The IRM Risk Forum 2005
The World at Risk? – learning from today, preparing for tomorrow

Workshop Title

Using ISO 9001 & ISO 14001 Systems to support Sarbanes-Oxley compliance

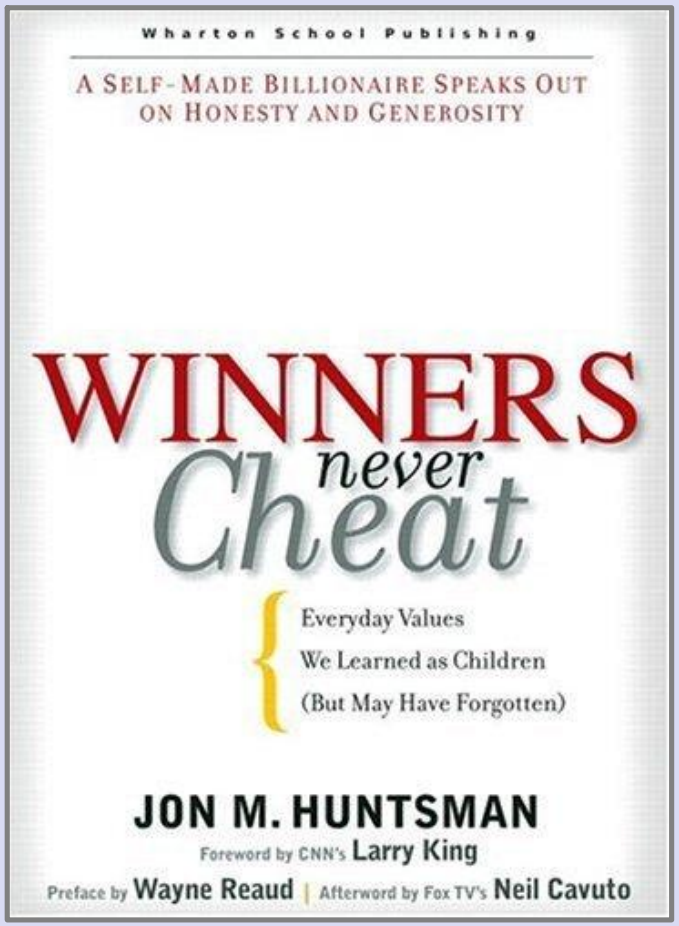
Workshop Leader

John Darby

European Quality Processes Manager

Huntsman Polyurethanes

HUNTSMAN VALUES



"We believe that ethical and moral standards are the foundation of good business policies, and will operate with integrity."

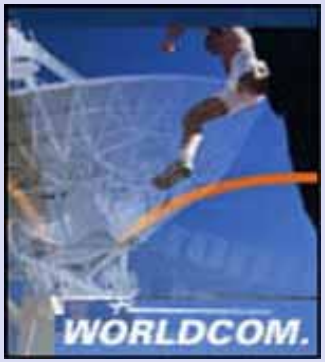
Jon & Karen Huntsman

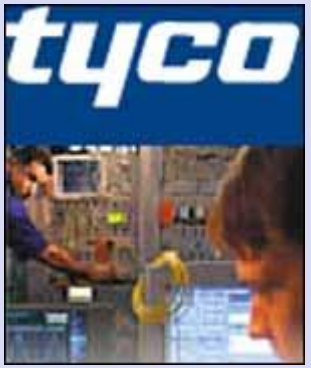
Risks Faced by Top Management

- **Risk from Major Incidents, accidents, disasters**
  - Chernobyl, Bhopal, Serveso, Piper Alpha etc.
- **Risk of trade non-compliance**
  - chemical weapons, drug-precursors, restricted parties, homeland security etc.
- **Government-mandated environmental requirements**
  - Risk of fines, shutdowns or criminal prosecution
- **Risk of ineffective management systems – customer complaints, lost business**
- **Risk from outsourced supply chain**
  - Some outsource 60-80% of their products / services
- **Risk of non-compliance with Sarbanes-Oxley Law**
  - Loss of investor confidence caused by misrepresentation of company accounts and poor internal controls
  - Heavy fines and imprisonment

What is Sarbanes-Oxley? (SOX, SarbOx)

- U.S. government's response to financial scandals, under the remit of the Securities and Exchange Commission (SEC) :
  - Enron,
  - WorldCom,
  - Tyco,
  - other large US companies





