

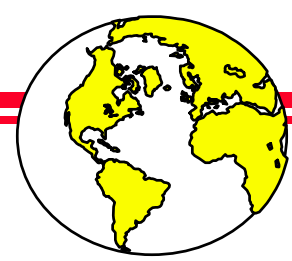
How Quality and Environmental Management Systems can support Internal Financial Auditing in response to the requirements of the Sarbanes-Oxley Law (SOX)

John Walz

ASQ's Annual Quality Conference

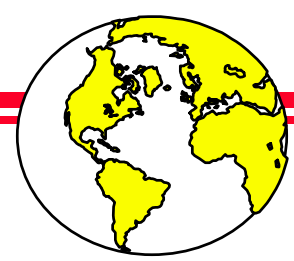
Toronto, Ontario, Canada

May 24-26

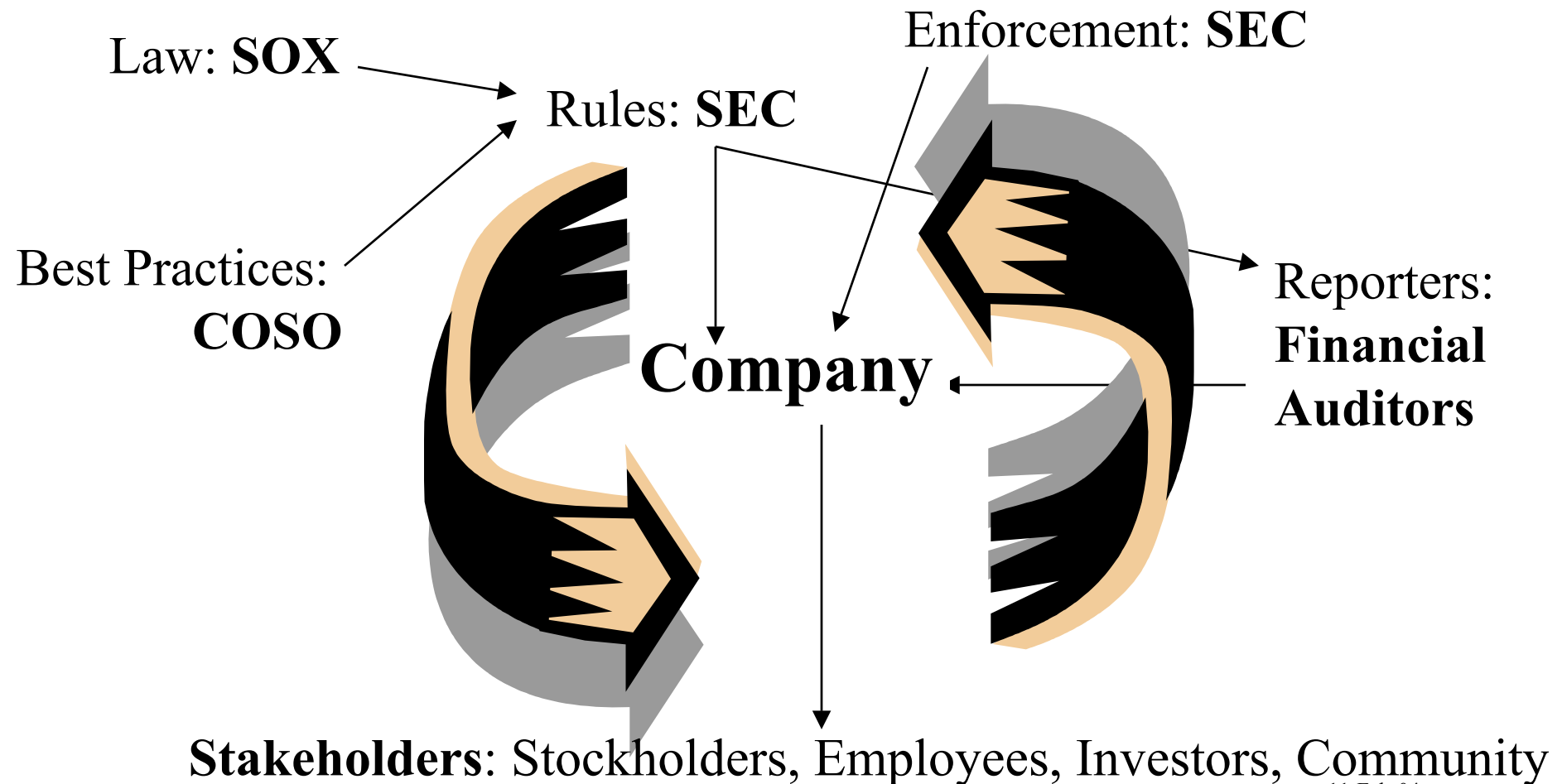


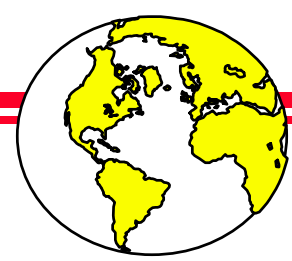
Today's Schedule

- First Session (Sandford Liebesman)
 - What is the Sarbanes-Oxley Act (SOX)?
 - System of Internal Controls
 - Risks Faced by Top Management
- **Second Session (John Walz)**
 - **How Quality/Environmental Management Systems can Support Internal Financial Auditing**
- Third Session (Paul Palmes)
 - Case Study: Northern Pipe Inc.



