KirkpatrickPrice

PRISM INTERNATIONAL

Risk Assessment Guide

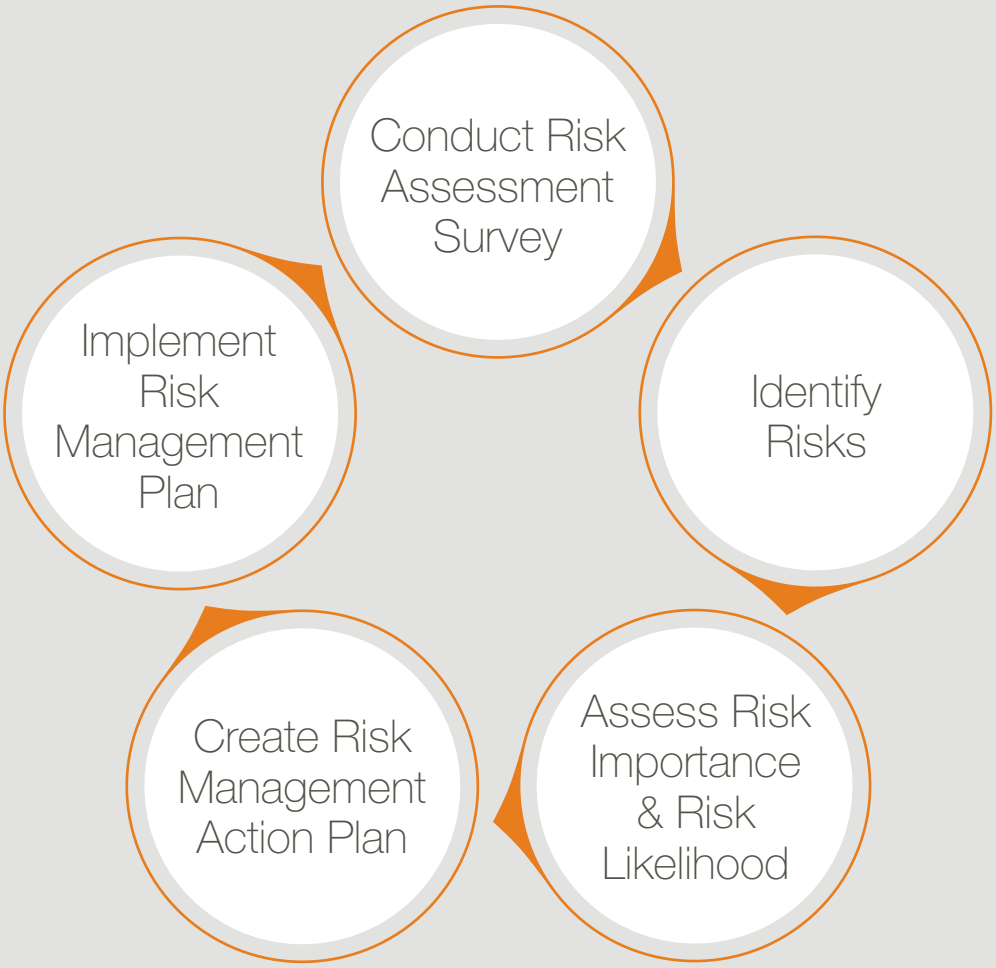
Designed Exclusively for PRISM International Members

KirkpatrickPrice. | innovation. integrity. delivered.

1.2012

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.

Function:
Storing customer information in IT database(s)

Type of threat	Type of vulnerability	Risk importance 1=low 2=med 3=high	Risk likelihood 1=unlikely 2=possible 3=probable	Control recommendation
Confidentiality	Viruses or malware attacking servers/PCs			Anti-virus and anti-malware utilities installed on all servers and PCs
Confidentiality	Hacker attacking through public Internet or wireless connections			Firewall installed at each Internet connection and between any wireless network
Confidentiality	Unknown publicly available vulnerabilities			External vulnerability scans performed quarterly
Confidentiality	Release of patches or exploits that notify hackers of potential problems			Patch management performed quarterly and within 30 days of critical releases
Confidentiality	Unintended access to unauthorized employees			Company employees' access privileges are limited based on job function
Confidentiality	Weak passwords that unauthorized individuals or programs could guess			Network is configured to enforce strong password construction (at least 7 characters, alpha/numeric, requiring at least one special character)
Confidentiality	Perpetual access to systems with compromised passwords			Company employees' network passwords are changed at least every 60 days
Confidentiality	Old or unnecessary accounts are still available for access			Company has a formal process for terminating employees which includes removal of access to IT network resources

