Information Security
Risk Assessment Checklist

Introduction

Information security is a critical issue for any organization. Increased access to information and various services has occurred as companies increasingly move their core activities to the Internet. As more information and services become available, these Internet-based technologies become a greater risk of potential liability and cost. Information Technology Departments play a unique role as the managers and caretakers of some of the largest collections of critical systems, applications, and databases. These systems, applications, and databases often house information which is subject to strict controls and protections by law, including the data collected, stored, shared, and transmitted that was once very difficult to obtain. Risk assessment tools, like this one, can assist in determining the gaps in its information security program and provide guidance and direction for improvement.

Use of this simple Checklist is not required, nor is it intended to cover all of the issues related to information security, but its use will provide a high-level view of the security posture when measured against general information security practices.

This tool should be used in conjunction with the following steps:

1. This Checklist should be completed by the Information Security Officer (ISO), in cooperation with the Chief Information Officer. A response to the items in each section should be prepared to accurately reflect the “point in time” picture of the organizations security posture.
2. Identify the levels of risk associated with any of the items that result in a “no” response.
3. Develop an appropriate action plan to mitigate the identified risk.
4. Assign roles and responsibilities for implementing and monitoring timely completion of the action plan.

Information Security Risk Assessment Checklist

	Yes/No
A. Organizational and Management Practices	
1. Security Program Governance – Executive Management has assigned roles and responsibilities for information security across its organization. This includes, but is not limited to, the following: documenting, disseminating, and periodically updating a formal information security program that addresses purpose, scope, roles, responsibilities, applicable laws and regulations, and the implementation of policies, standards, and procedures.	
2. Confidentiality Agreements – Implement confidentiality or non-disclosure agreements with contractors and external entities to ensure the companies need for protection of confidential information is met.	
3. Risk Assessments – A review process at planned intervals is implemented to ensure the continuing suitability and effectiveness of the companies approach to managing information security.	
4. System Security – A formal document that provides an overview of the security requirements for information systems and describes the security controls in place (or planned) for meeting those requirements is maintained.	
5. System Certification – An assessment of the security controls in place for existing systems and those planned for new systems is conducted at least once each year. Assessment tools are readily available through security organizations, like National Institute of Standards and Technology (NIST), SysAdmin, Audit, Network, Security (SANS) Institute, and other reputable sources. The ISO reviews and approves actions taken to correct any deficiencies identified. Responsible technical or operational management are included in the review process.	
6. Configuration Change Control – Changes made to information systems are controlled and documented. The changes are reviewed and approved in accordance with written policy and procedures, including a process for emergency changes.	
7. Security Categorization – Procedures to classify systems and information that is stored, processed, shared, or transmitted with respect to the type of data (e.g., confidential or sensitive) and its value to critical business functions are in place.	
8. Vulnerability Scanning – A regular occurring (e.g., bi-annual, quarterly, monthly) process using specialized scanning tools and techniques that evaluates the configuration, patches, and services for known vulnerabilities is employed.	
B. Personnel Practices	
1. Security Awareness – Training is provided to all employees and contractors on an annual basis that addresses acceptable use and good computing practices for systems they are authorized to access. Content of training is based on policies addressing issues, such as, privacy requirements, virus protection, incident reporting, Internet use, notification to staff about monitoring activities, password requirements, and consequences of legal and policy violations.	
2. Human Resources Security – Policies and procedures that address purpose, scope, roles, responsibilities, and compliance to support personnel security requirements, such as access rights, disciplinary process, etc. are in place.	
3. Position Categorization – Procedures for identifying system access needs by job function and screening criteria for individuals performing those functions are in place.	

