Cybersecurity Challenges and Resolutions for Simulator & Training Systems

Douglas E. Wedel
Defense Security Service, IOFND
Beavercreek, OH 45431
douglas.wedel.@dss.mil

Dr. Ilya Lipkin
USAF AFMC AFLCMC/WING
Wright-Patterson AFB, OH
ilya.lipkin@us.af.mil

Lt. Luis Cintron
USAF AFMC AFLCMC/WNSEB
Wright-Patterson AFB, OH
luis.cintron.2@us.af.mil

ABSTRACT

Cybersecurity (CS) requirements and considerations have increasingly been impacting special-purpose systems with embedded Information Technology (IT) such as simulator and training systems in recent years. This is primarily driven by increased insider threats, proliferation of network interconnections, and the rise of mobile computing (smartphones/tablets) as well as increased capabilities of nation states, organized crime, and political activists to gather and exploit information about current capabilities. In the past CS measures have been applied through either Risk Avoidance "shutting down a capability until the risk is eliminated" or Risk Ignorance, "operating a system without regard to the risk because of a perceived functional or operational need". However, through the use of Risk Management, CS can balance these two areas by assuring the mission and protecting the systems, networks and information by properly categorizing the system and the information through a risk based assessment process. To avoid mission impact previous policy was compliance based and risk was typically avoided or waived rather than mitigated. The DoD Risk Management Framework (RMF) (DoDI 8500.01, 2014) seeks to address the shortfalls that compliance management imposed on systems. However, a clear understanding of how to apply risk is needed to provide a balanced approach to CS. To support CS requirements this paper will present an approach for assessing risk to simulator and training systems and outline the steps necessary to overcome and mitigate said issues through a process that focuses on applicability, compliance, mitigation, and reduction of impact. This paper is not a description of the DoD RMF, but seeks to provide a process to assess CS requirements by addressing the "Spirit and Intent" of the CS requirement, its applicability, probability, and impact of applying or not applying that requirement, and identifying solutions that resolve the finding or reduces the impact to an acceptable level for authorization. This paper will strive to provide a practical approach to assessing system risk by providing initial framework examples that will demonstrate its applicability to manage new technology insertions, network connectivity, existing program limitations and mobile computing impacts to existing simulator and training systems.

ABOUT THE AUTHORS

Douglas E. Wedel serves as an Information Systems Security Professional (ISSP) for the Defense Security Service (DSS), Industrial Security Field Operations Directorate. DSS is a separate agency of the Department of Defense responsible for overseeing the protection of US and foreign classified information in the hands of cleared industry by providing information technology services that support the industrial and personnel security mission of DoD and its partner agencies. A charter member of the Air Force Platform IT Working Group and recognized expert in Cybersecurity Risk Assessment Management, Mr. Wedel addresses cybersecurity activities to include the Assessment and Authorization (A&A) and oversight of cleared contractor's Information Systems (IS). His broad breadth of experience technically assessing IS directly supports the Authorizing Official (AO) in establishing procedures and standards supporting consistent and efficient A&A activities. His current research interests include enhancing the understanding of risk based processes that evaluate stand-alone, special-purpose systems with embedded IT that have critical functions, enabling managers to understand cybersecurity risk and apply a quantifiable risk assessment to their operation. Mr. Wedel has a Bachelor's Degree in Management Consultancy, a MBA in e-Business and IT, an MS in Information Technology and Security Management and is currently a Doctoral Student at Colorado Technical University (CTU) in Computer Science and Information Assurance/Cybersecurity.

Dr. Ilya Lipkin is a project software engineer for AFLCMC. Previously he was assigned to AESG/EN MQ-1 and MQ-9 Training Systems, Global Hawk Simulations project engineer at Wright Patterson AFB. He is a member of the AFLCMC software working group AFSIP, Future Airborne Capability Environment (FACE), and Sensor Open Systems Architecture (SOSA) working groups. His current research interests are in software architecture and sensor systems decomposition. He has MSE computer engineering University of Michigan, an MBA in Operations Management, and PhD Software Project Productivity from University of Toledo's College of Business Administration.

Lt. Luis Cintron is an ISSM and Training Systems Engineer for the ATARS-II and JTC-TRS programs at the Simulators Division, Wright Patterson AFB. Lt. Cintron received his Bachelor of Science in Computer Engineering from the University of South Florida. His areas of expertise include embedded systems, cross-platform mobile development, enterprise application services, service-oriented architectures, and web development and security. He has led the development of major enterprise level applications as well as commercial mobile applications and web services.

Cybersecurity Challenges and Resolutions for Simulator & Training Systems

Douglas E. Wedel
Defense Security Service, IOFND
Beavercreek, OH 45431
douglas.wedel.@dss.mil

Dr. Ilya Lipkin
USAF AFMC AFLCMC/WING
Wright-Patterson AFB, OH
ilya.lipkin@us.af.mil

Lt. Luis Cintron
USAF AFMC AFLCMC/WNSEB
Wright-Patterson AFB, OH
luis.cintron.2@us.af.mil

INTRODUCTION

This paper seeks to provide guidance to practitioners on the assessment of cybersecurity risk and the tailoring of security requirements to reduce the probability, consequences, and impacts to special-purpose, stand-alone systems with embedded Information Technology (IT) as early as possible in the design, development, testing, operational deployment and sustainment of simulator and training systems. Increasingly simulator systems are embedding Information Technology (IT) capabilities to deliver state-of-the-art functions to the users. These systems are most often identified within IT as stand-alone systems, special enclaves, or private networks that perform specialized functions which are commonly referred to as "Tactically Embedded or Platform Information Technology (PIT) Training and Simulator (T&S) systems (DoDI 8500.01, 2014). Although T&S systems are designed for training purposes they are also required to provide critical information to both external and internal users. Thus T&S organizations are encouraged to be proactive in assessing and managing risks to these systems and their underlying mission processes. However, most often risk is assessed to cost and schedule impacts associated with the acquisition of the T&S system or the operational mission of the system. These functional requirements tend to avoid the "What If" conjecture of the Cybersecurity (CS) risk. It is common knowledge that the cyber threat environment is escalating, with targeted attacks having the capability to physically damage infrastructure, deny or degrade its mission, or compromise critical information.

