CISA CPG Research

July 2023

Software Engineering Institute

Software Engineering Institute
Carnegie Mellon University
Pittsburgh, PA 15213

[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution.

Copyright 2023 Carnegie Mellon University.

This material is based upon work funded and supported by the Department of Homeland Security 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 sponsored by the United States Department of Defense.

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.

NO WARRANTY. THIS CARNEGIE MELLON UNIVERSITY AND SOFTWARE ENGINEERING INSTITUTE MATERIAL IS FURNISHED ON AN "AS-IS" BASIS. CARNEGIE MELLON UNIVERSITY MAKES NO WARRANTIES OF ANY KIND, EITHER EXPRESSED OR IMPLIED, AS TO ANY MATTER INCLUDING, BUT NOT LIMITED TO, WARRANTY OF FITNESS FOR PURPOSE OR MERCHANTABILITY, EXCLUSIVITY, OR RESULTS OBTAINED FROM USE OF THE MATERIAL. CARNEGIE MELLON UNIVERSITY DOES NOT MAKE ANY WARRANTY OF ANY KIND WITH RESPECT TO FREEDOM FROM PATENT, TRADEMARK, OR COPYRIGHT INFRINGEMENT.

[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.

This material may be reproduced in its entirety, without modification, and freely distributed in written or electronic form without requesting formal permission. Permission is required for any other use. Requests for permission should be directed to the Software Engineering Institute at permission@sei.cmu.edu.

Carnegie Mellon®, CERT®, CERT Coordination Center® and OCTAVE® are registered in the U.S. Patent and Trademark Office by Carnegie Mellon University.

DM23-0692

Agenda

1. Background
2. Project Objectives
3. CPG Tasks
4. Initial Development Efforts
5. Deliverables

© 2023 Carnegie Mellon University

[DISTRIBUTION STATEMENT A] Approved for public release and unlimited distribution.

Introduction – CPG Background

The cross-sector CPGs are a prioritized subset cybersecurity practices that critical infrastructure owners and operators may voluntarily implement to meaningfully reduce the likelihood and impact of known risks. CPGs are a common set of fundamental cybersecurity practices, which will specially help small- and medium-sized organizations kickstart their cybersecurity efforts.

CISA has the lead role in promoting CPG usage, analysis of CPG assessment data, and providing reporting on the impact of CPG usage to improve national cybersecurity outcomes.

© 2023 Carnegie Mellon University
[DISTRIBUTION STATEMENT A] Approved for public release and unlimited distribution.

CISA CPGs Promise to Deliver

The community is excited about CPG application in terms of:

- Establishing baseline practices to reduce risk exposure
- Benchmarking for improved maturity
- Prioritizing security practices
- May lead to a greater understanding of aggregate risk to the nation

Challenges for community acceptance may include:

- Currently voluntary
- **Estimates of cost, complexity, and impact provided**
- Approaches for quantification may vary based on context

© 2023 Carnegie Mellon University

[DISTRIBUTION STATEMENT A] Approved for public release and unlimited distribution.

Objectives of Project

SEI will work to further evolve the CISA CPGs, into holistic cyber-security ratings, establishing direct definition and means of measurement for the complexity, cost and impact ratings associated with CPGs. These efforts will clarify the benefits of CPGs and may include methodology development, identification of data sets, and possible testing to validate the ratings provided.

Tasks

1. Quantification
2. CPG/SSG Progress Factors
3. Cyber Resilience Review (CRR)

© 2023 Carnegie Mellon University
[DISTRIBUTION STATEMENT A] Approved for public release and unlimited distribution.

Task 1 - Quantification

CISA will support further efforts to prioritize CPG and Sector Specific Goals (SSG) goals based on projected Cost, Impact, and Complexity.

Foundational Activities

CPG cost, complexity, and impact will be defined and quantified to support fact-based prioritization and promote good decision making. SEI will develop a risk quantification function, that considers key factors such as Cost, Complexity, and Impact to support prioritization of CPG initiatives to mitigate the top cyber risks.

