Compliance Risk Management

Seventh Annual
University Compliance Conference Society for Corporate Compliance and Ethics
May 30, 2009

Robert F. Roach, NYU University Ethics and Compliance Officer
Robert.Roach@nyu.edu

NEW YORK UNIVERSITY

Risk Management - Overview

Risk Management Involves Several Steps:

1. **Organization**: What are your organization's objectives, structure and operations?
2. **Identification:** What are the possible risk events your organization faces?
3. **Assessment:**
   - What is the likelihood of the risk event happening?
   - What is the potential impact of the risk event?
   - What is your organizations "appetite" for risk?
4. **Priority Setting:** Having assessed the risks, what are the most important risks to address?
5. **Mitigation:** What steps must be taken to mitigate the risks Identified?
6. **Monitoring and Corrective Action:**
   - Are internal controls working effectively to mitigate risk?
   - Is there any corrective action needed?

ERM vs. Compliance Risk Management

Risk Management issues we will address:

Compliance Risk Management: Will we be audit by NSF and is our "time and effort" reporting system functioning effectively?

Enterprise Risk Management issues we will not address:

- **Strategic Risks: Should we open a marine biology program in Somalia now?**
- **Investment Risks: Is now the time to invest our endowment in Madoff's hedge fund?**
- **Non-compliance Operational Risks: Will the Mississippi flood our campus for the 10th time this year?**
- **Financial Statement Risk: Do our financial statements accurately reflect the financial condition of the organization?**

NEW YORK UNIVERSITY

I. Risk Management in Context

Elements of an Effective Compliance Program

II. Risk Management Theory

A. COSO: Internal Control - Integrated Framework

With Simple Application

B. COSO: Enterprise Risk Management – Integrated Framework

III. Application of Risk Management Theory

Advanced Tools and Techniques

Risk Assessment and Management

Elements of an Effective Compliance Program

NEW YORK UNIVERSITY

History of Compliance

1. Federal and State Corporate Criminal Liability

2. **1986** - Defense Industry Initiative on Business Ethics and Conduct
   - Created in response to concerns about corruption
   - Encourage an environment of ethical conduct
   - Develop/train on Code of Ethics; encourage internal reporting with no retaliation
   - ***No provisions for risk assessment***

3. **1991** – U.S. Federal Sentencing Guidelines
   - Gives credit to organizations with "an effective program to prevent and detect violations of law." (Seven basic elements, discussed below).
   - Hallmark = "due diligence in seeking to prevent and detect ***criminal conduct***."
   - ❖ Risk that "certain types of offenses might occur" must be considered, but ***no requirement for comprehensive risk assessment.***

History of Compliance (continued)

4. **1992** - The COSO Report, *Internal Control – Integrated Framework* , provides that an organization's Internal Controls should be designed to achieve:

- Board of Directors has a fiduciary responsibility to assure that the company has an effective compliance program following FSG.
- Effectiveness And Efficiency of Operations
- Reliability of Financial Reporting, and
- ***Compliance With Applicable Laws And Regulations***
- ***Establishes Methodology for Comprehensive Risk Assessment***

5. 1996 - ***In re Caremark International Inc. Derivative Litigation***, 698 A.D. 2d 959 (Del Ch. 1996)

- Board of Directors has a fiduciary responsibility to assure that the company has an effective compliance program following FSG.

History of Compliance (continued)

6. 2002 - Enron and WorldCom Corporate Scandals

- **Federal Sentencing Guidelines**
  - Amended to require corporations to "promote an organizational culture that ***encourages ethical conduct*** and a commitment to compliance with the law."
  - Amended to add "eighth" element of an effective compliance program: "In implementing [an effective compliance program], the organization shall ***periodically assess the risk of criminal conduct*** and shall take appropriate steps to design, implement, or modify each requirement [for an effective compliance program] ***to reduce the risk of criminal conduct identified through this process.*"**

History of Compliance (continued)

7. **2002** - Sarbanes Oxley Act (Requirements for risk assessments)
   - Sarbanes –Oxley Act Of 2002, Section 404
   - Public Company Accounting Oversight Board (Pcaob) Auditing Standard No. 5
   - Institute Of Internal lia *Performance Standard 2130*
   - Auditors (lia), *Audit Committee Effectiveness – What Works Best*, 2nd Edition

History of Compliance (continued)

8. **2004** - COSO: Enterprise Risk Management – Integrated Framework adopted.

