Got Risk? Developing a Risk Management Foundation for a QMS

Carl Johansen & Ian Sheridan

Session W19 – Wednesday, May 2, 2018
Topics of Discussion

- What is Quality Management?
  - Terms & Definitions
  - Quality management system (QMS) design process

- Risk Requirements and QMS Context
  - ISO 9001:2015 requirements
  - Siloed vs Integrated Management System Framework

- Capability and Implementation Strategy Development
  - System strategy development using risk tools & techniques
  - Hybrid capability & maturity self-assessment

- Self-Assessment, Control Testing, Communication
  - GRC application (Archer) implementation
  - Performance dashboard application (Tableau)
Quality Management System

The scientific approach to managing defined expectations of business programs and processes built on a foundation of comprehensive risk management, in the pursuit of operational excellence.

Con Edison
www.ConEd.com
“Each and every employee can see the flow of value to the customer, and fix that flow before it breaks down”

Institute for Operational Excellence
www.instituteopex.org
Lean Management

“A non-zero-sum principle-based management system focused on creating value for customers and eliminating waste, unevenness, and unreasonableness using the scientific method”

Dr. M.L. “Bob” Emiliani
www.bobemiliani.com
QMS Design Process

- **Context**: Understand:
  - Management system framework,
  - Compliance obligations, and
  - Business objectives

- **Capability**: Determine capability to achieve:
  - Conformance obligations,
  - Compliance obligations, and
  - Business objectives

- **Execution & Maintenance**: Evaluate and implement:
  - Risk and control process, and
  - Controls testing process
Focus on continual improvement of:
  - Business processes, and
  - Controls
QMS Design Process

Context

Understand:
- Management system framework,
- Compliance obligations, and
- Business objectives

Capability

Determine capability to achieve:
- Conformance obligations,
- Compliance obligations, and
- Business objectives

Execution & Maintenance

Evaluate and implement:
- Risk and control process, and
- Controls testing process

Focus on continual improvement of:
- Business processes, and
- Controls
When planning for the quality management system, the organization shall consider the issues in (4.1) and requirements in (4.2)
Then, shall determine threats and opportunities that need to be addressed to give assurance that system can achieve intended results and achieve improvement (6.1.1)
The organization shall plan actions to address threats and opportunities and how to integrate and implement actions into its quality system processes (4.4)
The organization shall maintain documented information of its processes and retain documentation to have confidence that processes are being carried out as planned (4.4.2)
Putting the Risk Puzzle Together

1. Shall establish, implement and maintain process(es)

2. Shall determine threats and opportunities of QMS

3. Shall plan, integrate and implement actions into QMS & other business processes

4. Shall maintain documented information
Siloed System Framework

Business objectives and compliance obligations

ISO 19600 Compliance Management

ISO 50001 Energy Management

SA 8000 Social Accountability

API 1173 Pipeline Safety

ISO 22301 Business Continuity

ISO 55001 Asset Management

ISO 14001 Environmental

ISO 45001 Health and Safety

ISO 9001 Quality Management

ISO 50001
Energy Management

ISO 14001
Environmental

ISO 9001
Quality Management

ISO 55001
Asset Management

ISO 45001
Health and Safety

API 1173
Pipeline Safety

SA 8000
Social Accountability

ISO 22301
Business Continuity

ISO 19600
Compliance Management
Integrated Systems Framework

ISO 9001 Quality Management Systems

- ISO 19600 Compliance Management
- ISO 14001 Environmental
- ISO 22301 Business Continuity
- ISO 50001 Energy Management
- ISO 55001 Asset Management
- SA 8000 Social Accountability
- ISO 45001 Health and Safety
- API 1173 Pipeline Safety

Business objectives and compliance obligations
Risk Portfolio?

An accurate and exhaustive list of an organization's risk organized in either a matrix or multiple matrices by risk topic or predefined categories.
QMS Risk Matrix

• QMS Aptitude Assessment
  ▪ Assurance that system can achieve objectives (6.1.1)

• Organizational Aspect Assessment
  ▪ Compliance obligations (4.2)
  ▪ Internal issues (4.1)
  ▪ External issues (4.1)
  ▪ Environmental conditions (4.1)
  ▪ Interested parties (4.2)
QMS Applicable Standards

- Committee of Sponsoring Organizations of the Treadway Commission (COSO)
  - June 2017 *Enterprise Risk Management, Integrating with Strategy and Performance*

- Open Compliance and Ethics Group (OCEG)
  - GRC Capability Model v.3 (Red Book)
  - GRC Assessment Tools v.3 (Burgundy Book)

