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

INTELEX


MAERSK LINE
INTELEX

Office and project locations

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*

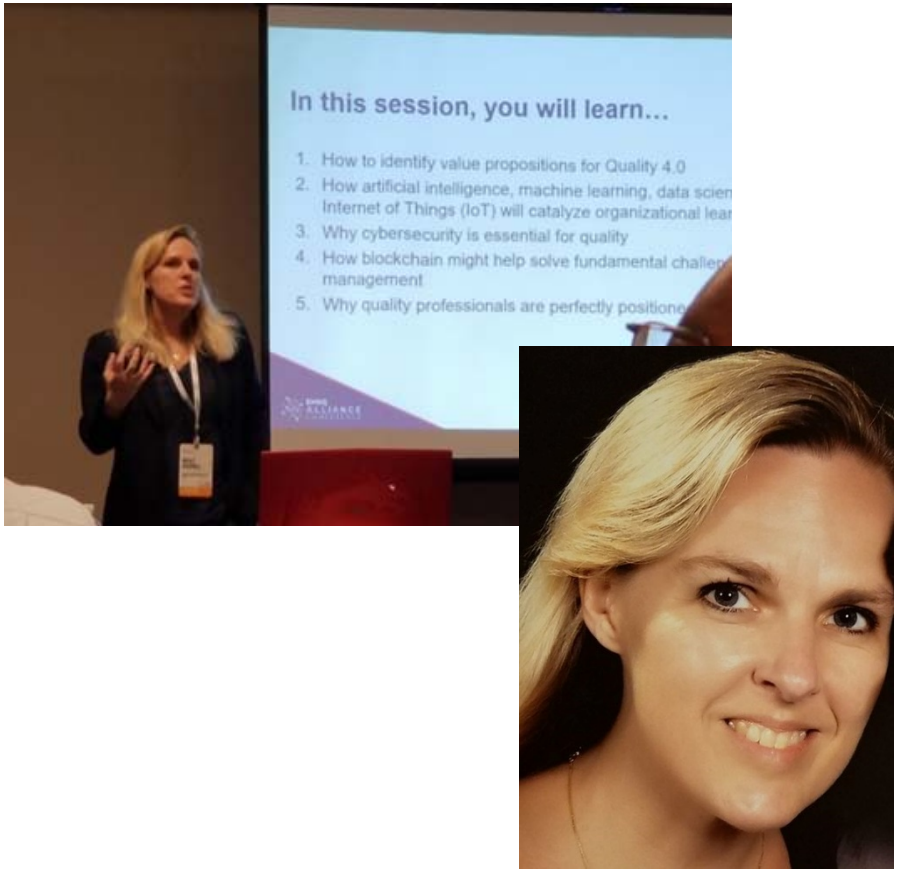
Previously:

•Project Manager, Solution Architect, Engagement Manager in Meteorological Research, Telecom, Manufacturing, Software, High Tech 1995-2002

•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



INTELEX

Objectives

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

INTELEX

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!

INTELEX

1: Risk Management

in ISO 9001:2015, Baldrige/EFQM, and Enterprises

INTELEX

Risk

"the effect of **uncertainty** on **outcomes**"

From ISO 31000

"**anything** that can prevent an organization from achieving its **objectives**"

From Kendall, K. (2017). The Increasing Importance of Risk Management in an Uncertain World. The Journal for Quality and Participation, 40(1), 4.

INTELEX

Risk is Relative

"the effect of **uncertainty** on…"
successfully crossing the road

From ISO 31000

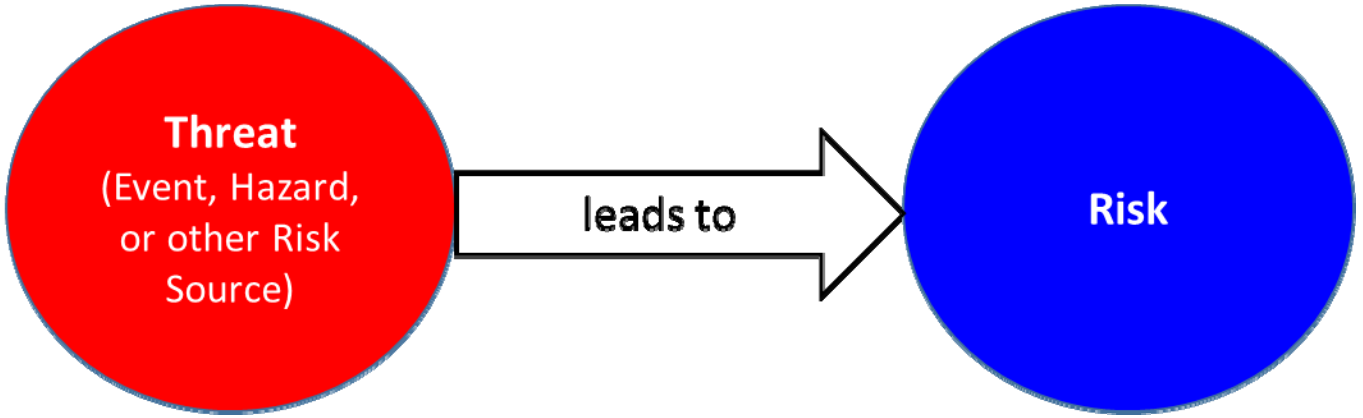
"**anything** that can prevent…"
someone or something from
successfully crossing the road

From Kendall, K. (2017). The Increasing Importance of Risk Management in an Uncertain World. The Journal for Quality and Participation, 40(1), 4.

INTELEX

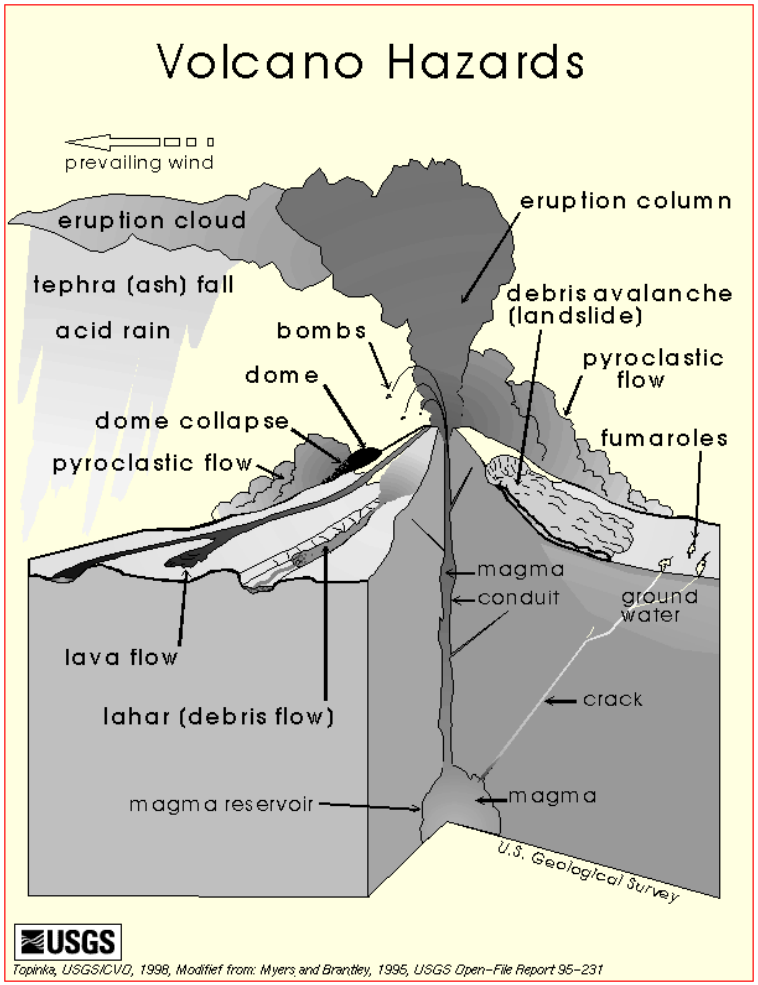
Hazard
(inactive)

Threat
(active)



1. Respond to risks with --- outcomes
2. Take risks with +++ outcomes
3. Increase capabilities + reduce vulnerabilities = improve resilience

