MAVEN Information Security Governance, Risk Management, and Compliance (GRC): Lessons Learned

Eduardo Takamura, Carlos Gomez-Rosa, Kevin Mangum, Fran Wasiak
NASA/Goddard Space Flight Center
Greenbelt, MD USA

Abstract—**As the first interplanetary mission managed by the NASA Goddard Space Flight Center, the Mars Atmosphere and Volatile EvolutioN (MAVEN) had three IT security goals for its ground system: COMPLIANCE, (IT) RISK REDUCTION, and COST REDUCTION. In a multi-organizational environment in which government, industry and academia work together in support of the ground system and mission operations, information security governance, risk management, and compliance (GRC) becomes a challenge as each component of the ground system has and follows its own set of IT security requirements. These requirements are not necessarily the same or even similar to each other's, making the auditing of the ground system security a challenging feat. A combination of standards-based information security management based on the National Institute of Standards and Technology (NIST) Risk Management Framework (RMF), due diligence by the Mission's leadership, and effective collaboration among all elements of the ground system enabled MAVEN to successfully meet NASA's requirements for IT security, and therefore meet Federal Information Security Management Act (FISMA) mandate on the Agency. Throughout the implementation of GRC on MAVEN during the early stages of the mission development, the Project faced many challenges some of which have been identified in this paper. The purpose of this paper is to document these challenges, and provide a brief analysis of the lessons MAVEN learned. The historical information documented herein, derived from an internal pre-launch lessons learned analysis, can be used by current and future missions and organizations implementing and auditing GRC.**

Keywords—IT security, information security, information security management, cyber security, FISMA, risk, risk management, compliance, regulations, governance, GRC

TABLE OF CONTENTS

This paper was sponsored by NASA's Mars Atmosphere and Volatile EvolutioN (MAVEN) Project based at Goddard Space Flight Center in Greenbelt, MD.

1. INTRODUCTION

One of the main drivers for deploying Information Technology (IT) products and services within an organization is to automate business processes. Whether information technology is used to process and store vast amounts of data, to facilitate the exchange of information internally and externally, or to contribute to one's knowledge, IT enables the business. Ground systems rely on information systems to support mission operations. Mission Operation Centers (MOCs) and Mission Support Areas (MSAs) are equipped with systems (hardware and software) and networks that assist in spacecraft command and control; data processing and storage; science and engineering data analysis; etc. Regardless of the cost of the mission, these information systems must provide assurance that the confidentiality, integrity and availability of the mission's information are protected. Governing laws and regulations exist to ensure this protection is applied to federal information systems such as those supporting NASA missions. NASA's Mars Atmosphere and Volatile EvolutioN (MAVEN) mission successfully met information system security mandates, although not without encountering certain challenges along the way. Some of these challenges along with identified root causes, potential impact if not addressed, and resulting mitigating strategies are documented in this paper. The intent is to share some of the lessons learned from this compliance-seeking journey with individuals and organizations responsible for implementing similar or identical GRC strategies. While each mission/organization is unique, some of the challenges they face are commonplace, especially as budgets are trimmed down, and how information technology (IT) and information security (IS) are, unfortunately, often seen as both expensive and expendable. By considering some of the lessons from MAVEN's implementation and auditing of information security governance, risk management, and compliance, individuals and organizations in like environments could potentially prevent similar barriers towards meeting their GRC goals.

2. FEDERAL INFORMATION SYSTEM SECURITY MANAGEMENT AND SUPPORT

Every U.S. federal government agency, whether civilian or military, is required to meet the minimum information security requirements established by the Office of

Management and Budget (OMB) in Circular A-130, Appendix III, *Security of Federal Automated Information Resources* [1]. Agencies like NASA are required by the Federal Information Security Management Act (FISMA) to effectively manage IT security risks following guidelines set by the National Institute of Standards and Technology (NIST). While the model for managing risks is deemed by many to be outdated and ineffective, it is still the current federal government methodology for securing and managing the security of its information systems[1]. The basis of this methodology is the NIST Risk Management Framework (RMF) [2] designed to help federal agencies and organizations implement a security program focusing on technical, operational and management security controls. Together, these controls form layers of security protecting the information system.

NASA information systems – including mission operations and contractor-operated systems – must be protected to ensure the confidentiality, integrity and availability of data and resources. By implementing and auditing governance, risk management, and compliance (GRC) on MAVEN's ground systems, the Project ensured that the above requirement for protecting NASA information systems is met. NIST defines governance as "the set of responsibilities and practices exercised by those responsible for an organization (e.g., the board of directors and executive management in a corporation, the head of a federal agency) with the express goal of: (i) providing strategic direction; (ii) ensuring that the organizational mission and business objectives are achieved; (iii) ascertaining that risks are managed appropriately; and (iv) verifying that the organization's resources are used responsibly. [3]" Information security governance, specifically, is 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 alignment of responsibility, all in an effort to manage risk. [4]" This risk pertains to information security risks due to vulnerability/exposures in IT systems (hardware and software) with the potential to incur risks to other areas such as project schedule and cost. Risk management, on the other hand, is "a comprehensive process that requires organizations to: (i) frame risk (i.e., establish the context for risk-based decisions); (ii) assess risk; (iii) respond to risk once determined; and (iv) monitor risk on an ongoing basis using effective organizational communications and a feedback loop for continuous improvement in the risk-related activities of organizations.[5]" The Merriam-Webster dictionary defines compliance as "conformity in fulfilling official requirements. [6]" MAVEN's official requirement for IT security was simple: To meet NASA's requirements for IT security. The verification of this level 3 requirement was based on a successful Assessment and Authorization (A&A)[2] of the ground system.

