Internal Control Fundamentals and Introduction to Fraud
- Spring 2010 -

Brenda M. Shannon, CPA, CIA
Chief Audit Executive
New Mexico State University
Objectives

• To give participants a high-level overview of internal control fundamentals and to raise awareness levels with regard to fraud in the workplace.
Outline

- Video on Internal Controls
- Internal Control Fundamentals
- Introduction to Fraud
VIDEO - Internal Controls for Colleges & Universities
(20 minutes)

Association of College & University Auditors
Internal Control Fundamentals under the COSO Model

(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
(Committee of Sponsoring Organizations)

• Sponsoring organizations – AICPA, AAA, FEI, IIA, IMA
• History – several business failures in the 1980’s prompted creation of a committee in 1985 to examine causes of fraudulent financial reporting.
  – Committee charged with creating a control model.
COSO
(Committee of Sponsoring Organizations)

• COSO model was considered to be best practices, but had no “teeth”.
• Renewed interest more recently because of accounting scandals and Sarbanes-Oxley Act of 2002 (SOX). The COSO model is still considered by many to be the best internal control guidance available.
Sarbanes-Oxley Act of 2002
(Corporate Governance & Accounting Reform Legislation)

• Applies to SEC companies (but relevant to us)
• Reforms aimed at companies, auditors, board members and lawyers
• Section 404 provision – requires companies to adopt and evaluate internal controls.
COSO Definition of Internal Control

Internal control is a process…designed to provide *reasonable* assurance regarding the achievement of objectives in the following categories:

- Effectiveness and efficiency of operations (including protection of assets)
- Reliability of financial reporting
- Compliance with applicable laws and regulations
Types of Controls

Internal controls may be:

• **Preventive** - designed to keep errors or irregularities from occurring.

• **Detective** - designed to detect errors or irregularities that have already occurred.

• **Corrective** - designed to correct errors or irregularities that have been detected.
Examples of Controls

Personal –

• Installing locks/alarm systems on homes and vehicles.
• Reviewing bills and credit card statements before payment.
• Reconciling bank statements.
• Securing valuables such as jewelry, blank checks, credit cards and cash.
• Establishing rules and curfews for our children.
• Purchasing insurance.
Examples of Controls

Society –

• Laws and Regulations
  – Minimum age limits for legally driving a car or drinking alcohol
  – Traffic regulations
  – Court hearings and trials
  – Zoning ordinances

• Religious doctrine
Examples of Controls

University –

• NMSU Policy Manual; Business Procedures Manual; Student Code of Conduct
• Required use of computer passwords, anti-virus software
• Locking offices, buildings, state vehicles
• Securing laptops, procurement cards and petty cash funds
• Reconciling financial and P-card reports against receipts
• Requiring authorization from Purchasing for large purchases
• Requiring approvals for travel, timesheets and leave reports
• Running background checks, credit checks, motor vehicle checks
• I.D. cards
• Degree requirement audits
Who is Responsible for Internal Control?

- The organization’s leadership is responsible for establishing the control environment.
- **Everyone** in an organization plays some role in effecting control. All personnel are responsible for communicating problems in operations, deviations from established standards, and violations of policy or law.
- Auditors evaluate whether appropriate controls have been implemented and are functioning as intended, but they are not responsible to establish or maintain them.
Five Components of an Integrated System of Internal Controls

• Control Environment
• Risk Assessment
• Control Activities
• Information & Communication
• Monitoring
Control Environment (1) — ethical tone established by management; “tone at the top”, control consciousness (soft controls)

Factors include:

- Integrity & Ethical Values – must be clearly communicated, in writing and by example.
- Commitment to Competence
- Management Philosophy & Operating Style
- Organizational Structure
- Human Resource Policies & Procedures – practices related to hiring, training, evaluation, promoting, compensating, etc.
How do you Evaluate Soft Controls?