As a result of the increased threat environment, the Department of Defense (DoD) has revised the Certification and Accreditation (C&A) process to incorporate RMF (DoDI 8510.01, 2014). The RMF, was developed in consultation with owners and operators, and is a tool to assist organizations with identifying and mitigating risk for systems including PIT systems. Thus RMF can be used to assess and manage risk exposure and identification measures to manage or mitigate risk to an acceptable level.

IMPORTANCE OF RISK MANAGEMENT FOR THE T&S SYSTEMS

It is increasingly being understood by the international community that, although T&S stand-alone and interconnected systems are reliable for interconnectivity, they are highly vulnerable and very difficult to secure when they are interconnected to other systems or networks that require information exchange such as Distributed Mission Operations (DMO) environments. These systems have been interconnected with each other in order to create a common virtual world, reduce cost, and provide instant updates such as operational status of a system for maintenance/sustainment purposes, as well as for sharing data with external users or other services on the network. With the infrastructure of the World-Wide-Web (WWW) connecting these systems has been relatively easy. However, it opens the door to external threats. Furthermore, the digital age has injected internal threats from insiders moving, managing, and manipulating larger amounts of data. As a result there is a clear need to understand threats, vulnerabilities, impact as well as associated risks to these systems. The challenges facing T&S systems, and the underlying reasons as to why these systems are especially vulnerable, include issues surrounding increased connectivity, interdependencies/supply chains, complexity, unmanaged changes to the configuration, continued use of legacy systems and devices, interoperability, and interconnectivity.

The compromise of the T&S system can result in the failure or disruption of the day-to-day management of services to the operational user causing the significant loss of mission assurance that affects the overall confidence in a T&S organizations ability to manage the CS risk of its systems and networks. It can also involve legal actions and penalties for non-compliance with regulatory requirements.

BACKGROUND

In July 2006 the Department of Defense Guidance for the Certification and Accreditation of Automated Information Systems (AIS) and networks was published. It established rules of engagement for AIS systems with objective of meeting the DoD Enterprise Architecture Strategy which was geared to a Unified Business approach to operations of Global Information Grid (GIG). This led to the implementation of Standardized Desktop Configuration (SDC) and One Network Strategies. Stand-alone systems were treated as AIS unless they met special criteria. However, there

was no direction beyond a short definition as to what these special stand-alone systems were, nor how to uniformly designate, certify and accredit them (DoDD 8500.01, 2006).

The DoD Information Assurance Certification & Accreditation Process (DIACAP) identified that Platform Information Technology (PIT) systems were not required to complete Certification and Accreditation (C&A). This led to organizations and programs stating that their systems were PIT in order to avoid what they considered a paperwork exercise that impacted their cost and schedule and levied unrealistic requirements on their systems that hindered functionality. It was understood that T&S systems were classified as PIT, because most of these systems could not comply with AIS security requirements without affecting functionality, or critically increasing cost and schedule impacts. Further, contractual requirements to the traditional engineering and design of these systems drove managers to seek "Waivers" from IA requirements by declaring that they were PIT systems.

However, Federal and DoD processes for managing Information Assurance (IA) required that these systems address and manage risk within their systems. In 2008 the Air Force CIO directed that all PIT systems address IA, validate and verify IA risks and be Certified and Accredited by an identified Accrediting Official. As a result while DIACAP did not apply, the C&A Risk Management Methodology was deemed as the right solution. To further develop this approach, Air Force CIO established a Working Group to address PIT Systems. Final product of the working group was issuance of a General Memorandum to address Platform IT within the Air Force. This memorandum was applied through the Air Force Certification and Accreditation Program (AFCAP) under Air Force Instruction 33-210, and the creation of the Air Force Platform IT Guidebook which established a Risk Management Process to identify, designate, assess, validate, and authorize Platform IT systems within the Air Force (AFI 33-210, 2014).

PROBLEM STATEMENT

As part of the acquisition process, T&S systems require a validation and verification of the CS risk in their systems as well as an understanding that Risk Mitigation, rather than compliance to requirements is critical for their ability to perform the mission in a secure and functional manner. T&S Program Managers and Engineers have to understand system's mission, security, and functional requirements beyond their impact to cost and schedule. Therefore, it is imperative that assessment of CS as well as functional requirements occurs as early as the design and development

Figure 1: Compliance Management vs. Risk Management (Source AFLCMC/EZAS)

phase for T&S systems. Conversely, T&S Operational Managers must understand that applying Information Systems requirements without a serious CS risk assessment can impact the overall Air Force training mission. Thus deploying systems without assessing risk to T&S as well as security can have a catastrophic impact to the mission, organization, and people.

With the issuance of the new DoD Risk Management Framework (RMF), risk identification is critical as presented in Figure 1. This issuance establishes that program managers and senior leaders are required to identify CS requirements and risk as early in the process as possible. The DoD RMF provides structured approach to categorizing and identifying baseline CS requirements for a given system. However, once these requirements are

identified, it is of utmost urgency for T&S systems to determine if the baseline requirements are applicable or non-applicable, compliant or non-compliant, and what processes or technical implementation will meet said requirements. Furthermore, if those requirements cannot be met technically what mitigation strategies can be applied to lower the risk for a T&S system to an acceptable level for authorization?

