The Risk Management Framework and Cyber Resiliency

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

Abstract. Cyber resiliency and the Risk Management Framework (RMF) are two broad constructs, which at first glance appear to be orthogonal. But when advanced cyber threats are considered, cyber resiliency can be seen as essential to achieving the goals of the RMF. This paper presents several perspectives on the RMF, and indicates how cyber resiliency fits into the RMF from each perspective.

Introduction

The Department of Defense (DoD), Intelligence Community (IC), and Federal agencies via representation by the National Institute of Standards and Technology (NIST) have collectively taken action to move from a compliance-oriented approach to cyber security to one based on risk management. The efforts of the Joint Task Force Transformation Initiative (JTI) have produced a variety of publications to support this transition. At the same time, policy makers across Government and industry have become increasingly aware of advanced cyber threats and the need to "fight through" and rebound not only from acute and immediately recognizable cyber attacks, but also persistent, sophisticated, and covert adversary activities. Thus, cyber resiliency is increasingly cited as a goal for organizations, missions, and systems.

This white paper describes several perspectives on the risk management framework, and indicates how cyber resiliency fits into it from each perspective.

- The first perspective is definitional: How are the RMF and cyber resiliency defined, and how do those definitions relate to each other?
- The second perspective is at the organizational level: How does cyber resiliency fit into the general risk management process defined in NIST Special Publication (SP) 800-39 [1], as applied at the organizational tier in the NIST SP 800-39 multi-tier approach to risk management?
- The third is the mission and business process perspective: Again using NIST SP 800-39, how does cyber resiliency fit into risk management activities at the mission and business process tier?
- The fourth is the system perspective: How does cyber resiliency fit into the six system level steps defined in NIST SP 800-37 [2]? How does cyber resiliency relate to the security control baselines identified in NIST SP 800-53R4 [3] and in Committee on National Security Systems Instruction (CNSSI) 1253 [4]? How can tailoring help a system achieve a risk-appropriate balance between conventional cyber security and cyber resiliency?

The RMF and Cyber Resiliency: Multiple Definitions, but Inherent Compatibility

The phrase "risk management framework" (RMF) has various interpretations depending up on context. As defined in CNSSI 4009 [1], the RMF is *a structured approach used to oversee and manage risk for an enterpris*e. This high-level and general definition encompasses risk management at all tiers (organization, mission / business process, and system) in the multi-tiered approach to risk management defined in NIST SP 800-39, as illustrated in Figure 1.

© 2016 The MITRE Corporation. All rights reserved.
Approved for Public Release; Distribution Unlimited. Case No. 16-0776.

However, the term has been widely interpreted in other ways. Some focus on its primary purpose: as a framework designed to help authorizing officials (AO) make near real-time, risk informed decisions. Others tend to use the term RMF as a shorthand for referring to various documents (e.g., NIST SP 800-53, NIST SP 800-39, NIST SP 800-37, NIST SP 800-30R1 [6], CNSSI 1253, etc.) that support and underlie the broader RMF construct. Still others use the term to refer to the six step process defined in NIST SP 800-37. *Each of these uses is valid; it is the context that matters.* And, as this paper indicates, cyber resiliency is compatible with each use.