9. Up to Present - Other Regulatory Requirements:

- OIG Guidelines
- The American Institute of Certified Public Accounts (AICPA) Auditing Standards (SAS 78 – AU 319) made the COSO Framework applicable to all U.S. research universities. *See also* SAS 112 and OMB Circulars A-110 and A-133.
- FDA, OHRP, ORI (specialized risk assessment requirements)

Elements of an Effective Compliance Program

To have an effective compliance program, an organization must establish and maintain an organizational culture that

"encourages ethical conduct and a commitment to compliance with the law."

U.S. Federal Sentencing Guidelines §8B2.1(a)(2)

Elements of an Effective Compliance Program

There are Seven Elements of an Effective Compliance Program:

1. High level company personnel who exercise effective oversight;
2. Written policies and procedures;
3. Training and education;
4. Lines of communication;
5. Standards enforced through well-publicized disciplinary guidelines;
6. Internal compliance monitoring; and,
7. Response to detected offenses and corrective action plans.

1. High level company personnel who exercise effective oversight

A. The organization's governing body should:

- Be knowledgeable about the program;
- Exercise oversight.

B. Specific "high level" personnel should:

- Have overall responsibility for the compliance program;
- Ensure that the program is effective.

C. Day to day responsibility

- Specific individuals (preferably a compliance officer) shall have overall responsibility for the day to day operations of the compliance program;
- The compliance officer must periodically report status to high level personnel and/or the governing body
- The compliance officer must have adequate resources, appropriate authority and direct access to governing body

2.Written Policies and Procedures

A. Develop policies and programs that:

- Explain legal requirements so that employees understand their obligations and how to conform their behavior to meet them;
- Encourage managers and employees to report suspected fraud and other improprieties without fear of retaliation.

B. The Code of Ethical Conduct:

- Is the centerpiece of an effective ethics and compliance program.

3. Training and Education

A. Reasonable and practical steps must be taken to provide face to face dissemination of information about the organization's compliance program and its policies and processes;

B. Training should be provided to the governing body, high level executives, employees and, where appropriate, the organization's agents.

4. Lines of Communication

Information about the compliance program must be widely communicated at all levels of an organization. To enhance the effectiveness of the compliance program, the program must establish lines of communication whereby:

- **Employees and agents may seek guidance and report concerns, including the opportunity to report *anonymously* (such as a compliance hot line)**;
- **There are assurances that there will be *no retaliation* for good faith reporting**.

5. Standards Enforced Through Well-Publicized Disciplinary Guidelines

The organization's compliance and ethics program should be promoted and enforced consistently through well-publicized guidelines that provide:

- Incentives to support the compliance and ethics program;

- Disciplinary measures for disobeying the law, the organization's policies, or the requirements of the compliance and ethics program.

6. Internal Compliance Monitoring

The organization shall take reasonable steps, including monitoring and auditing, to:

- Ensure that the organization's compliance and ethics program is followed;

- Periodically evaluate the effectiveness of the organization's compliance program.

7. Response to Detected Offenses and Corrective Action Plans

After monitoring and auditing of the compliance program, the organization shall take reasonable steps to:

- Respond appropriately to any violations of the law or policies to prevent future misconduct;

- Modify and improve the organization's compliance and ethics program.

8. Periodic Risk Assessments

For a compliance and ethics program to be truly effective, an organization must periodically access the risk of non-compliance or misconduct and take appropriate steps to design, implement, or modify the program to reduce the risk of non-compliance or misconduct identified through this process.

II. Risk Management Theory

A. COSO: Internal Control - Integrated Framework

B. COSO: Enterprise Risk Management – Integrated Framework

NEW YORK UNIVERSITY

A. COSO: Internal Controls

An Integrated Framework

NEW YORK UNIVERSITY

Background

• The COSO Internal Controls Integrated Framework was established in 1992 by the Committee of Sponsoring Organizations (COSO) of the Treadway Commission, which consisted of all of the major U.S. professional accounting organizations. COSO's mission was to establish a methodology to minimize the opportunity for fraud in companies, and to help assure that companies complied with all applicable laws.

• The American Institute of Certified Public Accounts (AICPA) Auditing Standards (SAS 78 – AU 319) made the COSO Framework applicable to all U.S. research universities. *See also* SAS 112 and OMB Circulars A-110 and A-133.

