MTR100308

MITRE TECHNICAL REPORT

MITRE

Cyber Security Governance

A Component of MITRE's Cyber Prep Methodology

Deb Bodeau, Steve Boyle, Jenn Fabius-Greene, Rich Graubart

September 2010

Sponsor:
Dept. No.: G020
Contract No.:
Project No.: 01CCG005-AD

This page intentionally left blank.

Abstract

Cyber Prep is a conceptual framework, together with a practical methodology, which an organization uses to define and implement its strategy for addressing adversarial threats related to its dependence on cyberspace. In particular, Cyber Prep enables organizations to articulate their strategies for addressing the advanced persistent threat (APT). The Cyber Prep framework defines five levels of organizational preparedness, characterized in terms of

- The organization's perspective on, and/or assumptions about, the threat it faces;
- The organization's strategy for addressing the threat, including which adversary tactics, techniques, and procedures (TTPs) it addresses; and
- The organization's approach to cyber security governance.

This white paper presents the governance component of Cyber Prep. As with the component that addresses technical and operational security measures, Cyber Prep expects that organizations apply sound principles for information systems security governance and make effective use of standards of good practice for security management. The cyber security governance component of Cyber Prep focuses on what organizations must do differently from or in addition to generally accepted information security governance practices in order to address the APT. In Cyber Prep, the five levels of organizational preparedness entail different approaches to

- Strategic integration. To what extent is the cyber security strategy integrated with other organizational strategies? To what extent does the strategy extend beyond the organization?
- Disciplines. What disciplines are part of, or aligned with, cyber security?
- Risk mitigation approaches. To what extent does the organization focus on compliance with standards vs. state of the practice security engineering vs. state of the art?
- Adaptability / agility of cyber decision making. To what extent do governance and decision making address the concern that adversaries may target decision makers and decision processes?
- Senior engagement. What is the highest level of official or staff member within the organization actively engaged in cyber security decision making?
- Cyber risk analytics. How are threats modeled and risks contextualized and assessed?

This page intentionally left blank.

Table of Contents

List of Tables

This page intentionally left blank.

Cyber Security Governance

1 Introduction

Cyber Prep is a conceptual framework, together with a practical methodology, which an organization uses to define and implement its strategy for addressing adversarial threats related to its dependence on cyberspace. In particular, Cyber Prep enables organizations to articulate their strategies for addressing the advanced persistent threat (APT). The Cyber Prep framework [1] defines five levels of organizational preparedness, characterized in terms of

- The organization's perspective on, and/or assumptions about, the threat it faces [2],
- The organization's overall strategy for addressing the cyber threat (see Table 1, below), including which adversary tactics, techniques, and procedures (TTPs) it addresses.
- The organization's approach to cyber security governance.

This white paper presents the governance component of Cyber Prep, which is driven by the organization's overall cyber security strategy.[1] The governance component complements the part of Cyber Prep that addresses technical and operational security measures, which is driven by the organization's assumptions and/or knowledge about adversary TTPs as well as its strategies regarding

- Which architectural approaches the organization takes;
- Which technical and operational security measures the organization selects from generally accepted standards of good practice, tailors, supplements, and uses [3];
- When and how the organization adopts new architectural, technical, and/or operational approaches.[2]

Cyber Prep expects that organizations apply sound principles for information systems security governance (see Appendix B) and make effective use of standards of good practice for security management.[3] The cyber security governance component of Cyber Prep focuses on what organizations must do differently from or in addition to generally accepted information security governance practices in order to address the APT. Cyber security governance determines how generally-accepted management controls (including, in particular, risk assessment controls) are tailored, supplemented, and used in the face of the APT. Cyber security governance also reflects the overall enterprise risk management strategy and enterprise risk governance framework. In Cyber Prep, the five levels of organizational preparedness entail different approaches to

- Strategic integration. To what extent is the cyber security strategy integrated with other organizational strategies? To what extent does the strategy extend beyond the organization?
- Disciplines. What disciplines are part of, or aligned with, cyber security?

[1] In the Cyber Prep methodology, cyber security is characterized by the goal of reducing mission, organizational, and personal risks due to dependence on cyberspace in the presence of adversarial threats. Cyber security thus differs from conventional information security in its emphasis on cyberspace (see footnote 6, below), in its emphasis on adversarial threats (as contrasted with threats of human error, natural disaster, or infrastructure failure), and by its relationship with mission assurance (see Section 2.2 below).

[2] See the Cyber Prep Concept of Operations [4] for more information about how the organization defines, applies, and monitors the effects of these strategies.

[3] Implementing sound information security governance and management is part of achieving Cyber Prep levels 1 and 2. Cyber Prep levels 3-5 assume this as a foundation.

- Risk mitigation approaches. To what extent does the organization focus on compliance with standards vs. state of the practice vs. state of the art?
- Adaptability / agility of cyber decision making. To what extent do governance and decision making address the concern that adversaries may target decision makers and decision processes?
- Senior engagement. What is the highest level of official or staff member within the organization actively engaged in cyber security decision making?
- Cyber risk analytics. How are threats modeled and risks contextualized and assessed?

These detailed aspects of cyber security governance are presented in Section 2. A given organization may not achieve a uniform level across these aspects. However, since the aspects are interdependent, broad disparities in levels of different aspects draw the overall cyber security governance level toward the lowest common denominator. Section 3 presents a unified view, for each Cyber Prep level, of cyber security governance at that level. Readers who want to understand how cyber security governance applies to their organization may prefer to use Table 1 to identify the Cyber Prep level that best reflects their organization's strategy, look at the unified view of cyber security governance for that level in Section 3, and then refer to Section 2 for details.

1.1 Governance

In general, *governance* is the set of responsibilities and practices exercised by those responsible for an enterprise (e.g., the board and executive management in a corporation, the agency head for a Federal agency) with the goal of providing strategic direction, ensuring that objectives are achieved, ascertaining that risks are managed appropriately and verifying that the enterprise's resources are used responsibly.[4] Risks and resources can be associated with different domains (e.g., information technology or IT, finance, legal and regulatory compliance, information security), and different domains require specialized expertise in order to manage risks. Thus, enterprise governance frequently is organized by domain.[5]

Cyber security governance refers to the component of enterprise governance that addresses the enterprise's dependence on cyberspace in the presence of adversaries.[6] Cyber security governance thus encompasses information systems security governance; whether information systems security governance can be identified with information security governance depends upon how narrowly or broadly the enterprise construes information security.[7] However, while aspects of information security governance may address information outside of cyberspace, the flow of information between the non-cyber and cyber realms is so prevalent that in general it is preferable for cyber security governance to encompass information security governance.

---

[4] This definition is adapted from the IT Governance Institute (ITGI) [5]. The Chartered Institute of Management Accountants (CIMA) and the International Federation of Accountants (IFAC) also adopted this definition in 2004. Governance – particularly risk governance or cyber security governance – can have a trans-organizational and even trans-national form. This is outside the scope of Cyber Prep; see Appendix B.2.1 for further discussion.

[5] For more information on IT governance and information security governance, see Appendix B.

[6] In Cyber Prep, cyberspace is ~~"t~~he collection of information communications and technology (ICT) infrastructures, applications, and devices on which the organization, enterprise, or mission depends, typically including the Internet, telecommunications networks, computer systems, personal devices, and (when networked with other ICT) embedded sensors, processors, and controllers." This definition is intended to be consistent with a variety of existing characterizations [6, 7, 8].

[7] For example, [9] distinguishes between information system security and information security; the latter includes protection of information in spoken and hardcopy paper forms. However, for Federal systems, information security applies to information systems, the definition of which does not specify information technology [10].

While governance entails day-to-day management activities, its perspective is inherently strategic. In the Cyber Prep framework, each Cyber Prep level is characterized by an underlying organizational strategy for addressing the cyber threat, as indicated in Table 1. The organizational strategy, cyber security governance, and security safeguards for each level build on those of all lower levels.

Table 1. Underlying Organizational Strategies for Cyber Prep Levels

Cyber Prep Level	Organizational Strategy
5: Pervasive Agility	The organization maintains operations on a continuing basis and adapts to current and future coordinated, successful attacks, regardless of their origins. The organization employs a highly agile, adaptive, and flexible structure that permeates all aspects of the organization (including planning, supply chains, collaboration, architecture, governance, and resources), allowing the organization to continually and dynamically reshape all aspects of its technology and operations in face of changing, successful attacks.
4: Architectural Resilience	The organization shapes its business or mission processes and system architecture to provide attack tolerance, designing and operating systems with the concepts of resilience and protection through multiple distinct enclaves, so that the organization can limit exfiltration of critical information, contain adversaries, and operate through (even in degraded mode) and recover from a successful attack.
3: Responsive Awareness	The organization deploys capabilities to detect and respond to indications of attempts to gain a foothold within the organization's information infrastructure, complementing these capabilities with procedures to better understand the methods of the adversary.
2: Critical Information Protection	The organization identifies and protects critical data regardless of its location, using encryption, enhanced identification & authentication and access control methods.
1: Perimeter Defense	The organization establishes and defends the information system perimeter; protects against the introduction of known malicious code/malware and discourages unauthorized internal access; and uses commercial security products and professionally manages perimeter and desktop systems.

An organization's cyber security governance structures and practices enables it to make consistent and understandable decisions about

- Investing in security measures:
    - What is the long-term plan for investing in cyber security? Which security measures need to be integrated into enterprise systems and/or mission or business functions first?
    - For which security measures (if any) is the organization willing to be an early adopter?
- Aligning cyber security risk management with other aspects of enterprise risk management:
    - What is the relative priority of cyber security investment as compared with other types of investments?

- Which cyber security investments are also investments in mission assurance and/or business continuity? Which are intended primarily to demonstrate due diligence or compliance with standards of good practice?
- How can the organization make cyber security investment decisions and other information and communications technology (ICT) investment decisions synergistically rather than antagonistically? In particular, how will the organization evolve its enterprise architecture to provide improved resilience and/or to address an increasingly adaptive threat?

- Managing the organization's cyber security posture:
  - Which cyber security investment decisions are reserved for the organization's senior management (e.g., Chief Information Officer or Chief Information Security Officer), and which are delegated to sub-organizations?
  - Which cyber security operational decisions are reserved for the organization's senior management, and which are delegated to sub-organizations and/or operators of specific systems, applications, or networks?
  - How does senior management ensure coordination and reporting of sub-organizational decisions and their consequences?

1.2 Governance and Maturity

A growing body of governance models are often accompanied by (generic or security-specific) capability maturity models. In general, maturity levels are based on the set of models in the Capability Maturity Model Integration (CMMI, [11, 12]). Maturity models for information security development and/or management processes are discussed in more detail in Appendix B.