Recent Major European Frauds

- **SHELL**
  - About 25% of Oil and Gas reserves existed only in the imagination of the board members

    4 billion barrels @ $ 60/barrel = $bn 240

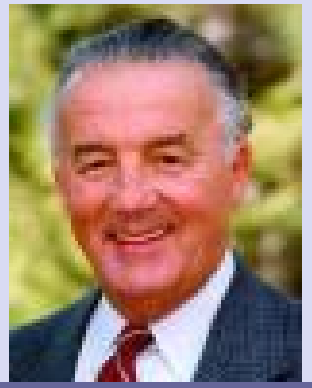
    Market value of Shell shares = $bn 140

- **PARMALAT**
  - €10bn found missing from the corporate accounts

- **AHOLD**
  - admitted overstating earnings at subsidiaries in the U.S. and Argentina by at least $500 million in 2001 and 2002

SOX Objectives

- To restore public trust and confidence in the public securities market
- To improve corporate governance
- To enhance transparency of financial statements and disclosures
- To ensure that company executives are informed and aware of material information from a well-controlled environment



Senator
Paul S. Sarbanes (MD)

Congressman
Michael G. Oxley (OH)

Sarbanes-Oxley Act

One Hundred Seventh Congress
of the
United States of America

AT THE SECOND SESSION

Begun and held at the City of Washington on Wednesday, the twenty-third day of January, two thousand and two

An Act

To protect investors by improving the accuracy and reliability of corporate disclosures made pursuant to the securities laws, and for other purposes.

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled,

SECTION 1. SHORT TITLE; TABLE OF CONTENTS.

(a) SHORT TITLE.—This Act may be cited as the "Sarbanes-Oxley Act of 2002".

SOX Law ceremony

“The only fair risks are based on honest information.”

“Tricking an investor into taking a risk is theft by another name.”

“Corporate executives must set an ethical tone for their companies.”

George W Bush,
30 July 2002

Senator Paul Sarbanes and Congressman Michael Oxley at White House ceremony as the Public Company Accounting Reform and Investor Protection Act of 2002 became law by presidential signature.

Sarbanes-Oxley Act

- Increased auditor independence
- Personal accountability for CEOs and CFOs
- Additional accountability for corporate boards
- Increased criminal and civil penalties
- Increased disclosure regarding executive compensation
- Certification of internal audit work by external auditors

SOX Reach is Global

- All US-listed Companies, including multi-nationals and ‘foreign companies’, must comply by 15 July 2006
- more than 7000 EU Companies are affected
- The European Commission's proposed directive on auditing will be “tougher” than Sarbanes-Oxley when implemented
  - EU Corporate Governance Action Plan
  - Disclosure of annual corporate governance statements

Sarbanes-Oxley Act - Summary

- **Section 103:**
  Auditing, Quality Control, and Independence Standards and Rules
- **Section 302:**
  Corporate Responsibility for Certifying Financial Reports
- **Section 404:**
  Management Assessment of Internal Controls
- **Section 409:**
  Real Time Issuer Disclosures
- **Section 806:**
  Whistle Blower Protection
- **Section 906:**
  Requirements for Certifying Periodic Reports & Criminal Penalties

KEY Section 302

- CEOs and CFOs to sign attestation to the annual and quarterly reports:
  - "I didn't know" is no longer an appropriate defence.
  - Attest to having accepted responsibility for internal controls over their financial processes.

Ignorance is no defense

Pleaded ignorance, still held accountable

"I was just the coach. I am a country boy. I really did not know what was going on."

Bernie Ebbers

(WorldCom CEO)

Bernard and Kristie Ebbers leaving court *(WSJ On-line March 16, 2005)*

KEY Section 404

- Clearly defined Risk Management Program
- Financial processes established & documented
- Information (computer) Systems integrity for financial reporting
- Examine / eliminate employee opportunity for fraud.

Section 404 requires a "System of Internal Control"

- **Internal control is a process designed to achieve**
  - Effectiveness and efficiency of operations
  - Reliability of financial reporting
  - Compliance with applicable laws and regulations
- **Controls must be preventive and corrective**
  - Eliminate potential risks
  - Provide a mechanism to manage risk

Which Standards Apply?

- **The Sarbanes-Oxley Act requires that:**
  - companies perform internal controls audits
  - CEO's and CFO's attest to the audit findings

- **Financial Statements are required by the SEC to conform with US GAAP (Generally Accepted Accountancy Principles) – a set of accountancy rules**

Which Standards Apply?