This paper covers mission ground systems supporting mission operations. Administrative and development systems, Supervisory Control And Data Acquisition (SCADA) systems, infrastructure elements, and non-mission information systems are outside of the scope of the Mission's IT security efforts, and therefore outside of the scope of this paper. The terms Information Security (IS) and Information Technology (IT) Security are used interchangeably throughout this paper.

The information specific to MAVEN presented here has been reviewed and approved for public release by the MAVEN Information System Owner (ISO) and Information System Security Official (ISSO). Finally, there is no Controlled Unclassified Information (CUI), no Sensitive But Unclassified (SBU) information, no export controlled information per the International Traffic in Arms Regulations (ITAR), or any information in this paper that could potentially put the Mission at risk.

3. MISSION OVERVIEW

The Mars Atmosphere and Volatile EvolutioN (MAVEN) mission is the first interplanetary mission managed by NASA's Goddard Space Flight Center (GSFC)[3], home of the "largest organization[4] of scientists and engineers dedicated to learning and sharing their knowledge of Earth, the Sun, the solar systems, and the universe. [7]" Goddard is also providing two of the science instruments onboard the Lockheed Martin-built spacecraft. "MAVEN will be the first spacecraft mission dedicated to exploring the upper atmosphere of Mars. [It] will study the nature of the red planet's upper atmosphere, how solar activity contributes to atmospheric loss, and the role that escape of gas from the atmosphere to space has played through time." This Mars Scout Program mission is led by Principal Investigator (PI) Dr. Bruce Jakosky from the University of Colorado which, in addition to building some of the instruments, is responsible for the science operations as well as for the education and public outreach (EPO). Management of the program is performed by the Jet Propulsion Laboratory[5] which also provides data relay communications, navigation support, and Deep Space Network operations. [8] The

[1] At the time of writing of this paper.

[2] NASA's equivalent to the FISMA Certification and Accreditation (C&A) process.

[3] Under the Planetary Science Projects Division (Code 430) of the Flight Projects Directorate (Code 400).

[4] In the United States.

[5] Under the Mars Exploration Program.

University of California at Berkeley (UCB) will provide management for the Particles and Fields (P&F) Package, and will provide various instruments and components.

IT Security Management and Support Approach

The management and support of MAVEN information security was a joint collaboration between the Project Information System Owner (ISO) and the Project Information System Security Official (ISSO), assisted by IT security support personnel. The Mission Operations and Ground System Manager took on and held the role and responsibilities of the ISO, while the ISSO role and responsibility was taken and held by a GSFC Flight Projects Directorate (FPD) IT/IS Manager whose primary responsibility was to advise the ISO on all matters related to IT security. In addition to the ISO, ISSO and IT security support teams, the following actors were also identified: FPD Subordinate System Officials (IT Manager, FPD ISSO, FPD IT security support personnel), Authorizing Official (AO), Center (GSFC) Chief Information Security Officer (CISO), among other officials.

Once the IT security leadership was established, three IT security goals were defined for the MAVEN project as identified in table 1: COMPLIANCE, (IT) RISK REDUCTION, and COST REDUCTION.

Table 1 MAVEN Goals for IT Security

COMPLIANCE	• Support the planning and implementation of the NIST Risk Management Framework (RMF) (per NIST Special Publication (SP) 800-37), and assessing the implementation of the NIST SP 800-53 security controls. • Document existing compliance status, and where each element is in the security life cycle (system categorization – security control selection – control implementation – control assessment – authorization – monitoring). • Track compliance and non-compliance.
(IT) RISK REDUCTION	• Establish communication channel(s) between MAVEN Project Management Office (PMO) (via the ISSO) and the sites/facilities (IT security points of contact (POCs)). • Compile and analyze MAVEN project IT security status reports including security metrics. • Continuously monitor risks to the ground system.
COST REDUCTION	• Create an IT Security Working Group comprising of IT security representatives from and knowledgeable about each MAVEN ground system element who can be Goddard MAVEN PMO points of contact for faster knowledge sharing & incident response. • Use NASA-adopted standards and NASA-approved templates instead of developing new ones from the ground up.

MAVEN's level 3 requirement for data security stated that the "MOS/GDS[6] shall ensure the security of its data management system per NASA security document (NPR 2810.1, latest revision)." NASA Procedural Requirement (NPR) 2810.1, *Security of Information Technology*, is NASA's implementation of the NIST RMF, and contains references to individual, theme-specific IT security handbooks (ITS-HBKs) containing NASA-defined values to guide in the implementation of the security controls per NIST SP 800-53, *Recommended Security Controls for Federal Information Systems and Organizations*. The following approach for meeting this requirement was established for the ground system (covering all of its elements):

- Determine NPR 2810.1A & NIST SP 800-53 compliance across all elements.
- Identify and document existing security control implementation.
- Establish and maintain security baselines.

[6] Mission Operations System/Ground Data System.

- Develop and track Plan of Actions and Milestones (POA&Ms) for mitigating or accepting risks.

In addition to the above goals, level 3 requirement, and approach, MAVEN set itself the following objective: To attain an Authorization To Operate (ATO) from NASA by at least 6 months prior to launch.[7]

For each of the identified ground system element, an IT security point of contact (POC) was designated to participate in and support the MAVEN IT Security Working Group (ITSWG). The ITSWG, in collaboration with the Network Connectivity Working Group (NCWG), identified ground system boundaries based on networks, interconnections, jurisdictions, and other considerations. Knowing the boundaries of the system was one of the first steps in the inventorying of information pertaining to IT security processes (e.g., security assessments), procedures (e.g., incident response, contingency planning), and products (e.g., system security plans (SSPs)).

