NETCENTRICS

Leveraging the CCRI process to support Ongoing Authorization within the Risk Management Framework

Marvin Marin, NetCentrics Corporation

June 2016

Issue: Risk analysts struggle to calculate, prioritize and communicate risks to the Authorizing Official (AO), who accepts or denies the risk in support of a system's accreditation based on a risk report. A major problem not addressed by either the Defense Information Assurance Certification and Accreditation Program (DIACAP) or the National Institute of Standards and Technology (NIST) Risk Management Framework (RMF) is the difficulty of quantifying the level of risk an accredited system poses and the failure to provide a method to consistently reach the same conclusion given different analysts, agencies, or auditors. The key to providing consistency is in changing how the systems are evaluated and scored. The proposed new approach suggests using a well-known benchmark, such as the Defense Information System Agency (DISA) Cyber Command Readiness Inspection (CCRI) method, to remove ambiguity, provide consistency across approving agencies and also to dramatically decrease the time between the test event and approval/denial of the system to operate. This recommended approach can dramatically reduce response time and provide greater confidence in the conclusions of the analysts.

Keywords: Assessment & Authorization (A&A), Certification & Accreditation (C&A), RMF, DIACAP, CCRI, Risk Management, Information Security Continuous Monitoring, Ongoing Assessment & Authorization.

INTRODUCTION AND BACKGROUND

As cyber security has become more prominent, cyber analysts must simultaneously increase situational awareness while reducing reaction time to identify and respond to cyber threats. This makes the need for faster risk-based decisions without sacrificing accuracy paramount. Paper-based and document-driven processes and models are time consuming, support an outdated information technology acquisition process, and don't keep up with the evolution and development of exploits against static targets.

Generally, the A&A process may take on average 3-18 months to complete and culminates with a review of a volume of documents, artifacts, and technical findings to create an artifact that conveys the risk to

an AO so an accreditation decision can be made. The A&A process defined by the RMF process is comprised of six phases (Figure 1) that document the information system, attributes (requirements, applicable security controls, etc.); technical and non-technical weaknesses, and a risk-based decision in order to authorize.

RMF

The overall RMF process is intended to be iterative so that as the cycle continues the individual steps can build upon each other, act independently, or trigger functions and tasks in a different step (NIST 800-37). For example, a security control that was documented as inherited from another service or program may be assessed as non-compliant requiring a change in how the control is documented, which leads to an additional assessment to validate the control. Therefore, instead of a rigid linear process, RMF encourages flexibility and agility to meet mission requirements while providing a structured framework that encourages mitigating risk of operation

