KirkpatrickPrice

Risk Assessment Guide

KirkpatrickPrice. | innovation. integrity. delivered.

v2.1_3.2011

Document Purpose

The Risk Assessment Guide document is used to analyze vulnerabilities, potential threats and risks for an organization, and the organization's IT systems.

This guide is based on controls found in the NIST Special Publication 800-53, the Shared Assessments Program Agreed Upon Principles, ISO 27001 and other highly regarded industry standards. This guide is meant to trigger a thought process to identify vulnerabilities and risks particular to your organization and is not meant to be a comprehensive list of potential risks.

Risk Identification

Identifying risk for an IT system requires an understanding of the system's processing environment. Therefore, the risk assessor must first collect system-related information, which is usually classified as follows:

- Hardware;
- Software;
- System interfaces (e.g., internal and external connectivity);
- Data and information;
- Persons who support and use the IT system;
- System mission (e.g., the processes performed by the IT system);
- System and data criticality (e.g., the system's value or importance to an organization); and
- System and data sensitivity.

The use of information technology poses a wide variety of risks. Obviously, there is the risk of malicious attack from hackers, but certain other risks are often overlooked. User error can destroy or leak data, or take down a system. Adverse events such as fires, floods and other natural disasters can wreak havoc in any business environment. The following table lists many such events:

Potential Adverse Events

Air Conditioning Failure	Earthquake	Nuclear Accident
Aircraft Accident	Electromagnetic Interference	Pandemic
Biological Contamination	Fire	(Major or Minor) Power Loss
Blackmail	Flooding/Water Damage	Sabotage
Bomb Threat	Fraud/Embezzlement	Terrorism
Chemical Spill	Hardware Failure	Tornado, Hurricane, Blizzard
Communication Failure	Human Error	Unauthorized Access or Use
Computer Crime	Loss of Key Personnel	Vandalism and/or Rioting
Cyber-Terrorism	Malicious Use	Workplace Violence

The adverse impact of a security event can be described in terms of loss or degradation of any, or a combination, of the following three security goals: integrity, availability, and confidentiality. The following list provides a brief description of each security goal and the consequence (or impact) of its not being met:

- **Loss of Integrity.** System and data integrity refers to the requirement that information be protected from improper modification. Integrity is lost if unauthorized changes are made to the data or IT system by either intentional or accidental acts. If the loss of system or data integrity is not corrected, continued use of the contaminated system or corrupted data could result in inaccuracy, fraud, or erroneous decisions.

  Also, violation of integrity may be the first step in a successful attack against system availability or confidentiality. For all these reasons, loss of integrity reduces the assurance of an IT system.

- **Loss of Availability.** If a mission-critical IT system is unavailable to its end users, the organization's mission may be affected. Loss of system functionality and operational effectiveness, for example, may result in loss of productive time, thus impeding the end users' performance of their functions in supporting the organization's mission.

- **Loss of Confidentiality.** System and data confidentiality refers to the protection of information from unauthorized disclosure. The impact of unauthorized disclosure of confidential information can range from the jeopardizing of national security to the disclosure of Privacy Act data. Unauthorized, unanticipated, or unintentional disclosure could result in loss of public confidence, embarrassment, or legal action against the organization.

The remainder of this guide is a risk assessment matrix, which you may use to analyze vulnerabilities, threats and the overall risk to your organization. We do not claim the following to be fully comprehensive. Our hope is that the risk assessment matrix will stimulate thought and help your organization to perform a thorough risk assessment.