The bulk of the initial IT security work focused on such inventorying. Every ground system element had to be covered by a security plan. MAVEN IT Security took into account existing signed and current ATOs and SSPs from the various ground system elements. Based on existing documentation, and through ITSWG bi-weekly meetings, interviews, and other means of communication, specific security control implementation was inventoried. The objective of this initial gathering of security control implementation information, based on NIST SP 800-53 security controls, was to re-define requirements, if needed, after performing gap and risk analysis over the implementation by each element. Partial or non-implementation of security controls may constitute an increase of risk to the overall ground system. The gap and risk analysis of the collected information was an important step in identifying deviations from the Agency requirements documented in NPR 2810.1A. From this analysis, a risk rating of low, moderate or high risk was obtained according to impact (to the element/ground system) vs. the likelihood of the risk.

4. CHALLENGES, ROOT CAUSES & CONSEQUENCES, RESOLUTIONS, OPPORTUNITIES FOR IMPROVEMENT

Late Start

One of the most important IT security lessons that the Project learned regarding the implementation and auditing of GRC on MAVEN pertains to requirements. The project instituted its IT security requirements following its Preliminary Design Review (PDR), and as such, put the IT security management and support (ITSM&S) work one major project milestone behind. Between PDR (NOV 2010) and the critical design Engineering Peer Review (EPR) (SEP 2011), the Project defined a level 3 (L3) requirement for IT security; developed an approach for managing and supporting IT security based on NPR 2810.1A; and began executing its IT security management plan for the ground system.

Whether a Project starts late, on-time, or has a head-start in its security work, the GRC implementation and auditing methodology can greatly influence the outcome of the security work. Another important factor that can contribute to a successful GRC implementation is having the right management and support personnel to champion and carry on the IT security work. MAVEN's System Owner had a gradual, cumulative knowledge of GRC from a previous and related role in support of another federal government organization. IT security-knowledgeable MAVEN project managers were also involved in and supportive of the GRC implementation work.

Using a divide-and-conquer approach, the Project established an IT Security Working Group (ITSWG) comprised of IT security representatives from each element of the ground system working together with the MAVEN Information System Security Official (ISSO) and Information System Security Engineer (ISSE) on GRC activities. Championed by the MAVEN Information System Owner (ISO), the collaborative work by the ITSWG resulted in a clearer understanding of the ground system boundary; in the identification of system security plans, and in knowledge regarding the implementation of security controls across the ground system.

Although this approach – coupled with experienced ITSM&S personnel – promoted an accelerated schedule of IT security activities, the Project still received a Request For Action (RFA) at its Critical Design Review (JAN 2012) as a consequence of being one major project milestone behind. The RFA was successfully closed, and all IT security activities fully caught up with planned schedule by the Project's Mission Operations Review (MOR) (NOV 2012).

In theory, IT security considerations should be given throughout the mission phases with special emphasis on the initial design and development phases. The earlier the considerations are given, the higher the probability of a successful security control implementation.

[7] Launch window for MAVEN: November 18, 2013 until December 7, 2013.

Multi-Organizational Architecture in Heterogeneous Environment

MAVEN, like most NASA missions, taps the knowledge and expertise of not only its government civil servants and support contractors, but also of its industry and academia partners who play key roles in mission and science operations. While this "inter-industry" collaboration is welcomed, encouraged and beneficial to all, each "industry" has and follows its own set of security requirements; has different levels of risk tolerance; and – as a result – exerts disparate, culturally-driven IT security practices. Because of the heterogeneous nature of the overall project organization, this disparity posed challenges to the implementation and auditing of security controls across the ground system.

Even within a particular "industry" such as the federal government, there are many departmental silos with their own set of requirements (standards, processes, etc.) that may not fit in another department's security practices. In the case of NASA, as an agency, a superset of IT security requirements exist, but meeting such requirements by its field centers, by the directorates (divisions) within the centers, and by the projects within the directorates can differ substantially. Also, NASA's procedural requirements for information security are only applicable to contractors and external entities to the extent of what is established within their respective contracts.

Early in the initial/development phase of the MAVEN ground system, the assumption was that all security boundaries would abide to this Agency superset of information security requirements; however, that was not the case. On the MAVEN ground system, each component (or element) fell under either GSFC, JPL[8] or other institutional IT security purview. While logistically this organization helped the (project) management of specific ground system components, the distinct security baselines applied to each security boundary required additional risk reviews to ensure that the standards and processes implemented in one jurisdiction did not open up new risks on another jurisdiction. That was the case of the MAVEN MSA[9] being under the purview of JPL IT Security while the MAVEN Backup MSA (bMSA)[10] was under GSFC's responsibility. Both had distinct IT security requirements to meet, but both required similar configuration settings due to their relationship with one another (the bMSA is the MSA's alternate command and monitoring site during the critical Mars Orbit Insertion (MOI) event). While the bMSA information systems met NASA's requirements, it was unknown whether the MSA did. The MSA is a critical component of the ground system: It is responsible for MAVEN's mission operations; thus, the MAVEN ISO commissioned an internal risk assessment of the MSA by the Mission's internal IT security team to verify that appropriate security controls were in place to protect MAVEN's command and control (C&C) center. In addition to the extra risk assessment to ensure the security implementation would satisfy the minimum requirements or, if not, if risks could be accepted, agreements between two security boundary officials were documented in the form of an Interconnection Security Agreement (ISA) which outlined how each boundary protected Mission data both locally and cross boundaries. ISAs were developed for all external security boundaries exchanging Mission data with internal NASA systems.

Even though security requirements differed across the ground system, the MAVEN project managed its overall IT risks by identifying them, and taking actions to ensure that the ground system is protected regardless of which security standard and requirement were being followed by a particular ground system element. The focus was on the criticality of the component with regard to its role within the ground system, as well as on securing loose ends (the weakest links).

Current and newer missions should decide whether or not to require all of its components including external entities to follow the Agency's superset requirements. The pros and cons of such directive is outside of the scope of this paper, but should the mission decide to enforce, for instance, the Agency's requirements and implementation methodology, the decision must be authoritative across the entire ground system. Projects should also engage their Contracting Officers (COs) to validate applicability of IT security requirements against all contracts[11].