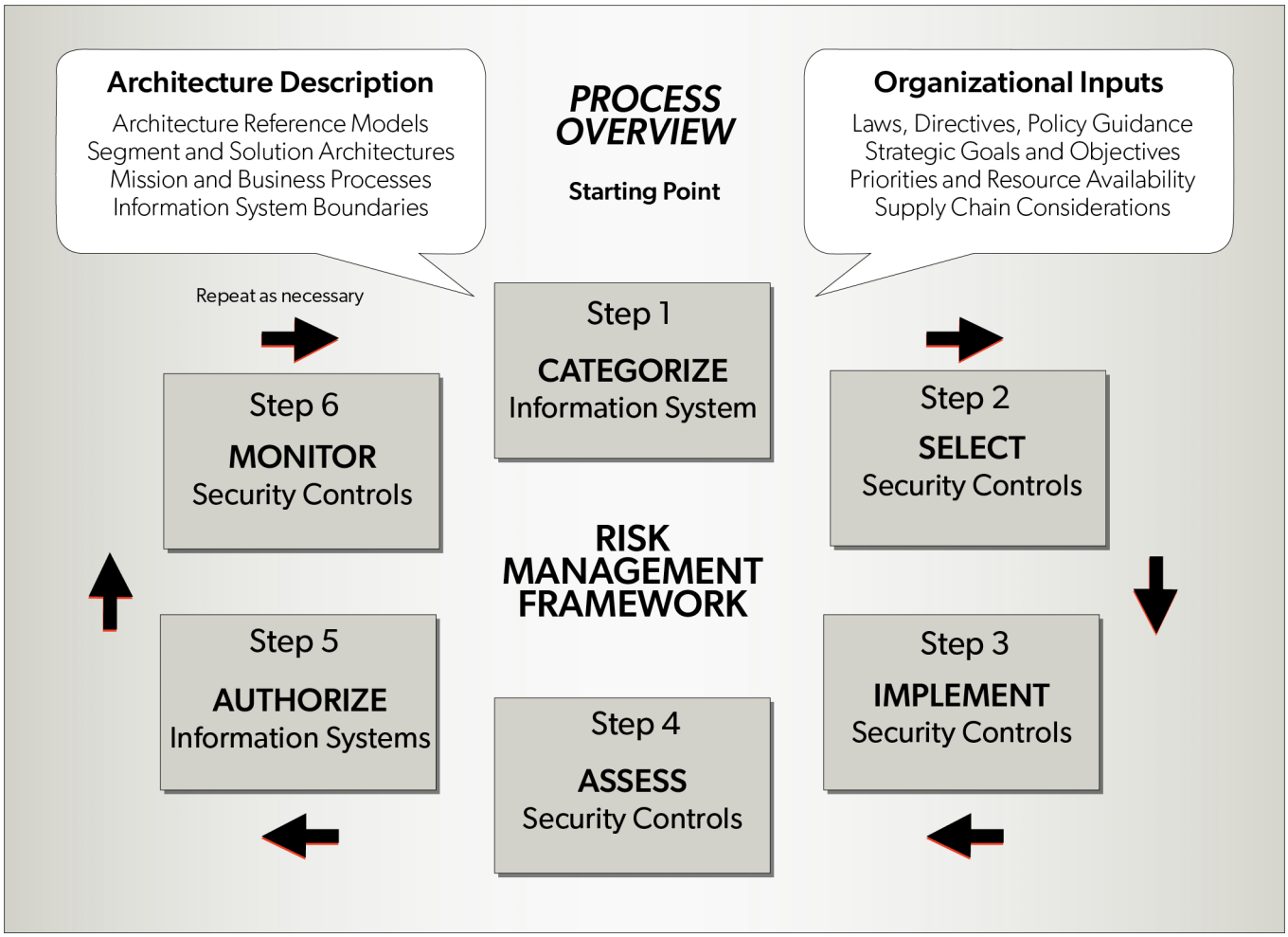

Figure 1 Risk Management Framework

In practice, navigating through the RMF process tends to be a tedious and time consuming exercise that emphasizes documentation over control implementation and testing. The RMF process is not necessarily a failure point; rather, some implementations of the framework put a higher emphasis on the review of documents instead of the evaluation of technical security controls and the overall risks. While within the purview of the AO's risk acceptance and decision making authority, this also makes sharing security information across enclaves and organizations much more difficult. For example, some organizations may perform a vulnerability scan and cursory review of documentation to determine if the system has met required security requirements. Other organizations may be more proactive and test every asset against a required baseline such as the Security Technology Implementation Guide (STIG) or the United States Government Configuration Baseline (USGCB) and then perform manual Independent Verification and Validation (IV&V) on non-technical controls (e.g. physical and environmental controls). ***This disparity between how organizations implement the process is a major hindrance to sharing security information and causes delays that could be rectified through the use of a consistent and repeatable process.***

CCRI

The CCRI process is used to assess Department of Defense (DOD) systems against a known minimum security baseline so that a system or network can resist a cyber-attack. The process combines the evaluation of technical and non-technical controls against established baselines and outputs a metric that can be applied to every DOD service to determine if an assessed site meets the minimum requirements to operate on the Department of Defense Information Network (DODIN). A failing score demonstrates that the site has a negative security posture and that US Cyber Command (USCC) may terminate that site's connection to the DODIN as it provides an unacceptable level of risk that should not be shared with the entire defense community. Additional information about the CCRI process is available to personnel with a Common Access Card (CAC) by visiting the Defense Information Systems Agency (DISA) website http://www.disa.mil.