- the standard against which to audit the system of internal controls is not defined.
- The COSO ERM framework *(and the equivalent COBIT framework for IT controls)* has most support from the SEC as a model for internal controls
- Both frameworks share the fundamentals of ISO 9001 / ISO 14001

The COSO ERM Framework

different perspectives:

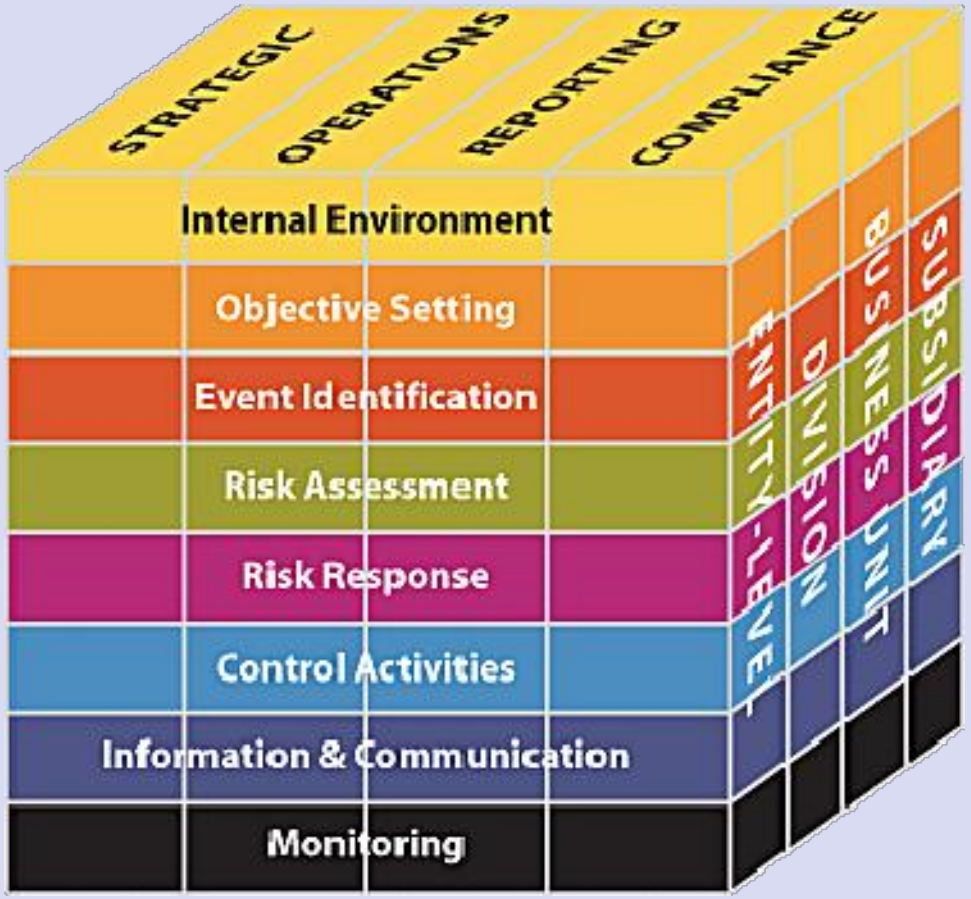
- Enterprise-level
- Division or subsidiary
- Business unit processes

how individual risks interrelate:

- Strategic
- Operations
- Reporting
- Compliance

eight components of the framework:

- internal environment
- event identification
- risk assessment
- risk response
- control activities
- information & communication
- monitoring



System of Internal Control

Required Structure

1. Internal control environment
2. Risk identification, assessment & response
3. Control activities
4. Information and communication
5. Monitoring

1. Internal Control Environment

- **Provides fundamental values, discipline and structure.**
  - **Foundation for all other components of internal control**
  - **Includes objectives & performance against the objectives**

- **The Process Approach is an example of a control environment.**

2. Risk Identification, Assessment & Response

- **Precondition to risk assessment**
  - **Establish objectives, linked at various levels**
- **Identify and assess risks vs. achieving objectives**
- **Determine how to manage the risks**
- **mechanism for dealing with change**

3. Control Activities

- Policies and procedures that ensure management directives are carried out
  - Approvals, authorizations, verifications, performance reviews, etc.
- Ensure actions are taken to address risk
- Auditing the policies and procedures is an essential component of the Control Activities