INTELEX



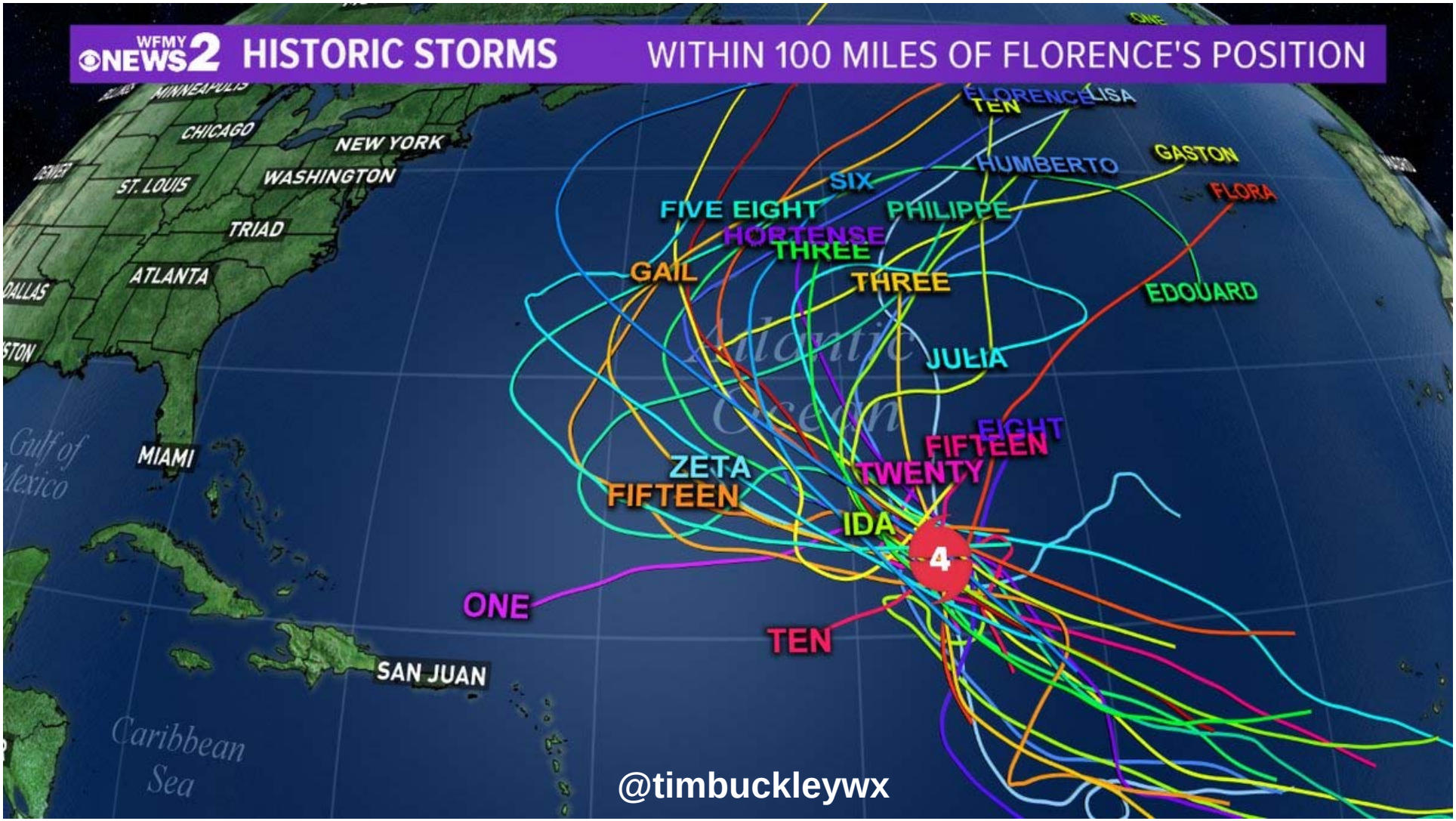
Is a hazard a threat? Examine:

- 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

INTELEX


WFMY NEWS 2
HISTORIC STORMS
WITHIN 100 MILES OF FLORENCE'S POSITION
MINNEAPOLIS
CHICAGO
NEW YORK
DENVER
ST. LOUIS
WASHINGTON
TRIAD
ATLANTA
DALLAS
MIAMI
Gulf of Mexico
Caribbean Sea
SAN JUAN
Atlantic Ocean
FLORENCE
LISA
TEN
HUMBERTO
GASTON
FLORA
SIX
FIVE EIGHT
PHILIPPE
HORTENSE
THREE
GAIL
THREE
EDOUARD
JULIA
EIGHT
FIFTEEN
ZETA
TWENTY
FIFTEEN
IDA
4
ONE
TEN
@timbuckleywx

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

From Willumsen, P., Oehmen, J., Rossi, M., & Welo, T. (2017). Applying lean thinking to risk management in product development. In Proc. 21st Intl. Conf. on Engr. Design (ICED 17), Vancouver, 269-278.

"… 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

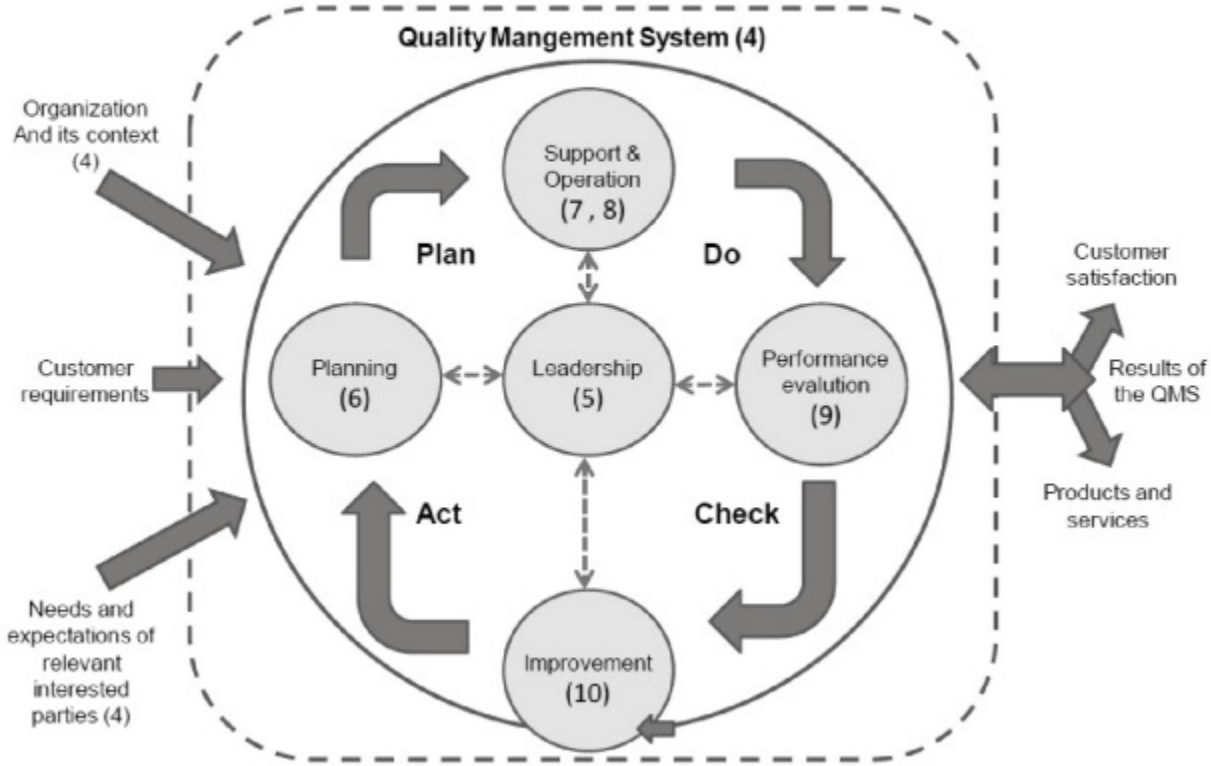
INTELEX

ISO 9001:2015 Updates

- **Risk-based thinking**
- Organizational context & stakeholder analysis
- Greater flexibility with documentation
- Alignment with other ISO standards (Annex SL)

INTELEX

Figure 3: Clauses of ISO 9001:2015 in accordance with the PDCA cycle



From Illés, B. C., Szuda, C., & Dunay, A. (2017). Quality and management – Tools for continuous and systematic improvement of processes.

INTELEX

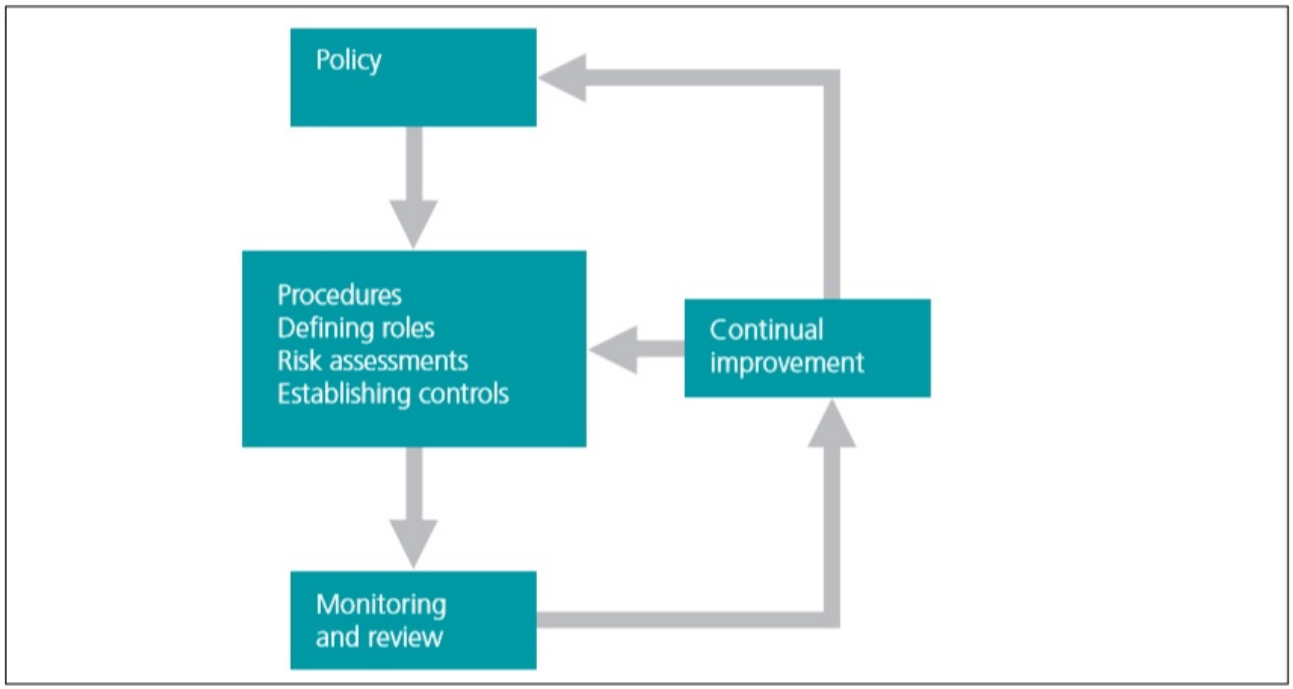


Figure 1: Basic systematic risk management

From Institution of Occupational Safety and Health (IOSH UK) (2017). Joined-up working – an introduction to integrated management systems.

