IT Security Management

Risk Analysis and Controls

Steven Gordon

Document No:
Revision 770

3 December 2013

1 Introduction

This document summarises several steps of an IT security risk analysis and subsequent implementation of security controls. Most of the material is based on the following sources:

- Stallings and Brown, *Computer Security: Principles and Practice*, 2nd Edition, Pearson Education, 2012. Specifically chapters 14 and 15.
- NIST, *Standards for Security Categorization of Federal Information and Information Systems*, FIPS PUB 199, February 2004.
- NIST, *Guidelines for Conducting Risk Assessments*, Special Publication 800-30 Revision 1, September 2012.
- NIST, *Security and Privacy Controls for Federal Information Systems and Organizations*, Special Publication 800-53, Revision 4, April 2013.

The above sources (as well as the other standards that they refer to) describe detailed methodologies for IT security risk analysis and implementing security controls. This document selects parts from these methodologies that are suitable for performing a simplified risk analysis for IT security students.

Most of the figures, tables and text are copied directly from the original NIST standards (which as US Government works, are in the public domain).

2 IT Security Management

Figure 1, taken from Stallings and Brown, presents an overview of IT security management. From the top, an IT security policy and aspects of the organisation are initial inputs to a risk analysis. The risk analysis can be performed in several ways: baseline, informal, formal, or combined. From the risk analysis a set of security controls should

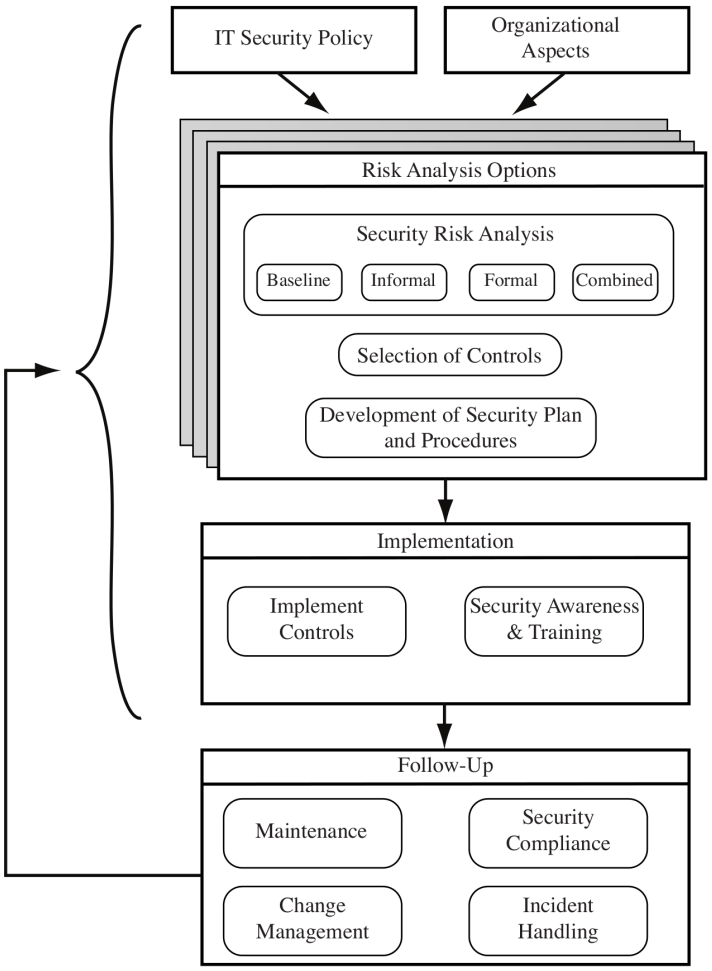

Figure 1: An Overview of IT Security Management [Figure 14.1 from Stallings and Brown]

be selected for the organisation and a plan and procedure for implementing the controls prepared.

The selected controls are implemented, employees made aware of the security issues and given appropriate training. There are several follow-up steps which may lead to further risk analysis and implementation changes.

