RISK MANAGEMENT &
ISO 9001:2015

Greg Hutchins PE CERM
Quality + Engineering
CERM Academy
GregH@CERMAcademy.com
800.COMPETE or 503.233.1012
Who is Quality + Engineering?

Background:
Portland Oregon based Engineering company
800.COMPETE or 503.233.1012
GregH@QualityPlusEngineering.com

Greg Hutchins’s background
Certified under Safety Act for Critical Infrastructure Protection: Forensics, Assurance, Analytics®
Conduct technical, forensic, process, operational, cyber, and other operational assessments
Author of 12 books, including ISO 9000 (8 languages), Standard Manual of Quality Auditing, Supply Management Strategies
Developer of Value Added Auditing®
Author of more than 300 articles on assurance and technology
Discussion Topics

1. ISO 9001 background
2. Overall ISO 9001:2015 direction?
3. “Risk Based Thinking”
4. Risk fundamentals
5. ISO risk assessments
6. Case study – Safety Management System (SMS)
7. ISO 9001 futures
1. ISO 9001 Background

- Developed in 1987
- Most broadly accepted quality standard
  - 1.1 registered companies
  - 400K companies who use the standard
- Updated every 6 or so years
- Upcoming revision the most significant
ISO Trends

### Worldwide total of ISO 9001 - Quality Management Systems - Requirements certificates

<table>
<thead>
<tr>
<th>Year</th>
<th>2000</th>
<th>2001</th>
<th>2002</th>
<th>2003</th>
<th>2004</th>
<th>2005</th>
<th>2006</th>
<th>2007</th>
<th>2008</th>
<th>2009</th>
<th>2010</th>
<th>2011</th>
</tr>
</thead>
<tbody>
<tr>
<td>Dec</td>
<td>457,834</td>
<td>510,349</td>
<td>561,767</td>
<td>497,919</td>
<td>660,132</td>
<td>773,867</td>
<td>896,929</td>
<td>951,486</td>
<td>982,832</td>
<td>1,064,785</td>
<td>1,118,510</td>
<td>1,111,698</td>
</tr>
</tbody>
</table>

### Top 10 countries for ISO 9001 certificates (2010)

<table>
<thead>
<tr>
<th>Rank</th>
<th>Country</th>
<th>No. of certificates</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>China</td>
<td>297,037</td>
</tr>
<tr>
<td>2</td>
<td>Italy</td>
<td>138,892</td>
</tr>
<tr>
<td>3</td>
<td>Russian Federation</td>
<td>62,265</td>
</tr>
<tr>
<td>4</td>
<td>Spain</td>
<td>59,854</td>
</tr>
<tr>
<td>5</td>
<td>Japan</td>
<td>59,287</td>
</tr>
<tr>
<td>6</td>
<td>Germany</td>
<td>50,583</td>
</tr>
<tr>
<td>7</td>
<td>United Kingdom</td>
<td>44,849</td>
</tr>
<tr>
<td>8</td>
<td>India</td>
<td>33,250</td>
</tr>
<tr>
<td>9</td>
<td>United States</td>
<td>25,101</td>
</tr>
<tr>
<td>10</td>
<td>Korea, Republic of</td>
<td>24,778</td>
</tr>
</tbody>
</table>

Source: ISO Survey 2010
My ISO 9001 Journey

- Started quality for utility company in 1985
- Was involved with first TAG in 1987
- Joined one of the first NA registrars – training, etc.
- Quality consultant in 7 sectors including auto, gas, electric, etc. for 15 years
- Wrote 8 books on ISO and quality auditing = 4 others – best selling books in world in mid 1990’s
- Moved to risk in 2002
- 2005 – Critical Infrastructure Protection: Forensics, Assurance, Analytics® for homeland security
  - Cybersecurity, asymmetric war
  - Developed CERM for Dep of Homeland Security.
- 2013 developed ISO 9001:2015 risk community
  - Doubling each year
  - Currently 32 K members
- Updated ISO books for ISO 9001:2015
Greg's ISO Books

- The ISO 9000 Implementation Manual: Ten Steps to ISO 9000 Implementation
- Quality Management, Assurance, and Control
- The ISO 9000 Workbook
- Taking Care of Business
- Standard Manual of Quality Auditing
- Value Added Auditing: The Standard Manual of Risk-Based, Process Auditing
ISO 9001:2015 Development

- Development cycle:
  - Committee Draft (CD)
  - Draft International Standard (DIS)
  - Final Draft International Standard (FDIS)
  - Standard

- Final standard will be available in August/September 2015
2. Overall ISO 9001:2015 direction?