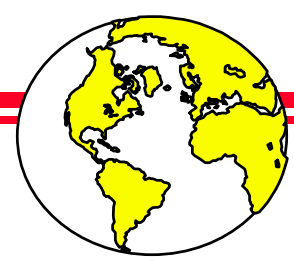
Common Goal: To provide Top Management and the board of directors with an **accurate** understanding of the organization's **status**





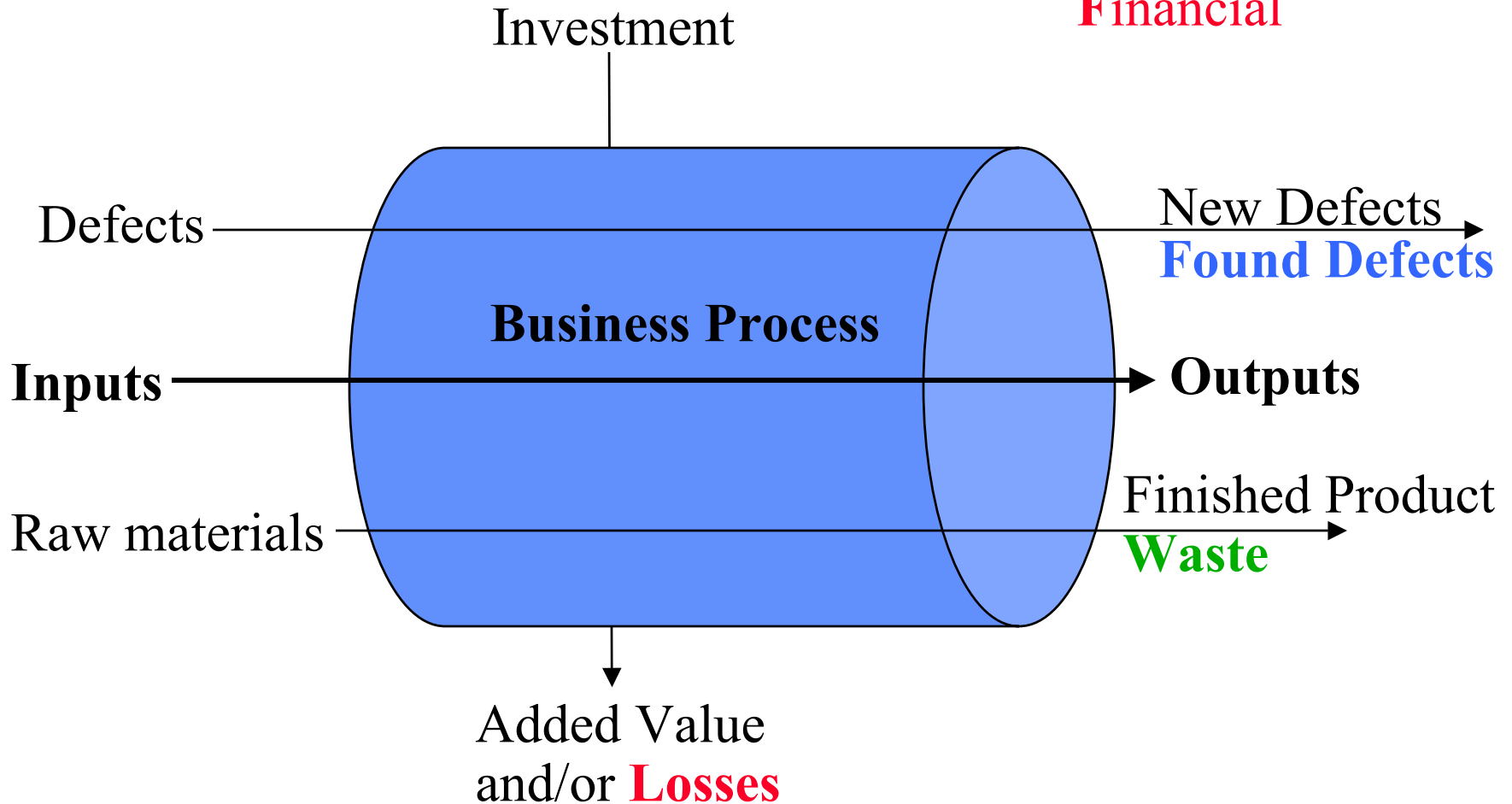
How Quality/Environmental Management Processes Can Help

- **Business Processes**
- Managing Risk,
- Internal controls,
- Value-added auditing,
- Integrating QMS/EMS and SOX

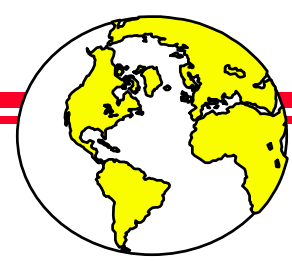


Process Attributes

Quality
Environmental
Financial

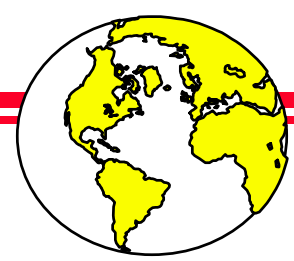


where **SOX** and **Quality** / **Environment** meet



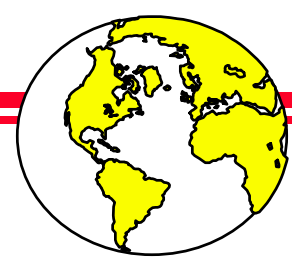
How Quality/Environmental Management Processes Can Help

- Business Processes
- **Managing Risk**
 - The Achilles Heel of Organizational Progress
- Internal controls
- Value-added auditing
- Integrating QMS/EMS and SOX



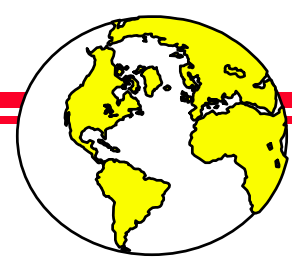
Managing Risk - Examples

- Highly outsourced supply chain
- Revenue Recognition
- Homeland Security
- Government-mandated environmental requirements
- General risk of ineffective management systems