© 2023 Carnegie Mellon University
[DISTRIBUTION STATEMENT A] Approved for public release and unlimited distribution.

Task 2 – CPG/SSG Progress Factors

SEI will develop guidance for assessing implementation of the CPG capabilities at the levels of: Not Started, Scoped, In Progress, Implemented. SEI will develop general guidance applicable to implementation for all CPG goals, as well as detailed guidance on assessing implementation levels for each of the CPG goals. This will assist organizations to understand and self-assess their progress towards meeting CPG/SSGs.

Foundational Activities

Progress factors will have associated questions that assess whether minimum standards of implementation for each goal are being met.

© 2023 Carnegie Mellon University

[DISTRIBUTION STATEMENT A] Approved for public release and unlimited distribution.

Task 3 – Cyber Resilience Review (CRR)

SEI will recommend one set of foundational maturity model-based security controls/practices supporting the CPG. This will help organizations understand how to progress towards meeting performance CPG Goals.

Foundational Activities

The SEI will analyze the CPG baseline in comparison to the existing base practices and maturity model within the CRR and CMMC Level 1 Cybersecurity Framework and propose an appropriate set of foundational USG security controls/baseline to support the CPG.

The SEI will analyze practices and maturity model within existing frameworks (e.g., CSF v2, CMMC Level 3 Cybersecurity Framework, VADR) in comparison to the existing CRR and propose a selection of USG security controls/guidance for a “CPG for Cyber Resilience” methodology (CPG-CRR). The SEI will incorporate the CPG implementation levels into the CPG-CRR.

The SEI will provide guidance on prioritizing new and unique additional goals to CPG-CRR.

© 2023 Carnegie Mellon University
[DISTRIBUTION STATEMENT A] Approved for public release and unlimited distribution.

Initial Efforts

Task 1 - Quantification

- Define each of the measures of CPG performance (as well as quantification measures) to include complexity, impact, and cost

Task 2 - CPG/SSG Progress Factors

- Develop general guidance for assessing implementation of the CPG capabilities at the levels of: Not Started, Scoped, In Progress, Implemented.
- Deliverables due in December 2023

Task 3 - Cyber Resilience Review (CRR)

- Develop cross-walk from CPG baseline to CRR questionnaire.
- Identify gaps in questionnaire to support a CPG-CRR

© 2023 Carnegie Mellon University
[DISTRIBUTION STATEMENT A] Approved for public release and unlimited distribution.

Deliverables – Task 1

- **Define** each of the measures of CPG performance to include complexity, impact, and cost.
- Identify and **document potential data sources** that may provide basis of calculation for the complexity, impact and cost measures.
- Conduct research and **draft findings** for novel means to understand "complexity" within the context of the CISA CPGs with consideration of:
  - Complexity of control implementation
  - Complexity of control use
- Conduct research and **draft findings** for novel means to understand "impact" within the context of the CISA CPGs with consideration of:
  - Efficacy of controls
  - Impact of use in terms of burden on the organization
- Conduct research and **draft findings** for novel means to understand "cost" within the context of the CISA CPGs with consideration of:
  - Cost of procurement
  - Cost of implementation
  - Cost of maintenance
- **Document** CPG complexity, impact and cost **findings** and define **metric** for measurement

© 2023 Carnegie Mellon University
[DISTRIBUTION STATEMENT A] Approved for public release and unlimited distribution.

Deliverables – Tasks 2 and 3

Task 2

- **Define** progress factors and associated measures of CPG goal implementation.
- Identify and **document potential data sources** for assessing goal implementation.
- **Document** alignment of CPG **progress factors** to implementation levels and cross walk to a question set.
- **Develop CPG scoring plan** to document quantification process -cybersecurity posture and prioritization of risk factors to buy down risk.
- **Develop strategy plan** for long term maintenance and analysis

Task 3

- **Document** CPG Baseline Updates
- **Document** "CPG - Cyber Resilience Review"
- Document Prioritization guidance for new and unique additional goals to CPG-CRR.