•The next slide illustrates and describes the COSO methodology.

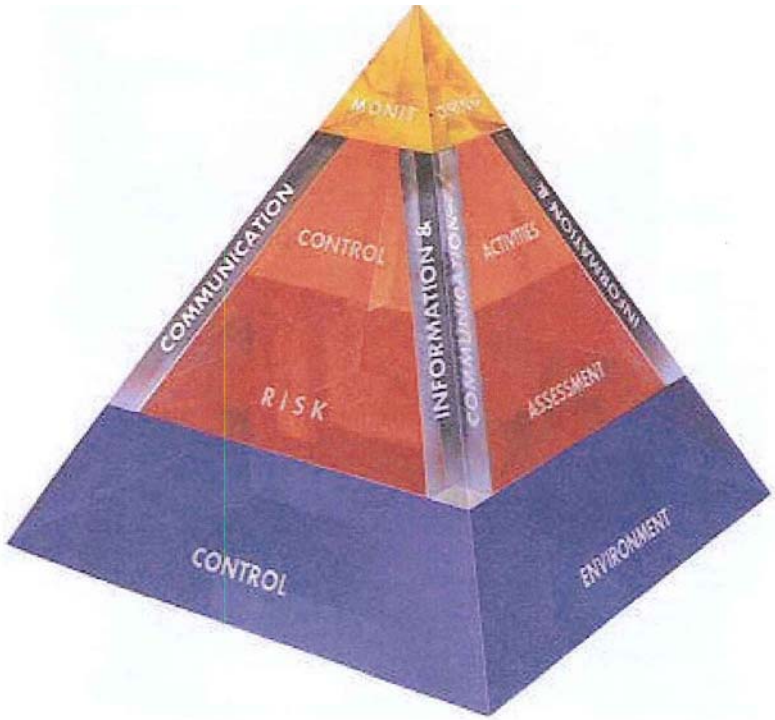
COSO- Internal Controls Defined

Internal Control is a process:

- Affected by an organization's Board of Trustees, Management, and other personnel
- Designed to achieve:
  - Effectiveness and efficiency of operations
  - Reliability of financial reporting; and
  - ***Compliance with applicable laws and regulations***

A. Internal Control
An Integrated Framework

Each section of the pyramid is critical to a successful integrated compliance program



- **5. Information and Communication** = Clear message from top management to all personnel that control responsibilities must be taken seriously and embrace their own role in the internal control system. Ready means for personnel to communicate information upstream.
- **4. Monitoring** = assessing compliance controls through on-going activities and evaluations, with modifications made as appropriate.
- **3. Control Activities** = compliance policies and procedures.
- **2. Risk Assessment** = The identification and analysis of risks relevant to achieving objectives.
- **1. Control Environment** = The environment in which personnel operate, including the people, their individual attributes, and expectations for integrity, ethical values and competence — and create the environment in which they operate.

NEW YORK UNIVERSITY

1. Control Environment

The Control Environment is the organization's *culture*:

- It reflects the overall attitude, awareness, and actions of the organizations board, management and others regarding the importance of value, ethics and compliance in the organization.

- It is the foundation of all other components of internal control.

1. Control Environment (continued)

- The Control Environment is the Organization's ***Culture,*** which is an inference derived from observable behaviors- a description of prevalent relationships

  - Culture describes what a group does in fact, as opposed to what it says it does.

- "As officers and employees of [the company] …we are responsible for conducting the business affairs of the Company in accordance with all applicable laws and in and moral and honest manner.

Enclosed…is a Certificate of Compliance to be signed by you as a statement of your personal agreement…to comply with the policies stated herein.

Kenneth Lay

Introduction to Enron Code of Ethics, July 1, 2000"

1. Control Environment (continued)

Factors affecting culture/control environment

- **Board and Audit Committee**
  - Independent and engaged?
- **Management's Philosophy and Operating Style ("Tone at the Top")**
  - Communicates by word and action support their support for compliance and commitment to ethics?
  - Code of Conduct?
  - HR Practices and Policies: Recruitment and hiring; orientation; evaluation, promotion and compensation; disciplinary actions
- **Organizational Structure**
  - Centralized vs. Decentralized
  - Assignment of Authority and Responsibility
- **Risk Culture (Appetite and Tolerance)**

2. Risk Assessment

There are several steps to risk assessment:

- Identify Possible Risk Events;
- Assess the Likelihood or Frequency of the Risk Occurring;
- Estimate Significance or Impact of the Risk;
- Determine How the Risk Should be Managed, and
- Assess What Actions Should Be Taken.