- ISO
  - 9001:2015, *Quality management systems - Requirements*
  - 9004:2009, *Managing for the sustained success of an organization – A quality management approach*
  - 9004:2018, *Quality management – Quality of an organization – Guidance to achieve sustained success*
  - 31000:2009, *Risk management – Principles and guidelines*
QMS Design Process

Context

Understand:
- Management system framework,
- Compliance obligations, and
- Business objectives

Capability

Determine capability to achieve:
- Conformance obligations,
- Compliance obligations, and
- Business objectives

Execution & Maintenance

Evaluate and implement:
- Risk and control process, and
- Controls testing process

Focus on continual improvement of:
- Business processes, and
- Controls
What is COSO?

“joint initiative dedicated to providing thought leadership through the development of frameworks and guidance on enterprise risk management, internal control and fraud deterrence”

Committee of Sponsoring Organizations of the Treadway Commission (COSO)
www.coso.org
What is COSO?

• All about developing frameworks and guidance on:
  - Enterprise risk management (ERM)
  - Internal control
  - Fraud deterrence

• 2017 ERM framework update
  - Highlights importance of risk in both strategy-setting process and driving performance
  - Set of Principles across five interrelated components
    - Governance and culture
    - Strategy and Objective-Setting
    - Performance
    - Review and Revision
    - Information, Communication, and Reporting
What is GRC?

“GRC is the integrated collection of capabilities that enable an organization to reliably achieve objectives, address uncertainty and act with integrity”

Open Compliance and Ethics Group (OCEG)
www.oceg.org
What is GRC?

• Was an acronym of:
  - Governance, Risk, and Compliance

• Now about integrating business functions and assessing the capability of each to achieve Principled Performance
  - G.R.A.C.E.-IT is set of Elements across six functions
    - Governance and strategy
    - Risk management
    - Auditing
    - Compliance management (including legal)
    - Ethics and culture
    - Information Technology and Security
OCEG GRC Capability Model

Learn
- External Context
- Internal Context
- Culture
- Stakeholders

Align
- Direction
- Objectives
- Identification
- Assessment
- Design

Perform
- Controls
- Policies
- Communication
- Education
- Incentives
- Notification
- Inquiry
- Response

Review
- Monitoring
- Assurance
- Improvement

ASQ
What is ISO 9004?

“while ISO 9001:2015 focuses on providing confidence in an organization’s products and services, (9004:2018) focuses on providing confidence in the organization’s ability to achieve sustained success”

International Organization for Standardization (ISO)
www.iso.org
What is ISO 9004?

- Guidance to achieve sustained success
  - Set of abilities across seven Clauses
    - Context
    - Identity
    - Leadership
    - Process management
    - Resource management
    - Performance
    - Improvement, learning, and innovation
## ISO 9004 Maturity Model (Annex A)

<table>
<thead>
<tr>
<th>Key element</th>
<th>Maturity level towards sustained success</th>
<th>Level 1</th>
<th>Level 2</th>
<th>Level 3</th>
<th>Level 4</th>
<th>Level 5</th>
</tr>
</thead>
<tbody>
<tr>
<td>Element 1</td>
<td>Criteria 1</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Criteria 1</td>
</tr>
<tr>
<td></td>
<td>Base level</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Best practice</td>
</tr>
<tr>
<td>Element 2</td>
<td>Criteria 2</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Criteria 2</td>
</tr>
<tr>
<td></td>
<td>Base level</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Best practice</td>
</tr>
<tr>
<td>Element 3</td>
<td>Criteria 3</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Criteria 3</td>
</tr>
<tr>
<td></td>
<td>Base level</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Best practice</td>
</tr>
</tbody>
</table>
QMS Aptitude Model Basics

• 33 Characteristics
  ▪ Hybrid of all 33 ISO Elements, 20 COSO Principles, and 20 OCEG Elements

• Seven Focal Areas
  ▪ Context
  ▪ Purpose and Culture
  ▪ Governance and Leadership
  ▪ Process Management
  ▪ Resource Management
  ▪ Risk and Compliance Management
  ▪ Improvement and Innovation
QMS Aptitude Model Maturity

• Five Maturity Levels
  § Level 1 – Informal activities
    - Baseline activities are in place to manage quality and risk but are isolated and fragmented
  § Level 2 – Defined functions
    - Quality and risk functions focused on improving effectiveness are underway to stabilize processes
  § Level 3 – Managed and effective functions
    - Quality and risk functions have evolved into a steady state and are now effective, repeatable, and sustainable
  § Level 4 – Coordinated business functions
    - Transformative initiatives are executed to correlate business objectives with effective, repeatable, and sustainable quality and risk management functions
  § Level 5 – Advantaged enterprise environment
    - Enterprise functions are optimized and balanced by business context, quality, and risk priorities
Self-Assessment & Gap Analysis

• Does our system have the aptitude to achieve our;
  ▪ Business objectives,
  ▪ Compliance obligations, and
  ▪ Conformance obligations?