INTELEX

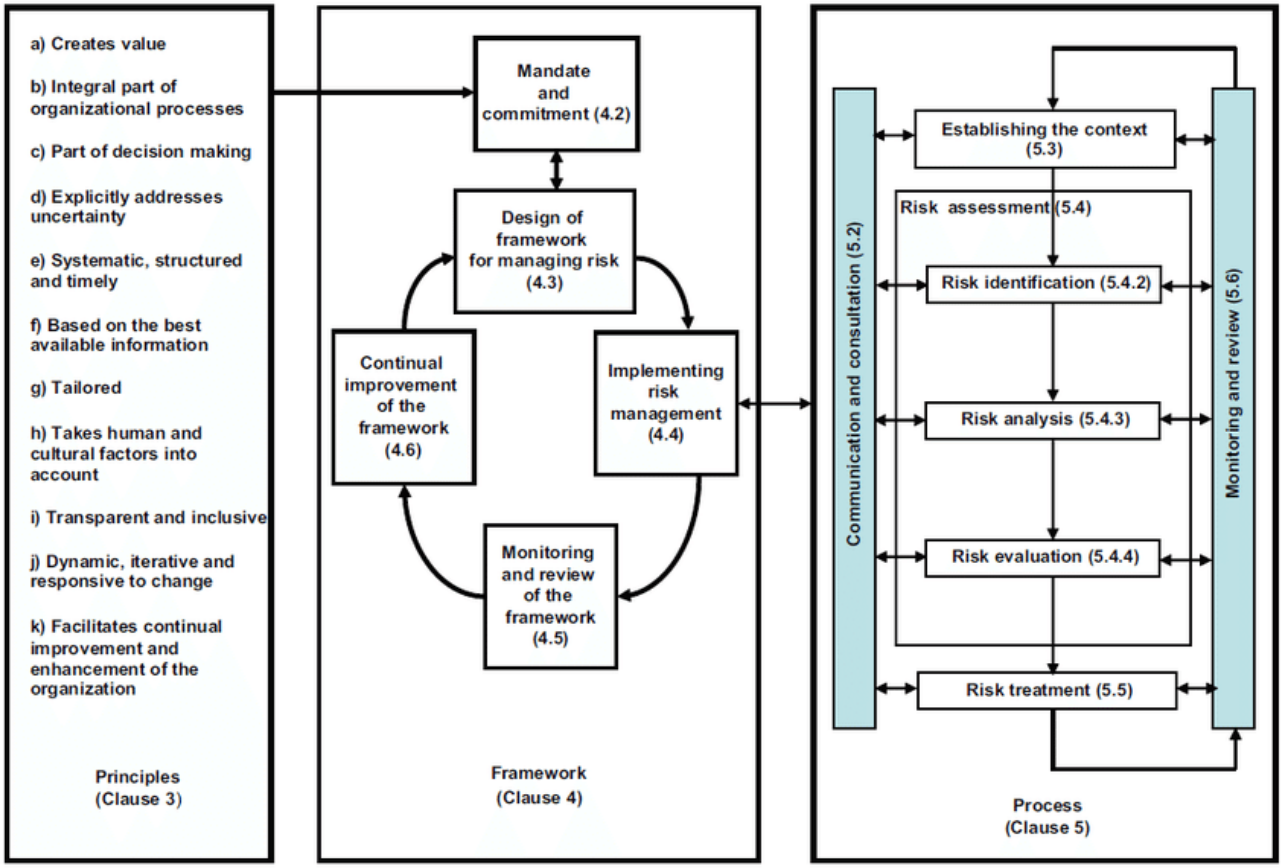
Clause by Clause

- **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

From Hoyle, D. (2017). ISO 9000 Quality Systems Handbook-updated for the ISO 9001: 2015 standard: Increasing the Quality of an Organization's Outputs. Routledge.

INTELEX

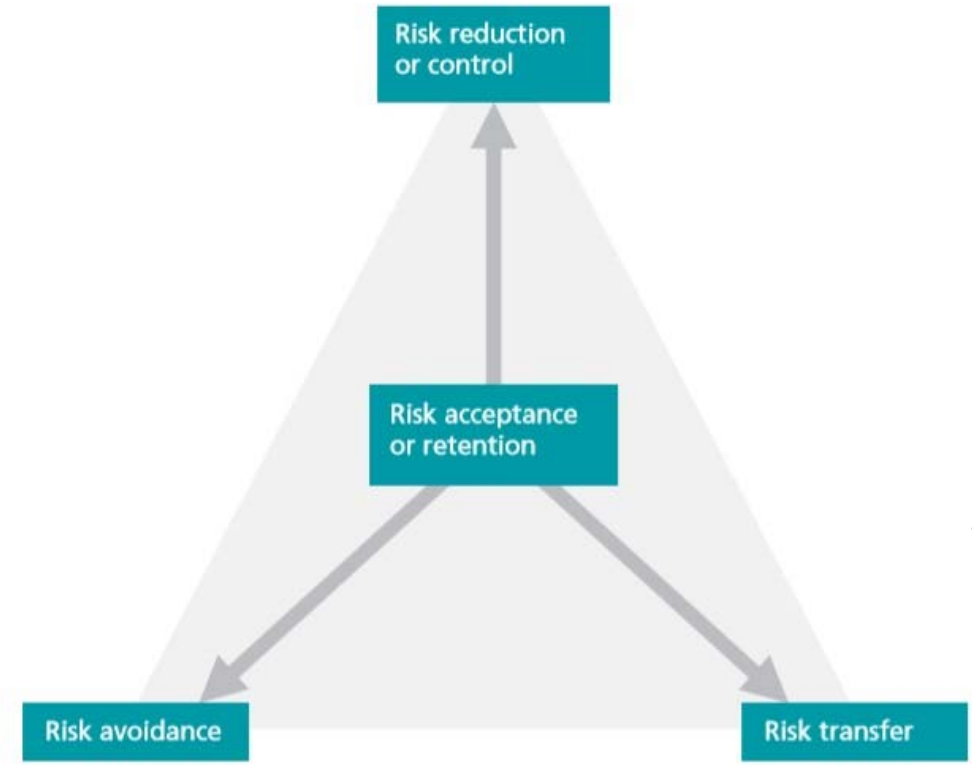
ISO 31000

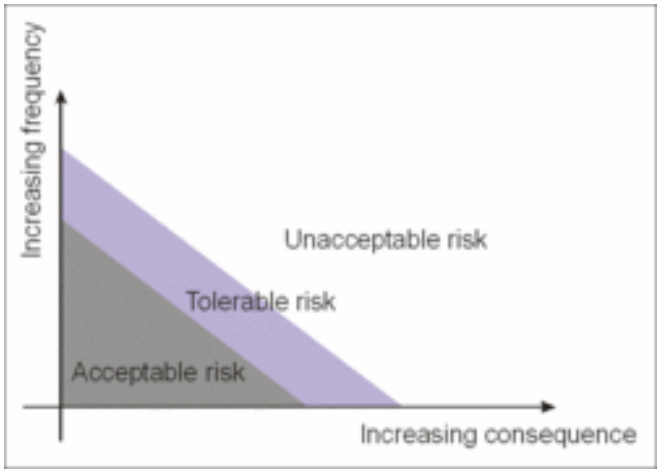


From Beker, I., Delić, M., Milisavljević, S., Gošnik, D., Ostojić, G., & Stankovski, S. (2015). Can IoT be used to mitigate food supply chain risk? International Journal of Industrial Engineering and Management, 6(4), 221-226.

INTELEX

Risk Treatment (5.5)



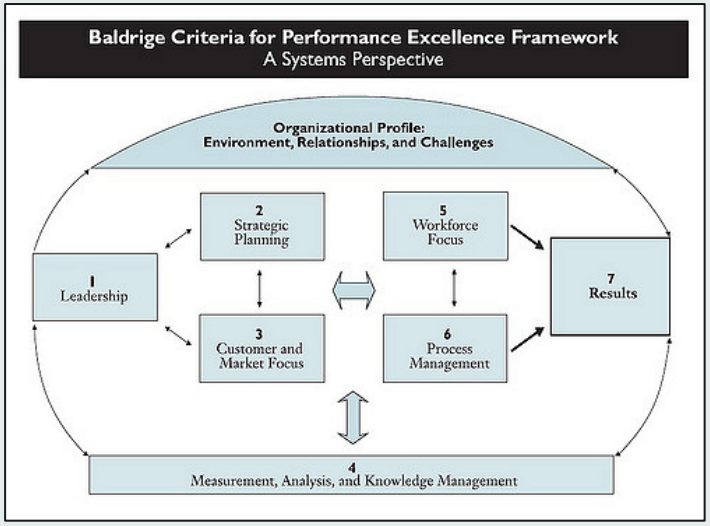


What's acceptable? http://daad.wb.tu-harburg.de/?id=1273

From Institution of Occupational Safety and Health (IOSH UK) (2017). Joined-up working – an introduction to integrated management systems.