3. Control Activities

Control Activities are the policies and procedures necessary to help mitigate identified risks.

Code of Conduct

University Policies

4. Monitoring

Monitoring ensures that internal controls continue to operate effectively

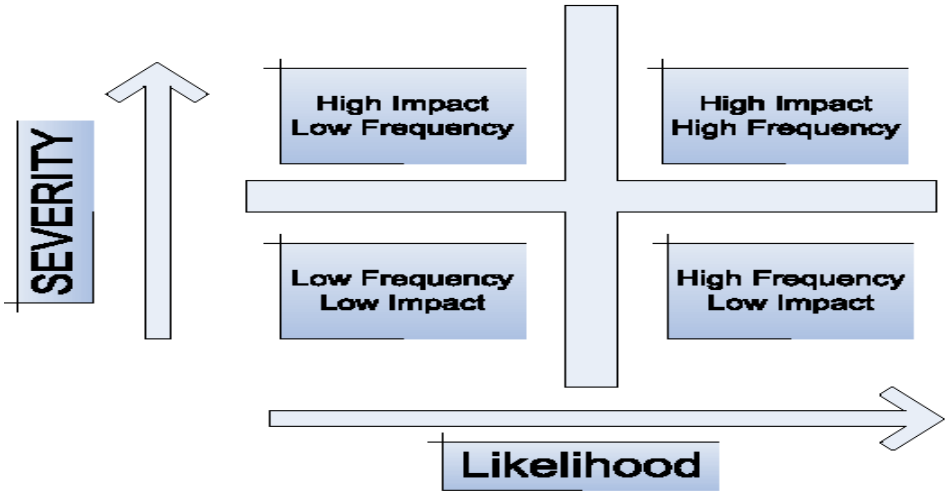
- Ongoing or separate evaluations
- Identify control deficiencies and communicate to responsible parties for corrective action.

5. Information and Communication

There are two aspects to communication

- **Clear message from top management** to all personnel to take seriously their control responsibilities and to embrace their own role in the internal control system.
- **Communication "upstream" from employees** to managers.
  - Reports from monitoring activities
  - Informal communications from employees to managers
  - Anonymous reporting lines

