# Got Risk? Developing a Risk Management Foundation for a QMS

Carl Johansen & Ian Sheridan

Session W19 – Wednesday, May 2, 2018

ASQ
The Global Voice of Quality

# 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)

ASQ

# 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**

ASQ

# Operational Excellence

"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**

ASQ

# Lean Management

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

**Dr. M.L. "Bob" Emiliani**
**www.bobemiliani.com**

ASQ

# 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

ASQ

# 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

ASQ

# ISO 9001 Risk Requirement – Part 1

When planning for the quality management system, the organization shall consider the issues in (4.1) and requirements in (4.2)

# ISO 9001 Risk Requirement – Part 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)

ASQ

# ISO 9001 Risk Requirement – Part 3

The organization shall plan actions to address threats and opportunities and how to integrate and implement actions into its quality system processes (4.4)

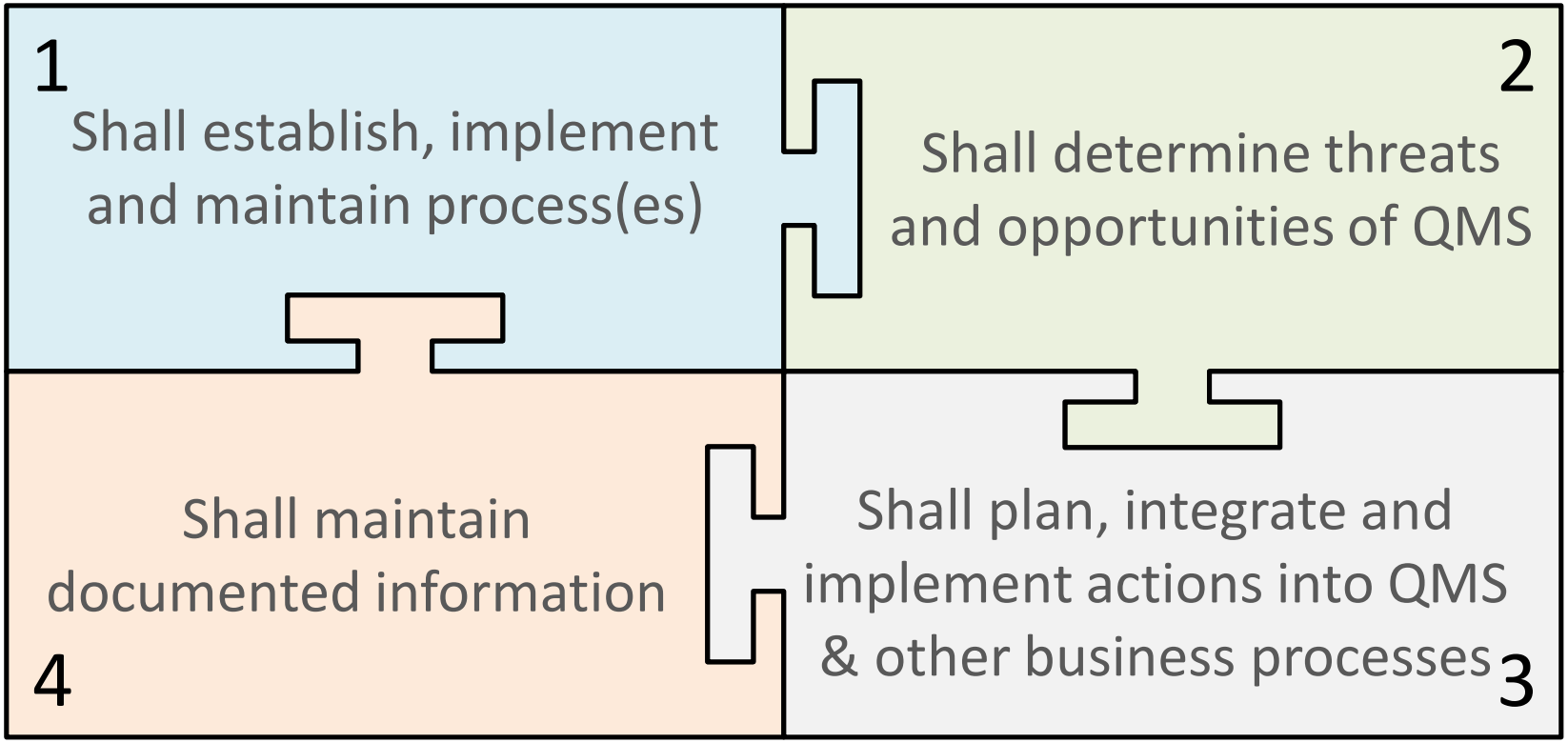
ASQ

# ISO 9001 Risk Requirement – Part 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)

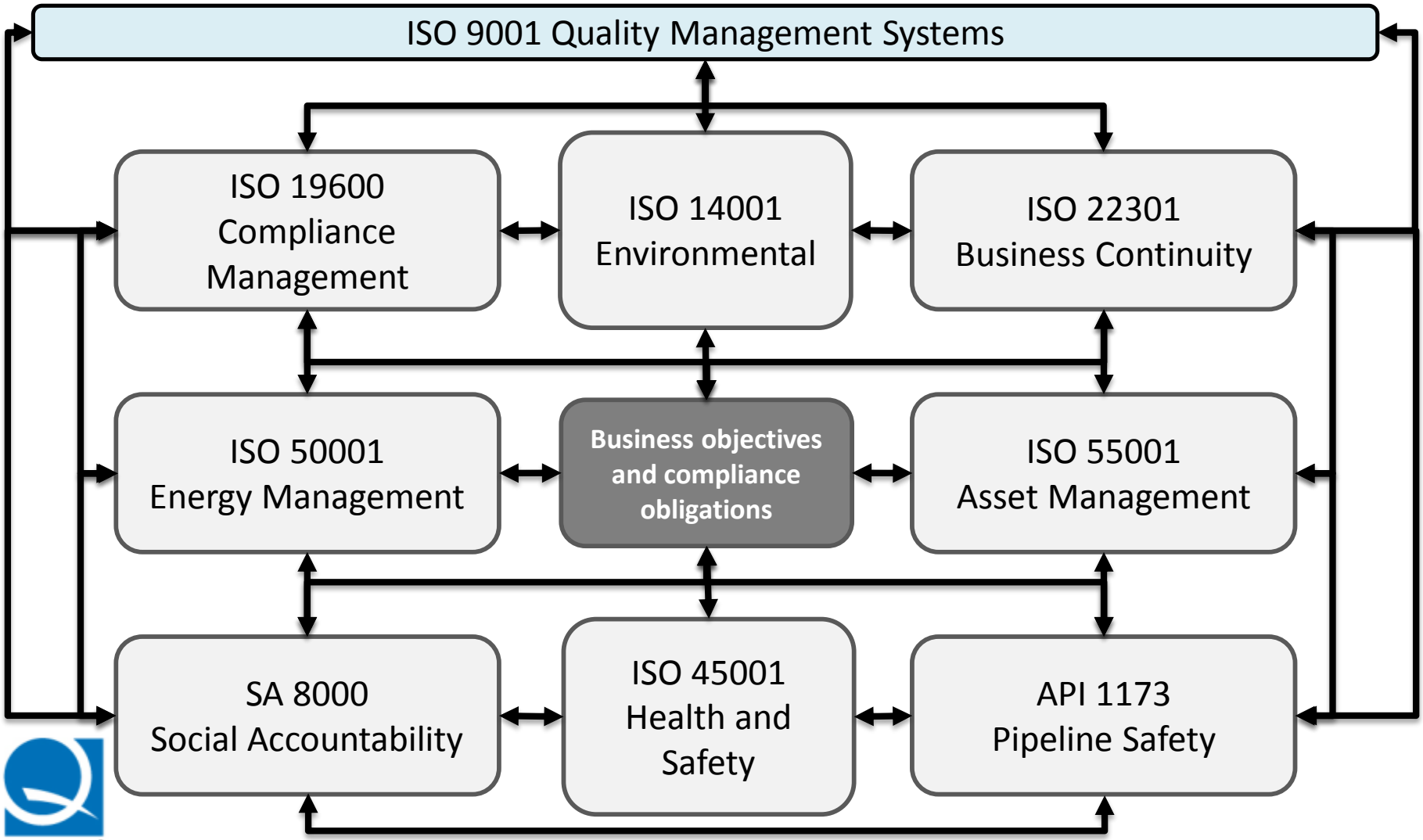
ASQ

# Putting the Risk Puzzle Together



# Siloed System Framework

# Integrated Systems Framework




ASQ

# Risk Portfolio?

An accurate and exhaustive list of an organizations risk organized in either a matrix or multiple matrices by risk topic or predefined categories.

ASQ

# 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)

ASQ

# 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***
  - 13053-2:2011, *Quantitative methods in process improvement – Six Sigma – Part 2: Tools and techniques*
  - 31000:2009, *Risk management – Principles and guidelines*
  - **31000:2018, *Risk management - Guidelines***
  - 31010:2009, *Risk management – Risk management techniques*
  - ISO/TR 31004:2013, *Risk management – Guidance for the implementation of ISO 31000*

ASQ

# 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

ASQ

# 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**

ASQ

# 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

ASQ

# COSO ERM Framework

ENTERPRISE RISK MANAGEMENT


**Governance & Culture**

1. Exercises Board Risk Oversight
2. Establishes Operating Structures
3. Defines Desired Culture
4. Demonstrates Commitment to Core Values
5. Attracts, Develops, and Retains Capable Individuals

**Strategy & Objective-Setting**

6. Analyzes Business Context
7. Defines Risk Appetite
8. Evaluates Alternative Strategies
9. Formulates Business Objectives

**Performance**

10. Identifies Risk
11. Assesses Severity of Risk
12. Prioritizes Risks
13. Implements Risk Responses
14. Develops Portfolio View