An organization should plan to achieve the equivalent of maturity level 2 (defined process) as part of achieving either Cyber Prep level 1 or 2. For Cyber Prep levels 3-5, consideration of the APT requires the organization to extend its IT / information security governance structures and practices to facilitate inter-organizational collaboration for attack sensing, warning, and response as well as to provide for essential mission continuity. Thus, for Cyber Prep levels 3-5, minimum governance maturity levels roughly map to Cyber Prep levels (e.g., Cyber Prep level 4 entails the equivalent of "managed and measurable" governance, to use CMMI-speak).

1.3 Governance and Organizational Structure

Cyber Prep does not specify a type of organizational structure for governance, but does assume some decisions must be centralized.[8] In this, Cyber Prep is consistent with NIST SP 800-100 [13, 14]. Cyber Prep thus accommodates but does not require the more specific "wiring diagrams" provided by the IT Governance Institute (ITGI, [9, 15]) and the Software Engineering Institute at Carnegie Mellon University (SEI/CMU, [16]).

For Federal departments and agencies, the Joint Task Force Transformation Initiative Interagency Working Group has defined a three-tiered risk management hierarchy in its Risk Management Framework (RMF, [17]). At the top or organizational tier, the Risk Executive (Function) (REF) provides oversight and governance; the organization establishes its risk assessment methodologies, risk mitigation approaches, overall risk tolerance, and risk

[8] See Appendix B for a discussion of the different approaches (centralized, decentralized, and federated or hybrid) to IT and, by extension, information security governance.

monitoring approaches. Cyber security governance in Cyber Prep is situated at this tier: it establishes the structures, processes, and practices that enable the organization as a whole to identify its target Cyber Prep level, define a roadmap for achieving that target, and ensure that its cyber security roadmap is consistent with strategic planning activities in other domains of enterprise governance.

However, governance at the top tier is informed by and determines activities at lower tiers. Related activities at the middle or mission / business process tier include defining and implementing an enterprise architecture; categorizing critical information, functions, and information flows; and ensuring that the organization-wide information protection strategy informs all mission or business processes. Related activities at the lowest or information system tier include selecting, supplementing, and tailoring system security controls. In Cyber Prep, the organization's strategy for addressing the cyber threat is informed by and shapes activities at these two lower tiers. In particular, decision-making agility is needed to ensure organizational resilience in the face of disruptive attacks.

2 Aspects of Cyber Security Governance

In Cyber Prep, the five levels entail different approaches to security engagement, strategic integration, allied disciplines, cyber risk mitigation, adaptability or agility of cyber decision making, and cyber risk analytics. These approaches affect how standards of good practice for security management are adapted, tailored, and supplemented to enable the organization to be prepared for the threat it faces. This section describes how the approaches vary depending on the organization's target cyber preparedness level.[9] For an integrated description of cyber security governance at each Cyber Prep level, see Section 3.

2.1 Strategic Integration

Strategic integration addresses the extent to which the cyber security strategy is *integrated* into enterprise risk management (ERM), and larger mission assurance and security strategies within and beyond the enterprise. This ranges from *no integration* (as each program or business process defines and implements its own security strategy) to *consistency*, in which the officials responsible for different mission, business, or risk domains[10] ensure that execution of strategy in one domain will not preclude execution of strategy in another domain, to *coordination*, in which the officials responsible for different strategies work together on execution planning to make more effective use of enterprise resources, to *full integration*, in which strategies for different domains are included in an overarching enterprise-wide mission assurance strategy across each enterprise mission or across the critical infrastructure sector of which the enterprise is a part.

More specifically, strategic integration addresses the extent to which the cyber security strategy relates to, is informed by and informs other organizational risk management strategies. These typically include strategies in the areas of acquisition and/or program management, architecture, business continuity, and (at the higher levels) mission assurance, as indicated in Table 2.

[9] Cyber Prep assumes that an organization will adapt these approaches to its organizational – and hence governance – structure, as well as to its cyber risk orientation (described in more detail in the Cyber Prep Concept of Operations [4]).

[10] Organizations structure ERM in different ways, depending in part on organizational structure, mission, and culture. Thus, for some organizations mission or business functions are the central aspects of enterprise risk management. Others define different risk domains – e.g., financial, regulatory, operational – and rely on specialized expertise in those domains. Cyber Prep does not assume any specific approach to enterprise risk management; however, at the higher Cyber Prep levels, an organization is assumed to perform ERM.

Table 2. Integration of Cyber Security Strategy with Other Organizational Strategies[11]

Cyber Prep Level	Integration of Cyber Security Strategy with Other Organizational Strategies
5: Pervasive Agility	**Full integration of cyber security into the organization's mission assurance strategy, which is a significant** part of the organization's mission and enterprise risk management strategies.
4: Architectural Resilience	**Coordination of** architectural and acquisition strategies **with** cyber security strategy; cyber security **strategy** is part of **mission assurance strategy, which** is part of **the organization's mission and** enterprise risk management **strategies**.
3: Responsive Awareness	**Consistency between cyber security, architectural, and acquisition strategies; cyber** security is part of **enterprise** risk management.
2: Critical Information Protection	**Coordination of information security with business continuity;** information security is part of **larger-scale risk management (e.g., coordinated management of information, IT, compliance, and business risks).**
1: Perimeter Defense	**No integration; information security is part of programmatic risk management.**

Strategic integration has a ~~"b~~eyond the enterprise" component, reflecting the ways in which the organization engages with service providers, business partners or suppliers, with customers, and with other organizations in the organization's critical infrastructure sector. With respect to cyber security practices, this extra-organizational integration takes such forms as information sharing, coordination, agreement on standards for information exchange, agreement on standards of good practice, etc., and complements other forms of integration or collaboration beyond the enterprise.[12] With respect to risk governance,[13] strategic integration beyond the enterprise ranges from working relative isolation to participation in the ongoing discussion which is shaping the collective understanding of the cyber security problem domain. Levels of strategic integration beyond the enterprise are indicated in Table 3.

[11] Bolding indicates an incremental change from the level below. Unless otherwise noted, the characteristics of each Cyber Prep level include and build on those of all lower levels.
[12] For example, approaches to securing the supply chain (which are addressed as part of the Security Measures component of Cyber Prep) entail extra-organizational integration.
[13] See Appendix B.2 for more information on risk governance.

Table 3. Strategic Integration Beyond the Enterprise

Cyber Prep Level	Degree of Cyber Security Integration Beyond the Enterprise
5: Pervasive Agility	Coordinate with cyber security counterparts in **other organizations in the organization's mission or critical infrastructure sector, as well as in** partner, supplier, and customer organizations, to support shared **information-gathering about, analysis of, preparation for, and** response to threats, and so that the organization's cyber security strategy is **part of a mission-wide or sector-wide mission assurance strategy**. Engage with (or, at a minimum, maintain awareness of the activities of) bodies working on better understanding **the cyber security problem domain and related trade-offs.**
4: Architectural Resilience	**Coordinate** with cyber security counterparts in partner, supplier, and customer organizations, to support shared **response to** threats **and so that the organization's cyber security strategy is not undermined by strategic weaknesses in those organizations. Engage with (or, at a minimum, maintain awareness of the activities of) bodies working on better understanding of cyber threats, consequences, and risk mitigation approaches.**
3: Responsive Awareness	**Engage** with cyber security counterparts in **peer**, partner, supplier, and **customer** organizations, to support shared awareness of threats and detect incidents. Engage with owners and operators of systems, services, and infrastructures beyond the organization, to ensure that dependencies do not impose unknown or intolerable risks on the organization.
2: Critical Information Protection	Share information with cyber security **counterparts in partner and** supplier organizations, **to support shared awareness of threats and detect incidents. Engage with owners and operators of systems, services, and infrastructures beyond the organization, to ensure that dependencies do not impose unknown or intolerable risks on the organization**.
1: Perimeter Defense	**Share information about security needs and concerns with cyber security staff in ICT supplier organizations.**

2.2 Allied Disciplines

At a minimum, cyber security includes the disciplines of information system or IT security and communications security. However, other technical security disciplines, depending on how cyberspace is defined, can also be part of cyber security. At the higher Cyber Prep levels, the focus moves from cyber security to mission assurance in the presence of cyber threats.

Cyber security relies on effective security measures outside of cyberspace. The relationship between other disciplines and cyber security at the different Cyber Prep levels, particularly information security, is indicated in Table 5. The key difference is between *alignment* and *integration*. Alignment involves information sharing and coordination among operational managers in the different areas, as well as some coordination among the strategic planners in those areas. Integration involves a shared understanding of threats and consequences, and closely coupled risk management strategies among the strategic planners for the different areas, possibly leading to changes in how the areas are defined or managed. Operationally, integration involves collaboration among practitioners in the different disciplines.

Table 4. Relationship of Cyber Security to Other Security and Mission Assurance Disciplines

Cyber Prep Level	Relationship of Cyber Security to Other Security and Mission Assurance Disciplines
5: Pervasive Agility	Physical security, personnel security, business continuity, SCRM, ICT architecture, business process engineering, operations security, and cyber security are integrated with mission assurance.
4: Architectural Resilience	Physical security, personnel security, business continuity, **supply chain risk management (SCRM)**, ICT architecture, **business process engineering**, operations security, **and cyber security are integrated with mission assurance**.
3: Responsive Awareness	Physical security, personnel security, business continuity, **ICT architecture, and operations security are integrated** with cyber security.
2: Critical Information Protection	Physical security, **personnel security, and business continuity are** aligned with cyber security. Cyber security **includes** ICT, **information, and communications** security.
1: Perimeter Defense	**Physical security is aligned with cyber security. Cyber security is identified with ICT security.**

2.3 Cyber Risk Mitigation Approach

The organization's cyber risk mitigation approach reflects its relative priorities regarding compliance with standards of good practice versus proactive investment in new mitigation techniques. At the lower Cyber Prep levels, the organization can focus on compliance with standards of good practice, so that cyber security governance is strongly identified with compliance.[14] At the higher levels, the persistence, inventiveness, and adaptability of the adversary motivate the organization to push the state of the practice and even the state of the art.

At the higher levels, the organization needs to make trade-offs, for example between mitigating the cyber security risks associated with adversary TTPs and increasing the programmatic risks of integrating new technologies into the organization's systems or enterprise architecture. In some situations, novel approaches to mitigating cyber security risks can diverge from standards of good practice. For example, the organization could decide that the benefits of increasing knowledge about the adversary could warrant a period of increased exposure to malicious activity, while standard practice would be to shut down avenues of suspicious behavior. The organization's trade-offs are guided by its risk tolerance.[15]

[14] Thus, organizations at the lower levels may treat cyber security governance as part of governance, risk and compliance (GRC). See Appendix B for further discussion of GRC. For information security, standards of good practice include NIST publications, the ISO 27000 series, and COBIT [15]. For broader risk management, standards of good practice include ISO 31000 and the Enterprise Risk Management (ERM) framework promulgated by the Committee of Sponsoring Organizations of the Treadway Commission (COSO).

[15] See the Cyber Prep Concept of Operations for further discussion of risk tolerance.

