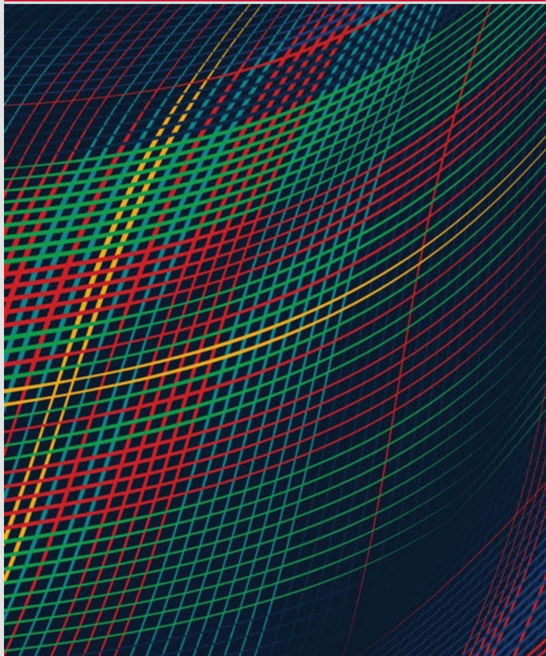
Carnegie Mellon University
Software Engineering Institute

# Cyber Risk Management: Program Development for Risk-Based Decision-Making

BRETT TUCKER, PMP, CSSBB, CISSP, CGRC

TECHNICAL MANAGER, CYBER RISK MANAGEMENT



The view, opinions, and/or findings contained in this material are those of the author(s) and should not be construed as an official Government position, policy, or decision, unless designated by other documentation.

DM25-0625

# Agenda

CERT Overview

Risk Program Considerations

- Governance
- Appetite
- Policy and Procedure

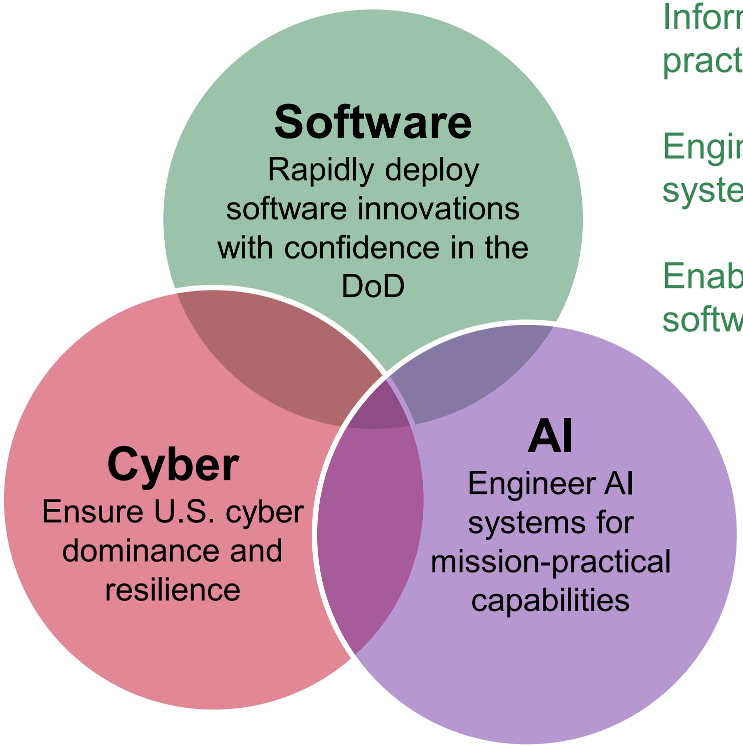
# Carnegie Mellon University (CMU) Software Engineering Institute (SEI)

*Source: https://www.sei.cmu.edu/about/*

**Bringing innovation to the U.S. government**

- A federally funded research and development center (FFRDC) chartered in 1984 and sponsored by the U.S. Department of Defense (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