• If not, develop a plan to address gaps
QMS Design Process

Context

Understand:
• Management system framework,
• Compliance obligations, and
• Business objectives

Capability

Determine capability to achieve:
• Conformance obligations, 
• Compliance obligations, and 
• Business objectives

Execution & Maintenance

Evaluate and implement:
• Risk and control process, and 
• Controls testing process

Focus on continual improvement of:
• Business processes, and
• Controls
Risk Tool Box

A modified process failure mode and effects analysis (PFMEA) allows an organization to prioritize its QMS risk based on business bias and risk appetite
PFMEA Risk Tool

• Process Failure Mode Effects Analysis
  ▪ Well understood concept
  ▪ Risk Priority Number (RPN) concept - SxOxD
  ▪ Ability to define & determine criteria
  ▪ Ability to quantify for ranking
Organizational Aspect

“an organizational input from internal or external issues, environmental conditions, compliance obligations, or interested parties (4.1 & 4.2) that affects or can affect the organization's intended outcome of its quality management system"
Organizational Aspect Assessment

Operational Impact x ERM x Regulation Impact

- Operational Impact
  - Insignificant (2) – Catastrophic (10)

- Enterprise Risk Management (ERM)
  - ERM score = sum of all aspects affected if risk event occurs

- Regulation Impact
  - Aspect associated with any regulations?
    - Yes = 2 No = 1
QMS Risk Matrix Results

• QMS Aptitude Assessment
  ▪ Initial maturity; “Where we are”
  ▪ Desired maturity; “Where we want to be”

• Operational Aspect Assessment
  ▪ 65 operational aspects determined
  ▪ Five Key Aspects determined (high risk)
    - Highest RPN for each of the five inputs
## Context Example

<table>
<thead>
<tr>
<th>Model Framework</th>
<th>Characteristics</th>
<th>Maturity Level</th>
<th>CON1 - Enterprise Process Comprehension</th>
<th>CON2 - Relevant interested parties</th>
<th>CON3 - External and internal issues</th>
<th>CON4 - Self-assessment</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td>5</td>
<td>X</td>
<td>4</td>
<td>2</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>0.25</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Advantaged</td>
<td>Processes and the interactions with relevant interested parties are determined and used as inputs into process determination</td>
<td>Level 5</td>
<td>Process and the interactions with relevant interested parties are fully aligned to the organization's mission and values and are determined and aligned to the organization's mission and values.</td>
<td>Process and the interactions with relevant interested parties are determined and used as inputs into process determination. The needs and expectations of all relevant interested parties are addressed, including their importance and relevance.</td>
<td>Process and the interactions with relevant interested parties are determined and used as inputs into process determination. The needs and expectations of all relevant interested parties are addressed, including their importance and relevance.</td>
<td>Process and the interactions with relevant interested parties are determined and used as inputs into process determination. The needs and expectations of all relevant interested parties are addressed, including their importance and relevance.</td>
</tr>
<tr>
<td>Coordinated</td>
<td>Processes and their interactions are systematically determined to ensure continuous support and the organization's sustainability and success.</td>
<td>Level 4</td>
<td>Processes and their interactions are systematically determined to ensure continuous support and the organization's sustainability and success.</td>
<td>Processes and their interactions are systematically determined to ensure continuous support and the organization's sustainability and success.</td>
<td>Processes and their interactions are systematically determined to ensure continuous support and the organization's sustainability and success.</td>
<td>Processes and their interactions are systematically determined to ensure continuous support and the organization's sustainability and success.</td>
</tr>
<tr>
<td>Managed</td>
<td>Influential factors relating to the organization's performance are determined and used in process determination.</td>
<td>Level 3</td>
<td>Influential factors relating to the organization's performance are determined and used in process determination.</td>
<td>Influential factors relating to the organization's performance are determined and used in process determination.</td>
<td>Influential factors relating to the organization's performance are determined and used in process determination.</td>
<td>Influential factors relating to the organization's performance are determined and used in process determination.</td>
</tr>
<tr>
<td>Defined</td>
<td>Key processes, such as those related to critical business factors, are determined. Interactions between processes are well determined.</td>
<td>Level 2</td>
<td>Key processes, such as those relating to the needs and expectations of relevant interested parties, are determined. Interactions between processes are well determined.</td>
<td>Key processes, such as those relating to the needs and expectations of relevant interested parties, are determined. Interactions between processes are well determined.</td>
<td>Key processes, such as those relating to the needs and expectations of relevant interested parties, are determined. Interactions between processes are well determined.</td>
<td>Key processes, such as those relating to the needs and expectations of relevant interested parties, are determined. Interactions between processes are well determined.</td>
</tr>
<tr>
<td>Informal</td>
<td>Processes for determining relevant interested parties are not determined or consistent.</td>
<td>Level 1</td>
<td>Processes for determining relevant interested parties are not determined or consistent.</td>
<td>Processes for determining relevant interested parties are not determined or consistent.</td>
<td>Processes for determining relevant interested parties are not determined or consistent.</td>
<td>Processes for determining relevant interested parties are not determined or consistent.</td>
</tr>
</tbody>
</table>