Table 5. Cyber Risk Mitigation Approach

Cyber Prep Level	Approach to Cyber Risk Mitigation
5: Pervasive Agility	Cyber security builds on standards of good practice, but pushes **the state of the art to ensure continued security evolution in the face of an innovative adversary**.
4: Architectural Resilience	Cyber security **builds on** standards of good practice, but pushes the state of the practice **by incorporating state of the art techniques, sometimes at the expense of non-compliance with standards of good practice**.
3: Responsive Awareness	**Cyber security includes conformance** with standards of good practice, **but pushes the state of the practice to address the advanced threat**.
2: Critical Information Protection	Information security is identified with compliance with standards of good practice, **in the context of broader risk management**.
1: Perimeter Defense	**Information security is identified with compliance with standards of good practice.**

2.4 Adaptability and Agility

Adversary activities can affect the organization's ability to carry out its normal business or mission functions, including those functions that are designed to enable the organization to handle disruptions. Computer security incident handling is part of generally accepted information security governance practices (see Appendix B for further discussion), and handling of ICT disruptions is commonly part of business continuity planning. However, business continuity planning does not usually address adversary activities, which can be intended to disrupt decision making (or can have such disruption as a side effect). Thus, adaptability and agility need to be built into cyber security decision making processes, providing alternative lines of communications, control, and processing.

At the lower Cyber Prep levels, the effects of adversary activities are assumed to be only moderately disruptive; attacks are assumed to be of limited scope and duration, and not targeted at decision makers. Thus, disruption of decision making processes is also expected to be limited. At the higher Cyber Prep levels, the organization needs well-defined alternative processes for communications and decision making. These processes need to consider the fact that adversaries may target decision makers and decision processes.

Table 6. Adaptability and Agility

Cyber Prep Level	Approach to Adaptability and Agility
5: Pervasive Agility	The organization has defined, implemented **and exercised** a process that provides for alternate cyber decision making, allowing for timely decisions and delegation of responsibilities, in the event that the adversary's actions results in a successful long term **destruction or severe** disruption of the primary decision making process, **or otherwise prevents it from acting in a timely manner**.
4: Architectural Resilience	The organization has defined **and implemented** a process that provides for alternate **critical** cyber decision making, **allowing for delegation of responsibilities**, in the event that the adversary's action **results in a successful long term disruption** of **key** aspects of the primary decision making process.
3: Responsive Awareness	The organization has **defined a** process that provides for limited alternate cyber decision making in the event that the adversary's action **disrupts critical** aspects of the primary decision making process.
2: Critical Information Protection	The organization **has an informal process intended to provide some limited alternate cyber decision making in the event** that the adversary's action results in minor or short term disruption of some aspects of the primary decision making process**.**
1: Perimeter Defense	**The organization's processes for decision making in the event that the adversary's action results in minor or short term disruption of some aspects of the primary decision making process are ad-hoc.**

2.5 Senior Engagement

This aspect of cyber security governance addresses how far up in the organization active engagement in cyber security strategic decision making goes. *Active engagement* involves strategic planning for, as well as enterprise-wide response to, situations in which adversaries might exploit the organization's dependence on cyberspace. A key indicator of active security engagement in the organization is the extent that senior leadership remains apprised of the organization's current posture vis-à-vis the threat (e.g., by an enterprise dashboard, by regularly scheduled and frequent briefings or emails). Active engagement can be contrasted with oversight, particularly with oversight to ensure compliance with laws, regulations, and standards of good practice, as a compliance orientation tends not to address the dynamic and adaptive nature of the advanced persistent threat.

As noted above, Cyber Prep accommodates a wide range of decision making structures, just as the Risk Management Framework accommodates a variety of ways in which the Risk Executive Function can be performed. Specific decision responsibilities may be delegated, particularly for day-to-day operations, or assigned to a group. However, at the higher Cyber Prep levels most strategic decisions – and even some operational decisions – require the engagement of the more senior members of management of the organization. For example, at level 4, actions needed to restore some mission or business functions or to limit damage from an attack may entail curtailing or limiting other functionality or connectivity, temporarily violating contractual agreements; the CEO or agency head typically needs to be involved in the decision to take such actions.

Table 7. Senior Engagement in Cyber Security Strategic Decision Making

Cyber Prep Level	Highest Level for Active Engagement in Cyber Security Strategic Decision Making
5: Pervasive Agility	**CEO or Agency head** actively engaged in **mission assurance** decisions**; senior official responsible for cyber security strategy** closely coordinates with near-term decision-makers; some near-term decisions are reserved for **the CEO or agency head** (or designated **senior official(s)** in cases of disruption).
4: Architectural Resilience	**Dedicated** corporate officer or agency official actively engaged in enterprise-level cyber security decisions; **closely coordinates with near-term decision-makers; some near-term decisions are reserved for the senior official (or designated alternate in cases of disruption).**
3: Responsive Awareness	**Responsible corporate officer or agency official** actively engaged in **enterprise-level cyber** security decisions.
2: Critical Information Protection	**Information Security Officer or Information Security Program Officer** actively engaged in information security decisions.
1: Perimeter Defense	**Program manager or business process owner actively engaged in information security decisions.**

2.6 Cyber Risk Analytics

To inform its decision making and strategic planning, the organization needs to identify, contextualize, and assess those cyber risk factors that inform its decisions. Key aspects of cyber risk analytics in Cyber Prep include

- Threat modeling. Cyber Prep allows an organization to tailor its governance and security measures to the threat it faces. The Cyber Prep levels differ in how explicit, specific, and up-to-date the organization's threat models need to be, in order to inform threat-based strategic planning as well as operational decisions. In addition, the Cyber Prep levels differ in terms of expected sources of threat information. At the lower levels, the organization can be expected to rely on public sources. At the higher levels, to provide support strategic integration, the organization needs to assess the credibility and relevance of its sources, and to work with other entities in its mission / business sector (e.g., via information sharing and analysis centers or ISACs, as part of a group such as the Defense Industrial Base or DIB[16]).
- Consequence modeling. The Cyber Prep levels differ in the types of consequences the organization considers, and the extent to which mission or business process dependencies on cyber resources are made explicit.
- Assessment. Cyber risk can be modeled in terms of a variety of factors, including factors related to threats, vulnerabilities, and consequences. While Cyber Prep does not specify a detailed risk model or risk taxonomy, it does assume that cyber security governance entails organizational awareness of some risk factors in order to inform decision making. The Cyber Prep levels differ in which types of risk factors are assessed, and how often.

[16] See http://www.dc3.mil/dcise/dciseAbout.php for more information about the Department of Defense (DoD)-Defense Industrial Base Collaborative Sharing Environment (DCISE).

At the higher levels, assessment is intended to support not only cyber security risk management, but also mission assurance and enterprise risk management.

Table 8. Cyber Risk Analytics

Cyber Prep Level	Cyber Risk Analytics
5: Pervasive Agility	The organization models different adversaries separately as feasible and appropriate to the organization and the missions it supports. The organization **continually** updates threat models based on observations, indicators, **assessed** information from external sources, **and closely-held information from trusted sources.** The organization models business / mission threads and their dependencies on cyber resources **as they change during the course of operations**, so that the consequences of compromise and response can be identified and managed **dynamically**. The organization defines and **continuously** assesses organization- **and/or mission/business sector-**related cyber risk factors to inform enterprise risk management.
4: Architectural Resilience	The organization **models different adversaries separately as feasible and appropriate to the organization.** The organization **frequently** updates threat models based on observations, indicators, and information from external sources, explicitly considering the APT. The organization models business / mission business / mission **threads and their** dependencies on cyber resources, so that the consequences of compromise **and response** can be identified and managed. The organization **defines and periodically** assesses **organization-related** cyber risk factors **(e.g., factors that characterize adversary capabilities, motivations, or activities; factors that indicate system resilience) to inform enterprise risk management.**
3: Responsive Awareness	The organization **periodically** updates its threat model **(or models)** based on observations, **indicators,** and information from external sources, **explicitly considering the advanced persistent threat**. The organization **models** business / mission dependencies on **cyber** resources, so that the consequences of **compromise** can be identified and managed. The organization assesses **common cyber risk factors (e.g., vulnerabilities, indicators of penetration activities), using tool-based assessment as possible**, and assesses the organizational consequences of **compromise of cyber resources.**
2: Critical Information Protection	The organization **periodically** updates its threat model **based on observations and information from external sources (e.g., CERT, ISAC, ICT industry members).** The organization identifies **business / mission dependencies on** information resources, **so that the consequences of disclosure or corruption can be identified and managed.** The organization assesses **organizational consequences of loss of information confidentiality, integrity, availability, and/or accountability (typically, low, moderate, or high).**
1: Perimeter Defense	**The organization updates its threat model infrequently, to reflect conventional wisdom (e.g., SANS, what is represented in relevant standards, what appears in the general business press, and/or what appears in the business press for the organization's business sector). The organization identifies high-value ICT resources (systems, applications, communications). The organization assesses vulnerabilities as produced by tools.**

3 Assessing an Organization's Cyber Security Governance

This section presents characteristics of cyber security governance for each Cyber Prep level. An approach for assessing how well an organization's cyber security governance conforms with a given Cyber Prep level is also provided. For each Cyber Prep level, the organization assesses how well a set of key assertions hold; the assessment is augmented with annotations explaining why the statement fails to be completely true. The organization will use those annotations to identify gaps in cyber security governance.

Depending on organizational preferences for how to present decision support values, the organization can express its assessments in qualitative and/or quantitative terms (i.e., as a score). The organization's culture and risk framing determine how the organization will assess its cyber security governance. For any statement that fails to be completely true of the organization, the organization takes into consideration how important or relevant that aspect of cyber security governance is to the organization. For example, an organization constrained by legal or regulatory requirements could be unable to push the state of the art (cyber risk mitigation approach at Level 5). Figure 9 provides an assessment scale that organizations can use. The organization can also weight the statements used in the assessment; if the organization defines a weighting, the second descriptions of High and Low in Table 9 should be deleted.

Table 9. Governance Assessment Scale

Qualitative Value	Description	Range	Typical Value
High	The statement, when applied to the organization, is true. *or* The ways in which the statement fails to be true of the organization are not meaningful or important, give the organization's culture, missions, and constraints. At the extreme, the statement is not applicable to the organization.	**90-100**	**95**
Medium	The statement, when applied to the organization, is largely true, with some caveats.	**50-89**	**70**
Low	The statement, when applied to the organization, is partially true. *or* The statement, when applied to the organization, is false, and the statement is somewhat meaningful or important to the organization.	**1-49**	**30**
None	The statement, when applied to the organization, is false, and the statement is meaningful and/or important to the organization.	**0**	**0**

3.1 Cyber Prep Level 1

At Cyber Prep Level 1, the organization believes the cyber threat is largely external and system-targeted, and that adversaries can be kept from penetrating perimeter defenses; thus, the situation is largely manageable via due diligence. The organization's strategy is to establish and defend the information system perimeter; protect against the introduction of known malicious code/malware and discourage unauthorized internal access; and use commercial security products and professionally manages perimeter and desktop systems. Thus, the focus is on information security at the program level. While Table 11 presents assertions that could be used in assessing Level 1 governance, an organization could also use one of the information security program maturity models mentioned in Appendix B.

