



American Society For Quality -Toronto Section

“ISO 14001 & ISO 18001 Legal Compliance

Know Your Risk - Reduce your Risk”

Copyright: Coudenys Management Systems Inc.

Your Full Service Risk Management Provider

RISK DEFINED



$$\begin{aligned} &\text{Occurrence of the event} \\ &\quad \times \\ &\quad \text{Impact of the event} \\ &\quad = \\ &\quad \underline{\text{RISK}} \end{aligned}$$

RISK MANAGEMENT

Is a structured approach to Managing Uncertainty related to a threat (Risk),

a sequence of human activities including: [risk assessment](#), [strategies](#) development to manage it, and mitigation of risk using managerial resources.

POTENTIAL RISK TREATMENTS

- Once risks have been identified and assessed, all techniques to manage the risk fall into one or more of these four major categories:
- **Avoidance** (eliminate)
- **Reduction** (mitigate)
- **Transference** (outsource or insure)
- **Retention** (accept and budget)

MANAGEMENT SYSTEMS

- Risk management is simply a practice of systematically selecting cost effective approaches for minimising the effect of threat realization to the organization.
- All risks can never be fully avoided or mitigated simply because of financial and practical limitations.
- Therefore all organizations have to accept some level of residual risks.

MANAGEMENT SYSTEMS

A management system is defined as:

“A system to establish policy and objectives and to achieve those objectives

Note: A management system of an organization can include different management systems, such as a quality management system, a financial management system or an environmental management system.

ISO 9000:2005, 3.2.2

MANAGEMENT SYSTEMS

- Focus on a structured methodology that when effective identifies risk potential and deploys activities to mitigate that risk.
- Effective **Systems** Should :
 - Tell you what is working
 - Tell you what is not working
- Effective **Management System** Should through conformance of the system provide:
 - Manage the risk of what is not working
 - Improve the results of what is working

CONFORMITY VS. COMPLIANCE

Conformity:

- Fulfillment of a requirement
- Nonconformity can lead to suspension or revocation of registration
- ***Voluntary***

Compliance:

- Fulfillment of legal/statutory requirements
- Noncompliance can lead to fines/incarceration
- ***Mandatory***

MANAGEMENT SYSTEM

- Is a conformity based activity using process controls , definitions, procedures etc. that when followed can equal
 - Compliance to Regulation
 - Compliance to Customer Specifications
 - Reduced Risk
 - Increased Performance
 - Financial
 - Due Diligence

Corrective/
Preventive
Actions



Magnitude of
Risk



COMMON RISK TO EVERY COMPANY

1/ Product - Product warranty / Recall

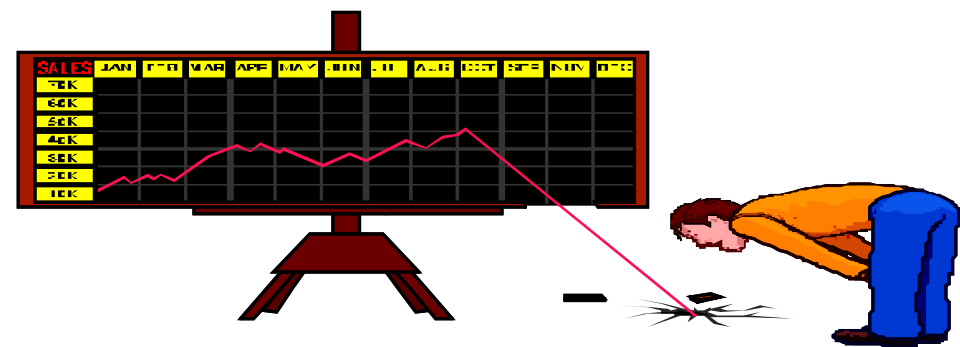
2/ People - Health & Safety

3/ Community - Environmental

4/ Legal - Compliance to Regulations

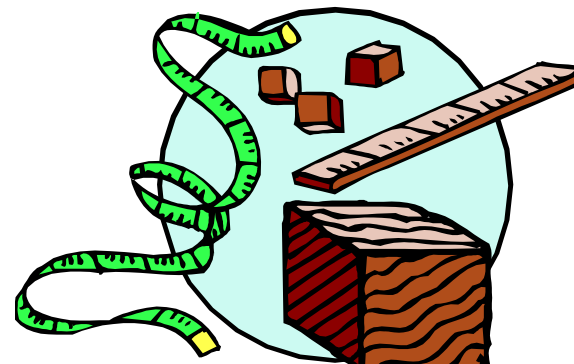
KEY ACTIVITIES

- 1/ Management Structure
 - Defines ownership, responsibility and accountability
- 2/ Documentation Structure
 - Defines requirements to control activity
- 3/ Records
 - Validates the completion of the structure
- 4/ Performance
 - Validates effectiveness of a structure