Institutional Culture Clash

An experienced workforce is one of the greatest assets of a mission. Most NASA missions utilize support personnel who have worked together on previous projects, and so it is not uncommon to find people or teams collaborating on multiple missions, past and present. This "re-use" of personnel allows for continued team dynamics, but at the same time contributes to the perpetuation of a set of cultural baggage carried on by each team. While this baggage can bring positive results to the project, it can also impact the understanding and adaptability to project-wide requirements, especially new or even slightly distinct

[8] Jet Propulsion Laboratory in Pasadena, CA, operated by CalTech.

[9] Located at the Lockheed Martin facility in Littleton, CO.

[10] Located at Goddard Space Flight Center in Greenbelt, MD.

[11] For instance, enforcing IT security requirements as defined by Federal Acquisition Regulation (FAR) clause 1852.204-76.

requirements pertaining to information security that perhaps have not been addressed before by the teams.

On MAVEN, this culture clash was visible between GSFC-managed elements and JPL-managed elements. Multiple standards, conventions, processes, etc. can be a challenge, specifically to auditors who must understand both sets of requirements to figure out if residual risks exist on either jurisdictions. MAVEN handled this issue by finding a common ground between system boundaries managed by different organizations. For instance, while JPL does not follow NASA's implementation of FISMA (through NPR 2810.1A), it has in fact adopted the NIST Risk Management Framework (RMF) which NPR 2810.1A is based on.
An element cannot impose changes to or deviations from existing information security policies and procedures of another element, but the Mission can establish a project-wide information security "standard," "convention," etc. that is applicable to most and preferably all elements. The challenge is obtaining buy-in from all stakeholders to ensure that any project-wide directive is applicable to most if not all elements, and that it is flexible enough to be molded or adapted by each element. Very rarely does a one-size-fits-all approach succeed in standardizing security implementation practices, and projects must take into consideration that change often brings resistance from stakeholders. Being aware of possible culture clash between stakeholders, carefully managing stakeholder expectations, and early conflict identification and resolution are advised.

A culture clash should not be confused with a stakeholder agenda. ISOs must be aware, understand, accept and exercise his/her roles and responsibilities per NASA policy in order to ensure that this clash of cultures does not negatively impact the (IT security) work of the mission. ISOs must be empowered to make preemptive risk mitigation/acceptance decisions on behalf of the Authorizing Official (AO) in order to reduce risks.[12] The MAVEN ISO and the MAVEN project leadership in general focused on managing (IT) risks to the overall ground system rather than on the different elements forming the ground system. It is true that such cultural differences can negatively impact the (IT security) work if unacceptable behavior from any party leads to additional risks, especially those related to the non-compliance of information security regulations. Failure to comply with such regulations can result in risks not only to the project but also to other projects as well as to the entire Agency depending on what is being protected. In the end, it is the AO who is ultimately responsible for the risks of the project, but the ISO must be proactive in ensuring that the ground system (IT) risks are documented and tracked, mitigated or accepted (by the Authorizing Official), and partially mitigated with compensating controls whenever feasible if the risks cannot be mitigated.

Applicability of IT Security Requirements

Knowing to whom the information security requirements are applicable is as important as defining the actual requirements themselves. Overall, information security requirements define how information and information technology resources must be protected. If a given requirement is not applicable to a ground system element, for instance, then how are resources protected within that element? The security posture of the mission cannot be assessed if the security posture of one or more component is unknown. If the requirement for information security on one or more component is non-existent, then the security implementation cannot be audited because if there is no requirement, there is no compliance "obligation" on the part of the component. The System Owner must ensure that whichever requirement is applicable to this element, that the requirement is defined and meets or exceeds the Project's overall requirement. If the requirement is unknown to the project leadership, then a closer look at how the element has met the requirement(s) can enable the project to analyze the risk level at the element.

The Goddard MAVEN PMO had no initial visibility into the documented JPL IT security requirements covering the MSA and other components. The previously mentioned internal security assessment of the MSA element provided the MAVEN PMO with the necessary visibility to the security posture of the JPL-managed component. From this point on, the Project engaged in the risk management process for documenting, mitigating and tracking risks at the MSA.

Although JPL IT security requirements were not disclosed to the MAVEN PMO prior to MAVEN's internal security assessment of the MSA, it is important to note that the JPL IT security team collaborated with the MAVEN IT security team, and provided excellent support before, during and after the internal security assessment of the MSA. There was one work product in particular that greatly helped with the analysis of the JPL security control implementation: An internal JPL document mapping the JPL security control implementation to the NIST security controls as documented in NIST SP 800-53 [9]. This delta document helped translate JPL's security control implementation into a workable checklist that could be used against NASA's implementation of the NIST security controls. This reference document provided by JPL facilitated the translation of the requirements by looking at the actual implementation details rather than at the requirement itself. The use of standards can be a common denominator when different requirements are in place.

[12] Note: AOs will ultimately make the decision for the organization.

Systems Engineering Approach vs. IT Security Management Approach

The management of federal information system security is based on a specific risk management approach. This approach is similar to risk management processes in systems engineering & project management, but it is not the same. The unfamiliarity of federal information security management processes by certain stakeholders including decision makers across the ground system became a challenge not only to the implementation aspect of GRC, but also to GRC auditing. Similar to the institutional culture clash, each group brings their knowledge and experience to the project. Because of the risk management similarities between system engineering/project management and "the FISMA way" of conducting risk management, some of the expectations were obfuscated, especially with regard to requirements verification.

