APPLICATION OF THE NIST STANDARDS OF RISK MANAGEMENT

A Framework for Applied Enterprise Risk Management

by Joshua Burnett, VTS Founder and CTO

If you cannot say that you do it, write down how you do it, and prove that you do it that way… Then you don't do it.

Before we get started, I'd like you to take a few minutes to jot down some personal notes. Getting a baseline of the "who, why, and where" of your particular approach to the NIST Risk Management Framework (RMF) will help you identify areas of this course that are most important to your function.

First, I want you to identify what organization you work for. Think about what this might mean for the information types and system type that you may come into contact with, or even be responsible for protecting. Next, and the first question should assist you with your response to this question, why is the NIST Risk Management Framework important to you? Is it a mandatory course or action, or are you here because you believe in the power of pro-active, technical, and operational security across your organization? Maybe both? Now, what level of professional experience with information and network security do YOU possess?

Lastly, identify the goals you and your organization have for understanding the NIST standards. Do you plan on simply achieving a level set understanding of the NIST RMF and its processes, procedures, and policies? Do you plan on leveraging the information as the foundational baseline for your (ISC)² Cap exam, to achieve the Certified Authorization Professional certification? Is the intent for you to be relevant and ready in your organization's RMF implementation that is being mandated by legislation or executive order? Whatever the reason… you truly are in the right place, at the right time.

Why "everyone" should be aware and informed.

While some of the facets of the NIST based cybersecurity frameworks of RMF and CSF may be more geared towards specific roles, it is never a bad idea for engineers and administrators to understand enterprise level risk decisions. It is equally important for executives in management and oversight roles to understand the importance of, and sometimes "headache" of, the task performed by those who are more "hands on" with systems and data.

In addition to preparing organizations for the proper, industry standard, compliant security of their information systems, the NIST Risk Management Framework serves as the foundation for the International Information Systems Security Certification Consortium (ISC)² Certified Authorization Professional (CAP) exam.

It is important to remember that, while United States legislation and Federal Agencies were the driving force behind much of this process and framework development, the NIST standards of the Risk Management Framework are referenced by most every applicable controls-based cybersecurity and information security framework around the globe. Through the implementation of legislation, these now apply to ALL Federal agencies across the government of both the United States and Canada and have associated timelines that are federally mandated. Additionally, there is not only a wide acceptance of these standards across multiple critical infrastructure industries, but these frameworks are also becoming the de-facto standard across other non-regulated, private sector industries as well. The process, policies, and procedures should mirror each other as closely as possible. This is the only way to maintain the intended **RECIPROCITY** (a key term within the NIST 800 Series guidelines) within the framework from one agency, system, or organization to another.

It is essential that we begin with a common understanding of the environment that influences RMF. To meet this goal, we must address a broad introduction to the most relevant legislation, policy, and regulations driving security and the development and implementation of RMF. It is also extremely important to establish a common vocabulary and lexicon for discussing security, specifically in the context of RMF.

14900 Conference Center Dr,
Suite 200
Chantilly, Virginia 20151

info@vtscyber.com
703.498.2150 703.498.2149

NIST PUBLISHED STANDARDS AND GUIDELINES

Federal Information Security Management Act - Title III of E-Government Act of 2002 (Public Law 107-347)

FISMA gave OMB the legal and legislative oversight of E-Government.

Federal Government (Organizations and IG's) must report IA status to OMB annually and quarterly.

OMB provides reports to Congress annually - Congressional Cyber Security Grade.

Follow on legislation would lead to OMB taking on "acquisition and budgeting" enforcement over FISMA with legal reporting and enforcement being passed to the Department of Homeland Security (DHS).

NSA SERVES AS TECHNICAL ADVISOR

Initially, all Federal Government agencies were mandated to follow NIST A&A processes, with the exception of Defense and Intelligence organizations. Defense and Intelligence agencies have since followed suit implementing "customized" versions of the NIST framework. The DoD and Intelligence Agencies across the Federal space are now working with CNSSI 1253 and ICD 503 – Agency level policy documents designed to modify, standardize, and enforce the framework implementation across enterprises supporting National Security capabilities.

The RMF process, while cyclical, is also linear, and tasks can and will be performed in parallel. For example, a system can be operating at full capacity within Step 6 – Continuous Monitoring, while simultaneously, controls being monitored will be readdressed and the system will be going through Steps 2, 3, and 4 for continuous system security improvements.

Assurance: Grounds for confidence that an information-technology (IT) product or system meets its security objectives.

Assurance is one of the most critical concepts to grasp. Assurance is based on trust; however, trust cannot always be quantified precisely. System specification, design, and implementation can provide a basis for determining "how much" to trust a system. This aspect of trust is called assurance. It is an attempt to provide a basis for specifying how much one can trust a system. Assurance in the computer world refers not only to security, but also to the operational quality of that system. Specific steps ensure that the computer will function properly, as well as securely. The sequence of steps includes detailed specifications of the desired (or undesirable) behavior; an analysis of the design of the hardware, software, and other components to show that the system will not violate the specifications; and arguments or proofs that the implementation, operating procedures, and maintenance procedures will produce the desired behavior.

Assurance

NIST 800-53 defines assurance in this way: Assurance is the grounds for confidence that the security controls implemented within an information system are effective in their application. Assurance can be obtained in a variety of ways including: (i) actions taken by developers and implementers of security controls in the design, development, and implementation techniques and methods; and (ii) actions taken by security control assessors during the testing and evaluation process to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system.