UNDERSTANDING PLATFORM IT SECURITY REQUIREMENTS

When identifying CS requirements which apply to T&S platform IT systems, the Information Systems Security Manager/Officer (ISSM/O) should identify a baseline of controls which apply to the system annotating them on the Security Control Requirements Traceability Matrix (SRTM). The categorization of the system/information is the first step in developing a baseline of requirements found in the National Institutes of Standards and Technology (NIST) 800-53 and Committee on National Security Systems Instruction 1253 (CNSSI 1253). T&S platform IT systems should end up with a tailored set of CS requirements addressing risk. The (CNSSI) No. 1253 Overlay for Platform IT systems adds compensating controls. This Industrial Control Systems (ICS) Overlay applies to Platform IT (PIT) systems as stated in DoDD 8500.01 Cybersecurity Directive, Enclosure 3 (CNSSI 1253 Overlay, 2014).

In the Simulation and Training Systems domain this would apply to the following platforms that may include PIT are but not limited to the Aircrew Training Device (ATD), Weapons System Trainer (WST) Maintenance Training Device (MTD), Operational Flight Trainer (OFT), Boom Operator Weapons System Trainer (BOWST), and their support-and-development systems such as the Training Systems Support Center (TSSC) which acts as a development and test center. Before deploying upgraded software or equipment, these systems must be tested to assess their functionality and reliability in order to avoid negatively affecting the training mission.

T&S platform IT systems are stand-alone systems that perform a specialized function through embedded IT hardware and software applications that are usually event driven and frequently apply simulation, stimulation, emulation and real-time software applications or devices with embedded software technology. These types of specialized systems are pervasive throughout the DoD infrastructure and are required to meet numerous and often conflicting functions that support the mission. In the Simulation and Training systems world, Platform IT systems are usually non-critical systems, such as the ATD (Aircraft Cockpit) where the downtime or loss of a system would not critically affect the Air Force Training Mission, however, such loss or unavailability would impact the AF Training Mission in a rippling to cost, schedule, flight hours and new aircrew pipeline issues.

Historically within the simulation and training industry, simulator systems were contractor managed and supported, with little consideration given to the CS impacts. As a result, T&S systems are slowly implementing the latest DoD requirements for CS and in some cases are unable to meet latest guidelines due to cost or schedule impacts to the systems. However, T&S systems are now being connected to each other in order to provide greater training opportunities through virtualization scenarios and distributed training capabilities. These Platform IT systems require interconnections using Controlled Interfaces (CIs). They sometimes require Human Machine Interfaces (HMIs) to monitor the processes. Current Platform IT Simulator systems and subsystems are now a combination of Operational Technologies (OT) and Information Technologies (IT) posing a significant challenge to properly understand and secure these systems.

To assist in evaluating CS impacts to T&S systems, an emerging concept was introduced for special-purpose systems called Cyber-Physical Systems (CPS). "CPS are engineered systems that are built from and depend upon the synergy of computational and physical components such as hydraulic, video display, gyros and interoperable devices" (CNSSI 1253 Overlay, 2014). Through live virtualization and distributed training scenarios these emerging CPSs will be coordinated, distributed, and connected and must be robust and responsive. The CPS of tomorrow will need to far exceed the systems of today in capability, scalability, availability, reliability, resiliency, safety, security, and usability. Examples of CPS application areas include live virtual exercises that connect multiple simulators together from around the globe to provide interactive and realistic training. Identification of security requirements for T&S systems is critical to the interoperability of these systems and their ability to realistically train in a robust and distributed virtual reality.

Due to the issues identified above, the U.S. Air Force (AF) implemented an engineering Risk Management Framework (RMF) and established the AF Platform-IT Working Group. This multidiscipline group created a guidebook that addressed Risk Management for Platform IT systems. The DoD has since implemented RMF enterprise wide and should leveraged many lessons learned from AF Platform-IT Working Group as a tool to assist organizations with Platform-IT systems in assessing risk exposure as well as to identify measures for mitigating risk to an acceptable level as early in the acquisition process as possible. It is acknowledged domestically and

internationally that the cyber threat environment is escalating, with targeted attacks having the capability to compromise confidentiality, availability, integrity and non-repudiation of an organization's information. Further, with an estimated 75-92 percent of threats coming from the applications layer, the enemy is already within the fortress (Verizon Vulnerability Assessment, 2010).

PLATFORM-IT RISK MANAGEMENT FRAMEWORK

The DoD RMF is a high-level document that provides a structured and standards-based approach to identifying and assessing risks for owners and operators of Platform IT systems. It is a tailored approach that conforms to the special purpose mission of Platform IT systems and their security and functional requirements, providing guidance as well as advice on how information security risks can be applied and included within an existing framework. The RMF utilizes national standards such as the CNSSI 1253 and NIST 800-53 Risk Management Principles and Guidelines. As such, it is a tool for Senior Executives, Program Managers and CS Managers to determine risk exposures for their systems and networks that they share information to by using a common language and terminology approach (DoDI 8500.01, 2014).

Scope of Platform-IT Risk Management Framework

The RMF provides broad guidance to owners and operators of Platform IT systems for managing the risks that are designed to be adaptable to the need of the different T&S functions. RMF identifies common enterprise level individual risk factors through a verification and validation process that includes continuous monitoring of systems that identify Threat and Risk Assessment processes and outlines a generic 'Risk Assessment Plan for fixing or mitigating identified risks.

