when searching for facts. Investigative techniques that might be quite legal and commonly used by law enforcement are not employed at Microsoft. No deception of any kind is used in either our investigations or our interviews. Proving that an allegation is unfounded is just as important as finding that it is.

In this post-SOX era, how can management create a culture of compliance?
Outstanding companies view Sarbanes-Oxley, the United States' Federal Sentencing Guidelines, and other worldwide compliance enhancements as opportunities for improved corporate compliance and governance. They understand and embrace the importance of implementing a strong fraud prevention program and internal control system. Companies that embrace a culture of compliance gain a competitive advantage. Business leaders, employees, and shareholders have learned firsthand what fraud examiners have long known. Fraud and abuse can happen anywhere, and the damaging impact goes far beyond the financial loss. The loss of reputation can be long lasting and often fatal. Warren Buffett, the billionaire investor and CEO of Berkshire Hathaway, has said, "It takes 20 years to build a reputation and five minutes to ruin it. If you think about that, you'll do things differently." Management that take Buffett's comments to heart will make a culture of compliance that much easier.

There are many things that executives and managers can do to create a culture of compliance. The ACFE's Fraud Prevention Check-Up **[www.ACFE.com/document/Fraud_Prev_Checkup_IA.pdf]** is an excellent guide to determine how vulnerable your company is to fraud. The Check-Up includes questions about the organization's fraud risk, risk tolerance, risk assessment, antifraud controls, and fraud detection. By taking this simple, yet effective test of your company's fraud prevention health, you can determine if you have adequate controls in place to prevent it.

"Tone at the top" is another important element for a culture of compliance. It is leading by example. Chief executives, directors and other leaders set an important tone with their every word and action. Their accountability and integrity and how they consistently convey that message to every employee may be the most important aspect in building a compliant culture.

I also recommend the use of the "Management Antifraud Programs and Controls: A Guidance to Prevent and Deter Fraud," that is an exhibit to SAS 99 **[www.ACFE.com/documents/AntifraudDocument.pdf]**. This document provides organizations a detailed road map in creating a culture of honesty and high ethics, evaluating antifraud processes and controls, and developing an appropriate oversight process. Included in the guidance is the importance of setting and maintaining tone at the top, the role of the audit committee, effective internal audit, truly independent external auditors, and the value of having Certified Fraud Examiners as part of an anti-fraud program.

We always hear about encouraging the tone at the top. Practically, how do you do it?
Senior management largely guides an organization's culture. The leadership sets the tone for the rest of the organization, and the culture reflects these actions, whether positively or negatively. Employees pay careful attention, whether consciously or not, to their leadership and their actions. We try to build the tone at the top through our professional compliance department and the FIU, ongoing and mandatory training in our code of conduct, a highly skilled and effective internal audit function, a strong and independent board of directors, and the support of executive leadership.

Communicating the importance of compliance is another way to demonstrate tone at the top and encourage ethical conduct. Microsoft's Office of Legal Compliance publishes the Compliance & Ethics Quarterly Report that is distributed to all employees around the world and serves to highlight Microsoft's policies, investigations, and trainings. It includes details on upcoming training, answers compliance questions posed by employees, provides contact information for reporting compliance concerns and questions, and recent compliance investigations.

A company's code of conduct is a further reinforcement of tone at the top. Our Standards of Business Conduct states, "As responsible business leaders, it is not enough to do things rights, we must also do them in the right way. That means making business decisions and taking appropriate actions that are ethical and in compliance with applicable legal requirements." The company leadership also encourages people to speak up and ask for guidance on a particular business practice or compliance issue or to report a possible violation.

From the ACFE's inception, Chairman Wells has emphasized prevention and deterrence. How does the FIU stress those components among Microsoft employees?
In his seminal book on corporate fraud, "Corporate Fraud Handbook: Prevention and Detection," Joe Wells emphasized the importance of deterrence and employee education when he stated, "The fraud-educated workforce is the fraud examiner's best weapon – by far." In employee and management training sessions, FIU team members share examples of compliance failures and how to make sure they are not repeated in their groups. We contribute case studies to the Compliance & Ethics Quarterly Report to provide further awareness and prevention. The Office of Legal Compliance and human resources also provide ongoing training in our policies and procedures.

Can you talk a bit more about the company's codes of conduct?
As part of its operations, Microsoft investigates suspected illegal activities that might harm the corporation and its customers, such as spamming, hacking, piracy, malware, and fraud. On occasion and upon request, the company might also assist law enforcement agencies in the investigation of suspected criminal activity. Microsoft also conducts internal investigations of alleged employee misconduct including violations of law and Microsoft policies. In all aspects of its investigative work, the company seeks to uphold the highest ethical and legal standards, as outlined in the company's Investigations Code of Professional Conduct and Standards of Business Conduct.

Microsoft strives for the most professional level of investigators and to lessen non-compliance issues to avoid liability for failure to comply with appropriate investigative procedures. All Microsoft employees involved in investigations, including investigators and attorney or non-attorney managers overseeing investigations and the work of investigators, as well as outside vendors retained for investigative work, will acknowledge and certify their compliance with the Investigations Code of Professional Conduct on an annual basis.

The company's code states that investigators:

- will conduct investigations in an unbiased, diligent, and professional manner;
- will conduct their investigations with honesty and integrity and will use only those investigative techniques that comport with the highest ethical standards;
- will gather and handle information and other evidence in a manner that respects the privacy rights of customers, partners and subjects of investigations, and protects the integrity of that evidence; and
- will comply with all applicable laws, regulatory requirements, Microsoft policies, and this Code of Conduct.

Microsoft's code of conduct for its employees worldwide, the Standards of Business Conduct, summarizes and is supported by the principles and policies that govern our global businesses in several important areas: legal and regulatory compliance; trust and respect of consumers; partners and shareholders; protection and management of Microsoft assets; sustainability of a cooperative, diverse and productive work environment; and our com-

mitment to citizenship. These standards provide information, education, and resources to help employees make good, informed business decisions and to act on them with integrity.

Microsoft is a global company, and our business operations are subject to the laws of many different countries. Employees doing business internationally must comply with applicable laws and regulations and uphold the Standards of Business Conduct at all times. Cultural differences or local laws and customs might require a different interpretation of our standards. If this situation arises, we encourage our employees to always consult their manager, the law and corporate affairs departments, or the director of compliance before taking any action.

How has your experience as a U.S. Postal Inspector and director of litigation and investigative services in the fraud investigation practice at BDO Seidman LLP prepared you for this position?

My years investigating fraud as a U.S. Postal Inspector and then later as an investigative consultant positioned me well for my role at Microsoft. As a federal agent, I saw firsthand the government's enforcement and prosecution role in protecting individuals and businesses. In my investigations, I learned how personal and business failures contributed to the many asset misappropriation, financial accounting, and corruption cases I investigated. In my career, I arrested hundreds of fraudsters. But no matter how many I successfully investigated and prosecuted, others quickly surfaced to take their places. Prosecutions didn't return the financial losses to businesses. Few cases ever resulted in full restitution to victims. It was even harder to restore lost reputations to organizations crippled by fraud. I grasped the need to do more than just react when a compliance failure was discovered.