PRODUCT CONTROLS

- Supplier control
 - Risks
 - How are they controlled
 - Does the supplier have the control
- Internal
 - Process validation
 - Maintenance
 - Inspection & Test
 - Calibration



PEOPLE CONTROLS

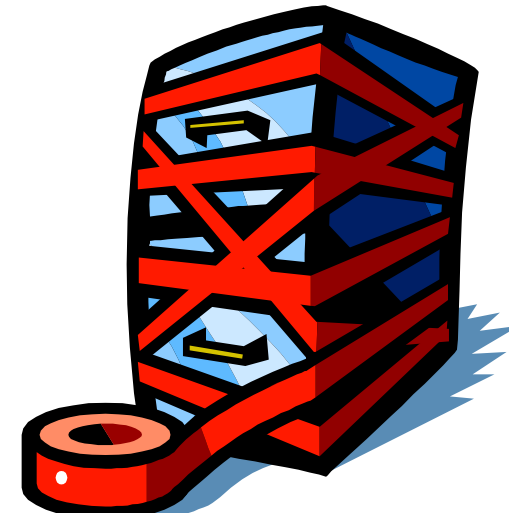
- Competence
 - Identified
 - Controlled
 - Validated
 - Managed



- Safety
 - Bill C45 -Safety related
 - Employees / Visitors / Subcontractors
- Privacy - information – records

COMMUNITY CONTROLS

- Environmental / Health & Safety Risk
 - MSDS
 - Safety
 - Spillage
 - Records reporting
 - Disposal
 - Transportation of dangerous goods
 - Contractors
- Legal Obligation & Compliance
 - Risk can be large



LEGAL CONTROLS

- Compliance to regulation
 - Didn't know – not acceptable
 - Records are key
 - No record of compliance = Non-compliance
- Effects all aspects of the company
 - Product design
 - Health & Safety
 - Environmental
- Helps manage and reduce risk!!



ISO 14001 / OHSAS 18001

- ISO 14001:2004 Focus
 - Community
 - Environmental Awareness / reduction and preservation
 - Are Children
- OHSAS 18001:2007 Focus
 - Employee
 - Accident awareness / reduction & prevention
 - Our Families

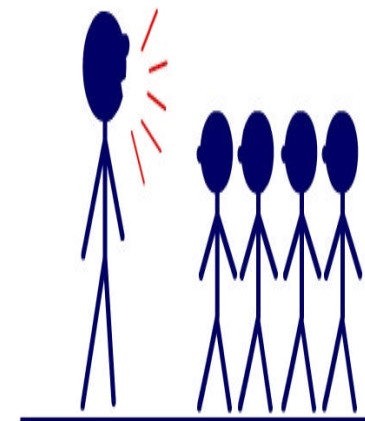
LEGAL

- Both standards have a high linkage to legal compliance and ownership
 - 4.3.2 - Legal and other requirements
 - 4.5.2 - evaluation

4.3.2 LEGAL AND OTHER REQUIREMENTS

The organization must establish a consistently used method for:

- Identifying and accessing legal and any other related requirement that it has to meet
 - Keeping information on legal and other requirements up-to-date
 - Communicating relevant information to all personnel and interested parties
- Why is this done?
 - To promote awareness and understanding of the legal and other responsibilities of the organization.



4.5.2 EVALUATION OF COMPLIANCE

The organization shall:

- Establish, implement, and maintain procedures for periodically evaluating compliance with applicable legal requirements
- Keep records of the results of the periodic evaluations



4.5.2 EVALUATION OF COMPLIANCE

- New clause within the 2004 and 2007 versions of ISO 14001 & 18001
- Broken down into 4.5.2.1 and 4.5.2.2
- 4.5.2.1 – Legal Requirements,
- 4.5.2.2 – Other Requirements.

