Abstract

Cyber-security is based upon risk management principals applied to securing systems against a variety of either threats or vulnerabilities that would compromise system due to authorized or unauthorized users, failures in software or hardware or from external sources including environmental to natural disasters. The National Institute of Standards and Technology (NIST) has been charged by the current administration to develop Cyber-Security Framework based on the NIST Risk Management Framework (RMF) (NIST SP800-37)[2] and NIST Security controls (NIST SP800-53)[3]. The Department of Defense (DoD) is now moving to use the NIST risk and security controls frameworks to replace the "dated" DoD 8500 series of guidance for security management used to Certify and Accredit (C&A) systems based upon Confidentiality (Classification Levels) and Integrity and Availability (Mission Assurance Category – MAC levels).

This author believes the weakness in the current and proposed NIST cyber-security framework has a weakness for systems' under development. The NIST 800-37 Security RMF is applied in the during Categorize IS and Select (of the baseline) security controls, but is not continually retained and applied during the Security Requirements Management steps, and important attribute (RISK) is not used to monitor the progress to correct security weaknesses and deficiencies. Risk "re-enters" in the Authorize steps as part of Plan of Action and Milestones (POA&M) document, prior to submitting the ATO.

The standard contractor process is to apply System Engineering principals, which is to convert a baseline set of security controls into security requirements, followed by requirements decomposition down to functional or allocated requirements. Then verification and testing begin to determine if the security requirements are being meet. Validation is used to determine that the secure system meets the intentions of the customer prior to deployment (ATO). The contractor develops a set of security requirements and conducts risk assessment at the beginning, again during the developmental stages and then lastly during the testing of the system.

This author proposes to continue the Security RMF "security risk life cycle" as a key component of the requirements development, decomposition and allocation cycle. The principal is based upon continuation of the risk levels used during the selection of the baseline security controls.

- Security controls at "Low" Risk are risk accepted & may not need mitigation.
- Security controls at "Medium Risks" inherit risk levels and requirements' inherit risk levels.
- Security controls at "High Risk" inherit risk levels:
  - Risk levels are attributes of the requirement & the "children" requirements.
  - "Risk waterfall" mitigation steps have requirement(s) assigned,
  - Risk waterfall requirements verification criteria success determines mitigation success.

This accomplishes two very important steps,

1) It prioritizes requirements that mitigate the primary security risks to the system and,
2) It provides quantitative risk mitigation evaluation metrics as to how successful the requirement actually lessoned the risk to the system.

1 Introduction

Risk "is a measure of the extent to which an entity is threatened by a potential circumstance or event, and function of: (i) the adverse impacts that would arise if the circumstance or event occurs; and (ii) the likelihood of occurrence."[1]

NIST Risks Management Framework (RMF) (Figure 1)[1] shows the first two steps (Categorize IS and Select Security Controls) to apply risk processes to the selection of security controls "as needed based on risk assessment".[1]

