Risk-Based Thinking: New Requirements for ISO 9001:2015 and Integrated Management Systems

Nicole M. Radziwill, PhD, MBA
ASQ Fellow & Editor, Software Quality Professional
Quality Practice Leader
Nicole Radziwill

Quality Practice Lead, Intelex
Fellow, American Society for Quality (ASQ)
CSSBB #11962 & CMQ/OE #9583
Ph.D. Quality Systems, Indiana State
Editor, Software Quality Professional

Previously:
• Division Head, Software, Green Bank Observatory, 2002-2006
• Assistant Director of End to End Operations, National Radio Astronomy Observatory, 2006-2009
• Associate Professor of Data Science & Production Systems, James Madison University, 2009-2018
You will learn about:

1. The role of **risk management** in ISO 9001:2015 and other quality management systems like Baldrige and EFQM

2. How to **incorporate risk-based thinking** into your organization

3. Identifying **strategies for** risk-based thinking in connected, intelligent, automated environments – especially **integrated management systems**

4. Using **agile methods** to reduce technical debt and compliance complacency
Caveat!

People spend *entire careers* studying risk and how to better work with it.

This presentation only covers a small part of the risk universe!
1: Risk Management
in ISO 9001:2015, Baldrige/EFQM, and Enterprises
“the effect of uncertainty on outcomes”
From ISO 31000

“anything that can prevent an organization from achieving its objectives”
Risk is Relative

“the effect of uncertainty on…” successfully crossing the road
From ISO 31000

“anything that can prevent…” someone or something from successfully crossing the road
1. Respond to risks with --- outcomes
2. Take risks with +++ outcomes
3. Increase capabilities + reduce vulnerabilities = improve resilience
Is a hazard a threat? Examine:
- Type of volcano
- History of past behavior
- Leading indicators like earthquakes and gaseous emissions

Risk is relative, and depends on:
- Who and what is in the path of the hazards when they become active threats
- Level of vulnerability
- Extent of capabilities (social, economic, political, technological to prepare, respond, & recover)
- Degree of resilience
- Perception of risk
Why Incorporate Risk-Based Thinking?

To make better decisions in uncertain environments:
• Reduce frequency of losses
• Reduce likelihood of losses
• Reduce costs of losses
• Improve response time
• Reduce stress
• Increase communication
• Enhance learning
• Capture opportunities for improvement


“… in the end it is all about how organizational insights and knowledge are turned into strategic insights and advantage.”

Harry Hertz, Director Emeritus Baldrige Performance Excellence Program
ISO 9001:2015 Updates

- Risk-based thinking
- Organizational context & stakeholder analysis
- Greater flexibility with documentation
- Alignment with other ISO standards (Annex SL)
Figure 3: Clauses of ISO 9001:2015 in accordance with the PDCA cycle

Figure 1: Basic systematic risk management

Clause by Clause

4 — Identify risks to organization
5 — Executive commitment to risk-based thinking and promoting awareness
6 — Identify and manage risks to QMS
7 — Provide resources to support risk
8 — Institute processes to manage risks and take advantage of new opportunities
9 — Monitor risks and respond to signals
10 — Continuously improve processes in a manner sensitive to risks and opportunities

Risk Treatment (5.5)

Risk avoidance

Risk acceptance or retention

Risk transfer

Increasing frequency

Increasing consequence

Unacceptable risk

Tolerable risk

Acceptable risk

What's acceptable? [http://daad.wb.tu-harburg.de/?id=1273](http://daad.wb.tu-harburg.de/?id=1273)

Elements of Risk Addressed by Baldrige

- Governance risk (policy decisions and communication)
- Decision on acceptable levels of risk (appetite)
- Statement of overall organizational risk strategy
- Risk management infrastructure
- Identification of current risks (both opportunities and threats)
- Analysis of risks
- Evaluation of risks and decisions to engage
- Allocation of resources
- Development and implementation of risk protocols
- Risk management training
- Monitoring of performance
- Evaluation and improvement

From https://www.nist.gov/baldrige/enterprise-risk-managementRequires-systems-perspective
Elements of Risk Addressed by EFQM 2010

• **Item 1.1**—How do senior leaders create an environment for innovation and *intelligent risk taking*, achievement of strategic objectives, and organizational agility?