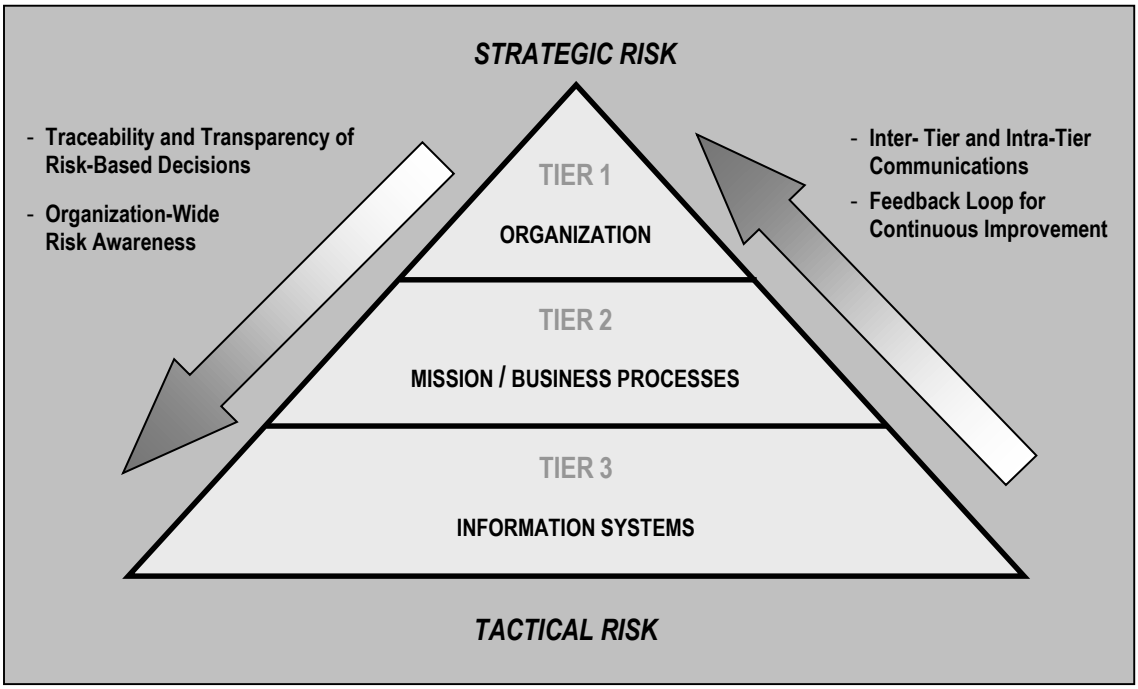

Figure 1: Multi Tiered Organization-Wide Risk Management (Source: NIST SP 800-39)

Similarly, multiple definitions of resilience (and of resilience with some modifier, e.g., information system resilience, network resilience, operational resilience) are provided by various publications, including Presidential Policy Directive (PPD) 21 [1], DoD Instruction (DoDI) 8500.01 [2], and NIST SP 800-39 [3]. Each definition at a minimum includes the capabilities to withstand and to recover from some form of adversity; in addition, many definitions (including frameworks used in the discipline of Resilience Engineering) also include the capabilities to anticipate and adapt. However, there is currently no authoritative definition of *cyber* resilience. For the purpose of this paper, cyber resilience is defined as

© 2016 The MITRE Corporation. All rights reserved.
Approved for Public Release; Distribution Unlimited. Case No. 16-0776.

The ability to anticipate, withstand, recover from, and adapt to adverse conditions, stresses, attacks, or compromises on cyber resources.[1] [2]

Advanced cyber threats can simulate or take advantage of all other forms of adversity, and can establish and maintain a persistent and covert presence. Therefore, cyber resiliency techniques *focus* on providing the ability to anticipate, withstand, recover from, and adapt to cyber attacks and compromises, thereby maximizing mission continuity despite the presence of an adversary in a system. Analysis of how cyber resilient a system, a mission or business function, or an organization is, is typically performed with reference to a representative set of threat scenarios, which focus on the adversarial threat but may also include other representative adverse events such as software and operator errors, failures of supporting infrastructures (e.g., power), and natural events with cyber effects (e.g., solar weather that affects satellite communications).

Analysis of cyber resilience requires more depth than can easily be derived from the high-level goals of anticipate, withstand, recover, and adapt. In this document, cyber resiliency constructs used to provide a basis for analysis are drawn from the MITRE Cyber Resiliency Engineering Framework (CREF) [4]. That framework, as depicted in Figure 2, consists of four goals, eight objectives, and fourteen techniques.

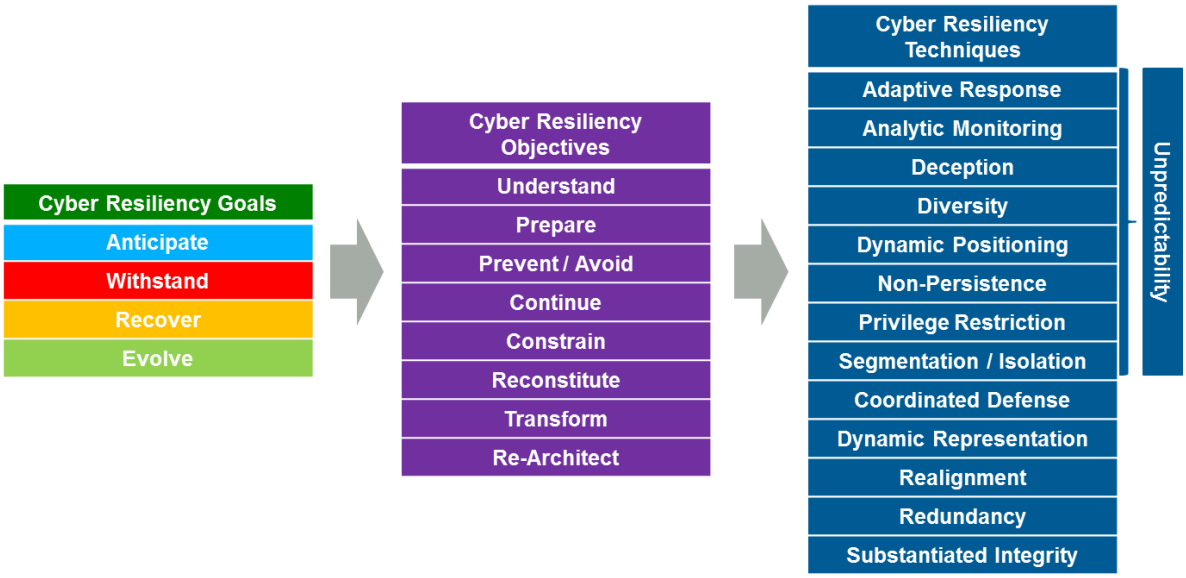

Figure 2: Cyber Resiliency Engineering Framework

Cyber resiliency assumes that other protective and restorative disciplines and associated measures (e.g., conventional cybersecurity measures intended to preserve the confidentiality, integrity, and availability