Risk Assessment Matrix

Vulnerability	Threat	Risk Summary	Analysis / Recommendations
Risk management or risk assessments are not addressed by management in the course of their duties.	Unknown Threats / Risks	The organization is not proactive in addressing potential threats and associated risks.	
There is no information security policy that incorporates the key areas of security.	Malicious Acts	There is no clear security policy direction. No high-level definition of secure behavior exists.	
The information security policy is not kept up-to-date.	Malicious Acts	The security policy is no longer suitable, adequate, or effective.	
Employees are not aware of their responsibility to protect confidential information.	Malicious Acts	Informational assets may be used inappropriately allowing the system or data to be compromised.	
Background checks are not executed on employment candidates.	Malicious Acts	Unqualified and untrustworthy candidates may be hired increasing the risk of malicious behavior in the workplace.	
There is no clearly identified inventory of assets.	Infrastructure / Configuration	Critical components are not identified and applicable security controls are not applied.	
Employees receive no security awareness training.	Malicious Acts	Employees are not aware of information security threats, as well as their security related responsibilities.	

Risk Assessment Matrix (Continued)

Vulnerability	Threat	Risk Summary	Analysis / Recommendations
Employees, contractors and third party users do not surrender all of the organization's assets in their possession upon termination of their employment, contract or agreement?	Data leakage / Malicious Acts	Proprietary or other sensitive information may leave the organization with the possibility of future malicious acts.	
The organization relies on a "wet pipe" sprinkler system for fire suppression.	Availability	A burst water pipe in the ceiling could significantly damage equipment and the workplace environment.	
The air conditioning system in the data center is reaching capacity.	Availability	Critical devices could overheat resulting in downtime, equipment failure and loss of data.	
The data center's backup power supply may not be sufficient to ensure there is time for an orderly shutdown of equipment.	Availability	Equipment may incur stress because of a hard power cycle. Data could be lost because there is not enough time for machines to perform a "sync" or equivalent to flush cached or real time data.	
Telecommunications equipment do not have redundant routes?	Recovery / Availability	A single point of failure could result in a prolonged outage.	
Entrances and exits are not monitored, by personnel or video cameras.	Unauthorized Access	Facilities are susceptible to undetected intrusions resulting in theft, vandalism, or loss of confidential data.	

Risk Assessment Matrix (Continued)

Vulnerability	Threat	Risk Summary	Analysis / Recommendations
There are no motion sensors or burglar alarm systems enabled during non-working hours.	Unauthorized Access	Facilities are susceptible to undetected intrusions resulting in theft, vandalism, or loss of confidential data.	
Access to sensitive work areas is not logged and visitors are not appropriately badged.	Unauthorized Access	Unauthorized access to facilities may result in theft, vandalism or a network security breach.	
Sensitive data leaves the internal network via laptops, thumb drives and other mobile devices	Data Leakage / Malicious Acts	Weak security controls over mobile storage devices may lead to data loss.	
Unauthorized communications may penetrate the firewall and reach the internal network.	Malicious Acts	Intrusion attempts have a high success rate without correctly configured firewalls.	
The border firewall performs packet filtering, but lacks stateful inspection capabilities.	Malicious Acts	A stateless firewall examines each packet in isolation and is therefore susceptible to spoofing attacks.	
Unauthorized firewall rule changes are made.	Infrastructure / Configuration	Unauthorized changes may be introduced into the system. Even if the changes are not malicious in nature, they could cause unnecessary disruption if not reviewed and approved.	

Risk Assessment Matrix (Continued)

Vulnerability	Threat	Risk Summary	Analysis / Recommendations
There is no IDS/IPS system in place to effectively monitor and detect intrusion attempts or other malicious activity.	Malicious Acts	Malicious activity may go undetected.	
Network administrators use Telnet to access network devices.	Unauthorized Access	UserIDs and passwords are easily intercepted since credentials are sent in plain text.	
Certain network devices are accessed using default, vendor-supplied passwords.	Unauthorized Access	Default passwords are well-known and the network is easily breached unless passwords are changed from the default.	
Network vulnerability scans are not performed periodically.	Malicious Acts	Vulnerable network configurations and unpatched devices will not be detected, leaving the network open to attack.	
Log-on attempts are not captured and stored for accountability and audit requirements.	Malicious Acts	The investigation of a security breach may be unsuccessful if logging is not enabled.	
Event and security logs are not enabled on all network devices.	Malicious Acts	The investigation of a security breach may be unsuccessful if logging is not enabled on all network devices.	