• **Item 2.1**—How do you decide which strategic opportunities are *intelligent risks* for pursuing?

• **Item 5.2**—How does (your performance management system) reinforce *intelligent risk taking to achieve innovation*, reinforce a customer and business focus, and reinforce achievement of your action plans?

• **Item 6.2**—How do you pursue strategic opportunities that you determine are *intelligent risks*?

---

2: Practical Risk-Based Thinking
& how to incorporate it into all levels of your organization
“… a ‘card‐returned‐then‐cash‐dispensed’ ATM dialogue design was at least 22% more efficient (in withdrawal time) and resulted in 100% fewer lost cards (i.e. none) compared with a ‘cash‐dispensed‐then‐card‐returned’ dialogue design.”

Risk-based thinking (RBT) is a “mindset to proactively improve the certainty of achieving outcomes utilizing methods that consider threats and opportunities.”

Risks:
• Can be both positive and negative
• Can hide within processes
• Can lurk outside processes
• Can emerge as a result of changing environmental conditions, and
• Can hide in our cognitive biases

Risk management has historically emphasized loss prevention – RBT incorporates strategically leveraging risk.

From https://community.intelex.com/library/peer-resources/demystifying-risk

Raimund Laqua
Founder, Chief Compliance Engineer
Lean Compliance Consulting Inc.
Step 0: Set Expectations

“A quality system is embedded in every other system of an operating company, whether it is realized or not.”

QMS can be used for:
• Setting overall organizational strategy
• Reducing waste and lowering costs
• Improving processes and results
• Improving communications & shared understanding
• “Doing the things right” and doing them consistently
• Engaging staff

Step 1: Which Risks?

**Society of Actuaries:**
- Market Risk
- Credit Risk
- Insurance Risk
- Liquidity Risk
- Strategy Risk
- Operational Risk
- Reputation Risk
- Group Risk (Supply Chain/Networks)

**Baldrige:**
- Strategic Risk
- Operational Risk
- Reporting Risk
- Compliance Risk (regulations)

**Institutes Risk Group:**
- Hazard Risk
- Operational Risk
- Financial Risk
- Strategic Risk

**Willumsen et al. (2017):**
- Process Risk
- Product Risk
- Design Risk

**PEST(ILE):**
- Political
- Economic
- Social
- Technological
- Industry
- Legal
- Environmental
Business Risk Taxonomy
(Inherent within the Stratex framework)

From http://ascendore.com
Step 2: Identify Significant Risks

Focus groups, surveys, analyzing data from your QMS (e.g. in Pareto Charts); classify or use Risk Priority Number (RPN) to understand and prioritize

Step 3: Ask Why?

Root Cause Analysis: 5 Whys, A3, 8D, FTA, Kepner-Tregoe, Barrier Analysis, Ishikawa/Fishbone, Design of Experiments (DOE), Factor Analysis, PCA
Step 4: Prevent Occurrence

• Poka-yoke (mistake-proofing)
• Improve training
• Redesign processes

Step 5: Improve the QMS

• Identify ways you can anticipate future related issues
• Deploy lessons learned across the organization
Risk-Based Thinking = Preventive Action
Incorporate Risk-Based Thinking

- **Step 0:** Know what to expect from your processes (establish your QMS)
- **Step 1:** Identify classes of risk
- **Step 2:** Identify most significant problems or sources of variability affecting outcomes in each category (from QMS)
- **Step 3:** Why is problem happening?
- **Step 4:** Prevent occurrence
- **Step 5:** Improve QMS & propagate lessons learned
- *Repeat on a regular basis*
Figure 4.1 The four cornerstone habits of thought associated with Risk-Based Thinking. Risk-Based Thinking emphasizes knowing the facts relevant to the work at hand—assets, hazards, their pathways, and respective human touchpoints.
3: Strategies for Integrated Management Systems
and connected, intelligent, automated environments
Figure 5: Health, safety and environmental management
Industry 4.0: Connected, Automated, Intelligent

