ISACA San Francisco 2013 Fall Conference

Session G21 - Issues, Challenges and Practical Approaches to IT Security Risk Metrics & Reporting

Presented by Arun Sivaraman, Director, SOAProjects

HANDOUT C: Sample metrics for select IT Process and control areas

Note: The following table includes selected IT Process and Control areas and several sample metrics. These metrics are selected to highlight process risks, process inefficiencies and control gaps.

This handout is provided for illustrative purposes only. Organizations may require metrics that cover various attributes such as control effectiveness, process efficiency, coverage efficiency, cost of implementation, cost of operation, etc. In such cases, the metrics program manager(s) should consider their business requirements and select appropriate metrics.

Process area:	Sample Process objective	Common Process and Control activities	Suggested Metrics, based on risks, process and control objectives
Identity and Access Management	• User Roles and authorizations are defined based on defined business rules. • User accounts are provisioned and maintained based on approved business requirements, and de-provisioned in a timely manner.	• Define, test and approve standardized and non-standard roles and authorizations • Request, create, modify and disable/delete user accounts • Manage privileged and generic/service user accounts and associated risks • Validate and recertify the appropriateness of roles, users and role assignment to users • Maintain and enforce SOD rules, and to ensure manual mitigation controls are performed as intended.	• Number of functional roles with corresponding user profiles / Total functional roles • Number of non-standard user profiles / Total user profiles • Number of systems or applications integrated with the central directory or SSO / Total systems or applications • For a given system or application environment: Total number of accounts with admin privileges / Total number of users • Total number of user profiles and accounts not modified or terminated in a timely manner / Total number of users whose profile has changed or terminated. • Number of terminated users with administrative access, where the termination was not timely. • Number of late or missed access control reviews, log reviews or recertifications.
IT asset management and oversight	• Ensure authorized assets are deployed and unauthorized assets are prevented, or identified and removed in a timely manner • Business owners understand their role as information owners and take necessary steps to classify and protect	• Information classification guidelines and awareness • Information system classification and appropriate protection • Scans to identify assets and determine their appropriateness or take corrective action • Completeness and accuracy of information asset inventory	• Pervasiveness of information classification amongst the user base (assuming policy is not enforced through tools, and metrics data is collected through sampling, inquiries and inspections) • Accuracy of IT and information asset inventory (ex., valdiated against BCP initiatives) • Number of unauthorized infrastructure components identified / total assets in a given scope (add dimensions such as groups or locations as needed)

	their assets • IT and Information Assets are used to drive risk assessments and control activities • IT / Information Assets are securely deployed and maintained.	• Usage of security guidelines for the deployment and maintenance of IT infrastructure • Periodic validation of guidelines and security specifications • Ensuring non-standard assets are kept within permitted scopes (ex., Labs).	• Number of IT assets tied to business or IT Processes at the time of provisioning • Number of insecure or out-of-box IT assets deployed / total assets deployed (Add dimensions such as groups, locations etc. as needed)
Vendor management	• Authorized vendors and personnel are allowed access to the organization's IT and information assets and unauthorized users are denied access • Vendors are meeting contractual obligations (i.e., organization's security requirements) • Vendor resources follow organization's security policies and procedures • Access to vendors is securely managed monitored and maintained in accordance with risk levels	• Vendor classification schema Initial and Ongoing Vendor security assessments • Initial and Ongoing Vendor contract reviews and updates • Review of vendor related risks identified in third party audit reports • Security awareness and conduct guidance for vendor resources • Identity management processes and controls extended to systems shared with vendors	• Number of vendors for whom security review was not performed / Total number of vendors • Number of vendors deemed as High risk / Total number of vendors • Quantity of unique vendor security risks not addressed by the vendor since last review • Number of vendor resources who did not complete the required awareness programs on time (per Vendor, if needed) • Number of security incidents tracked to vendors / total number of security incidents tied to users or their insecure behavior • Number of active (or terminated) vendor resources with active access to sensitive IT systems
IT Change Management	• Changes to IT environment are tested and approved prior to implementation • Emergency Changes are performed in accordance with established processes • Segregation of duties are maintained during the execution of change management process • Roll back plans are developed as part of change planning, and utilized as necessary	• Well defined Change management process that covers authorization, implementation, roll back plans (as applicable), testing, approval, scheduled and emergency changes, post-implementation review, and documentation • IT SOD Verification	• Number of IT systems or infrastructure elements that are covered by the formal change management process vs. Number of IT systems or infrastructure elements that are NOT covered by the process (data collected through inquiries and inspections) • Number of documented changes for non-regulated systems / Number of actual changes made to non-regulated but sensitive systems (collected through the use of system logs, etc.) • Number of emergency change tickets / Total number of unplanned outages and outage extensions • Number of unplanned incidents where roll back process was not effective (collected through the list of extended, unplanned outages)

