Structured Cyber Resiliency Analysis Methodology (SCRAM)

Deborah Bodeau, dbodeau@mitre.org
Richard Graubart, rdg@mitre.org
The MITRE Corporation

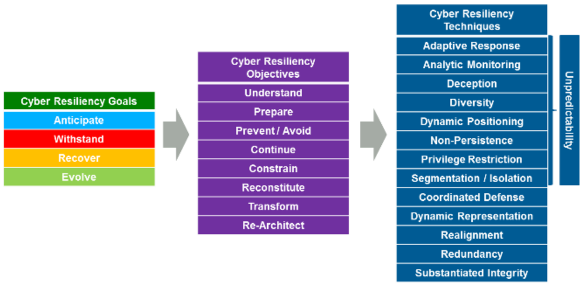
Abstract: The Structured Cyber Resiliency Analysis Methodology (SCRAM) defines processes, supported by such resources as frameworks and models, value scales, and datasets, that can be used to perform cyber resiliency analyses (CRAs) with varying scopes and purposes, at different points in the lifecycle of a system, system-of-systems (SoS), or mission. SCRAM uses MITRE's Cyber Resiliency Engineering Framework (CREF) as a common structuring mechanism, enabling results of CRAs under different circumstances to be compared or used together. This paper presents a high-level description of SCRAM, and identifies some representative resources.

Introduction

Cyber resiliency can be defined as "the ability to anticipate, withstand, recover from, and adapt to adverse conditions, stresses, attacks, or compromises on cyber resources." Cyber resiliency is increasingly a concern for systems, missions (and the systems-of-systems that support them), organizations, and critical infrastructure sectors. A wide range of stakeholders – including Program Managers (PMs), Program Executive Offices (PEOs), mission owners, cyber defenders, and Authorizing Officials (AOs) – seek to learn whether the cyber resources for which they are responsible or on which they depend are sufficiently resilient against advanced cyber threats to meet mission needs and, if not, what can be done to improve cyber resiliency. The Structured Cyber Resiliency Analysis Methodology (SCRAM) provides a way to answer questions about cyber resiliency.

SCRAM builds on and extends prior work on architectural assessment of cyber resiliency [1] [2] and analytic measurement of resilience [3] [4], and experience applying these to systems in different phases of the system development lifecycle (SDLC) or acquisition lifecycle (ALC) [5]. The types of systems, missions, and SoS about which cyber resiliency questions can be posed vary widely. Therefore, SCRAM is designed to be highly tailorable. Examples of specific applications of SCRAM include a cyber resiliency component of an Analysis of Alternatives (AoA), a CRA of an operational environment such as a data center, an architectural analysis, and a cyber resiliency component of a cybersecurity risk analysis.

The form in which the results of a CRA are presented can range from a "Top Ten" list or a color-coded scorecard to a detailed report. In addition to its final results, a CRA involves the development of intermediate artifacts (e.g., lists, spreadsheets, diagrams, threat scenarios) which can be used in other activities throughout the ALC. In particular, CRA artifacts can serve as inputs to or supporting documentation for artifacts produced as a program applies the Risk Management Framework (RMF). Because SCRAM uses the Cyber Resiliency Engineering Framework (CREF) as a foundational structuring mechanism, the various types of CRA and forms of

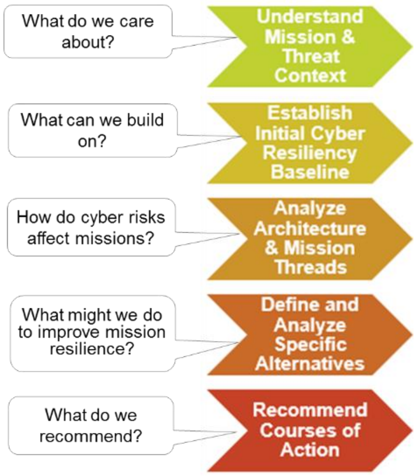


results share a common set of concepts, terminology, and analytic approaches, facilitating reuse and consistence.

This white paper presents a high-level description of SCRAM, and identifies representative resources that could be used to support specific activities in a CRA. Cyber resiliency analysis can be integrated into – or made an aspect of – different forms of analysis or assessment [6], including for example security risk assessment as defined in NIST SP 800-30 [7] or analytic processes in systems security engineering (SSE) [8]. In particular, CRA can be integrated with the steps in the Risk Management Framework (RMF) [9] throughout the ALC [10]. This document describes the SCRAM process, initially at a high level. Subsequent sections revisit the SCRAM steps again, each in more detail. Examples of sources of information, lifecycle processes, and roles are drawn from the DoD ALC; however, SCRAM is sufficiently general that it can be applied to any organization.

SCRAM Process Overview

The figure at right illustrates the general process for a cyber resiliency analysis. It consists of five steps, each intended to answer a specific question related to the process.