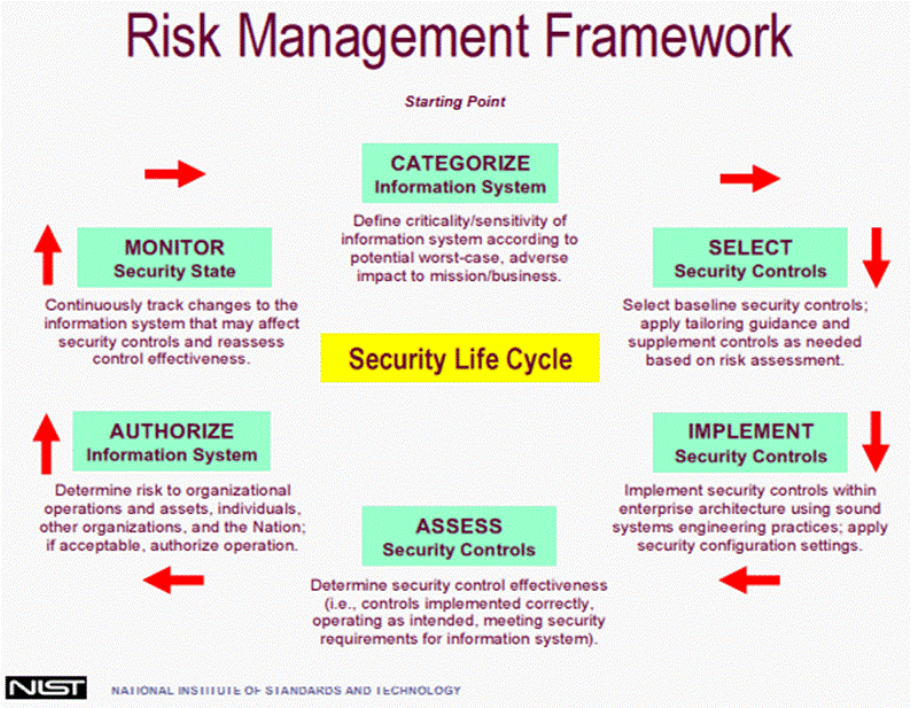

Figure 1 NIST Risk Management Framework (RMF) [1]

The NIST (NIST SP800-37) guidelines are now expanding beyond the "DoD" and are recognized as an import risk assessment for other industries, large businesses and others to use. NIST has recognized that "it is imperative that leaders at all levels of an organization understand their responsibilities for achieving adequate information security and for managing information system-related security risks"[1] and that is why standards like NIST, ISO, COBIT and others are being developed.

1.1 Extending th Ris Assessment process into Requirements Management

believe a process can be developed to bridge a gap between using the new NIST Cyber-Security Framework (NIST SP800-37 R1 Risk Management Framework) and the NIST Security controls (NIST SP800-53).

The process starts with the NIST processes (1 & 2) below:

1. Develop the risk assessment for likelihood (L) & consequences (C) and determine the types of risks the business, enterprise or program will need to address.
2. Develop a set of Security Controls for each risk in the risk assessment matrix. Each risk has one or more associated Security Controls that when implemented will mitigate the risk to an acceptable level.

Second, each requirement is decomposed following a typical "INCOSE V" of requirements management decomposition:

3. Each "High" or "Medium" risk has its' corresponding Security Control(s), and those control(s) decomposes into security requirements.
4. Security requirements are decomposed into derived and functional requirements.

Last, extend the risk "Security Life Cycle" (Figure 1) process where each security related requirement inherits the Security Control's risk value as an attribute keeping the risk and requirements management life-cycle synchronized:

5. Require mitigation waterfall to mitigate every "High" security risk (start the POA&M tracking process at initial requirements generation).
6. For "High" security risks, risk waterfall must be developed, and set of mitigation weightings for each "step" in the risk mitigation waterfall must be assigned. Functional requirement(s) are assigned to each step in the "High" risk "waterfall" mitigation activity.
7. Requirements verification must address how the methods and criteria will mitigate the security risk (High or Medium), and what the "L & C" value will be reduced *To* before the requirements verification can be successful.
8. Successful completion of mitigation step provides a quantitative value that can assess how the security risk reduction is progressing.

Figure 2 is an illustration of steps 1-8.