© 2023 Carnegie Mellon University
[DISTRIBUTION STATEMENT A] Approved for public release and unlimited distribution.

Initial Development Efforts

© 2023 Carnegie Mellon University

[DISTRIBUTION STATEMENT A] Approved for public release and unlimited distribution.

Definition: Complexity

Complexity – condition of cybersecurity that inhibits strategic objectives at the organizational level.

- We recognize that this could also mean impacting tactical performance as well.
- Does CISA agree that complexity could be a balance between good and bad?
  - Is there fundamental agreement that some complexity is necessary?
  - If so, the math must give credit as much as deduction – identify the tipping point

Context Greatly Influences Each of the Measures

© 2023 Carnegie Mellon University
[DISTRIBUTION STATEMENT A] Approved for public release and unlimited distribution.

Definition: Cost

Cost – the resources necessary to implement, maintain, and eventually dispose of a performance goal

- Can we leverage current Treasury work?
  - Focuses on BIA for loss, but provides good decomposition of costs if practices not followed – possible determination of return on risk investment
  - Cost is based upon a significant number of factors:
    - Procurement of control(s)
    - Hiring and/or training of personnel
    - Maintenance of technology and/or proficiency
    - Burden on the greater organization, and not just the CISO support team
    - Disposal and/or transition to new technologies
  - These base factors may be amplified with **"multipliers" that provide bias** for context
    - Number of employees in an organization
    - Gradient in necessary skill sets and knowledge
    - Lifecycle of practice
    - Degree of implementation

© 2023 Carnegie Mellon University
[DISTRIBUTION STATEMENT A] Approved for public release and unlimited distribution.

Potential Sources of Information

Cost

- Survey of commercial off the shelf tools, cybersecurity professional average salaries, and other related factors would provide quantified ranges of control costs
  - Total cost that spans the life of the control should be considered to enable organizational asset planning and management

- Improved cost estimates may inform procurement planning and prioritization

© 2023 Carnegie Mellon University
[DISTRIBUTION STATEMENT A] Approved for public release and unlimited distribution.

Definition: Impact

Impact – each performance goal should yield a degree of effect that either protects the organization or increases its resilience.

- Should we consider negative impacts of goals?
  - This may be covered by the complexity factor
  - Looks at performance goals on a time continuum
    - Impact could be low upon initial implementation
    - Impact increases over time given proper advocacy and use
    - Impact may decline with advent of new threat actor tactics and techniques

© 2023 Carnegie Mellon University
[DISTRIBUTION STATEMENT A] Approved for public release and unlimited distribution.