What do we care about?
Understand Mission & Threat Context
What can we build on?
Establish Initial Cyber Resiliency Baseline
How do cyber risks affect missions?
Analyze Architecture & Mission Threads
What might we do to improve mission resilience?
Define and Analyze Specific Alternatives
What do we recommend?
Recommend Courses of Action

- *What do we care about?* This step establishes the purpose of the CRA. Those performing the CRA and the stakeholders who will use the results of the CRA establish a common understanding of the mission and threat context, agree on what information will be provided to analysts, as well as what will be assumed, and identify factors that constrain the selection of cyber resiliency techniques.
- *What can we build on?* Cyber resiliency techniques overlap with or leverage techniques for cybersecurity, survivability, continuity of operations planning (COOP), and reliability, maintainability, and availability (RMA). Activities in this step establish a baseline assessment of the system, which includes capabilities which have already been built in and which, if used in a way that takes malicious cyber activities into consideration, could enhance cyber resiliency.
- *How do cyber risks affect mission risks?* Cybersecurity techniques – designed to ensure confidentiality, integrity, and availability, or to enable cyber defenders to protect against, detect, and respond to cyber attacks effectively – are intended to reduce cyber risks. Cyber risks are an increasingly significant contributor to mission risks. Activities in this step look at the mission architecture (including system architectures as well as mission threads) to identify how advanced cyber adversaries, by taking advantage of architectural and design decisions and affecting mission-critical resources, could impair mission effectiveness.
- *What might we do to improve mission resilience?* A wide variety of cyber resiliency techniques, expressed as design principles and realized by implementing specific approaches and technologies, can be identified. Some of these will not be feasible in the context for which the CRA is performed. Activities in this step identify and analyze specific alternatives for improving cyber resiliency.

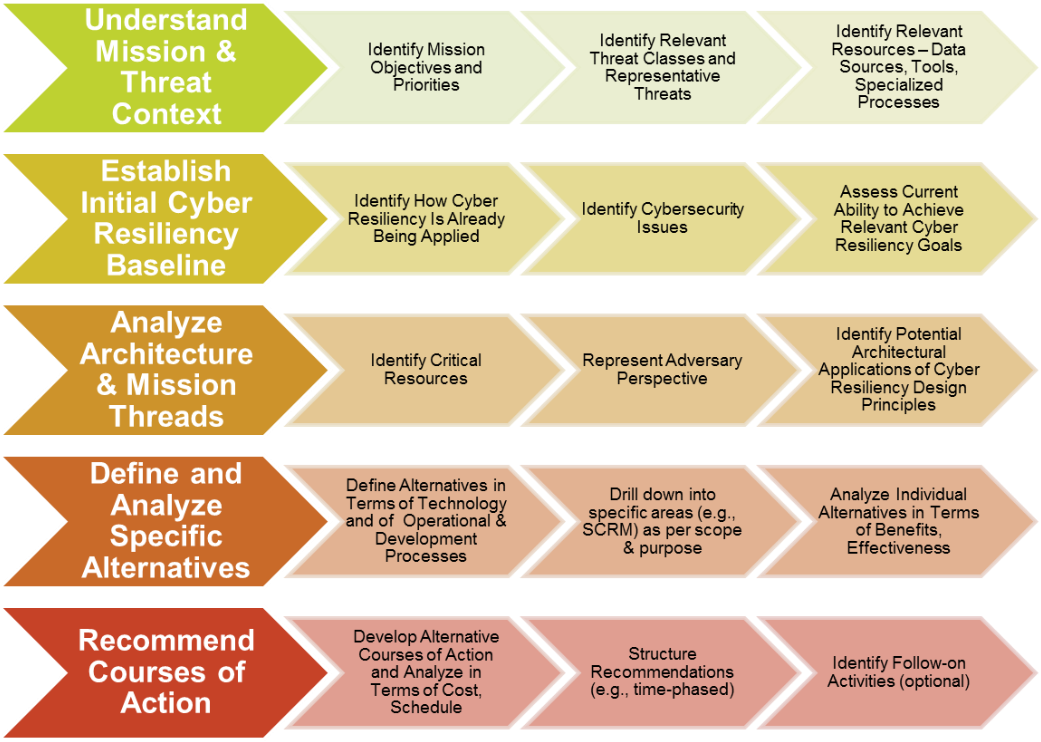
- *What do we recommend?* Cyber resiliency techniques are interdependent, and also interact with techniques for cybersecurity, COOP, and RMA. Thus, activities in this final step analyze combinations of specific alternatives into potential courses of action (CoAs), in the context of the constraining factors identified earlier. This step produces recommendations consistent with the identified purpose of the CRA.

This general process is designed to support systems engineering and risk management activities throughout the SDLC or ALC. Thus, it is intended to be repeated or revisited, as new decision points are reached or as new questions about system resilience are asked.

Activities in a Cyber Resiliency Analysis

The figure below identifies specific activities that can be included in the five high-level steps of a CRA. For each of these activities, representative inputs, outputs, and supporting resources (e.g., frameworks, value scales, models, and datasets) are identified. The assumptions throughout is that a CRA is performed by a team that includes cyber resiliency subject matter experts (SMEs), system SMEs (e.g., architects, engineers, technology specialists as needed), and stakeholder representatives.

Stakeholder engagement is crucial. While cyber resiliency SMEs typically lead a CRA, strong engagement of program office staff and system SMEs is needed throughout. Early in the ALC, representatives of the user community must also be engaged. Late in the ALC, and particularly for systems in the Operations and Maintenance (O&M) phase, cyber defenders responsible for protecting against, detecting, and responding to cyber attacks should also be engaged. Throughout the ALC, inputs from and coordination with representatives of Authorizing Officials should also be part of the CRA. Without strong engagement of these stakeholders, the results of a CRA (as with other types of analyses) risk becoming shelfware.