[1] Cyber resources are separately manageable resources in cyberspace, including information in electronic form, as well as information systems, systems-of-systems, infrastructures, shared services, and devices (see NIST SP 800-39). The set of cyber resources in question can be identified with any of the three tiers (and in the case of some systems-of-systems, can go beyond the organization).

[2] Consistent with PPD 21 and the JTI publications, this definition can be applied to systems, missions or business functions (and systems-of-systems that support them), organizations, critical infrastructure sectors, and the nation. In practice, it is most relevant to missions or business functions; cyber resiliency is increasingly essential to mission continuity.

© 2016 The MITRE Corporation. All rights reserved.
Approved for Public Release; Distribution Unlimited. Case No. 16-0776.

of information; continuity of operations) are in place and provide an underlying foundation for techniques and implementation approaches specific to cyber resiliency.

Cyber resiliency is compatible with the RMF at each tier in the multi-tiered approach to risk management. At the organizational tier, the organization's risk management strategy can include a cyber resiliency perspective. At the mission or business process tier, cyber resiliency can be a concern for owners of organizationally-critical missions or business processes; it can also be reflected in the enterprise architecture and information security architecture. At the information system tier, cyber resiliency is one of many attributes or factors that an authorizing official considers in making a risk management judgement and trying to reduce risk to an acceptable level.

Tier 1: Considering Cyber Resiliency in the Organization's Risk Management Process

NIST SP 800-39, *Managing Information Security Risk*, introduces a risk management process (see figure 3 below) which consists of four steps: frame, assess, respond, and monitor. Each step is executed via a series of tasks. Many of these tasks can be directly linked to cyber resiliency. This section illustrates how cyber resiliency relates to tasks that are part of implementing the general risk management process at the organizational tier. The ultimate result of activities at Tier 1 is an organizational risk management strategy, which guides risk management activities at Tiers 2 and 3. As this section illustrates, cyber resiliency can be part of an organization's risk management process.

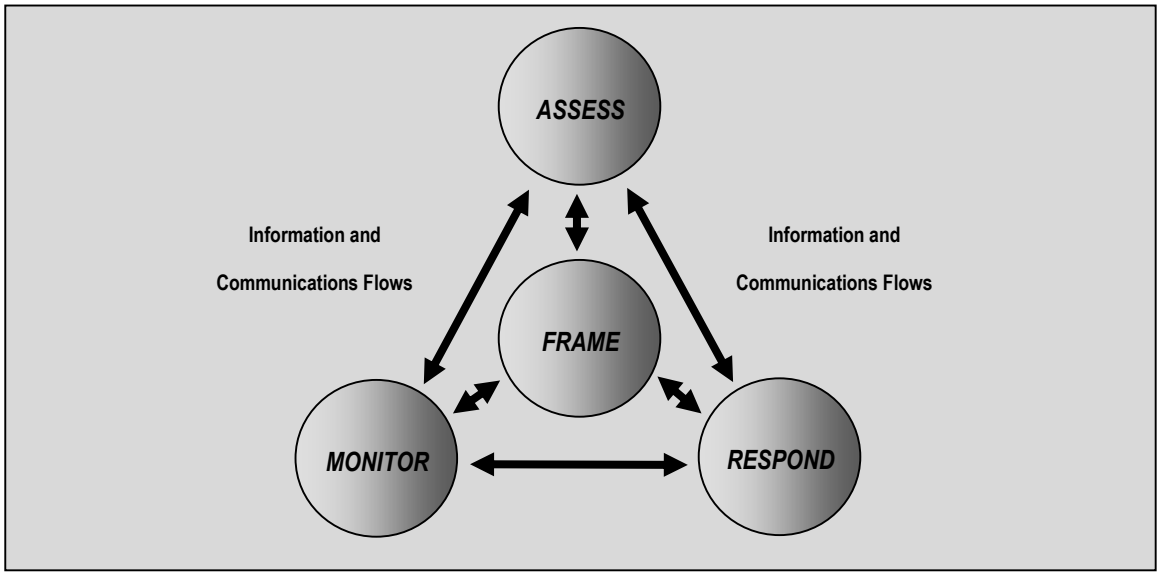

Figure 3: Risk Management Process (Source: NIST SP 800-39)

Risk Framing Task 1-1: Identify assumptions that affect how risk is assessed, responded to, and monitored within the organization.