This document focusses on three parts:

1. The inputs to the risk analysis, specifically a categorization of the information systems in an organisation based on their security objectives (Section 3).

2. The formal risk analysis (Section 4).

3. The security controls that are available for selection and implementation (Section 5).

3 Security Categorization

NIST, in FIPS 199, present a method for categorizing information and information systems based on security objectives. The three *security objectives* defined are:

Confidentiality: Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information. A loss of confidentiality is the unauthorized disclosure of information.

Integrity: Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity. A loss of integrity is the unauthorized modification or destruction of information.

Availability: Ensuring timely and reliable access to and use of information. A loss of availability is the disruption of access to or use of information or an information system.

There are three levels of *potential impact* on organisations and individuals if a security breach occurs:

Low: The loss of confidentiality, integrity, or availability could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals.

Moderate: The loss of confidentiality, integrity, or availability could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals.

High: The loss of confidentiality, integrity, or availability could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals.

A security category, SC, is applied for different *information types*, which assigns a potential impact to each of the objectives for that information type. The general format is:

$$\mathrm{SC}_{\mathit{informationtype}} = \{(\text{confidentialty}, \mathit{impact}), (\text{integrity}, \mathit{impact}), (\text{availability}, \mathit{impact})\}$$

Examples of information types include: user data on a website, student records, financial records, personnel information. Examples of categorizations are given in FIPS 199.

An information system may have multiple types of information. From the security categorization of the different information types, a security categorization of the information system can be specified:

$$\mathrm{SC}_{\mathit{informationsystem}} = \{(\text{confidentialty}, \mathit{impact}), (\text{integrity}, \mathit{impact}), (\text{availability}, \mathit{impact})\}$$

The potential impact for the information system is the highest (maximum) value from the set of information types in the system for that objective. For example, consider a student management system that contains two information types with categorizations:

$$\mathrm{SC}_{\text{grades}} = \{(\text{confidentialty}, \text{moderate}), (\text{integrity}, \text{high}), (\text{availability}, \text{low})\}$$

$$\mathrm{SC}_{\text{contactinfo}} = \{(\text{confidentialty}, \text{moderate}), (\text{integrity}, \text{low}), (\text{availability}, \text{low})\}$$

For the confidentiality objective, both impacts are moderate, giving the highest value of moderate. Hence the potential impact for the information system is moderate. For integrity, although one impact is low, the other is high, so the highest value, high, is the potential impact for the information system.

$$\mathrm{SC}_{\mathrm{studentsystem}} = \{(\mathrm{confidentialty}, \mathrm{moderate}), (\mathrm{integrity}, \mathrm{high}), (\mathrm{availability}, \mathrm{low})\}$$

Further examples are in FIPS 199.

4 Risk Analysis

A simplified risk analysis consists of:

1. Identify assets that need protection. Assets include computer and communications hardware, software, data, documentation, and the people who manage these systems.

2. Identify threats and vulnerabilities. Threats come from particular sources. Table 1 classifies typical threat sources. Sources and threats may be adversarial (i.e. others trying to gain advantage from an attack) or non-adversarial (e.g. due to your own mistakes). A list of adversarial threat events (attacks), split across five tables (Tables 2 to 6), is given. Non-adversarial threat events are listed in Table 7.

3. Determine the likelihood of threat events occuring. The likelihood depends on many factors, but a simple view is to give each threat event a ranking from Very Low to Very High in terms of likelihood of it being initiated (see Tables 8 and 9), and then ranking the likelihood that if it occurs, it will have adverse impacts (see Table 10). From the likelihood of occurring and likelihood of having adverse impacts, an overall likelihood can be determined (see Tables 11).

4. Calculate the level of risk for each event. The overall likelihood from the previous step is used, as well as a rating (from Very Low to Very High) if the impact on the organisation if the threat event occurs. Table 12 lists examples of impacts, while Table 13 gives the rating levels for impact. The risk level can then be determined using Table 14. The risk levels are further described in Table 15.