The six phases or steps of the NIST Risk Management Framework security life cycle are shown in Figure 1:

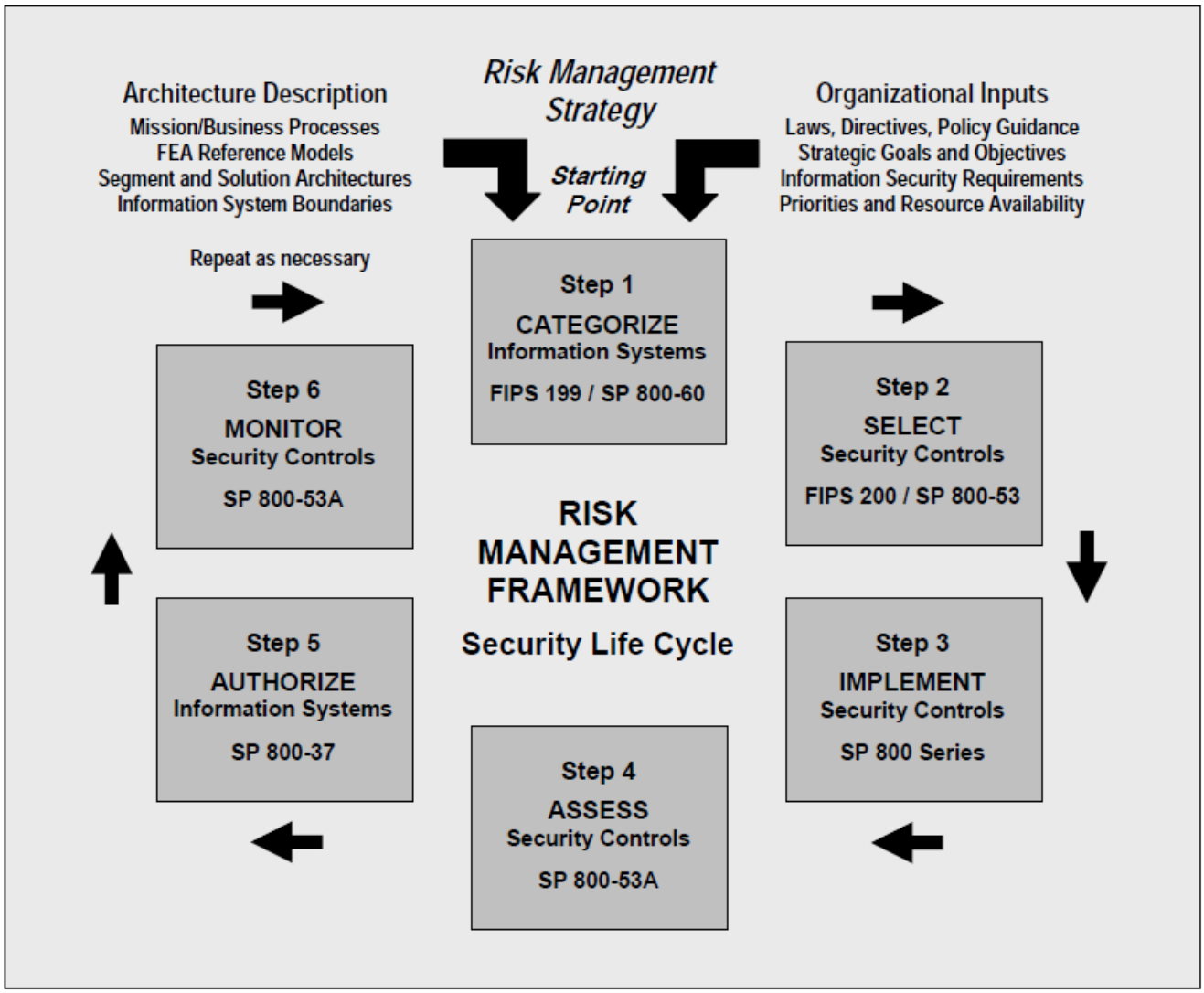

Figure 1 NIST RMF Security Life Cycle [10]

The numbers under each step title (e.g., FIPS 199 / SP 800-60) correspond to the applicable NIST guidance publication. The publications are available for download from the Computer Security Resource Center of the NIST Computer Security Division.[13]

[13] http://csrc.nist.gov/publications/

Figure 2 depicts the same phases or steps in terms of processes with inputs and outputs. This alternate representation of the RMF provides another view of the security life cycle that could facilitate its understanding from an engineering perspective. With the exception of the first and last steps, the output of one process is the input of the next process. This means that each step depends on the successful completion of the previous step.

For MAVEN, because most of its ground system elements had already selected and implemented security controls (steps 2 and 3), the Project performed a security categorization (step 1) as part of its requirements definition, and then focused on steps 4 (security control assessment) and 5 (information system authorization) to verify that the requirements were being satisfied. If a gap analysis showed the need for implementing additional controls and/or control enhancements, then steps 2 (selection of security controls) and 3 (implementation of security controls) were repeated.