# Our technical research connects software, AI, and cyber strategies for **maximum** impact



**Software**

Rapidly deploy software innovations with confidence in the DoD

**Cyber**

Ensure U.S. cyber dominance and resilience

**AI**

Engineer AI systems for mission-practical capabilities

*Source: Author's Own*

Inform DoD software policy and practice to accelerate acquisition

Engineer intelligent software systems

Enable DoD mission capability with software innovation

Advancing Cyber by Design

Enhancing Cyber Resilience

Moving the Market and Shaping the Future

AI for leap-ahead software engineering and cyber capabilities

Mature the discipline of AI engineering

Apply and integrate AI technologies in DoD and related mission capabilities

# CERT Division – Birthplace of Cyber Research

*Source: https://www.sei.cmu.edu/about/*

**Our Legacy and Today's Role in Shaping the Future:**

**1988**

Computer Emergency Response Team formed in response to the Morris Worm

**2022**

Cybersecurity Engineering and Resilience Team conducting collaborative and innovative evidence-based research to fortify the cyber ecosystem and protect national security and prosperity

**Why CERT Matters:**

**Trusted**

Conducting research for the U.S. government in a nonprofit, public-private partnership

**Valued**

Innovating solutions with a global collaboration of military, industry, and academia

**Relevant**

Achieving results for our mission partners

# The SEI is Engaged Broadly in Cyber Resilience and Risk Research and Delivery

**Vulnerability Analysis**

- Coordinated Vulnerability Disclosure
- Unified Extensible Firmware Interface (UEFI)

**Federal Civilian Agency Assessment**

- High Value Asset (HVA) Assessment
- Assessor Workbench

**Training Cyber Operators**

- President's Cup Cybersecurity Competition
- Assessment Evaluation and Standardization (AES)

**Network Situational Awareness/Threat Hunting**

- Network Traffic Analysis: SiLK, Mothra, YAF
- Unexpected Outbound Protocol (UNX-OBP)

**Risk Assessment**

- OCTAVE FORTE (Operationally Critical Threat, Asset, and Vulnerability Evaluation FOR The Enterprise) Appraisals
- FAIR Assessments
- CERT-RMM Risk Management

**Benchmarking Capabilities**

- Cyber Performance Goals (CPGs)
- Cyber Resilience Review/Analysis (CRR/CRA)
- External Dependencies Management (EDM)
- Energy Sector Cybersecurity Capability Maturity Model (C2M2)
- CERT Resilience Management Model (CERT-RMM)
- Tabletop Exercises (TTX)

**Identifying and Mitigating Insider Risk**

- Insider Threat Control Economics Framework
- NEAT (Networked Employee Assurance Tool)

**Cybersecurity Maturity Model Certification** (CMMC) steward for DoD Chief Information Officer

*Source: Author's Own*

# Overview of Risk Program Development

Carnegie Mellon University Software Engineering Institute

# Establish Risk Governance and Appetite

Three fundamental pillars of the risk organization is established:

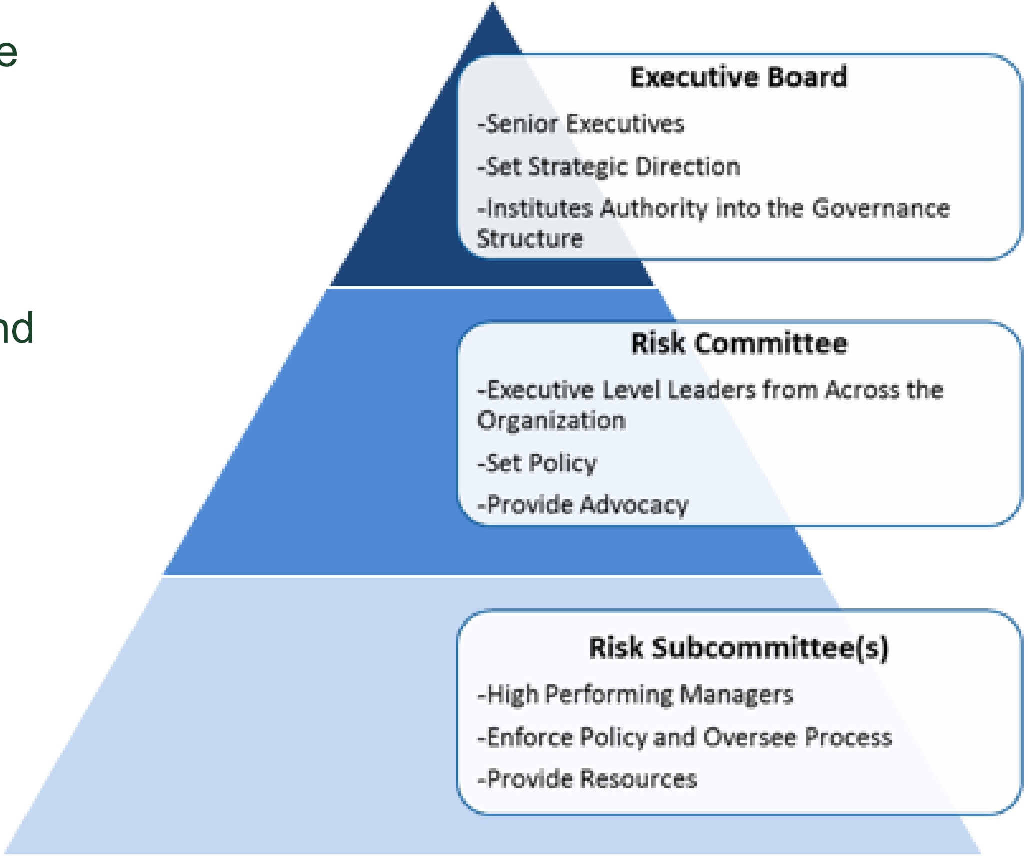
1. Governance
   - Who is making the risk-based decision?
   - Who provides resources and advocacy?
   - How is that done?
2. Appetite
   - At what level of the organization can risk decisions be made?
   - Provides a way to standardize assessment and action
3. Policy and Procedure
   - If it isn’t written down, will anyone ever do it?
   - Driving proper behaviors in the organization

# Risk Program Governance

## *Empowers Executives and Management to Manage Risk*

To make a tiered committee structure more effective:

- Use charters to set member duties, committee expectations, and goals
- Members should have access to and authority over resources
- Train members in enterprise risk management techniques