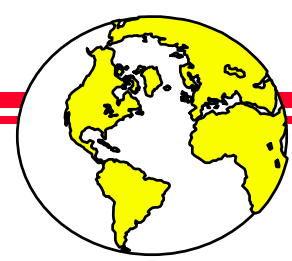
How Quality/Environmental Management Processes Can Help

- Business Processes
- Managing Risk
- **Internal controls**
- Value-added auditing
- Integrating QMS/EMS and SOX



Using ISO 9001 and 14001 to support the System of Internal Controls

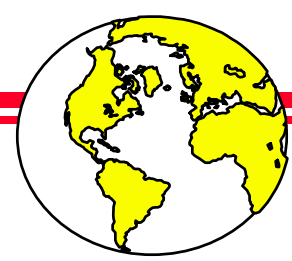
- ISO **QMS** / **EMS** standards provide
 - process management,
 - corrective, & preventive action,
 - data analysis, and
 - continual improvement.
- Other standards elements:
 - customer focus,
 - top management involvement,
 - document control, and
 - resource management.



Internal Controls – COSO requirements

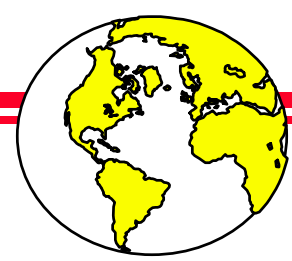
ISO 9001 and **ISO 14001** framework can satisfy the five internal controls requirements

1. Control Environment
2. Information And Communication
3. Risk Assessment
4. Monitoring
5. Control Activities



1. Internal Control Environment

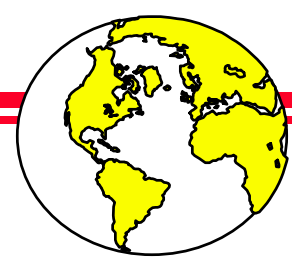
- ISO 9001 Clause 4.1 Processes, Methods, Resources, Continually Improved
- ISO 9001 Clause 5.3 **quality policy**
- ISO 14001 Clause 4.1 **environmental policy**
- ISO 9001 Clause 5.4.1 Measurable Objectives
- ISO 14001 Clause 4.2.3 **Environmental** Objectives
- ISO 9001 Clause 5.5.3, “Internal Communication”
- ISO 14001 Clause 4.3.3 “Internal Communication”



Internal Control Environment

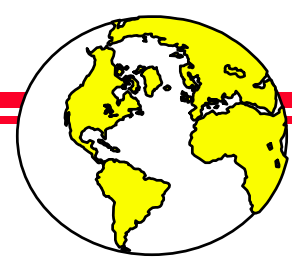
The above ISO clauses result in:

- Linkage between the management processes and internal controls
- Decision making process is enhanced through improved Information & Communication
- Line management's understanding of internal controls will be extended and linked to the organization's objectives
- Insure the reliability of accounting and disclosure policies, including environmental liability



2. Information and communication

- ISO 9001 and 14001 are structured to enhance the relevance and reliability of information
- ISO 9001 Clauses:
 - 4.2 Quality manual, policy and objectives, documented procedures and records,
 - 5.5.3 Internal communication
 - 7.2.3 Customer communication
 - 7.4.2 Supplier communication
 - 5.1 Top management communication



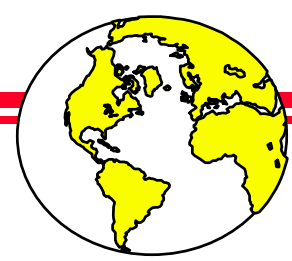
3. Risk Assessment

- ISO 9001/14001 Compliance
 - helps manage risks that could jeopardize organization's objectives
- ISO 9001 Clauses:
 - 8.2.3 & 8.2.4 Monitoring and Measurement of Processes & Products,
 - 8.4 Analysis to demonstrate QMS suitability & effectiveness
- ISO 14001, Clauses Helps identify the major **environmental risks**
 - 4.2.1 Identify **environmental aspects**
 - 4.3.6 Identify operations & activities associated with significant **environmental aspects**



4. Monitoring

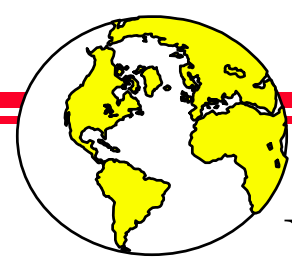
- ISO 9001 Clauses:
 - 8.2.3 Monitor and measure Processes
 - 8.2.4 Monitor and measure Products
 - 8.2.1 Monitoring and measurement of customer satisfaction
 - 8.4 Analysis of customer satisfaction data
 - 8.5.1 Continual improvement of the effectiveness of the QMS
- ISO 14001 Clause 4.4.1
 - Monitor & measure key characteristics of operations & activities that have significant impact on the **environment**
- ISO 9001 Clause 5.6 and 14001 Clause 4.5
Management Review



5. Control Activities

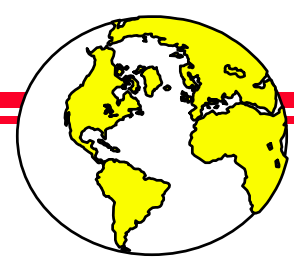
ISO 9001 Clauses 8.5.2 & 8.5.3, and ISO 14001,
Clause 4.4.2

- Corrective and Preventive Actions
- Improved alignment of functions and tasks with the Organization's Objectives
- Improvement in the effectiveness & predictive nature of the controls



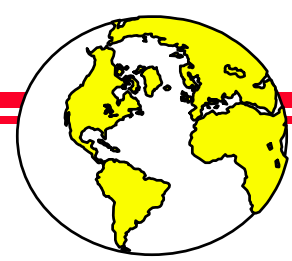
Results of Effective Internal Controls

- ISO 9001 **QMS** and ISO 14001 **EMS**
 - Major support of the internal controls and reporting procedures required by Sarbanes-Oxley.
 - Provide a structured supporting system for the management of internal controls.
 - Encourage a proactive approach to system management and a philosophy of continual improvement.
 - Regular auditing of the management system, which can add value to the organization.