### Model Framework

- **CON1 - Enterprise Process Comprehension**
  - Maturity Level: 5 (Level 5)
  - Description: Processes and the interactions with relevant interested parties are fully aligned to the organization's mission and values and are determined and aligned to the organization's mission and values.

- **CON2 - Relevant interested parties**
  - Maturity Level: 0.25 (Level 5)
  - Description: The needs and expectations of all relevant interested parties are addressed, including their importance and relevance.

- **CON3 - External and internal issues**
  - Maturity Level: 4 (Level 4)
  - Description: Influential factors relating to the organization's performance are determined and used in process determination.

- **CON4 - Self-assessment**
  - Maturity Level: 2 (Level 2)
  - Description: Key processes, such as those related to critical business factors, are determined. Interactions between processes are well determined.
## QMS Aptitude Model Scorecard

<table>
<thead>
<tr>
<th>Focal Area Legend</th>
<th>&gt;= 80%</th>
<th>&gt;=60% &lt;79%</th>
<th>&gt;=30% &lt;59%</th>
<th>&lt;=29%</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Level achieved or exceeded</td>
<td>Major progress</td>
<td>Some progress</td>
<td>Little to no progress</td>
</tr>
</tbody>
</table>

### Model Framework

<table>
<thead>
<tr>
<th>Maturity Level</th>
<th>Context</th>
<th>Purpose and Culture</th>
<th>Governance and Leadership</th>
<th>Process Management</th>
<th>Risk and Compliance Management</th>
<th>Improvement and Innovation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Advantaged</td>
<td>0.25</td>
<td>0.20</td>
<td>0.20</td>
<td>0.40</td>
<td>0.20</td>
<td>0.00</td>
</tr>
<tr>
<td>Coordinated</td>
<td>0.50</td>
<td>0.50</td>
<td>0.40</td>
<td>0.60</td>
<td>0.40</td>
<td>0.40</td>
</tr>
<tr>
<td>Managed</td>
<td>0.75</td>
<td>0.75</td>
<td>0.80</td>
<td>1.00</td>
<td>1.00</td>
<td>1.00</td>
</tr>
<tr>
<td>Defined</td>
<td>1.00</td>
<td>1.00</td>
<td>1.00</td>
<td>1.00</td>
<td>1.00</td>
<td>1.00</td>
</tr>
<tr>
<td>Informal</td>
<td>1.00</td>
<td>1.00</td>
<td>1.00</td>
<td>1.00</td>
<td>1.00</td>
<td>1.00</td>
</tr>
</tbody>
</table>

### Focal Area Legend

- **Little to no progress**
- **Some progress**
- **Major progress**
- **Level achieved or exceeded**
Organizational Aspect Example

“Failure of contractor employees to follow company policies & procedures (Threat)”

• Rank
  ▪ One

• Context of Organization Input
  ▪ Internal Issues

• Aspect Significance Score
  ▪ $8 \times 4,712 \times 2 = 75,392$
QMS Aptitude Continual Monitoring

• Enterprise GRC application
  ▪ RSA Archer
    – Track compliance obligations & risk register
    – Maintain QC/QA review results & corrective actions

• Interactive data visualization application
  ▪ Tableau
    – Present QMS aptitude assessment results
Questions?

Carl Johansen
Section Manager, Utility Shared Services Quality Management
Con Edison
johansenc@coned.com

Ian Sheridan
Project Specialist, Utility Shared Services Quality Management
Con Edison
sheridani@coned.com