Proposed Solution

The proposed solution is a model that focuses on the combination of the A&A and CCRI processes to support automated assessments. The use of the CCRI methodology to evaluate a system for technical and non-technical weaknesses creates a consistent, repeatable and reliable metric. Additionally, if the scoring metric is agreed upon in advance (e.g., any score over 90%) an enterprise application such as a Governance Risk Compliance (GRC) tool could automatically issue an Approval to Operate (ATO) letter without further human intervention (e.g. the AO). Finally, if a common metric is used across the Federal Government and/or DoD, reciprocity reviews could also be quickly completed with limited human review thereby assisting in the transition of the organization from the use of Static Authorization to an Ongoing Authorization mode of operation. **The solution increases consistency across agencies or organizations, reduces response time, decreases time and labor cost to the Government, and simplifies systems integration and data exchange, since risk will be assessed in the same way.**

While this paper focuses on the CCRI as the testing methodology to use, any testing methodology could be used to drive the same result. For example, the Marine Corps has experimented with "C&A in a day," an Ongoing Authorization model, where an evaluated system is placed in a lab and multiple vulnerability scanning and penetration tools are used to evaluate weaknesses. Their GRC tool (RSA Archer) can then aggregate the information, conduct a comparison between weaknesses and known upscale protection mechanisms, (i.e., the security stack) and make a determination if the system meets the minimum certifiable threshold. When successfully tested against a Program of Record (POR), the evaluation to provide a simulated ATO took two days and found undisclosed faults by the vendor, whereas receiving an ATO letter through the commonly accepted practice would have taken more than three months.

While the actual scoring metric is outside the scope of this document, a score of 90% or greater is used as an example solely for this article and does not directly reflect what is required to pass a CCRI. Organizations are free to use whatever passing score they feel meets the criteria for their risk profile with the understanding that reciprocity would require a passing score to be equal to or greater than the passing score of the receiving organization. Organizations within the DoDIN would be encouraged to use the CCRI passing score as it reflects the most consistent metric available.

The automation of security control testing is supported and encouraged under NIST SP 800-53A and the proposed model is simply stated, the substitution of the assessment of security controls, the authorization process, and a focus on operationalizing the Monitor step by applying facets of Continuous Diagnostics and Mitigation (CDM).

We are proposing that the Assess, Authorize, and Monitor steps as depicted below in Figure 2 be adjusted to incorporate the CCRI process (Assess), CCRI score evaluated against AO approved metrics (Authorize) and a Plan of Action & Milestones (POA&M) (Monitor) be implemented. Figure 3 depicts the proposed adjustments to the applicable phases or steps that may be implemented within the RMF.