Later, as a consultant in litigation and investigative services, my clients included public and private companies, both foreign and domestic. I saw how compliance worked, but more often than not, how and why it didn't. I was shocked at the number of companies of all types and sizes that had either no compliance programs or poorly conceived ones. My clients never thought they would be victims of fraud or involved in committing a fraud. The compliance failures they encountered were wake-up calls for them. My experience in both government and consulting has given me great insight into the fraud and compliance issues that organizations of all types face as well as best practices and strategies for success in preventing them.

Dick Carozza *is editor in chief of* Fraud Magazine. *His e-mail address is:* ***dcarozza@ACFE.com***.

ETHICS AND COMPLIANCE WILL ALWAYS MATTER

BUILDING COMPLIANCE PROGRAMS

Compliance programs have to be more than faddish reactions to corporate scandals. Management must commit to not only obeying laws but devising programs that they will enthusiastically support with funding, skilled personnel, and a determined attitude to do what's right – over and over again.

This article is excerpted and adapted from "Building A World-Class Compliance Program: Best Practices and Strategies for Success," by Martin T. Biegelman with Daniel R. Biegelman. Published by John Wiley & Sons Inc.

Imagine this nightmare scenario: A publicly traded company whose domineering leadership rules by fear. Dissenting opinion in any form is met with immediate termination of employment. A culture where written policies and procedures are few and far between and internal controls are shunned. Training is sporadic and lacking. Eventually, this company's most senior executives conspire to prematurely and fraudulently recognize revenue to meet or exceed Wall Street's expectations. They conduct this massive fraud year after year. The board is totally in the dark and accepts management's explanations and assurances without independent verification. When their accounting practices finally are scrutinized and the government starts an inquiry, these executives attempt a cover-up by fabricating a story, obstructing the investigation, and suborning perjury by instructing other employees to lie to the government and outside counsel. Ultimately, eight of the company's senior executives, including the CEO, CFO, and general counsel, plead guilty to securities fraud and/or obstruction of justice charges. Shareholders lose more than $10 billion because of the massive accounting fraud.

Employees are left shocked and demoralized that their leaders have lied and defrauded their company. Investors are also horrified at seeing their investments diminish and that no one in the company did anything to stop it. Add to this explosive mixture the fact that the company had no compliance program. That's right, no compliance program. Think this couldn't happen? Think again because it did.

By Martin T. Biegelman, CFE, ACFE Fellow, with Daniel R. Biegelman, J.D.

This all occurred at Computer Associates, now called CA Inc. These blatant transgressions happened because an effective ethics and compliance program was not in place. Compliance involves many different elements; knowing and following all the relevant laws, rules, and policies is but one part of the mix. An effective compliance program would have made a difference at CA. A strong compliance program is absolutely necessary to protect an organization both internally and externally.

Compliance means following the law and more. It's making sure organizations adhere to all applicable legal requirements. It is a detailed and complex process. For any particular situation one must be aware of all potentially applicable laws and regulations – federal, state, local, as well as internal company-instituted rules. A company is obligated to be aware of and understand these rules and laws. That in itself can be an onerous process as even experienced and sophisticated lawyers sometimes have a difficult time deciphering the cryptic "legalese" that passes for statutory language. This compliance obligation is important because everyone in authority is charged with knowledge of the law. Ignorance of the law is no excuse. A person cannot escape a criminal charge or civil liability by claiming that he or she did not know the law was being broken. This is the role of compliance, to make sure people know the rules beforehand and help to ensure that they continuously follow them.

Simply following the law so that one doesn't get into trouble is not full compliance. State-of-the-art compliance involves a successful blending of compliance – following rules, regulations, and laws – with ethics – developing and sustaining a culture based on values, integrity, and accountability, and always doing the right things. True compliance ensures consistency of actions to eliminate, or at least lessen, opportunities for harm from criminal conduct or other compliance failures.

Knowledge and understanding of the law is the first step. Businesses also have to know to what and where it applies. Furthermore, once one has this information, one must implement it in an effective compliance program. But what does effective mean? A company must carefully craft a program, hire experienced compliance professionals, issue detailed policies and guidance, institute training, and promote all other aspects of the program to ensure the knowledge is spread to all who need it. This process must be continuous. The compliance program is the engine of compliance, putting all of this into effect.

Knowing the law and following it is only one side of compliance. Compliance goes much deeper than that, true compliance anyway. Simply following the law so that one doesn't get into trouble is not full compliance. State-of-the-art compliance involves a successful blending of compliance – following rules, regulations, and laws – with ethics – developing and sustaining a culture based on values, integrity, and accountability, and always doing the right things. True compliance ensures consistency of actions to eliminate, or at least lessen, opportunities for harm from criminal conduct or other compliance failures. It means going beyond the minimum requirements. More importantly, it involves the ongoing commitment from senior leaders in the organization to promote ethical conduct and compliance with the law. Leading by example and establishing the tone at the top set the stage for every other element of compliance.

The problem that can occur is when people use compliance as an excuse – those who profess to believe in it but use a compliance program to mask their own negligence or even wrongdoing. It may be said that this is even more dangerous than having no compliance program at all. That is because it gives shareholders, employees, vendors, and the public the false belief that the company cares about following the law when in fact, all it wants is to deceive others into believing so. Let us not forget that Enron had a 65-page code of conduct, but in the end, it was nothing more than empty words.

Enacting a compliance program and instituting training programs but not supporting them through lack of funding, lack of skilled personnel, or by management undercutting them in various ways, is also dangerous and counterproductive. Real compliance means that one believes in what one is doing day in and day out. It is not merely lip service; it's putting your money where your mouth is. This is the two-tiered approach to compliance – one's actions and one's mind-set. An organization cannot have effective compliance without both of them. One alone will not work. This is tied into the idea of setting a positive tone at the top. If management believes in compliance and reinforces it by their actions, over and over again, then people below will follow their lead.

ETHICS IS JOB ONE

Executives are constantly confronted with the realities of business compliance. They must ensure compliance with their internal rules and policies. Those from public companies must follow the requirements of the Sarbanes-Oxley Act and other reporting enhancements. All organizations must follow federal, state, and local laws and all must comply with the United States' Federal Sentencing Guidelines, which mandate the creation of compliance programs. Moreover, a raft of other laws must be complied with, from anti-bribery rules to free trade provisions. Yet, chief among these requirements is the idea of ethics, the concept that lies at the heart of every corporate governance requirement.