**Executive Board**

-Senior Executives

-Set Strategic Direction

-Institutes Authority into the Governance Structure

**Risk Committee**

-Executive Level Leaders from Across the Organization

-Set Policy

-Provide Advocacy

**Risk Subcommittee(s)**

-High Performing Managers

-Enforce Policy and Oversee Process

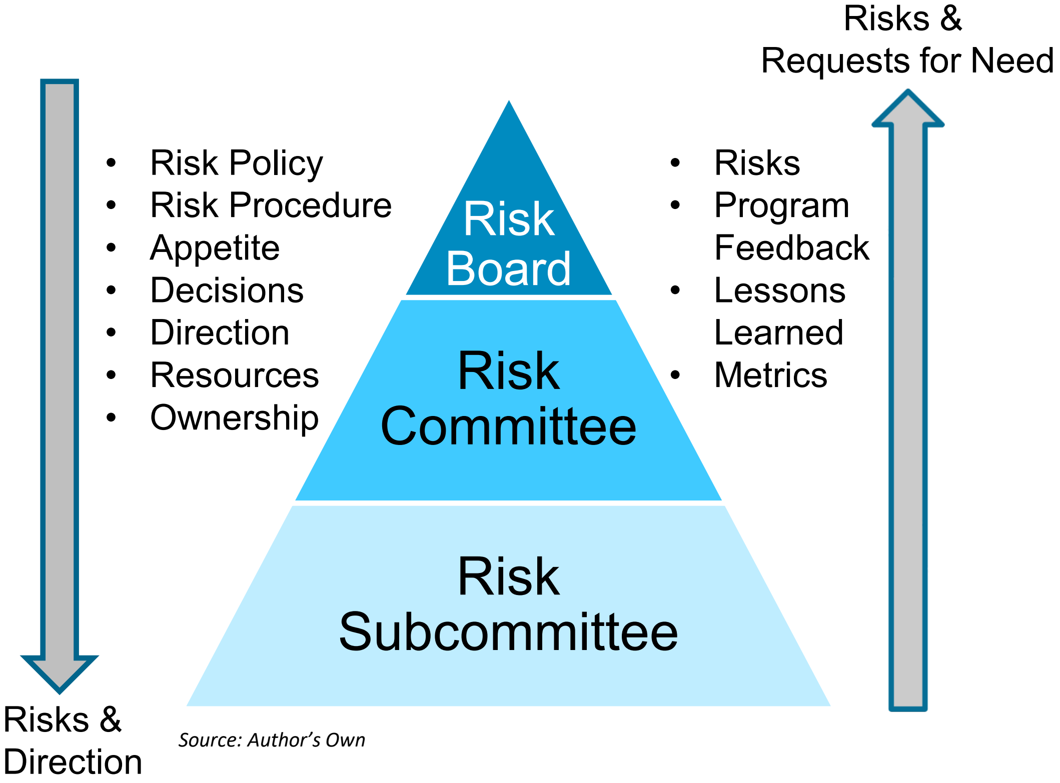
-Provide Resources

*Source: Author's Own*

[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution. Please see Copyright notice for non-US Government use and distribution.

# What does the governance structure do?

*Each Tier Focused on Decisive Action*



Risks & Requests for Need

- Risk Policy
- Risk Procedure
- Appetite
- Decisions
- Direction
- Resources
- Ownership

Risk Board

Risk Committee

Risk Subcommittee

- Risks
- Program Feedback
- Lessons Learned
- Metrics

Risks & Direction

*Source: Author's Own*

Risks are addressed at every tier

Distribute decision-making accountability using risk appetite documentation

Subcommittees segmented by categories, functions, geography, etc.

Each tier involved in all risk decisions but focuses efforts on its assigned risk areas

# 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**.”*

*“The amount of risk an organization can actually cope with.”*

# 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 particular 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

# 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 |

*Source: Author's Own*

***Appetite May Also Be Characterized by Likelihood, Adaptability, and Others***

# Example of a Risk Appetite Statement (continued)

## *Other Aspects of Risk May Be Used to Gauge Appetite*

| | **Likelihood -- Probability of Risk Occuring** |
|---|---|
| **Red - Executive Attention** | Risk is between **75 - 99%** likely to occur.  Alternatively, this risk has come to fruition within the industry within the past year. |
| **Yellow - 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. |
| **Green - 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** |
|---|---|
| **Red - Executive Attention** | No funding provided -- No business case may exist to justify resource commitment |
| **Yellow - Management Attention** | Funding provided and implementation of response plan in progress |
| **Green - Front Line Attention** | Response plan implemented and effectiveness is being monitored |

*Source: Author's Own*

# Policy and Procedure

*Will people follow an unwritten path?*

Key features to a strong policy statement:

- Simple to read and easy to follow
  - Use understanding of organization’s culture
- Enforceable Policies
  - Requires program owner
  - Specify procedure
  - Include implementation and change management plan
  - Provide audit team support
- Scalable in accordance with applicability
- Regularly review for update

# Starting Out With Scope and Charter to Develop Methodology

*Think Big… Marathon NOT a Sprint*

When defining the scope of the program, consider:

- Think about roles and responsibilities – RASCI?
- What are the goals of the program?

Start with the strategy of the business and link the program goals to meeting those objectives