Based on RMF guidance program management includes strategies for financial, competitive, strategic, global, reputation, legal and community risks. However, these arrangements sometimes omit other risk categories such as people, management and control measures, information management, communication and computer network connectivity, software, hardware, field devices, and interdependencies, such as simulator and training systems in a Live Virtual or Distributed environment. These systems are also essential to the development of risk mitigation and the ongoing functionality of organizational mission assurance needs and have to be considered as part of the assessment.

Advantage of RMF Approach

The RMF is generic, and as such, is designed to be a useful tool for users and operators of Platform IT systems. The Air Force has used the RMF structure to address Platform IT systems for more than 8 years. The RMF clearly identifies impact, consequences and major stakeholders responsible for common points of failure, whether they are malicious, accidental, natural or environmental to ensure confidentiality, integrity, availability and non-repudiation of Platform IT systems and specialized information they contain and deliver.

These factors must be stated in plain language and in such a way that Boards, CEOs, Senior Executives, Program Managers, technical and operational personnel can agree on the identification of requirements and the documentation, decisions and actions for their Platform IT systems. These are:

- Standards based best practices
- Consistent with governance
- Manage access to the systems and information
- Apply corporate policies and practices
- Technically applicable
- Cost and schedule responsive

T&S PLATFORM IT SYSTEMS SECURITY REQUIREMENTS

Before assessing risk for T&S Platform IT systems, the system and information have to be categorized, baseline security requirements have to be identified and the authorization boundary defined. This implies that need lines are identified or data flow requirements developed, and established controlled interfaces with other Platform IT or non-Platform IT systems, networks and functional requirements are integrated into the baseline security requirements. Each security requirement will be assessed for applicability, implementation, risk assessment and management. Risk management is not a prescriptive solution; rather, it should be used as a tool by Information Systems Security Managers/Engineers, Authorizing Officials, and Senior Agency Information Security Officers to select and agree upon appropriate protections for systems (CNSSI 1253).

Applicability

Once the system and information have been categorized and baseline Security Requirements have been identified, each requirement has to be assessed for applicability to the system and how it can protect the system and information appropriately. Each security requirement has to be evaluated as to its applicability or non-applicability against the systems security posture. The spirit and intent of each controls implementation, the likelihood, and consequences of not applying the control and the level of impact should something happen is assessed. Applying Security Controls for compliance alone can have serious consequences to the T&S platform IT systems functional capabilities as well as mission, cost and schedule impacts of the organization.

T&S PIT systems are among several categories of systems that can be adequately secured without implementation of all the technical features specified for general purpose IT systems. These PIT systems are not "exceptions" or "special cases" where risk is not addressed or waived, because applying technical security requirements to these systems can result in unnecessary costs and operational impacts. In general, the technical questions are "where", "when", and "how" to apply a given set of protection measures, rather than "*whether"* to apply the measures. T&S platform IT systems can mitigate risk by applying strategies such as physical security protections for the system, establishing required access control guidelines and services, proxy servers that isolate data from the Platform IT systems critical functions, and providing information to the users on a need-to-know and need-to-use basis.

Understanding the spirit and intent of security requirements is critical to RMF's applications, especially with T&S PIT systems. During identification of security requirements, a list of applicable and non-applicable requirements should be developed with a brief explanation for non-applicable items as to why the requirement is not applicable to the system. This is addressed in the Plans of Actions and Milestones (POA&M) documentation. It is then up to the AO to accept the Security Control Traceability Matrix and sign off on the POA&M.

Implementation

As soon as applicability for security requirements are established the next step is to look at the system to see if it is compliant with the spirit and intent of controls implementation. Implementation for the T&S system has to address each applicable requirement as well as identify if the requirement has been met appropriately. If the requirement has not been met, what measures are there to implement the requirement? For T&S platform IT systems this is where the RMF is best applied. Sometime implementing a technical requirement can affect functionality of the special-purpose T&S system that has to match operational functionality. Applying a technical requirement which causes systems functionality to fail is counterproductive. RMF allows for this problem to be resolved by identifying mitigations that reduce risk to an acceptable level but support mission assurance requirements. However, occasionally applying a security requirement can technically be implemented, but can be cost and schedule prohibitive. In the Simulators and Training environment implementing a security requirement for compliance sake alone can impose negative cost, schedule and functionality impacts, while applying non-value added security requirements to the system.

When a security requirement cannot be applied either in part or in full because of technical or cost and schedule impacts to the system, T&S organizations should consult all the appropriate stakeholders to identify mitigation strategies that can address and reduce the risk, as well as develop a plan to meet the requirements if possible. Waivers should be the last resort presented to an AO.

RISK ASSESSMENT

Risk Assessment (RA) involves application of technical controls (security requirements) processes and procedures that address shortfalls or findings which could present a vulnerability to systems operational use. For T&S platform IT systems RA will be used to determine a quantitative or qualitative value associated with operational employment of the said system as it relates to a concrete threat or finding. Risk will be addressed by either reducing impact, consequence or likelihood impact for T&S system being evaluated. An acceptable risk to the T&S system is a risk that is understood, addressed, mitigated, or tolerated usually because cost or technical implementation of effective countermeasures for associated vulnerability exceeds the expectation for its loss.

To assist in assessing a T&S systems risk prior to the RMF validation process, the sections below will outline step-by-step implementation flow diagrams that can be used by the T&S program office's in their pursuit for authorization. Utilizing these products and flow diagrams, it is possible to examine findings of an assessment and determine if the findings are applicable. If the findings are applicable, identification of the required steps to address them in order to reduce probability, consequences and impact to the T&S system. For the findings that cannot be technically addressed, program managers should identify what processes and procedures or alternate technical

mitigations can be applied in order to reduce the findings impact to an acceptable level for the Authorizing Official (AO).