Ethics include integrity and proper business conduct; it refers to standards and values by which an individual or organization behaves and interacts with others.[1] The famed Greek philosopher Aristotle in his "Nicomachean Ethics" argued that "moral behavior is acquired by habituation" and that without question, "moral behavior is good."[2] It is no different today. Ethics and compliance are clearly on the minds of executives, as well as investors, the public, and the government. Ethics has become a hot-button topic, thanks to the many corporate scandals of the past years. *(See page 28, to read how ethics programs can help the bottom line. – ed.)* This is hardly news to anyone. Despite the increased awareness given to ethics and compliance programs, the problem has not been solved. For instance, the Hewlett-Packard (HP) spying and pretexting scandal involved key executives and illustrates that there is more to successful compliance than just a code of conduct. HP had a comprehensive Standards of Business Conduct (including, slightly ironically now, several pages on how to handle sensitive information), yet it still was engulfed by negative front-page headlines and a shakeup among its leadership. Even great corporations like HP can, at times, face compliance failures. Merely having a program in and of itself is not the solution to protecting a company and keeping it in good graces with shareholders and the government. A truly successful compliance program goes far deeper.

The push toward compliance, especially since the enactment of the Sarbanes-Oxley Act and the reaction to the scandal culture of the Enron era, could almost be described as an "ethics fad." Sarbanes-Oxley strengthened corporate accountability and governance of public companies through rules covering conflicts of interests, financial disclosures, board oversight, and certification of financial statements.[3] The Act's passage left companies hurrying to comply. All of a sudden, every company had to have an ethics code; if there wasn't one there was scrambling to get one, or else be left behind. This rush merged with heightened concerns stemming from the penalties imposed on companies for ethical breaches. From the lighter treatment afforded to companies who came clean and "restated" their earnings, as compared to those formally investigated and charged by the government, companies got the message that it was in their best interest to cooperate and that having a compliance program would be something that would lessen potential penalties should the company commit further misdeeds.

Companies that the government caught red-handed had to pay very stiff financial and reputational penalties, not to mention the personal impact on those executives prosecuted and sent to prison. This sent companies searching for ways to avoid this disastrous outcome. At the same time, ethics enjoyed a renewed focus throughout the corporate world, first as companies struggled to understand the new requirements placed on them by the passage of Sarbanes-Oxley, and then rushed to embrace ethical conduct for chief executives and others. The ethics fever swept every industry and that was a good thing, a very good thing. While this practice makes compliance easier, there is still much to do as compliance lapses and criminal conduct persist. The Securities and Exchange Commission (SEC) has continued its strong enforcement program over the last few years.

Ethics and ethical behavior are not things that can merely be created or attained solely through corporate expenditure. They require a deeper commitment, one that can only be achieved through time, effort, and yes, expenditure. Though it is a cliché, quality matters here far more than quantity. In many senses, a little goes a long way. Building a world-class compliance program requires smart decisions in building it, maintaining it, and sustaining it; by doing so, a company will be able to achieve truly effective compliance over the long term.

THE NYPD AND AN ETHICAL CULTURE

A commitment to ethical conduct cannot be accomplished by simply initiating a program and then checking the box that the process is complete. Building a culture of compliance takes time. Integrity and character bring out the best in people and are critical components in ethics and compliance. Yet, human beings are not perfect creatures and tend to falter from time to time. The importance of ethical conduct needs to be nurtured, reinforced, and repeated over and over again lest people forget and stray from the course. There is no better example of this continuous need for attention to ethical conduct than the various police corruption scandals that have impacted the New York City Police Department (NYPD) over the past 100 years. Even legendary institutions can face the firestorm created when law enforcement officers forget their oaths and turn to crime and corruption.

The feeling of déjà vu that the NYPD faced was due to not learning from the past. The NYPD of the 21st century has made great strides in understanding that ethical lapses can seriously impact a long-standing reputation. In building its compliance program, the NYPD starts with police recruits as soon as they enter the police academy. Look at what is presented to recruits in its "Police Student's Guide: Introduction to the NYPD":

Our history is a source of great pride to us, and we have very little tolerance for officers who do not treat our hard won reputation with the respect it deserves…. When things go right in this Department – when we succeed in reducing crime; when we make spectacular arrests; when we make dramatic rescues – our actions are described in news reports throughout the country and across the world, and our officers are treated like heroes. But, when things go wrong – when officers are caught in scandal, or when they make some tragic mistakes – the same reporters and leaders who are quick to praise us are quick to condemn us. When this happens, the public often does not recognize that the problem may be limited to one or only a few officers. Instead, in the eyes of many people, we all become suspect, and the mistakes and sins of a few are generalized to all of us. This breeds distrust among the public, and makes it tougher for all of us to do the job the way we should. . . . Make certain that you carry yourself in a manner that brings only respect to yourself and to your brothers and sisters in this Department.[4]

Warren Buffett, the billionaire investor and CEO of Berkshire Hathaway Inc., has said, "It takes 20 years to build a reputation and five minutes to ruin it. If you think about that, you'll do things differently." The NYPD understands this and so must all organizations. Yet, we often fail to learn from the past. The disclosure of stock option backdating scandals in 2006 at dozens of companies, large and small, in the United States brought back distressing memories of the accounting scandals of just a few short years ago. How could so many smart people forget the lessons of Enron, WorldCom, Adelphia, and others? The sheer number of companies involved is striking. Much of the misconduct took place

a number of years ago and was only recently disclosed. Still, the participants were chief executives and other high-level employees who should have known better. More importantly, their compliance programs did not work.

WHAT IS COMPLIANCE?

Compliance is a state of being in accordance with established guidelines, specifications, or legislation.[5] The Compliance and Ethics Leadership Council defines compliance as "a company's or an individual's observance of relevant laws, regulations, and corporate policies. ... Companies must have various programs, policies, and controls in place in order to be defined as being 'compliant' with certain laws, rules, regulations, or policies."[6]

The United States Department of Justice (DOJ) has strongly reinforced the importance of effective compliance programs. The DOJ defines compliance programs as follows:

Compliance programs are established by corporate management to prevent and to detect misconduct and to ensure that corporate activities are conducted in accordance with all applicable criminal and civil laws, regulations, and rules. The Department encourages such corporate self-policing, including voluntary disclosures to the government of any problems that a corporation discovers on its own. However, the existence of a compliance program is not sufficient, in and of itself, to justify not charging a corporation for criminal conduct undertaken by its officers, directors, employees, or agents. Indeed, the commission of such crimes in the face of a compliance program may suggest that the corporate management is not adequately enforcing its program. In addition, the nature of some crimes, e.g., antitrust violations, may be such that national law enforcement policies mandate prosecutions of corporations notwithstanding the existence of a compliance program.[7]

> While quality matters more than quantity, a solid compliance program needs a proper balance between the two. An under-funded and unsupported program is doomed to fail. Without sufficient support by the company and the management, a program cannot succeed in its objectives of changing and influencing employee behavior.

The key to effectiveness is whether the program is adequately designed to ensure compliance. The United States' Federal Sentencing Guidelines for Organizations (FSGO) state that "to have an effective compliance and ethics program, an organization shall exercise due diligence to prevent and detect criminal conduct; and otherwise promote an organizational culture that encourages ethical conduct and a commitment to compliance with the law."[8] The constantly evolving compliance landscape requires executives and managers to constantly ensure that their programs are "best in breed" to fully protect organizations.