• Subjective - the only valid measure of their effectiveness may be employees’ perceptions.
• Most internal control evaluation practices have a strong element of self-assessment
  – Control Self-Assessment (CSA)
Risk Assessment (2) – mechanism to identify, analyze and manage risks relevant to meeting our objectives.

Factors:

- **External Factors** - economic changes, changing needs & expectations of clients, legislation & regulations, technological developments, natural disasters.

- **Internal Factors** - new personnel, new computer systems/processes, low morale.
Risk Assessment continued…

• After risks have been identified, they must be analyzed as to likelihood of occurrence and impact, and then we must consider how to manage the risk.

• We cannot anticipate every potential risk

• Risk assessment should be an integral part of the strategic planning and budgeting process.
Control Activities (3) - policies (what should be done) and procedures (how it should be done) designed to help ensure that objectives are achieved. (Hard controls)

Types of control activities:
• Transaction Approvals, Authorizations, Verifications (limits to authority)
• Reconciliations (explain differences between two sets of data), Verifications
• Performance reviews (programs, people, departments), benchmarking, trend analysis
Control Activities continued...

- Physical controls - restrict access to equipment, conduct inventories, secure/count cash, etc.
- Segregation of Duties - different people should ideally be responsible for:
  - authorizing transactions
  - recording transactions (accounting)
  - handling the related assets (custody)
  - monitoring transactions (reconciling, verifying).
Information System Control Activities

General controls:

- Segregation of duties within IT environment
- Backup and recovery policies & procedures
- Program development & documentation controls
- Hardware / access controls (i.e. passwords)
- Virus detection software
- Firewalls
Information System Control Activities

Application controls:
- Input controls (authorization, validation, error notification – i.e. field checks, limit checks, sequence checks)
- Processing controls – batch totals, audit trails
- Output controls – listing of master file changes, error listings
Controls – What Kind and How Many do you Need?

• Enough to ensure that you are managing your significant risks, as determined by the risk assessment process.
Information & Communication (4)- how we identify/capture/communicate information in a way that allows employees to carry out their responsibilities.

To be effective, the information system must have adequate resources and be able to provide data that is:

• Relevant to established objectives (operational, financial, compliance-related)
• Accurate and in sufficient detail
• Understandable and in usable form
• Provided to the appropriate people in a timely manner
Monitoring (5) – assessing the quality of the system of internal controls over time.

Activities include:
- Management review of financial reports for propriety and trends.
- Review and analysis of tips and complaints from external sources.
- Comparison of recorded data with physical assets.
- Self assessments, internal audits, external reviews
- Established means to report and correct deficiencies
Internal Control Components

Establish Control Environment

- Information
- Goals & Objectives
- Perform Risk Assessment
- Implement Control Activities
- Monitor Performance
- Communication
Limitations of Internal Controls

- **Judgment** - decisions are made by people, often under pressure and time constraints, based on information at hand.

- **Breakdowns** - Employees may not understand instructions or may simply make mistakes. Errors may result from new systems and processes.

- **Controls may be Outdated** — Waste of time and money.
Limitations of Internal Controls continued...

• **Management Override** - high level personnel may be able to override prescribed policies and procedures.

• **Collusion** - two or more individuals, working together, may be able to circumvent controls.

It is one thing to establish controls and quite another to ensure that they are operating as intended.
Perhaps the lesson to be learned from the 1980’s Savings & Loan scandals; the 1990’s corporate governance failures of Enron, WorldCom, Tyco and the like; and the more recent subprime mortgage debacle, is that you cannot legislate ethics or morality, and an Internal Control System is only as good as the people who administer it.
Balancing Risks and Controls

Cost vs. Benefit - The risk of failure and the potential effects must be weighed against the cost of establishing controls.
Balancing Risk and Controls – not having an effective balance may cause:

• **Excessive Risks** –
  - Loss of Assets, Donors, Grants & Contracts, State funding
  - Poor Business Decisions
  - Noncompliance with laws & regulations
  - Increased Regulations
  - Public Scandals
Balancing Risk and Controls — not having an effective balance may cause:

- **Excessive Controls** —
  - Increased Bureaucracy
  - Increased Complexity
  - Increased Cycle Time
  - Increase in Non-Value Added Activities
  - Reduced Productivity
Integrated System of Internal Controls

An effective system of internal controls requires:

• All 5 components working together
  – Control Environment
  – Risk Assessment
  – Control Activities
  – Information & Communication
  – Monitoring

• Everyone in the organization playing an active role

*Internal Controls are Everyone’s Business!*
QUESTIONS?

(Internal Control Training Supplement on Segregation of Duties)
Introduction to Fraud
What is Fraud?

- **Occupational Fraud** – The use of one’s occupation for personal enrichment through the deliberate misuse or misapplication of the employing organization’s resources or assets. (Generally referred to as white-collar crime.)

(Source: Association of Certified Fraud Examiners 2008 Report to the Nation on Occupational Fraud and Abuse)
The study was based on data compiled from 959 cases of occupational fraud that were investigated between January 2006 and February 2008. All information was provided by the Certified Fraud Examiners (CFEs) who investigated those cases. The 2008 report is the fourth of its kind, with other reports produced in 2002, 2004 and 2006.
Measuring the Cost of Fraud
(Source: Association of Certified Fraud Examiners 2008 Report to the Nation on Occupational Fraud and Abuse)

Fraud, by its very nature, does not lend itself to being scientifically observed or measured in an accurate manner. One of the primary characteristics of fraud is that it is clandestine, or hidden, and almost all fraud involves the attempted concealment of the crime.
Types of Occupational Fraud and Abuse
(Source: Association of Certified Fraud Examiners 2008 Report to the Nation on Occupational Fraud and Abuse)

- **Asset Misappropriation** – theft or misuse of an organization’s resources. (i.e., theft of cash, equipment or supply inventory; submitting false invoices, timesheets, or expense reports; abuse of leave)

- **Corruption** – an employee wrongfully uses his/her influence in business transactions in a way that violates their duty to their employers in order to obtain a benefit for themselves or someone else. (i.e., engaging in conflicts of interest; receiving or offering bribes; extorting funds from third parties)

- **Financial Statement Fraud** – making a company appear more/less profitable (i.e., booking fictitious sales or inventories, recording income/expense in wrong period)
Occupational Fraud by Category
(Source: Association of Certified Fraud Examiners 2008 Report to the Nation on Occupational Fraud and Abuse)
Occupational Fraud by Category – Median Losses
(Source: Association of Certified Fraud Examiners 2008 Report to the Nation on Occupational Fraud and Abuse)
Occupational Fraud Schemes in Government and Public Administration
(Source: Association of Certified Fraud Examiners 2008 Report to the Nation on Occupational Fraud & Abuse)
Occupational Fraud Schemes in the Education Industry
(Source: Association of Certified Fraud Examiners 2008 Report to the Nation on Occupational Fraud & Abuse)
Fraud Statistics
(Source: Association of Certified Fraud Examiners 2008 Report to the Nation on Occupational Fraud and Abuse)

It is estimated that the average organization loses:

- about 7% of annual revenues to fraudulent activity
- This translates into ~$994 billion in annual fraud losses applied to the estimated 2008 U.S. Gross Domestic Product
- NMSU had operating revenues of over $500 million in FY08. 7% of that would be over $35 million.
Fraud Statistics continued…

Who commits more fraud – men or women?

- Men are the perpetrators in 60% of all fraud cases
- Median $ losses caused by men are twice those caused by women.
Gender of Perpetrator — Frequency

Source: Association of Certified Fraud Examiners 2008 Report to the Nation on Occupational Fraud and Abuse
Who commits more fraud – employees, managers or owner/executives?