- Initial impressions are based on Committee Draft (CD)
  - Based on experience 90% of final standard is in CD
- Wow! Lots of changes in standard
- Impacts will be felt by Certification Bodies, certified companies, consultants, etc.
Overall ISO 9001 Changes

- Risk concepts is woven throughout the document
- ‘Products and Services’ replace ‘Products’
- ‘Documented Information’ replaces ‘document’ and ‘records’
  - ‘Quality Manual’ is dropped
- Process approach is required and more prescriptive including inputs, process, outputs and measures
- ‘Context of the Organization’ is added and implies a broader approach to QMS design
- ‘Management Representative’ is dropped but company needs to identify person (s) to manage QMS
Overall ISO 9001 Changes

- Quality objectives must be more specific to include who, what, where, and how
- ‘Planning of Changes’ is required
- Managing knowledge is required
- Move quality management systems to general management systems
- More process based
- Less documentation and more applicable evidence
- Emphasis on “Risk Based thinking”
3. “Risk Based Thinking”

- Risk-based thinking is automatic and often sub-conscious
- Concept of risk has always been implicit in ISO 9001 – this revision makes it more explicit and builds it into the whole management system
- Risk-based thinking is already part of the process approach
- Risk-based thinking makes preventive action part of the routine
- Risk is positive (opportunity) and negative (negative impacts)

Source: Risk Based Thinking, ISO deck, 12/2013
Importance of Risk

- Concept of “risk” in the context of ISO 9001 relates to the uncertainty in achieving these objectives.
- Provide confidence in the organization’s ability to consistently provide customers with conforming goods and services.
- Enhance customer satisfaction.
What Are ISO 9001:2015 Risk Requirements?

- in Clause 4 the organization is required to determine the risks which can affect its ability to meet these objectives
- in Clause 5 top management are required to commit to ensuring Clause 4 is followed
- in Clause 6 the organization is required to take action to address risks and opportunities
ISO 9001 Risk Requirements

- Clause 8 - the organization is required to have processes which identify and address risk in its operations
- Clause 9 the organization is required to monitor, measure, analyse and evaluate the risks and opportunities
- In Clause 10 the organization is required to improve by responding to changes in risk
ISO’s Reasons for “Risk Based Thinking?”

- Improve customer confidence and satisfaction
- Assure consistency of quality of goods and services
- Establish a proactive culture of prevention and improvement
- Successful companies intuitively take a risk-based approach
ISO: What Should You Do?

- Use a risk-driven approach in your organizational processes

  - Identify what the risks and opportunities are in your organization — it depends on context
    - ISO 9001:2015 will not automatically require you to carry out a full, formal risk assessment, or to maintain a “risk register”
    - ISO 31000 ("Risk management — Principles and guidelines") will be a useful reference (but not mandated)
Why Did ISO 9001 Add Risk?

1. Are senior executives and directors in your company spending more time on risk management?*
   (Number of responses: 205)
   - Yes, they are spending more time (117) 57%
   - No, they are spending less time (29) 14%
   - There has been no change (54) 26%
   - Unsure (5) 2%

   *Due to rounding, responses do not equal 100 percent.

2. Has your company improved the quality and timeliness of information shared with the Board to assist with decision making and better risk management?  
   (Number of responses: 264)
   - Yes, it has improved (154) 58%
   - No, it has worsened (32) 12%
   - There has been no change (70) 27%
   - Unsure (8) 3%

3. Who has direct responsibility for risk management at your company?*
   (Number of responses: 533)
   - Chief Executive Officer (227) 43%
   - Chief Operating Officer (99) 19%
   - Chief Risk Officer (108) 20%
   - Lead Director (41) 8%
   - Other (58) 11%

   *Due to rounding, responses do not equal 100 percent.
Certification Bodies Are Now Risk Bodies

- **BSI**
  - BSI wants to move their entire marketing to supply chain risk management

- **DNV**
  - Tag Line: Managing Risk
  - Redesign service offerings around Risk Management

- **LRQA**
  - Rebranding to new assurance services
  - Workshops (Food Safety, SCM, etc.)

- **ABS**
  - Free Webinar

- **Lloyd's Register**
  - Aerospace Risk Mgmt.
  - Managing Risk throughout the supply chain.
4. Risk Fundamentals

- **Risk** – Chance of something happening that will have an impact upon objectives. It is measured in terms of consequences and likelihood. (AS/NZA 4360, 1999, Risk Management)

- **Risk** – Situation or circumstance, which creates uncertainties about achieving program objectives. (FAA Programmatic Risk Management, 2002.)

- **Risk** – Possibility that an event will occur and adversely affect the achievement of objectives. (COSO, Enterprise Risk Management Framework, web, 2003.)


Example:
- Project Risk – Measure of the inability to achieve project objectives within cost, schedule, and quality constraints.
What Is a Risk Framework?

- A framework is a **structure** upon which to build **strategy**, reach **objectives** and monitor **performance**.