Organizations that run afoul of the law and commit crimes such as fraud, face severe penalties from the courts. Under the FSGO, organizations found guilty can face additional penalties based on certain aggravating factors calculated by a "culpability score." As stated in the FSGO, the factors contributing to increased penalties and fines include whether:

- senior executives within the organization "participated in, condoned, or [were] willfully ignorant of the offense";
- "tolerance of the offense by substantial authority personnel was pervasive throughout the organization";
- there was prior history of a similar offense in the company's past and/or;
- the organization obstructed justice by impeding the investigation or prosecution.[9]

The FSGO also provide a significant "carrot" or benefit in that there are mitigating factors that can significantly lessen the penalties for criminal convictions. The questions that will determine if these factors are to be considered include:

- if the subject "organization had in place at the time of the offense an effective compliance and ethics program";
- if the organization promptly "reported the offense to appropriate government authorities" once they became aware of its existence;
- if the organization "fully cooperated in the investigation"; and
- if the organization "clearly demonstrated recognition and affirmative acceptance of responsibility for its criminal conduct."[10]

While quality matters more than quantity, a solid compliance program needs a proper balance between the two. An under-funded and unsupported program is doomed to fail. Without sufficient support by the company and the management, a program cannot succeed in its objectives of changing and influencing employee behavior. Compliance requires direct input by company leadership, and the key support of a qualified compliance officer running a reliable compliance department, accessible to the rank and file to answer their questions and provide them with appropriate direction. However, spending too much money (without proper guidance on how to spend and direct funds) can lead to incredible inefficiency, and be just as ineffective as not spending.

Regardless, a sound compliance program *has* to become the heart and lungs of an organization infusing new oxygen into its lifeblood. Management cannot just give it lip service but must support it wholeheartedly by daily examples of ethical and compliant conduct.

Martin T. Biegelman, CFE, ACFE Fellow**, is director of financial integrity for Microsoft Corporation in Redmond, Wash. His e-mail address is: **martinbi@microsoft.com

Daniel R. Biegelman, J.D.**, is a 2006 graduate of St. John's University School of Law and currently practices in New York City. His e-mail address is: **dbiegelma@yahoo.com

[1] "Preempting Compliance Failures: Identifying Leading Indicators of Misconduct." Compliance and Ethics Leadership Council. April 26, 2007.
[2] Aristotle. *Nicomachean Ethics*. Translated by Martin Ostwald. (Englewood Cliffs, NJ: Prentice Hall, 1962), xix.
[3] Martin T. Biegelman and Joel T. Bartow. *Executive Roadmap to Fraud Prevention and Internal Control: Creating a Culture of Compliance*. (Hoboken, NJ: John Wiley & Sons, 2006), 64.
[4] New York City Police Department. *Police Student's Guide: Introduction to the NYPD*. July 2005, 4–5, **home2.nyc.gov/html/nypd/html/dctraining/pdf/2005%20Police%20Students%20Guide/1st%20Trimester/01-Intro%20to%20the%20NYPD.pdf**.
[5] Definition of compliance found at PEMCO Corporation Corporate Services library site, **www.pemcocorp.com/library/glossary.htm**.
[6] "Preempting Compliance Failures."
[7] Paul J. McNulty, "Principles of Federal Prosecution of Business Organizations." Department of Justice. December 2006. **www.usdoj.gov/dag/speech/2006/mcnulty memo.pdf**.
[8] *Federal Sentencing Guidelines*. Chapter 8, Part B, Effective Compliance and Ethics Programs. **www.ussc.gov/2005guid/8b2 1.htm**.
[9] *Federal Sentencing Guidelines*. Chapter 8, Part C, Fines. **www.ussc.gov/2005guid/8c2 5.htm**.
[10] Ibid.

CA INC. GETS A SECOND CHANCE

It's not often that a person or an organization gets a second chance to right an awful wrong. But redemption and positive change can occur, even from the wreckage of corporate fraud and scandal. Such is the case with CA Inc. (formerly Computer Associates), which is a major technology company with worldwide operations. CA suffered through several years of a very public government investigation, media headlines of accounting fraud at the highest levels, prosecutions and convictions of many in its executive leadership, and a negative impact on its reputation and shareholder value. The fact is that CA did not have a compliance program when the massive accounting fraud was occurring. Yet, the very positive changes that CA subsequently made provide learning points and best practices for other organizations. Ultimately, CA endured a very painful process and survived as a company, albeit a much changed and better one.

Patrick J. Gnazzo, is senior vice president and general manager for CA's U.S. public sector business, but he joined the company in January 2005 as the company's first compliance officer (CCO). Gnazzo was responsible for developing and implementing a comprehensive compliance and ethics program. He also directed government regulatory compliance and the establishment of a records and information management program. Prior to joining CA, Gnazzo served as CCO at United Technologies Corporation (UTC) for 10 years. As vice president for business practices at UTC, he built and led an ethics program that is among the best in the world.

Gnazzo provides his five best practices for a world-class compliance program, but he qualifies it by saying that there are other important aspects too.

1. The CCO needs to be "seen at the table" with other top executives. That's everyone with a "c" at the beginning of their title. That person must have complete access to everyone at the company, no matter their level, and not have to make an appointment to meet. The CCO must be highly visible at the company and have significant experience and standing in the field.
2. The CCO must be independent with a solid reporting line to the audit committee and a dotted line to the general counsel.
3. The company must have an open communication program in which anyone can report an allegation or issue through many different channels and have it addressed quickly.
4. The company must have a strong investigative response and process for allegations. The compliance department must have skilled investigative professionals who know how to obtain and analyze information, conduct interviews, report on findings and improve the compliance and ethics program.
5. A best practice is embedding business practice officers in offices worldwide.

In addition, Gnazzo believes that not just the audit committee but the entire board needs to be heavily involved in compliance. All board members need to know the CCO and interact with him or her. They must thoroughly understand how the compliance program works. Gnazzo got before the entire board each year to discuss a topic or issue. He interacted closely with each member. This puts the compliance program on par with all the other business operations and programs at CA. It is clear that the CCO is a valuable part of the equation for compliance excellence.

A world-class CCO needs a variety of knowledge, skills, and abilities. Business acumen is an absolute requirement. A CCO who can meet with a business division president and talk the same language is a tremendous asset to the compliance program's standing.