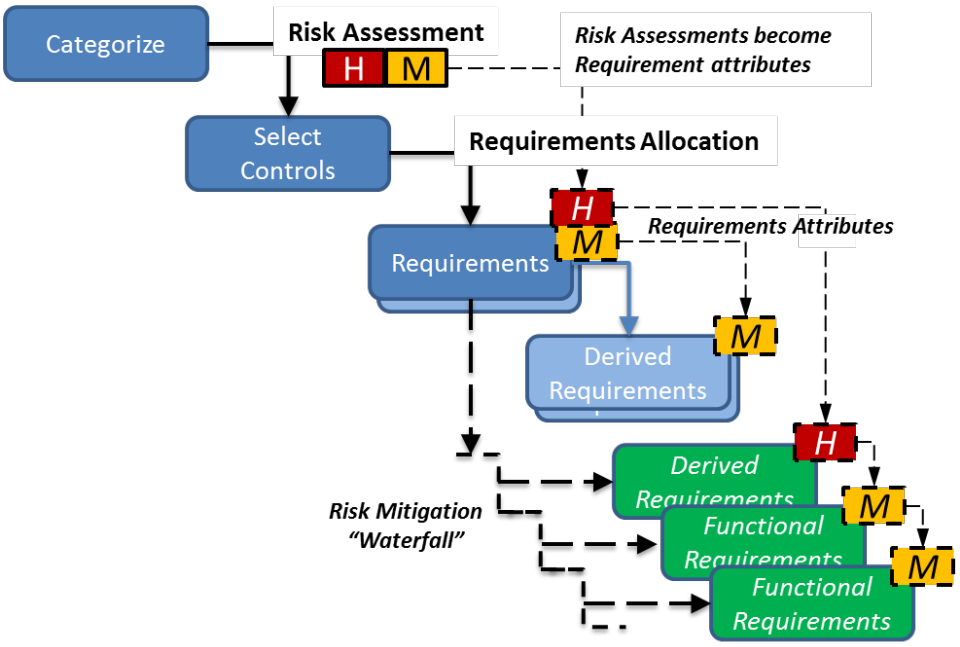

Figure 2 Risk - Requirement Management integration

Both of steps & inherit a quality approach because:

- matrix of the "weights" of a normalized set of "L&C" values assigned to all Medium to High risks will form a quality index as to how the program is both progressing over time and how much "security risk" is left at any point in time.
- The risk manager and the team that evaluates and accepts the step in the risk mitigation are independent (i.e. a Quality Management function). Each step is also analyzed and accepted by a member of program or executive management who must accept the overall risk level at the end of the program.

2 Candidate Security Assessment Groups

have developed a candidate examples using the Verizon Data Breach Investigation Report (DBIR)[4] and "Military, NASA other agencies hit in series of attacks"[7] about UK Hacker as my sources:

2.1 Larg Business Espionage Example

This example comes from an article where prosecutors have charged a U.K. hacker in connection with a year-long series of attacks on U.S. government and other networks that resulted in the theft of the personal information of government employees and massive amounts of other sensitive data, causing damages in the millions of dollars. The co-conspirators exploited weaknesses in Structured Query Language (SQL) databases and Adobe ColdFusion Web application, breaching thousands of computer systems in networks run by Army, U.S. Missile Defense Agency, Environmental Protection Agency and NASA. They used automated scanners to look for vulnerabilities among large array of IP addresses. They would then use SQL injection attacks, exploit ColdFusion exploits and other tactics to gain access, and plant shells or backdoors on the networks so they could return.[7] The following Table 1 is a partial history of the attacks:[7]

Date	Organization	Type of attack	Data involved
Oct. 2012	Army Corps — Engineer Research & Development Center	ColdFusion	Demolition and disposal of military facilities
Oct. 2012	Army Corps	ColdFusion	Natural resource management
Oct. 2012	U.S. Army, Network Enterprise Command	SQL injection	PII (> 1,000 individuals)
Oct. 2012	U.S. Army — Army Contracting command, Redstone Arsenal	SQL injection	Nonpublic competitive acquisition bid data and attachments
Oct. 2012	U.S. military — Plans and Analysis Integration Office	ColdFusion	Defense program budget data
Oct. 2012	U.S. DoD — Missile Defense Agency	ColdFusion	PII (> 4,000 individuals)
Dec. 23, 2012	Army Corps — Engineer Research & Development Center	ColdFusion	Not specified in indictment
Jan. 11, 2013	U.S. Army War College	ColdFusion	Not specified in indictment
July 10, 2013	NASA	ColdFusion	PII of NASA employees
Jan. 3, 2013	EPA — Federal Facilities Compliance Assistance Center	ColdFusion	Non-PII personnel data

Table 1 Espionage - Data Breach example

The "Security Controls"