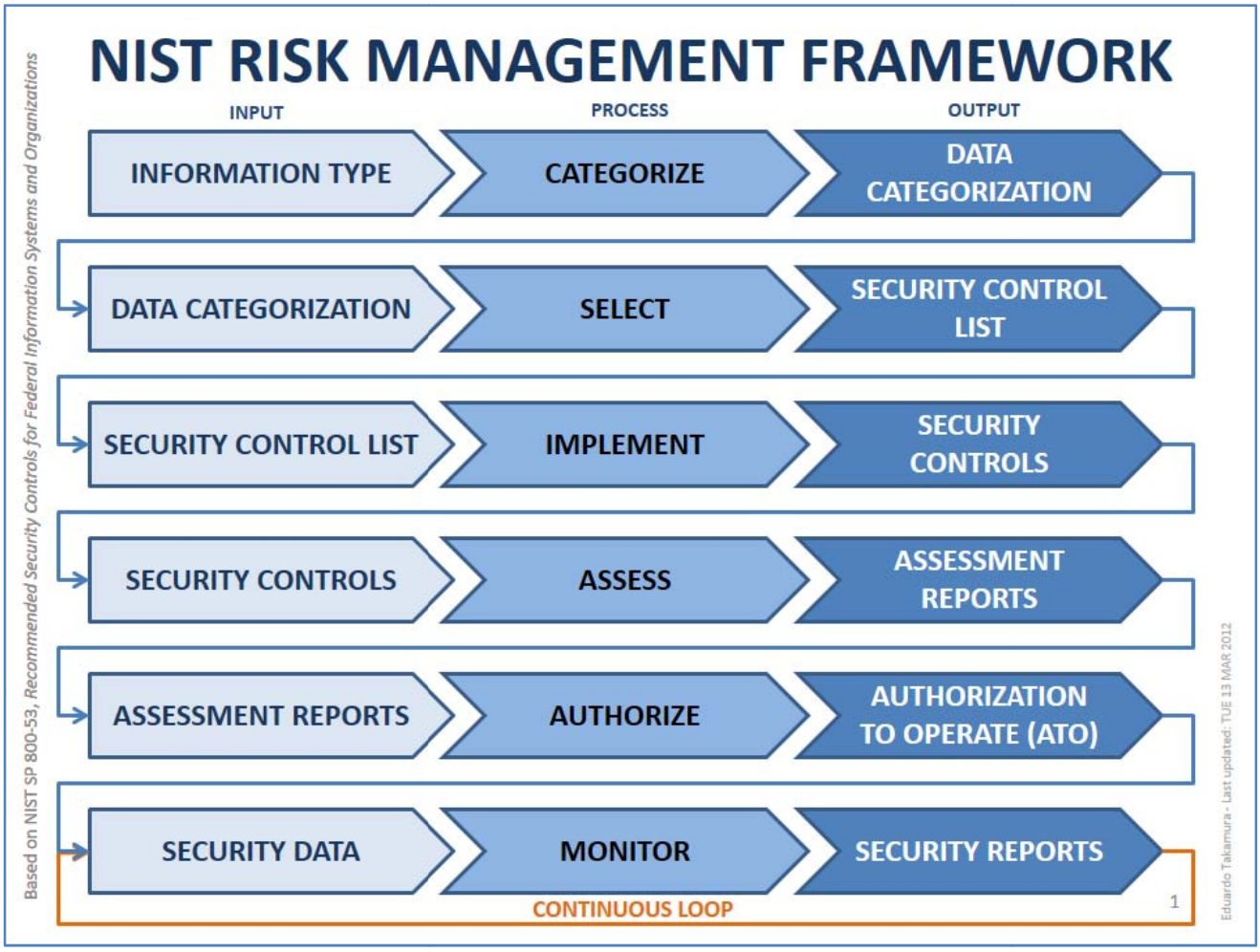

Figure 2 Inputs and Outputs to the NIST RMF Processes

The above risk management process focuses on selecting the appropriate level of protection as required by the information system. The monitoring part (step 6), which is and should be continuous, is where there is closer resemblance with the standard project risk management process in which the risk is *identified*, *analyzed* and *controlled*.

The auditing work performed on MAVEN was based on the NIST Risk Management Framework which is security control-based. The technical, operational and management security controls are audited (verified) through security assessments. This auditing is not a one-time event; the verification of the security control implementation (and operation) must be performed frequently. Continuous Monitoring is an important security process per FISMA; it is almost like an on-going requirement verification in systems engineering terms. Like safety, ground system security is more of a process or service than a product. Security products help automate some of the security processes, but no product can ensure security without appropriate processes in place. Information assurance is like mission/safety assurance: It requires constant monitoring and frequent inspections, especially with the ever evolving threat landscape that can pose risks to the Mission's information systems.

Even with a well-defined requirement and a good requirement verification plan, if there is a lack of understanding of the requirement by stakeholders, IT security teams may experience resistance to support IT security activities by stakeholders. Therefore, it is important to make sure everyone involved understands what the project is expected to comply with, knowing that such understanding is subject to interpretation by stakeholders who will see things from different angles, and respond according to their view of security. One of the first steps is acknowledging that the IT security management work will follow its own risk management methodology, different than systems engineering's, for instance.

Heritage Mentality

In product development, having heritage parts/components can be very beneficial, especially if they have been successfully deployed on a previous project/mission. In information technology and information security; however, the term "heritage" is not always good; it can imply obsolescence. Having heritage teams with knowledge and experience from serving previous missions is excellent provided these teams keep up with current requirements, especially with IT security requirements.

"We've always done it this way."

"We've never had to do it before."

"If it ain't broke, don't fix it."

These were some of the stakeholder affirmations that were heard during the planning and development stages of the mission with regard to certain IT security activities. The resistance to change is expected, but such resistance must be dealt with early in the project's initial stages using change management techniques including outreach and security briefings.

The requirements for IT security change over time. FISMA was signed in 2002, but it was revamped in 2010. NASA provided guidance for implementing the 2010 version of FISMA in 2011. As part of the FISMA requirements, plans and procedures are reviewed annually, and some of the reviewed plans and procedures may contain modifications, such as those based on updated organizationally defined values (ODVs) that dictate how a given security control is implemented. Like technology management, information security management must keep up with the evolving threats to ensure data and resources are protected against them.

Misconception: IT Security Activities Cease After ORR

Upon successful Operational Readiness Review (ORR), MAVEN established and enforced a configuration freeze on both the MSA and the backup MSA. This meant that no changes to systems were to be made until launch. These changes included but were not limited to changes to security configuration due to software patching. Other recurring IT security activities such as system monitoring, risk analysis and reporting, etc. were planned and still expected to be performed. There was apparent confusion by certain stakeholders regarding the continuation of the security work after the ORR, and one component of the ground system reallocated (human) resources that were originally supporting the IT security work to other activities based on an assumption that its IT security commitment ended at ORR.