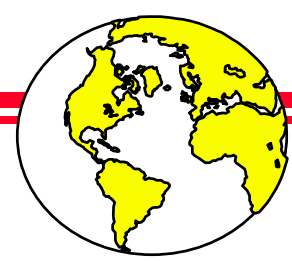
How Quality/Environmental Management Processes Can Help

- Business Processes
- Managing Risk
- Internal controls
- **Value-added auditing**
- Integrating QMS/EMS and SOX



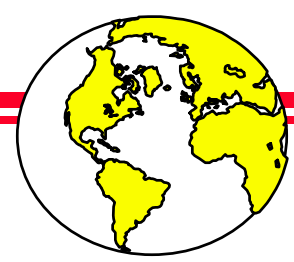
Value-Added Auditing

- **Goal:** To provide Top Management and the board of directors with an accurate understanding of the organization's status
- Companies need to **combine** its **QMS** and **EMS** “tools” with **financial** auditing function & procedures
 - Use the continual improvement processes to create a more effective organization



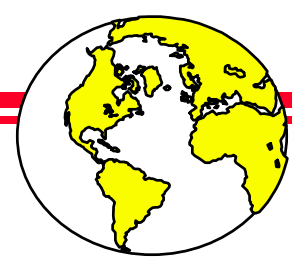
Value-Added Auditing

- **Quality** and **Environmental** auditors collaborating with internal **financial** auditor to provide consolidated audit reports to the Board of Directors' audit committee
 - Combined/Joint audits will increase efficiency and understanding of the organization's status
 - Consolidated report for the Board of Directors to understand the current state of the organization
 - Tiered approach for Non-Conformance Management
- Strengthens the internal controls of the organization
- Helps organizations achieve Business Strategies & Objectives



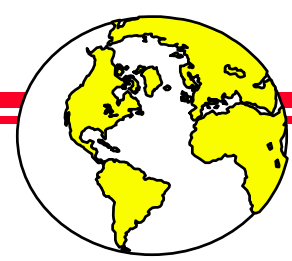
How Quality/Environmental Management Processes Can Help

- Business Processes
- Managing Risk
- Internal controls
- Value-added auditing
- Integrating **QMS/EMS** and **SOX**



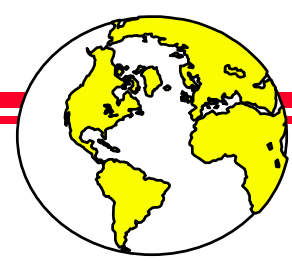
A New Standard is Needed

- Companies need to report publicly information used internally to manage their business
- Expanding the audit structure provides information needed by CEOs and CFOs to certify financial statements appropriateness as required by SOX
- Merging **quality**, **environmental**, & internal **financial** auditing & procedures can assure
 - Transparency in an organization and
 - Focus efforts on continual improvement



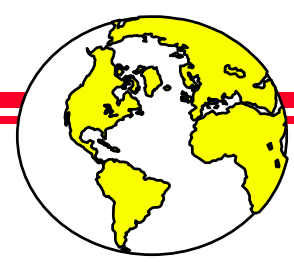
IT / Software Products to address the SOX requirements

- Provides continually updated document compilation and data collection for entire corporate operations
- Integrates company procedures and shapes internal controls according to **QMS** & **EMS** ISO requirements
- Interject SOX requirements into corporate procedures while simultaneously accounting for **QMS** & **EMS** ISO standards

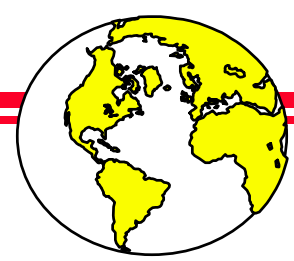


Conclusions

- **Goal:** To provide Top Management and the board of directors with an accurate understanding of the organization's status
- **QMS** & **EMS** aligned with SOX along with combined **Q/E/Financial** audits & procedures will meet the intent of the SOX law