> **Cyber Resiliency View***:* In this task, the organization articulates its assumptions about its dependence on cyber resources and about the adversarial threat it faces. Can the organization achieve its missions or business functions if the information and communications technology those missions use cannot be relied on? Does the organization assume that its security measures (whether in place or planned) are sufficient to keep its adversaries out? Does the organization assume that it

© 2016 The MITRE Corporation. All rights reserved.
Approved for Public Release; Distribution Unlimited. Case No. 16-0776.

is a target of a capable, well-resourced adversary? Does the organization assume that an adversary can achieve an effective, and persistent foothold within its infrastructure? If the organization assumes that the answers to these questions are "no," "maybe," "yes," and "yes," then its risk management strategy needs to include a cyber resiliency perspective, as indicated in the remaining tasks described in this section.

Risk Framing Task 1-2: *Identify constraints on the conduct of risk assessment, risk response, and risk monitoring activities within the organization*.

Cyber Resiliency View: As part of this task, the organization identifies the factors that need to be considered in the eventual selection of resiliency techniques. For example, one organization might prefer employing well established solutions, while another might be open to employing less traditional, but possibly more effective architectural approaches and specific technologies.

Risk Framing Task 1-3: *Identify the level of risk tolerance for the organization*.

Cyber Resiliency View: As part of this task the organization's stakeholders (e.g., mission or business process owners, representatives of consumers or the general public) need to articulate how concerned they truly are about penetration of the organization's infrastructure by an adversary, and about the effects an adversary's activities could have. What degree of compromise or disruption of the infrastructure, and of missions or business functions, are they able to accept?

Risk Framing Task 1-4: *Identify priorities and trade-offs considered by the organization in managing risk*.

Cyber Resiliency View: From a cyber resiliency perspective one of the key trade-offs to consider is how much emphasis the organization should place on resiliency measures vs. on preventative measures. In other words, the organization needs to determine how much investment should focus on trying to keep the adversary from achieving a foothold in the system (via protection, immediate detection, and rapid response) vs. how much investment should be oriented toward containing, curtailing, expunging, or otherwise responding to the adversary once they achieve a foothold. Still another cyber resiliency trade-off is with regards to the resiliency goals. How much emphasis should be placed on withstanding an attack vs. recovering from an attack? How much emphasis should be place on anticipating an attack? Learning from an attack and adapting to be better able to address similar attacks in the future?

As indicated in Task 1-1, at Tier 1 the organization identifies its missions or business functions. From the standpoint of cyber resiliency, the organization needs to prioritize these, and to determine the relevance and relative priority of the cyber resiliency goals and objectives as applied to them.

The risk framing step, executed via the preceding four tasks, results in the organization's risk management strategy. That strategy reflects the organization's approach to cyber resilience, and includes organizational priorities and trade-offs as well as guidance on how to execute the remaining steps.

© 2016 The MITRE Corporation. All rights reserved.
Approved for Public Release; Distribution Unlimited. Case No. 16-0776.

Risk Assessment Task 2-1: *Identify threats to and vulnerabilities in organizational information systems and the environments in which the systems operate*.

Cyber Resiliency View: From the standpoint of cyber resiliency, the focus is more on an adversary's capabilities, intent and targeting[3] than on specific tactics, techniques, and procedures (TTPs). An adversary rated high or very high in these three areas is likely to be able to establish a foothold in organizational information systems. Such an adversary potentially could achieve that foothold and ultimately threaten the organization's ability to achieve its missions.

From the standpoint of cyber resiliency, identification of vulnerabilities focuses not on known or identifiable technical vulnerabilities, indicative of some error or flaw that can be patched or corrected.[4] Rather, the focus is on inherent weaknesses in mission / business processes, weaknesses in information security and cyber defense processes, and above all architectural weaknesses[5]. Such inherent weaknesses cannot be patched, but cyber resiliency can be employed to provide a risk response and ensure mission continuity.

For each of the cyber resiliency objectives that the organization has identified as relevant and important to one or more missions or business functions, the key question is: If this objective is not achieved, why not? Answers to these questions enable weaknesses to be identified, and point towards cyber resiliency techniques to consider as part of risk response.

Risk Assessment Task 2-2: *Determine the risk to organizational operations and assets, individuals, other organizations, and the Nation if identified threats exploit identified vulnerabilities*.

Cyber Resiliency View: From the standpoint of cyber resiliency, risk is associated not with situations in which "identified threats exploit identified vulnerabilities" but rather with situations in which the effects of adverse events on cyber resources lead to adverse effects on missions / business functions, and thence on individuals, the organization, or the Nation. That is, discussions of risk in a cyber resiliency context emphasize consequences rather than likelihood.