Cybersecurity Risk Assessment Process "Start Here"

The First step in this process is to perform a site visit, audit, system assessment, or scan using appropriate tools/processes for the effort. The combined results from this first step will be used to either proceed toward a solution where there are no findings detected or to assess findings and determine their applicability based on system and operational use requirements. If there are "NO FINDINGS" The SCA then validates the findings and the process terminates successfully through steps outlined in process flow A, Figure 2. All findings should be assessed for applicability. If not applicable, document the rationale and annotate on the POA&M and send to SCA for validation as outlined in process flow A, Figure 2.

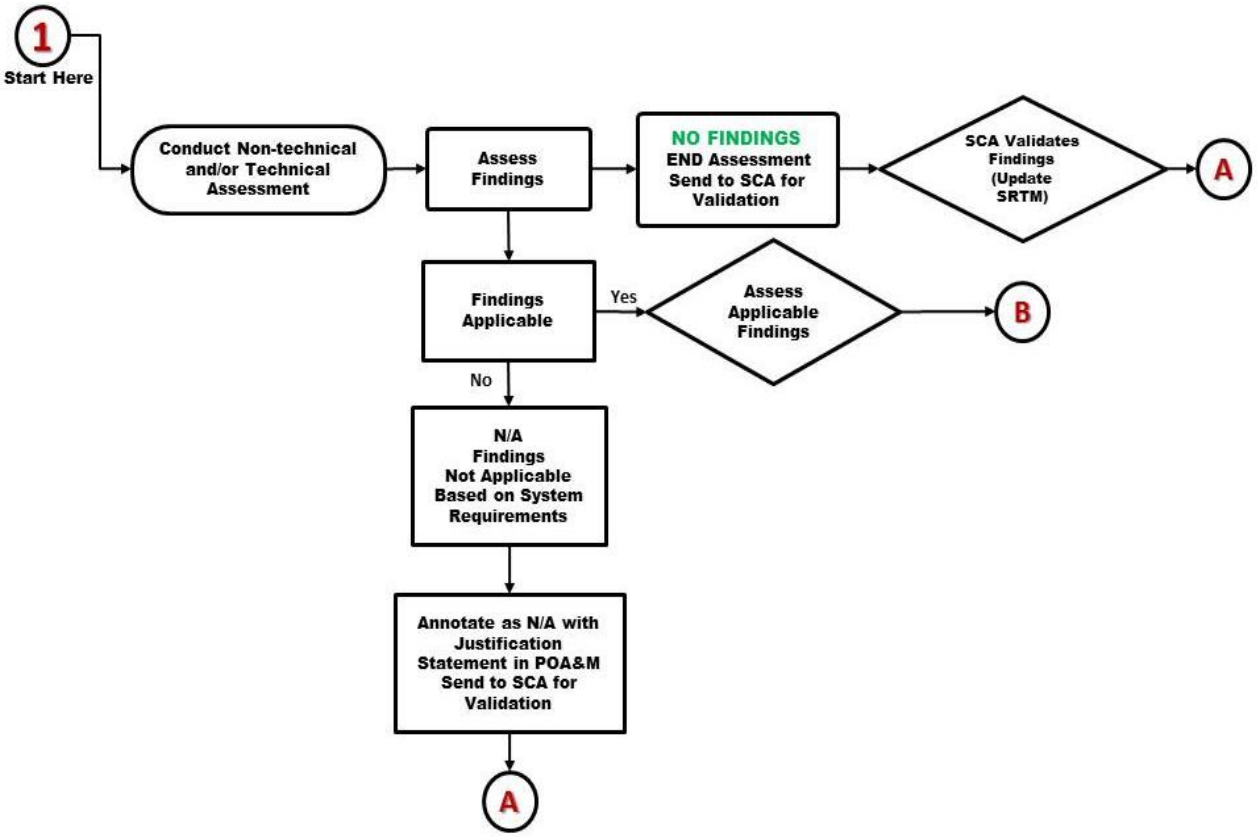

Figure 2: Start Assessment Process

The next step is to evaluate alternative paths to SCA validation where there are findings detected against the T&S system which may either lead back to process flow A (best case scenario) or process flow B which is the most common scenario for standard IS (Non-Platform IT systems).

For example on a standard Aircrew Training System (ATS) where there no requirements for enterprise network connectivity, i.e. it can perform its functional mission (train aircrew) as a stand-alone system. If a system scan detects findings which are applicable to network connected devices, such as unused open ports, remote access, screen lockout, etc., in the context of the ATS they will be "Non Applicable" (N/A), annotated with appropriate justifications in the POA&M and the process will continue through process flow A. If at a future date this requirement changes and network connectivity is now part of the ATS requirements then additional steps in process flow B will be required in order to complete the assessment Figure 4. Network connectivity should be assessed to the interconnection piece only, as either part of the Platform IT or the Network (DoDI 8500.01, 2014).

Process Flow A

When entering process flow A, there are two possible outcomes for the assessment. A solution to the findings is applied and the SCA issues an authorization recommendation based on validation of scan results and additional

mitigation strategies or solutions. Or alternatively, further investigation may be required through either process flow B or C until the SCA recommendations are accepted, Figure 3.