Like insurance, information security tasks are often seen as costly and expendable but only until an incident occurs. The cost of security incident breaches and clean-up is high, and preventive IT security work must continue throughout the mission life. It does not end after a major project milestone and/or after launch, except of course when the Project reaches its final milestone: Completion/termination.

In the case of MAVEN, after the ground system is developed, tested, verified and placed into operations (launch and post-launch), the total number of development Full Time Employees (FTEs) decrease but the security processes that have been implemented will continue to be executed throughout the life of the Mission. The monitoring of network traffic, system usage, resource access attempts, hardware and software maintenance, and other activities must continue. Special attention should be paid to system vulnerabilities due to obsolete software. The patching of vulnerable software, and the verification that no unacceptable vulnerability exists via credentialed vulnerability scanning are some of the expected tasks to reduce system vulnerabilities, and ultimately maintain or increase the security of the mission's information systems.

ISOs must ensure that GRC-related activities continue to be performed according to the organization's requirements. NASA's implementation of a more continuous monitoring-centric approach to security assessment will reduce much of the overhead caused by the documentation-heavy, security snapshot approach that current missions undergo. Nonetheless, risk management decisions will continue to be documented, and risk decision makers will continue to be held accountable for their actions (or lack thereof). Stakeholders, in general, are also accountable for security, and they are reminded each year by IT security awareness training programs.

5. CONCLUSION

MAVEN is an exciting mission that will enable us to better understand the Red Planet's atmosphere, and obtain answers to questions that previous Mars missions did not or could not answer. The engineering is amazing, and the science work promising, but all the systems engineering and scientific investigations depend on the security of the information systems supporting the ground system and mission operations to ensure that, for instance, mission operations have control of the spacecraft, scientific results are trusted and not skewed (i.e., does not lack integrity), and that the Mission in general is not compromised due to a security breach of the ground system. While the IT security component is miniscule compared to other aspects of the Mission, it plays an important role in information assurance much like safety and mission assurance plays a key role in protecting the Mission.

The MAVEN IT Security team was not directly responsible for the implementation of the security controls across the ground system, but it assisted the different elements of the ground system ensure that controls were in place; risks were identified and acted upon; and that the Mission complied with NASA's requirements for IT security. Like laws, IT security policies and requirements exist for protection. Projects rely on information technology to conduct business. Information systems enable the ground system to operate the mission, and their confidentiality, availability and integrity must be protected.

There is no one-size-fits-all solution for such protection. There is no silver bullet, no technology capable of eliminating IT security risks. That is why risks must be managed so that as vulnerabilities are reduced, the security of the ground system is increased. Information assurance is as important as mission assurance, and project leadership is expected to use due diligence in managing IT risks. The championing of the Mission IT security work for MAVEN evolved over time just like the Mission's GRC work evolved from a no requirement for IT security at PDR to a fully FISMA compliant ground system at ORR. The road to MAVEN IT security compliance was not a straight, leveled line; it was rough and at times required the Project to pave the path that had not been cleared before.

The lessons learned captured in this document are just a concise summary of some of the IT security challenges that the Project faced and dealt with. This paper does not brag about the successes of MAVEN's GRC implementation; to the contrary, it shows how the planning and implementation of GRC were imperfect, and highlights some of the mistakes made during the process. MAVEN leadership could simply keep this information internal, without disseminating it to the public; instead, the lessons learned by the Project are being shared to the aerospace community so that current and future missions can take these lessons in consideration as they plan and implement GRC. Each mission/organization is unique, and special considerations must be taken by projects if following the recommendations herein. While the approach for implementing and auditing GRC will differ from mission to mission, projects/organizations may likely experience similar challenges faced by MAVEN and other NASA missions.

Table 2 Lessons Learned Recapitulation

MAVEN is an exciting mission that will enable us to better understand the Red Planet's atmosphere, and obtain answers to questions that previous Mars missions did not or could not answer.
Lesson #1: **START EARLY.**
Lesson #2: **FIND COMMON (IT SECURITY) DENOMINATOR IN A DIVERSE ENVIRONMENT.**
Lesson #3: **RESPECT CULTURAL/INSTITUTIONAL DIFFERENCES, BUT DON'T LET THEM NEGATIVELY INTERFERE WITH THE GRC WORK.**
Lesson #4: **CLEARLY DEFINE IT SECURITY REQUIREMENTS SCOPE.**
Lesson #5: **FOLLOW APPROPRIATE GRC IMPLEMENTATION METHODOLOGY.**
Lesson #6: **HERITAGE CAN BE GOOD AND BAD.**
Lesson #7: **ASSURE CONTINUOUS MONITORING.**

ACKNOWLEDGEMENTS

IT security management and support can only be successful if the team behind it is backed by project leadership that understands GRC concepts as well as Agency requirements for IT security. The MAVEN management team led by Mr. David Mitchell and Ms. Sandra Cauffman ensured that the System Owner had the autonomy and the resources to exercise his roles and responsibilities to protect the ground system. Without the MAVEN IT Security Working Group (ITSWG) support, the ISSO would not be able to effectively manage and support MAVEN IT security. Thanks to the current MAVEN ITSWG members: Don Gritzmacher (LASP), Chris Gersbach (JPL), Matt Goman (LM), Tim Quinn (UCB); and to past members and guests: Gary Ramah (JPL), Jonathan Loran (UCB), Dave Childs (JPL), George Wofford (designAmerica). Thanks to the NASA/GSFC FPD IT/IS management and support team – Ms. Cecilia Czarnecki, Mr. Carl Will, Ms. Angela Hess and Ms. Holly Wyrostek – and to the JPL/LM team who supported the security assessment of the MAVEN Mission Support Area (MSA) in Littleton, CO – Ms. Sherry Stukes, Mr. Robert Miller, Mr. David Greiner, Mr. Michael Griffin, Mr. Tom McKenzie, Mr. Mike Haggard, Mr. Wayne Sidney. Thanks to MAVEN support personnel – Ms. Leslie Cusick and Ms. Brittany Lewis – for the configuration management and logistical support for some of the IT security work performed. Finally, big thanks to MAVEN PI Dr. Bruce Jakosky for his vision, commitment, and support.