Risk Response Tasks 3-1, 3-2, 3-3*:* *Identify, evaluate, and decide upon alternative courses of action to respond to risk determined during the risk assessment*[6].

Cyber Resiliency View: Cyber resiliency is one means to mitigate the risk that a critical mission or business function will not be executed, or will not be executed well enough. In these three tasks, the organization determines how it plans to ensure adequate resilience in face of the adversary. In

[3] These terms are defined, and value scales provided, in Appendix D of NIST SP 800-30. Note that the adversary's intent can be characterized in terms of organizational effects (e.g., reputation loss, financial loss), effects on missions / business functions (e.g., denial, disruption, degradation, destruction), and cyber effects (e.g., degradation, interruption, modification, fabrication, unauthorized use, interception [9]).

[4] In part, this is because a well-resourced, highly motivated, highly sophisticated adversary can create new vulnerabilities. See the Defense Science Board Report [10].

[5] The following example illustrates the distinction between flaws and weaknesses: The fact that an air base is situated somewhere prone to hurricanes is a weakness; that airplanes are left on the tarmac as opposed to being placed in shelter during a hurricane is a flaw.

[6] To facilitate readability, three tasks are merged together here.

© 2016 The MITRE Corporation. All rights reserved.
Approved for Public Release; Distribution Unlimited. Case No. 16-0776.

particular, the organization identifies, assesses the current use of, and determines which cyber resiliency techniques it will apply. The organization determines the circumstances in which its courses of action focus more on constraining the advance of an adversary (even at the expense of impacts on missions / business functions), vs. limiting the effects of adversary activities on missions / business functions, vs. reconstituting after a successful attack. The organization also determines whether or under what circumstances its selected courses of action focus on techniques that are largely augmentations of traditional security solutions (e.g., redundancy, privilege restriction, substantiated integrity), vs. less traditional solutions (e.g., diversity, deception, dynamic positioning) that change the attack surface.

Risk Monitoring Task 4-1: Develop a risk monitoring strategy for the organization that includes the purpose, type, and frequency of monitoring activities.

> **Cyber Resiliency View***:* Monitoring can serve multiple purposes, including (i) monitoring for compliance, (ii) monitoring for effectiveness, (iii) monitoring to detect changes to systems, and (iv) monitoring to detect changes in how systems are used. While all of these have some value and linkage to cyber resiliency, monitoring for effectiveness is probably the most closely linked to cyber resiliency. That is because the underlying purpose of cyber resiliency is to ensure / maximize mission continuity. Thus, monitoring the effectiveness of the selected resiliency techniques helps ascertain how well mission continuity is being assured.

Tier 2: Cyber Resiliency for Mission / Business Processes

Cyber resiliency is increasingly recognized as essential to mission continuity. Missions and business processes are usually supported by a system-of-systems (SoS) [5] [6]. Thus, cyber resiliency for SoS is a Tier 2 consideration [7].

Section 2.4 of NIST SP 800-39 describes three major risk management activities at Tier 2: the identification and establishment of risk-aware missions and business processes; the development and implementation of an enterprise architecture; and the definition and implementation of the organization's information security architecture. The requirements for information systems at Tier 3 are informed by these Tier 2 risk management activities. NIST SP 800-39 identifies resilience as an important consideration in each of these activities.

Risk-aware (also referred to as risk-informed) processes are those whose definition takes into consideration threats, potential consequences, and expected mission resilience in light of expected information system resilience. The definition of such processes includes identifying the types of information needed, the sensitivity and criticality of the information, and information flows (both within and beyond the organization). When mission / business function owners set requirements or establish measures of effectiveness (MOEs) for mission / business processes in a risk-aware way, they (implicitly or explicitly) establish targets for cyber resiliency MOEs. (For example, how long can an outage be tolerated? How quickly can recovery to an acceptable level of performance be achieved? How much confidence in the correctness of functioning or the quality of data is needed?) The implementation of risk-aware processes requires an understanding of relationships and dependencies, among missions / business functions as well as of mission / business activities on cyber resources. That understanding is gained in part by cyber resiliency analysis.

© 2016 The MITRE Corporation. All rights reserved.
Approved for Public Release; Distribution Unlimited. Case No. 16-0776.

The development and implementation of an enterprise architecture – including technical standards, reference models, and more specific segment architectures[7] – enables an organization to manage its investments strategically and apply its risk management strategy consistently. As NIST SP 800-39 points out, enterprise architecture promotes segmentation, redundancy, and elimination of single points of failure. Depending on the organization's risk management strategy, the application of other cyber resiliency techniques can be enterprise-wide or segment-specific. Cyber resiliency objectives can be prioritized for, and techniques applied or not applied to, segments based on expected mission resilience.