Understand Mission & Threat Context
Identify Mission Objectives and Priorities
Identify Relevant Threat Classes and Representative Threats
Identify Relevant Resources – Data Sources, Tools, Specialized Processes
Establish Initial Cyber Resiliency Baseline
Identify How Cyber Resiliency Is Already Being Applied
Identify Cybersecurity Issues
Assess Current Ability to Achieve Relevant Cyber Resiliency Goals
Analyze Architecture & Mission Threads
Identify Critical Resources
Represent Adversary Perspective
Identify Potential Architectural Applications of Cyber Resiliency Design Principles
Define and Analyze Specific Alternatives
Define Alternatives in Terms of Technology and of Operational & Development Processes
Drill down into specific areas (e.g., SCRM) as per scope & purpose
Analyze Individual Alternatives in Terms of Benefits, Effectiveness
Recommend Courses of Action
Develop Alternative Courses of Action and Analyze in Terms of Cost, Schedule
Structure Recommendations (e.g., time-phased)
Identify Follow-on Activities (optional)

Understand the Mission and Threat Context

This step establishes the scope and purpose of the CRA, in dialog with the PM or PEO, and subsequently with other stakeholders and SMEs (e.g., a Chief Architect or Chief Engineer). Discussions with stakeholders are typically supported by informational briefings on the cyber threat and the Cyber Resiliency Engineering Framework (CREF) [11] [12]. Questions for discussion include:

- What is the focus? The focus of a CRA can be a specific capability provided by a system or SoS; a system; a mission (and the SoS that supports it); a set of systems, which may support multiple missions simultaneously or sequentially (e.g., a data center).
- At what point in the lifecycle is the system, SoS, or set of systems?
- What can be considered?
    - What is out of scope? The scope can include – or exclude, making clear assumptions about – elements of the system architecture, design, technologies; operational processes and procedures; the development and/or maintenance environment; shared services / common infrastructures on which the focus depends; and other external interfaces / external dependencies.
    - What types of recommendations can be implemented? What POET (political, operational economic, and technical) constraints must be applied?[1]
    - How will results (including interim analyses) be used in RMF / SSE activities?
- Which cyber resiliency goals and objectives are considered? Are any out of scope? (Note that this question will be revisited in the activity to Identify Mission Objectives and Priorities.)
- What classes of cyber adversaries, and what attack vectors, are considered? Are any out of scope? (Note that this question will be revisited in the activity to Identify Relevant Threat Classes and Representative Threats.)
- Is cost to be included? If so, what approach to cost analysis / assessment should be used? Examples include acquisition cost, operations cost, and maintenance cost.
- How is timeframe to be considered? The analysis can focus on recommendations that can be implemented in a given timeframe, or can include recommendations that can be phased in over time.
- How extensive or detailed should the analysis be? The analysis can be high-level, producing a Top Ten set of concerns and recommendations. It can include a detailed crown jewels analysis (CJA), or even a detailed threat and risk mitigation analysis.

Three specific activities are intended to establish the mission and threat context, and hence the scope and purpose of the CRA, in more detail.

Identify mission objectives and priorities

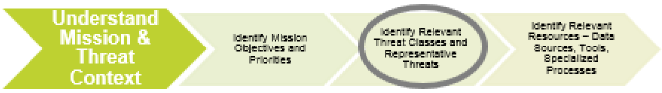
Understand Mission & Threat Context
Identify Mission Objectives and Priorities
Identify Relevant Threat Classes and Representative Threats
Identify Relevant Resources – Data Sources, Tools, Specialized Processes

Information to be obtained in this activity includes identification of missions and mission priorities, and identifies the system(s) to be considered in the CRA. The result of this activity is a list of mission objectives and priorities, including

[1] See Appendix E of [1]. For example, depending on the stage in the ALC, recommendations that could have schedule impacts might be out of scope.

mission impacts of concern that could result from cyber effects of adversary activities. As the SCRAM process is executed, cyber resiliency SMEs will later be able to translate mission objectives and concerns into a determination of which cyber resiliency goals and objectives are most relevant.

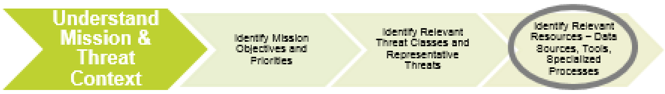
Identify relevant threat classes and representative threats


Understand Mission & Threat Context
Identify Mission Objectives and Priorities
Identify Relevant Threat Classes and Representative Threats
Identify Relevant Resources – Data Sources, Tools, Specialized Processes

Information to be obtained in this activity can include FIPS 199 / RMF Step 1 inputs; a general characterization of threats (e.g., using the Cyber Prep 2.0 categories [13]); and lists of threats to be considered in system risk assessments or adversarial testing. During or after the Materiel Solution Analysis (MSA) phase of the ALC, this information can usually be found in system or mission artifacts such as the program's Cybersecurity Strategy, Security Plan, System Threat Assessment Report (STAR), and Program Protection Plan (PPP). Alternately, or as validation of what can be found in the artifacts, this information can be obtained via discussions and structured interviews with program staff and other key stakeholders.

The result of this activity includes identification of relevant threat classes and representative threats (typically, a list of types or characteristics of adversaries, but potentially also includes a set of representative threat scenarios); and a list of mission impacts of concern that could result from cyber effects of adversary activities.

Identify relevant resources


Understand Mission & Threat Context
Identify Mission Objectives and Priorities
Identify Relevant Threat Classes and Representative Threats
Identify Relevant Resources – Data Sources, Tools, Specialized Processes

This activity identifies sources of information (e.g., SMEs, documents, datasets), as well as resources to be used in the CRA. SMEs can include a Chief Architect, a Chief Engineer, SSEs, mission owner(s), system or facility operator(s), representatives of the Intelligence community, and experts in specific technologies used in the system(s) under consideration. Documentary sources include DoDAF (DoD Architectural Framework) and cybersecurity-related artifacts.[2] In addition, valuable information can be found in documentation of the system or mission concept of operations (CONOPS), concept of employment (CONEMP), the cyber defense CONOPS, or use cases.