Simple Risk Analysis



Identified Risks

Conflicts of Interest

Medicare/Medicaid Billing

Time and Effort Reporting

Tax Exempt Bonds

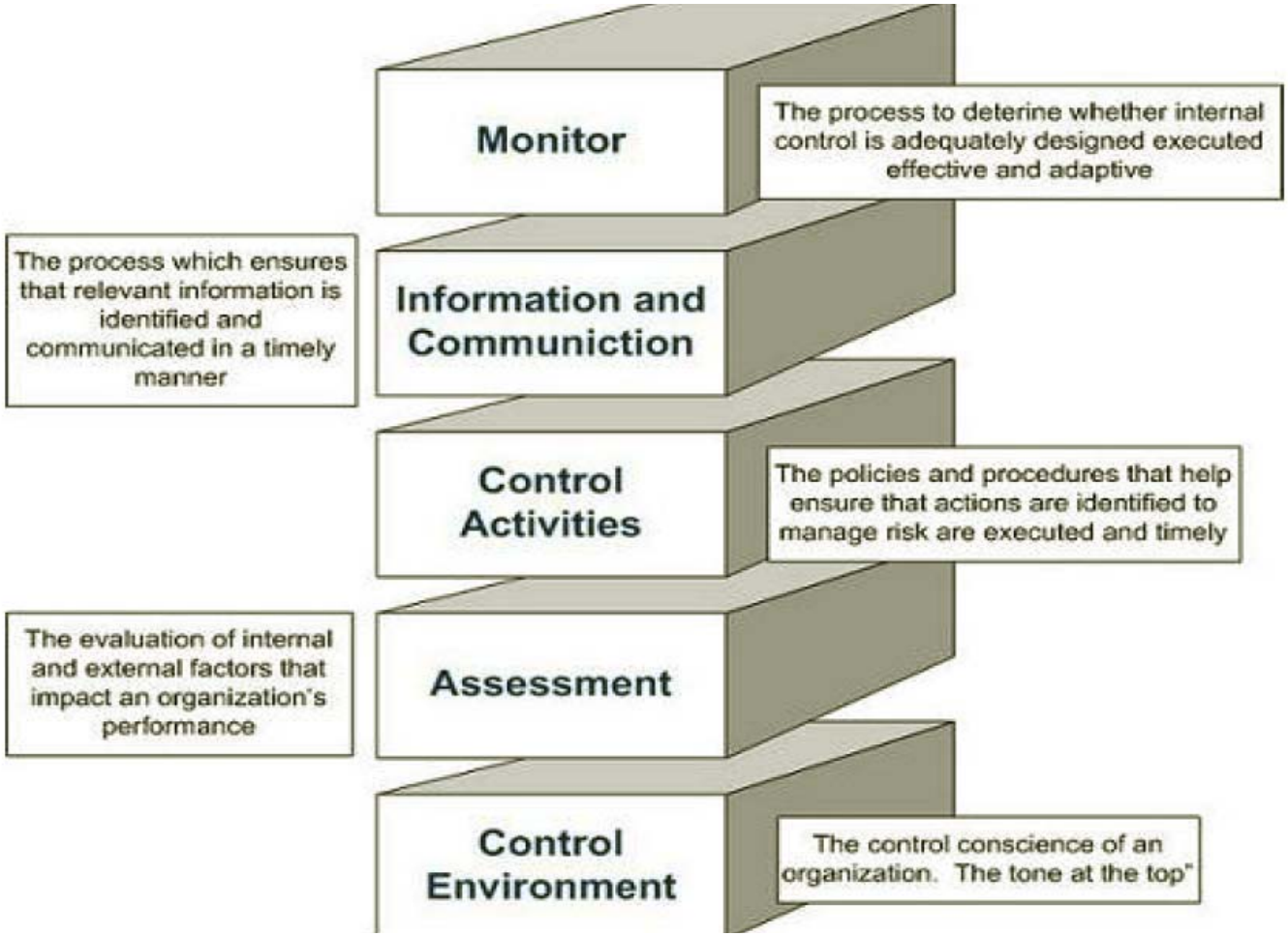
Executive Compensation

Record Retention

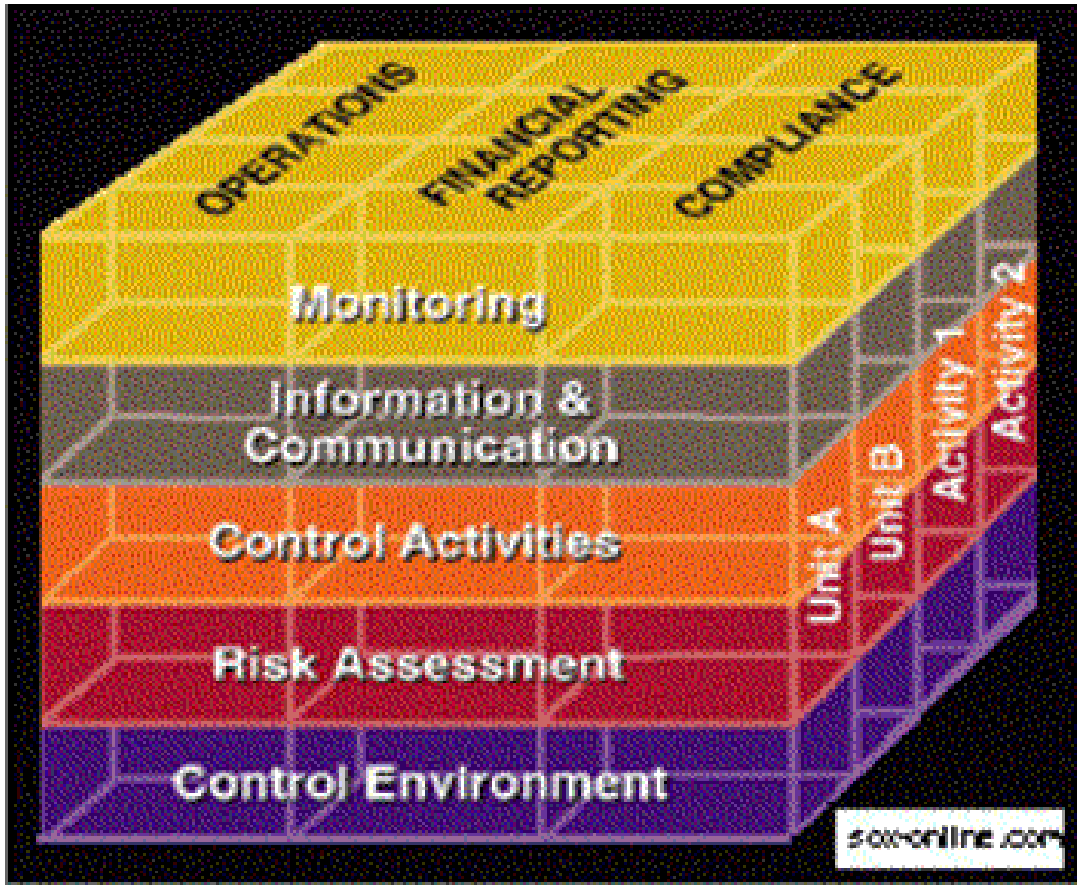
Export Controls

EEO/AA Laws