Once the risk analysis has been performed a security plan can be designed. The security plan should identify possible mechanisms that can be used to remove/minimize the risk from the set of threats. These mechanisms are referred to as *security controls*. Once the set of security controls are know, the threats should be ranked based upon the level of risk and the cost of implementing the controls. The ranking is used to determine which controls will be implemented. Ideally threats with highest risk will be addressed with security controls first, however the cost of implementing the controls must also be considered.

Section 5 lists some of the security controls available.

Type of Threat Source	Description	Characteristics

ADVERSARIAL
- Individual
  - Outsider
  - Insider
  - Trusted Insider
  - Privileged Insider
- Group
  - Ad hoc
  - Established
- Organization
  - Competitor
  - Supplier
  - Partner
  - Customer
- Nation-State
	Individuals, groups, organizations, or states that seek to exploit the organization's dependence on cyber resources (i.e., information in electronic form, information and communications technologies, and the communications and information-handling capabilities provided by those technologies).	Capability, Intent, Targeting

ACCIDENTAL - User - Privileged User/Administrator	Erroneous actions taken by individuals in the course of executing their everyday responsibilities.	Range of effects

STRUCTURAL
- Information Technology (IT) Equipment
  - Storage
  - Processing
  - Communications
  - Display
  - Sensor
  - Controller
- Environmental Controls
  - Temperature/Humidity Controls
  - Power Supply
- Software
  - Operating System
  - Networking
  - General-Purpose Application
  - Mission-Specific Application
	Failures of equipment, environmental controls, or software due to aging, resource depletion, or other circumstances which exceed expected operating parameters.	Range of effects

ENVIRONMENTAL
- Natural or man-made disaster
  - Fire
  - Flood/Tsunami
  - Windstorm/Tornado
  - Hurricane
  - Earthquake
  - Bombing
  - Overrun
- Unusual Natural Event (e.g., sunspots)
- Infrastructure Failure/Outage
  - Telecommunications
  - Electrical Power
	Natural disasters and failures of critical infrastructures on which the organization depends, but which are outside the control of the organization.
	Note: Natural and man-made disasters can also be characterized in terms of their severity and/or duration. However, because the threat source and the threat event are strongly identified, severity and duration can be included in the description of the threat event (e.g., Category 5 hurricane causes extensive damage to the facilities housing mission-critical systems, making those systems unavailable for three weeks).
		Range of effects

Table 1: Taxonomy of Threat Sources [Table D2 from SP800-30]