INTELEX

Elements of Risk Addressed by Baldrige

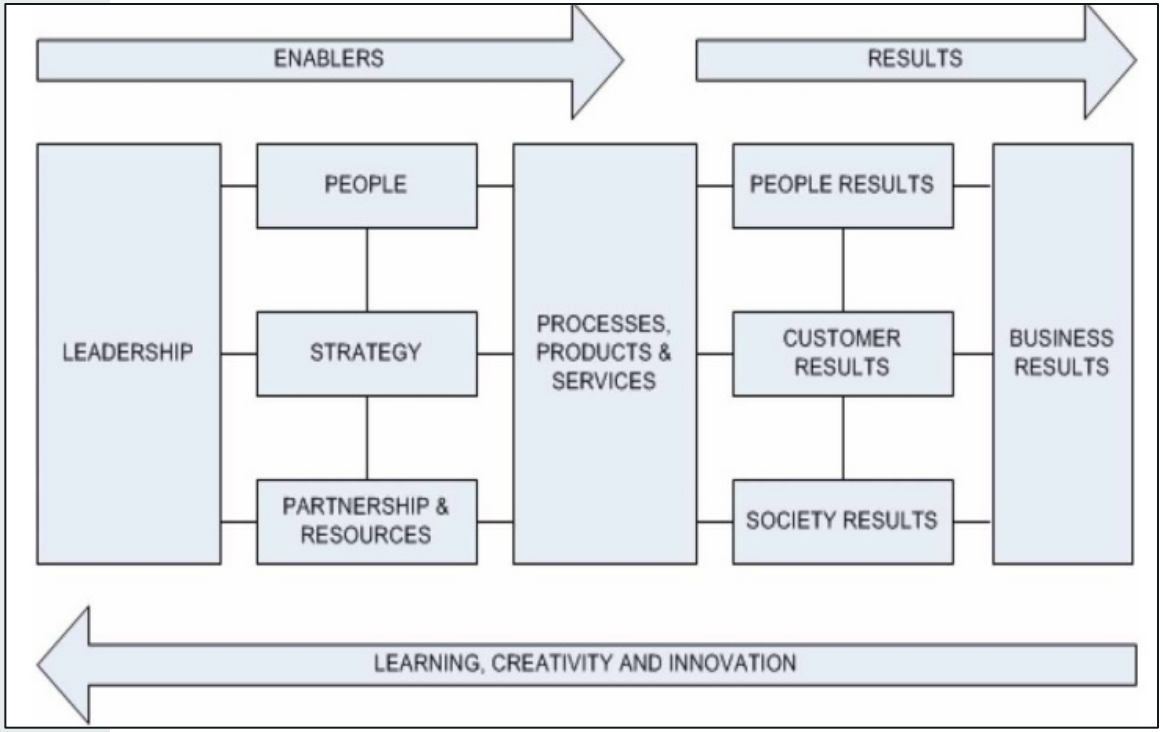


- Governance risk (policy decisions and communication)
- Decision on acceptable levels of risk (appetite)
- Statement of overall organizational risk strategy
- Risk management infrastructure
- Identification of current risks (both opportunities and threats)
- Analysis of risks
- Evaluation of risks and 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-management-requires-systems-perspective

INTELEX

Elements of Risk Addressed by EFQM 2010



From Akyuz, G. A. (2015). Quality excellence in complex supply networks: EFQM excellence model reconsidered. Total Quality Management & Business Excellence, 26(11-12), 1282-1297.

INTELEX

Taking Intelligent Risks (Baldrige 2013)

- **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**?

From Kendall, K. (2017). The Increasing Importance of Risk Management in an Uncertain World. The Journal for Quality and Participation, 40(1), 4.

INTELEX

2: Practical Risk-Based Thinking

& how to incorporate it into all levels of your organization

INTELEX

From Lockton, D., Harrison, D., & Stanton, N. A. (2010). The Design with Intent Method: A design tool for influencing user behaviour. Applied ergonomics, 41(3), 382-392.

INTELEX

"… 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."

Zimmermann, C. M., & Bridger, R. S. (2000). Effects of dialogue design on automatic teller machine (ATM) usability: transaction times and card loss. Behaviour & Information Technology, 19(6), 441-449.

INTELEX

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.

Raimund Laqua
Founder, Chief Compliance Engineer
Lean Compliance Consulting Inc.

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

INTELEX

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

From Peach, R. W. (1990). Creating a pattern of excellence. Target, 6(4), 15. Available from http://www.ame.org/sites/default/files/target_articles/90Q4A2.pdf

INTELEX

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

INTELEX

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

INTELEX

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

INTELEX

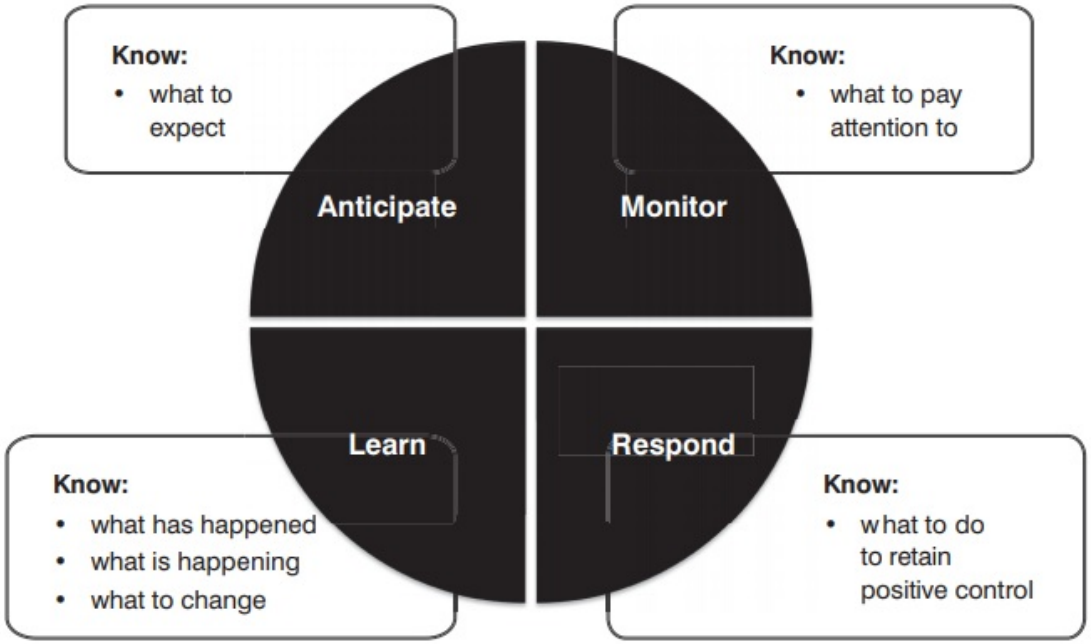
Risk-Based Thinking = Preventive Action

INTELEX

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*

INTELEX



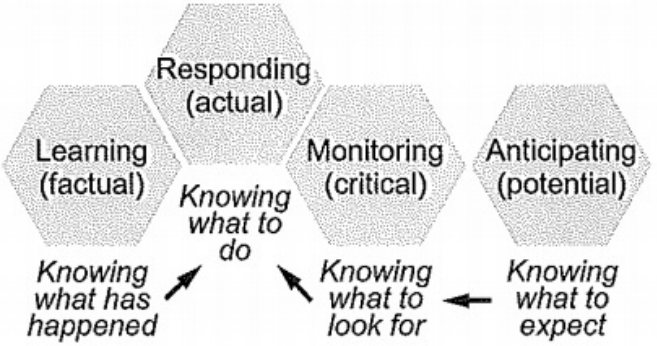


Figure 4.1 The four cornerstone habits of thought associated with RISK-BASED THINKING. RISK-BASED THINKING emphasizes knowing the facts relevant to the work at hand—**assets**, **hazards**, their **pathways**, and respective human **touchpoints**

From Muschara, T. (2017). *Risk-Based Thinking: Managing the Uncertainty of Human Error in Operations*. Routledge.

INTELEX

3: Strategies for Integrated Management Systems

and connected, intelligent, automated environments

INTELEX

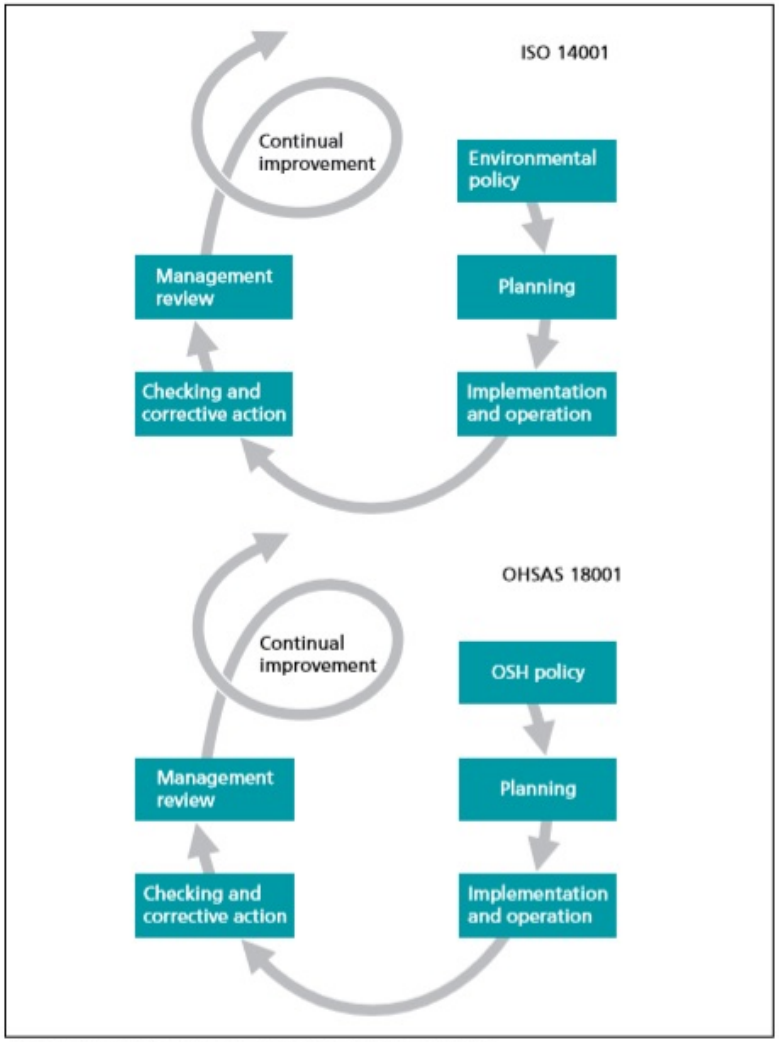


Figure 4: OHSAS 18001 and ISO 14001 models

From Institution of Occupational Safety and Health (IOSH UK) (2017). Joined-up working – an introduction to integrated management systems.