- A framework is a set of **controls** and/or **guidance** organized in categories, focused on a particular topic.
Common Frameworks

Mandate and commitment (4.2)

Design of framework for managing risk (4.3)
- Understanding the organization and its context (4.3.1)
- Establishing risk management policy (4.3.2)
- Accountability (4.3.3)
- Integration into organizational processes (4.3.4)
- Resources (4.3.5)
- Establishing internal communication and reporting mechanisms (4.3.6)
- Establishing external communication and reporting mechanisms (4.3.7)

Continual improvement of the framework (4.6)

Implementing risk management (4.4)
- Implementing the framework for managing risk (4.4.1)
- Implementing the risk management process (4.4.2)

Monitoring and review of the framework (4.5)
Risk Capability Maturity Model

Risk Management CMM†

- **Ad Hoc**: Overarching risk management philosophy or objectives are not defined
- **Fragmented**: Risk Management functions independently within business units
- **Comprehensive**: Risk Management is enterprise-wide and encompasses all risk types
- **Integrated**: Risks are treated as a portfolio at the enterprise level and are correlated and aggregated across risk types and business units
- **Strategic**: Risk Management is built into decision making. The organization selectively seizes opportunity because of its special ability to exploit risks

† Adapted from the Capability Maturity Model framework developed by Carnegie Mellon University
Types of Operational Risks

- **Enterprise risk – Governance** - Risk related to the operation of a business, execution strategy, systemic issues, material issues, etc.

- **Project risk** – ERM - Risk related to the planning and delivery of a product or service and not being able to meet project ‘triple constraints’ – scope/quality, schedule, cost including technology others.

- **Process risk – Compliance/Assurance** - Risk relating directly to planning and delivery of a product or service and not being able to meet 1. stability, 2. capability, 3. improvement; inability to achieve consistent outcomes.
5. ISO Risk Assessments

A. Objective – Risk – Controls – Assurance
B. Failure Modes and Effects Analysis
A. ORCA Approach

<table>
<thead>
<tr>
<th>Type of Risk</th>
<th>Level of Risk</th>
<th>Objective</th>
<th>Risk Number</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>[Image of risk matrix]</td>
<td></td>
</tr>
</tbody>
</table>

- **Objective**: Operations - Project Management Controls

- **Level/Priority**: Enterprise, Division/Process/Program, Transactional

- **Process/Program/Project Owner**: Dave Wright

- **Risk Description**: Project management controls reflecting the size and complexity of the projects managed by engineering are lacking.

- **Risk Points**: 20

- **Risk Matrix**: [Image of risk matrix grid]

- **Legend**:
  - P = People
  - PR = Process
  - T = Technology
High Level Severity Matrix

Severity of Impact

<table>
<thead>
<tr>
<th>Likelihood</th>
<th>Negligible</th>
<th>Marginal</th>
<th>Serious</th>
<th>Critical</th>
<th>Catastrophic</th>
</tr>
</thead>
<tbody>
<tr>
<td>Highly Probable</td>
<td></td>
<td></td>
<td></td>
<td>Pending legislation adds 2 days to on-dock time</td>
<td>Non-ISO verified vendors</td>
</tr>
<tr>
<td>Probable</td>
<td>Nationalization of MRO supplier</td>
<td>Non-ISO certified vendors</td>
<td>Critical component lost shipments</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Occasional</td>
<td>Key component delivery late 26%</td>
<td>Sole source vendor in tornado alley</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Remote</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Improbable</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
B. FMEA Approach

- **FMEA**: Systematic method and a documented process to: recognize, evaluate, and prioritize potential failures and their effects. Identify the actions which could eliminate or reduce the chance of potential failure occurring.

- **Process FMEA**: Process to: identify potential failure modes and rate the severity of their effects; rank order of potential deficiencies; focus on prevention; mitigate risk before it stops you.

- **Failure modes**: Way in which the systems, process, component, subassembly or product could fail to perform its intended function. Failure modes may be the result of upstream operations or may cause downstream operations to fail.

- **Failure effects**: Outcome of the occurrence of the failure mode on the system, product, or process. The “IMPACT” on the customer.

Source: Keith Ridgeway
### FMEA Example

#### Process/Product Failure Modes and Effects Analysis (FMEA)

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>What is the process step/function under investigation?</td>
<td>Is what the process step/function potentially fail to meet process requirements or intent?</td>
<td>What is the impact on the Key Output Variables (Customer Requirements) or internal requirements?</td>
<td>How often is the defect experienced by the customer?</td>
<td>What are the causes of this Failure Mode? Typical failure cause result from process inputs.</td>
<td>What are the existing controls and procedures (inspection and test) that prevent the cause or the Failure Mode? Should include an SOP number.</td>
<td>What are the actions for reducing the occurrence of the Cause, or improving detection? Should have actions only on high RPM's or easy fixes.</td>
<td>Whose responsible for the recommended action?</td>
<td>What are the completed actions taken with the recalculated RP? Be sure to include completion month/year</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Identify output failures and impacts**

**Assess inputs**

**Prioritize**

**Determine actions and impact**
Types of FMEA’s

- **Strategic** - used to develop contingency plans for new business or operating strategies. Focuses on risk elements including: markets; competition; technology; Health, Safety and Environmental System

- **System** - used to analyze systems and sub-systems in the early concept and design stages. Focuses on potential failure modes associated with the functions of a system caused by the design.