Risk Assessment Matrix (Continued)

Vulnerability	Threat	Risk Summary	Analysis / Recommendations
Logs are not aggregated from multiple sources in order to track and alert on user access throughout the enterprise.	Malicious Acts	Malicious activity may go undetected if logs are not concentrated in a central location where they can be parsed and analyzed with the help of a third party tool.	
System and network logs are not retained for a sufficient period of time to allow for the successful auditing of historical events, to meet legal requirements, and also, if needed, for forensic purposes.	Malicious Acts	Past logs are not available for troubleshooting, resource tracking, and security if they are not stored or are overwritten.	
Virus protection software is not deployed on all devices susceptible to viruses or malware.	Malicious Acts	Computers not protected with antivirus software are susceptible to viruses, Trojans, keyloggers, hijackers, dialers, and other code that vandalizes or steals computer content.	
A Privacy Policy has not been developed and clearly communicated to all end users.	Data leakage / Disclosure	The organization's data and/or customer's data must be managed in a secure manner, or risk data disclosure and possible legal action.	
Sensitive information may be sent using the company's email system.	Data Leakage	Lack of policy and controls for email use exposes the organization to data leakage and possible regulatory non-compliance.	

Risk Assessment Matrix (Continued)

Vulnerability	Threat	Risk Summary	Analysis / Recommendations
Obsolete devices and media are not destroyed or otherwise made unusable by data wiping.	Data leakage / Malicious Acts	Sensitive information may be recovered and used for unauthorized purposes.	
Backup media may be lost or misplaced while in transit.	Data leakage / Malicious Acts	Lost backup media may be recovered and used for unauthorized purposes.	
Confidential data is not encrypted while stored or in transit.	Data leakage / Malicious Acts	Sensitive information may be intercepted and used for unauthorized purposes.	
Intruders may access company informational resources using the company's wireless network.	Unauthorized Access	Unauthorized access to the internal network is possible if the wireless network is not using secure protocols.	
The network is a flat architecture with no segmentation.	Infrastructure / Configuration	An intruder would have access to the entire network.	
Not all implemented network services are formally approved and authorized.	Infrastructure / Configuration	Unused or unnecessary services may be misconfigured allowing hackers entry into the system.	
No IDS/IPS system is deployed on the network.	Infrastructure / Configuration	Intrusion attempts may go undetected.	
Disaster recovery procedures are not tested periodically.	Recovery / Availability	The organization may not be able to recover business processes in a timely manner after an event.	

Risk Assessment Matrix (Continued)

Vulnerability	Threat	Risk Summary	Analysis / Recommendations
Backup tapes are not tested periodically for readability.	Recovery / Availability	Restoration of business processes would not be possible if backup tapes cannot be read.	
Network changes are not formally documented or approved.	Malicious Acts / Availability	Unauthorized changes may lead to network disruptions.	
Programming changes are not fully tested in a test environment prior to implementing the changes into the production environment.	Availability	Loss of productivity would result if changes need rework after implementation.	
Programmers are allowed update access to the production environment.	Malicious Acts	Improper segregation of duties increases the risk of fraud and other malicious activity.	
There is no formal change control methodology.	Malicious Acts / Availability	Unauthorized changes may be introduced into the system. Even if the changes are not malicious in nature, they could cause unnecessary disruption if not reviewed and approved.	
Password complexity and other password controls do not follow industry best practices.	Unauthorized Access	The network is more likely to be breached with lax password controls.	
Many departments use generic user IDs for various functions.	Unauthorized Access	Intentional misuse and inadvertent errors cannot be traced to unique individuals.	