INTELEX

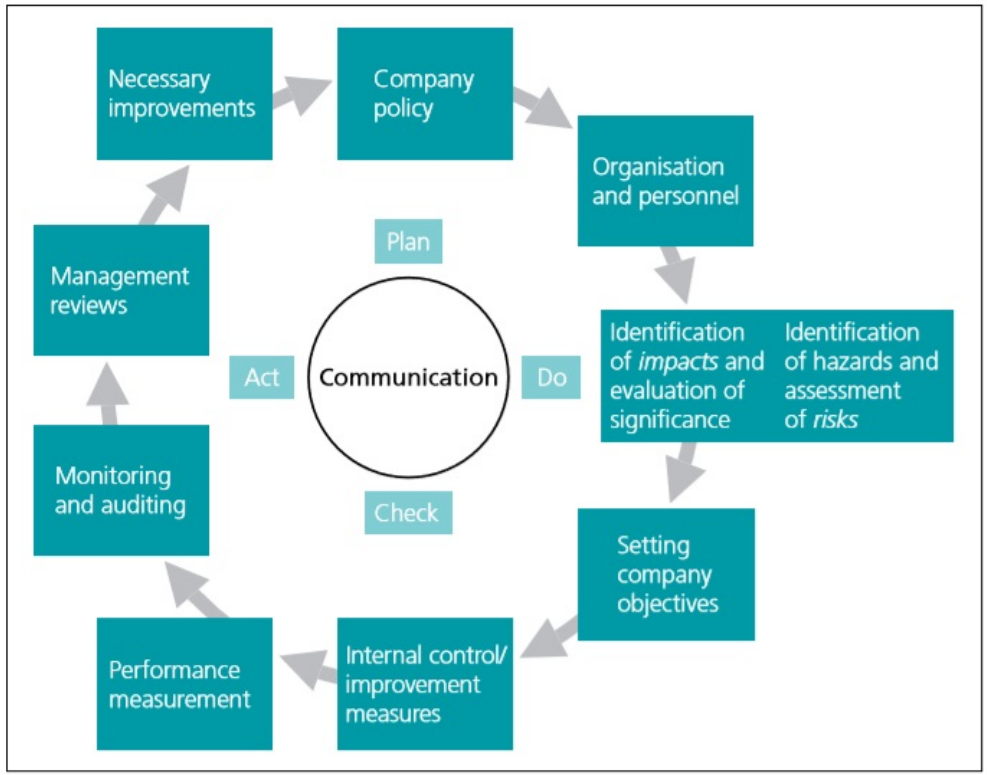
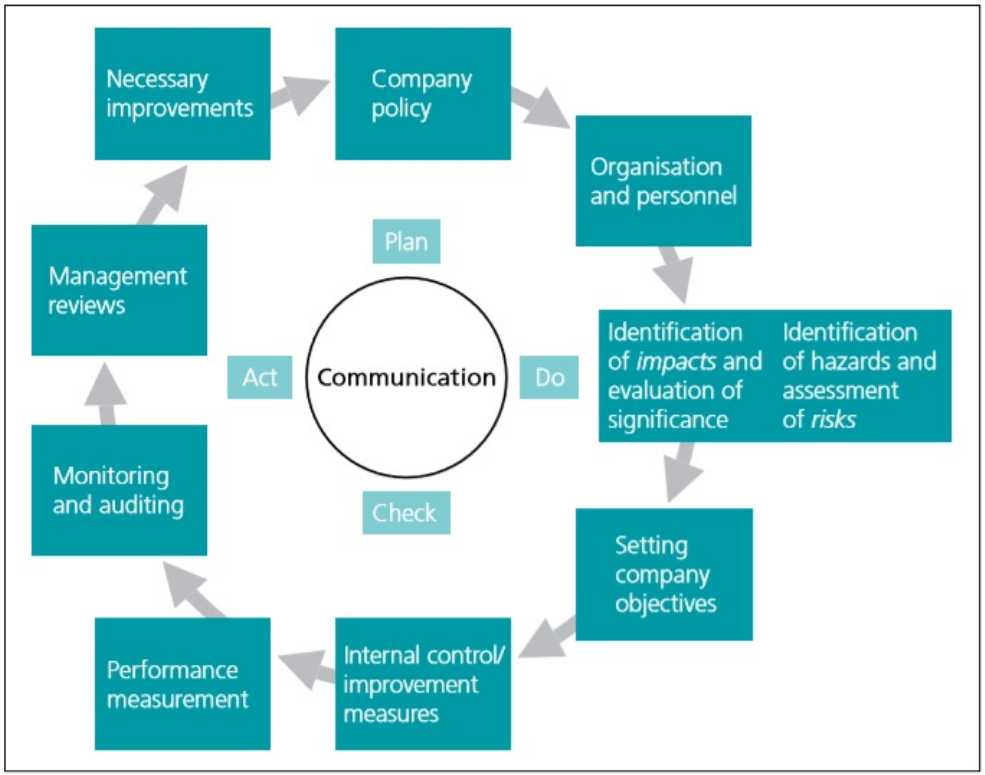


Figure 5: Health, safety and environmental management

From Institution of Occupational Safety and Health (IOSH UK) (2017). Joined-up working – an introduction to integrated management systems.

INTELEX

Industry 4.0: Connected, Automated, Intelligent



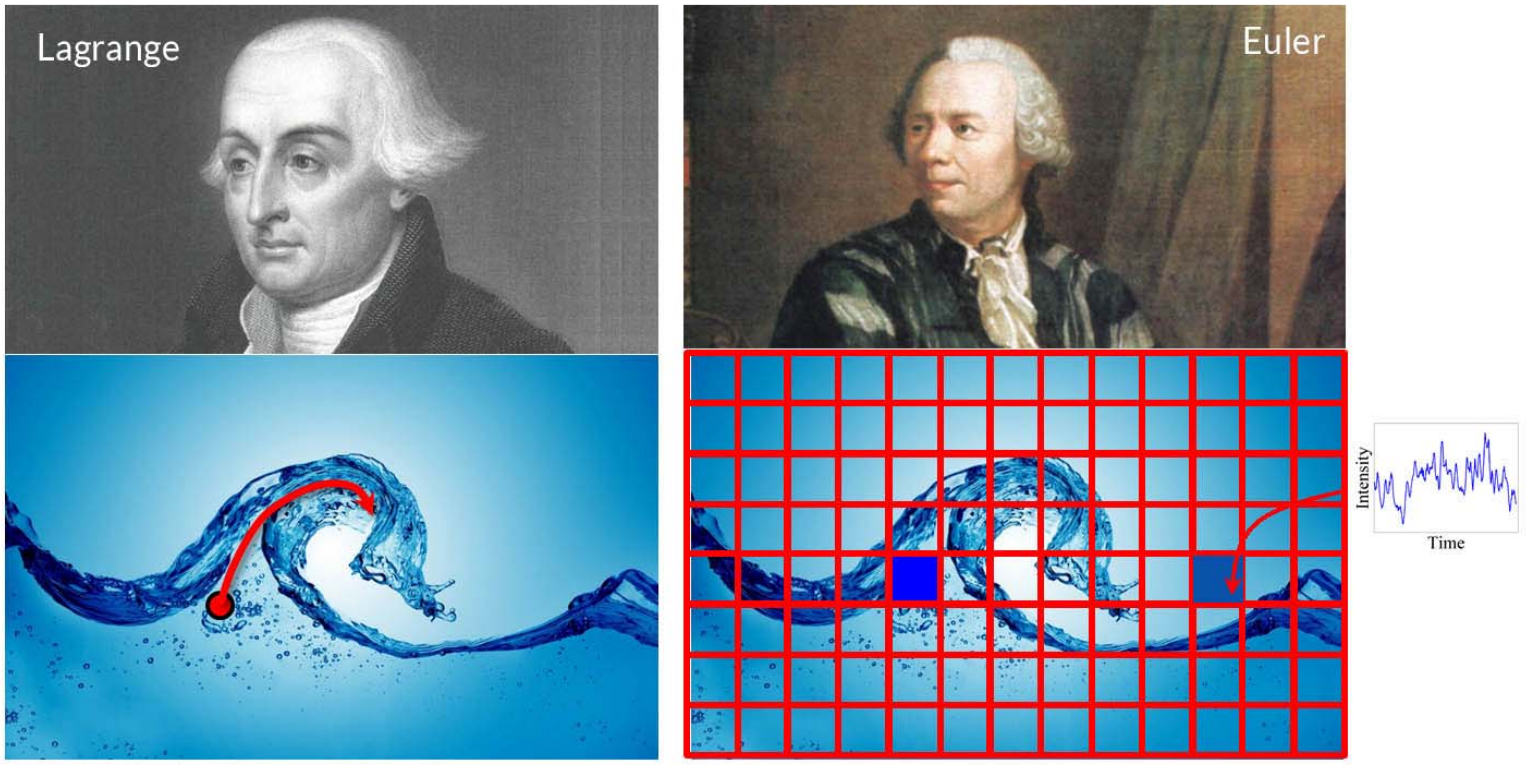
AI/ML Integrity

Cybersecurity

From Institution of Occupational Safety and Health (IOSH UK) (2017). Joined-up working – an introduction to integrated management systems.