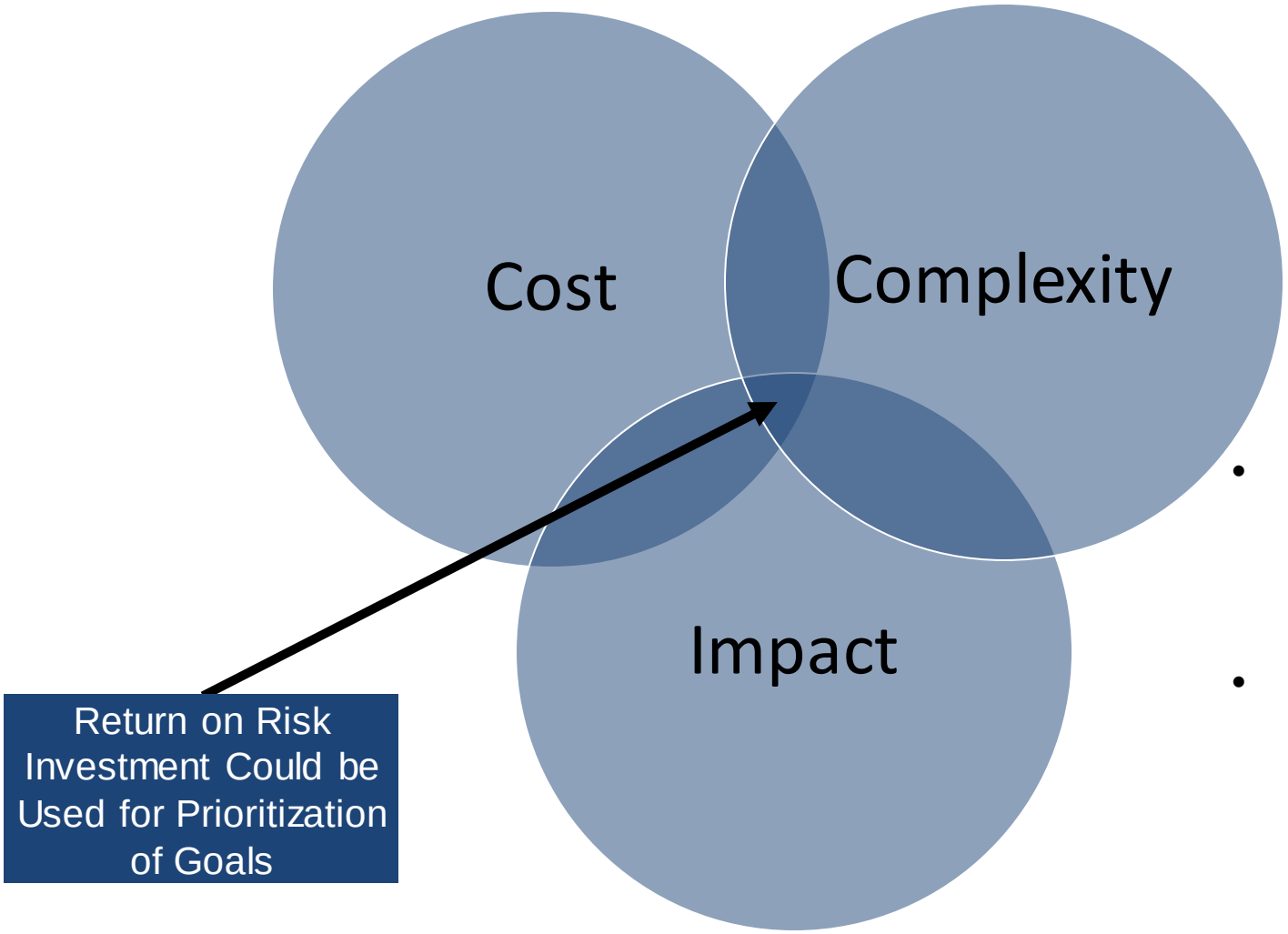
Additional on Quantification of Impact

Impacts

- Several frameworks and methodologies exist for quantifying risk impacts, yet few help with control efficacy
- For the CPG framework, the means of measure for impact may vary from specific goal to specific goal.
- Must consider primary impacts as well as secondary
  - Various response strategies suggested by the CPGs may overlap or amplify each other
  - For example, 7.2 Incident Response Plans may be enhanced with 4.3 and 4..4 Cybersecurity Training

© 2023 Carnegie Mellon University
[DISTRIBUTION STATEMENT A] Approved for public release and unlimited distribution.

Convergence of Measures in Each Goal



- Do these fluctuate based upon each goal?
- Are there goals without overlap?

© 2023 Carnegie Mellon University
[DISTRIBUTION STATEMENT A] Approved for public release and unlimited distribution.

Discussion

© 2023 Carnegie Mellon University

[DISTRIBUTION STATEMENT A] Approved for public release and unlimited distribution.