14900 Conference Center Dr,
Suite 200
Chantilly, Virginia 20151

info@vtscyber.com
703.498.2150 703.498.2149

Cybersecurity means prevention of damage to, protection of, and restoration of computers, electronic communications systems, electronic communication services, wire communications, and electronic communications, including information contained therein, to ensure its availability, integrity, authentication, confidentiality, and non-repudiation.

Security is defined as:
1. A condition that results from the establishment and maintenance of protective measures that ensure a state of inviolability from hostile acts or influences.
2. With respect to classified matter, the condition that prevents unauthorized persons from having access to official information that is safeguarded in the interests of national security.
3. Measures taken by a military unit, an activity or installation to protect itself against all acts designed to, or which may, impair its effectiveness. (Joint Pub 1-02)

In the context of cybersecurity, security is obtained through the characteristics of **confidentiality, availability, and integrity**.

Confidentiality: Assurance that information is not disclosed to unauthorized entities or processes.

Availability: Timely, reliable access to data and information services for authorized users.

Integrity: Quality of an information system reflecting the logical correctness and reliability of the operating system; the logical completeness of the hardware and software implementing the protection mechanisms; and the consistency of the data structures and occurrence of the stored data. Note that, in a formal security mode, integrity is interpreted more narrowly to mean protection against unauthorized modification or destruction of information.

Controls are the security measures that are put in place to ensure confidentiality, integrity, and availability.

Within the NIST RMF, there are a total of 3 Classes and 18 Families (See Class Share) from which the baseline sets are formed. Each security control describes an objective cybersecurity condition achieved through the application of specific safeguards, or through the regulation of specific activities. The objective condition is testable, compliance is measurable, and the activities required to achieve the objective condition for every security control are assignable, and thus accountable. The security controls specifically address availability, integrity, and confidentiality requirements, but also take into consideration the requirements for non-repudiation and authentication.

Information is not protected by just one control. Multiple layers of controls used effectively is a cybersecurity strategy called "Defense-In-Depth". Referred to as the "Castle Approach", this allows system security controls to be used specifically for their purposes and relied on to protect the system in conjunction with the control sets around them as a "team". A castle has high walls, surrounded by a moat and stationed with guards. Information systems must employ similar layers of controls for protection. Defense-In-Depth strategy integrates People, Operations, and Technology capabilities to establish cybersecurity protection across multiple layers and dimensions. Successive layers of controls will cause an adversary who penetrates or breaks down one barrier to promptly encounter another Defense-In-Depth barrier, and then another, until the attack is detected. We can then react to the attack by either blocking or counter-attacking.

Remember that security is based on a "Layers of Defense" approach. No single or even several layers of defenses is an absolute safeguard. With each added layer of defense added to each system you help harden it against all but the most aggressive intruder.

We are using our controls effectively when we have reduced the risk to our information and systems to an **acceptable** level. But what does it mean when risk is "acceptable"? We need to define what constitutes risk and what level of risk is acceptable in a standard manner across the Enterprise. Later, we will see how the Federal Government defines risk and what level of risk is acceptable.

14900 Conference Center Dr,
Suite 200
Chantilly, Virginia 20151

info@vtscyber.com
703.498.2150 703.498.2149

When the right set of controls is in place, the information system is ready to be **assessed** and **authorized** to ensure the **level of risk** introduced by the system is **acceptable**.

The A&A Process

The process of **Assessment & Authorization (A&A)**, previously called Certification and Accreditation (C&A), is the process by which information system controls are evaluated to ensure they preserve an acceptable level of risk to an organization's data, networks, and dependent operations.

Assessment —
In the risk management framework, security control **assessment** replaces the DoD DIACAP's certification process. NIST defines assessment as the testing and/or evaluation of the management, operational, and technical security controls to determine the extent to which the controls are implemented, operating as intended, and producing the desired outcome with respect to meeting the security requirements for an information system or organization. The outcome of assessment is the security assessment report. The report provides essential information used by authorizing officials to make system authorization decisions. An assessment is usually performed by a Security Control Assessor and the staff and contractors working for him/her. Security Control Assessors and their staff normally do not have a stake in the system, but are cybersecurity professionals with expertise in controls testing and evaluation.

Authorization —
As the Designated Approving Authority (DAA), under the older C&A frameworks, accredited the information system as a result of certification, a senior organizational official within the RMF title Authorizing Official (AO), **authorizes** the operation of an information system and accepts the risk based on a security control assessment.

The senior organizational official balances the benefits of operating an information system against the potential adverse impacts to the organization if the system or information suffers a loss of confidentiality, integrity, or availability.

System authorization is the end to the system deployment process and the beginning to ongoing security maintenance. The system authorization package includes information about how the system has been implemented, but also information about how the organization and system owner will manage security over time.

At it's foundational basis...
RMF ensures that you and your organization:

1. ***Can say that you do it***
2. ***Write down how you do it***
3. ***Prove that you do it that way***

Which shows that you ACTUALLY do it.

In simple cyber industry lexicon... it is documented evidence that due diligence and due care is actually taking place.

14900 Conference Center Dr,
Suite 200
Chantilly, Virginia 20151

info@vtscyber.com
703.498.2150 703.498.2149