Source: "Building A World-Class Compliance Program" by Martin T. Biegelman with Daniel R. Biegelman

Risk & Control Self-Assessment

RCSA Fraud Risk Statements

Risk Type	Risk Category	Corporate Risk Statement	Definitions	Schemes/Examples
1. Internal Fraud	1.1 **Fraudulent Financial Statements:** Financial Statement Misrepresentation or Manipulation	1.1.1 Risk of Improper Revenue Recognition	Intentional overstatement of revenue in the Company's financial statements by means such as recording fictitious revenue, or by prematurely recognizing revenue.	Improper calculation of amortization; Improper Side letter agreements
		1.1.2 Risk of Misrepresentation of Assets	Intentional misrepresentation of assets in the Company's financial statements to improperly record asset value. This could include, assigning an improper value to recorded assets, recording of fictitious assets, or use of improper valuation methodology.	Improper valuation of investments and derivative transactions; Overstated or fictitious assets; Incorrect amounts are recorded in the general ledger; Journal entries that include intentional errors are posted to the general ledger.
		1.1.3 Risk of Misrepresentation of Liabilities and Expenses	Intentional misrepresentation of liabilities and expenses in the Company's financial statements. This could include improper capitalization of expenses, inflating balance sheet or misstating reserves.	Misstating accounting estimates or payables; Improperly recording expenses as prepaid expenses thereby improving entity's income statement and inflating balance sheet or understating reserves; Improper use of foreign currency rates; Delaying the recording of expenses made near the closing period until the next accounting period; Misrepresentation or misuse of the reserves.
	1.2 **Giving Misinformation about the Company:** Improper Disclosure of Business Information by Internal Parties	1.2.1 Risk of Misrepresentation of Financial or Non-Financial Information to Internal Parties	Intentional omission or misstatement, for improper gain, of material business information to internal parties, excluding financial statement misrepresentations of financial statements as defined in 1.1.	Intentional misrepresentation of budget information; Intentional misrepresentation of periodic financial or operational reporting; Concealing losses or inflating profit at the business unit level.
		1.2.2 Risk of Misrepresentation of Financial or Non-Financial Information to External Parties	Intentional omission or misstatement of material information in public filings or in communications with regulators, analysts, investors or counterparties in audited financial statements, unaudited filings, or other non-financial business information, excluding financial statement misrepresentations of financial statements as defined in 1.1.	Omission or misstatement of material financial disclosures in public filings; Intentionally providing misleading information in unaudited filings such as the Management Discussion & Analysis portion of the 10K; Intentionally providing misleading information on executive compensation; Intentionally providing misleading information to counterparties, vendors or partners in connection with business plans, contracts, products or risk.

Risk & Control Self-Assessment

RCSA Fraud Risk Statements

Risk Type	Risk Category	Corporate Risk Statement	Definitions	Schemes/Examples
	1.3 **Theft**: Asset Misappropriation by Internal Parties	1.3.1 Risk of Cash Asset Misappropriation from Company or External Parties	Employee theft of monetary assets from Company, or external parties, for improper gain.	Misdirected wires; Payroll fraud; Fictitious vendors; Improper (overpayment) disbursements to third parties in return for kickbacks to employee; Falsifying documents for purchasing authorization; Collusion with customer for employee and/or customer benefit. Manipulate pricing or contract terms in collusion with a customer to benefit the employee and/or customer.
		1.3.2 Risk of Physical, Information or Intellectual Property Asset Misappropriation from Company or External Parties	Employee theft of physical, information or intellectual assets owned by Company or external parties, for improper gain.	Theft of computers or other fixed assets; Theft of confidential customer pricing information; Theft of Company portfolio modeling information; Theft of customer data.
	1.4 **Falsifying Information about Business Transactions:** Misrepresentation of Business Transactions	1.4.1 Risk of Improper Receipts and Expenditures	Revenue, assets, costs or expenses are manipulated or presented in a manner that does not reflect their fair values, for purposes of improper gain.	Illegal marketing; Improper loan acquisitions; Improper trading arrangements; Overbilling customers; Tax evasion; Fraudulent avoidance of brokerage fees or contractual obligatory payments
		1.4.2 Risk of Money Laundering by Internal Parties	The act of intentionally transforming proceeds illegally obtained into seemingly legitimate funds.	Funneling cash through various accounts to conceal the illegal source.
	1.5 Insider Trading	1.5.1 Risk of Insider Trading	The intentional buying and selling of Company shares or of a third party's shares for improper benefit, by internal or external parties with access to material, nonpublic information.	Insider trading based on privileged information; Providing privileged information to third parties who engage in trades.
	1.6 **Wrongdoing by Senior Management:** Misconduct by Privileged Employees	1.6.1 Risk of Misconduct by Senior Management (SVP and above) and by individuals with significant authority over financial reporting	Risk of intentional misconduct by Senior Company employees with significant authority or influence.	Conflicts of Interest; Related Party Transactions; Business Expense Fraud; Illegal Political Contributions; Improper use of Fiduciary Funds; Bribery.

Risk & Control Self-Assessment

RCSA Fraud Risk Statements

Risk Type	Risk Category	Corporate Risk Statement	Definitions	Schemes/Examples
2. External Fraud	2.1 **Theft**: Asset Misappropriation by External Parties	2.1.1 Risk of Cash Asset Misappropriation from Company by External Parties	Theft of Company's monetary assets by an external party, or theft of an external party's monetary assets, where Company is associated with the transaction.	Misdirected cash payments; Overbilling; Non-delivery of paid asset; Direct theft of Company monetary asset.
		2.1.2 Risk of Physical, Information or Intellectual Property Asset Misappropriation by External Parties	Theft of Company or external party physical, information or intellectual assets by external parties for improper gain.	Illegal acquisition of trade secrets or company confidential information; Improper disposal or safeguarding of Company proprietary or confidential data in order to facilitate third party or personal gain (e.g., stealing consumer information, social security numbers, etc.); Theft of laptop.
	2.2 **Falsifying Business Information:** Misrepresentation of Information by External Parties	2.3.1 Risk of Misrepresentation of Financial Information to Company by External Parties	External parties misrepresent themselves to Company such that they do not reflect their true financial situation or business capacity.	Falsify business capacity; Falsify financial statement information; Lenders intentionally making changes to their organization without informing Company in order to hide assets or deficiencies and retain or gain favorable terms from Company.
		2.3.2 Risk of Misrepresentation of Business Information by External Parties to Company Shareholders, Regulators, Investors, Customers or the General Public	External parties intentionally misrepresent their association with Company to other third parties, or intentionally misrepresent Company business information material to a transaction or other activity.	External parties misrepresent Company mortgage product details to customers; Third parties improperly imply partnership arrangement with Company to the public; Community redevelopment project misrepresents its association with Company in order to gain support.
		2.3.3 Risk of Money Laundering by External Parties	The act of intentionally transforming proceeds illegally obtained into seemingly legitimate funds.	Funneling cash through various accounts to conceal the illegal source.

THE WHITE PAPER

JAN/FEB, MAR/APR 2004

Designing a Robust Fraud Prevention Program

By Martin T. Biegelman, CFE, ACFE Fellow

There may not be a more opportune time for a fraud examiner to press for a full-fledged fraud prevention program.

New York Attorney General Eliot Spitzer, Wall Street's corporate cop, has made headlines the last few years with his highly publicized probes, prosecutions, and billion-dollar settlements involving brokerage firms and mutual funds that defrauded and misled investors. The subjects of his investigations read like a Who's Who of the investment world. Credit Suisse First Boston, Merrill Lynch, and Salomon Smith Barney were accused of issuing fraudulent research reports and paid fines totaling in the hundreds of millions of dollars to settle their cases. Spitzer's office obtained the conviction of the vice chairman and chief mutual fund officer of Fred Alger & Company, a prominent mutual fund. Other ongoing investigations involve some of the top mutual funds.