Vulnerability Management	• Vulnerabilities in IT systems and applications are identified in a timely manner through vendor or external announcements and internal assessments • Patches and bug-fixes, where available, are applied to relevant systems in a timely manner and tested thoroughly • Workarounds are implemented and tested when patches are not available • System baselines and images are updated with patch / workaround information in a timely manner	• Periodic vulnerability assessment scans are performed for relevant systems • IT teams track ongoing vulnerability announcements and take appropriate corrective action • Application security assessments are performed for in-house applications by qualified personnel • Application security gap remediation are implemented prior to moving the application to production • Patch management process exists, and covers patch announcement tracking, testing, timely deployment and support	• Scope of coverage for vulnerability scans / total number of similar systems and applications • Periodicity of vulnerability assessment scans • Number of unremediated vulnerabilities (per system or application) identified by successive scans (or over a period of time) • Number of incidents due to unpatched vulnerabilities (per system or org. unit) • Number of vulnerabilities identified by scanners or internal resources / Number of vulnerabilities identified by external specialists • Number of vulnerabilities not addressed prior to moving to production (i.e., per system or group) / total number of vulnerabilities identified during pre-production assessment • Vulnerabilities found across development groups or business units (indicating underlying education problems) mapped to top ten or top 25 lists • Number of systems that are not periodicially patched as they are "critical" / total number of Internet-connected systems • Time taken between patch announcement to patch deployment • Number of unpatched systems susceptible to zero day attacks / total number of systems (Internal or Internet connected)
Malware management	• Organization's IT systems and assets are continually protected from malware and APT infections.	• All end points are protected by Antivirus and Anti-malware measures • Up to date Antivirus software is deployed on all relevant systems • Antivirus updates are pushed to clients in a timely manner • End points are periodically scanned and exceptions are acted upon in accordance with policy • Exceptions to the published antivirus policy are acted upon in a timely manner	• Number of clients protected by AV / total number of clients (including those not protected by AV) • Number of systems without the right AV software version / Number of clients protected by AV • Number of systems without the right definition database version / Number of clients protected by AV • Number of clients that have very outdated AV (ex., months as against weeks) / total number of clients (or number of clients with outdated AV) • Number of clients where AV scan completions are not reported in a timely manner • Total number of virus infections cleaned or quarantined

		• The organization uses a different gateway product (i.e., from a different vendor) to scan ingress and egress traffic to identify malware missed by the AV clients • Websites visited by end users are scanned for viruses	by client AV during a period / Total number of virus infections identified by the gateway or secondary product • Number of virus infections traced to various sources (i.e., user behavior, software vulnerability, unsupported software, etc.) over a period of time • Number of incidents from visiting external websites • Number of Viruses detected on network shares (over a period of time, or across user groups etc.) Number of hours spent on manual clean up (over time / across user groups / etc.)
Incident management (security)	• Incidents are identified, contained, analyzed and resolved in a timely manner • Well defined process is followed to communicate with and update stakeholders (to prevent negative publicity)	• "Good configuration" of systems and applications are 'known' to the organization, and it has adequate technical and human-resource capability to detect any 'unknown' or suspected changes to the baseline. • Staff has received training on identifying, isolating, containing suspected incident cases. • Expertise is available in-house or on-demand to analyze incidents, identify the area of intrusion and method used, extent of intrusion, data compromised, follow established digital forensics procedures as needed, provide guidance on recovering and preventing future intrusions • The incident response steps are carried out in a timely and well defined manner • Lessons learned are captured for future reference, and made available to relevant teams	• Number of systems where the Good configuration is known to the IT team / Total number of systems • Number of IT specialists trained on incident response procedures and provided with sufficient tools • Number of systems impacted in a given incident, correlated to unpatched vulnerabilities and unsupported software • Time elapsed between incident exploit or intrusion to detection • Time elapsed between incident detection to incident containment • Time elapsed between incident detection to service recovery • Total man hours spent per incident • Total business losses estimated per incident • Total losses (hours + cost) for a given duration, correlated with number of internet-exposed systems

--- End of document ---