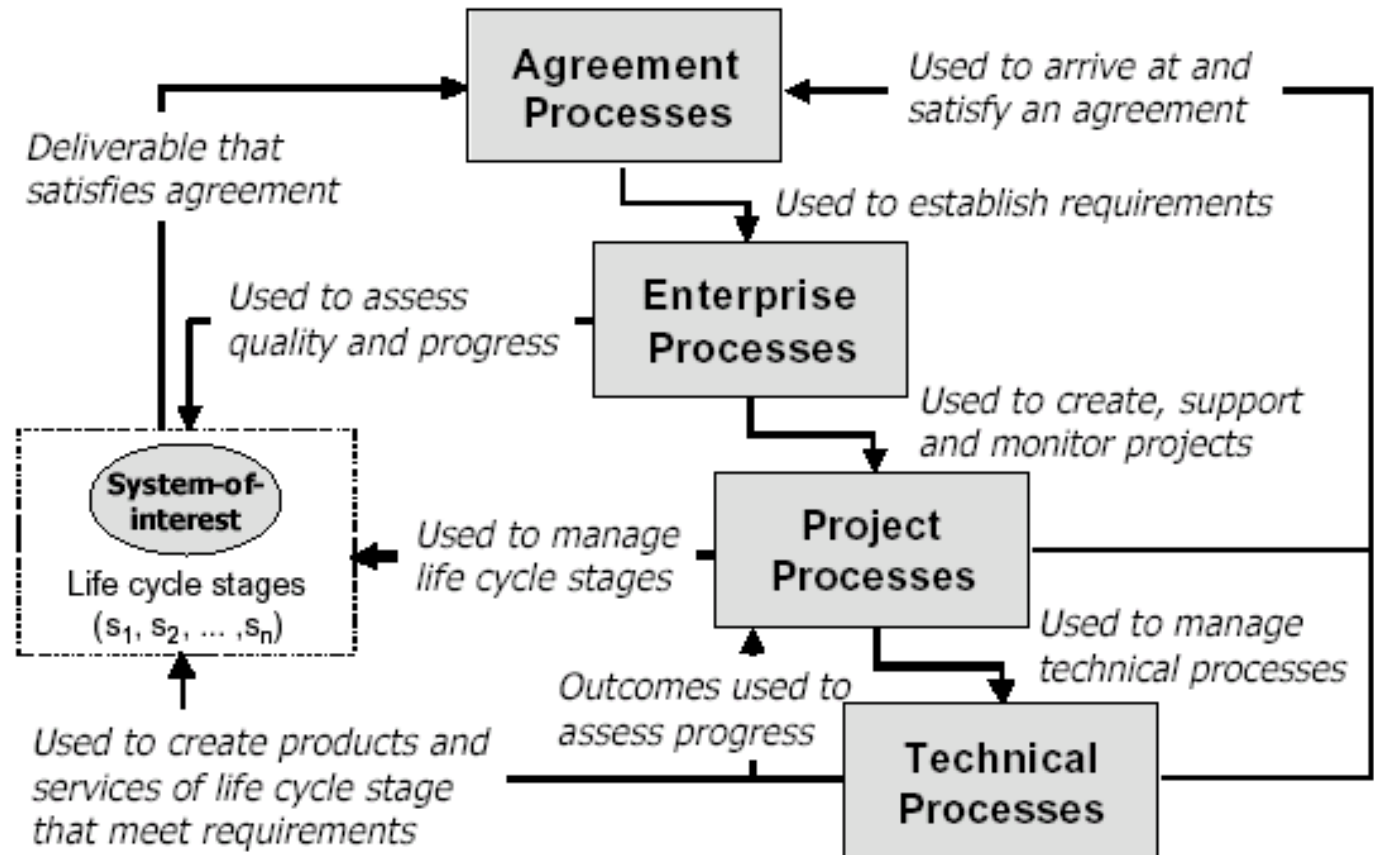


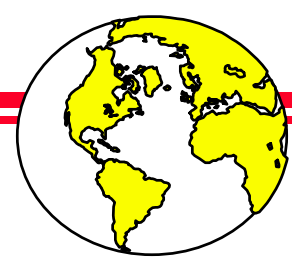
BACK-UP SLIDES



Business Processes

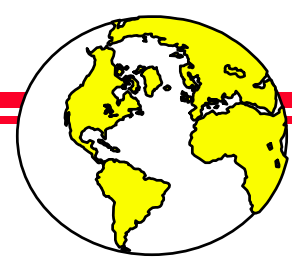
- Where **SOX** and **Quality** / **Environment** meet
- Types of Processes





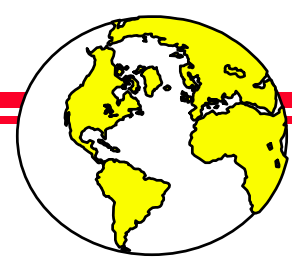
Managing **Quality** Risks - Outsourcing

- Outsource major parts of the supply chain
- Outsource Work model
 - Outsource what the organization does not do well
 - Keep the core processes
- Manage the outsourced processes
 - as if still under organizational complete control
- Supply chain management performance metrics



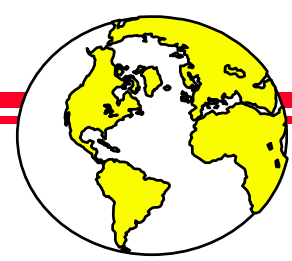
Supply chain management performance metrics

- **Delivery Performance**
 - on-time delivery,
 - performance to commit,
 - fill rate, and
 - return rates / **warranty**
 - (**Accounts Payable** trigger)
- **Cycle Time**
 - promised lead time,
 - actual lead time,
 - **rework** time, and
 - supply chain cycle time
- **Inventory and Cash Management**
 - inventory days of supply,
 - days sales outstanding,
 - days payables outstanding, and
 - cash-to-cash conversion
- **Supply Chain Costs**
 - overall supply chain,
 - order management,
 - inventory carrying,
 - supply chain finance and planning,
 - supply chain IT, and
 - procurement department staffing



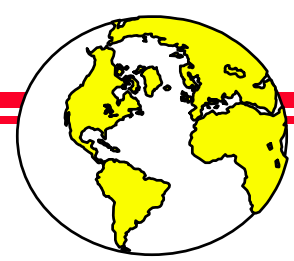
Managing **Quality** Risks – **Revenue** Recognition

- Key to SOX
- Breakdown for many dishonored companies
 - Restate earnings triggering falling stock price
- ISO 9001 Sect. 7 – **Product Realization**
 - Overlap of **QMS** and Internal **Financial** Auditing
 - Investments,
 - Costs,
 - Sales, Invoices, Payments



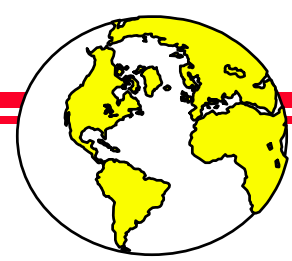
Managing Security Risks – Homeland Security

- Shipping containers
 - Risk of concealing weapons of mass destruction
- Finished goods
 - Screening and transport to the customer
- Security requires new processes to be developed and managed
 - ISO 9001:2000 is well suited to the design, development, and control of these processes