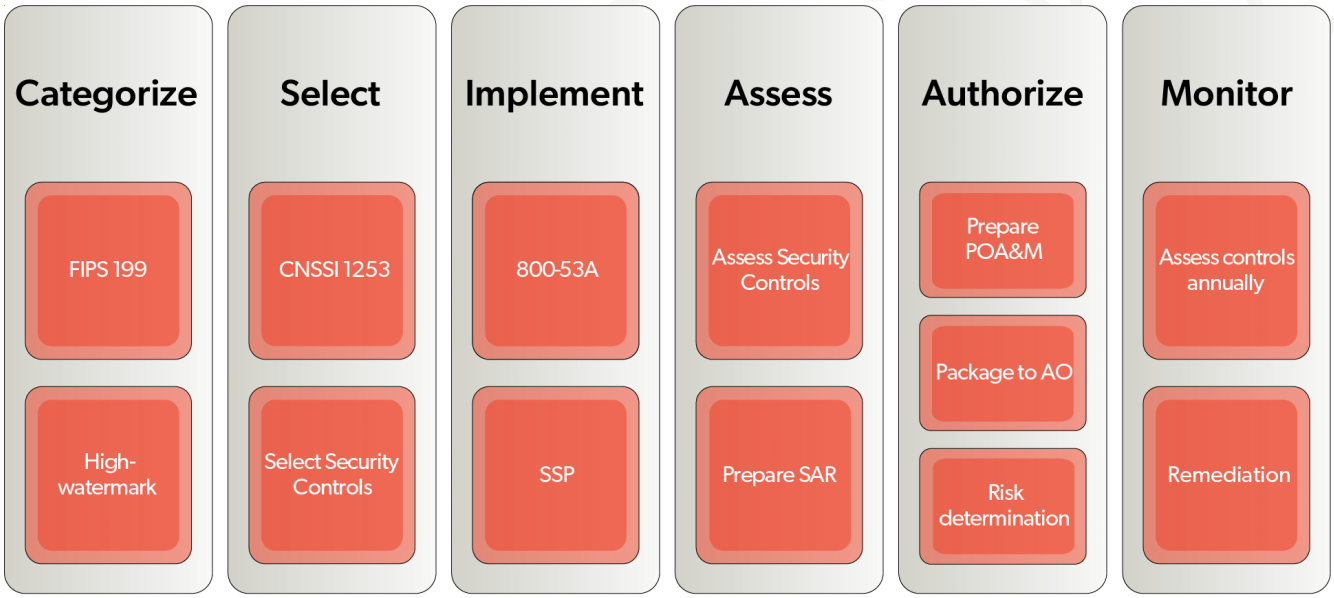

Figure 2 RMF Phases

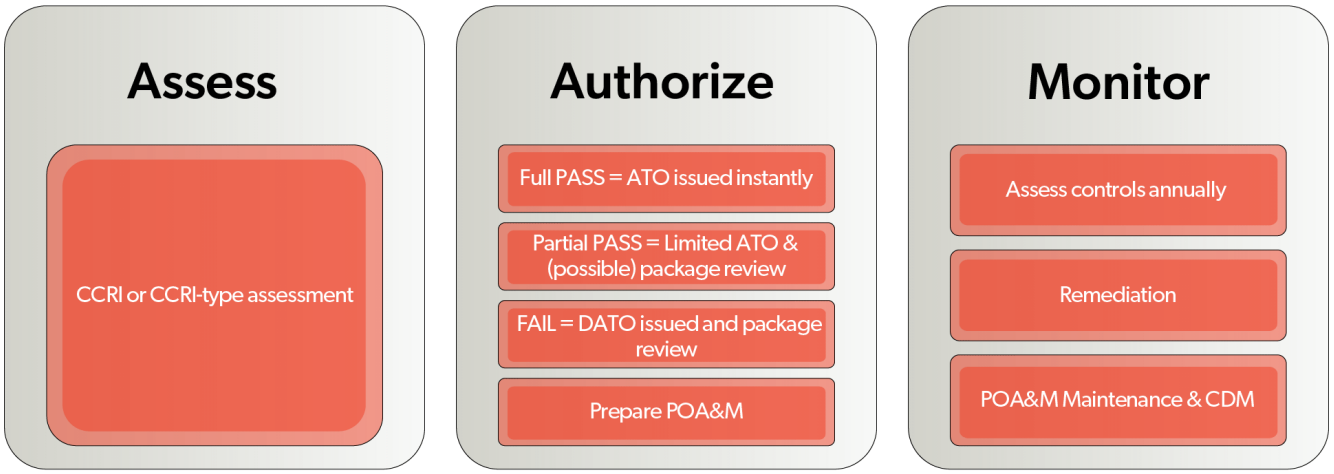

Figure 3 Proposed modifications to Assess, Authorize and Monitor

The Assess phase would be replaced with the CCRI to perform an assessment of the system or networks adherence to technical and non-technical security controls. The culmination of the CCRI will be a score that will take the place of the Security Assessment Report (SAR). The output of the CCRI test event will also allow the operational teams to begin conducting remediation or mitigation actions and to prepare appropriate POA&Ms, if necessary.