Build the program in a scaled fashion with reasonable goals

- Evolution may follow a maturity model approach

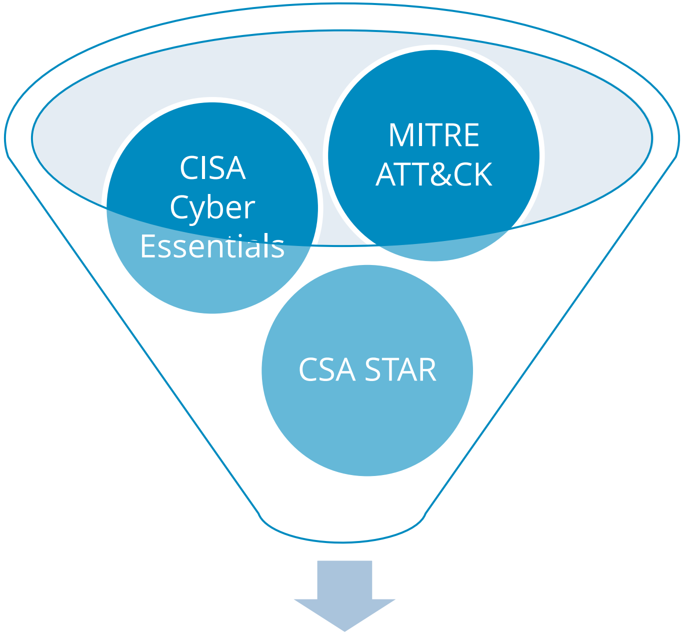
# Taking the Best From Several Places

Best practices must prevail:

- Diverse resources with varied focus helps
- Assessment may remain the same, but the solutions may not

Other sources of help exist:

- Trusted advisors
- Cyber insurance
- Other assessments



Tailored to Scope and Needs of the Customer Set

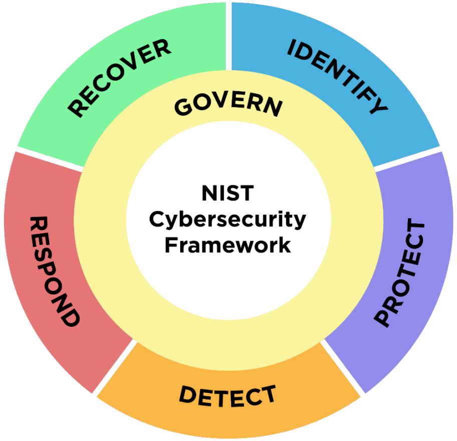
*Source: Author's Own*

# Given the Variety of Frameworks Available…

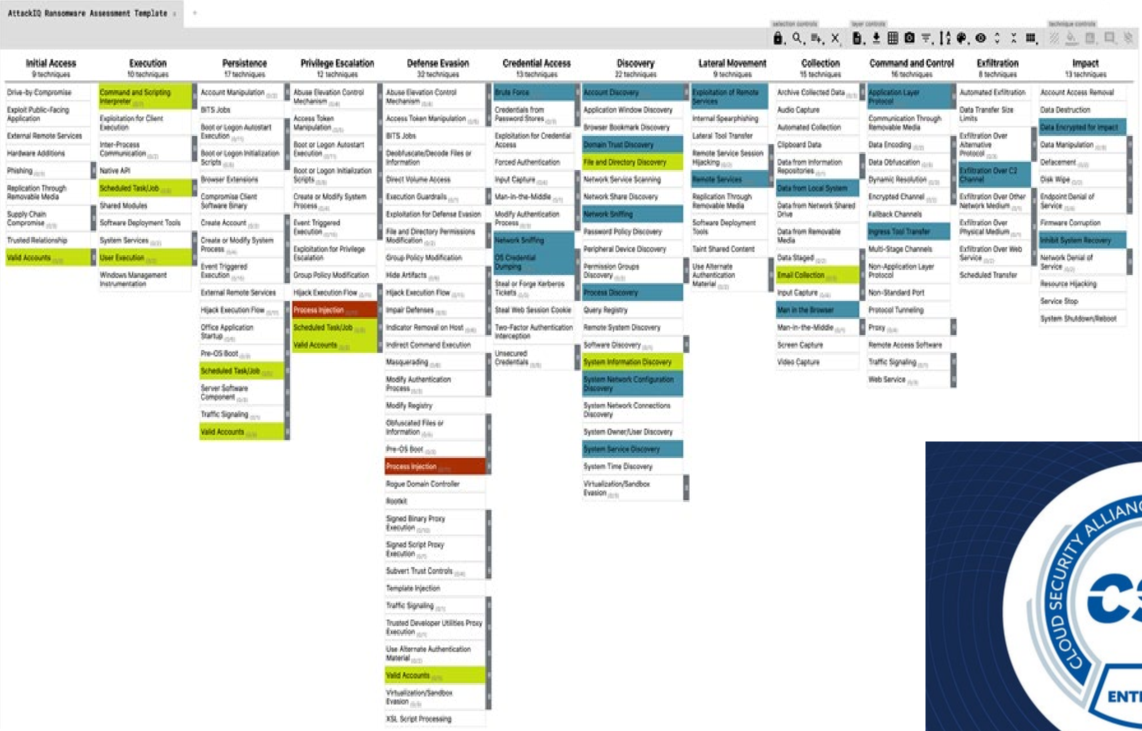
*What Qualities Should a Program Have?*

- Continuous process
- Aligns with strategic business objectives
- Accommodates all lines of the business
- Deliberate
- Measurable
- Auditable
- Easy to convey and understand
- Evolutionary
- Creates advocacy at senior levels of the organization
- Provides value
- Involves internal and external stakeholders

# You Are Not Alone:  Many Standards and References to Help



*https://www.nist.gov/news-events/news/2023/08/nist-drafts-major-update-its-widely-used-cybersecurity-framework*