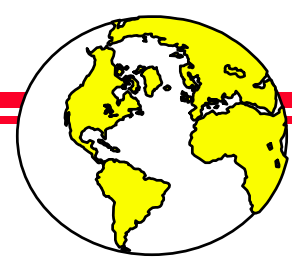
Managing **Environmental** Risks - Examples

- Purchasing department shifts from a domestic to a foreign chemical supplier,
- Downsizing results in key environmental manager not being replaced,
- Material specification change requires a new “Material Safety Data Sheet,” which has not been developed



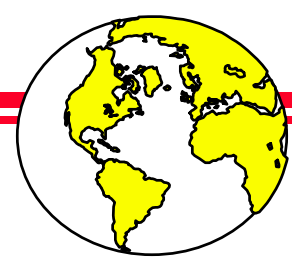
Managing **Environmental** Risk

- If ISO 14001 is not on top management's radar screen, **then** fulfilling environmental management requirements can be very **risky**
- EPA recognizes the value of ISO 14001
 - EMS Framework is P-D-C-A
 - EPA established the *National Environmental Performance Track*
- EMS implementation
 - can have benefits beyond satisfaction of governmental regulations



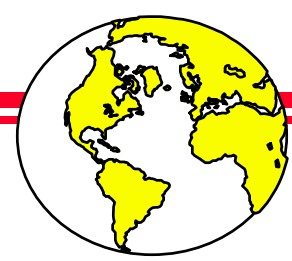
Internal Controls

- Internal controls are designed to assure
 - achievement of objectives and goals,
 - especially in the effectiveness and efficiency of operations,
 - reliability of financial reporting and
 - compliance with applicable laws and regulations
- Controls
 - preventive to eliminate potential risks or
 - corrective to identify and correct events, which are causing risk to the organization.



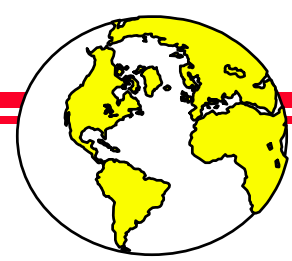
1. Internal Control Environment

- ISO 9001:2000 Clause 4.1
 - Identification of all **processes** needed by the organization and the determination of the sequence & interaction of these processes
 - Methods to ensure that the processes are effective,
 - Needed resources are available,
 - Processes are monitored and measured and continually improved



Internal Control Environment

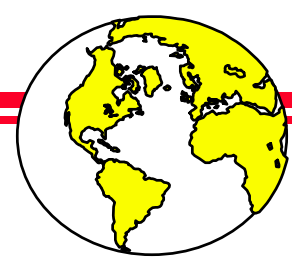
- ISO 9001 Clause 5.3
 - Top management ensure the **quality policy** “includes a commitment to comply with requirements and continually improve the effectiveness of the quality management system and provides a framework for establishing and reviewing quality objectives.”
- ISO 14001 Clause 4.1
 - Top management to establish an **environmental policy** that includes a commitment to continual improvement and a framework for setting and reviewing environmental objectives and targets



Internal Control Environment

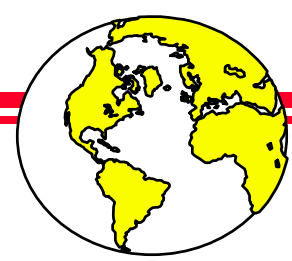
Organization's objectives is a key element of control

- ISO 9001 Clause 5.4.1
 - Top management to establish measurable objectives in the organization
- ISO 14001 Clause 4.2.3
 - Documented **environmental** objectives and targets
- ISO 9001 Clause 5.5.3, “Internal Communication”
 - Top management must establish communication processes regarding the effectiveness of the quality management system
 - (Clause 4.3.3 of 14001 has similar communications requirements)



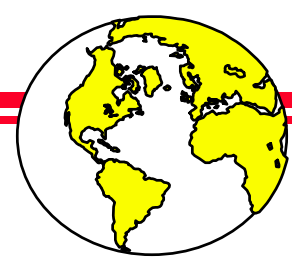
2. Information and communication

- ISO 9001 and 14001 are structured to enhance the relevance and reliability of information
- ISO 9001 Clause 4.2
 - Quality manual,
 - Documented quality policy and objectives,
 - Specific documented procedures and records,
 - Documents needed to ensure the effective planning, operation, and control of its processes
- The documentation forms the basis of objective evidence required during a value-added audit



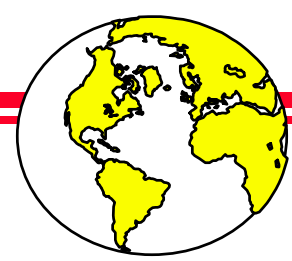
Information and communication

- ISO 9001 Clauses 5.5.3, 7.2.3, 7.4.2, 5.1
 - Internal communication
 - Customer communication
 - Supplier communication
 - Top management communication
 - importance of meeting customer as well as statutory and regulatory requirements



3. Risk Assessment

- ISO 9001/14001 Compliance
 - helps manage risks that could jeopardize organization's objectives
- ISO 9001 Clauses 8.2.3 & 8.2.4 & 8.4
 - Monitoring and Measurement of Processes & Products,
 - Analysis to demonstrate QMS suitability & effectiveness
 - helps identify the major operational risks

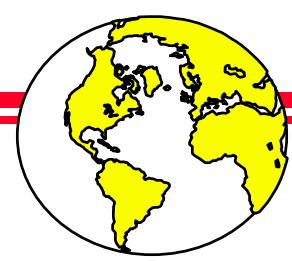


Risk Assessment

ISO 14001, Clauses 4.2.1 & 4.3.6

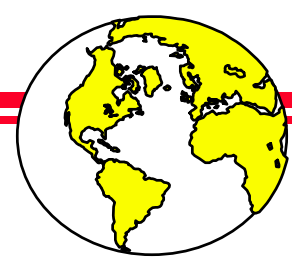
- Identify **environmental aspects**
 - “elements of an organization’s activities, products or services which can interact with the environment”
- Identify operations & activities associated with significant **environmental aspects**