Spitzer and his team of investigators and prosecutors have become the de facto fraud detection and prevention arm of these firms because the firms couldn't do the job themselves. These companies obviously had fraud prevention programs that didn't work and didn't protect their firms, their employees, or their shareholders from the devastating charges and resultant publicity. Where were the fraud prevention basics that should have been in place?

Many high-profile corporations have learned the hard way about the devastating effects of fraud. Enron, WorldCom, and Tyco – among many corporations – all had security departments but they couldn't do anything to protect employees and shareholders from executives determined to loot their own companies.

All entities – including yours – need robust fraud prevention programs staffed with savvy and cunning fraud examiners. The ideal program will protect a company from itself by:

- instituting a hotline;
- setting the principled "tone at the top";
- developing a code of conduct and a confirmation process;
- creating a positive environment;
- hiring and promoting appropriate employees;
- instituting continuous training;
- having fair and balanced discipline;
- identifying and measuring fraud risks;
- implementing and monitoring internal controls;
- having a strong and independent audit committee;
- hiring effective internal auditors and Certified Fraud Examiners;
- contracting independent external auditors;

- constructing a Fraud Investigation/Financial Integrity Unit;
- using case management and technology tools; and
- emphasizing cross-group collaboration.

I know – You've heard it all before. But as a fraud examiner you may now have some extra clout fueled by enraged stakeholders and the public, and fortified enforcers. There may be no better time to try to institute these important principles into our entities. It's either a cliché or a time-honored proverb but an ounce of prevention is worth a pound of cure.

Robust not Wimpy

Robust is defined as “having or exhibiting strength or vigorous health, firm in purpose or outlook, and strong.” Nothing less than a robust fraud prevention program is de rigueur in today's corporate environment. If companies don't get their fraud mitigation houses in order, government investigators will come knocking at their doors with search and arrest warrants.

Stopping fraud before it happens is the ultimate goal of a successful prevention and awareness program.

COSO History Lesson

Let's review a little history. The Committee of Sponsoring Organizations (COSO) is a voluntary private-sector organization dedicated to improving the quality of financial reporting through business ethics, effective internal controls, and corporate governance. COSO was formed in 1985 to sponsor the National Commission on Fraudulent Financial Reporting, an independent private-sector initiative which studied the causal factors that can lead to fraudulent financial reporting and developed recommendations for public companies and their independent auditors.

COSO believes that internal controls are an important component of a robust fraud prevention program. Internal controls can only provide reasonable, not absolute, assurance and should be geared to the achievement of objectives. In 1992, COSO issued a landmark report on internal controls that if adopted by a company would aid in (1) efficient and effective operations, (2) accurate financial reporting, and (3) compliance with laws and regulations. The report outlined the five essential elements of an effective internal controls program:

- the control environment, which is the basis for the system by providing fundamental discipline and structure;
- risk assessment, which involves the identification and analyses by management of risks to achieving predetermined objectives;
- control activities or policies, procedures and practices to ensure that management objectives and risk mitigation are achieved;
- information and communication by management so that all employees are aware of their control responsibilities and their requirement to support them; and
- monitoring, which encompasses external oversight of internal controls by management and independent auditors outside the process to determine the quality of the program and compliance.

A COSO framework is the standard for many major corporations in the United States and there is no reason the same framework could not be universally used worldwide.

However, the voluntary COSO didn't stop many corporations from imploding. Enron had controls in place but they could and were overridden by senior management. Arthur Andersen, its auditor, developed Enron's risk assessment framework but Enron didn't follow it. Enron's “push the envelope” environment, emanating from the highest levels of the company, contributed to its implosion.

History Lesson Continues: Sarbanes-Oxley and AUS 210

And now for some recent history. The U.S. corporate scandals occurring in the last few years resulted in the government's response – the Sarbanes-Oxley Act of 2002 (SOX). A falling stock market, billions of dollars in investor losses, and an outcry from an angry public forced the government to act. SOX is intended to improve corporate accountability and responsibility, improve fraud detection and prevention, and reassure investors that it is safe to invest in the American stock market. (See The White Paper, March/April 2003.)

Even before SOX, the Australian government introduced in April 2002, a new auditing standard, AUS 210, to hold management responsible for the detection and prevention of fraud. Like SOX, AUS 210 requires management to provide the independent auditor with an acknowledgment of management's responsibility to implement internal control systems designed to mitigate fraud. The standard also says that management could be held accountable if prevention programs are not in place but fraud occurs.

Both AUS 210 and SOX make it easier for whistle-blower employees to report suspected fraud. SOX requires that the audit committee of each publicly traded company establish procedures for receiving, retaining, and responding to complaints received by the issuers including the confidential, anonymous submission of questionable accounting, internal accounting controls or auditing matters.

With our history lessons behind us, let's concentrate on what works.

Hotlines are Still Hot

Responsible employees will use hotlines to report irregularities anonymously without fear of retaliation. The ACFE's 2002 Report to the Nation on Occupational Fraud reported that hotlines can cut an organization's fraud losses by approximately 50 percent. A third-party vendor can set up whistle-blower hotlines, receive and screen confidential calls, and provide information to entities for action.

Communicate the existence and benefits of the hotline to all employees and others who might have knowledge of improper business practices.

CASE IN POINT: I was involved in one case in which an employee said if she hadn't known the company had a hotline, she wouldn't have reported the allegations. It's a good thing she did use the hotline; her call uncovered an employee-vendor fraud of several thousands of dollars.

Management Antifraud Programs and Controls

In 2002, the Fraud Task Force of the American Institute of Certified Public Accountants (AICPA) commissioned a study to provide guidance to help prevent and detect fraud. The study was sponsored by the ACFE, the AICPA, the Institute of Internal Auditors , and other organizations. The resulting Management Antifraud Programs and Controls report released in November of 2002, is a road map for fraud mitigation. The document encourages entities to take proactive steps to prevent and deter fraud to preserve their financial integrity, reputations, and futures.

The study found that entities can take three actions to mitigate fraud: create a culture of honesty and high ethics, evaluate anti-fraud processes and controls, and develop an appropriate oversight process. The following fraud prevention principles are taken from the report found on the ACFE Web site at: www.CFEnet.com/services/FrdPrevCheckUp.asp. (Also check out the Fraud Prevention Check Up and the Small Business Fraud Prevention Manual on the same Web page. The check up is a simple but powerful test of your company's fraud health. The manual is designed to address small business' specific fraud-fighting needs.)

Setting Tone at the Top

An entity's senior management team sets the moral and ethical compass for all others to follow. How often have we seen CEOs or CFOs of companies display less than ethical conduct and ultimately they and a number of lower-level employees are indicted for corporate crimes? Employees want to believe and emulate their leaders. Management must clearly communicate a zero tolerance for fraud and reinforce the message daily. CEOs can simply pledge at company meetings that what happened at Enron will never happen at their companies and then describe the fraud mitigation program. The CEOs then need to follow the pronouncement with education and awareness campaigns to reinforce polices and procedures.