Threat Events (Characterized by TTPs)	Description
Perform reconnaissance and gather information.	
Perform perimeter network reconnaissance/scanning.	Adversary uses commercial or free software to scan organizational perimeters to obtain a better understanding of the information technology infrastructure and improve the ability to launch successful attacks.
Perform network sniffing of exposed networks.	Adversary with access to exposed wired or wireless data channels used to transmit information, uses network sniffing to identify components, resources, and protections.
Gather information using open source discovery of organizational information.	Adversary mines publically accessible information to gather information about organizational information systems, business processes, users or personnel, or external relationships that the adversary can subsequently employ in support of an attack.
Perform reconnaissance and surveillance of targeted organizations.	Adversary uses various means (e.g., scanning, physical observation) over time to examine and assess organizations and ascertain points of vulnerability.
Perform malware-directed internal reconnaissance.	Adversary uses malware installed inside the organizational perimeter to identify targets of opportunity. Because the scanning, probing, or observation does not cross the perimeter, it is not detected by externally placed intrusion detection systems.
Craft or create attack tools.	
Craft phishing attacks.	Adversary counterfeits communications from a legitimate/trustworthy source to acquire sensitive information such as usernames, passwords, or SSNs. Typical attacks occur via email, instant messaging, or comparable means; commonly directing users to websites that appear to be legitimate sites, while actually stealing the entered information.
Craft spear phishing attacks.	Adversary employs phishing attacks targeted at high value targets (e.g., senior leaders/executives).
Craft attacks specifically based on deployed information technology environment.	Adversary develops attacks (e.g., crafts targeted malware) that take advantage of adversary knowledge of the organizational information technology environment.
Create counterfeit/spoof website.	Adversary creates duplicates of legitimate websites; when users visit a counterfeit site, the site can gather information or download malware.
Craft counterfeit certificates.	Adversary counterfeits or compromises a certificate authority, so that malware or connections will appear legitimate.
Create and operate false front organizations to inject malicious components into the supply chain.	Adversary creates false front organizations with the appearance of legitimate suppliers in the critical life-cycle path that then inject corrupted/malicious information system components into the organizational supply chain.
Deliver/insert/install malicious capabilities.	
Deliver known malware to internal organizational information systems (e.g., virus via email).	Adversary uses common delivery mechanisms (e.g., email) to install/insert known malware (e. g., malware whose existence is known) into organizational information systems.
Deliver modified malware to internal organizational information systems.	Adversary uses more sophisticated delivery mechanisms than email (e.g., web traffic, instant messaging, FTP) to deliver malware and possibly modifications of known malware to gain access to internal organizational information systems.
Deliver targeted malware for control of internal systems and exfiltration of data.	Adversary installs malware that is specifically designed to take control of internal organizational information systems, identify sensitive information, exfiltrate the information back to adversary, and conceal these actions.
Deliver malware by providing removable media.	Adversary places removable media (e.g., flash drives) containing malware in locations external to organizational physical perimeters but where employees are likely to find the media (e.g., facilities parking lots, exhibits at conferences attended by employees) and use it on organizational information systems.

Table 2: Adversarial Threat Events a [Table E2 from SP800-30]

Threat Events (Characterized by TTPs)	**Description**
Insert untargeted malware into downloadable software and/or into commercial information technology products.	Adversary corrupts or inserts malware into common freeware, shareware or commercial information technology products. Adversary is not targeting specific organizations, simply looking for entry points into internal organizational information systems. Note that this is particularly a concern for mobile applications.
Insert targeted malware into organizational information systems and information system components.	Adversary inserts malware into organizational information systems and information system components (e.g., commercial information technology products), specifically targeted to the hardware, software, and firmware used by organizations (based on knowledge gained via reconnaissance).
Insert specialized malware into organizational information systems based on system configurations.	Adversary inserts specialized, non-detectable, malware into organizational information systems based on system configurations, specifically targeting critical information system components based on reconnaissance and placement within organizational information systems.
Insert counterfeit or tampered hardware into the supply chain.	Adversary intercepts hardware from legitimate suppliers. Adversary modifies the hardware or replaces it with faulty or otherwise modified hardware.
Insert tampered critical components into organizational systems.	Adversary replaces, though supply chain, subverted insider, or some combination thereof, critical information system components with modified or corrupted components.
Install general-purpose sniffers on organization-controlled information systems or networks.	Adversary installs sniffing software onto internal organizational information systems or networks.
Install persistent and targeted sniffers on organizational information systems and networks.	Adversary places within internal organizational information systems or networks software designed to (over a continuous period of time) collect (sniff) network traffic.
Insert malicious scanning devices (e.g., wireless sniffers) inside facilities.	Adversary uses postal service or other commercial delivery services to deliver to organizational mailrooms a device that is able to scan wireless communications accessible from within the mailrooms and then wirelessly transmit information back to adversary.
Insert subverted individuals into organizations.	Adversary places individuals within organizations who are willing and able to carry out actions to cause harm to organizational missions/business functions.
Insert subverted individuals into privileged positions in organizations.	Adversary places individuals in privileged positions within organizations who are willing and able to carry out actions to cause harm to organizational missions/business functions. Adversary may target privileged functions to gain access to sensitive information (e.g., user accounts, system files, etc.) and may leverage access to one privileged capability to get to another capability.
Exploit and compromise.	
Exploit physical access of authorized staff to gain access to organizational facilities.	Adversary follows ("tailgates") authorized individuals into secure/controlled locations with the goal of gaining access to facilities, circumventing physical security checks.
Exploit poorly configured or unauthorized information systems exposed to the Internet.	Adversary gains access through the Internet to information systems that are not authorized for Internet connectivity or that do not meet organizational configuration requirements.
Exploit split tunneling.	Adversary takes advantage of external organizational or personal information systems (e.g., laptop computers at remote locations) that are simultaneously connected securely to organizational information systems or networks and to nonsecure remote connections.
Exploit multi-tenancy in a cloud environment.	Adversary, with processes running in an organizationally-used cloud environment, takes advantage of multi-tenancy to observe behavior of organizational processes, acquire organizational information, or interfere with the timely or correct functioning of organizational processes.
Exploit known vulnerabilities in mobile systems (e.g., laptops, PDAs, smart phones).	Adversary takes advantage of fact that transportable information systems are outside physical protection of organizations and logical protection of corporate firewalls, and compromises the systems based on known vulnerabilities to gather information from those systems.
Exploit recently discovered vulnerabilities.	Adversary exploits recently discovered vulnerabilities in organizational information systems in an attempt to compromise the systems before mitigation measures are available or in place.