Table 10. Characteristics of Cyber Security Governance at Cyber Prep Level 1

Characteristic	Cyber Security Governance
Strategic Integration	Information security is part of program risk management. The organization shares information about security needs and concerns with cyber security staff in ICT supplier organizations.
Allied Disciplines	Physical security is aligned with cyber security. Cyber security is identified with ICT security.
Cyber Risk Mitigation Approach	Information security is identified with compliance with standards of good practice.
Adaptability and Agility	The organization's processes for decision making in the event that the adversary's action results in minor or short term disruption of some aspects of the primary decision making process are ad-hoc.
Senior Engagement	Each program manager, business process owner, or business component manager is responsible for determining the cyber security policies and processes that apply to their component. Each manager is answerable to one or more corporate officers (e.g., General Counsel) for compliance with enterprise-wide policies, procedures, and practices that are determined by law, regulation, or contractual agreement.
Cyber Risk Analytics	The organization updates its threat model infrequently, to reflect conventional wisdom (e.g., SANS, what is represented in relevant standards, what appears in the general business press, and/or what appears in the business press for the organization's business sector). The organization identifies high-value ICT resources (systems, applications, communications). The organization assesses vulnerabilities as produced by tools.

Table 11. Assessing Conformance with Cyber Prep Level 1 Governance

Characteristic	Assertion	Assessment	Score[17]
Strategic Integration	Information security is part of program risk management.		
	The organization shares information about security needs and concerns with cyber security staff in ICT supplier organizations. *(Identify ICT supplier organizations, points of contact, and any organizational policies or procedures for sharing security information.)*		
Allied Disciplines	Physical security is aligned with cyber security. *(Indicate how the level of physical protection accorded to ICT resources is determined.)* Cyber security is identified with ICT security.		
Cyber Risk Mitigation Approach	Information security is identified with compliance with standards of good practice. *(Indicate which standards the organization seeks to comply with – e.g., NIST Risk Management Framework, ISO 27000 series.* [18]*)*		
Adaptability and Agility	The organization's processes for decision making in the event that the adversary's action results in minor or short term disruption of some aspects of the primary decision making process are ad-hoc.		
Senior Engagement	Each program manager, business process owner, or business component manager is responsible for determining the cyber security policies and processes that apply to their component.		
	Each manager is answerable to one or more corporate officers (e.g., General Counsel) for compliance with enterprise-wide policies, procedures, and practices that are determined by law, regulation, or contractual agreement. *(Identify security-cognizant corporate officers.)*		
Cyber Risk Analytics	The organization updates its threat model infrequently, to reflect conventional wisdom (e.g., SANS, what is represented in relevant standards, what appears in the general business press, and/or what appears in the business press for the organization's business sector). *(Identify the sources of information the organization uses regularly.)*		
	The organization identifies high-value ICT resources (systems, applications, communications). *(Identify the organization's process or procedures for doing so.)*		
	The organization assesses vulnerabilities as produced by tools. *(Identify the organization's vulnerability assessment tools.)*		
Overall Assessment	Extent to which the organization's cyber security governance enables it to maintain cyber preparedness at level 1 (if the organization uses quantitative scores, average or weighted average of scores for the six characteristics)		

3.2 Cyber Prep Level 2

At Cyber Prep Level 2, the organization believes the cyber threat is largely external and that adversaries can be kept from penetrating perimeter defenses; thus, the situation is largely manageable via due diligence. However, the organization recognizes that information, in any form or location, is also a target; the organization therefore recognizes the importance of identifying and safeguarding critical information, whether internal, external or transiting the organization's perimeter. While Table 13 presents assertions that could be used in assessing

[17] The score (if the organization uses quantitative scores) is the (weighted) average of scores for individual assertions.

[18] The Risk Management Framework (RMF) includes FIPS 199, FIPS 200, NIST 800-60, NIST SP 800-53, NIST SP 800-53A, and NIST SP 800-37. The International Standards Organization (ISO) family of standards for information security includes ISO 27000-27006 and 27011; others are in preparation.

Level 2 governance, an organization could also use one of the information security program maturity models mentioned in Appendix B.

Table 12. Characteristics of Cyber Security Governance at Cyber Prep Level 2

Characteristic	Cyber Security Governance
Strategic Integration	Information security is coordinated with business continuity; information security is part of larger-scale risk management (e.g., coordinated management of information, IT, compliance, and business risks). The organization shares information with cyber security counterparts in partner and supplier organizations, to support shared awareness of threats and detect incidents. The organization engages with owners and operators of systems, services, and infrastructures beyond the organization, to ensure that dependencies do not impose unknown or intolerable risks on the organization.
Allied Disciplines	Physical security, personnel security, and business continuity are aligned with cyber security. Cyber security includes ICT, information, and emanations security.
Cyber Risk Mitigation Approach	Information security is identified with compliance with standards of good practice, in the context of broader risk management.
Adaptability and Agility	The organization has an informal process intended to provide some limited alternate cyber decision making in the event that the adversary's action results in minor or short term disruption of some aspects of the primary decision making process.
Senior Engagement	An Information and/or Information Systems Security officer or program manager is responsible for determining and implementing controls to protect cyber assets, and for ensuring compliance with enterprise-wide policies, procedures, and practices for protecting information that are determined by law, regulation, or contractual agreement. This manager is answerable to one or more corporate officers or Agency officials (e.g., the Chief Technology Officer or CTO, the General Counsel).
Cyber Risk Analytics	The organization periodically updates its threat model based on observations and information from external sources (e.g., CERT, ISAC, ICT industry members). The organization identifies business / mission dependencies on information resources, so that the consequences of disclosure or corruption can be identified and managed. The organization assesses organizational consequences of loss of information confidentiality, integrity, availability, and/or accountability (typically, low, moderate, or high).

Table 13. Assessing Conformance with Cyber Prep Level 2 Governance

Characteristic	Assertion	Assessment	Score[19]
Strategic Integration	Information security is coordinated with business continuity; information security is part of larger-scale risk management (e.g., coordinated management of information, IT, compliance, and business risks). *(Identify coordination bodies, e.g., committees.)*		
	The organization shares information with cyber security counterparts in partner and supplier organizations, to support shared awareness of threats and detect incidents. *(Identify partner and ICT supplier organizations, points of contact, and any organizational policies or procedures for sharing security information.)*		
	The organization engages with owners and operators of systems, services, and infrastructures beyond the organization, to ensure that dependencies do not impose unknown or intolerable risks on the organization. *(Identify coordination bodies, e.g., committees).*		
Allied Disciplines	Physical security, personnel security, and business continuity are aligned with cyber security. Cyber security includes ICT, information, and emanations security. *(Identify coordination bodies, e.g., committees).*		
Cyber Risk Mitigation Approach	Information security is identified with compliance with standards of good practice, in the context of broader risk management. *(Indicate which standards the organization seeks to comply with. Identify standards or guidelines for broader risk management.)*		
Adaptability and Agility	The organization has an informal process intended to provide some limited alternate cyber decision making in the event that the adversary's action results in minor or short term disruption of some aspects of the primary decision making process. *(Describe the informal process.)*		
Senior Engagement	An Information and/or Information Systems Security officer or program manager is responsible for determining and implementing controls to protect cyber assets, and for ensuring compliance with enterprise-wide policies, procedures, and practices for protecting information that are determined by law, regulation, or contractual agreement.		
	This manager is answerable to one or more corporate officers or Agency officials (e.g., the Chief Technology Officer or CTO, the General Counsel). *(Identify security-cognizant corporate officers.)*		
Cyber Risk Analytics	The organization periodically updates its threat model based on observations and information from external sources (e.g., CERT, ISAC, ICT industry members). *(Identify the sources of information the organization uses regularly.)*		
	The organization identifies business / mission dependencies on information resources, so that the consequences of disclosure or corruption can be identified and managed. *(Describe the process.)*		
	The organization models business / mission threads and their dependencies on cyber resources as they change during the course of operations, so that the consequences of compromise and response can be identified and managed dynamically. *(Describe how the organization's model is maintained.)*		
	The organization assesses organizational consequences of loss of information confidentiality, integrity, availability, and/or accountability (typically, low, moderate, or high). *(Identify the organization's assessment guidance.)*		
Overall Assessment	Extent to which the organization's cyber security governance enables it to maintain cyber preparedness at level 2 (if the organization uses scores, (weighted) average of scores for the six characteristics.)		

[19] The score (if the organization uses quantitative scores) is the (weighted) average of scores for individual assertions.

3.3 Cyber Prep Level 3

At Cyber Prep Level 3, the organization understands that adversaries are penetrating its information infrastructure, and thus that it can no longer assume that perimeter-based protection will keep internal systems secure. The organization recognizes the need for a high degree of awareness to identify and respond to attempted incursions. The organization's objective is to deter adversaries from gaining a foothold in the organization's information infrastructure. The organization's strategy is to deploy capabilities to detect and respond to targeted penetration attempts within its information infrastructure, and to complement these capabilities with procedures to better understand adversary TTPs.

Table 14. Characteristics of Cyber Security Governance at Cyber Prep Level 3

Characteristic	Cyber Security Governance
Strategic Integration	The organization seeks consistency between its cyber security, architectural, and acquisition strategies; cyber security is part of enterprise risk management. The organization engages with cyber security counterparts in peer, partner, supplier, and customer organizations, to support shared awareness of threats and detect incidents. The organization engages with owners and operators of systems, services, and infrastructures beyond the organization, to ensure that dependencies do not impose unknown or intolerable risks on the organization.
Allied Disciplines	Physical security, personnel security, business continuity, ICT architecture, and operations security are integrated with cyber security.
Cyber Risk Mitigation Approach	Cyber security includes conformance with standards of good practice, but pushes the state of the practice to address the advanced threat.
Adaptability and Agility	The organization has defined a process that provides for limited alternate cyber decision making in the event that the adversary's action disrupts critical aspects of the primary decision making process.
Senior Engagement	A responsible corporate officer or agency official is actively engaged in enterprise-level cyber security decisions.
Cyber Risk Analytics	The organization periodically updates its threat model (or models) based on observations, indicators, and information from external sources, explicitly considering the advanced persistent threat. The organization models business / mission dependencies on cyber resources, so that the consequences of compromise can be identified and managed. The organization assesses common cyber risk factors (e.g., vulnerabilities, indicators of penetration activities), using tool-based assessment as possible, and assesses the organizational consequences of compromise of cyber resources.