1. Defense in Depth: DMZ, intra-nets, IDS, Server isolation, un-used ports, protocols and services (PPS) USB disabled.
    - NDA, MOA with Supply Chain; and the supply chain is change board and configuration managed.
    - STIG testing, assume penetration has occurred, now in continuous monitoring and detect & react times for anomalies.
        - STIG test includes Registry & RAM for C2.
2. Audit Logs: review and look for changes. Also, protect against malicious activity and "ransom ware" by using separate archive for both backups and for audit logs.
3. Real-Time monitor for large file transfer & VPN traffic, especially in off-hours. Implement time and privilege user times.
    - AV updated (daily), patched weekly, Firewalls patched weekly.
    - SEA&T: training, awareness & education.
        - Includes email phishing, social media.

- Anti-virus o BYOD, data-at-rest (DAR) policy, Cloud policy (where data is being stored is as important as to what the confidentiality level of the data is.

3 Summary

3.1 Metrics and Quality driven NIST Security RMF

Using NIST SP800-37 risk management processes and the draft Framework (Figure **2** to select the NIST SP800-53 security controls and apply a weighted normalized assessment to each control (Figure 3):

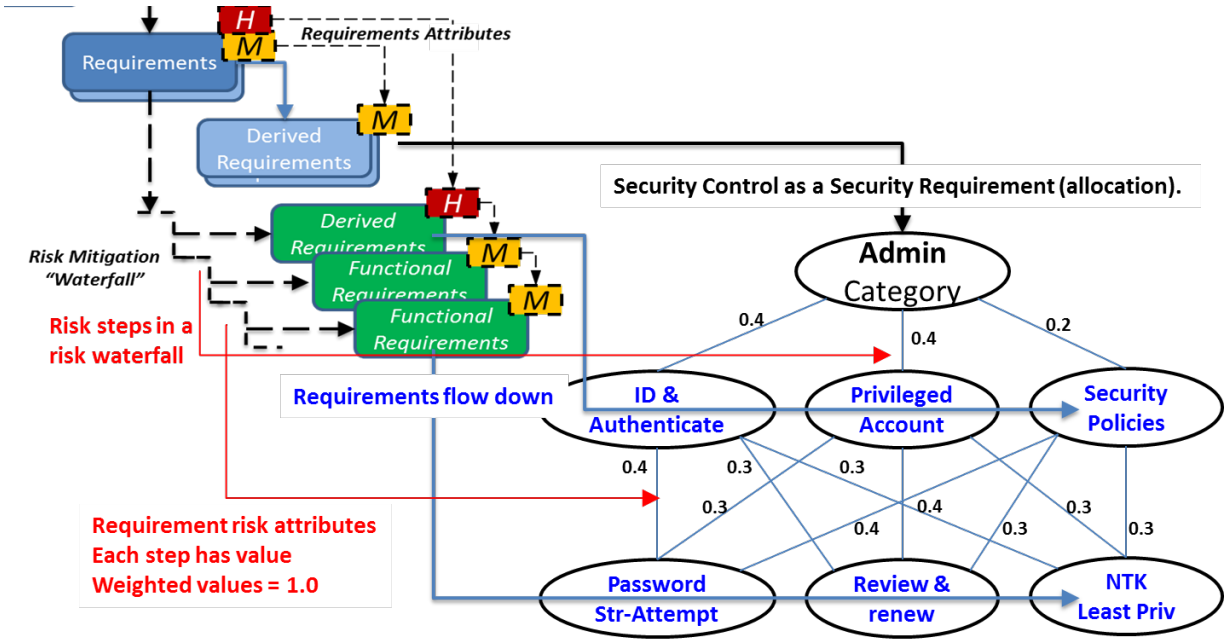

Figure 3 Normalized / Weighted set of RMF attributes per Requirement

3.2 Requirements Management

Security control are converted to security requirements, and those requirements are decomposed and flowed down to a functional level that addresses the security of the system, behavior and components of the system to be approved.

1. Assign at least one security requirement per (risk waterfall) step.
2. Requirements verification success mitigates the risk to a lower (L or C) value.

