Risk Appetite Development

Brett Tucker, PMP, CSSBB, CISSP, CAP

January 2023

Software Engineering Institute
Carnegie Mellon University
Pittsburgh, PA 15213

This material is based upon work funded and supported by the Department of Defense under Contract No. FA8702-15-D-0002 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center.

DM23-0039

Carnegie Mellon University (CMU)

Pioneering discoveries that enrich the lives of people on a global scale

- Turning disruptive ideas into success through leading-edge research
- 2021 *U.S. News and World Report* rankings:
  - #1 in computer engineering, AI, cybersecurity, and software engineering
  - #2 in overall computer science
  - #3 in data analytics/science

CMU Software Engineering Institute (SEI)

Bringing innovation to the U.S. government

- A Federally Funded Research and Development Center (FFRDC) chartered in 1984 and sponsored by the DoD
- Leader in researching complex software engineering, cyber security, and artificial intelligence (AI) engineering solutions
- Critical to the U.S. government's ability to acquire, develop, operate, and sustain software systems that are innovative, affordable, trustworthy, and enduring

The CERT Division: Birthplace of Cybersecurity

Trusted
Conducting research for the U.S. Government in a non-profit, public-private partnership

Valued
Collaborating with military, industry, and academia globally to innovate solutions

Relevant
Achieving technology and talent results for our mission partners

Risk Appetite

- How appetite fits into a program
- A brief discussion on governance
- Defining appetite
- Developing an appetite statement
  - Potential examples of an appetite statement

Risk Programs

Where do we begin building?

- There are three fundamental elements that underpin a risk program
  - **Governance** – A body that provides authority, advocacy, and a decision making
  - **Appetite** – A central understanding of risk attitude that provides quantitative constraints for analysis and prioritization
  - **Policy and Procedure** – Provides direction and tools needed

- Program development may only be necessary one time
  - Periodic update and maintenance accommodate organizational change

- Program should be tailored to meet scope and scale requirements

This Presentation is Scaled to Meet Customer Needs Starting with Executives Through Practitioner

Implementing Risk Appetite

Linked to Culture, Drives Decisions

ISO 31000:

"Amount and type of risk that an organization is prepared to pursue, retain or take."

"An organization's approach to assess, and eventually pursue, retain, take or turn away from risk."

Institute for Risk Management:

*"The amount and type of risk that an organization is willing to take in order to **meet their strategic objectives**."*

Tolerance is, "…the amount of risk an organization can actually cope with."

Risk Program Governance

Empowering Executives and Management to Manage Risk

- A tiered committee structure is effective
  - Tiers may include board level executives down through practitioners
  - Risks, decisions, and direction should flow up and down the tier structure
  - Each level communicates and relates through the use of an appetite statement

What Does the Governance Structure Do?

Each Tier Contributes to the Process

- Risks should flow freely across tiers to receive attention
- Risk appetite statement helps to determine the appropriate tier to address the correct order of magnitude risk
- Each tier in the structure must contribute value as a **decision making** body

Risk Appetite Statement

Quantify and Prioritize Risk

Why do we need it?

- Define how much risk is tolerable in pursuit of strategic objectives
- Appetite derives from the organization's inclination to seek or avoid risks
- Appetite statement assists in analyzing and prioritizing risks

Look at it this way:

- Organizational strategy is the highway to follow to achieve objectives
- Risk appetite is the guard rail

Developing a Risk Appetite
Practical Ideas on Building One

"*The risk appetite statement is generally considered the hardest part of any enterprise risk management implementation. However, without clearly defined, measurable tolerances the whole risk cycle and any risk framework is arguably at a halt.*"

- *Jill Douglas, Head of Risk, Charterhouse Risk Management*

- Senior management must provide input
- Strategy documents provide a starting point
- Categories come from stated strategic values
- Individual interviews are recommended
- Board should approve

Examples of Risk Appetite Statements

There is NO standard

- High level statements
  - "…do not take action that may degrade the value of the firm."

- Add clarity with categorization and possibly some quantification
  - "…do not take any operational action that may erode profits more than 10% per quarter."

- Make statement(s) concrete for decision makers
  - "…make capital investment that reduces the number unplanned outages to no more than 1 per quarter."