	Yes/No
4. Personnel Separation – A process to terminate information system and physical access and ensure the return of all company-related property (keys, id badges, etc.) when an individual changes assignments or separates from the company is developed and implemented.	
5. Third Party or Contractor Security – Personnel security requirements for third-party providers and procedures to monitor compliance are in place. Requirements are included in acquisition-related documents, such as service-level agreements, contracts, and memorandums of understanding.	
6. Personnel Screening – Employee history and/or a background check is performed on employees who work with or have access to confidential or sensitive information or critical systems.	
C. Physical Security Practices	
1. Physical and Environmental Program – Policy and procedures that address the purpose, scope, roles, responsibilities, and compliance for physical and environmental security, such as security perimeter and entry controls, working in secure areas, equipment security, cabling security, fire detection and suppression, room temperature controls, etc. are in place.	
2. Physical Access Monitoring – The need for monitored access to business areas is evaluated. In monitored areas, records for approved personnel access and sign-in sheets for visitors are maintained. Logs are periodically reviewed, violations or suspicious activities are investigated, and action is taken to address issues.	
3. Physical Access Control – Physical access to facilities containing information systems is controlled and individual's authorization is verified before granting access.	
4. Environmental Controls – The necessary environmental controls, based on a requirements assessment, which includes but is not limited to backup power to facilitate an orderly shutdown process, fire detection and suppression, temperature and humidity controls, water damage detection and mitigation are provisioned and properly maintained.	
5. Secure Disposal of Equipment – Processes are in place to permanently remove any sensitive data and licensed software prior to disposal.	
D. Data Security Practices	
1. Disaster Recovery Planning – A Disaster Recovery Plan (DRP) is in place that supports the current business continuity needs of the agency. The DRP plans for the recovery of technology and communications following any major event that disrupts the normal business environment, provides for periodic updating and testing of the plan, and its documentation includes, but is not limited to:	
Recovery based on critical and sensitive business needs.	
Location of regular backups of systems and data, with documentation.	
Regularly updated information about where copies of the plan reside, including appropriate off-site locations.	
Training for appropriate personnel.	
2. Information Back-up – Backup copies of information and software are completed on a routine schedule, tested regularly, and stored off-site.	
3. Monitoring – System logging, and routine procedures to audit logs, security events, system use, systems alerts or failures, etc. are implemented and log information is in placed where it cannot be manipulated or altered.	

	Yes/No
4. Data Classification – Policies and processes to classify information in terms of its value, legal requirements, sensitivity, and criticality to the organization are in place.	
5. Access Controls – Policies and procedures are in place for appropriate levels of access to computer assets. Access controls include, but are not limited to:	
Password management, including the use of strong passwords, periodic password change, and restriction of sharing access and/or passwords. System access is authorized according to business need and password files are not stored in clear text or are otherwise adequately protected.	
Wireless access restrictions are in place, with organizational control over access points, prohibition and monitoring against rogue access points, appropriate configuration of wireless routers and user devices, and policy, procedure, and training for technical staff and users are in place.	
Secure remote access procedures and policies are in place, and are known and followed by users.	
Mobile and portable systems and their data are protected through adequate security measures, such as encryption and secure passwords, and physical security, such as storing devices in a secure location and using cable locking devices.	
The tracking of access and authorities, including periodic audits of controls and privileges is in place.	
Networks challenge access requests (both user and system levels) and authenticate the requester prior to granting access.	
6. Least Privilege – Configuration to the lowest privilege level necessary to execute legitimate and authorized business applications is implemented.	
7. Data Storage and Portable Media Protection – Policies and procedures to protect data on electronic storage media, including CDs, USB drives, and tapes are in place. Procedures include labels on media to show sensitivity levels and handling requirements, rotation, retention and archival schedules, and appropriate destruction/disposal of media and data.	
E. Information Integrity Practices	
1. Identification and Authentication – Policies and procedures for identification and authentication to address roles and responsibilities, and compliance standards are in place.	
2. User Identification and Authentication (typically userid and password) – Information systems/applications uniquely identify and authenticate users when it is appropriate to do so.	
3. Device Identification and Authentication – Information systems/applications identify and authenticate specific devices before establishing a connection with them.	
4. System and Information Integrity – Policies and procedures for system and information integrity to address roles, responsibilities, and compliance standards are in place.	
5. Malicious Code Protection – A regular patching process has been implemented to protect against malicious code. The process is automated when possible.	
6. Intrusion Detection – Tools and techniques are utilized to monitor intrusion events, detect attacks, and provide identification of unauthorized system use.	
7. Security Alerts and Advisories – The appropriate internal staff members receive security alerts/advisories on a regular basis and take appropriate actions in response to them.	