Helps identify the major **environmental risks**



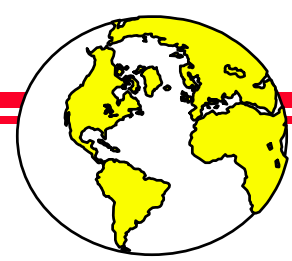
4. Monitoring

- ISO 9001 Clauses 8.2.3, 8.2.4, 8.2.1, 8.4
 - Monitor and measure Processes
 - Monitor and measure Products
 - Monitoring and measurement of customer satisfaction
 - Analysis of customer satisfaction data
- ISO 14001 Clause 4.4.1
 - Monitor & measure key characteristics of operations & activities that have significant impact on the **environment**
- Provide:
 - First warning signs of risk and
 - Data to evaluate problems and suggest solutions



Monitoring

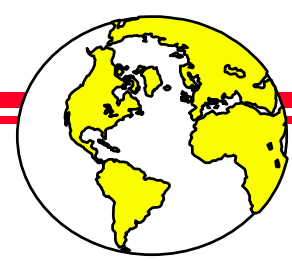
- Key to monitoring the health of the organization is the “**improvement loop**”
- ISO 9001, Clause 8.5.1
 - Continual improvement of “the effectiveness of the QMS through the use of:
 - quality policy,
 - quality objectives,
 - audit results,
 - analysis of data,
 - corrective and preventive actions and
 - management review.”



Monitoring

ISO 9001 Clause 5.6 and 14001 Clause 4.5

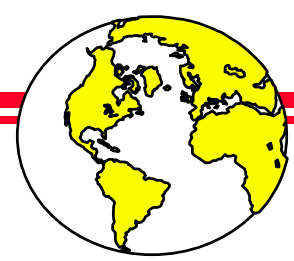
- Management Review ties Improvement Loop together
 - Top management’s responsibility to “review QMS at planned intervals, to ensure its continuing suitability, adequacy and effectiveness.”
 - Assessment of “opportunities for improvement and need for changes to the QMS, including the quality policy and quality objectives.”
- Management Review intent:
 - Top management to understand the **status** of the controls used to manage the organization



5. Control Activities

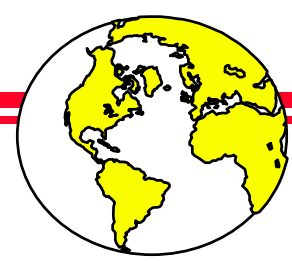
ISO 9001 Clauses 8.5.2 & 8.5.3,

- Corrective and Preventive Actions
 - Determination of causes or potential causes of nonconformities (risks),
 - Evaluate the need for action,
 - Determine and implement the actions needed
 - Review the actions taken
 - Actions taken must be recorded
- Similar ISO 14001, Clause 4.4.2



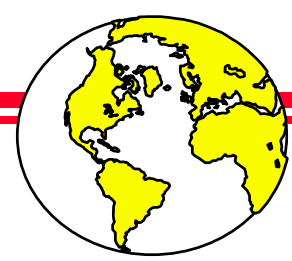
Control Activities

- Improved alignment of functions and tasks with the Organization's Objectives
- Improvement in the effectiveness & predictive nature of the controls



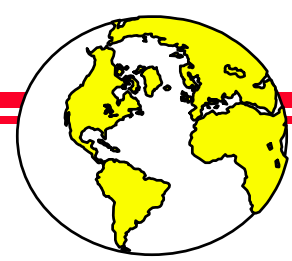
Value-Added Auditing

- Changing Internal **Financial** Auditing scope:
 - **Traditional**: evaluating internal financial controls and ensuring compliance to regulations
 - **Future**: evaluating operational effectiveness and the control and management of risks
- More effective Processes Audits are needed to evaluate the status of the organization.
- **ISO 9001** and **ISO 14001** promotes
 - Process approach and
 - Process Audits as the foundation of the new audit structure



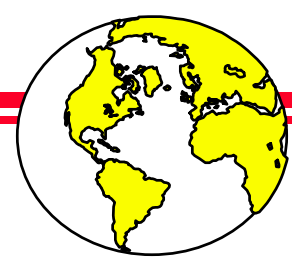
Q/E Management Systems

- ISO 9001 / ISO 14001 Schema:
 - Institutions,
 - Systems,
 - IT Infrastructure
- System Pyramid:
 - Policies,
 - Procedures,
 - Work instructions,
 - Records
 - Infrastructure



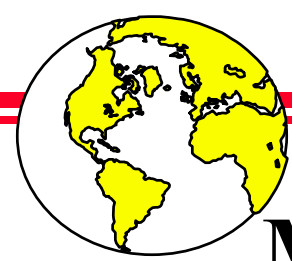
Managing Risk – the Achilles Heel of Organizational Progress

- Intrinsic relationship between the management of **quality** and the management of risks
- Enterprise Risk Management
 - COSO Enterprise Risk Mgmt Framework
 - Risk Management standard for Systems & Software Engineering
 - Consultants
 - IT systems
- Corporate Governance Quotient ratings
 - Provides guidance on publicly traded company stocks