- While employees (40%) and managers (37%) account for the majority of offenses, median losses caused by owners/executives were 5 times more than those caused by managers, and 11 times more than those caused by rank and file employees.
Fraud Statistics continued…

Who commits more fraud – younger people (<40) or older people?

• More than half of cases studied involved a fraudster over the age of 40, and over one-third were individuals between 41 and 50
• The older they were, the greater the median losses incurred
Age of Perpetrator — Frequency

Age of Perpetrator — Median Loss

Source: Association of Certified Fraud Examiners 2008 Report to the Nation on Occupational Fraud and Abuse
Fraud Statistics continued…

Who commits more fraud – those with more education or less education?

• While slightly more than half of all frauds were committed by people with no college degree, median $ losses caused by perpetrators with college degrees were up to 5 times greater than losses caused by those without college degrees.
**Education of Perpetrator — Frequency**

- **Postgraduate Degree**:
  - 2008: 10.9%
  - 2006: 12.2%
- **Bachelor's Degree**:
  - 2008: 34.4%
  - 2006: 33.4%
- **Some College**:
  - 2008: 20.8%
  - 2006: 21.6%
- **High School Graduate**:
  - 2008: 33.9%
  - 2006: 32.8%

**Education of Perpetrator — Median Loss**

- **Postgraduate Degree**:
  - 2008: $550,000
  - 2006: $425,000
- **Bachelor's Degree**:
  - 2008: $210,000
  - 2006: $200,000
- **Some College**:
  - 2008: $196,000
  - 2006: $200,000
- **High School Graduate**:
  - 2008: $100,000
  - 2006: $100,000
Who commits more fraud – those with more money or those with less money?

- While the number of frauds decreased as income brackets rose, the median loss increased directly with the annual income of the perpetrator.
- The schemes perpetrated by individuals who earned over $500,000 were associated with a median loss of $50 million dollars — 50 times that of any other income bracket.
Median Loss Based on Perpetrator’s Annual Income

Source: Association of Certified Fraud Examiners 2008 Report to the Nation on Occupational Fraud and Abuse
Why?

Older, more educated males tend to occupy more positions of authority and trust, and have a greater degree of control over company assets.
Profile of a Typical Fraudster

- White Male
- College educated
- Over the age of 40
- Occupies position of authority and trust
- Often married, well respected in the community, etc.
- Under stress

As women and minorities move into more positions of authority, this profile is changing.

In our industry, the typical fraudster does not necessarily fit this profile – it could be anybody, and it is often the person you would least expect.
Fraud Statistics continued…

• The typical perpetrator is a first-time offender.
• The average fraud scheme lasts approximately 24 months before detection.
• Small businesses (and small departments) are the most vulnerable to fraud and abuse.
• Cash is the asset most frequently targeted by dishonest employees.
Fraud Statistics continued…

What is the most common method for detecting fraud?

- Internal controls?
- Internal audit?
- By accident?
- Tip from employee, vendor, customer, other?
- External audit?

- The most common method for detecting fraud is a tip from an employee, customer, vendor or anonymous source.

- The next most common method is by internal controls, followed by accident or from an internal audit.
Fraud Detection

(Source: Association of Certified Fraud Examiners 2008 Report to the Nation on Occupational Fraud & Abuse)

Initial Detection of Occupational Fraud

<table>
<thead>
<tr>
<th>Type of Detection</th>
<th>2008</th>
</tr>
</thead>
<tbody>
<tr>
<td>Tip</td>
<td>34.2%</td>
</tr>
<tr>
<td>By Accident</td>
<td>20.0%</td>
</tr>
<tr>
<td>Internal Audit</td>
<td>19.4%</td>
</tr>
<tr>
<td>Internal Controls</td>
<td>23.3%</td>
</tr>
<tr>
<td>External Audit</td>
<td>9.1%</td>
</tr>
<tr>
<td>Notified by Police</td>
<td>3.2%</td>
</tr>
</tbody>
</table>

Percent of Cases

NM State University
Percent of Tips by Source
(Source: Association of Certified Fraud Examiners 2008 Report to the Nation on Occupational Fraud & Abuse)
Fraud Statistics continued…

Which measures are most helpful in preventing fraud?