3.2.1 Risk Weightings

Using a Pough diagram, calculate the weights for Risk Management Security Controls that first mitigate Likelihoods (L) and then mitigate Consequences (C) assigning weights to the "Risk Waterfall".

1. Requirement validation is the only way to demonstrate and document successful risk mitigation steps.
2. Weights and Normalization provide: 1) priorities, 2) a repeatable and quantitative risk reduction process and collection process for security (risk tracking) processes (POA&M), (Figure 4).

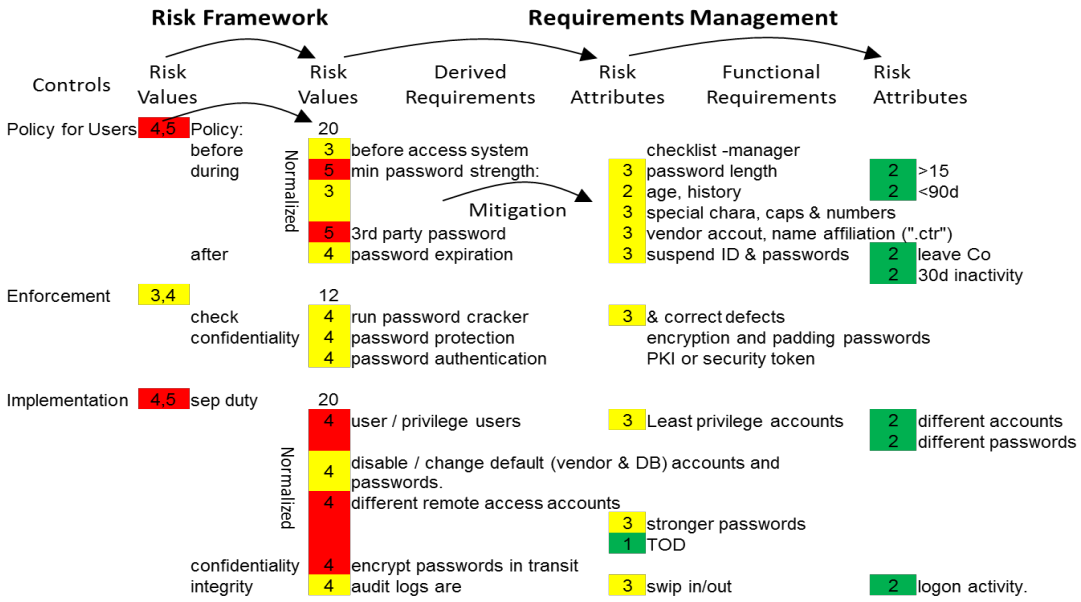

Figure 4 Integrated Risk & Requirements Frameworks

References

NIST "Risk Management Framework" PowerPoint slides, slide 3: http://csrc.nist.gov/groups/SMA/fisma/documents/risk-management-framework-2009.pdf

NIST SP800-37 Rev1 "Guide for Applying the Risk Management Framework to Federal Information Systems, A Security Life Cycle Approach", February 2010. http://csrc.nist.gov/publications/nistpubs/800-37-rev1/sp800-37-rev1-final.pdf

NIST Special Publication 800-53 Rev 4 "Security and Privacy Controls for Federal Information Systems and Organizations" April 2013. http://dx.doi.org/10.6028/NIST.SP.800-53r4

4 Verizon "2013 Data Breach Investigations Report", http://www.verizonenterprise.com/DBIR/2013/

NIST: "Draft Illustrative Framework Example" http://www.nist.gov/itl/upload/framework_example_electric-tysubsector_20130830.pdf

7 Kevin McCaney, "Military, NASA other agencies hit in series of attacks", Oct 29, 2013 http://gcn.com/Articles/2013/10/29/UK-hacker.aspx?Page=1

9 Nina Easton "The CEO who caught the Chinese spies red-handed", Fortune Mag, July 22, 2013. Pp88-100.

Author: J Peeler (peelerja@cox.net or jpeeler@stevens.edu)