Frames of Reference

From http://hoskere2.web.engr.illinois.edu/cs445/finalProject/
Frames of Reference

- Order
- Part/Product
- Customer

From http://hoskere2.web.engr.illinois.edu/cs445/finalProject/
• PEST/PESTILE
• SWOT


For more methods, consult the text of ISO/IEC 31010 Risk management methods
Crossover Strategies

- Activate a strength to avert a threat
- Take advantage of an opportunity to overcome a weakness
4: Applying Agile Methods for Risk-Based Thinking to reduce technical debt and compliance complacency
Technical Debt

“We don’t have time to update the documentation, but it wasn’t a huge change anyway.”

“It’s not bullet-proof, but we got the change done and it should work.”

“A system’s technical debt at a given point in time could be defined as deferred investment opportunities or poorly managed risks.”


Compliance Complacency

“We got our ISO 9001 certificate so we’re totally safe, we’re doing everything right, and we have nothing to worry about. Our auditors love us.”

“Organizational satisfaction of the (compliance) status quo without regard to, or intent to learn of, potential compliance risks in the business.”

What Makes Agile Work?

- Process exists for continuously revisiting what you know, and integrating new information
- Individuals are empowered to adjust based on that new information
- The organization continually seeks to remove barriers to make it easy for those adjustments to be made
- Documentation focuses on essential elements required to communicate those changes

Risk-Based Thinking is Organizational Mindfulness THAT BUILDS RELATIONSHIPS & TRUST
Nicole Radziwill
Quality Practice Lead
nicole.radziwill@intelex.com
@nicoleradziwill

Wired: https://goo.gl/cdQM29
Slides: https://goo.gl/woXX9r
Supplemental Slides
COGNITIVE BIAS CODEX

What Should We Remember?
- We store memories differently based on how they were experienced.
- We notice things already primed in memory or repeated often.
- We notice when something has changed.
- We are drawn to details that confirm our own existing beliefs.
- We notice flaws in others; more easily than we notice flaws in ourselves.

To avoid mistakes, we aim to preserve authority and group status, and avoid irreversible decisions.
- To get things done, we tend to complete things we've invested time & energy in.
- To stay focused, we favor the immediate, reliable thing in front of us.

We Need To Act Fast
- To act, we must be confident; we can make an impact and feel what we do is important.
- We project our current mindset and assumptions onto the past and future.
- We think we know what other people are thinking.
- We simplify probabilities and numbers to make them easier to think about.

We favor simple-looking options and complete information over complex, ambiguous options.
- We discount specifics to form generalities.
- We don't notice when something has changed.
- We are drawn to details that confirm our own existing beliefs.
- We notice flaws in others; more easily than we notice flaws in ourselves.

Too Much Information
- We notice when something has changed.
- We are drawn to details that confirm our own existing beliefs.
- We notice flaws in others; more easily than we notice flaws in ourselves.
- We tend to find stories and patterns even when looking at sparse data.
- We fill in characteristics from stereotypes, generalities, and prior histories.

Not Enough Meaning
- We imagine things and people we're familiar with or fond of as better.
- We simplify probabilities and numbers to make them easier to think about.
- We think we know what other people are thinking.
- We project our current mindset and assumptions onto the past and future.
- We think we know what other people are thinking.

Visual & Algorithmic Design: John Varela
Concept & Categorization: Buster Benson
OWASP Risk Rating Methodology

\[
\text{RISK} = \text{THREAT} \times \text{VULNERABILITY} \times \text{CONSEQUENCE}
\]

\[
\text{RISK} = \text{LIKELIHOOD} \times \text{IMPACT}
\]

- OWASP integrates skill of attacker, vulnerability (ease of discovery, ease of exploit, awareness, and risk of detection) into likelihood
- Impact includes technical (asset) and business (operations) impact
- Nearly identical to the risk equation, but provides additional guidance for determining values from a cybersecurity perspective