Table 3: Adversarial Threat Events b [Table E2 from SP800-30]

Threat Events (Characterized by TTPs)	Description
Exploit vulnerabilities on internal organizational information systems.	Adversary searches for known vulnerabilities in organizational internal information systems and exploits those vulnerabilities.
Exploit vulnerabilities using zero-day attacks.	Adversary employs attacks that exploit as yet unpublicized vulnerabilities. Zero-day attacks are based on adversary insight into the information systems and applications used by organizations as well as adversary reconnaissance of organizations.
Exploit vulnerabilities in information systems timed with organizational mission/business operations tempo.	Adversary launches attacks on organizations in a time and manner consistent with organizational needs to conduct mission/business operations.
Exploit insecure or incomplete data deletion in multi-tenant environment.	Adversary obtains unauthorized information due to insecure or incomplete data deletion in a multi-tenant environment (e.g., in a cloud computing environment).
Violate isolation in multi-tenant environment.	Adversary circumvents or defeats isolation mechanisms in a multi-tenant environment (e.g., in a cloud computing environment) to observe, corrupt, or deny service to hosted services and information/data.
Compromise critical information systems via physical access.	Adversary obtains physical access to organizational information systems and makes modifications.
Compromise information systems or devices used externally and reintroduced into the enterprise.	Adversary installs malware on information systems or devices while the systems/devices are external to organizations for purposes of subsequently infecting organizations when reconnected.
Compromise software of organizational critical information systems.	Adversary inserts malware or otherwise corrupts critical internal organizational information systems.
Compromise organizational information systems to facilitate exfiltration of data/information.	Adversary implants malware into internal organizational information systems, where the malware over time can identify and then exfiltrate valuable information.
Compromise mission-critical information.	Adversary compromises the integrity of mission-critical information, thus preventing or impeding ability of organizations to which information is supplied, from carrying out operations.
Compromise design, manufacture, and/or distribution of information system components (including hardware, software, and firmware).	Adversary compromises the design, manufacture, and/or distribution of critical information system components at selected suppliers.
Conduct an attack (i.e., direct/coordinate attack tools or activities).	
Conduct communications interception attacks.	Adversary takes advantage of communications that are either unencrypted or use weak encryption (e.g., encryption containing publically known flaws), targets those communications, and gains access to transmitted information and channels.
Conduct wireless jamming attacks.	Adversary takes measures to interfere with wireless communications so as to impede or prevent communications from reaching intended recipients.
Conduct attacks using unauthorized ports, protocols and services.	Adversary conducts attacks using ports, protocols, and services for ingress and egress that are not authorized for use by organizations.
Conduct attacks leveraging traffic/data movement allowed across perimeter.	Adversary makes use of permitted information flows (e.g., email communication, removable storage) to compromise internal information systems, which allows adversary to obtain and exfiltrate sensitive information through perimeters.
Conduct simple Denial of Service (DoS) attack.	Adversary attempts to make an Internet-accessible resource unavailable to intended users, or prevent the resource from functioning efficiently or at all, temporarily or indefinitely.
Conduct Distributed Denial of Service (DDoS) attacks.	Adversary uses multiple compromised information systems to attack a single target, thereby causing denial of service for users of the targeted information systems.
Conduct targeted Denial of Service (DoS) attacks.	Adversary targets DoS attacks to critical information systems, components, or supporting infrastructures, based on adversary knowledge of dependencies.
Conduct physical attacks on organizational facilities.	Adversary conducts a physical attack on organizational facilities (e.g., sets a fire).
Conduct physical attacks on infrastructures supporting organizational facilities.	Adversary conducts a physical attack on one or more infrastructures supporting organizational facilities (e.g., breaks a water main, cuts a power line).
Conduct cyber-physical attacks on organizational facilities.	Adversary conducts a cyber-physical attack on organizational facilities (e.g., remotely changes HVAC settings).