- Regardless of the type, the appetite should support strategic planning and day-to-day decision making

Linking to Appetite to Strategy

Making ERM part of corporate culture

- **Appetite must be aligned with strategy**
  - Categories aligned
  - Appetite should **provide a means to make decisions** that meet strategic objectives

- ERM appetite and process should support immediate tactical decisions as well as long term strategic ones

- Indication of maturity will come with regular use at various levels in the organization

Example of a Risk Appetite Statement

Quantitative and Functional

	Revenue (Operating Profit)	Safety	Operations	Reputation	Compliance	Human Capital	Projects
Escalate to Executive Attention	Any more than a 10% deviation from planned operating profit for a quarter	Loss of life or permanent disability	No more than three days of lost operations	Loss of market segment with multiple customers	Debarrment from a particular market segment linked to regulatory violation(s)	Any more than 5% high performer attrition from any business unit in a quarter	Liquidated damages that exceed contract value
Escalate to Management Attention	Any more than a 5% deviation from planned operating profit for a quarter	Time away or other reportable incident	No more than one day of lost operation	Loss of customer	Any fines or other penalties linked to regulatory violation(s)	Any more than 3% high performer attrition from any business unity in a quarter	Liquidated damages that erode the margin as sold
Provide Front Line Attention	Any deviations from planned operating profit for a quarter	Bumps, strains, bruises	No more than one shift of lost operation	Customer complaints or negative social media buzz	Any warnings linked to regulatory violation(s)	Any developing trend in high performer attrition	Minor disputes with limited contractual impact

Appetite May Also be Characterized by Likelihood, Adaptability, and Others

- Key is to prioritize risks based on defined criteria
- This is an example of an impact-based risk appetite statement
- Categories and values will differ depending upon the organization and its strategic goals

Example of a Risk Appetite Statement (continued)

Other Aspects of Risk May be Used to Gage Appetite

	Likelihood -- Probability of Risk Occuring
Executive Attention	Risk is between **75 - 99%** likely to occur. Alternatively, this risk has come to fruition within the industry within the past year.
Management Attention	Risk is between **30 - 74%** likely to occur. Alternatively, this risk has come to fruition within the industry within the past two years.
Front Line Attention	This risk is between **1 - 29%** likely to occur. Alternatively, the risk has come to fruition within the industry within the past 5 years.

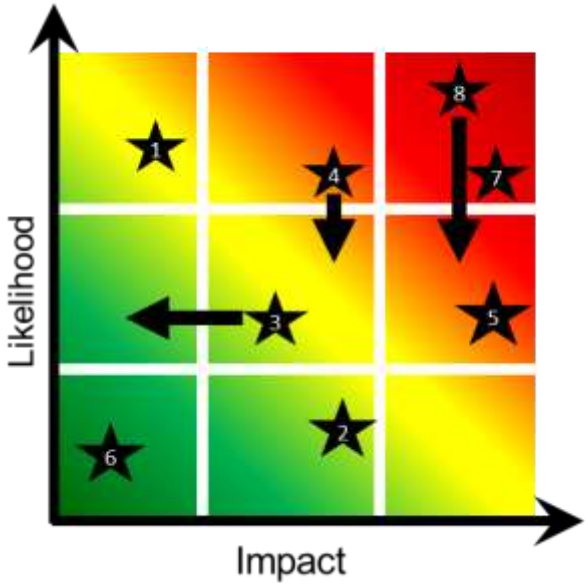
	Controllability - Progress in Responding to a Risk
Executive Attention	No funding provided -- No business case may exist to justify resource commitment
Management Attention	Funding provided and implementation of response plan in progress
Front Line Attention	Response plan implemented and effectiveness is being monitored

- These appetite statements may be coupled with the impact statement
- Values may differ per organization
- For likelihood, there is a difference between risk occurrence and impact realization
- Not all response plans must be acted upon, especially in a financially constrained environment

Example of Appetite Visualized

Heat Maps Provide Priority at a Glance

Projected residual risk index from inherent scores, With implemented responses



Number	Risk
1	Cyber Breach – Loss of PCI
2	Workforce Walkout
3	Debarment from a Market
4	Loss of Reputation
5	Deadly Safety Incident
6	Overregulation
7	Collapse of Economy
8	Regional Conflict

Contact Information

Presenter / Point of Contact
Brett Tucker
Technical Manager, Cyber Risk Management
Telephone: 412.268.6682
Email: batucker@cert.org