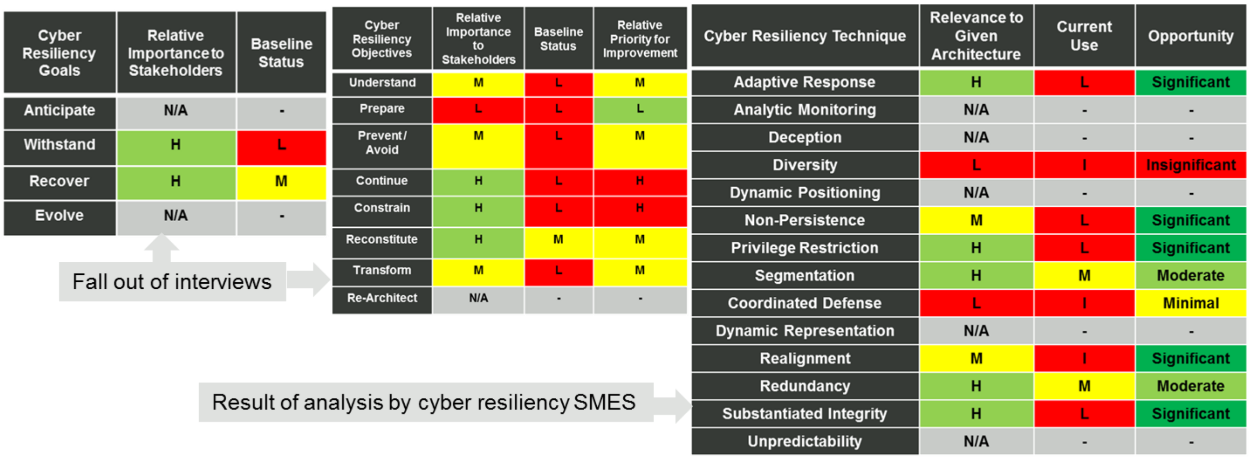
However, neither DoDAF nor Cybersecurity artifacts provide mission outcome metrics; descriptions of mission impacts or situations the system design seeks to avoid; temporal constraints and how they relate to impacts; or a network topology description. Sources of this information must be sought out, and often may exist as SME expertise rather than available documentation.

Resources to be used in the CRA can include datasets (e.g., threat databases), frameworks (e.g., the CREF), models (e.g., cyber attack lifecycle (CAL) or cyber kill chain (CKC) models), and tools (e.g., spreadsheets, modeling and simulation (M&S)) to help understand and analyze specific aspects of the problem. The specific resources used are determined by the CRA's scope, level of detail, and extent, and may also be determined by contractual or programmatic considerations.

[2] *The DoD Program Manager's Guidebook for Integrating the Cybersecurity Risk Management Framework (RMF) into the Acquisition Lifecycle* [10] identifies cybersecurity-related artifacts that could be used in a CRA. Note, however, that for many systems these artifacts do not exist or are woefully out of date.

Establish an Initial Cyber Resiliency Baseline

This step determines (1) the extent to which different aspects of cyber resiliency – goals, objectives, and techniques – are relevant to the system, (2) whether and how well existing architectural, implementation, and operational decisions achieve or apply those aspects, and (3) opportunities and priorities for improving relevant aspects. The initial cyber resiliency baseline can take the form of a cyber resiliency scorecard, as illustrated below. The initial cyber resiliency baseline can be updated with more accurate information, annotated with supporting rationale and references, and revisited as a shared focus for discussions throughout the remaining steps.


Fall out of interviews
Result of analysis by cyber resiliency SMES

Cyber Resiliency Goals	Relative Importance to Stakeholders	Baseline Status
Anticipate	N/A	-
Withstand	H	L
Recover	H	M
Evolve	N/A	-

Cyber Resiliency Objectives	Relative Importance to Stakeholders	Baseline Status	Relative Priority for Improvement
Understand	M	L	M
Prepare	L	L	L
Prevent/ Avoid	M	L	M
Continue	H	L	H
Constrain	H	L	H
Reconstitute	H	M	M
Transform	M	L	M
Re-Architect	N/A	-	-

Cyber Resiliency Technique	Relevance to Given Architecture	Current Use	Opportunity
Adaptive Response	H	L	Significant
Analytic Monitoring	N/A	-	-
Deception	N/A	-	-
Diversity	L	I	Insignificant
Dynamic Positioning	N/A	-	-
Non-Persistence	M	L	Significant
Privilege Restriction	H	L	Significant
Segmentation	H	M	Moderate
Coordinated Defense	L	I	Minimal
Dynamic Representation	N/A	-	-
Realignment	M	I	Significant
Redundancy	H	M	Moderate
Substantiated Integrity	H	L	Significant
Unpredictability	N/A	-	-

Three specific activities enable the development of a cyber resiliency baseline.

Identify how cyber resiliency is already being applied

Establish Initial Cyber Resiliency Baseline
Identify How Cyber Resiliency Is Already Being Applied
Identify Cybersecurity Issues
Assess Current Ability to Achieve Relevant Cyber Resiliency Goals

Key information artifacts used in this activity include the Philosophy of Protection (PoP) for the system[3], its architecture, and its design; security controls (some of which may be related to cyber resiliency [14]); and security view(s) of the system architecture. This information is typically found in the Cybersecurity Strategy and Security Plan.