AttackIQ Ransomware Assessment Template

| Initial Access<br>9 techniques | Execution<br>10 techniques | Persistence<br>17 techniques | Privilege Escalation<br>12 techniques | Defense Evasion<br>32 techniques | Credential Access<br>13 techniques | Discovery<br>22 techniques | Lateral Movement<br>9 techniques | Collection<br>15 techniques | Command and Control<br>16 techniques | Exfiltration<br>8 techniques | Impact<br>13 techniques |
|---|---|---|---|---|---|---|---|---|---|---|---|
| Drive-by Compromise | Command and Scripting Interpreter | Account Manipulation | Abuse Elevation Control Mechanism | Abuse Elevation Control Mechanism | Brute Force | Account Discovery | Exploitation of Remote Services | Archive Collected Data | Application Layer Protocol | Automated Exfiltration | Account Access Removal |
| Exploit Public-Facing Application | Exploitation for Client Execution | BITS Jobs | Access Token Manipulation | Access Token Manipulation | Credentials from Password Stores | Application Window Discovery | Internal Spearphishing | Audio Capture | Communication Through Removable Media | Data Transfer Size Limits | Data Destruction |
| External Remote Services | Inter-Process Communication | Boot or Logon Autostart Execution | Boot or Logon Autostart Execution | BITS Jobs | Exploitation for Credential Access | Browser Bookmark Discovery | Lateral Tool Transfer | Automated Collection | Data Encoding | Exfiltration Over Alternative Protocol | Data Encrypted for Impact |
| Hardware Additions | Native API | Boot or Logon Initialization Scripts | Boot or Logon Initialization Scripts | Deobfuscate/Decode Files or Information | Forced Authentication | Domain Trust Discovery | Remote Service Session Hijacking | Clipboard Data | Data Obfuscation | Exfiltration Over C2 Channel | Data Manipulation |
| Phishing | Scheduled Task/Job | Browser Extensions | Create or Modify System Process | Direct Volume Access | Input Capture | File and Directory Discovery | Remote Services | Data from Information Repositories | Dynamic Resolution | Exfiltration Over Other Network Medium | Defacement |
| Replication Through Removable Media | Shared Modules | Compromise Client Software Binary | Event Triggered Execution | Execution Guardrails | Man-in-the-Middle | Network Service Scanning | Replication Through Removable Media | Data from Local System | Encrypted Channel | Exfiltration Over Physical Medium | Disk Wipe |
| Supply Chain Compromise | Software Deployment Tools | Create Account | Exploitation for Privilege Escalation | Exploitation for Defense Evasion | Modify Authentication Process | Network Share Discovery | Software Deployment Tools | Data from Network Shared Drive | Fallback Channels | Exfiltration Over Web Service | Endpoint Denial of Service |
| Trusted Relationship | System Services | Create or Modify System Process | Group Policy Modification | File and Directory Permissions Modification | Network Sniffing | Network Sniffing | Taint Shared Content | Data from Removable Media | Ingress Tool Transfer | Scheduled Transfer | Firmware Corruption |
| Valid Accounts | User Execution | Event Triggered Execution | Hijack Execution Flow | Group Policy Modification | OS Credential Dumping | Password Policy Discovery | Use Alternate Authentication Material | Data Staged | Multi-Stage Channels |  | Inhibit System Recovery |
|  | Windows Management Instrumentation | External Remote Services | Process Injection | Hide Artifacts | Steal or Forge Kerberos Tickets | Peripheral Device Discovery |  | Email Collection | Non-Application Layer Protocol |  | Network Denial of Service |
|  |  | Hijack Execution Flow | Scheduled Task/Job | Hijack Execution Flow | Steal Web Session Cookie | Permission Groups Discovery |  | Input Capture | Non-Standard Port |  | Resource Hijacking |
|  |  | Office Application Startup | Valid Accounts | Impair Defenses | Two-Factor Authentication Interception | Process Discovery |  | Man in the Browser | Protocol Tunneling |  | Service Stop |
|  |  | Pre-OS Boot |  | Indicator Removal on Host | Unsecured Credentials | Query Registry |  | Man-in-the-Middle | Proxy |  | System Shutdown/Reboot |
|  |  | Scheduled Task/Job |  | Indirect Command Execution |  | Remote System Discovery |  | Screen Capture | Remote Access Software |  |  |
|  |  | Server Software Component |  | Masquerading |  | Software Discovery |  | Video Capture | Traffic Signaling |  |  |
|  |  | Traffic Signaling |  | Modify Authentication Process |  | System Information Discovery |  |  | Web Service |  |  |
|  |  | Valid Accounts |  | Modify Registry |  | System Network Configuration Discovery |  |  |  |  |  |
|  |  |  |  | Obfuscated Files or Information |  | System Network Connections Discovery |  |  |  |  |  |
|  |  |  |  | Pre-OS Boot |  | System Owner/User Discovery |  |  |  |  |  |
|  |  |  |  | Process Injection |  | System Service Discovery |  |  |  |  |  |
|  |  |  |  | Rogue Domain Controller |  | System Time Discovery |  |  |  |  |  |
|  |  |  |  | Rootkit |  | Virtualization/Sandbox Evasion |  |  |  |  |  |
|  |  |  |  | Signed Binary Proxy Execution |  |  |  |  |  |  |  |
|  |  |  |  | Signed Script Proxy Execution |  |  |  |  |  |  |  |
|  |  |  |  | Subvert Trust Controls |  |  |  |  |  |  |  |
|  |  |  |  | Template Injection |  |  |  |  |  |  |  |
|  |  |  |  | Traffic Signaling |  |  |  |  |  |  |  |
|  |  |  |  | Trusted Developer Utilities Proxy Execution |  |  |  |  |  |  |  |
|  |  |  |  | Use Alternate Authentication Material |  |  |  |  |  |  |  |
|  |  |  |  | Valid Accounts |  |  |  |  |  |  |  |
|  |  |  |  | Virtualization/Sandbox Evasion |  |  |  |  |  |  |  |
|  |  |  |  | XSL Script Processing |  |  |  |  |  |  |  |

*Source: https://attack.mitre.org/resources/attack-data-and-tools/*

*Source: https://circle.cloudsecurityalliance.org/faqs/about-membership*

# Selection of the Appropriate Framework

*Organizations Learn How to Implement a Risk Program*

Things to remember in setting selection objectives:

- Establish a framework that scales to the size and strategy of the organization
  - Do not be afraid to use a patchwork of several
- Educate the workforce on process, tools, and programmatic features
- All frameworks will require facilitation for risk program development

Some principles to consider:

- Comprehensive enough to cover the enterprise
- Assessment for prioritization is essential given limited resources
- Process should be broadly applicable and easy to implement by most analysts regardless of expertise or background

# Suggestions for Risk Standard Selection

Understand the standards:

- Know the difference between standards and frameworks
- Standards are acceptable way of doing something—compliance
- Frameworks working guide to be adapted to how to do—not compulsory