Table 4: Adversarial Threat Events c [Table E2 from SP800-30]

Threat Events (Characterized by TTPs)	**Description**
Conduct data scavenging attacks in a cloud environment.	Adversary obtains data used and then deleted by organizational processes running in a cloud environment.
Conduct brute force login attempts/password guessing attacks.	Adversary attempts to gain access to organizational information systems by random or systematic guessing of passwords, possibly supported by password cracking utilities.
Conduct nontargeted zero-day attacks.	Adversary employs attacks that exploit as yet unpublicized vulnerabilities. Attacks are not based on any adversary insights into specific vulnerabilities of organizations.
Conduct externally-based session hijacking.	Adversary takes control of (hijacks) already established, legitimate information system sessions between organizations and external entities (e.g., users connecting from off-site locations).
Conduct internally-based session hijacking.	Adversary places an entity within organizations in order to gain access to organizational information systems or networks for the express purpose of taking control (hijacking) an already established, legitimate session either between organizations and external entities (e.g., users connecting from remote locations) or between two locations within internal networks.
Conduct externally-based network traffic modification (man in the middle) attacks.	Adversary, operating outside organizational systems, intercepts/eavesdrops on sessions between organizational and external systems. Adversary then relays messages between organizational and external systems, making them believe that they are talking directly to each other over a private connection, when in fact the entire communication is controlled by the adversary. Such attacks are of particular concern for organizational use of community, hybrid, and public clouds.
Conduct internally-based network traffic modification (man in the middle) attacks.	Adversary operating within the organizational infrastructure intercepts and corrupts data sessions.
Conduct outsider-based social engineering to obtain information.	Externally placed adversary takes actions (e.g., using email, phone) with the intent of persuading or otherwise tricking individuals within organizations into revealing critical/sensitive information (e.g., personally identifiable information).
Conduct insider-based social engineering to obtain information.	Internally placed adversary takes actions (e.g., using email, phone) so that individuals within organizations reveal critical/sensitive information (e.g., mission information).
Conduct attacks targeting and compromising personal devices of critical employees.	Adversary targets key organizational employees by placing malware on their personally owned information systems and devices (e.g., laptop/notebook computers, personal digital assistants, smart phones). The intent is to take advantage of any instances where employees use personal information systems or devices to handle critical/sensitive information.
Conduct supply chain attacks targeting and exploiting critical hardware, software, or firmware.	Adversary targets and compromises the operation of software (e.g., through malware injections), firmware, and hardware that performs critical functions for organizations. This is largely accomplished as supply chain attacks on both commercial off-the-shelf and custom information systems and components.
Achieve results (i.e., cause adverse impacts, obtain information)	
Obtain sensitive information through network sniffing of external networks.	Adversary with access to exposed wired or wireless data channels that organizations (or organizational personnel) use to transmit information (e.g., kiosks, public wireless networks) intercepts communications.
Obtain sensitive information via exfiltration.	Adversary directs malware on organizational systems to locate and surreptitiously transmit sensitive information.
Cause degradation or denial of attacker-selected services or capabilities.	Adversary directs malware on organizational systems to impair the correct and timely support of organizational mission/business functions.
Cause deterioration/destruction of critical information system components and functions.	Adversary destroys or causes deterioration of critical information system components to impede or eliminate organizational ability to carry out missions or business functions. Detection of this action is not a concern.
Cause integrity loss by creating, deleting, and/or modifying data on publicly accessible information systems (e.g., web defacement).	Adversary vandalizes, or otherwise makes unauthorized changes to, organizational websites or data on websites.
Cause integrity loss by polluting or corrupting critical data.	Adversary implants corrupted and incorrect data in critical data, resulting in suboptimal actions or loss of confidence in organizational data/services.

