PLATINUM
BUSINESS SERVICES, LLC

IT Security Governance: A Practical Approach

Platinum Business Services, LLC

Jody Venkatesan, CISA, CISM, CGEIT, CRISC, CDPSE
President & CEO

Email: jvenkatesan@weareplatinum.net
Phone: 301-651-1297
Fax: 301-483-0104
Website: weareplatinum.net

4SBA Certified 8(a) HUBZone, Service-Disabled Veteran Owned Small Business (SDVOSB), Veteran-Owned Small Business (VOSB), Small Business (SB), Small Disadvantaged Business (SDB)
4TIN/EIN: 26-3462811
4Cage Code: 59N47
4DUNS: 828491410
4UEI: PCNMDK3FLJB9
4CIOSP3 NIH CIOSP3 SDVO
(Contract #HHSN316201800030W)
4GSA MAS Professional Services #GS00F344CA
4GSA MAS IT #GS-35F-0067Y
4GSA 8(a) STARS 3 #47QTCB21D0108

IT Security Governance: A Practical Approach

Introduction

IT Security Governance (governance) is defined as the framework and processes implemented to support the mission of the organization. Governance provides the framework for managing the organization and protecting the information technology assets. In addition to defining necessary processes, it identifies who can make decisions, who has the authority to act for the organization, who is accountable, and how people should behave and perform to safeguard sensitive data, mitigate risks, and comply with regulatory requirements.

While there are many helpful resources for framing IT Governance policies, underlying all of them is one driving piece of legislation – the Federal Information Security Modernization Act (FISMA). For civilian federal agencies, FISMA directs compliance with the direction provided by the National Institute of Standards and Technology (NIST). The NIST Risk Management Framework (RMF) is the de facto standard for federal government work. Although the Department of Defense was initially exempted, they have now adopted the NIST framework and aligned their cybersecurity standards with the NIST standards. The Government Audit Office (GAO) conducts audits in accordance with the Federal Information System Controls Audit Manual (FISCAM), which references RMF compliance.

In summary, governance for any federal agency must look to the RMF as a significant driver. Based on our experience, Platinum has found that the RMF is an excellent roadmap to implementing robust cybersecurity governance. While classic thought is that implementing governance, policy, and process should take a top-down approach, a more pragmatic approach is to take the RMF as the starting point. This is particularly useful since the FISCAM audits begin by looking to verify that appropriate governance policies are in place to support RMF implementation. Taking this pragmatic standpoint allows for an effective and streamlined implementation of cybersecurity governance.

The RMF evaluation process consists of 20 control families, over 1,000 controls, and over 5,000 "determine if" statements. A significant portion of these "determine if" statements focus on the existence and application of written policy and processes. Through our extensive experience with the rigorous assessment and audit requirements set forth by RMF and FISCAM, Platinum has found that the practical approach is to address RMF policy and process requirements to drive a structured, effective, and enforceable approach to governance. This approach also aids in meeting the evolving federal policies, including the new criteria for implementing the zero-trust architecture, as outlined by RMF, GAO, and other relevant authorities.

IT Security Governance: A Practical Approach

Based on our analysis of the 20 control families, we note that they can be grouped into six clusters of related controls, as shown in the following table. We take these groups as the guiding indicators for how to structure policy. We then use the control families to structure our policy framework. We then define the related processes based on the specific controls and the "determine if" statements associated with each control family. This method gives us a sound basis for establishing an executable governance plan. This approach ensures our clients are well-prepared to successfully pass control audits, including those mandated by RMF and FISCAM.

Platinum's Grouping of RMF Control Families to Guide Policy Development	
Control Family	**Description**
Cluster 1: Access Permissions and Controls	
Access Control	Defines who has access to what assets, supports account management, the definition of system privileges, and remote access. Includes system logging to note when unauthorized access is attempted.
Identification and Authentication	Supports identification and authentication for all organizational and non-organizational users and how authentication is managed within the system.
Cluster 2: Security Risk Assessment, Audit, and Authorization	
Risk Assessment	Dictates risk assessment and vulnerability scanning standards, providing an integrated risk management solution.
Audit and Accountability	Defines security controls implemented and therefore auditable; this includes audit policies and procedures, audit logging, audit report generation, and protection of audit information.
Security Assessment and Authorization	Security assessments, authorizations (A&A, issuance of ATO), continuous monitoring, Plan of Actions and Milestones (POA&Ms), and system interconnections.
Cluster 3: Incident Response and Recovery	
Incident Response	Incident response policies and procedures include training, testing, monitoring, reporting, and response plans.
Contingency Planning	Contingency plan if a cybersecurity event should occur, including contingency plan testing, updating, training, backups, and system reconstitution.
Cluster 4: Personnel and Physical Security	
Personnel Security	Personnel protection through position risk, personnel screening, termination, transfers, sanctions, and access agreements. (Critical since an estimated 60% of security incidents are personnel-related.)
Physical and Environmental Protection	Protection for systems, buildings, and supporting infrastructure against physical threats, including physical access authorizations, monitoring, visitor records, emergency shutoff, power, lighting, fire protection, and water damage protection.
Awareness and Training	Security training and procedures for all staff, including security training records.
Cluster 5: System and Program Management	
Planning	Security planning defines the purpose, scope, roles, responsibilities, management commitment, coordination among entities, and organizational compliance.
Program Management	Defines who manages the cybersecurity program and its operations, including a critical infrastructure plan, information security program plan, Plans of Action Milestones, risk management strategy, and enterprise architecture.
System and Services Acquisition	The processes to allocate resources against an organization's system development life cycle include information system documentation, development configuration management, and developer security testing and evaluation.
Maintenance	Defining requirements for maintaining organizational systems and the tools used.
Configuration Management	Baseline configuration is used as the basis for future builds or changes to information systems, including information system component inventories and security impact analysis control.