Table 15. Assessing Conformance with Cyber Prep Level 3 Governance

Characteristic	Assertion	Assessment	Score[20]
Strategic Integration	The organization seeks consistency between its cyber security, architectural, and acquisition strategies; cyber security is part of enterprise risk management. *(Identify coordination bodies, e.g., committees.)*		
	The organization engages with cyber security counterparts in peer, partner, supplier, and customer organizations, to support shared awareness of threats and detect incidents. *(Identify organizations, points of contact, and any organizational policies or procedures for sharing security information.)*		
	The organization engages with owners and operators of systems, services, and infrastructures beyond the organization, to ensure that dependencies do not impose unknown or intolerable risks on the organization. *(Identify engagement forums – e.g., consortia – and mechanisms – e.g., contracts.)*		
Allied Disciplines	Physical security, personnel security, business continuity, ICT architecture, and operations security are integrated with cyber security. *(Identify the organizational structure, roles, and responsibilities.)*		
Cyber Risk Mitigation Approach	Cyber security includes conformance with standards of good practice, but pushes the state of the practice to address the advanced threat. *(Indicate which standards the organization seeks to comply with. Identify standards or guidelines for broader risk management. Describe how the organization decides when and how to push the state of the practice.)*		
Adaptability and Agility	The organization has defined a process that provides for limited alternate cyber decision making in the event that the adversary's action disrupts critical aspects of the primary decision making process. *(Describe the process.)*		
Senior Engagement	A responsible corporate officer or agency official is actively engaged in enterprise-level cyber security decisions. *(Identify the cognizant officer or official.)*		
Cyber Risk Analytics	The organization periodically updates its threat model (or models) based on observations, indicators, and information from external sources, explicitly considering the advanced persistent threat. *(Identify the sources of information the organization uses regularly.)*		
	The organization models business / mission dependencies on cyber resources, so that the consequences of compromise can be identified and managed. *(Describe the modeling process.)*		
	The organization assesses common cyber risk factors (e.g., vulnerabilities, indicators of penetration activities), using tool-based assessment as possible, and assesses the organizational consequences of compromise of cyber resources. *(Identify tools and assessment processes.)*		
Overall Assessment	Extent to which the organization's cyber security governance enables it to maintain cyber preparedness at level 3 (if the organization uses scores, (weighted) average of scores for the six characteristics).		

[20] The score (if the organization uses quantitative scores) is the (weighted) average of scores for individual assertions.

3.4 Cyber Prep Level 4

At Cyber Prep Level 4, the organization recognizes that it is not possible to keep the persistent adversary from, over time, establishing footholds within the organization's information infrastructure, including some which will remain undetected. The organization understands the importance of maintaining an operational capability in the face of adversaries who can launch successful cyber attacks from their persistent footholds. While continuing to deploy security measures to reduce the likelihood of successful attacks, the organization adopts a strategy of architectural resilience, designing and operating systems consistent with the concepts of resilience and protection through multiple distinct enclaves, so that the organization can limit exfiltration of critical information, contain adversaries, operate through (even in degraded mode), and recover from a successful attack.

Table 16. Characteristics of Cyber Security Governance at Cyber Prep Level 4

Characteristic	Cyber Security Governance
Strategic Integration	The organization's architectural and acquisition strategies are coordinated with its cyber security strategy; its cyber security strategy is part of its mission assurance strategy, which is part of the organization's mission and enterprise risk management strategies. The organization coordinates with cyber security counterparts in partner, supplier, and customer organizations, to support shared response to threats and so that the organization's cyber security strategy is not undermined by strategic weaknesses in those organizations. The organization engages with (or, at a minimum, maintains awareness of the activities of) bodies working on better understanding of cyber threats, consequences, and risk mitigation approaches.
Allied Disciplines	Physical security, personnel security, SCRM, business continuity, ICT architecture, business process engineering, operations security, and cyber security are integrated with mission assurance.
Cyber Risk Mitigation Approach	Cyber security builds on standards of good practice, but pushes the state of the practice by incorporating state of the art techniques, sometimes at the expense of non-compliance with standards of good practice.
Adaptability and Agility	The organization has defined and implemented a process that provides for alternate critical cyber decision making, allowing for delegation of responsibilities, in the event that the adversary's action results in a successful long term disruption of key aspects of the primary decision making process.
Senior Engagement	A dedicated corporate officer or agency official is actively engaged in enterprise-level cyber security decisions, and closely coordinates with near-term decision-makers. Some near-term decisions are reserved for the senior official (or designated alternate in cases of disruption).
Cyber Risk Analytics	The organization models different adversaries separately as feasible and appropriate to the organization. The organization frequently updates threat models based on observations, indicators, and information from external sources, explicitly considering the APT. The organization models business / mission business / mission threads and their dependencies on cyber resources, so that the consequences of compromise and response can be identified and managed. The organization defines and periodically assesses organization-related cyber risk factors (e.g., factors that characterize adversary capabilities, motivations, or activities; factors that indicate system resilience) to inform enterprise risk management.

Table 17. Assessing Conformance with Cyber Prep Level 4 Governance

Characteristic	Assertion	Assessment	Score[21]
Strategic Integration	The organization's architectural and acquisition strategies are coordinated with its cyber security strategy; its cyber security strategy is part of its mission assurance strategy, which is part of the organization's mission and enterprise risk management strategies. *(Identify the organization's strategic planning process, highlighting the role of cyber security.)*		
	The organization coordinates with cyber security counterparts in partner, supplier, and customer organizations, to support shared response to threats and so that the organization's cyber security strategy is not undermined by strategic weaknesses in those organizations. *(Identify coordinating bodies and/or individual organizations, points of contact, and any organizational policies or procedures for sharing security information or coordinating response.)*		
	The organization engages with (or, at a minimum, maintains awareness of the activities of) bodies working on better understanding of cyber threats, consequences, and risk mitigation approaches. *(Describe how the organization does this, e.g., via membership in consortia or councils, via attendance at conferences.)*		
Allied Disciplines	Physical security, personnel security, SCRM, business continuity, ICT architecture, business process engineering, operations security, and cyber security are integrated with mission assurance. *(Identify the organizational structure, roles, and responsibilities.)*		
Cyber Risk Mitigation Approach	Cyber security builds on standards of good practice, but pushes the state of the practice by incorporating state of the art techniques, sometimes at the expense of non-compliance with standards of good practice. *(Indicate which standards the organization seeks to comply with. Identify standards or guidelines for broader risk management. Describe how the organization decides when and how to use state-of-the-art techniques.)*		
Adaptability and Agility	The organization has defined and implemented a process that provides for alternate critical cyber decision making, allowing for delegation of responsibilities, in the event that the adversary's action results in a successful long term disruption of key aspects of the primary decision making process. *(Describe the process.)*		
Senior Engagement	A dedicated corporate officer or agency official is actively engaged in enterprise-level cyber security decisions, and closely coordinates with near-term decision-makers. *(Identify the cognizant officer or official. Describe the coordination mechanism.)*		
	Some near-term decisions are reserved for the senior official (or designated alternate in cases of disruption). *(Identify relevant policies and procedures.)*		
Cyber Risk Analytics	The organization models different adversaries separately as feasible and appropriate to the organization. *(Describe the modeling process.)*		
	The organization frequently updates threat models based on observations, indicators, and information from external sources, explicitly considering the APT. *(Describe the modeling process. Identify the sources of information the organization uses regularly.)*		
	The organization models business / mission business / mission threads and their dependencies on cyber resources, so that the consequences of compromise and response can be identified and managed. *(Describe the modeling process.)*		

[21] The score (if the organization uses quantitative scores) is the (weighted) average of scores for individual assertions.

Characteristic	Assertion	Assessment	Score[21]
	The organization defines and periodically assesses organization-related cyber risk factors (e.g., factors that characterize adversary capabilities, motivations, or activities; factors that indicate system resilience) to inform enterprise risk management. *(Describe the assessment process. Identify tools, practices, and sources of information.)*		
Overall Assessment	Extent to which the organization's cyber security governance enables it to maintain cyber preparedness at level 4 (if the organization uses scoring, (weighted) average of scores for the six characteristics).		

3.5 Cyber Prep Level 5

At Cyber Prep Level 5, the organization assumes that the adversary is taking continuous, overt actions against the organization from its persistent foothold within the information infrastructure, including a compromised supply chain, that will result in loss of some key systems and services; the organization assumes that data has been purposely been modified to mislead and confuse. The organization recognizes the need for agility and flexibility to ensure mission operations. The organization's strategy employs a highly agile, adaptive, and flexible structure that permeates all aspects of the organization (including planning, supply chains, collaboration, architecture, governance, and resources), allowing the organization to continually and dynamically reshape all aspects of its operations in face of changing, successful attacks.

Table 18. Characteristics of Cyber Security Governance at Cyber Prep Level 5

Characteristic	Cyber Security Governance
Strategic Integration	The organization's mission assurance strategy, fully integrating its cyber security strategy, is a significant part of the organization's mission and enterprise risk management strategies. The organization coordinates with counterparts in other organizations in the organization's mission or critical infrastructure sector, as well as in partner, supplier, and customer organizations, to support shared information-gathering about, analysis of, preparation for, and response to threats, and so that the organization's cyber security strategy is part of a mission-wide or sector-wide mission assurance strategy. The organization engages with (or, at a minimum, maintains awareness of the activities of) bodies working on better understanding the cyber security problem domain and related trade-offs.
Allied Disciplines	Physical security, personnel security, SCRM, business continuity, ICT architecture, business process engineering, operations security, and cyber security are integrated with mission assurance.
Cyber Risk Mitigation Approach	Cyber security builds on standards of good practice, but pushes the state of the art to ensure continued security evolution in the face of an innovative adversary.
Adaptability and Agility	The organization has defined, implemented and exercised a process that provides for alternate cyber decision making, allowing for timely decisions and delegation of responsibilities, in the event that the adversary's actions results in a successful long term destruction or severe disruption of the primary decision making process, or otherwise prevents it from acting in a timely manner.
Senior Engagement	The CEO or Agency head is actively engaged in mission assurance decisions. The senior official responsible for cyber security strategy closely coordinates with near-term decision-makers. Some near-term decisions are reserved for the CEO or agency head (or designated senior official(s) in cases of disruption).
Cyber Risk Analytics	The organization models different adversaries separately as feasible and appropriate to the organization and the missions it supports. The organization continually updates threat models based on observations, indicators, assessed information from external sources, and closely-held information from trusted sources. The organization models business / mission threads and their dependencies on cyber resources as they change during the course of operations, so that the consequences of compromise and response can be identified and managed dynamically. The organization defines and continuously assesses organization- and/or mission/business sector-related cyber risk factors to inform enterprise risk management.