REFERENCES

[1] Appendix III to OMB Circular No. A-130, [online] http://www.whitehouse.gov/omb/circulars_a130_a130appendix_iii (Accessed: 15 November 2013).

[2] Joint Task Force Transformation Initiative, "Guide for Applying the Risk Management Framework to Federal Information Systems – A Security Life Cycle Approach," NIST Special Publication 800-37, February 2010.

[3] Joint Task Force Transformation Initiative, "Managing Information Security Risk – Organization, Mission, and Information System View," NIST Special Publication 800-39, p. 11, March 2011.

[4] P. Bowen, J. Hash, M. Wilson, "Information Security Handbook: A Guide for Managers – Recommendations of the National Institute of Standards and Technology," NIST Special Publication 800-100, p. 11, October 2006.

[5] Joint Task Force Transformation Initiative, "Managing Information Security Risk – Organization, Mission, and Information System View," NIST Special Publication 800-39, p. 6, March 2011.

[6] Compliance – Definition and More from the Free Merriam-Webster Dictionary, Merriam-Webster – an Encyclopaedia Britannica Company, [online] http://www.merriam-webster.com/dictionary/compliance (Accessed: 25 October 2013).

[7] About the Goddard Space Flight Center | NASA, [online] http://www.nasa.gov/centers/goddard/about/index.html (Accessed: 25 October 2013).

[8] MAVEN Mission Fact Sheet, FS-2012-9-125-GSFC, [online, PDF] http://www.nasa.gov/sites/default/files/files/MAVENFactSheet_Final20130610.pdf

[9] R. Miller, "JPL's Response to NASA Handbooks," 07 January 2013.

[10] Joint Task Force Transformation Initiative, "Recommended Security Controls for Federal Information Systems and Organizations," NIST Special Publication 800-53 revision 3, p. 17, August 2009.

BIOGRAPHIES

Eduardo Takamura *graduated cum laude with a B.S. in Computer Science from Bowie State University (BSU) in 1998, a M.S. in Computer Science from the Johns Hopkins University (JHU) in 2002, and became a Certified Information System Security Professional (CISSP) in 2008. He has been with NASA/GSFC for 15 years having previously served as UNIX/Linux System Administrator for the NASA Minority University-Space Interdisciplinary Network (MU-SPIN) education project as well as for the NOAA/NCEP Climate Prediction Center (CPC); Alternate Computer Security Official (ACSO) for the NASA/GSFC Computational and Information Sciences and Technology Office (CISTO); IT Manager for the NASA Sciences and Exploration Data Analysis (SESDA) II program; and IT Security Engineer/Auditor for the Landsat Data Continuity Mission (LDCM) Mission Operations Element (MOE), and NPOESS Preparatory Project (NPP). As an undergraduate student, Eduardo worked on research projects at BSU and at the Georgia Institute of Technology (Georgia Tech). Eduardo is currently serving the Mars Atmosphere and Volatile EvolutioN (MAVEN) mission as Information System Security Official (ISSO); the Origins Spectral Interpretation Resource Identification Security Regolith Explorer (OSIRIS-REx) as Information System Security Engineer (ISSE); and Space Science Mission Operations (SSMO) as Vulnerability Assessment Auditor.*

Kevin Mangum *is a 2002 graduate from the University of Maryland University College with a Bachelors of Science Degree in Technology Management. He has been with the General Dynamics C4S Corporation for 15 years and has supported various missions at NASA/GSFC for over 35 years. He has supervised system engineering groups for the development of near real time and level zero processing as well as management of operational teams. He has over 10 years experience within the IT security environment, obtaining his Certified Information System Security Professional (CISSP) certification from ISC2. Currently he is supporting the Space Science Mission Operations (SSMO) missions in the role of the Information System Security Official (ISSO).*

Carlos Gomez-Rosa *graduated magna cum laude with a B.S. in Electrical Engineering from the University of Puerto Rico in 1988 and in 1992 received a M.S. in Science from the Johns Hopkins University. Carlos has been working for NASA Goddard Space Flight Center (GSFC) since 1988. His work in IT Security goes back to GFSC's introduction to the Internet and preparations for Year 2000 (Y2K) event. He was the Information System Owner (ISO) and Operations Manager for the Earth Observing System (EOS) Data and Operations System (EDOS) from 2000 to 2007, Mission Operations Manager (MOM) for the NASA/NOAA GOES-O Mission (2007-2009), Deputy/Lead Systems Engineer for the GOES-R Ground Segment (2009-2011), and MAVEN's Ground System Manager, ISO and MOM since 2011.*

Francis Wasiak *received a B.S. in Mechanical Engineering from the State University of New York (SUNY) at Buffalo in 1989. His career started in the Mission Operations Directorate at the Johnson Space Center as a Payload Operations Engineer for the Space Shuttle Program. He has served as an Operations Director for the NASA Shuttle Small Payloads Program and Lead Instrument Operations Engineer for both the National Oceanic and Atmospheric Administration's Polar Orbiting Environmental Satellites (POES) program and the NASA Earth Observing System (EOS) Aqua Program. Currently, Fran is the Lead Ground Segment Engineer for the NASA James Webb Space Telescope (JWST) and is the Deputy Mission Operations Manager for the Mars Atmosphere and Volatile EvolutioN (MAVEN) mission. Fran has authored papers on the topic of JWST Integration and Test for SPIE and SpaceOps conferences.*