The Authorize phase would rely solely on the CCRI score and the grading criteria established by the AO. Figure 4 depicts an example of 3 systems undergoing an A&A process using the proposed solution. In the figure below, System A scored 95% which exceeds the minimum required CCRI Score (CS) of 90% to be issued an automatic ATO. System B scored a CS of 85% which is not sufficient to be granted an

automatic ATO but does exceed the level for which a Denial of Authorization to Operate (DATO) would automatically be issued. In this case, System B could be turned over for a manual review process or an ATO with Conditions (one year or less and potentially issued with stringent conditions) issued. System C scored a CS of 75% and did not achieve a sufficient score to be granted an ATO with Conditions. In this case, System C could be turned over for a manual review process and/or a DATO issued.

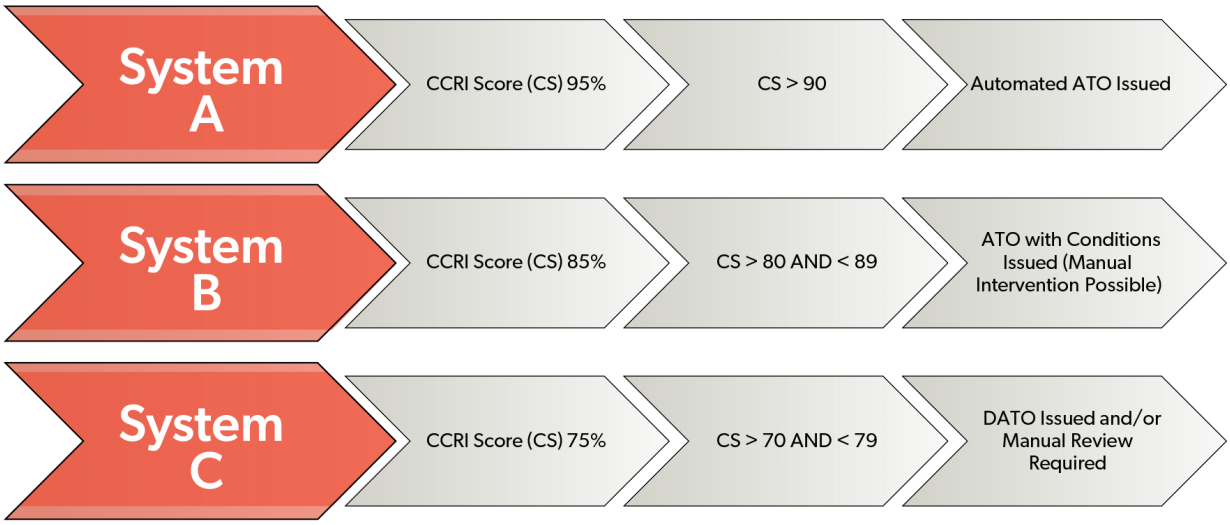

Figure 4 Examples of systems evaluated against a CCRI score

An artifact of the Assess phase will be all technical and non-technical findings against the system or network. This artifact can be used by operational support teams to correct weaknesses in the security posture of the system and to decrease the number of items that must be documented by a POA&M. For any weaknesses that are not remediated within an AO specified time-frame (e.g. 30 days) the system owner may submit the applicable POA&M('s).

The Monitor phase should align with CDM and mandate that POA&Ms be maintained in accordance with (IAW) organizational requirements (e.g., required updates every 30 days) and consistent with NIST 800-137 Information Security Continuous Monitoring (ISCM) for Federal Systems and Organizations.

CONCLUSION

Employing this new proposed solution can lead to the operationalizing of A&A and moving from Static Authorization to Ongoing Authorization. The model will provide for a significant improvement in the decrease in time between when a system is ready for evaluation and when an authorization decision is made. Additionally, the labor costs saved by moving personnel from documentation reviews to more operational roles could potentially have a positive ripple effect across DoD. Lastly, risk results can be iterative, allowing for a stronger baseline, and provide an AO with greater confidence in the risk assessment and overall process.