INTELEX

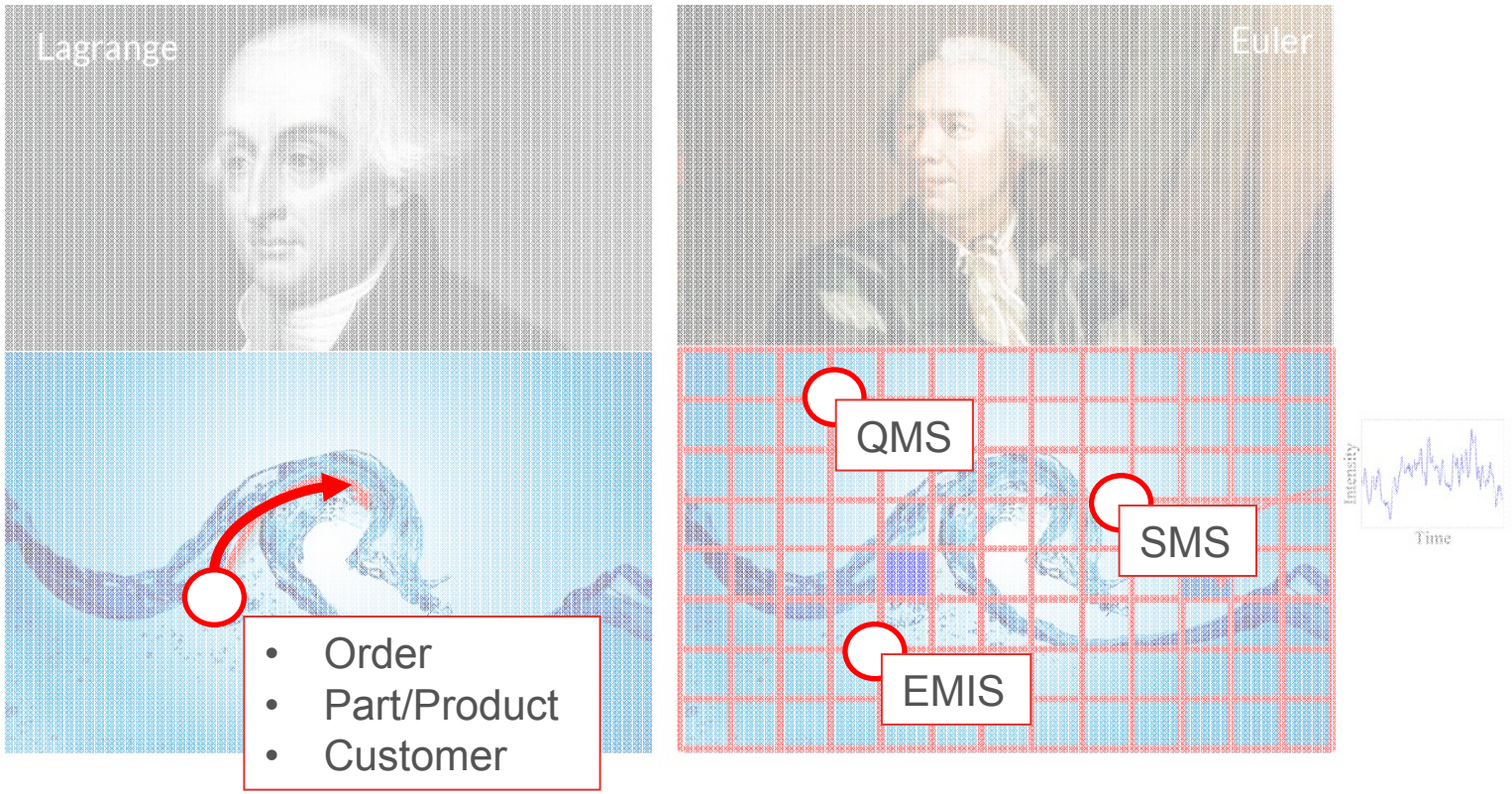
Frames of Reference



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

INTELEX

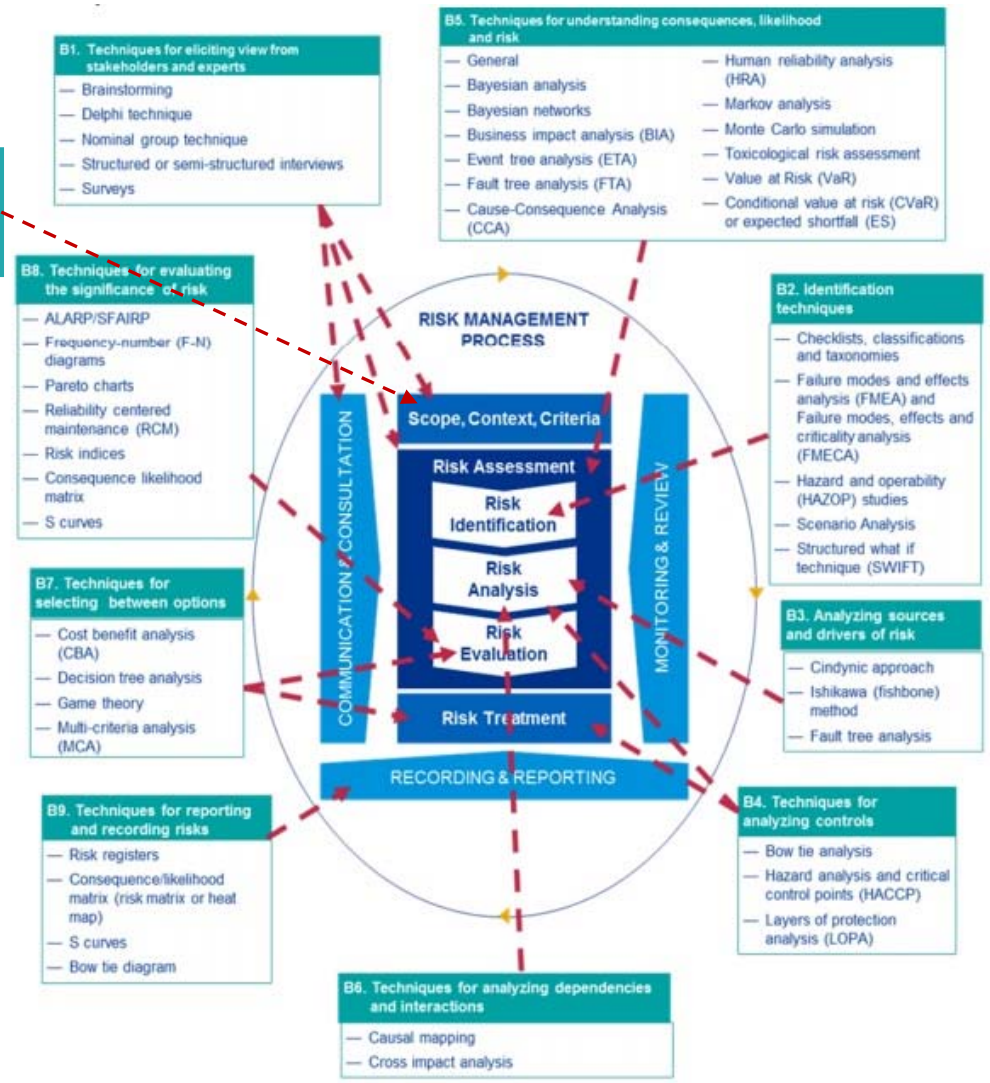
Frames of Reference



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

INTELEX

- PEST/PESTILE
- SWOT

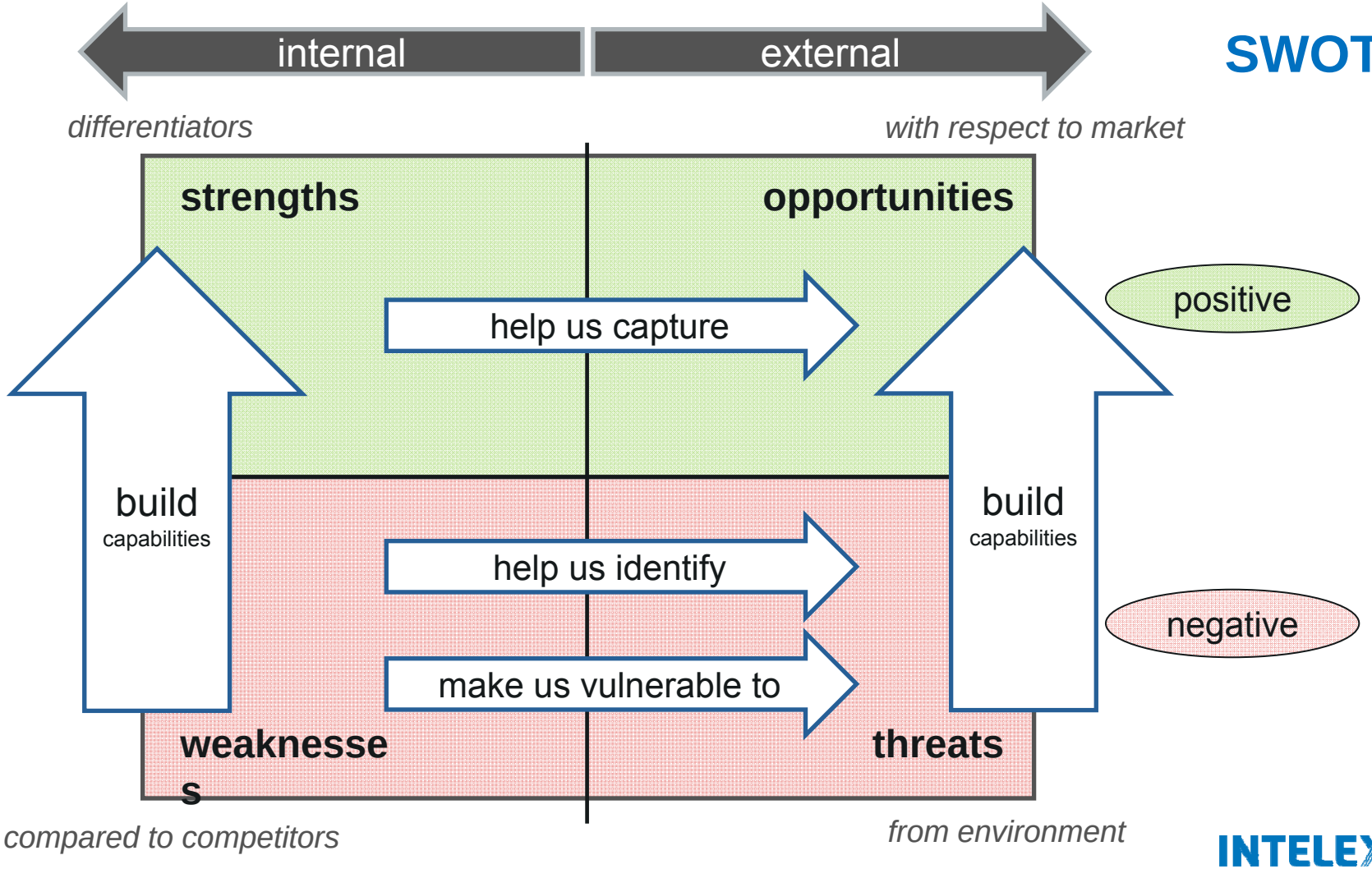


From Cross, J. (2017). ISO 31010 Risk assessment techniques and open systems. *Sixth Workshop on Open Systems Dependability*, Tokyo, October 21.

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

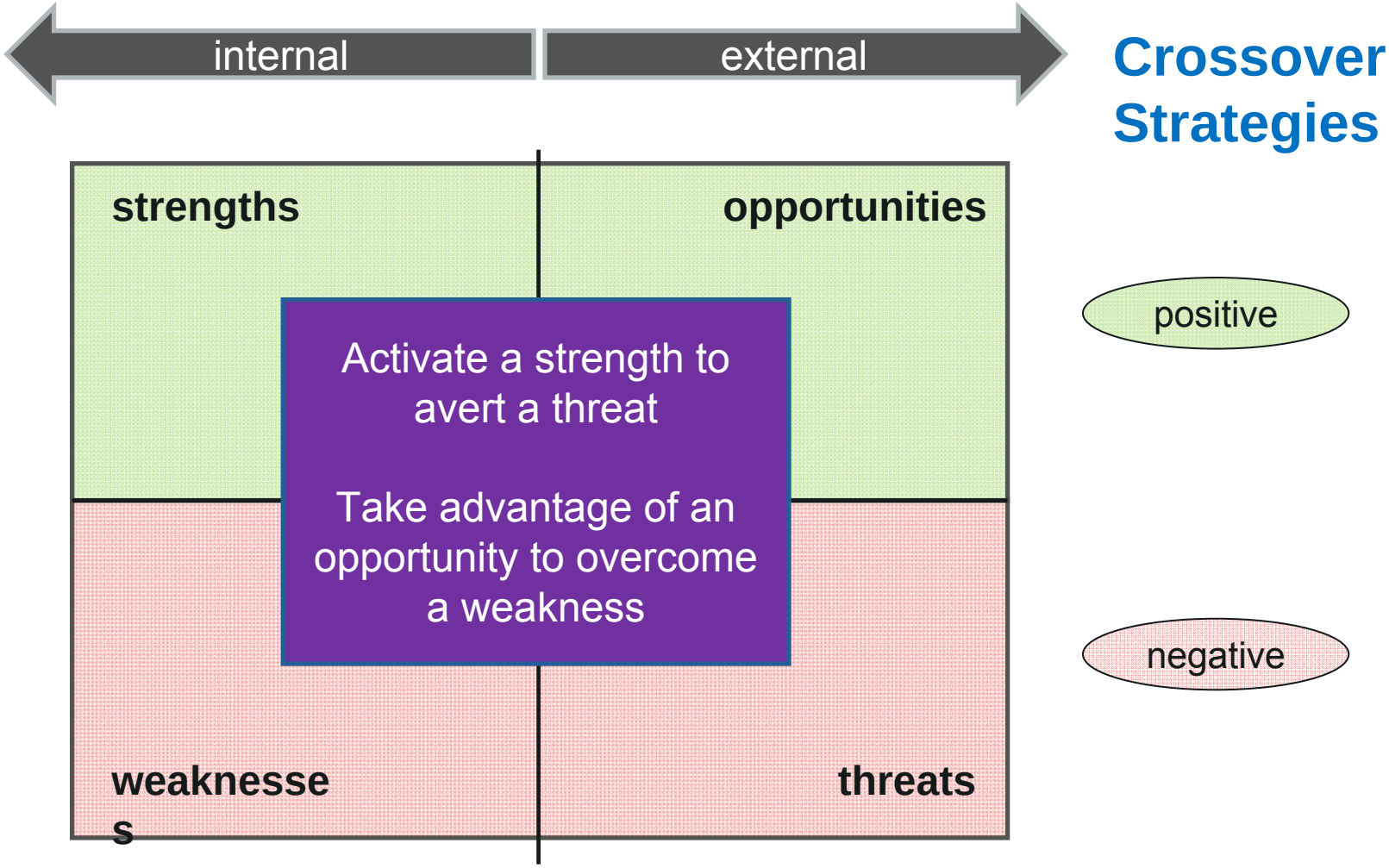
INTELEX

SWOT



INTELEX

Crossover Strategies



INTELEX

4: Applying Agile Methods for Risk-Based Thinking