CASE IN POINT: The tone at the top was discordant at HealthSouth, the largest U.S. provider of diagnostic imaging, outpatient surgery, and rehabilitation services. Last year, 16 corporate executives were charged with corporate crimes. Fifteen pleaded guilty including all five of the CFOs who ever worked for the company. The CEO was indicted in November of 2003. He was the first CEO to be charged under the Sarbanes-Oxley Act's fraudulent financial certification violations. Others charged included senior vice presidents, vice presidents, and assistant vice presidents. The bar was so low for the employees it almost touched the ground.

Develop Code of Conduct

As stated in the Management Antifraud Programs and Controls report, the cornerstone of an effective fraud prevention program is a culture with a strong value system founded on integrity. This value system often is reflected in a code of conduct. The code of conduct should reflect the core values of the entity and guide employees in making appropriate decisions during their workday.

A code of conduct must include written standards that are reasonably designed to deter wrongdoing. It must promote honest and ethical conduct by all employees no matter their positions within the company. It should advise employees what they can and cannot do and reinforce compliance with government laws, rules and regulations. The code of conduct should be provided in both a soft and hard copy to all employees and translated in appropriate languages. Consider writing specific codes for finance procurement employees, and vendors.

Confirmation Process

People with low integrity may not commit a fraud if they know the entity has an oversight and confirmation process. After giving the code of conduct to all employees, require that they sign a statement that says they have read and understood the code's requirements and will comply with them. Those who have signed the statement can't hide behind the claim of ignorance.

Creating Positive Environment

Obviously, a poor working environment provides a motive and rationalization to commit fraud. Here's a quick health check: does management appear not to care about their employees? Does it have unreasonable expectations or financial targets? Is the organization autocratic or participative? Is there a lack of training or promotion opportunities? Does management say one thing but do another? Are senior executives treated differently than rank and file employees when it comes to discipline?

Hiring and Promoting Appropriate Employees

Of course, it's important to minimize the possibility of hiring employees who lack appropriate values. The best indicator of future performance is past performance. Conduct background checks on new hires or promotions to positions of trust. Professional checks can uncover criminal convictions, credit history problems, questions about education and degrees received prior employment issues and integrity concerns.

Periodic employee training should include scenarios and discussion on ethical challenges relating to fraud, abuse, kickbacks, and other relevant issues. Regular performance reviews should measure each employee's demonstration of entity values and ethics. A review should include feedback on performance against objectives and detailed performance objectives for future review. If necessary, prepare plans to improve an employee's commitment to company values.

CASE IN POINT: I once investigated a senior executive at a private investment firm who was in charge of construction projects. I found that he had set up his own vendors and diverted money to them to build his multi-million dollar mansion. I also discovered that he had a history of bad credit and owed money to a number of creditors. A simple credit check would have saved the company thousands of dollars.

Nothing Like Training

Employees must understand the ethical behavior expected of them. New employee orientation should detail the organization's mission, values and code of conduct, types of fraud, compliance, their responsibility to report violations of ethical behavior and impropriety, and details of the hotline or other ways to report fraud and other integrity

concerns. Periodic training throughout an employee's career reinforces fraud awareness and the cost of fraud to an entity. (See “Recruiting an Anti-fraud Foot-soldier Army” on page 34.)

Fair and Balanced Discipline

Employees must know there is zero tolerance for improper business conduct or fraudulent behavior and that it will yield a professional examination, with any discovered evidence delivered to the legal and human resources departments to determine disciplinary action. Discipline must be fair, appropriate, and consistent for all employees. As a preventive measure, communicate the inappropriate behavior and resulting discipline without naming the offender.

CASE IN POINT: An investigation determined that an employee submitted fraudulent expense reports. The employee confessed but was surprised that the company prosecuted him because it had let other previous fraudsters apologize and escape with just a reprimand.

Identifying and Measuring Fraud Risks

Management must assess the vulnerability of the entity to fraudulent activity including financial statement fraud, misappropriation of assets, and corruption. Fraud can occur in any organization but the degree and detail involved in the risk assessment must be commensurate with the size and complexity of the organization.

Fraud risk is different from industry to industry and from country to country. Some nations have a greater vulnerability to corruption and bribery that contributes to fraud. Transparency International (TI) (www.transparency.org) is a leading non-governmental organization fighting world corruption. Each year TI publishes its Corruption Perceptions Index (CPI) reflecting the perception of business leaders, academics, and risk analysts in 133 countries. In its October 2003 study, corruption was found to be most pervasive in Bangladesh, Nigeria, Haiti, Paraguay, and Myanmar while least pervasive in Finland, Iceland, Denmark, New Zealand, and Singapore.

Implementing and Monitoring Internal Controls

A common denominator of the recent U.S. corporate frauds is that strong internal control systems weren't in place. Controls need to detect not only errors but also theft, misappropriation of company assets, or intentional manipulation of financial reporting.

Proper internal controls – a mandatory system for any entity – require that transactions are properly authorized, recorded, and reported, and that all assets are safeguarded. I'm familiar with a fraud and kickback scheme that was uncovered because finance personnel instituted a rotation of vendor account managers and separation of duties. As a result, red flags started flying that resulted in an investigation and the discovery of an employee's involvement in the scheme.

The Securities and Exchange Commission has its own definition of internal controls and how they should be used in the design of a robust fraud prevention program:

A process designed by, or under the supervision of, the registrant's principal executives and principal financial officers, or persons performing similar functions, and affected by the registrant's board of directors, management and other personnel, to provide reasonable assurance regarding the reliability of financial reporting and the preparation of financial statements for external purposes in accordance with generally accepted accounting principles and includes those policies and procedures that:

(1) Pertain to the maintenance of records that in reasonable detail accurately and fairly reflect the transactions and dispositions of the assets of the registrant;

(2) Provide reasonable assurance that transactions are recorded as necessary to permit preparation of financial statements in accordance with generally accepted accounting principles, and that receipts and expenditures of the registrant are being made only in accordance with authorizations of management and directors of the registrant; and

(3) Provide reasonable assurance regarding prevention or timely detection of unauthorized acquisition, use or disposition of the registrant's assets that could have a material effect on the financial statements.

Independent Audit Committee

An audit committee of the board of directors should be the independent eyes and ears of the investors, employees, and other stakeholders. Their role is to evaluate management's identification of fraud risks, the implementation of antifraud measures and (again) provide the tone at the top that fraud won't be accepted in any form. The audit committee should hire independent auditors to assess the internal controls and report on the financial health of the company. The outside auditors should only report to the audit committee and not to management. The audit committee is also responsible for ensuring that management doesn't engage in fraudulent conduct. In its policeman role, the audit committee is responsible for senior management's compliance with appropriate financial reporting and the potential for management override of controls or other inappropriate influence over the reporting process.

CASE IN POINT: The Securities and Exchange Commission is going after board members who ignore corporate wrongdoing. In April 2003, the SEC charged a company of fraudulently overstating revenue in 1998 by 177 percent. A member of the audit committee knew of the financial transgressions but still approved the company's financial statements. The SEC said that the board member “completely neglected his duties as a director and an audit committee member.”