	Yes/No
8. Secure System Configuration – The security settings on systems are configured to be appropriately restrictive while still supporting operational requirements. Non-essential services are disabled or removed when their use is not necessary as to eliminate unnecessary risk.	
9. Software and Information Integrity – Information systems/applications detect and protect against unauthorized changes to software and information.	
10. Information Input Accuracy, Completeness, and Validity – Information systems/applications check data inputs for accuracy, completeness, and validity.	
11. Flaw Remediation – Information system/application flaws are identified, reported, and corrected.	
F. Software Integrity Practices	
1. System and Services Acquisition – Policies and procedures for system and services acquisition are in place to address roles and responsibilities, and processes for compliance checking.	
2. Software Integrity Practices – Policies and procedures associated with system and services acquisition and product acceptance are in place.	
Acquisitions – Security requirements and/or security specifications, either explicitly or by reference, are included in all information system acquisition contracts based on an assessment of risk.	
Software Usage Restrictions – Controls or validation measures to comply with software usage restrictions in accordance with contract agreements and copyright laws are in place.	
User Installed Software – An explicit policy governing the downloading and installation of software by users is in place.	
Outsourced Information System Services – Controls or validation measures to ensure that third-party providers of information system services employ adequate security controls in accordance with applicable laws, policies and established service level agreements are in place.	
Developer Security Testing – A security test and evaluation plan is in place, implemented, and documents the results. Security test results may be used in support of the security certification process for the delivered information system.	
G. Personal Computer Security Practices – Personal computing devices include desktops, laptops, notebooks, tablets, Personal Device Assistants (PDA), and other mobile devices.	
1. Device Hardening – Operating system and application level updates, patches, and hot fixes are applied as soon as they become available and are fully tested. Services on the computing devices are only enabled where there is a demonstrated business need and only after a risk assessment.	
2. Lock-Out for Inactive Computing Devices – The automatic locking of the computing device after a period of inactivity is enforced.	
3. Data Storage – Data that needs additional protection is stored on pre-defined servers, rather than on computing devices, for both data protection and backup/recovery reasons. Confidential, sensitive, and/or personal (notice-triggering) information is not stored on computing devices without a careful risk assessment and adequate security measures.	

	Yes/No
H. Network Protection Practices	
1. Network Protection – Network and communication protection policies and procedures are in place. These documents outline the procedures to authorize all connections to network services. Authorization is based on an evaluation of sensitive or critical business applications, classification of data stored on the system, and physical location of the system (e.g., public area, private access, secure access, etc.).	
2. Boundary Protection – Equipment designed for public access (i.e. Web servers dispensing public information) is protected. These are segregated from the internal networks that control them. Access into internal networks by authorized staff is controlled to prevent unauthorized entry.	
3. Protect and Secure Network Infrastructure – Policies and procedures for technology upgrades, network equipment (e.g., servers, routers, firewalls, switches), patches and upgrades, firewall and server configurations, and server hardening, etc are in place.	
4. Transmission Integrity and Confidentiality – Data is protected from unauthorized disclosure during transmission. Data classification is used to determine what security measures to employ, including encryption or physical measures.	
I. Incident Response Practices	
1. Incident Response – Incident response policies and procedures consistent with applicable laws and policies are in place. These include but are not limited to identification of roles and responsibilities, investigation, containment and escalation procedures, documentation and preservation of evidence, communication protocols, and lessons learned.	
2. Incident Reporting – Proper incident reporting policies and procedures are in place. These include training employees and contractors to identify and report incidents, the reporting of incidents immediately upon discovery, and preparation and submission of follow-up written reports.	