**Review & Revision**

15. Assesses Substantial Change
16. Reviews Risk and Performance
17. Pursues Improvement in Enterprise Risk Management

**Information, Communication, & Reporting**

18. Leverages Information and Technology
19. Communicates Risk Information
20. Reports on Risk, Culture, and Performance

ASQ

# 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**

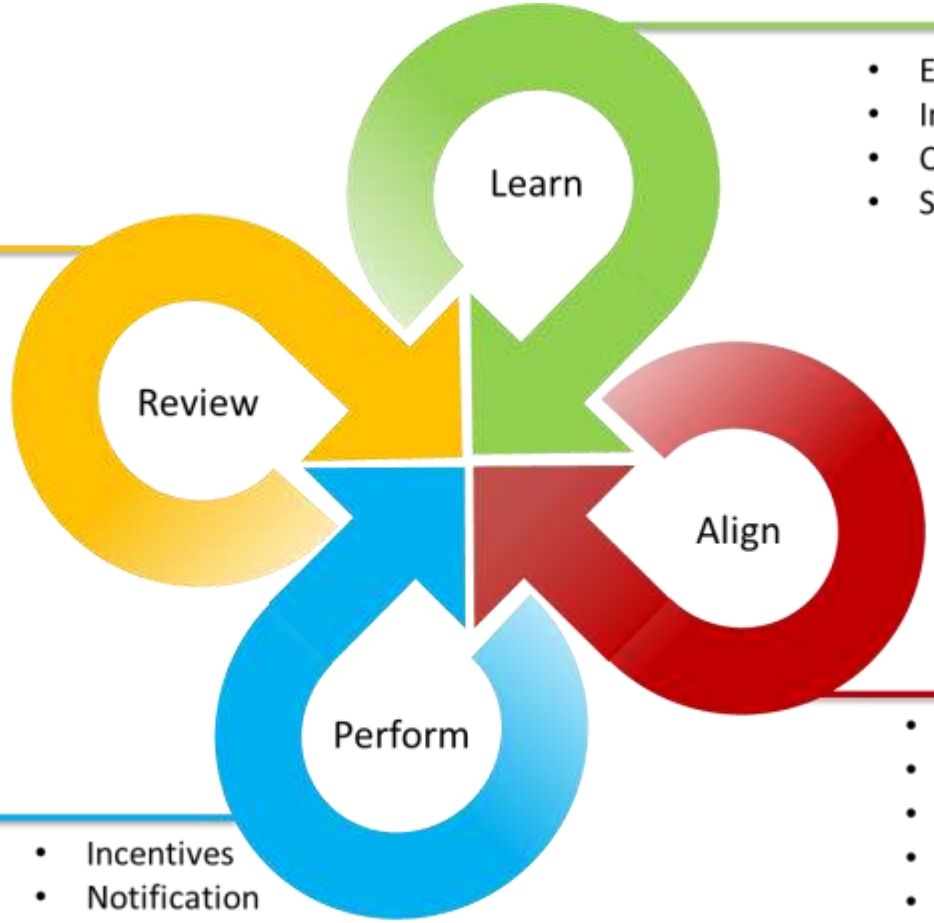
ASQ

# 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

ASQ

# OCEG GRC Capability Model




- External Context
- Internal Context
- Culture
- Stakeholders

- Direction
- Objectives
- Identification
- Assessment
- Design

- Controls
- Policies
- Communication
- Education

- Incentives
- Notification
- Inquiry
- Response

- Monitoring
- Assurance
- Improvement

# 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**

ASQ

# 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

ASQ

# ISO 9004 Maturity Model (Annex A)

| Key element | Maturity level towards sustained success | | | | |
|---|---|---|---|---|---|
| | Level 1 | Level 2 | Level 3 | Level 4 | Level 5 |
| Element 1 | Criteria 1<br>Base level | | | | Criteria 1<br>Best practice |
| Element 2 | Criteria 2<br>Base level | | | | Criteria 2<br>Best practice |
| Element 3 | Criteria 3<br>Base level | | | | Criteria 3<br>Best practice |