to reduce technical debt and compliance complacency

INTELEX

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**.”

Kruchten, P., Nord, R. L., & Ozkaya, I. (2012). Technical debt: From metaphor to theory and practice. Ieee software, 29(6), 18-21.

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."

Ball, R. (2011). Fighting Compliance Complacency. *Specialty Gas Report,* 44-46.

INTELEX

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

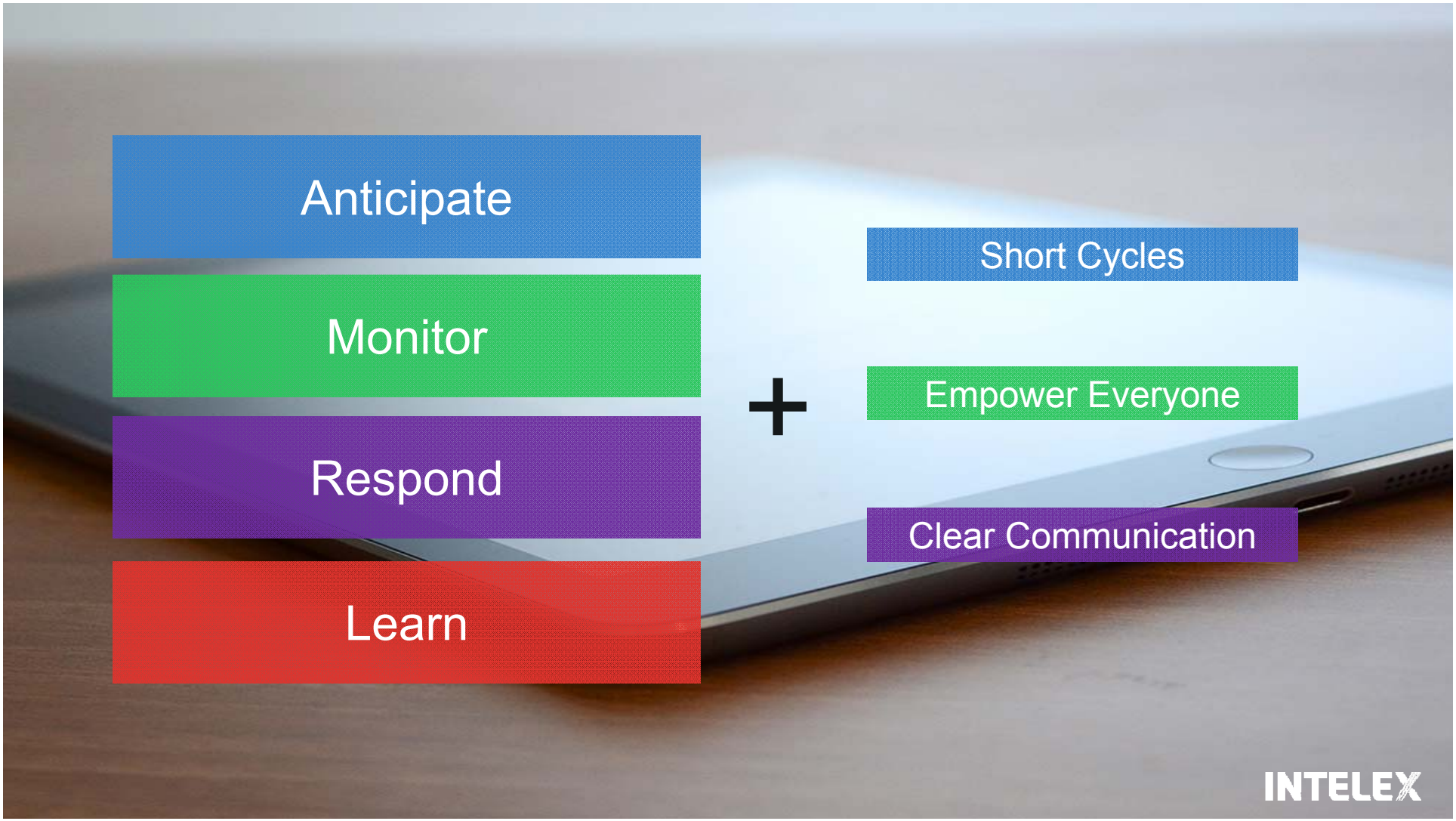
Short Cycles

Empower Everyone

Clear Communication

From Ambler, S. (2002). Agile modeling: effective practices for extreme programming and the unified process. John Wiley & Sons.