Risk Assessment Matrix (Continued)

Vulnerability	Threat	Risk Summary	Analysis / Recommendations
User access rights are not revoked in a timely manner upon termination.	Unauthorized Access	Former employees may access informational resources.	
Provisioning of user access does not follow a formal user registration and approval procedure.	Unauthorized Access	Users' access may not be authorized and excessive access may be granted.	
Network and application access levels are not based on job responsibilities.	Malicious Acts	Segregation of duties will not be enforced increasing the risk of fraud and other malicious activities.	
Users acquire excess access rights over time because their level of access is not reviewed and adjusted accordingly after a job change or change in duties.	Malicious Acts	Segregation of duties will not be enforced increasing the risk of fraud and other malicious activities.	
Inactive user accounts are not disabled at regular, predefined intervals.	Unauthorized Access	Inactive accounts may be used for unauthorized network access.	
Network sessions are left unattended.	Malicious Acts / Data Leakage	Unattended terminals and workstations increase the risk of data loss and malicious activity.	
Physical access to facilities is available to terminated employees and former contractors.	Unauthorized Access	Unauthorized access to facilities poses a risk of theft, vandalism, or loss of confidential data.	

Risk Assessment Matrix (Continued)

Vulnerability	Threat	Risk Summary	Analysis / Recommendations
Business applications may contain undetected vulnerabilities.	Infrastructure / Configuration	Internally developed applications installed without code reviews and/or application vulnerability assessments may contain unknown vulnerabilities.	
Web-facing applications are not developed using industry standards such as OWASP.	Infrastructure / Configuration	Unsecure applications may be introduced in the production environment.	
Servers are built without following any configuration standards or a formalized hardening process.	Infrastructure / Configuration	Servers may not be in a secure state when introduced into the production environment.	
Software patches are installed piecemeal. There is no particular software update management process.	Infrastructure / Configuration	Unpatched applications, operating systems and databases are targets for intruders.	
Software developers lack training in secure coding practices.	Infrastructure / Configuration	Poorly written applications with security vulnerabilities may be introduced into the production environment.	
Network sessions are left unattended.	Malicious Acts / Data Leakage	Unattended terminals and workstations increase the risk of data loss and malicious activity.	

Risk Assessment Matrix (Continued)

Vulnerability	Threat	Risk Summary	Analysis / Recommendations
Applications developed internally, as well as third-party applications, may contain undetected security risks or vulnerabilities.	Infrastructure / Configuration	Applications installed without code reviews and/or application vulnerability assessments may contain unknown vulnerabilities.	
If a security breach or incident should occur, it may take time for personnel to react and decide on a course of action.	Data Loss / Recovery / Availability	A lack of incident response procedures may result in increased downtime and/or data loss.	
Not all business critical systems are identified.	Unknown Threats / Risks	Systems not under centralized control of IT may not have appropriate security controls in place.	
Should a business interruption occur, it may take time for personnel to react and decide on a course of action.	Recovery / Availability	A lack of documented disaster recovery procedures may increase the time required to restore business functions.	
The disaster recovery plan is not tested regularly.	Recovery / Availability	Untested disaster recovery plans may fail during an actual event.	
Disaster recovery documentation is out-of-date.	Recovery / Availability	Out-of-date disaster recovery plans may fail during an actual event.	

Risk Assessment Matrix (Continued)

Vulnerability	Threat	Risk Summary	Analysis / Recommendations
There is no data retention policy.	Availability	Needs for data retention are not specified, based on: 1) Legal requirements 2) Business requirements 3) Personal requirements The organization could be accused of negligence if electronic evidence cannot be produced.	
Not all data has a specified data owner.	Unauthorized Access / Availability	There is no one to determine how much risk to accept and who is permitted to access the information.	
There are no requirements for confidentiality or non-disclosure agreements.	Data Leakage	Confidential information is not legally protected from disclosure.	
Third-parties do not have adequate security policies and procedures in place and leave the company's confidential data in their possession susceptible to compromise.	Data Leakage	The organization's data is susceptible to unauthorized or accidental modification, damage, destruction, or disclosure.	
The company is not in compliance with HIPAA, PCI and other regulatory mandates.	Regulatory Noncompliance	Penalties, fines and loss of goodwill may result from noncompliant business practices and IT systems.	

KirkpatrickPrice

Kirkpatrick Price, LLC
1228 East 7th Ave., Suite 200
Tampa, FL 33605
800.977.3154

v2.1_3.2011