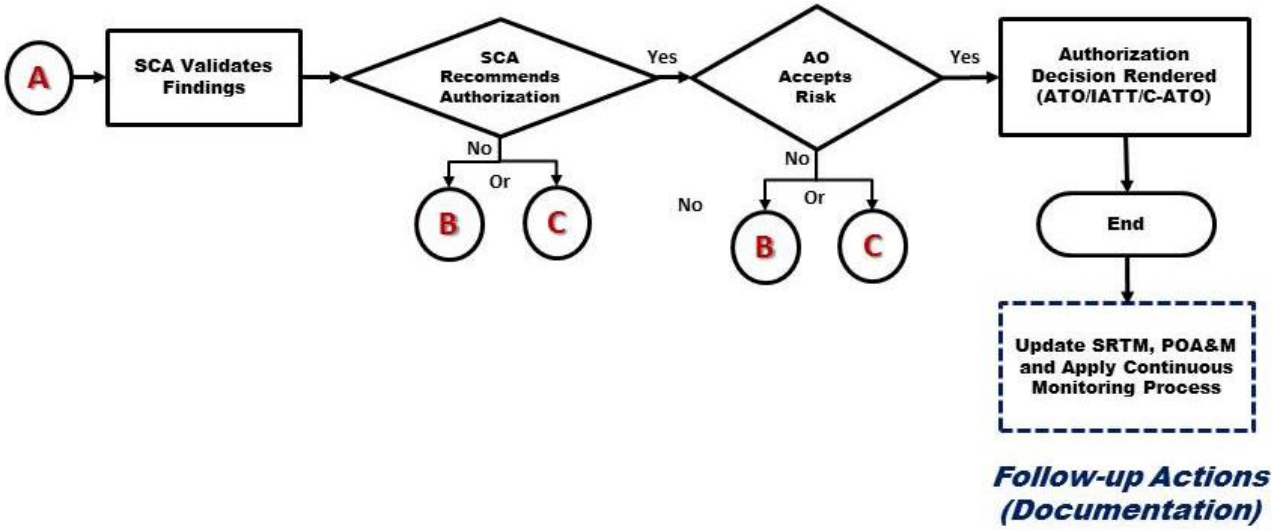

Figure 3: Process Flow A

An example demonstrating this process flow would be during a scan of the T&S system it was identified that the system will not lock a user out after three unsuccessful attempts to log into the system. The use of the screen lockout function for access control is designed to keep unauthorized personnel from accessing a system and its information. For enterprise connected systems not implementing this control is considered a Category I vulnerability or "High" risk if not applied to the systems operational environment. However, applying this security requirement to a system like an ATS could cause loss of a training event. Locking the aircrew out of their system has negative mission impact, and is a non-value added security control. Alternative mitigation strategies to prevent unauthorized access at the position could include applying group access controls based on discretionary and/or role based access, as well as processes and procedures which physically restrict access to an ATS system such as guards, gates, guns and dogs. This type of mitigation approach can reduce risk significantly when technical controls cannot be applied.

Process Flow B

Process flow B has two possible outcomes, either there are technical controls such as Security Technical Implementation Guides (STIGs) available to fix or mitigate risks or compensating controls and mitigation strategies

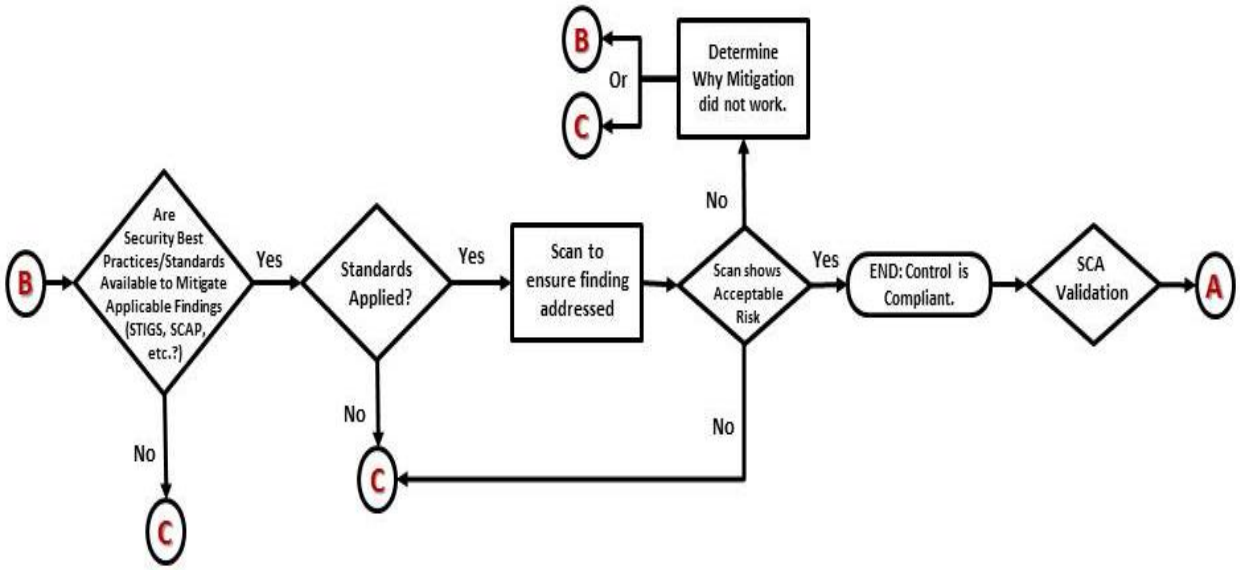

Figure 4: Process Flow B

when technical controls are not suitable, or sufficient. In this case these findings will result in resolution of identified

risk at which point the next step is to validate the applied STIGs, address the findings, and go back to Process Flow A completing the assessment. Alternatively if there technical controls suitable or sufficient to address the findings then process flow B continues to process flow C, in order to develop alternative approaches for risk mitigation and resolution Figure 4.