- **Process** - used to analyze our operations. Focuses on process steps and inputs.

- **Design** - used to analyze product designs before they are released to production. Focuses on product function.

- **Defects** - used to error proof processes. Focuses on process steps and errors.
When to Use FMEA’s

- Early in the process improvement investigation, after a process map has been developed.
- When new systems, processes and products are being designed.
- When existing designs or processes are being changed.
- When carry-over designs are used in new applications.
- After system, product, or process inputs and outputs functions have been defined, but before specific hardware is selected or released to manufacturing (ideally).

Source: Keith Ridgeway
FMEA Examples

- **Design:** A designer needs to design a brake pad for a new caliper assembly. How do we identify the effect the new brake pad will have on the caliper assembly?

- **New Manufacturing:** A new lifting machine with improved capability is going to be added to the final assembly. What effect will this have?

- **Process:** A customer has added a requirement for particulate air test to be carried out. How do we plan to measure and control it?

- **Logistics:** A logistics manager needs to determine how a new kanban process will impact the movement of parts to line side storage and buffer stock. How would he know what factors to identify that would impact customer deliveries?

- **Administrative:** A HR manager needs to determine how a change from a weekly payment to monthly payment will have an impact on contract staff. How would he know what factors to identify?

Source: Keith Ridgeway
6. Case study – Safety Management System (SMS)

- **What is SMS?**
  - “Safety Management System (SMS) is becoming a standard throughout the aviation industry worldwide.”
  - Regulatory and global – 191 countries

- **What does it do?**
  - A structured means of safety risk management decision making
  - A means of demonstrating safety management capability before system failures occur
  - Increased confidence in risk controls though structured safety assurance processes
  - An effective interface for knowledge sharing between regulator and certificate holders
  - A safety promotion framework to support a sound safety culture

Source: FAA website
### Scope of SMS

<table>
<thead>
<tr>
<th>Category</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Air Operator, MRO, Training Organization</td>
<td>Air Carriers, Air Taxi, Air Tour, Maintenance under 121, Repair Stations, Non-Certificated Repair Facilities, Flight Schools, Simulator Facilities, etc. (FAA Oversight by Flight Standards)</td>
</tr>
<tr>
<td>Design and Manufacturing Organizations</td>
<td>Design Approval Holders, Suppliers, Production Certificate Holders, PMA, TC Holders Producing under TC (FAA Oversight by; Aircraft Certification, Manufacturing Inspection District Offices (MIDO), Aircraft Engineering Group (AEG))</td>
</tr>
<tr>
<td>Airports</td>
<td>Airports</td>
</tr>
<tr>
<td>Air Traffic</td>
<td>Air Navigation, Airway Facilities</td>
</tr>
<tr>
<td>The Regulator</td>
<td>Information for FAA offices and employees that have oversight responsibility for the aviation sectors above</td>
</tr>
</tbody>
</table>
SMS Impacts

- Sector quality standards will incorporate 1. Risk based, problem solving and 2. Risk based, decision making
- Integration of risk management and quality management
- New risk language, metrics for risk management, risk assurance, risk auditing, etc.
- Increased changes in sectoral standards such as AS 9100
7. Quality Futures

Challenge/Risk is growing complexity.

Program/Project Complexity

GAPS:
- Greater variances
- Cost
- Schedule
- Scope
- Technology
- Quality

Existing Processes

Time +

Quality is largely based on horizontal line.
Processes are stable and capable of meeting requirements.
SEC Risk Reporting Requirements

1. Inadequate disclosure issues
2. Market for products and services
3. Reliance on suppliers, customers, governments
4. Going concern
5. Effects of regulatory changes
6. Legal exposures and reliance on legal positions
7. Ineffective internal or disclosure controls
8. Reliance on certain employees
9. Conflicts of interest/related party issues
10. History of operating losses

SEC Top 10 Risks, CFO Magazine, Nov, 2010
Board Reporting on Quality Risk
Our Solution:

Certified Enterprise Risk Manager®

- Enterprise Risk Management (COSO)
- Risk Assurance (GAGAS)
- Project Risk Management (ISO 31k)
THANK YOU FOR YOUR TIME

QUESTIONS?