The organization's information security architecture (part of its enterprise architecture) provides information on how security capabilities (e.g., identity and access management) are to be placed and used in the enterprise architecture. It allocates security requirements and controls to common services or infrastructures. It also provides a foundation for achieving risk-appropriate information system resilience, determining under what circumstances and which cyber resiliency controls (i.e., security controls that apply cyber resiliency techniques) apply to information systems.

Tier 3: Cyber Resiliency and the System Level RMF Process

At the system tier, the RMF defines, per NIST SP 800-37, a six-step process; this process is illustrated in Figure 4. Step 2 is where security control baselines are selected and tailored by the organization to reflect their needs, and will be discussed in sub-sections below. However, cyber resiliency can be a consideration in all steps. In Step 1, criticality assessment involves understanding the role of the system in supporting critical missions or business processes, and thus the extent to which cyber resiliency matters to the system. In Step 3, trade-offs are made between alternative implementations and placements of mechanisms that provide security and resilience-related functionality. Those trade-offs take into consideration the relative importance of the aspects of cyber resiliency (anticipate, withstand, recover, adapt), based on the organization's risk management strategy (see discussion of Task 1-4, above). They can also take into consideration the potential effects of different implementations and architectural decisions on adversary activities. Different approaches to implementing cyber resiliency techniques have been analyzed in terms of potential effects on the adversary.

[7] Segments are typically identified with missions, business areas, or common services or infrastructures provided across the organization.

© 2016 The MITRE Corporation. All rights reserved.
Approved for Public Release; Distribution Unlimited. Case No. 16-0776.

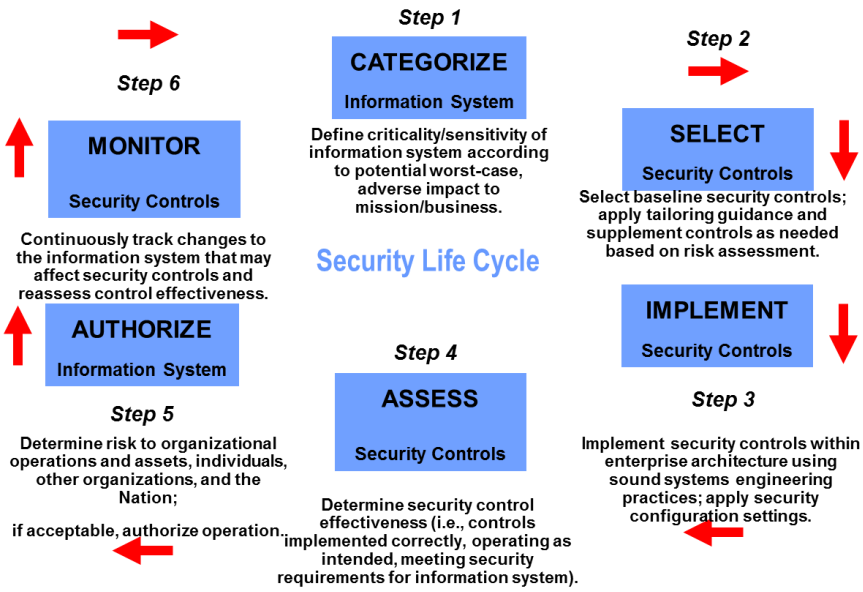

Figure 4: RMF at the System Level

As part of Step 4, system testing can include adversarial or penetration testing, which can result in recommended procedures to improve resilience in the presence of compromise. (See, for example, the DoD Guidelines for Cybersecurity DT&E [8].) When risk is determined in Step 5, the risk reduction associated with improved cyber resilience is taken into consideration. Risk is a combination of likelihood and impact. While cyber resilience measures (e.g., architectural decisions, technical mechanisms, operational procedures) can (by providing capabilities to Anticipate) reduce the likelihood of specific adversary actions, their primary benefit comes from how they reduce the severity of the impacts of attacks by reducing the intensity, scope or scale, or duration of attack effects.

As noted in the discussion of Task 4-1 above, risk monitoring can include monitoring of the effectiveness of implementations of cyber resiliency techniques.

Cyber Resiliency and the NIST SP 800-53 and CNSSI 1253 Baselines

Both the NIST and the CNSSI 1253 baselines have only a limited consideration of cyber resiliency. There are 155 cyber resiliency controls in NIST SP 800-53 R4. The CNSSI 1253 HHH baseline consists of 462 controls and the NIST High baseline consists of 342 controls. Of those 68 in the CNSSI 1253 HHH baseline (or about 15%) and 30 for the NIST High baseline (or about 6%) are resiliency focused. Even in the CNSSI 1253 HHH baselines the resiliency controls that are selected are those that largely support techniques such as privilege restriction, analytic monitoring, redundancy, substantiated integrity, and privilege restriction. Controls that support techniques such as diversity, deception, non-persistence, and dynamic positioning are largely not included in the baselines.