Table 19. Assessing Conformance with Cyber Prep Level 5 Governance

Characteristic	Assertion	Assessment	Score[22]
Strategic Integration	The organization's mission assurance strategy, fully integrating its cyber security strategy, is a significant part of the organization's mission and enterprise risk management strategies. *(Identify the organization's mission assurance strategy, highlighting the role of cyber security.)*		
	The organization coordinates with counterparts in other organizations in the organization's mission or critical infrastructure sector, as well as in partner, supplier, and customer organizations, to support shared information-gathering about, analysis of, preparation for, and response to threats, and so that the organization's cyber security strategy is part of a mission-wide or sector-wide mission assurance strategy. *(Identify coordinating bodies – e.g., ISACs – and/or organizations, points of contact, and any organizational policies or procedures for sharing security information or coordinating response.)*		
	The organization engages with (or, at a minimum, maintains awareness of the activities of) bodies working on better understanding the cyber security problem domain and related trade-offs. *(Describe how the organization does this, e.g., via membership in consortia or councils, via attendance at conferences.)*		
	Score = average of assessed values for individual assertions.		
Allied Disciplines	Physical security, personnel security, SCRM, business continuity, ICT architecture, business process engineering, operations security, and cyber security are integrated with mission assurance. *(Identify the organizational structure, roles, and responsibilities.)*		
Cyber Risk Mitigation Approach	Cyber security builds on standards of good practice, but pushes the state of the art to ensure continued security evolution in the face of an innovative adversary. *(Indicate which standards the organization seeks to comply with. Identify standards or guidelines for broader risk management. Describe how the organization decides when and how to use state-of-the-art techniques.)*		
Adaptability and Agility	The organization has defined, implemented and exercised a process that provides for alternate cyber decision making, allowing for timely decisions and delegation of responsibilities, in the event that the adversary's actions results in a successful long term destruction or severe disruption of the primary decision making process, or otherwise prevents it from acting in a timely manner. *(Describe the process. Identify when and how it is exercised.)*		
Senior Engagement	The CEO or Agency head is actively engaged in mission assurance decisions.		
	The senior official responsible for cyber security strategy closely coordinates with near-term decision-makers. *(Identify the cognizant officer or official. Describe the coordination mechanism.)*		
	Some near-term decisions are reserved for the CEO or agency head (or designated senior official(s) in cases of disruption). *(Describe which decisions may – or may not – be delegated.)*		
	Score = average of assessed values for individual assertions.		
Cyber Risk Analytics	The organization models different adversaries separately as feasible and appropriate to the organization and the missions it supports. *(Describe the modeling process.)*		

[22] The score (if the organization uses quantitative scores) is the (weighted) average of scores for individual assertions.

Characteristic	Assertion	Assessment	Score[22]
	The organization continually updates threat models based on observations, indicators, assessed information from external sources, and closely-held information from trusted sources. *Describe the modeling process. Identify the sources of information the organization uses regularly.)*		
	The organization models business / mission threads and their dependencies on cyber resources as they change during the course of operations, so that the consequences of compromise and response can be identified and managed dynamically. *(Describe the modeling process.)*		
	The organization defines and continuously assesses organization- and/or mission/business sector-related cyber risk factors to inform enterprise risk management. *(Describe the assessment process. Identify tools, practices, and sources of information.)*		
	Score = average of assessed values for individual assertions.		
Overall Assessment	Extent to which the organization's cyber security governance enables it to maintain cyber preparedness at level 5 (if the organization uses scoring, (weighted) average of scores for the six characteristics).		

4 Conclusion

Cyber security governance is the component of enterprise governance that treats organizational dependence on cyberspace in the presence of adversaries as a domain of enterprise risk management. Cyber security governance is increasingly recognized as an important area for sharing research and lessons-learned [18]. Cyber Prep provides a framework for assessing, and identifying gaps or possible areas of evolution in, an organization's cyber security governance structures and practices. Achieving cyber security governance consistent with its target Cyber Prep level enables an organization to make consistent and understandable decisions about

- Investing in security measures;
- Aligning cyber security risk management with other aspects of enterprise risk management; and
- Managing the organization's cyber security posture.

Appendix A References

[1] D. J. Bodeau, R. D. Graubart, and J. Fabius-Greene, "Improving Cyber Security and Mission Assurance via Cyber Preparedness (Cyber Prep) Levels," Proceedings of the 2010 IEEE International Conference on Social Computing / IEEE International Conference on Privacy, Security, Risk and Trust, pp. 1147-1152 or *Improving Cyber Security and Mission Assurance via Cyber Preparedness (Cyber Prep) Levels*, The MITRE Corporation, 2009, PR 09-4656, http://www.mitre.org/work/tech_papers/2010/09_4656/09_4656.pdf

[2] D. J. Bodeau, R. D. Graubart, and J. Fabius-Greene, "How Do You Assess Your Organization's Cyber Prep Level?", The MITRE Corporation, 2010, PR 10-2914

[3] D. J. Bodeau, S. Boyle, R. D. Graubart, and J. Fabius-Greene, "Addressing Traditional and Advanced Persistent Cyber Threats – the Cyber Prep Approach to Selecting Security Measures," The MITRE Corporation, 2010, PR 10-3539

[4] D. J. Bodeau, S. Boyle, R. D. Graubart, and J. Fabius-Greene, Using Cyber Prep: The Concept of Operations for MITRE's Cyber Preparedness Methodology, MTR100313, The MITRE Corporation, 2010 (submitted for public release)

[5] IT Governance Institute (ITGI), Board Briefing on IT Governance, 2nd Edition, USA, 2003, www.itgi.org

[6] National Defense Industrial Association (NDIA), Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure, 2009, http://www.ndia.org/Advocacy/PolicyPublicationsResources/Documents/Cyberspace_policy_review_2009.pdf

[7] Department of Defense, National Military Strategy for Cyberspace Operations, 2006, http://www.dod.gov/pubs/foi/ojcs/07-F-2105doc1.pdf

[8] International Telecommunications Union (ITU) Study Group 17, Overview of Cybersecurity, Draft ITU-T Rec. X.1205, 2008

[9] ITGI and ISACA, Information Security Governance: Guidance for Boards of Directors and Executive Management, 2nd Edition, 2006, http://www.isaca.org/ContentManagement/ContentDisplay.cfm?ContentID=34997

[10] National Institute of Standards and Technology (NIST), FIPS 199, http://csrc.nist.gov/publications/fips/fips199/FIPS-PUB-199-final.pdf

[11] CMMI (Capability Maturity Model Integration) Architecture Team, Introduction to the Architecture of the CMMI® Framework, Software Engineering Institute (SEI), Carnegie-Mellon University (CMU), Technical Note CMU/SEI-2007-TN-009, July 2007, http://www.sei.cmu.edu/reports/07tn009.pdf

[12] CMMI Product Team, Capability Maturity Model® Integration (CMMI), Version 1.1: CMMI for Systems Engineering, Software Engineering, and Integrated Product and Process Development – Staged Representation, CMU/SEI-2002-TR-004 and ESC-TR-2002-004, December 2001, http://www.sei.cmu.edu/reports/02tr004.pdf

[13] NIST, Information Security Handbook: A Guide for Managers, NIST SP 800-100, October 2006, http://csrc.nist.gov/publications/nistpubs/800-100/SP800-100-Mar07-2007.pdf

[14] NIST, Information Security Guide for Government Executives, NISTIR 7359, January 2007, http://csrc.nist.gov/publications/nistir/ir7359/NISTIR-7359.pdf

[15] ITGI, COBIT (Control Objectives for IT and Related Technology), V4.1, 2007

[16] SEI / CMU, Governing for Enterprise Security (GES) Implementation Guide, August 2007, CMU/SEI-2007-TN-020, http://www.cert.org/archive/pdf/07tn020.pdf

[17] Joint Task Force Transformation Initiative, Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach, NIST SP 800-37 Revision 1, February 2010, http://csrc.nist.gov/publications/nistpubs/800-37-rev1/sp800-37-rev1-final.pdf

[18] Proceedings of the 1st ACM Workshop on Information Security Governance, 13 November 2009

[19] Gary McGraw, Brian Chess, and Sammy Migues, BSIMM2 (Building Security In Maturity Model), May 2010, http://bsimm2.com/download/

[20] ISM3 Consortium, Information Security Management Maturity Model, V. 2.10, http://www.ism3.com/

[21] IT Policy Compliance Group, "IT Governance, Risk, and Compliance: Improving business results and mitigating financial risk," 2008

[22] NIST, Program Review for Information Security Management Assistance (PRISMA), NISTIR 7358, January 2007, http://csrc.nist.gov/publications/nistir/ir7358/NISTIR-7358.pdf

[23] Gustavo Alberto de Oliveira Alves, Luiz Fernando Rust da Costa Carmo and Ana Cristina Ribeiro Dutra de Almeida, "Enterprise Security Governance: A practical guide to implement and control Information Security Governance (ISG)," The First IEEE/IFIP International Workshop on Business-Driven IT Management, 2006. BDIM '06, pp. 71 - 80

[24] International Risk Governance Council (IRGC), "Risk Governance Deficits: An Analysis and Illustration of the Most Common Deficits in Risk Governance," 2009, http://www.irgc.org/IMG/pdf/IRGC_rgd_web_final.pdf

[25] IRGC, "Risk Governance: Toward an Integrative Approach," IRGC White Paper No. 1, September 2005, http://www.irgc.org/IMG/pdf/IRGC_WP_No_1_Risk_Governance__reprinted_version_.pdf

[26] GAO, Cyberspace: United States Faces Challenges in Addressing Global Cybersecurity and Governance, GAO-10-606, July 2010, http://www.gao.gov/new.items/d10606.pdf

[27] Piet Selke and Ortwin Renn, "Risk Governance of Pervasive Computing Technologies," The International Journal of Technology, Knowledge, and Society, Volume 4, Number 1, 2008

[28] IRGC, "An Introduction to the IRGC Risk Governance Framework," 2008, http://www.irgc.org/IMG/pdf/An_introduction_to_the_IRGC_Risk_Governance_Framework.pdf

[29] Lynn Mueller, Matthew Magee, Petr Marounek, and Andrew Phillipson, IBM IT Governance Approach: Business Performance through IT Execution, IBM Redbooks, February 2008, http://www.redbooks.ibm.com/redbooks/pdfs/sg247517.pdf

[30] Theresa A. Pardo, Donna S. Canestraro, Jana Hrdinová, Anthony M. Cresswell, and Anna Raup-Kounovsky, Creating Enhanced Enterprise Information Technology Governance for New York State: A Set of Recommendations for Value-Generating Change, Center for Technology in Government (CTG), State University of New York at Albany, August 2009, http://www.ctg.albany.edu/publications/reports/itgov_recommendations/itgov_recommendations.pdf

[31] Alan Calder, *IT Governance: Implementing Frameworks and Standards for the Corporate Governance of IT*, ISBN:9781905356904

[32] International Standards Organization (ISO), Corporate governance of information technology, ISO/IEC 38500:2008, 2008

