**<<Organization> IT Risk Management Workgroup Guidelines - Version 1.0**

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **1.0 Overview** These guidelines are intended to provide a framework for activities to be performed by the <<Organization> IT Risk Management Workgroup (ITRMW).  **2.0 Purpose**  This document details the composition, responsibilities, and tasks to be performed by the ITRMW over time. Where possible, these activities will be mapped to the federal NIST 800-53 revision 4 standards.  **3.0 Scope** This standard applies to the ITRMW, which represents multiple disciplines and therefore to all information systems management for <<Organization>.  **4.0 Standards**  **4.1 ITRMW Meeting Schedule**  The ITRMW will meet on a regular basis, and on an as needed basis. The group will convene on at least a quarterly basis; in addition to meeting on an as-needed basis discuss specific issues or developments. Occurrences that may initiate an off-schedule meeting of the ITRMW include events such as:   * Purchasing of new hardware, software or services * Identifying and planning security requirements for new <<Organization> initiatives * Budgetary planning * Response to security incidents or concerns * Review of audit findings, security requirements and regulations * Changes in staffing or security responsibilities * Creation of new security policies, procedures and guidelines * Track security developments such as releases of 0-day exploits and new vulnerabilities * Identify and plan for changes in IT and other industries * Other events as needed   **4.2 ITRMW Composition**  The ITRMW is composed of key internal and external stakeholders in <<Organization> Information security efforts. The following table details the roles currently identified for the ITRMW, including both management and Subject Matter Experts (SMEs):   | **Position / Role** | **Current representatives** | **Attendance required** | | --- | --- | --- | |  |  |  | |  |  |  | |  |  |  | |  |  |  | |  |  |  | |  |  |  | |  |  |  | |  |  |  |   **4.3 ITRMW Tasks and Responsibilities** The primary function of the ITRMW is to regularly track discuss and prioritize security issues at <<Organization>. The level of effort spent in any one area may vary depending upon the current situation. For some meetings, a specific focus on one topic may dominate the workgroups discussion while at other times a brief review of each issue may be performed.  As a baseline, the following tasks and issues are considered as responsibilities of the ITRMW and should be discussed at each meeting:     | **Task / Area** | **NIST Mapping(s)** | **Description / Notes** | | --- | --- | --- | | Develop, maintain and disseminate IS security plans | PM-1(a), PM-1(b),  PM-1(c), PM-1(d), PM-9,  PM-11 | Maintain overall security guidance documents, including an overall risk management strategy, management commitment, coordination between entities and compliance. Review plans at least *annually* and update as needed. Protect plans from unauthorized access or modification. Define the mission of IS security efforts. Obtain administrative approval of plans and procedures. | | Identify and assign IS security roles and responsibilities | PM-1(a)(2), PM-2,  PM-13 | Identify which individuals will have responsibility for IS security functions, including both technical and non-technical representatives. Define knowledge and skills required, training needs, and means of testing employee security awareness and competency. Identify staff to monitor listserves and industry bulletins. | | Information security resources | PM-3 | Ensure capital planning and investment, maintain business cases, budgets and plans | | Maintain a plan of action / milestones / task list | PM-4 | Maintain a list of tasks that must be performed, identify the individual(s) responsible for these tasks, the current state of the tasks, and timelines for completion | | Maintain an IS inventory | PM-5 | Create / review / maintain a list of IS inventory including hardware, software, licenses and security controls | | Identify / review / monitor key performance indicators for IS security performance | PM-6 | Identify a list of security benchmarks or Key Performance Indicators (KPIs) that can be used to track security function performance and activity levels over time. For example:   * The number of systems infected by malware * The number of security investigations performed * The number of system currently in or out of compliance with mandatory standards (i.e. STIGS, PCI, etc.) * The number of system logs reviewed or not reviewed * Accounts provisioned * System uptime and compliance with SLAs * Monitored vs. un-monitored systems * Number of active vulnerabilities * Number of notifications acknowledged * Number of systems patched/updated * Other KPI’s TBD | | Create / maintain an enterprise information systems architecture | PM-7 | Create and maintain documents and standards about the overall <<Organization> security architecture, including items such as:   * Inventories * IP addressing schemes * Network maps (layer 2, layer 3) * System interdependencies and data flows * Other documents TBD | | Manage enterprise identification and authorization processes and procedures | PM-10,  CA-ALL | Document the security state of systems that use authorization systems (i.e. Active Directory, application access, etc), the procedures used, and the individuals responsible for these systems. | | Identify the risk from insider threats and identify compensating controls | PM-12 | Maintain a cross-discipline approach to managing the risk from trusted insiders (i.e. employees and consultants) | | Maintain a security workforce awareness program | PM-14,  PM-15,  PM-16,  AT-ALL | Maintain a plan to train employees on security awareness topics such as regulatory compliance, resistance to phishing, identification of malware, etc. | | Maintain a security testing program | PM-14,  CA-ALL | Maintain a set of standards for how security will be tested, including items such as vulnerability scanning, peer review, change management, etc. | | Maintain a security monitoring program | PM-14 | Maintain a set of standards for how security will be monitored at <<Organization>, including items such as log review, monitoring anti-virus systems, etc. | | Maintain organizational contacts with third parties | PM-15 | Maintain lines of communication with internal and external parties to assist in security training and awareness, incident response, etc. | | Maintain documentation of ITRMW activities and discussion | PM-ALL | Maintain meeting notes and documentation about discussions and tasks performed by the ITRMW. Make these documents available via SharePoint and other means to authorized parties | | Create and maintain Disaster Recovery / Business Continuity Planning systems | PE-ALL,  SC-ALL,  CP-ALL, PE-ALL | Maintain and review current DR/BCP practices and procedures. Identify current shortcomings, risks and threats. Identify tasks to be completed to maintain the plan including hardware and software implementation; plan testing ; review of backup logs; maintain and document redundancy, power and server health systems; monitoring, etc. | | Create and maintain access and authorization systems | AC-ALL | Maintain documented procedures for managing access to IS systems. Include items such as how requests will be created and validated, the level of detail that must be provided to provision access, and validation of access. Identify the parties responsible for requesting user access. Include granting, changing, and revoking access. | | Create and maintain systems for managing mobile devices | AC-19 | Mobile device management (phones and tablets) | | Create and maintain activity audit and accountability systems | AU-ALL | Identify how system activity will be logged and monitored. Consider identifying different systems based on system criticality and/or location (i.e. enclave systems, regular internal IS systems, public kiosks, etc.) | | Maintain configuration management procedures and systems | CM-ALL | Create and maintain systems to manage change (i.e. change management) over time at <<Organization> | | Maintain media handling and protection procedures | MP-ALL, RA-2 | Identify various classifications of data and how these types of data must be handled. Include topics such as workstation data, use of flash drives and removable media, and data destruction at a minimum. | | Maintain procedures for the acquisition of secure goods and services | SA-ALL | Include items such as minimum standards for security purchases, security expectations of vendors, etc. | | Maintain personnel security procedures | PS-ALL | Maintain systems for the acquisition and retention of employees. Include items such as pre-hire background checks, degrees and certifications, etc. | | Perform and review technical security risk assessments | RA-ALL | Regularly perform assessments of security including network scans, application security scans, reviews of as-configured access rights, etc. and maintain a list of items to be addressed as needed. | |
|  |