4.5.2.1 – LEGAL REQUIREMENTS

- Consistent with commitment to compliance, the organization shall:
 - establish,
 - implement
 - maintain
 - a procedure
 - periodically evaluating compliance with applicable legal requirements.
- The organization shall keep records of the results of the periodic evaluations.

4.5.2.2 OTHER REQUIREMENTS

- The organization shall evaluate compliance with other requirements to which the organization subscribes.
- The organisation may wish to combine this with the activity in 4.5.2.1 or to establish a separate procedure.
- Organization shall keep records of the results of the periodic evaluations.

4.5.2 EVALUATION OF COMPLIANCE

- In 4.3.2, the organisation determines which legal and other requirements apply to the organisation.
- This clause requires the organisation, at a period it determines, to review the legal and other requirements and assess their compliance against the requirements.
- You must go through the legal and other requirements section by section and determine compliance.

CONFORMITY VS. COMPLIANCE

Conformity:

- Fulfillment of a requirement
- Nonconformity can lead to suspension or revocation of registration
- ***Voluntary***

Compliance:

- Fulfillment of legal/statutory requirements
- Noncompliance can lead to fines/incarceration
- ***Mandatory***

DETAIL REQUIRED

- The expected level of detail is as follows:

Regulation/Act	Requirement	Finding
OHSA Sec. 9(2) a	A joint health and safety committee is required, at a workplace at which twenty or more workers are regularly employed;	There are 25 employees, therefore JHSC is required. Objective evidence of speaking with management and workers, training and postings indicate a JHSC has been established.
OHSA Sec. 9(7)	At least half the members of a committee shall be workers employed at the workplace who do not exercise managerial functions.	There are two worker representatives.

4.5.2 EVALUATION OF COMPLIANCE

- For each legal and other requirement to which the organisation subscribes, the relevant portions need to be picked out and assessed.
- An affirmative or negative statement of compliance is not acceptable.
 - For example – we comply with the OHSA.

4.5.2 EVALUATION OF COMPLIANCE

- The person or persons who complete the evaluation must prove competence through training, education and experience.
- Records must be available for the person or persons completing this evaluation to prove the above statement.

4.5.2 EVALUATION OF COMPLIANCE

- The period for which these evaluations must be completed is not explicitly stated in the standard.
- Periodic assessments on a sampling basis may satisfy the requirement, if over time and taken together they cover all legal and other requirements over the period defined by the organization.

HOWEVER...

- With the transition period ending June 30, 2009 the organization must demonstrate a full audit of all requirements by this time.
- If this isn't demonstrated, no recommendation can be put forward – not even if you have a corrective action in place stating you know it is not done.
- Check your Conditions of Contract with Registrar.

REASON FOR CHANGE

- Focus on due diligence.
- This part of the standard is very weak and poorly done by the majority of organisations.
- Lack of understanding of requirement so it was made into a stand alone clause.
- Liability.

POSITIVES FOR HAVING A 3RD PARTY COMPLETE THE COMPLIANCE AUDIT

- 3rd party Consultants are able to make the report and subsequent findings
 - privileged/confidential and therefore restrict access.
- Outside party brings a fresh perspective.
 - Broad knowledge of environmental & Health & Safety legislation.
- Competencies
 - If report is not completed by someone with adequate knowledge,
 - it requires more work on the part of the third party auditor
 - to determine whether the report is sufficient,
 - complete and meets the requirements.
- Competence should be the determining factor when hiring a consultant
 - The registrar will be looking for when completing the audit.
 - Reduction of risk to the company

COMMON REGISTRAR REQUIREMENTS FOR EVALUATION OF COMPLIANCE

- Evaluation of Compliance
 - must be completed by a competent person, i.e. sufficient knowledge of legislation that applies to the organization.
- Person(s) completing the evaluation
 - provide a sufficient report to the organization, i.e. all media (safty, air, water etc) is covered
 - report provides enough information in order for the organization to understand issues
 - provides enough information to facilitate corrective action.
- Frequency of evaluation of compliance is defined and documented.
- Corrective actions resulting from evaluation are taken in a timely fashion and are consistent with what was found in the evaluation.
 - Focus Timely with Risk

CMSI CAN HELP YOU!!!

- Complete compliance audits
 - Analyzing your risk
 - Identifying your gaps
- Aspect / Impact review
- Hazard / Risk review
- Understanding your own risk and ways to place controls in place