This activity takes the form of discussions or structured interviews with the PM or PEO, staff, other stakeholders, and system SMEs. Based on these, cyber resiliency SMEs determine whether and how cyber resiliency objectives and techniques are represented in the design principles identified in the PoP, as well as whether and which cyber resiliency controls are included.

This activity produces the part of CREF Baseline Profile that relates to objectives and techniques (While an initial and notional CREF Profile may be developed during the planning steps, the scorecard produced by this step will be based on programmatic evidence.) This activity can also result in recommended updates to the PoP (e.g., cyber resiliency design principles).

[3] If the cyber resiliency goals, cyber resiliency objectives, and cyber threats to be considered are not identified in the organization's Philosophy of Protection, documentation of them via the Cyber Resiliency Analysis will support multiple SSE activities.

Identify cybersecurity issues

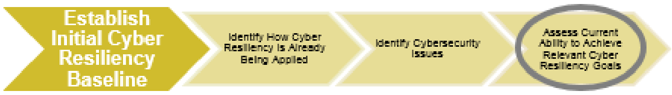
Establish Initial Cyber Resiliency Baseline
Identify How Cyber Resiliency Is Already Being Applied
Identify Cybersecurity Issues
Assess Current Ability to Achieve Relevant Cyber Resiliency Goals

This activity takes the form of discussions or structured interviews with the PM or PEO, staff, other stakeholders, and system SMEs. Based on these, cyber resiliency SMEs determine whether and how security issues should be reflected in the cyber resiliency baseline, as well as whether a reorientation of the CRA might be warranted.

Cyber resiliency builds on a foundation of cyber security and other security disciplines (e.g., physical security, OPSEC). Therefore, knowledge or identification of security issues can result in revision of the CRA Plan, to focus on security controls and requirements needed as foundation for cyber resiliency, or to include specific types of threats or attack vectors in the analysis. In addition, cyber resiliency alternatives identified in later steps can be analyzed in light of how they might resolve security issues or mitigate security risks.

Key information elements used in this activity includes system security controls and requirements; security view(s) of system architecture; and assessments of security controls and requirements if available (e.g., from Steps 4-6 of the RMF). This information is typically found in such system artifacts as the Cybersecurity Strategy and Security Plan.

Assess Current Ability to Achieve Relevant Cyber Resiliency Goals


Establish Initial Cyber Resiliency Baseline
Identify How Cyber Resiliency Is Already Being Applied
Identify Cybersecurity Issues
Assess Current Ability to Achieve Relevant Cyber Resiliency Goals

This activity produces the remaining part of the cyber resiliency baseline, which assesses the current ability to achieve cyber resiliency goals in the context of the identified in-scope threats, as well as a high-level mapping of attack scenarios to cyber effects and level of effect on mission. Note that, based on the scope of the CRA and stakeholder input, it may be the case that some cyber resiliency goals are not considered relevant.

The assessments of cyber resiliency objectives can be combined to produce an initial assessment of the cyber resiliency goals; this is then modified based on consideration of potential mission effects, in discussion with stakeholders.

If possible, cyber resiliency SMEs use the set of attack scenarios (identified in an earlier activity from the System Threat Assessment Report and Program Protection Plan); if not, they must develop a representative set. Additional input elements include security view(s) of system architecture and/or risk assessment reports (an appendix or reference in the Security Plan).

Analyze Architecture and Mission Threads

In this step, critical resources – which provide mission-critical capabilities, and which therefore are candidates for increased resilience – are identified. The system or mission architecture, and mission threads[4] are analyzed from the standpoint of mission assurance in the face of advanced cyber adversaries. Opportunities for architectural improvement, via application of cyber resiliency design

[4] "A mission thread is a sequence of end-to-end activities and events that takes place to accomplish the execution of an SoS capability. The mission thread takes place in the context defined by a vignette, which is a short story about environment [sic]. We identify three basic types of mission threads: 1) operational, 2) development, and 3) sustainment." [21] Mission thread analysis can be used as part of security risk analysis [22].

principles, are also identified. The results of this step enable specific alternatives for cyber resiliency improvement to be identified in the next step.

Identify Critical Resources

Analyze Architecture & Mission Threads
Identify Critical Resources
Represent Adversary Perspective
Identify Potential Architectural Applications of Cyber Resiliency Design Principles

Critical assets can be identified using mission thread analysis, Crown Jewels Analysis (CJA) [15], Functional Network Dependency Analysis (FDNA) [16], Cyber Mission Impact Assessment [17], or COOP processes such as Mission Impact Analysis (MIA) or Business Impact Analysis (BIA). This activity produces a list of crown jewels or critical resources, which can include identification of single points of failure, common infrastructure elements and shared services, as well as shared datasets or communications links. Note that a typical MIA or BIA identifies critical resources, but often misses some, particularly those an attacker uses in a multi-stage attack. Thus, this activity must be performed in conjunction with the second activity in this step, which considers the adversary's perspective.

The identification of critical resources uses architectural views that represent mission threads, information flows, and functional dependencies. DoDAF artifacts that could serve as inputs include Mission Model Elements (e.g., Functions – SV 4; Tasks/Activities – OV5, OV 6 a/b/c; Capabilities – CV 2; Organizations – OV 4 ; Platforms/Services – SV 1; Services – SvcV1; and Use cases – OV 1, CONEMP) and linkages between elements (e.g., Information-Flows – OV 2, OV 3, DIV 1-3; Functions-Tasks – SV 5a; Functions-Services – SV 4; Tasks-Capabilities – CV 6, OV 5b; Tasks-Services – SV5, SvcV5; Platforms-Capabilities – SV 5b; and Services-Capabilities – CV 7).