Internal Auditors

As stated in the Standards for the Professional Practice of Internal Auditing issued by the Institute of Internal Auditors, “The internal auditor should have sufficient knowledge to identify the indicators of fraud but is not expected to have the expertise of a person whose primary responsibility is detecting and investigating fraud.” Internal auditors evaluate fraud risk and internal controls and report on their findings. They should work in conjunction with an entity's fraud examiners for follow-up to fraud risks that are identified. As stated in the Management Antifraud Programs and Controls report, internal auditors should determine whether:

• the organizational environment fosters control consciousness;
• realistic organizational goals and objectives are set;
• written policies (such as a code of conduct) exist that describe prohibited activities and the action required whenever violations are discovered;
• appropriate authorization policies for transactions are established and maintained;
• policies, practices, procedures, reports, and other mechanisms are developed to monitor activities and safeguard assets, particularly in high-risk areas;
• communication channels provide management with adequate and reliable information; and
• recommendations need to be made for the establishment or enhancement of cost-effective controls to deter fraud.

Independent External Auditors

Independent outside auditors can provide management and the audit committee an assessment of the organization's internal controls environment and compliance, and checks and balances to protect the company from fraud. The key word is independence. The process only will work if the outside auditors are truly objective and have no ties to the entity that would impair their judgment. The corporate scandals in the United States caused many people to ask, “Where were the accountants?” As a result, there is now greater government oversight of auditors to ensure true independence and truthful reporting of fraud and fraud risks.

Certified Fraud Examiners

The Certified Fraud Examiner certification has become the gold standard in fraud detection and prevention. CFEs are known the world over as fraud-fighting experts. The ACFE has built a respected organization that is at the forefront of fraud research and education. Robust fraud prevention programs must use CFEs as staff members or consultants. CFEs can also assist the audit committee, internal auditors, and independent auditors in their oversight capacities. CFEs in fraud prevention programs can be deterrents to potential fraud perpetrators.

Fraud Investigation/Financial Integrity Unit

The mandatory investigative response component is responsible for the detection, investigation and prevention of fraud and the recovery of assets. Senior management and the audit committee must strongly support the unit so that all know the entity is ready to respond quickly and appropriately respond to any fraud allegations.

Though most fraud investigation units (FIUs) are based within corporate security departments, it's more beneficial for them to be in internal audit departments because the unit employees will have access to internal and independent auditor findings. Proactive FIUs need audit findings to find red flags.

The FIU must communicate its entity-wide fraud prevention program mission and written objectives to its stakeholders. The unit also should work closely with other entity departments such as legal, human resources, and the office of compliance.

Case Management and Technology Tools

What good is a fraud prevention program if it doesn't track cases, weaknesses in controls and lessons learned? Fraud examiners must review statistical information to capture trends and metrics and share information with stakeholders. Also, they must identify key performance indicators to improve investigative performance. Automate the case management system to include all information from initiation through resolution.

Whether it's Benford's Law, Microsoft's Excel and Access or fraud detection software from ACL and I2 – today's forensic sleuths are embracing computers and technology to mitigate fraud. “Classic signs of impropriety can be identified faster and more regularly with the help of technology,” says Toby J. F. Bishop, CFE, CPA, FCA, President and CEO of the ACFE. “Identifying patterns is a key strength of a computer,” he says.[1]

Today's modern fraud investigation unit must have digital evidence recovery capabilities for identifying, preserving, recovering, and examining electronic evidence and forensic data analysis tools to identify anomalies or irregularities in electronic data that are indicative of fraud or abuse. The investigative staff must be trained in the use of these technology tools but a fraud investigation unit also should have a dedicated forensic data analyst to support complex investigations.

Importance of Cross-group Collaboration

The members of the fraud investigation unit cannot work in a vacuum; they need to collaborate with senior management, the legal department, human resources, the compliance officer, internal audit, corporate security, and public relations. Employees from these groups may need to resolve employment, legal and public relations concerns.

Watchword is Always Prevention

As detailed in the ACFE's 2002 Report to the Nation, occupational fraud and abuse are on the rise. Of course, that's not news to any fraud examiner. Fraud has always been a growth industry. Yet, the explosion of fraud worldwide has changed the way we not only look at fraud but how we prevent it. Fraud prevention and reduction programs are a necessity in today's business environment. Incorporating the elements described in this article will do much to establish a culture that puts fraud prevention at the forefront of a successful business strategy. An ounce of prevention does equal a pound of cure. That must be the rallying cry for global entities as they design robust fraud prevention programs.

Martin T. Biegelman, CFE, ACFE Fellow, is the director of the financial integrity unit at Microsoft Corporation in Redmond , Wash. A former U.S. postal inspector, he is a Regent Emeritus and an ACFE faculty member. His email address is martinbi@microsoft.com.

[1] “IT Matters,” Dec. 17, 2002, http://itmatters.com.ph/news/news_12172002h.html

SIDE BAR

Fraud Speaks Thousands of Languages

Regardless of the constant media reporting of high-profile U.S. corporate fraud cases, that nation has no monopoly on these crimes. For example, the Korea Herald reported that Korean prosecutors in October of last year indicted 34 business leaders from six major companies for cooking their books to obtain huge loans from the government. These executives allegedly masterminded this financial fraud to obtain public funds to bail out their supposedly cash-strapped corporations and then illegally funneled the money to other companies, which they controlled. The companies' losses were estimated to be as large as $345 million.

Time after time, global surveys tell us the same thing: Fraud is everywhere, and it's growing because of little emphasis on deterrence. PricewaterhouseCoopers' 2003 Global Economic Crime Survey, which polled 3,600 corporate executives in 50 countries, found that economic crime is a significant problem with no industry immune from its effects. (No surprise there.) The respondents' major concerns were financial loss, damage to reputation and brand, and the effect on employee morale. African entities reported the most fraud with 51 percent reporting significant economic crime. North America was second with 41 percent and the Asia Pacific Region was third with 39 percent. A third of the companies that suffered fraud weren't even able to guess how much they had lost. Fraud throughout Europe grew significantly from the last PWC survey conducted in 2001. The number of survey respondents reporting fraud in Western Europe grew from 29 percent in 2001 to 34 percent in 2003. In Central and Eastern Europe, fraud grew from 26 percent to 37 percent. (Weak internal controls were a major factor in the success of the schemes.)

In a 2002 KPMG survey of the major public and private companies in Malaysia, half of the companies surveyed reported that they had been the victims of fraud and occupational fraud was the most common. The survey found that 68 percent of respondents felt a lack of emphasis on fraud detection and prevention. (How many times have we heard this before?) A September 2003 study by CPA Australia, the largest accounting organization in Australia, found that one in four small businesses in Australia had been fraud victims. Again, employee fraud was the most common type of reported fraud and attributed it to a lack of internal controls and financial management processes. Judy Hartcher, business policy advisor for CPA Australia said, “small business owners can overcome fraud and customer collapse. Putting simple processes in place will help them improve their business potential and minimize incidents of scams, errors and loss.”