ASQ

# 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

ASQ

# 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

ASQ

# 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

ASQ

# 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

ASQ

# Risk Tool Box

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

# PFMEA Risk Tool

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

ASQ

# 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

ASQ

# 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

ASQ

# Focal Area Example

| Context | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| Model Framework | | | Characteristics | | | | | | | | |
| Maturity Level | | | CON1 - Enterprise Process Comprehension | 5 | CON2 - Relevant Interested parties | 4 | CON3 - External and Internal Issues | 2 | CON4 - Self-assessment | 3 |
| Advantaged | Level 5 | 0.25 | Processes and the interactions of influential factors are dynamically determined and used to establish and sustain the organization. | x | Processes and the relationships with relevant interested parties are fulfilled according to the relevant needs and expectations identified. This is done as part of understanding benefits, risks and opportunities of ongoing relationships.<br><br>The needs and expectations of all relevant interested parties are addressed such that improved performance, common understanding of objectives and values, and enhanced stability, include recognition of the benefits derived from these on-going relationships. | | Processes, their interactions and the affects or benefits related to addressing external and internal issues are dynamically determined according to the risks and opportunities identified and acted on based on past and current situations, as well as future plans as part of the organization's strategic direction. This includes the benefits of continuing to analyse, evaluate and apply actions as appropriate to these external and internal issues.<br><br>Processes for the on-going monitoring of external and internal issues are effectively implemented and are being maintained. | | Self-assessments are performed by the organization at all levels. The maturity of each element of the management system is understood comprehensively based on the correlations between the elements and their impacts on the organization's mission, vision and values. The results of selfassessments are communicated to relevant people in the organization and used to share understanding about the organization and its future direction. | |
| Coordinated | Level 4 | 0.50 | Processes and their interactions are systematically determined to ensure outputs continue to support the organization's ability to achieve sustained success.<br><br>All relevant factors and their interrelationships are considered in process determination | x | Processes and their interactions are systematically determined to ensure outputs and interrelationships continue to meet the needs and expectations of relevant interested parties. This includes actions arising from benefits, risks and opportunities as it relates to sustaining ongoing relationships.<br><br>All relevant interested parties and their needs and expectations are considered and those considered to be applicable are included in process determination. | x | Processes and theirinteractions are systematically determined to ensure out puts clearly determine the external andinternal needing to be addressed as part of accounting for risks and opportunitie srelated to sustained success.<br><br>All significant risks and potentially beneficial opportunities related to external and internal issuesare considered in process determination, and include analysis and evaluation of the processes. Past and current situations, as wellsome future plans, are accounted for. | | Self-assessment is used to determine the strengths and weaknesses of the organization well as its best practices, both at an overall level and at the level of its individual processes. Self-assessment assists the organization to prioritize, plan and implement improvements and/or innovations. | |
| Managed | Level 3 | 0.75 | Processes and the interactions are determined to address not only the influential factors but also the relationship of these factors with one another.<br><br>Influential factors related to achieving sustained success are used as inputs into process determination. | x | Processes and their interactions are determined to address not only the identification of relevant interested parties, but also the risks and opportunities, of establishing and sustaining these on-going relationships (e.g., improved performance, common understanding of objectives and value, and enhanced stability).<br><br>The needs and expectations of identified interested parties are used as inputs into the determination of processes, including their importance and relevance. | x | Processes and their interactions are determined to address not only the risks and opportunities, but also the process for continued monitoring of the external and internal issues. The relevant information, including that of the past and current situations, are used as inputs into the determination of processes and the methods used for monitoring those processes. | | Self-assessments are conducted in a consistent manner and the results used to determine the organization's maturity and to improve its overall performance. | x |
| Defined | Level 2 | 1.00 | Key processes, such as those related to identifying influential factors, are determined.<br><br>Interrelationships between processes are not well determined. | x | Key processes, such as those relating to the needs and expectations of relevant interested parties, are determined.<br><br>The interactions between processes, used to establish and sustain ongoing relationships, are not well determined. | x | Key processes relating to external and internal issues are determined (examples are provided in 5.3.1 and 5.3.2). Interactions between external and internal issues, including an ongoing process for monitoring these issues, are not determined. | x | Self-assessment is limited. | x |
| Informal | Level 1 | 1.00 | Processes to develop an understanding of the organization's context are carried out in an informal manner (i.e., lacking a determined and consistent approach). | x | Processes for determining relevant interested parties are done in an informal manner. | x | Processes for determining external and internal issues are informal. | x | Selfassessment is not implemented. | x |

# QMS Aptitude Model Scorecard

| Focal Area Legend | | |
|---|---|---|
| >= 80% | | Level achieved or exceeded |
| >=60% <79% | | Major progress |
| >=30% <59% | | Some progress |
| <=29% | | Little to no progress |

| Model Framework | | Focal Areas | | | | | | |
|---|---|---|---|---|---|---|---|---|
| Maturity Level | | Context | Purpose and Culture | Governance and Leadership | Process Management | Resource Management | Risk and Compliance Management | Improvement and Innovation |
| Advantaged | Level 5 | 0.25 | 0.20 | 0.20 | 0.40 | 0.20 | 0.00 | 0.40 |
| Coordinated | Level 4 | 0.50 | 0.50 | 0.40 | 0.60 | 0.40 | 0.40 | 0.80 |
| Managed | Level 3 | 0.75 | 0.75 | 0.80 | 1.00 | 1.00 | 1.00 | 1.00 |
| Defined | Level 2 | 1.00 | 1.00 | 1.00 | 1.00 | 1.00 | 1.00 | 1.00 |
| Informal | Level 1 | 1.00 | 1.00 | 1.00 | 1.00 | 1.00 | 1.00 | 1.00 |

ASQ

# 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 x 4,712 x 2 = 75,392

ASQ

# 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

ASQ

# Questions?

ASQ®
The Global Voice of Quality®

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