Represent Adversary Perspective

Analyze Architecture & Mission Threads
Identify Critical Resources
Represent Adversary Perspective
Identify Potential Architectural Applications of Cyber Resiliency Design Principles

In this activity, cyber resiliency SMEs identify attack vectors and analyze potential attacks. They perform an analysis, from an adversarial perspective, of how mission impacts of greatest concern could be achieved. To represent the adversarial perspective, they use CAL / CKC models and datasets (e.g., ATT&CK), or a threat model such as has been defined in the Cyber Security Game (CSG) [18] that considers how the network topology affects attacker options.

Sources of information can include critical resources as identified in the preceding activity; lists of attack vectors, adversary actions, or attack models; and information on vulnerabilities or susceptibilities of specific types of systems or technologies. This activity produces a list of resources at greatest risk – those considered critical and susceptible to successful attack.

Identify Potential Architectural Applications of Cyber Resiliency Design Principles

Analyze Architecture & Mission Threads
Identify Critical Resources
Represent Adversary Perspective
Identify Potential Architectural Applications of Cyber Resiliency Design Principles

This activity identifies potential cyber resiliency design principles[5] or opportunities to apply cyber resiliency techniques. Cyber resiliency SMEs analyze the architecture, selecting potential cyber resiliency techniques consistent with

[5] An initial set of cyber resiliency design principles can be found in Table 11 of [1]. An updated and extended set of potential cyber resiliency design principles is under development.

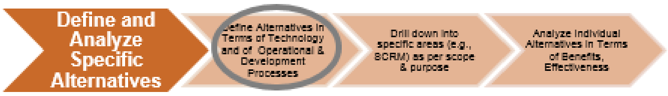
the system’s PoP and subject to the CRA constraints defined earlier. The cyber resiliency SMEs validate the results with the program’s Chief Architect, Chief Engineer, or SSEs if possible.

Inputs to this activity include architectural views as above, plus views that indicate which system elements are separately configured or managed; the system’s PoP or the CREF Profile produced in the second step of the CRA; results of critical asset identification; and stakeholder inputs on limitations on alternatives.

Define and Analyze Specific Alternatives

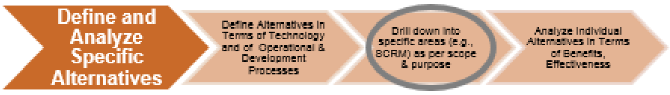
In this step, cyber resiliency SMEs in conjunction with systems engineering and/or operational staff define specific actions – architectural changes, ways to implement cyber resiliency techniques in the context of the existing architecture, ways to use existing system capabilities more effectively to improve resilience – and analyze them in terms of potential effectiveness. These specific alternatives form a menu, from which different combinations into courses of action can in the final step be constructed and analyzed.

Define Alternatives in Terms of Technology and of Operational & Development Processes


Define and Analyze Specific Alternatives
Define Alternatives in Terms of Technology and of Operational & Development Processes
Drill down into specific areas (e.g., SCRM) as per scope & purpose
Analyze Individual Alternatives in Terms of Benefits, Effectiveness

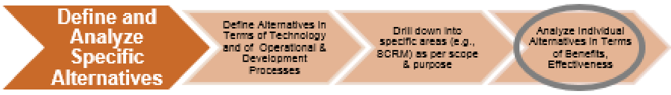
In this activity, cyber resiliency SMEs in conjunction with systems engineers turn potential applications of cyber resiliency techniques and approaches[6] into specific alternatives. Inputs to this activity include System Design Document(s) identifying products, protocols; operating procedures; and stakeholder input on limitations on alternatives.

Drill Down into Specific Areas as per Scope and Purpose


Define and Analyze Specific Alternatives
Define Alternatives in Terms of Technology and of Operational & Development Processes
Drill down into specific areas (e.g., SCRM) as per scope & purpose
Analyze Individual Alternatives in Terms of Benefits, Effectiveness

As determined by the scope and purpose of the CRA, alternatives can be developed in specific areas. Examples of areas include supply chain risk management (SCRM), capabilities to be added at external interfaces (e.g., Substantiated Integrity mechanisms), and external dependencies (e.g., shared services, common infrastructures).

Analyze Individual Alternatives in Terms of Benefits and Effectiveness


Define and Analyze Specific Alternatives
Define Alternatives in Terms of Technology and of Operational & Development Processes
Drill down into specific areas (e.g., SCRM) as per scope & purpose
Analyze Individual Alternatives in Terms of Benefits, Effectiveness

Each alternative can be analyzed in terms of its potential benefits and effectiveness from one or more perspectives. The perspectives applied in the analysis are determined by the scope of the CRA. For example, alternatives can be analyzed in terms of

- Potential effects on and effectiveness against adversary activities. This analysis produces a mapping of alternatives to the CAL or CKC, noting effects on adversary activities [19] [12], and can produce more detailed versions of attack scenarios.
- Potential reduction of mission risk [4].

[6] See the Cyber Resiliency Engineering Aid for a discussion of approaches.

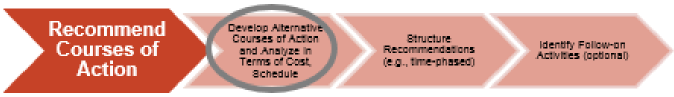
- POET factors, including consideration of technical maturity and lifecycle cost.
- Expected cyber resiliency benefits (e.g., in terms of ability to achieve relevant cyber resiliency objectives and goals, in terms of the survivability Key Performance Parameter (KPP)), in the context of the representative threats and of the mission priorities identified in earlier steps.
- Expected cyber security benefits. These benefits, in the form of reduction of security risks, can include
  - Achieving the intent of security controls that might be part of a relevant baseline but which cannot be implemented in the system (e.g., due to such factors as mobility, limitations on size, weight, and power (SWaP), or dependence on legacy technology).
  - Compensating for vulnerabilities that cannot be closed (e.g., due to dependence on external systems).
- Expected ease (or difficulty) of integration with the existing system architecture, system implementation, development or maintenance environment, Computer Network Defense (CND) environment, or operational processes.