Function:
Storing customer information in IT database(s) *(Continued)*

Type of threat	Type of vulnerability	Risk importance 1=low 2=med 3=high	Risk likelihood 1=unlikely 2=possible 3=probable	Control recommendation
Availability	Data lost and irretrievable			Database(s) backed up nightly, and tested monthly for restore capability
Availability	Data lost due to sudden power loss			Battery backup is in place
Availability	Data lost due to environmental pressures (such as temperature)			Proper cooling systems are installed in data center or server room to prevent overheating
Availability	Data lost due to fire			Fire detection and suppression systems in place in data center or server room
Integrity	Data lost due to employee or system error			Annual auditing of item locations in database versus physical locations

Function: Providing online customer access to information in IT database(s)

Type of threat	Type of vulnerability	Risk importance 1=low 2=med 3=high	Risk likelihood 1=unlikely 2=possible 3=probable	Control recommendation
Confidentiality	Data leaking through unencrypted Internet browser session			Secure socket layer encryption used during online access
Confidentiality	Unauthorized parties accessing online accounts			Access accounts are password protected
Confidentiality	Unauthorized parties posing as legitimate users			Access accounts are set up only after users provide valid authentication
Availability	Services unavailable due to loss of Internet connectivity			Backup Internet connection in place

Function: Storing customer records and information in company facilities

Type of threat	Type of vulnerability	Risk importance 1=low 2=med 3=high	Risk likelihood 1=unlikely 2=possible 3=probable	Control recommendation
Confidentiality	Unauthorized parties entering sensitive areas			All facility entrances are locked
Confidentiality	Unauthorized entry goes unnoticed			All entrances monitored by video surveillance, receptionist/guard and/or entrance tracked by access cards
Confidentiality	Unauthorized entry notice is delayed			Facility alarmed and third-party monitored
Confidentiality	Unknown parties enter sensitive areas			All facility visitors provide valid ID, sign a log book and are escorted by a company employee while on premises
Confidentiality	Malicious individuals working for vendors commit theft of information or disclose sensitive details			All vendors with access to facilities are contractually bound to privacy obligations, or are escorted by a company employee while on premises
Availability	Data loss due to fire			Fire suppression in place in all areas where employee information stored
Availability	Data loss due to flood			Facility located outside of flood plain areas
Availability	Data loss or lack of access due to power outage			Backup generator installed / Company has on-call relationship with third party capable of providing emergency power
Availability	Data inaccessible due to chemical spill or disaster			Facility located away from sources of toxic substances

Function: Storing customer records and information in company facilities *(Continued)*

Type of threat	Type of vulnerability	Risk importance 1=low 2=med 3=high	Risk likelihood 1=unlikely 2=possible 3=probable	Control recommendation
Integrity	Data irretrievable due to damage			Company has on-call relationship with third party capable of assisting with document preservation and remediation
Integrity	Data damaged due to inadvertent water damage from fire suppression systems			Company employees trained at least annually on responding to accidental discharge of sprinkler system

Function: Transporting customer records and information in company vehicles

Type of threat	Type of vulnerability	Risk importance 1=low 2=med 3=high	Risk likelihood 1=unlikely 2=possible 3=probable	Control recommendation
Confidentiality	Data stolen from delivery vehicle			All vehicles have distinct cargo area that is not accessible from driver cabin
Confidentiality	Data stolen due to employee forgetting to lock the cargo area of a vehicle			All vehicle cargo areas have self-locking mechanisms
Confidentiality	Thief attempting break-in of vehicle			All vehicles equipped with audible alarms
Confidentiality	Data lost due to vehicle theft			All vehicles equipped with GPS systems
Availability	Data availability delayed due to impounding			All vehicles are properly licensed and identified with company details (to prevent towing)
Integrity	Data damaged due to environmental conditions			All vehicle cargo areas are climate controlled (for vehicles transporting computer media)

Function: Handling of customer records and information by company employees

Type of threat	Type of vulnerability	Risk importance 1=low 2=med 3=high	Risk likelihood 1=unlikely 2=possible 3=probable	Control recommendation
Confidentiality	Untrusted employee steals information			Company performs background checks on all employees
Confidentiality	Employees access information with no contractual obligations assigned			All employees sign confidentiality agreements
Confidentiality	Employees do not understand privacy responsibilities			All employees receive privacy training at least annually and within 30 days of hiring
Integrity	Data loss due to lack of employee understanding of job responsibilities			Employees receive training on company policies and procedures at least annually and within 30 days of hiring
Integrity	Mistakes and procedural flaws go unnoticed			Employee activities related to handling customer records and information are regularly audited
Availability	Employees are unavailable to work during pandemic			Company encourages vaccination against disease by making vaccinations available at company expense
Availability	Employees are contagious during pandemic			Hand sanitizers installed in all facilities to help prevent disease spread

Risk Assessment History

Revision date:	**01/24/2012**
Original effective date:	
Last full review:	
Next full review:	

KirkpatrickPrice

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