- Audits – internal or external?
- Background checks?
- Internal Controls?
- Hotlines?
- Fraud Awareness/Ethics training?

- Strong internal controls are the best deterrent to fraud; however, organizations without fraud hotlines suffered fraud losses that were 2.5 times greater than those with hotlines.
- Organizations without internal audit functions suffered median losses more than twice those with an internal audit function.
- Organizations without fraud training had twice the median losses of those that did not have such training.
- Background checks are valuable, but almost 90% of fraudsters have no previous charges or convictions.
## Median Loss Based on Presence of Anti-fraud Controls

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

- Financial pressures are one of the key motivating factors of occupational fraud, and the two most commonly cited behavioral red flags among fraudsters were “financial difficulties” and “living beyond one’s means.”

- Given that financial difficulties are often associated with fraudulent behavior, it would seem advisable for organizations to devote more efforts to conducting credit background checks on new applicants.
Control Weaknesses that Contributed to Fraud
(Source: Association of Certified Fraud Examiners 2008 Report to the Nation on Occupational Fraud & Abuse)

Lack of controls, absence of management review, and override of existing controls were the three most commonly cited factors by survey participants, that allowed fraud schemes to succeed.
Necessary Components of Fraud

• Motive

• Opportunity

• Rationalization
Components of Fraud

**Motive** - some kind of pressure or perceived pressure, typically financial, such as the need to pay for:

- Hospital bills
- Child support or alimony
- Gambling debts or other addictions
- Extramarital affairs
- An expensive lifestyle
- Motive could also be greed, revenge, thrill seeking, etc.
Components of Fraud

**Opportunity** or perceived opportunity – typically caused by circumventing internal controls or by internal controls weaknesses.

Examples:
- Nobody counts supply inventory or checks deviations from specifications, so losses are not known.
- Equipment is checked on the inventory list without being physically located.
- The petty cash box is left unattended. Laptops and digital cameras are left out in the open in unlocked offices.
- People are given authority, but their work is not reviewed.
- Too much trust and responsibility placed in one employee - improper separation of duties.
- Employees that are caught stealing get fired, but aren’t prosecuted.
Opportunity continued…

More Examples:

• Supervisors set a bad example by using university equipment for personal use, padding travel expense reimbursements, not paying for personal long distance calls or copies, not reporting leave, etc.

• Supervisors set a bad example by not dealing with problem employees, showing favoritism, allowing employees to abuse privileges, etc.

• Monthly financial reports are not reviewed by managers.

• There are not expectations with regard to ethical behavior, no hotline, no internal audit function, no training on internal controls and fraud.

The perception of detection is the biggest deterrent to fraud.
Components of Fraud

**Rationalization** – some excuse or validation for actions, such as:

- I’m just borrowing the money and will pay it back; it’s only temporary until I get over this financial difficulty.
- I need it more than they do, and they will never miss it.
- Everybody else is doing it.
- No one will get hurt.
- It’s for a good purpose.
- I deserve it because I’ve been treated unfairly – the organization owes me.
Fraud Detection

Symptoms or indications that fraud may exist in an organization (Organizational “Red Flags”):

- **Internal Control Weaknesses** – lack of: segregation of duties, physical safeguards, independent checks, proper authorizations, proper documents and records, overriding of existing controls.