Recommend Courses of Action

Cyber resiliency techniques, approaches, and specific alternatives can interact in various ways. A given alternative can support, depend on, or interfere with another. Thus, the alternatives identified in the preceding step cannot simply be listed in a priority order based on potential benefits or effectiveness. In this step, cyber resiliency SMEs work with other SMEs to develop and analyze alternative courses of action (CoAs), and to define recommendations in such a way that they can be integrated into program planning. Follow-on activities – e.g., to identify security controls related to the recommended CoAs from NIST SP 800-53R4 and to define requirements – can also be recommended.

Recommended Courses of Action can take many forms, depending on the purpose and scope of the CRA. Outputs of this step might be in the form of a top ten list, a completed resilience scorecard, a portfolio analysis, and a description of any follow-on activities. In addition to the recommendations, all of the intermediate output artifacts produced during the CRA process can be assembled into a leave-behind for the customer, or integrated into existing programmatic artifacts. These SCRAM outputs can provide the necessary context in which the CRA was performed, and serve as a knowledge management artifact that can provide details not included in the final recommendations, and act as a starting point for any future CRAs that may follow.

Develop and Analyze Alternative Courses of Action


Recommend Courses of Action
Develop Alternative Courses of Action and Analyze in Terms of Cost, Schedule
Structure Recommendations (e.g., time-phased)
Identify Follow-on Activities (optional)

In this activity, sets of compatible alternatives are defined. The size of the sets is determined in part by the way the recommendations will be structured. Determining whether a set of alternatives is compatible involves analyzing interactions (dependencies, conflicts) among the alternatives and applying POET factors as identified in the scope. If in-scope, a cost analysis can also be performed.[7]

[7] Note that "cost" has multiple dimensions, and can include acquisition or development cost, maintenance cost, and impacts on existing operational processes.

Structure Recommendations

Recommend Courses of Action
Develop Alternative Courses of Action and Analyze in Terms of Cost, Schedule
Structure Recommendations (e.g., time-phased)
Identify Follow-on Activities (optional)

Recommendations can be structured in various ways, depending on the purpose and scope of the CRA. One form is a Top Ten list, in which a set of small CoAs is ordered based on decreasing cost-effectiveness, increasing cost, or increasing impact on existing operations. Another form is time-phased, aligned with programmatic or operational milestones. An updated version of the initial cyber resiliency baseline – e.g., showing what the scorecard would look like, assuming different alternative courses of action – can act as a visual aid.

Identify Potential Follow-on Activities

Recommend Courses of Action
Develop Alternative Courses of Action and Analyze in Terms of Cost, Schedule
Structure Recommendations (e.g., time-phased)
Identify Follow-on Activities (optional)

Follow-on activities to a CRA can include:

- Translate the resilience alternatives into new or changed requirements for the mission or system(s) and/or map security controls to requirements.[8]
- Identify cyber resiliency target measures. Inputs can include mission and system Measures of Effectiveness (MOEs), Measures of Performance (MOPs), and Key Performance Parameters (KPPs) from the system's Capability Development Document (CDD), as well as any security performance measures that have been defined. Cyber resiliency target measures can include target values for MOEs and KPPs for preserving, recovering, and reconstituting critical mission capabilities; these can be used in developmental test and evaluation (DT&E) and operational test and evaluation (OT&E).[9]
- Perform follow-on experimentation to validate the effectiveness of CoAs and refine procedures.

Conclusion

The Structured Cyber Resiliency Analysis Methodology described in this paper is tailorable to a wide variety of systems, stages in the acquisition lifecycle, and scopes of analysis. The description in this paper refers to resources for cyber risk-informed engineering developed and used by MITRE. Those resources are not required for SCRAM to be applied to a program. However, to ensure that an application of SCRAM (or any other analysis methodology) is repeatable, reproducible, and minimizes level of effort, use of a set of similar resources is recommended.

[8] Security controls as defined in NIST SP 800-53R4 [25] or as cited in the NIST Cybersecurity Framework [26], and descriptions of alternatives, are not stated in terms that can easily be integrated into contractual documents (e.g., a Functional Requirements Document or a Statement of Work).

[9] Because testing of cyber resiliency involves representing an adversarial threat rather than random failures, it fits with cybersecurity testing rather than, for example, verification of RMA requirements. See [23] [24].

References

[1] D. Bodeau and R. Graubart, "Cyber Resiliency Assessment: Enabling Architectural Improvement (MTR 120407, PR 12-3795)," May 2013. [Online]. Available: http://www.mitre.org/sites/default/files/pdf/12_3795.pdf.

[2] MITRE, "Cyber Resiliency Engineering: An Overview of the Assessment Process," May 2013. [Online]. Available: https://registerdev1.mitre.org/sr/cyber_engineering.pdf.

[3] D. Bodeau, R. Graubart, L. LaPadula, P. Kertzner, A. Rosenthal and J. Brennan, "Cyber Resiliency Metrics," April 2012. [Online]. Available: https://registerdev1.mitre.org/sr/12_2226.pdf.