A. Internal Control
An Integrated Framework



A. Internal Control
An Integrated Framework



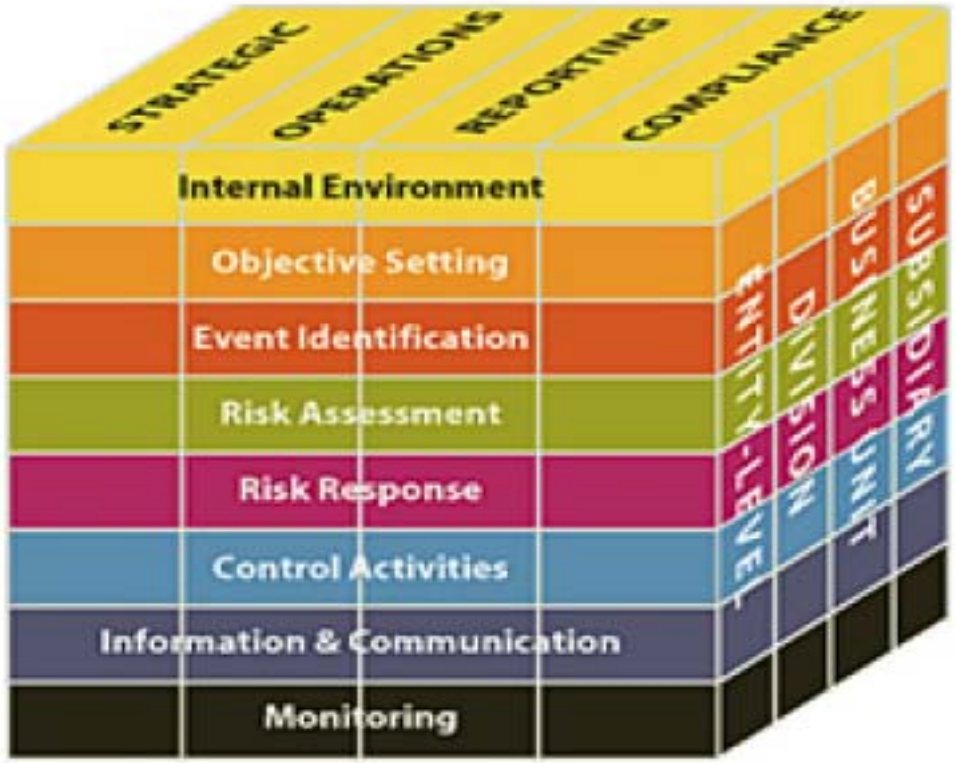
NEW YORK UNIVERSITY

II. Risk Management Theory

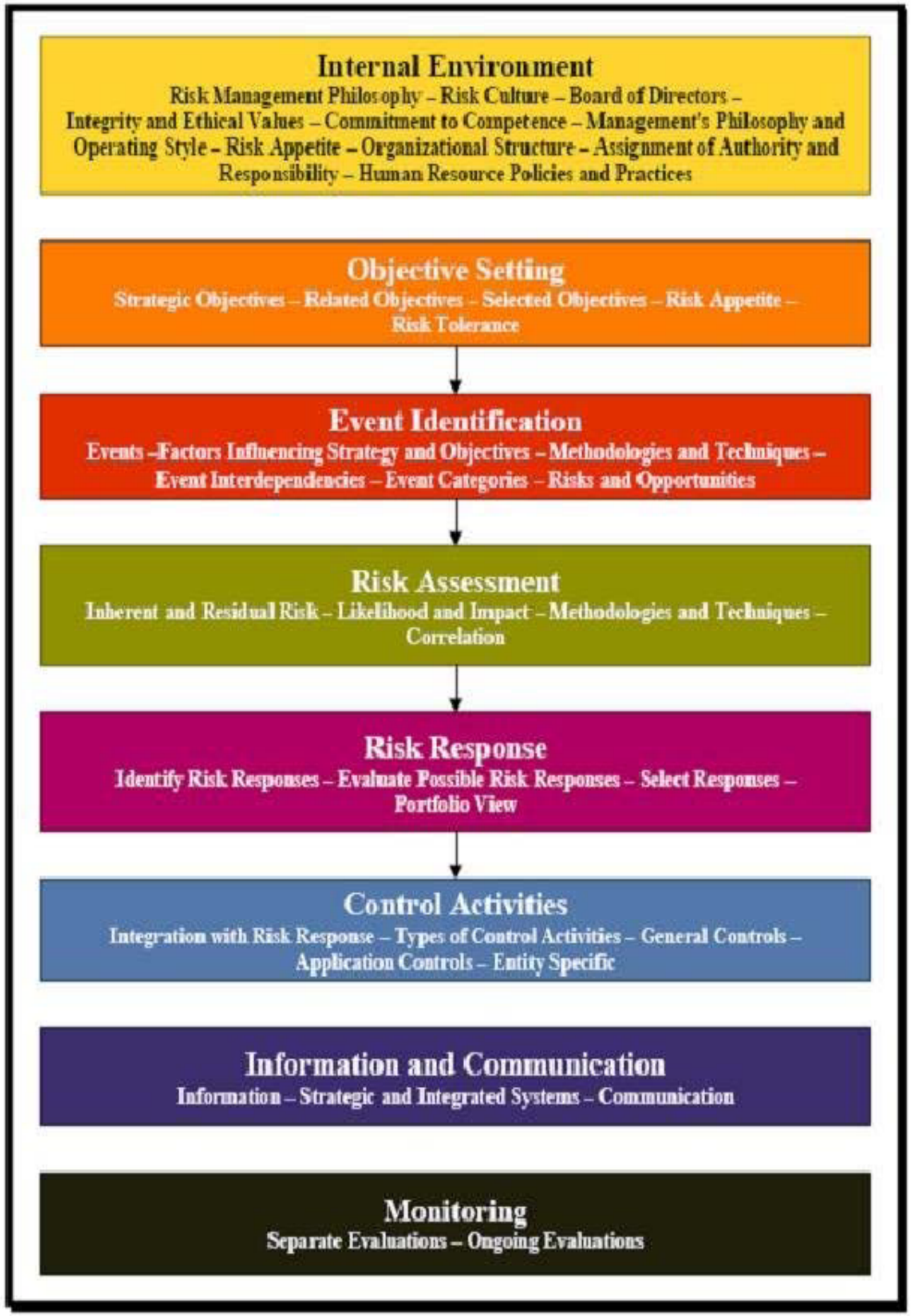
B. COSO: Enterprise Risk Management – Integrated Framework

NEW YORK UNIVERSITY

II. Risk Management Theory
B. COSO ERM



II. Risk Management Theory
B. COSO ERM



2. Objectives

- What is the Organizational Mission?
- What is the Organization's Risk Appetite in Pursing it's Mission?
- Compliance – What are the Organization's Compliance Objectives?