This is relevant because different techniques have different effects on the adversary. Various possible effects are described in Table 1.

© 2016 The MITRE Corporation. All rights reserved.
Approved for Public Release; Distribution Unlimited. Case No. 16-0776.

Potential Effects of Risk Mitigations on Adversary Activities
Redirect (includes Deter, Divert, and Deceive): *Direct adversary activities away from defender-chosen targets.*
Deter: Discourage the adversary from undertaking further activities, by instilling fear (e.g., of attribution or retribution) or doubt that those activities would achieve intended effects (e.g., that targets exist).
Divert: Lead the adversary to direct activities away from defender-chosen targets.
Deceive: Lead the adversary to believe false information about defended systems, missions, or organizations, or about defender capabilities or TTPs.
Preclude (includes Prevent and Preempt): *Ensure that specific threat events do not have an effect.*
Preempt: Forestall or avoid conditions under which the threat event could occur or result in an effect.
Prevent: Create conditions under which the threat event cannot be expected to result in an effect.
Impede (includes Degrade and Delay): *Make it harder for threat events to cause adverse impacts.*
Degrade: Decrease the likelihood that a given threat event will have a given level of effectiveness or impact.
Delay: Increase the amount of time needed for a threat event to result in adverse impacts.
Detect: *Identify threat events or their effects by discovering or discerning the fact that an event is occurring, has occurred, or (based on indicators, warnings, and precursor activities) is about to occur.*
Limit (includes Contain, Shorten, Recover, & Expunge): *Restrict the consequences of threat events by limiting the damage or effects they cause in terms of time, cyber resources, and/or mission or business impacts.*
Contain*:* Restrict the effects of the threat event to a limited set of resources.
Shorten: Limit the duration of a threat event or the conditions caused by a threat event.
Recover: Roll back the consequences of a threat event, particularly with respect to mission impairment.
Expunge: Remove unsafe, incorrect, or corrupted resources that could cause damage.
Expose (includes Scrutinize and Reveal): *Reduce risks due to ignorance of threat events, and possible replicated or similar events in the same or similar environments.*
Scrutinize: Analyze threat events and artifacts associated with threat events, particularly with respect to patterns of exploiting vulnerabilities, predisposing conditions, and weaknesses, to inform more effective detection and risk remediation.
Reveal: Increase awareness of risk factors and relative effectiveness of remediation approaches across the stakeholder community, to support common, joint, or coordinated risk response.

Table 1: Effects on the Adversary

From a security perspective it is best to have as broad an effect as possible on the adversary because the adversary's attacks will change and evolve over time, and the broad selection of possible effects on the adversary will provide greater flexibility and agility to the defender. Looking at the controls that are selected in the HHH baseline, and the techniques those controls support, the following observations can be made with regards to effects on the adversary:

- Well addressed: Detect and Recover
- Addressed: Analyze
- Partially addressed: Contain, Degrade and Delay
- Marginally addressed: Curtail, Prevent
- Missing: controls that Deter, Deceive, or Divert the adversary, or Expunge adversary modifications or insertions

Understanding which effects on the adversary are not covered by the HHH baseline controls may provide sufficient justification for an organization interested in maximizing mission continuity for selecting cyber resiliency controls that do not appear in the baseline.

© 2016 The MITRE Corporation. All rights reserved.
Approved for Public Release; Distribution Unlimited. Case No. 16-0776.

Cyber Resiliency and Tailoring: Supporting Risk-Related Trade-Offs

Some organizations might be hesitant to include cyber resiliency controls outside those specified in a baseline because they are concerned that this will impose an **additional** cost to implementing the new controls and the controls already identified in the baselines. That concern is based on a false assumption (that the controls in the baseline are mandatory) – but the truth is that the RMF does **not** require organizations to implement all the controls in a baseline. The entire purpose of the RMF is that organizations are to make risk management trade-offs with regards to security, just as systems engineers make trade-offs with regards to multiple drivers. Trading off conventional cyber security controls for those better suited for addressing cyber resiliency is consistent with the underlying principle of the RMF[8].

Thus an organization might select SC-36 (Honeypots), SC-35 (Honeyclients) and SC-44 (Detonation Chambers), none of which appear in any of the existing baselines, and trade-off controls focused on malware detection such as SI-3, SI-3 (1), and SI-3 (2). The rationale for the trade-off would be that SC-36, SC-35, and SC-44 reflect different ways to trigger and detect malware in a safe environment without the requiring malware (virus) signatures.

Alternatively an organization might choose to eliminate controls that support one resiliency technique and replace it with one that supports another technique. Thus for some parts of the infrastructure organization might choose to not implement SI-4 (2) [Information System Monitoring | Automated Tools for Real-Time Analysis], and instead implement SI-14 (Non-Persistence). The rationale for this choice would be that trying to detect the actions of the advanced persistent threat, who by definition is stealthy, is very challenging. Therefore, it might be better to periodically (possibly frequently) refresh services via non-persistence and in so doing effectively "flush" the adversary from the system even without detecting them. Again, this is something that the RMF allows.