Process Flow C

Process flow C is perhaps the most common flow because T&S systems do not fall perfectly under standard IT systems or aircraft operational flight safety software controls. Thus there are many scenarios in which there are no applicable technical solutions (i.e. STIGs) available to draw support from. Unlike other process flows there are several possible exit scenarios for this flow. Based on the level of risk reduction applied by risk mitigation approach there are three possible options to enter process flow D. This depends on risk/impact levels reductions to Moderate, Low or High (not Reduced). In all of the identified cases it is not possible to go directly to process flow A for completion of the assessment as that process flow requires a much lower level of assessment in order for an SCA recommendation to be acceptable Figure 4. In all cases the risk is annotated in the POA&M.

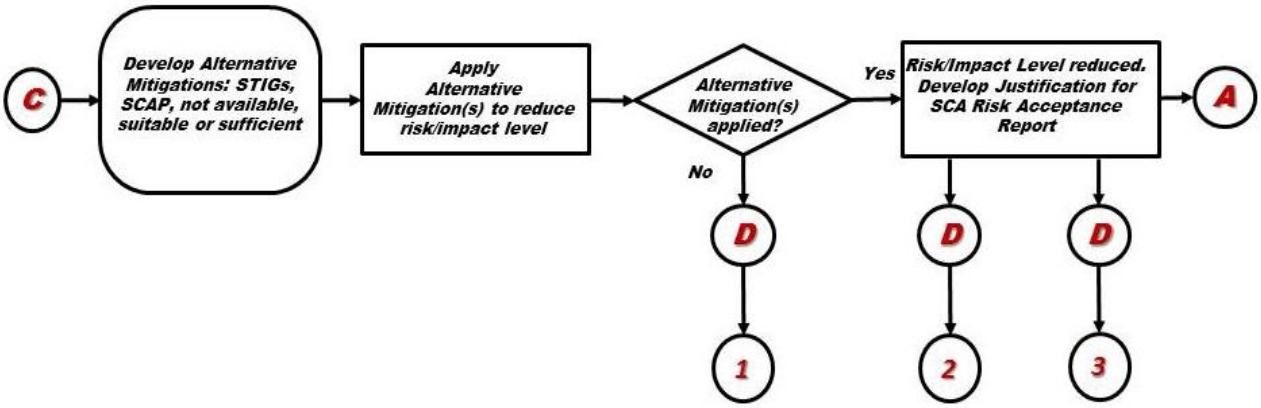

Figure 5: Process Flow C

For example during a scan a potential Category 1 security risk was found. The Operating System (OS) has reached end-of-life and is no longer supported. This is a known detected risk for network connected systems and there is guidance which directs programs to migrate to a newer supported OS within a 2-year timeframe. However, embedded IT for T&S systems usually have contractual support agreements built into their contract beyond that of the general desktop licenses. In most cases these systems are supported until the contract expires. Because T&S systems are Platform IT and operate as a standalone, non-network devices, loss of enterprise or network security patch support from Microsoft does not create or pose a high risk to the system. Furthermore upgrading outside of normal technology refreshment cycle to a new operating system adds no value compared to the negative impact to a T&S systems operational functionality, cost and schedule. The process flow takes us to making a recommendation to the accept the lower risk, and revisit findings at a future date to determine appropriate strategies to technologically refresh the system as part of its Lifecycle Management Process (LCMP).

If the findings, on the other hand, are adequately addressed then the next step is to go process flow A, which finalizes results and grants an Authority to Operate (ATO). However, if application of the control does not resolve the issue, then the process flow C takes us through the mitigation process to identify suitable alternatives to upgrade and address the findings through process flow D,1,2,or 3.

Process Flow D

This process flow resolves impacts from previous process flow C to develop justifications for unmitigated risks as to why they should be accepted by the AO. Process flow D provides risk acceptance justifications for risk/impacts that are reduced to Low or Moderate impacts which will lead to either ATO or a Conditional ATO (C-ATO) for T&S systems which may not be able to resolve identified risk, but are operationally essential to the Training Mission. In such cases the outlined process flow will support the authorization decision to accept the risk if use of the system justifies risk to its operation as presented. Output of this process flow will to go to process flow A for assessment despite known risks Figure 6.