3. Risk Identification

- Event Inventories
  - Organizational History
  - Events Common to Industry
- Facilitated Workshops
- Interviews, Questionnaires, Surveys
- Process Flow Analysis
  - See sample “Compliance Map” handout.
- Leading events and escalation triggers (ITS)

4. Risk Assessment

- Inherent Risk
  - Financial, Operational, Legal, and Reputational impact of each identified risk
  - Likelihood, frequency and significance of impact

- Residual Risk
  - Risk after accounting for current internal controls

5. Risk Response

- Avoidance
- Reduction/Mitigation (Internal Controls)
- Sharing (e.g. Insurance)
- Acceptance
  - Crisis Management Plans
  - Business Continuity Plans
  - Other Operational Plans

6. Control Activities

- Organizational/Process Controls
  - E.g. Separation of Duties
- Documentation
  - Written Policies and Procedures Essential
- Audit Trails
  - Final Results should be traceable back to originating transactions
- Security and Integrity
  - Access Controls

III. Application of Risk Management Theory

Advanced Tools and Techniques

NEW YORK UNIVERSITY

Example - Process Flow Analysis Attachment 1

Example -Risk Assessment Algorithm Attachment 2

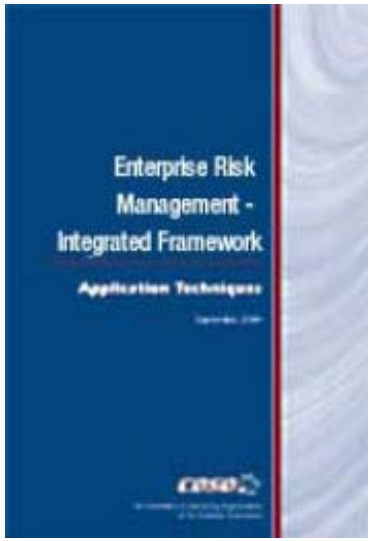
Resources

1. COSO http://www.coso.org/

Internal Controls

Integrated Framework

(1992)



Enterprise Risk Management

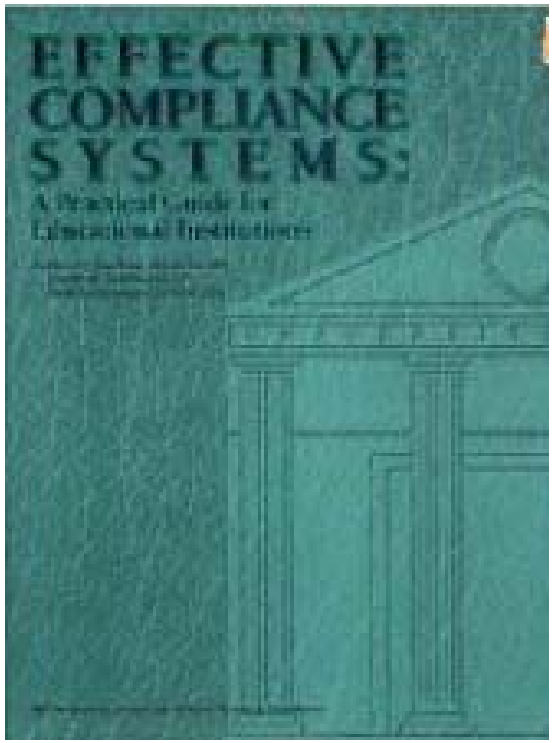
Integrated Framework

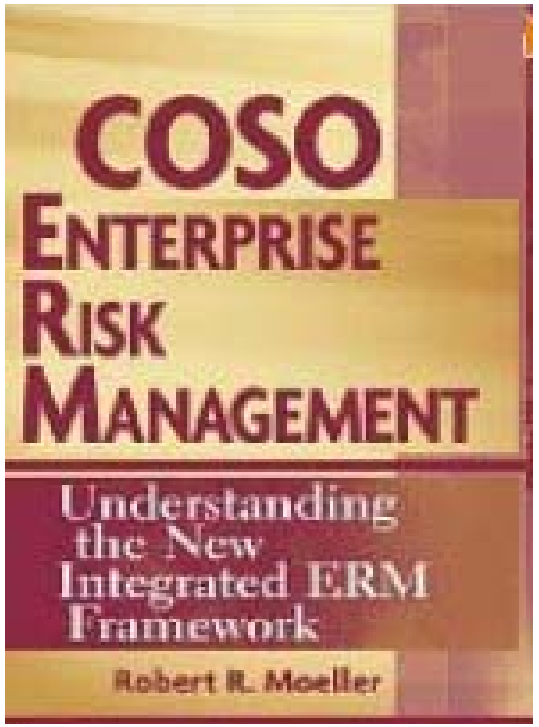
(1994)

2. Association of Corp Counsel www.ACC.com

Resources

Books www.amazon.com





NEW YORK UNIVERSITY

The End

Questions?

NEW YORK UNIVERSITY