[33] Mehdi Fasanghari, Fateme NasserEslami, and Mohammad Naghavi, "IT Governance Standard Selection Based on Two Phase Clustering Method," Fourth International Conference on Networked Computing and Advanced Information Management, DOI 10.1109/NCM.2008.251, IEEE, 2008

[34] Wolcott Group, Raising the Standard of Information Security Governance with ISO 27001, March 2007, http://www.wolcottgroup.com/documents/WG_ISO27001PoV_0607C2.pdf

[35] Tammy Clark and Toby Sitko, "Information Security Governance: Advancing the State of the Practice," Research Bulletin Issue 17, EDUCAUSE Center for Applied Research, 2008, http://net.educause.edu/ir/library/pdf/ERB0817.pdf

[36] The 2009 State of Cybersecurity from the Federal CISO's Perspective — An (ISC)$^{2®}$ Report, April 2009, http://media.haymarketmedia.com/Documents/7/FederalCISOSurveyReport_1638.pdf

[37] Business Software Alliance (BSA), Information Security Governance: Toward a Framework for Action, October 2003, http://www.bsa.org/country/Research%20and%20Statistics/~/media/BD05BC8FF0F04CBD9D76460B4BED0E67.ashx

[38] Corporate Governance Task Force, Information Security Governance – A Call to Action, 2004, http://www.cyber.st.dhs.gov/docs/Information%20Security%20Governance-%20A%20Call%20to%20Action%20(2004).pdf

[39] A. Da Veiga and J. J. P. Eloff, "An Information Security Governance Framework", Information Systems Management, 24: 4, 361 - 372, DOI: 10.1080/10580530701586136

[40] Shaun Posthumus and Rossouw von Solms, "A framework for the governance of information security", Computers & Security (2004) 23, pp. 638-646

[41] Janne J. Korhonen, Mehmet Yildiz, Juha Mykkänen, "Governance of Information Security Elements in Service-Oriented Enterprise Architecture," ispan Proceedings, pp.768-773, 2009 10th International Symposium on Pervasive Systems, Algorithms, and Networks, 2009

[42] Booz Allen Hamilton, Information Security Governance: Governance Considerations for the Cloud Computing Environment, 2009, http://www.boozallen.com/media/file/Information-Security-Governance.pdf

[43] Liberty Alliance Project, An Overview of the Id [Identity] Governance Framework, Version 1.0, October 2007, http://projectliberty.org/liberty/content/download/3500/23156/file/overview-id-governance-framework-v1.0.pdf

[44] Kenneth C. Brancik, The Computer Forensics and Cybersecurity Governance Model, 2003, Information Systems Audit and Control Association (ISACA), http://www.isaca.org/Template.cfm?Section=Home&Template=/ContentManagement/ContentDisplay.cfm&ContentID=15904

[45] NIST, DRAFT Managing Risk from Information Systems: An Organizational Perspective, DRAFT NIST SP 800-39, April 2008, http://csrc.nist.gov/publications/drafts/800-39/SP800-39-spd-sz.pdf

[46] NIST, Computer Security Incident Handling Guide, Revision 1, NIST SP 800-61 Rev. 1, March 2008, http://csrc.nist.gov/publications/nistpubs/800-61-rev1/SP800-61rev1.pdf

[47] Moira J. West-Brown, Don Stikvoort, Klaus-Peter Kossakowski, Georgia Killcrece, Robin Ruefle, and Mark Zajicek, Handbook for Computer Security Incident Response Teams, 2nd Edition, CMU/SEI-2003-HB-002, April 2003, http://www.cert.org/archive/pdf/csirt-handbook.pdf

[48] Department of Defense, Information Assurance (IA) and Computer Network Defense (CND), Chairman of the Joint Chiefs of Staff Instruction (CJCSI) 6510.01E, 15 August 2007, http://www.dtic.mil/cjcs_directives/cdata/unlimit/6510_01.pdf

[49] V. Sambamurthy and R. W. Zmud, –Arrangements for information technology governance: A theory of multiple contingencies.” MIS Quarterly, 23 (1999): 261-290

[50] Peter Weill and Jeanne Ross, ––A Matrixed Approach to Designing IT Governance,” MIT Sloan Management Review, Winter 2005

Appendix B Cyber Security Governance and Other Models

B.1 Maturity Models

Capability maturity models apply to organizational processes, and were initially defined for software development processes. Since the original CMM, the modeling construct has been extended to aspects of security, as well as a variety of other areas in which an organization might seek to improve its capability to execute a process. Unless otherwise stated, capability maturity models define five levels (or six, if a –level 0 – nothing is done” is included). These levels can be briefly characterized as follows:

1. Initial (chaotic, ad hoc, individual heroics). No process has been officially established, but some practices have been established over time.
2. Managed. The organization has established practices, and uses these to manage the process.
3. Defined. The organization has formally defined its process, and has decomposed it into manageable sub-processes.
4. Quantitatively managed. The organization has defined key performance parameters (KPPs) for its processes and sub-processes, and uses KPPs to support management decisions.
5. Optimized. The organization is committed to process improvement, seeking to optimize the process or sub-processes.

In addition, capability maturity models define key areas for processes and practices. The maturity of an organization’s processes and practices can be assessed in each area.

B.1.1 SSE-CMM

The System Security Engineering Capability Maturity Model (SSE-CMM, http://www.sse-cmm.org/index.html) addresses security engineering for a system or a set of related systems, and hence is primarily relevant to Tier 3 in the NIST risk management hierarchy.

B.1.2 BSI-MM

The three-level Building Security In Maturity Model (BSI-MM, [19]) is intended to facilitate planning of software security initiatives. It defines practices in twelve areas, in four security domains: governance, intelligence, software security development life-cycle, and deployment.

As with the SSE-CMM, this model is primarily relevant to the lowest tier in the risk management hierarchy. The governance domain in particular is specific to software development.

However, the intelligence domain includes understanding, analyzing, and preparing for adversary TTPs. This part of the BSI-MM is consistent with the cyber risk analytics aspect of governance in Cyber Prep; an organization that achieved BSI-MM level 3 would demonstrate Cyber Prep Level 3 cyber risk analytics.

B.1.3 ISM3 and SOMA

The Information System Security Management Maturity Model (ISM3, [20], http://www.ism3.com/) defines processes for strategic, tactical, and operational management of information security. With regard to governance, ISM3

- Defines a variety of security-related roles and responsibilities.
- Proposes an organizational structure with an Executive Security Committee (similar to the Risk Executive Function) consisting of the CEO and CIO, as well as a Security Committee (to oversee coordination between the disciplines of information security, physical security, and workplace security) and an Information Security Committee.
- Specifies the need for separation of duties for specific roles at different maturity levels.

While Cyber Prep does not specify an organizational structure or detailed practices, ISM3 is consistent with Cyber Prep. That is, an organization implementing ISM3 at level 3 or above would achieve Cyber Prep Level 3 governance. Because ISM3 does not address mission assurance, an organization at ISM3 level 5 would need to enhance its governance to achieve Cyber Prep Level 4 or 5 governance.

The Institute for Security and Open Methodologies (ISECOM) Security Operations Maturity Architecture (SOMA, http://www.isecom.org/research/soma.shtml) is work-in-progress, and is intended to supersede ISM3.

B.1.4 GRC MM

The Governance, Risk and Compliance Maturity Model (GRC MM) [21] focuses on managing IT security risks as a component of managing financial risks, and on achieving compliance with laws and regulations. An organization implementing GRC MM at level 3 or above would achieve Cyber Prep level 3 governance. Because GRC MM does not address mission assurance, an organization at GRC MM level 5 would need to enhance its governance – particularly with respect to cyber risk analytics – in to achieve Cyber Prep level 4 or 5 governance.

B.1.5 PRISMA

NIST's Program Review for Information Security Management Assistance (PRISMA, [22]) methodology defines five levels of IT Security Program maturity:

- Maturity Level 1: Policies
- Maturity Level 2: Procedures,
- Maturity Level 3: Implementation,
- Maturity Level 4: Testing, and
- Maturity Level 5: Integration

An organization implementing PRISMA at level 3 or above would achieve Cyber Prep Level 3 governance. Because PRISMA does not address mission assurance, an organization at PRISMA level 5 would need to enhance its governance – particularly with respect to cyber risk analytics – in to achieve Cyber Prep Level 4 or 5 governance.

B.1.6 Other

Maturity levels are factored into some governance models and frameworks, notably ITGI [9, 15] and the framework for enterprise security governance proposed by de Oliveiras Alves et al. [23].

B.2 Governance Models and Frameworks

B.2.1 Risk Governance Framework

The International Risk Governance Council (IRGC) defines risk governance as "the identification, assessment, management and communication of risks in a broad context. It includes the totality of actors, rules, conventions, processes and mechanisms concerned with how relevant risk information is collected, analysed and communicated, and how and by whom management decisions are taken and implemented." [24] IRGC focuses on systemic risks, i.e., "those risks that affect the systems on which society depends – health, transport, telecommunications, etc." [25] The types of risks, and thus the forms of risk governance, addressed by the IRGC require efforts that span organizational boundaries. As a recent report by the Government Accountability Office (GAO) points out [26], global efforts are needed to improve cyber security. However, consideration of such needs is beyond the scope of Cyber Prep.

IRGC has defined a conceptual approach to using risk characteristics to determine the most effective risk management strategy, appropriate instruments for implementing the strategy, and stakeholder participation [25]. This conceptual approach has been adapted for pervasive computing [27]. As indicated in Table 14, this approach can be adapted to risk governance for risks due to the advanced persistent threat. IRGC has also defined a process framework (referred to as the IRGC Risk Governance Framework) [28]. The process framework in the Cyber Prep Concept of Operations is consistent with the IRGC framework.

Table 20. Cyber Security Governance in the IRGC Approach

Risk Characteristics[23]	Recommended Approach[24]	Cyber Security Governance Considerations
Simple: Risks are well understood and manageable.	Routine-based risk management approach. Define an acceptable level of risk; identify key indicators of level of risk; use automated tools to monitor those indicators.	Relevant to well-understood information security risks, e.g., those that can be addressed by following standards of good practice and conventional information security governance. For Cyber Prep Levels 1 and 2, this approach may suffice to address current risks, but does not provide a foundation for future evolution.
Complex: Risks are induced by system complexity and/or interdependence, and thus are difficult to analyze.	Risk-informed analysis of systems and causal chains, and/or robustness-focused engineering, to produce a risk-absorbing system.	Relevant to systems security engineering and operations, particularly for systems that rely on a layered architecture, a service-oriented architecture (SOA), or are part of a system-of-systems. An organization's cyber security governance needs to include ways to engage owners and operators of systems, services, and infrastructures beyond the organization, to ensure that dependencies do not impose unknown or intolerable risks on the organization.
Uncertainty-induced: High uncertainty about potential damage and likelihood requires collective reflection on the problem, to avoid both under- and over-protection.	Precaution-based analysis and/or reliance-focused engineering, to improve the capability of stakeholders to cope with surprises.	Characteristic of many risks due to the advanced threat. The ongoing collective discourse on cybersecurity in different domains (e.g., defense [7], critical infrastructure protection) can be expected, in time, to provide the cognitive and evaluative approaches needed to decrease uncertainty. An organization's cyber security governance needs to include ways to engage with (or, at a minimum, be aware of the activities of) bodies working on better understanding of cyber threats, consequences, and risk mitigation approaches.
Ambiguity-induced: Major ambiguities are associated with the risk problem.	Discourse-based, to define conceptual frameworks for understanding the problem.	Characteristic of some risks due to the advanced threat. The ongoing collective discourse on cybersecurity, its relationship to other risk domains (e.g., privacy) at the national [6] and international [26] levels, and the relative responsibilities of government, industry, and members of the public can be expected, in time, to provide the cognitive, evaluative, and normative approaches needed to resolve ambiguities so that areas of uncertainty can be identified. An organization's cyber security governance needs to include ways to engage with (or, at a minimum, be aware of the activities of) bodies working on better understanding the problem domain and related trade-offs.