INTELEX


Anticipate
Monitor
Respond
Learn
+
Short Cycles
Empower Everyone
Clear Communication
INTELEX


Risk-Based Thinking is
Organizational Mindfulness
THAT BUILDS RELATIONSHIPS & TRUST

From https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/

CONTACT

Nicole Radziwill

Quality Practice Lead

nicole.radziwill@intelex.com

@nicoleradziwill

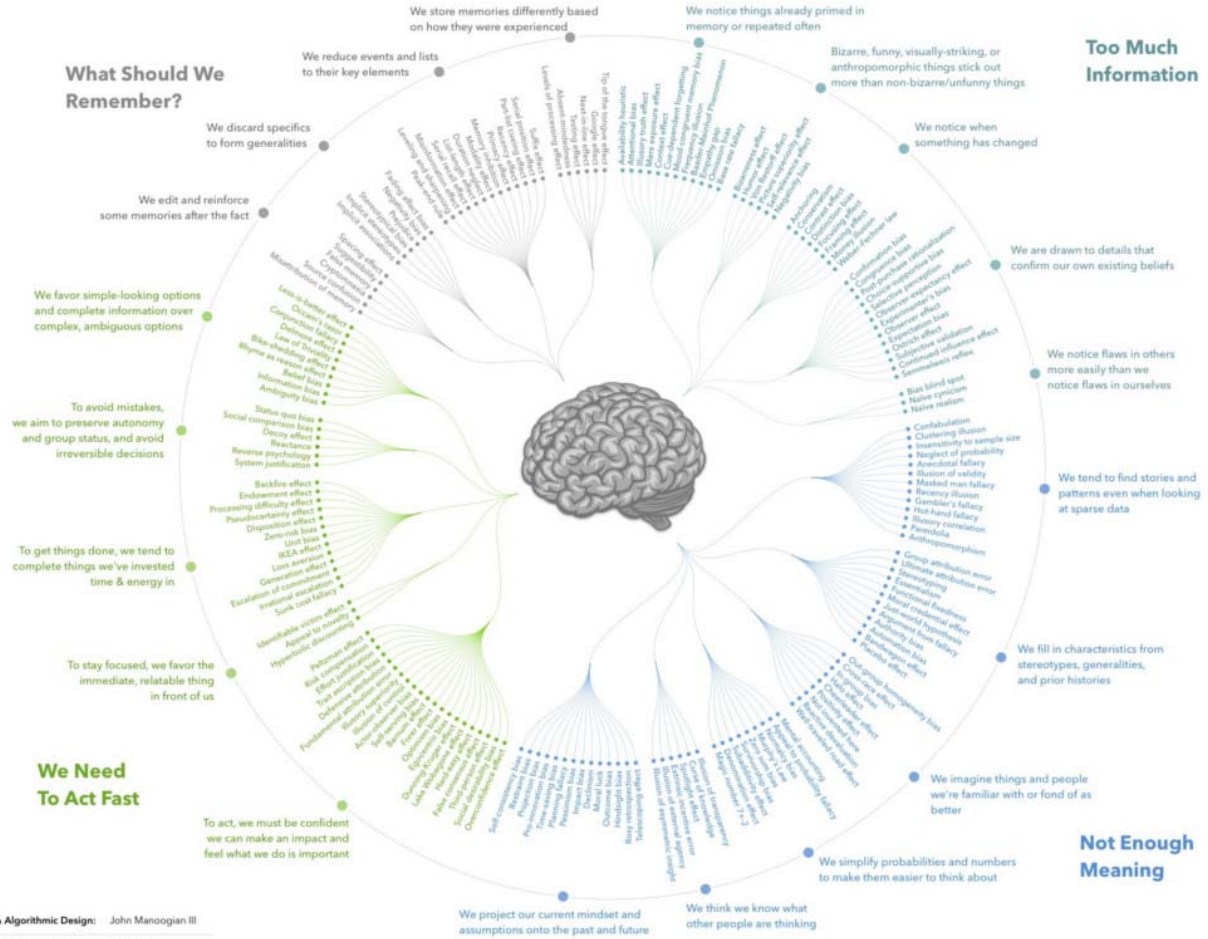
Wired: https://goo.gl/cdQM29

Slides: https://goo.gl/woXX9r

INTELEX

Supplemental Slides

COGNITIVE BIAS CODEX



Visual & Algorithmic Design:	John Manoogian III
Concept & Categorization:	Buster Benson
List of 188 Cognitive Biases:	Wikipedia

designhacks.co

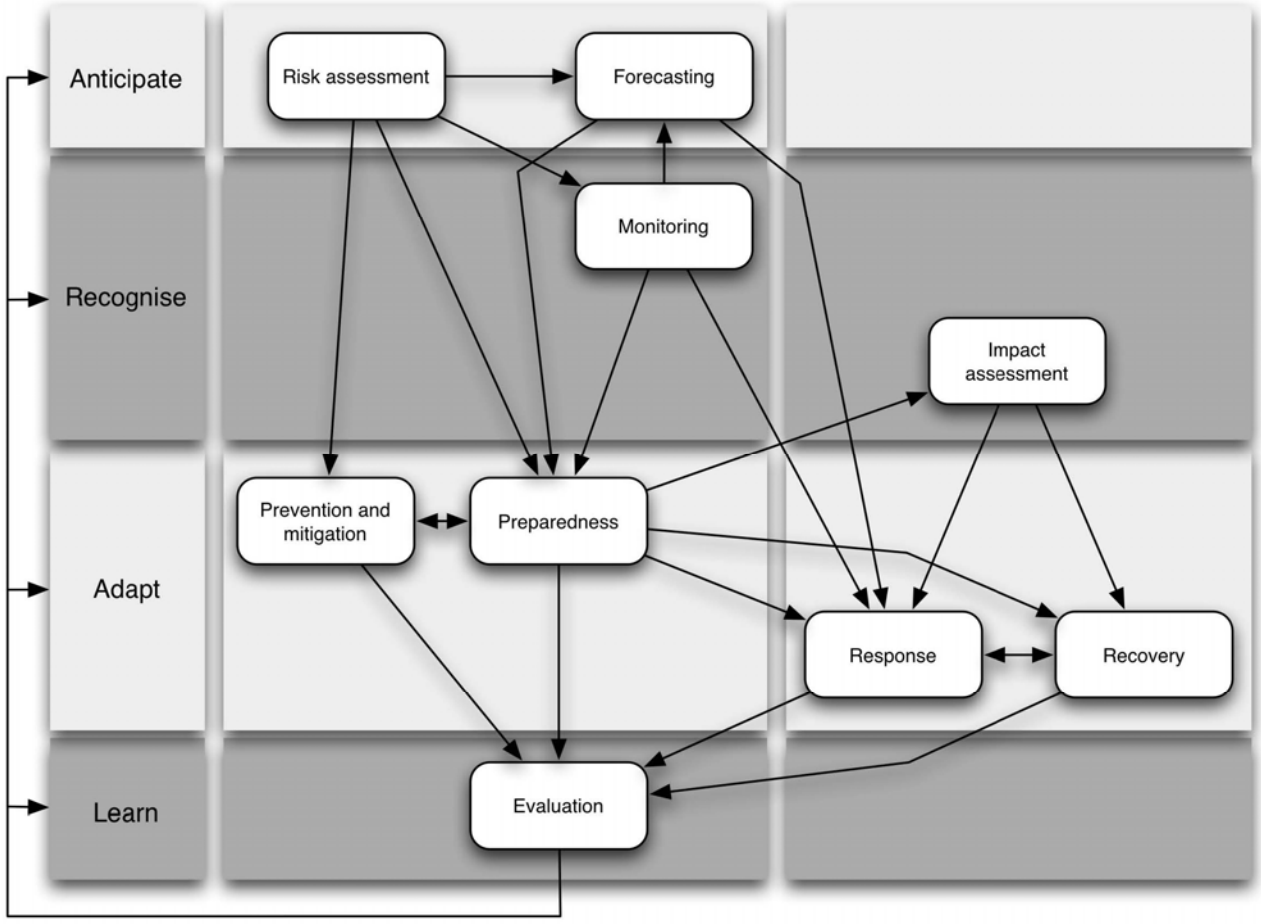
INTELEX

Anticipate

Monitor

Respond

Learn



From Becker, P., Abrahamsson, M., & Tehler, H. (2011). An emergent means to assurgent ends: community resilience for societal safety and sustainability. In Proceedings of the fourth resilience engineering symposium. Presses des MINES, Paris, France (pp. 29-33).

INTELEX

OWASP Risk Rating Methodology

RISK = THREAT x VULNERABILITY x CONSEQUENCE

RISK = LIKELIHOOD x 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

Overall Risk Severity				
Impact	HIGH	Medium	High	Critical
	MEDIUM	Low	Medium	High
	LOW	Note	Low	Medium
		LOW	MEDIUM	HIGH
	Likelihood			

INTELEX