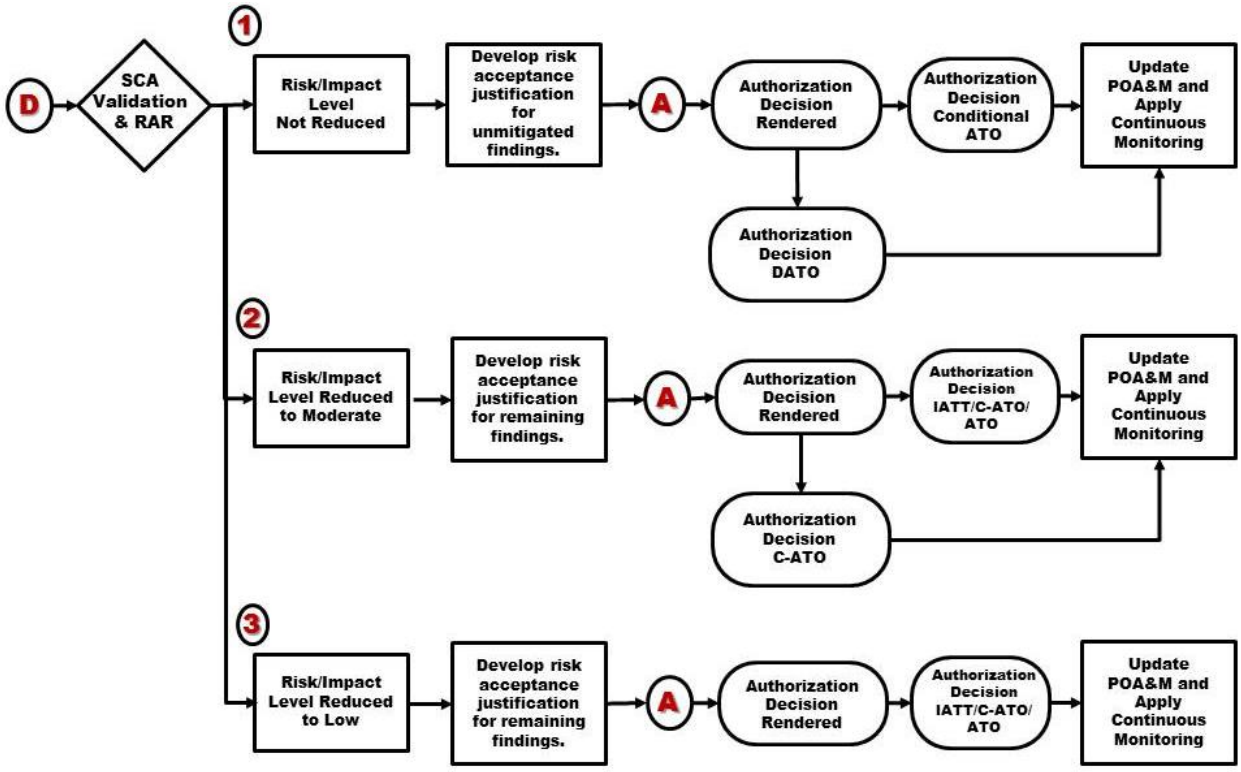

Figure 6: Process Flow D

An example of this would be when a T&S systems OS is setup in administrator mode for all users. However, this implementation does not comply with current requirements to implement Common Access Card (CAC) on the OS for access and logon. Implementing said capability will impose negative training impacts and adversely affect how the system is operated in the field. Thus, STIGs mandating CAC are not suitable or applicable to the system as fielded. As a result during assessment alternative mitigation strategies to reduce risk/impact levels have to be considered. One approach is to establish system user groups such as pilots, sensor operators, and administrators to control access and to implement strict DoD password requirements. However, this approach would negatively impact training as well, because this is not how the system operated and deployed in the field. Thus, due to operational use of the system device other controls have to be considered such as controlled access, additional processes to access T&S system or technical solutions such as biometrics have to be evaluated to reduce risk to lowest level possible. In this example; risk can be mitigated to either Low or Moderate with processes for accessing said devices through non-technical means or it can be considered not reduced if additional controls implemented to secure the system negatively affect its functionality.

SUMMARY

Providing Simulator and Training stakeholders with a practical tool to manage risk and CS is critical to balancing mission assurance and cybersecurity requirements. As T&S systems are becoming more interconnected through DMO or Live Virtual Simulation constructs to conduct interactive training missions and exercises, the potential impacts of CS to the T&S community will continue to grow. Implementing RMF to identify and manage CS risk requirements at all phases of development, from cradle to grave, will significantly reduce overall impact to the T&S system and system security. It is also important to note that systems risk management is a strategic element of simulation and training which impacts operational mission and is a living process.

The approach outlined in this paper and the implementation of appropriate governance with regulatory compliance requires that T&S organizations use a top-down, bottom-up approach which addresses issues that can mitigate or resolve risks to the lowest level possible. However, this requires organizations to not only address functionality of T&S systems, but also CS requirements of these systems as early as possible in order to support mission assurance. Addressing issues early on will provide extended cost and schedule savings. Applying risk management rather than compliance management allows organizations to identify CS requirements, assess their applicability, compliance,

technical and security mitigations and implements a plan of action to manage and continuously monitor platform IT systems. In this paper a practical process flow was presented that can be used for RMF assessment on T&S systems which can greatly improve how risk is being evaluated as well as provide a practical tool for addressing issues.

REFERENCES

AFI 33-210, AFGM3. (March 2014). *Air Force Guidance Memorandum immediately changing AFI 33-210, (AFCAP) providing updated guidance on Platform Information Technology (PIT) requirements…*

Committee on National Security Systems Policy 11. (June 2013). *National Policy Governing the Acquisition of Information Assurance (IA) and IA-Enabled Information Technology Products.* As amended

Committee on National Security Systems Instruction 1253. (March 15, 2012). *Security Categorization and Control Selection for National Security Systems.*

Committee on National Security Systems Policy 15. (October 1, 2012). *National Information Assurance Policy on the Use of Public Standards for the Secure Sharing of Information Among National Security Systems*.

DBIR. (2010). *2010 Verizon Data Breach Investigation Report (DBIR)*. Retrieved May 29, 2014, from http://verizon.com/enterprise/securityblog

DoD Instruction 8500.01. (14 Mar 2014). *Cybersecurity.*

DoD Instruction 8510.01. (12 Mar 2014). *Risk Management Framework (RMF) for DoD Information Technology.*

DoD Instruction 8520.02. (May 24, 2011). *Public Key Infrastructure (PKI) and Public Key (PK) Enabling.* Interim

DoD Instruction 5000.02. (November 25, 2013). *Operation of the Defense Acquisition System*.

National Institute of Standards and Technology Special Publication 800-30. (2014). *Guide for Conducting Risk Assessments.*

National Institute of Standards and Technology Special Publication 800-34. (2014). *Contingency Planning Guide for Federal Information Systems*. Revision 1.

National Institute of Standards and Technology Special Publication 800-37. (2014). *Guide for Applying the Risk Management Framework to Federal Information Systems.*

National Institute of Standards and Technology Special Publication 800-53. (2014). *Recommended Security Controls for Federal Information Systems and Organizations.*

National Institute of Standards and Technology Special Publication 800-53A. (2014). *Guide for Assessing the Security Controls in Federal Information Systems.*