- **Analytical Anomalies** – unexplained inventory shortages, deviations from specifications, increased scrap, purchases in excess of needs, too many voided transactions and returns, unusual cash shortages.
Fraud Detection continued…

More *possible* indications (Employee “Red Flags”):

• Lifestyle changes/Extravagant lifestyles
• Significant personal debt and credit problems
• Unusual behavior – most perpetrators are under stress caused by feelings of guilt and the fear of being caught. Stress causes behavioral changes such as insomnia, addictions, irritability.
• Missing or altered documents, denial of access to records, refusal to take vacations or sick leave.
Fraud Prevention

Create a culture of honesty -

• Set a good example and do not tolerate dishonest or unethical behavior in others
• Have a written code of ethics and make sure everyone is aware of it (NMSU Policy Manual Section 3.19)
• Check employee references, conduct background checks (NMSU Policy Manual Section 4.30.35)
• Train employees in fraud awareness
• Create a positive work environment
• Provide employee assistance programs (http://www.nmsu.edu/~eap/EAP.html)
Fraud Prevention continued…

Limit Opportunities for Fraud –

• Implement a strong system of internal controls and monitoring
• Make sure all employees are aware of and have access to policies and procedures
• Alert vendors and contractors to company policies
• Establish a hotline
  – [http://www.nmsu.edu/audit/reporting-line.html](http://www.nmsu.edu/audit/reporting-line.html)
• Create an expectation of punishment
• Proactively audit for fraud
How to Encourage Fraud
(Source: Fraud Examination for Managers & Auditors by Jack C. Robertson, PhD, CPA, CFE)

- Practice autocratic management
- Manage by power with little trust in people
- Manage by crisis
- Centralize authority in top management
- Measure performance on a short-term basis
- Make rewards punitive, stingy and political
- Give feedback that is always critical and negative
- Create a highly hostile, competitive workplace
More Ways to Encourage Fraud

• Let your secretary, accounting tech, audit/budget tech, records tech, administrative assistant do everything.

• While you’re at it, give them your passwords and approval access codes.

• Never look at or verify your monthly financial reports.

• Openly criticize and disregard institutional policies and procedures.
What to Do if You Suspect Fraud

• Contact Audit Services – by phone, fax, email or in person

• File a report through the NMSU Confidential Reporting Line at:
  www.ethicspoint.com
  or by calling: 1-866-ETHICSP
  (384-4277)

• For additional information, refer to Section 7.15 of the Business Procedures Manual
Office of Audit Services

Phone: 575/646-4912
Fax: 575/646-5846

MSC 3AU (Hadley Hall, Rm. 134)
New Mexico State University
P.O. Box 30001
Las Cruces, NM 88003-8001

E-mail: audit@nmsu.edu
Website: http://www.nmsu.edu/~audit
Sources of Additional Information

COSO - Internal Control Integrated Framework

AICPA Summary of Sarbanes-Oxley
  – http://www.aicpa.org (Type Sarbanes-Oxley into Search box & scroll down to item 5)

Association of Certified Fraud Examiners, 2008 Report to the Nation:
QUESTIONS OR COMMENTS?

THANK YOU FOR COMING!
Training Addendum

• COSO issued a new framework in September 2004 titled:

*Enterprise Risk Management – Integrated Framework*

This is a more ‘robust’ framework for an organization’s management to identify, assess and manage risk. Commonly referred to as ERM.

• Does not replace the Internal Control Framework issued in 1992, but does incorporate it into a broader risk management process.
Enterprise Risk Management Defined

• Enterprise risk management is a process, effected by an entity’s board of directors, management and other personnel, applied in strategy setting and across the enterprise, designed to identify potential events that may affect the entity, and manage risk to be within its risk appetite, to provide reasonable assurance regarding the achievement of entity objectives.
The ERM Framework

Entity objectives can be viewed in the context of four categories:

- Strategic
- Compliance
- Operations
- Reporting
Objectives

• Strategic – high-level goals, aligned with and supporting the mission
• Operations – effective and efficient use of resources
• Reporting – reliability of reporting
• Compliance – compliance with applicable laws and regulations
For more information:

http://www.coso.org/-ERM.htm