[4] S. Musman and S. Agbolosu-Amison, "A Measurable Definition of Resiliency Using "Mission Risk" as a Metric," March 2014. [Online]. Available: http://www.mitre.org/sites/default/files/publications/resiliency-mission-risk-14-0500.pdf.

[5] D. J. Bodeau, "Analysis Through a Resilience Lens: Experiences and Lessons-Learned (PR 15-1309) (presentation)," in *5th Annual Secure and Resilient Cyber Architectures Invitational*, McLean, VA, 2015.

[6] The MITRE Corporation (ed.), "2015 Secure and Resilient Cyber Architectures Invitational (PR case no. TBD)," The MITRE Corporation, Bedford, MA, 2016.

[7] NIST, "Guide for Conducting Risk Assessments, NIST SP 800-30 Rev.1," September 2012. [Online]. Available: http://csrc.nist.gov/publications/nistpubs/800-30-rev1/sp800_30_r1.pdf.

[8] NIST, "NIST SP 800-160, Systems Security Engineering: An Integrated Approach to Building Trustworthy Resilient Systems (Initial Public Draft)," May 2014. [Online]. Available: http://csrc.nist.gov/publications/drafts/800-160/sp800_160_draft.pdf.

[9] NIST, "Guide for Applying the Risk Management Framework to Federal Information Systems, NIST SP 800-37 Rev. 1," February 2010. [Online]. Available: http://csrc.nist.gov/publications/nistpubs/800-37-rev1/sp800-37-rev1-final.pdf.

[10] DoD, "DoD Program Manager's Guidebook for Integrating the Cybersecurity Risk Management Framework (RMF) into the System Acquisition Lifecycle, Version 1.0," 26 May 2015. [Online]. Available: https://acc.dau.mil/adl/en-US/722603/file/80119/Cybersecurity%20Guidebook%20v1_0%20with%20publication%20notice.pdf.

[11] D. Bodeau and R. Graubart, "Cyber Resiliency Engineering Framework (MTR110237, PR 11-4436)," September 2011. [Online]. Available: http://www.mitre.org/sites/default/files/pdf/11_4436.pdf.

[12] D. Bodeau, R. Graubart, W. Heinbockel and E. Laderman, "Cyber Resiliency Engineering Aid-The Updated Cyber Resiliency Engineering Framework and Guidance on Applying Cyber Resiliency Techniques, MTR140499R1, PR 15-1334," May 2015. [Online]. Available: http://www.mitre.org/sites/default/files/publications/pr-15-1334-cyber-resiliency-engineering-aid-framework-update.pdf.

[13] The MITRE Corporation, "Cyber Prep 2.0: Motivating Organizational Cyber Strategies in Terms of Preparedness (PR 15-0837)," The MITRE Corporation, Bedford, MA, 2015.

[14] D. Bodeau, Graubart and Richard, "Cyber Resiliency and NIST Special Publication 800-53 Rev.4 Controls (MTR 130531, PR 13-4037)," September 2013. [Online]. Available: http://www.mitre.org/sites/default/files/publications/13-4047.pdf.

[15] The MITRE Corporation, "Systems Engineering Guide: Crown Jewels Analysis," 2011. [Online]. Available: http://www.mitre.org/publications/systems-engineering-guide/enterprise-engineering/systems-engineering-for-mission-assurance/crown-jewels-analysis.

[16] P. R. Garvey and C. A. Pinto, Advanced Risk Analysis in Engineering Enterprise Systems, New York, NY: CRC Press, 2012.

[17] S. Musman, M. Tanner, A. Temin, E. Elsaesser and L. Loren, "A systems engineering approach for crown jewels estimation and mission assurance decision making," in *IEEE Symposium on Computational Intelligence in Cyber Security (CICS)*, 2011.

[18] S. Musman, "Playing the Cyber Security Game: A Rational Approach to Cyber Security and Resilience Decision Making (MTR 150371, PR 15-3140)," The MITRE Corporation, McLean, VA, 2016.

[19] D. Bodeau and R. Graubart, "Characterizing Effects on the Cyber Adversary: A Vocabulary for Analysis and Assessment (MTR 130432, PR 13-4173)," November 2013. [Online]. Available: http://www.mitre.org/sites/default/files/publications/characterizing-effects-cyber-adversary-13-4173.pdf.

[20] SEI, "Mission Thread Workshop," 2013. [Online]. Available: http://www.sei.cmu.edu/architecture/tools/establish/missionthread.cfm.

[21] C. Woody and C. Alberts, "Evaluating Security Risks Using Mission Threads," *CrossTalk,* pp. 15-19, September / October 2014.

[22] DOT&E, "Procedures for Operational Test and Evaluation ofCybersecurity in Acquisition Programs," 1 August 2014. [Online]. Available: http://www.dote.osd.mil/pub/policies/2014/8-1-14_Procs_for_OTE_of_Cybersec_in_Acq_Progs(7994).pdf.

[23] DoD, "Department of Defense Cybersecurity Test and Evaluation Guidebook, Version 1.0," 1 July 2015. [Online]. Available: http://www.dote.osd.mil/docs/TempGuide3/Cybersecurity_TE_Guidebook_July1_2015_v1_0.pdf.

[24] NIST, "Security and Privacy Controls for Federal Information Systems and Organizations (NIST SP 800-53 R4)," April 2013. [Online]. Available: http://dx.doi.org/10.6028/NIST.SP.800-53r4.

[25] NIST, "Framework for Improving Critical Infrastructure Security, Version 1.0," 12 February 2014. [Online]. Available: http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214.pdf.