IT Security Governance: A Practical Approach

Platinum's Grouping of RMF Control Families to Guide Policy Development	
Control Family	**Description**
Cluster 6: Network and Enterprise Systems Controls	
System and Communications Protection	Defines systems and communications protection procedures, including boundary protection, protection of information at rest, collaborative computing devices, cryptographic protection, denial of service protection, and many others.
System and Information Integrity	Correlates controls that protect the system and information integrity, including NIST SI 7, which involves flaw remediation, malicious code protection, monitoring, security alerts, software/firmware integrity, and spam protection.
Media Protection	Controls specific to access, marking, storage, transport policies, sanitization, and defined organizational media use.
Personally Identifiable Information	Protect sensitive data by emphasizing privacy and consent.
Supply Chain Risk Management	Methods to mitigate risks in the supply chain.

For each set of controls, we establish Standard Operating Procedures (SOPs) that comply with the RMF controls and are practical and usable to perform the functions needed to maintain the enterprise successfully. Like any documented process to manage the enterprise, we define quality assurance and quality control activities to ensure the operations are performed as established (QA) and the process outcomes are as expected (QC). QA is typically conducted as process audits or desk audits. QC is generally evaluated against a set of defined performance metrics.

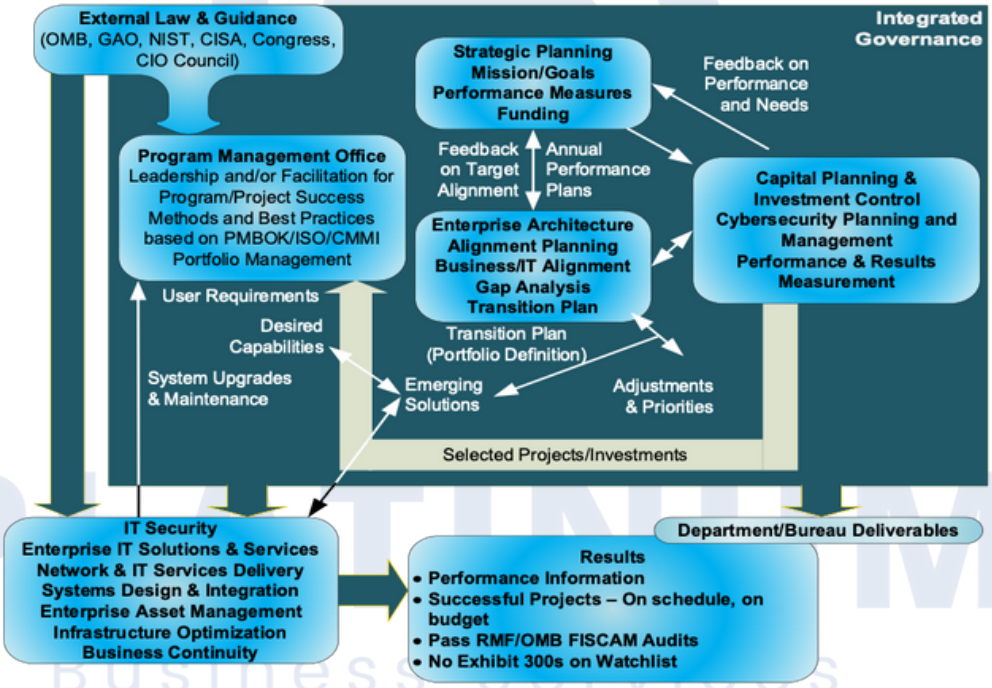
Realistically, governance should be an enterprise activity for security and all aspects of IT operations. We suggest that governance should be approached as an integrated, enterprise-wide process, not just a security issue. Our experts work closely with senior government management, strategic planners, enterprise architects, IT security specialists, Capital Planning and Control Officers, other finance and budget planners, and IT project managers to develop a comprehensive approach to governance, as shown in the graphic shown at the top of Page 3.

IT Security Governance: A Practical Approach

We develop governance plans using a four-step process.

Step 1: The first step is to identify and baseline all information related to elements of the IT management agenda and client criteria, including mission goals, capital planning, business cases, enterprise architecture, high-risk issues, and any other IT management-related issues our client currently tracks.

Step 2: We then create a Maturity Improvement Plan (MIP) that tracks progress using performance-related criteria to report monthly. This MIP is integrated with any client-created agreements with other Government entities. During this second step, we look for opportunities to implement best practices and apply quick improvement tips.



Step 3: During Step 3, Platinum's staff manage the overall MIP and any areas projected for improvement and progress on any of the areas mentioned in the overall Enterprise Architecture model to ensure IT management's success and proper management implementation of cybersecurity standards and controls. Platinum knows this support requires much collaboration and communication with government stakeholders and other vendors supporting projects and programs across the enterprise.

Step 4: In the final step, we stabilize the governance process while ensuring the delivery of continuous process improvements. We identify any new laws, guidance, requirements, OMB-issued criteria, NIST updates, and Cybersecurity and Infrastructure Security Agency (CISA) alerts and assess the impact of these changes on our client's IT Management and Governance processes.
Platinum is successfully providing this Integrated Governance Model to ensure successful IT management and cybersecurity for multiple Government clients, supporting successful metrics-based performance and NIST RMF, GAO, and FISCAM audits.