[23] Derived from Figure 4 (The Risk Management Escalator and Stakeholder Involvement (from simple via complex and uncertain to ambiguous phenomena)) in [25].
[24] Derived from Sellke and Renn [27].

B.2.2 Information Security Governance

Since failure of large IT projects has been recognized as a source of organizational risk, considerable effort has been expended to define and implement IT governance, starting by differentiating it from IT management:

> "A governance process, as described earlier, is used to define the chains of responsibility, authority, and communication to empower people, as well as to define the measurement and control mechanisms to enable people to carry out their roles and responsibilities. … A management process is the output from the governance process. Unlike a governance process, a management process implements the specific chain of responsibility, authority, and communication that empowers people to do their day-to-day jobs. The management process also implements appropriate measurement and control mechanisms that enable practitioners the freedom to carry out their roles and responsibilities without undo interruption by the executive team." [29]

The body of IT governance models, approaches, standards, and experiences is large and growing.[25] This characterization needs to be tailored to the information security domain. NIST SP 800-100 states that

> "Information security governance can be defined as the process of establishing and maintaining a framework and supporting management structure and processes to provide assurance that information security strategies are aligned with and support business objectives, are consistent with applicable laws and regulations through adherence to policies and internal controls, and provide assignment of responsibility, all in an effort to manage risk." [13]

IT governance has been identified as the foundation for information security governance, relying on information security standards.[26] An announcement by the International Standards Organization (ISO)[27] describes a new project within ISO/IEC JTC1/SC27 to develop an information security governance standard, based on the ISO IT governance standard. Federal CISOs have identified information security governance as one of their top priorities [35].

The general process for implementing (or evolving) IT governance described by Calder [31] is relevant to information security and cyber security governance:

- Confirm the pre-requisite conditions: senior leadership commitment to defining, implementing, and maintaining an IT governance framework.
- Performing a gap analysis and developing a plan to close gaps in IT governance practices.
- Integrating the IT strategy into the business strategy, by clarifying the business strategy and what it specifically requires of IT, and developing a plan to meet those requirements.

B.2.2.1 Information Security Governance Models and Frameworks

Several frameworks for information security governance have been defined. The Corporate Governance Task Force, building on prior work by the Business Software Alliance (BSA, [37]), defined a preliminary framework, consisting of actors, governance / business drivers, roles and

[25] For IT governance models or approaches, see [5, 9, 16, 30, 31, 32]. For IT governance standards, see [15, 32, 34].
[26] See [35, 36] for a discussion of how ISO 17999 and ISO 27001can be viewed as the foundation for information security governance.
[27] See http://www.iso27001security.com/html/27014.html.

responsibilities, and metrics / audit [38]. In addition to defining maturity levels, the ITGI guide [9] amplifies this framework, defining responsibilities for the Board of Directors / Trustees (assuming a corporate organizational model), senior executives, a steering committee (which essentially is responsible for enterprise risk management), and the Chief Information Security Officer (CISO).

Veiga and Eloff [39] propose a four-level framework, the strategic component of which is governance in the accepted sense of the term; their managerial / operational and technical components fit better into the security measures component of Cyber Prep. Posthumus and Von Solms [40] present a notional framework, highlighting the flows of direction and information between governance and management. De Oliveira Alves et al. [23] propose a framework which seeks to align COBIT [15], ISO 17799, and Balanced Scorecard.

Specialized information security governance frameworks have been defined in the service-oriented architecture (SOA) [41], cloud computing [42], identity management [43], and computer forensics [44] domains.

B.2.2.2 Information Security Governance and GRC

GRC refers to an approach to enterprise risk management in which organizational structures and processes for governance, risk management, and compliance are integrated. GRC can encompass all classes of enterprise risks, or can be focused on one particular risk area, e.g., financial risks, IT risks. IT governance frameworks, when described in terms of GRC [5, 9, 16, 21], treat information security governance as integral to GRC.

GRC approaches historically derive from the need to establish compliance with laws and regulations that include requirements for risk management and governance (in particular, the Sarbanes-Oxley Act or SOX). GRC has been extended, e.g., to include the role of governance in building business value[28], but the orientation toward a monitoring- or auditing-oriented approach toward governance remains evident. This orientation is consistent with Cyber Prep Levels 1 and 2, but does not accommodate the consideration of prospective adversary TTPs needed for the higher Cyber Prep levels. Cyber Prep differs from compliance-oriented approaches to risk management and strategic planning in its emphasis on (1) the changing and adaptive nature of the APT, and (2) the need for different organizations to tailor their security measures and governance to the different adversaries they face.

B.2.2.3 Key Principles of Information Security Governance

From the growing body of information security governance models, frameworks, and guidance, several key principles can be identified. Cyber Prep expects that an organization apply these principles. However, Cyber Prep does not assume any specific framework or governance model. In particular, Cyber Prep does not specify how to organize the more detailed practices or components of information security governance identified by different models, frameworks, and/or guidance. The key principles of sound information security governance that Cyber Prep expects are:

- Obtain senior leadership commitment to information security [16];
- Ensure that information security governance addresses

[28] See the IT Governance Domain Practices and Competencies Series from the IT Governance Institute at http://www.isaca.org/Template.cfm?Section=Preparation2&Template=/ContentManagement/ContentDisplay.cfm&ContentID=44205. ISACA now offers a Certificate in the Governance of Enterprise IT.

- Strategy and planning [16, 35, 38, 39];
- Risk management [9, 16];
- Policy and compliance [9, 21, 35];
- Integration with the system development life-cycle (SDLC) [16, 21, 35]; and
- Incident handling [45, 46, 47][29];

- Provide clear lines of communication (particularly, for direction, education, reporting, monitoring, and feedback) between the strategic, mission / business, and operational / system / program levels [37, 41].

B.2.2.4 Information Security Governance Organizational Approaches

In the area of IT governance, three major organizational approaches have been defined: centralized, decentralized, and federated [49]. These approaches can be amplified and tailored to the information security governance domain as follows:

The following is an attempt to characterize alternative approaches to information security governance:[30]

- In *centralized* information security governance, authority and decision making power are vested solely within a central body, which establishes processes for ensuring organization-wide involvement in decisions and implementation as well as creating formal communications mechanisms. A centralized approach to information security governance assumes strong, well-informed central leadership, and provides consistency throughout the organization.
- In *decentralized* information security governance, authority and decision-making power are reserved to individual sub-organizations (mission or business units), which establish their own processes for ensuring sub-organization-wide involvement in decisions and implementation as well as creating formal communications mechanisms. A decentralized approach to information security governance accommodates sub-organizations with divergent mission / business models, needs, and operating environments (e.g., as might result from mergers with or acquisition of different organizations), at the cost of consistency throughout the organization as a whole.
- In *hybrid* information security governance structure, authority over decision-making is distributed between a central body and individual sub-organizations. The central body establishes processes for ensuring organization-wide involvement in decisions that affect the entire organization (e.g., those related to shared infrastructure) and implementation as well as creating corresponding formal communications mechanisms; individual sub-organizations do the same for information security decisions that are specific to their information resources, mission / business needs and models, and operating environments. A hybrid approach to information security governance assumes strong, well-informed leadership both for the organization as a whole and for the sub-organizations, and provides consistency throughout the organization for those aspects of information security that affect the entire organization.

Cyber Prep expects that an organization has information security governance consistent with the NIST characterization, and focuses on the aspect of risk management that relates to the APT.

[29] Multiple models have been defined for incident handling. An organization's selection of a model depends in large part on its size and structure. For example, the Department of Defense has defined a three-tiered model [48].
[30] These characterizations are adapted from Weill and Ross [50].

Cyber Prep does not assume a specific information security governance framework. However, Cyber Prep does assume that the organization as a whole must achieve a minimum level of cyber preparedness, even when some sub-organizations need to achieve a higher level. Thus, Cyber Prep assumes either a centralized or a hybrid approach to information security and cyber security governance.

Appendix C Acronyms

APT	advanced persistent threat
BSI-MM	Building Security In Maturity Model
CEO	Chief Executive Officer
CERT	Computer Emergency Response Team
CIMA	Chartered Institute of Management Accountants
CIO	Chief Information Officer
CISO	Chief Information Security Officer
CMMI	Capability Maturity Model Integration
CMU	Carnegie Mellon University
COBIT	Control Objectives for IT and Related Technology
COSO	Committee of Sponsoring Organizations of the Treadway Commission
CTG	Center for Technology in Government
CTO	Chief Technology Officer
DCISE	DoD-Defense Industrial Base Collaborative Sharing Environment
DIB	Defense Industrial Base
DoD	Department of Defense
EMSEC	emanations security
ERM	enterprise risk management
GES	Governing for Enterprise Security
GRC	Governance, Risk and Compliance
GRC MM	GRC Maturity Model
ICT	information and communications technology
IFAC	International Federation of Accountants
IRGC	International Risk Governance Council
ISAC	Information Sharing and Analysis Center
ISACA	Information Systems Audit and Control Association
ISECOM	Institute for Security and Open Methodologies
ISM3	Information Security Management Maturity Model
ISO	International Standards Organization
IT	information technology
ITGI	IT Governance Institute
ITU	International Telecommunications Union

KPP	key performance parameter
NDIA	National Defense Industrial Association
NIST	National Institute of Standards and Technology
PRISMA	Program Review for Information Security Management Assistance
REF	Risk Executive Function
RMF	Risk Management Framework
SCRM	supply chain risk management
SEI/CMU	Software Engineering Institute at Carnegie Mellon University
SOA	service-oriented architecture
SOMA	Security Operations Maturity Architecture
SOX	Sarbanes-Oxley Act
SP	Special Publication
SSE-CMM	System Security Engineering Capability Maturity Model
TTPs	tactics, techniques, and procedures