4. Information and Communication

Pertinent information must be identified, captured and communicated

- Covers the information systems that produce reports containing operational, financial and compliance-related information
  - used to run and control the business
  - enable informed business decisions to be taken

5. Monitoring

- Monitoring is defined as “external oversight of internal controls by management or other parties”
- Traditional financial audits alone do not comply with this requirement
- Audit committee should annually review the monitoring program that management establishes

The COSO ERM framework

similarities with ISO9001 and ISO 14001:

- **The organisation must have objectives and know how it is performing against them, and what it would do if it didn't meet the objectives.**
- **The financial procedures and processes must be documented.**
  - ***flowcharts or process maps are recommended.***
- **Employees must be 'competent' - qualified and trained**

Equivalent Documents

• Process Narrative	≣	QEMS Manual (process approach)
• Flowcharts	≣	QEMS Procedures (process maps)
• Risk Control Matrix	≣	QEMS Control Plan
• Test Plan	≣	QEMS Audit Schedule
• Gap logs	≣	Internal QEMS Audit Findings

How Can QEMS Help?

ISO 9001 & ISO 14001 :

- describe a structure to manage risk (vs. customer, environmental, reputation, legal)
- describe the process approach to management
- define how competency of employees should be managed
- provide a measure of the status and effectiveness of the organisation
- add a focus on continual improvement
- require regular internal and external auditing

Management Systems

Help Satisfy Major Requirements of Sarbanes-Oxley:

- The System of Internal Controls
- Supplemental information to the Board of Directors (top-management review - health check)
- Information needed by CEOs and CFOs to certify the appropriateness of their financial statements

Value-Added Auditing

- Changing Internal Financial Auditing scope:
  - **Traditional**: evaluating internal financial controls and ensuring compliance to regulations / GAAP
  - **Future**: evaluating operational effectiveness and the control and management of risks

- ISO 9001 and ISO 14001 promotes
  - Process approach and
  - Process Audits

  as the foundation of the new audit structure

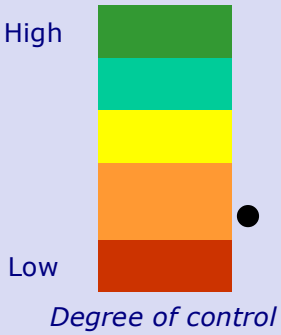
- Risk-Based Process Audits are needed to evaluate the status of the organization.

Risk-based QEMS Auditing

- DNV certification benchmarks an organisation's management system against national and international best practices - looking beyond compliance.
- the DNV certification process is tailored to the unique needs of each company to provide better information to top management on the organisation's ability to meet strategic objectives.
- DNV audits focuses on critical areas and issues identified by the organisation. For Huntsman, this includes SOX compliance.

DNV Audit Report

Focus Area 3 – Integration of Sarbanes Oxley compliance auditing into ISO9001 process audits



Currently, separate audits cover compliance to Sarbanes Oxley requirements with compliance and improvement audits to ISO9001.

Both the requirements of Sarbanes Oxley and ISO9001 should be embodied in the management system.

Initially the focus of the Sarbanes Oxley audit must be to ensure systems are in place to ensure compliance. Once this is established an integrated audit should monitor continuing compliance.

Benefits of QEMS Internal Audit Support:

- uses a team of people experienced in both compliance and process auditing
- helps lead to transparency in the organisation
- provides focus on continual improvement
- results in a more accurate measure of the status and effectiveness of the organisation.

Conclusion

Management Systems Support of Internal Financial Auditing Will Help:

- restore investor confidence in the marketplace
- provide reliable information for all stakeholders
- top management and the Board of Directors to identify and control business risks and prevent major surprises
- improve corporate governance
- achieve Sarbanes Oxley compliance

Workshop

Discuss the following questions:

- Is your organisation getting full value from it's ISO9001 and ISO14001 internal audits?
- Are Finance and Quality seen as unrelated activities in your organisation?
- Do your financial auditors recognise the contribution that internal QEMS audits could make towards control of financial risk?
- Are your certification body auditors helping you to assess your internal controls for your major risk areas?
- What issues are preventing your organisation from making maximum use of the QEMS at senior level?

Workshop

Present the following:

1. A SWOT analysis of your current internal control systems.

2. A Broad Action Plan to encourage your organisation to use all of its resources to manage financial risks – including the internal QEMS auditors and the external certification body auditors.