Summary

The RMF and cyber resiliency are compatible concepts. This paper illustrates their compatibility, whether the RMF is considered as an organizational approach to risk management (frame, assess, respond, and monitor); an application of that approach at the mission / business process tier to define enterprise, mission segment, and information security architecture; or as a set of steps that apply the approach to an information system (using the six steps in NIST SP 800-37 and DoDI 8500.01). For an information system, cyber resiliency fits particularly well into the RMF step for selecting and tailoring NIST SP 800-53 controls and associated baselines; the process of tailoring such baselines to add resiliency specific controls and potentially trade-off conventional security-focused controls for cyber resiliency-focused controls is totally consistent with the RMF. In all these cases, the relative concern for cyber resiliency is merely one more factor to consider in making risk management trade-offs.

[8] *"The use of the term baseline is intentional. The security controls and control enhancements in the baselines are a starting point from which controls/enhancements may be removed, added, or specialized based on the tailoring guidance…" per section 3.1 of NIST 800-53 R4.*

© 2016 The MITRE Corporation. All rights reserved.
Approved for Public Release; Distribution Unlimited. Case No. 16-0776.

References

[1] NIST, "NIST SP 800-39, Managing Information Security Risk: Organization, Mission, and Information System View," March 2011. [Online]. Available: http://csrc.nist.gov/publications/nistpubs/800-39/SP800-39-final.pdf.

[2] 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.

[3] 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.

[4] CNSS, "Security Categorization and Control Selection for National Security Systems (CNSSI No. 1253), Version 2," 15 March 2012. [Online]. Available: http://www.disa.mil/Services/DoD-Cloud-Broker/~/media/Files/DISA/Services/Cloud-Broker/cnssi-security-categorization.pdf.

[5] CNSS, "National Information Assurance (IA) Glossary (CNSS Instruction No. 4009)," 26 April 2015. [Online]. Available: https://www.cnss.gov/CNSS/openDoc.cfm?hldYMe6UHW4ISXb8GFGURw==.

[6] 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.

[7] Office of the President, "Presidential Policy Directive (PPD) 21 -- Critical Infrastructure Security and Resilience," 12 February 2013. [Online]. Available: http://www.whitehouse.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil.

[8] DoD CIO, "Department of Defense Instruction (DoDI) 8500.01, Cybersecurity (Draft)," 15 January 2013.

[9] 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 or http://www.defenseinnovationmarketplace.mil/resources/20150527_Cyber_Resiliency_Engineering_Aid-Cyber_Resiliency_Techniques.pdf.

[10] Body of Knowledge and Curriculum to Advance Systems Engineering (BKCASE) project of INCOSE, IEEE, and SERC, "Systems of Systems (SoS)," Systems Engineering Body of Knowledge, SEBoK v. 1.5.1, 18 December 2015. [Online]. Available: http://sebokwiki.org/wiki/Systems_of_Systems_(SoS).

[11] OSD, "Systems Engineering Guide for Systems of Systems, Version 1.0," August 2008. [Online]. Available: http://www.acq.osd.mil/se/docs/SE-Guide-for-SoS.pdf.

[12] D. Bodeau, J. Brtis, R. Graubart and J. Salwen, "Resiliency Techniques for System of Systems: Extending and Applying the Cyber Resiliency Engineering Framework to the Space Domain (MTR 130515, PR 13-3513)," September 2013. [Online]. Available: http://www.mitre.org/sites/default/files/publications/13-3513-ResiliencyTechniques_0.pdf.

[13] Department of Defense, "Department of Defense Cybersecurity Test and Evaluation (T&E) Guidebook, Version 1.0," 1 July 2015. [Online]. Available: https://acc.dau.mil/adl/en-US/722865/file/80161/Cybersecurity%20TE%20Guidebook%20July%201%202015%20v1_0.pdf.

[14] A. Temin and S. Musman, "A Language for Capturing Cyber Impact Effects, MTR 100344, PR 10-3793," The MITRE Corporation, Bedford, MA, 2010.

© 2016 The MITRE Corporation. All rights reserved.
Approved for Public Release; Distribution Unlimited. Case No. 16-0776.

[15] DoD Defense Science Board, "Task Force Report: Resilient Military Systems and the Advanced Cyber Threat," January 2013. [Online]. Available: http://www.acq.osd.mil/dsb/reports/ResilientMilitarySystems.CyberThreat.pdf.

© 2016 The MITRE Corporation. All rights reserved.
Approved for Public Release; Distribution Unlimited. Case No. 16-0776.