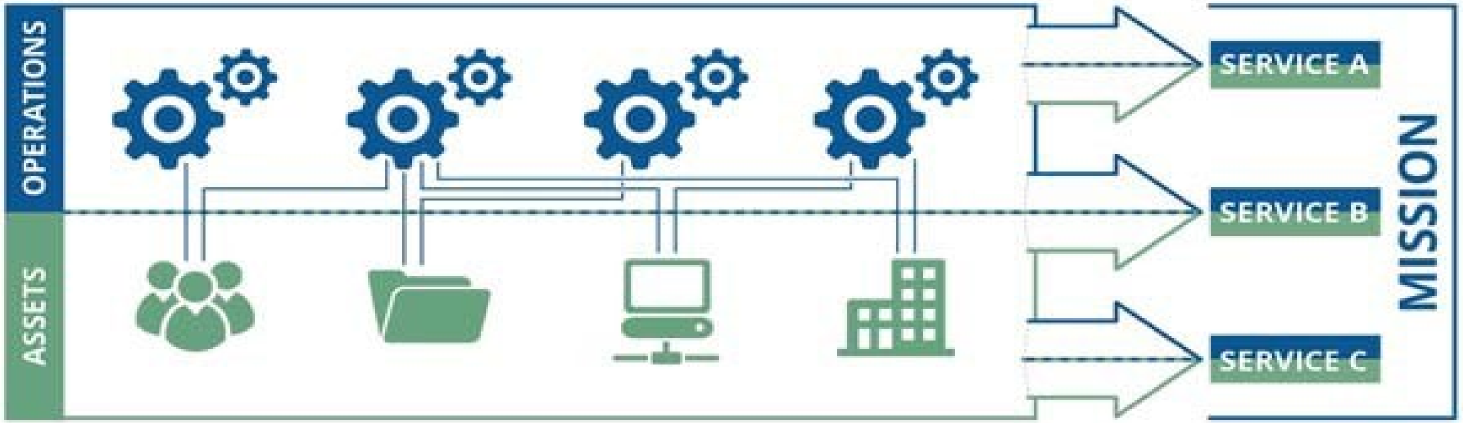
Recognize the diverse types of risk management standards:

- The number and variety benefit many industries and organizations all at once

Define the criteria to be used for selection:

- May consider organizational industry, size, culture, and regulation

# Link Cybersecurity to Business Objectives



*Source: Author's Own*

**People**:  those who operate and monitor the service

**Information**:  data associated with the service

**Technology**:  tools and equipment that automate and support the service

**Facilities**:  where the service is performed

**External Dependencies**:  value gained from relationships/supply chain

**!** **Assets derive their value from their importance in meeting the service mission.**

# Key Takeaways in Summary

Prioritize:

- Set priorities and remember that if everything is the priority, then nothing is a priority.
- Not all threats, vulnerabilities, and assets are equal—analyze and measure where possible.
- Select the most cost-effective controls to conserve resources.
- Strategies vary based upon confidentiality, integrity, and availability.

Specialize:

- Know your enemy and your environment.
- Target high-frequency vectors like spear phishing and ransomware.
- Tailor your security program to your organizational strategy.
- Demand an implementation roadmap.

# Contact Us

*Source: CMU SEI*

**Carnegie Mellon University**
Software Engineering Institute
4500 Fifth Avenue
Pittsburgh, PA 15213
888-201-4479
info@sei.cmu.edu
www.sei.cmu.edu

**Brett Tucker, PMP, CSSBB, CISSP, CGRC**
Technical Manager, Cyber Risk Management
412.268.6682
batucker@cert.org

# Discover more about our research at sei.cmu.edu

*Source: https://www.sei.cmu.edu/about/*

Download software and tools
Participate in education offerings
Attend an event
Search the digital library
Read the SEI Year in Review
Explore our research and capabilities
Collaborate with the SEI on a new project

**Carnegie Mellon University**
Software Engineering Institute
4500 Fifth Avenue
Pittsburgh, PA 15213
info@sei.cmu.edu

**Brett Tucker, PMP, CSSBB, CISSP, CGRC**
Technical Manager, Cyber Risk Management
batucker@cert.org