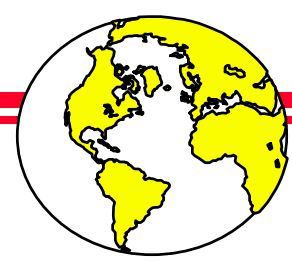
Managing Risk Methods

- Objectives, Risk, Controls, and Alignment (**ORCA**) methodology is a common organizational risk-assessment methodology. It requires that organizations:
 - Articulate organizational **OBJECTIVES**
 - Identify & Assess **RISKS** across the entire spectrum
 - Build in balanced **CONTROLS** to manage organizational risks
 - Ensure **ALIGNMENT** of objectives, risks and controls across the enterprise
- Assess the effectiveness of the business process to satisfy objectives and manage risks
 - When the organization reviews the effectiveness and makes changes in its processes, it has essentially completed the standard quality improvement technique: plan, do, check, & act (**PDCA**)



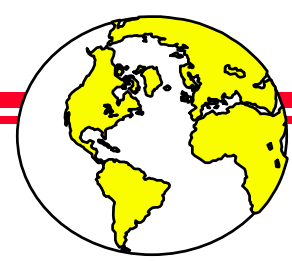
Managing Environmental Liabilities

- Corporate management generally shied away from fully investigating or disclosing potential **environmental liabilities**
- SEC invested comparatively few resources toward enforcing corporate investigations of **environmental liabilities**
- Unilateral disclosure of such **liabilities** could subject the corporation to a host of “unnecessary” responsibilities, such as
 - Required mitigatory cleanups,
 - Third party litigation,
 - Government enforcement



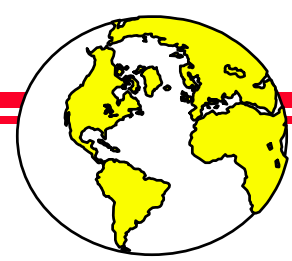
Managing Environmental Liability Disclosures Under SOX and EMS

- Companies relied on GAAP to comply with securities laws pertaining to consideration and disclosure of **environmental liabilities**
- SOX Sections 302 & 906 require corporate management to “fairly represent” a company’s financial status
 - A disclosure not limited to GAAP conformance
- EMS implementation allow companies to supplement GAAP and other internal control policies by providing a mechanism for managing **environmental risks** as well as for identifying and evaluating potential exposures to **environmental-related financial liability**
- EMS models such as ISO 14001 and 14004 function by elevating the hierarchical status of environmental, health and safety considerations within the corporate operation



Value-Added Auditing

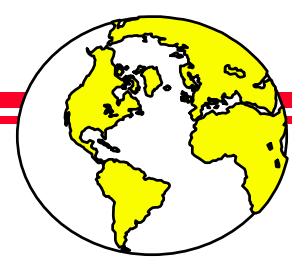
- The *Institute of Internal Auditors* (IIA) defines **value-added auditing** as
 - “a systematic, disciplined approach to evaluate and improve the effectiveness of risk management, control and governance processes.”
- IIA defines **Add Value**
 - “Value is provided by improving opportunities to achieve organizational objectives, identifying operational improvement, and/or reducing risk exposure through both assurance and consulting services.”



IT / Software Products to address the SOX requirements

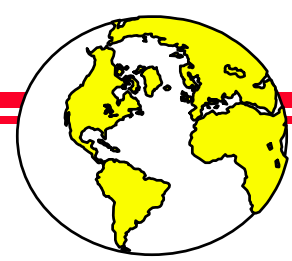
“The largest **expense** categories for most companies are IT expenditures in the capital group, and personnel costs in the expense group. Yet most companies budget by department, capture costs by department, and most projects are inherently multi-departmental. With the increased financial scrutiny, how long will external auditors sign off on the estimation of project costs without an audit trail? How long until auditors require that those costs be traceable back to individual employee timesheets?”

– Artemis International Solutions Corp



SOX Implementation

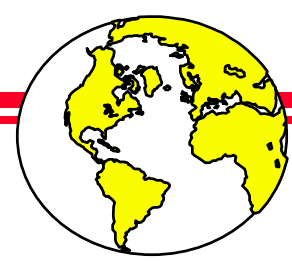
- Translate intent into improvement
- Avoid
 - bureaucracy
 - Non-value added activities
- In a global market, additional US costs must also bring advantages



SOX Implementation

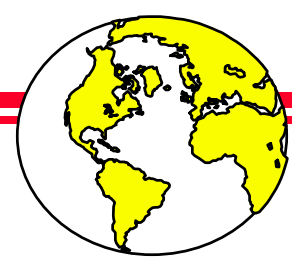
Skyrocketing prices

- Start-up investments in Section 404 compliance
 - \$480,000 average spending boost for such things as
 - Evaluation software,
 - Consulting, and
 - Worker training.
- External Financial Audits
 - New anti-fraud work alone has jacked up PwC audit fees by 15% to 20%
 - Internal-controls work the increases can be well over 50%
 - Includes auditor testing of corporate internal controls
- Information Technology (IT) has increased costs for SOX compliance
 - U.S. companies to spend more than \$2.5 billion to comply with SOX, with a significant chunk going to information technology projects



Existing Approaches To Integrating QMS/EMS With SOX Certifications/Disclosures

- Consulting firms offering SOX compliance services
 - Create or revise QMS/EMS in furtherance of SOX compliance
 - Develop individually tailored QMS/EMS procedures to address SOX requirements, by full-service reviews of:
 - companies' internal structuring,
 - culture,
 - decision-making processes,
 - practices, and
 - financial portfolios
- Information Technology / Software Products to address the SOX requirements



IT / Software Products to address the SOX requirements

- IT systems:
 - Enterprise **C**ontent Management
 - **P**ortfolio Management
 - Enterprise **P**roject Management
 - Corporate **A**uthorization Management
- Addresses SOX needs:
 - Reporting for material non-financial information
 - Information must flow from its source up through the organization on a continuous basis
 - Information must be evaluated according to defined procedures to ensure that all “material” information is brought to the attention of the officers and included in the SEC filing