Quantification Raises Confidence

Quantification of **cost, complexity, and impact** would make the CPG framework more robust

- Of the **36 sub-elements distributed over the 7 process areas**, a uniform standard of measurement would provide:
  - Consistent basis for analysis
  - Equivalent comparison that enables prioritization of resources

Proposed Approach Throughout the Project:

1. **Define** each metric explicitly to include means of measurement
2. **Establish a scoring scheme** that aligns measures with current scale
3. **Benchmark** scoring with existing industry best practices
4. Periodically refine and **update** scores with evolution of TTPs and technology

© 2023 Carnegie Mellon University
[DISTRIBUTION STATEMENT A] Approved for public release and unlimited distribution.

Potential Cost Approach Use Case Example

The Cost score should include initial investment in procurement, install, and training

Establish Scoring Scheme – notional tolerance bands could include

- $ = less than $100K
- $$ = $100K - $1M
- $$$ = $1M - $10M
- $$$$ = greater than $10M

These values may scale to context of the organization.

Benchmark – survey top three off the shelf solutions across at least three sectors

- How do we determine the "top" products or "practices"?
- Must think through goals that do not rely heavily on technology tools.

Update – periodic updates plus specific circumstances that would require update

© 2023 Carnegie Mellon University
[DISTRIBUTION STATEMENT A] Approved for public release and unlimited distribution.

Potential Impact Approach Use Case Example

Impact score includes consideration of control effect compared to potential loss

Establish Scoring Scheme – notional tolerance bands could include

- High – No more than 4 hours of operational downtime per year
- Medium – Between 4 – 24 hours of downtime per year
- Low – Greater than 24 hours of downtime despite practice in place

These values may scale to risk appetite of the organization.

Benchmark – examples for sources of information may include survey of sector SOCs for downtime despite practice(s) in place

Update – periodic updates plus specific circumstances that would require update

© 2023 Carnegie Mellon University
[DISTRIBUTION STATEMENT A] Approved for public release and unlimited distribution.

Complexity Approach Use Case Example

Complexity score may include consideration of system burden despite practice implementation, ease of implementation, and potential for errors (e.g., Tech debt, configuration, etc.)

Establish Scoring Scheme – notional tolerance bands could include

- High – Implementation could take up to a year or more
- Medium – Implementation could take up to 6 months to a year
- Low – Less than 6 months to implement

Benchmark – could compare with other analogous system implementation efforts?

Update – periodic updates plus specific circumstances that would require update

© 2023 Carnegie Mellon University
[DISTRIBUTION STATEMENT A] Approved for public release and unlimited distribution.

Additional Considerations

SEI recognizes that this project may result in a process or methodology for measuring cost, impact, and complexity for organizations.

- Consistent practice may reveal best practices to be adopted by all
- CISA may gain better appreciation for risk appetite across critical infrastructure sectors

CISA may identify some practices to be more desired in some sectors over others depending on how they are scored with this approach.

© 2023 Carnegie Mellon University
[DISTRIBUTION STATEMENT A] Approved for public release and unlimited distribution.

Decomposing Cybersecurity Complexity

The cybersecurity stack of any organization has many diverse elements.

These elements may be contributing in part or in tandem to create a complex ecosystem.

An optimal balance is necessary to deliver value to the organization.

Some elements may be “cross-cutting”.

Cross cutting considerations include:

- **Supply Chain**
- **Resource Constraints**

© 2023 Carnegie Mellon University
[DISTRIBUTION STATEMENT A] Approved for public release and unlimited distribution.

Index Will Come from an Integration of Parts

The three elements will each yield a quantitative measure.

- **Additional research needed** to determine the validity of the math.
- **Data sets or model systems must be identified** or built to validate the complexity index model.
- Other elements may be identified as the model evolves.
- **Weighting factors** may be a significant consideration as understanding evolves.

$$S_i = \sum_{j=1}^{n} S_{ij} W_j$$

- $S_i = CPG\ measurement\ for$ "i" elements
- $S_{ij} = the\ score\ of\ the\ ith\ element\ on\ the\ jth\ criterion$
- $W_j = the\ weight\ of\ the\ jth\ criterion$

© 2023 Carnegie Mellon University
[DISTRIBUTION STATEMENT A] Approved for public release and unlimited distribution.