Table 5: Adversarial Threat Events d [Table E2 from SP800-30]

Threat Events (Characterized by TTPs)	Description
Cause integrity loss by injecting false but believable data into organizational information systems.	Adversary injects false but believable data into organizational information systems, resulting in suboptimal actions or loss of confidence in organizational data/services.
Cause disclosure of critical and/or sensitive information by authorized users.	Adversary induces (e.g., via social engineering) authorized users to inadvertently expose, disclose, or mishandle critical/sensitive information.
Cause unauthorized disclosure and/or unavailability by spilling sensitive information.	Adversary contaminates organizational information systems (including devices and networks) by causing them to handle information of a classification/sensitivity for which they have not been authorized. The information is exposed to individuals who are not authorized access to such information, and the information system, device, or network is unavailable while the spill is investigated and mitigated.
Obtain information by externally located interception of wireless network traffic.	Adversary intercepts organizational communications over wireless networks. Examples include targeting public wireless access or hotel networking connections, and drive-by subversion of home or organizational wireless routers.
Obtain unauthorized access.	Adversary with authorized access to organizational information systems, gains access to resources that exceeds authorization.
Obtain sensitive data/information from publicly accessible information systems.	Adversary scans or mines information on publically accessible servers and web pages of organizations with the intent of finding sensitive information.
Obtain information by opportunistically stealing or scavenging information systems/components.	Adversary steals information systems or components (e. g., laptop computers or data storage media) that are left unattended outside of the physical perimeters of organizations, or scavenges discarded components.
Maintain a presence or set of capabilities.	
Obfuscate adversary actions.	Adversary takes actions to inhibit the effectiveness of the intrusion detection systems or auditing capabilities within organizations.
Adapt cyber attacks based on detailed surveillance.	Adversary adapts behavior in response to surveillance and organizational security measures.
Coordinate a campaign.	
Coordinate a campaign of multi-staged attacks (e.g., hopping).	Adversary moves the source of malicious commands or actions from one compromised information system to another, making analysis difficult.
Coordinate a campaign that combines internal and external attacks across multiple information systems and information technologies.	Adversary combines attacks that require both physical presence within organizational facilities and cyber methods to achieve success. Physical attack steps may be as simple as convincing maintenance personnel to leave doors or cabinets open.
Coordinate campaigns across multiple organizations to acquire specific information or achieve desired outcome.	Adversary does not limit planning to the targeting of one organization. Adversary observes multiple organizations to acquire necessary information on targets of interest.
Coordinate a campaign that spreads attacks across organizational systems from existing presence.	Adversary uses existing presence within organizational systems to extend the adversary's span of control to other organizational systems including organizational infrastructure. Adversary thus is in position to further undermine organizational ability to carry out missions/business functions.
Coordinate a campaign of continuous, adaptive, and changing cyber attacks based on detailed surveillance.	Adversary attacks continually change in response to surveillance and organizational security measures.
Coordinate cyber attacks using external (outsider), internal (insider), and supply chain (supplier) attack vectors.	Adversary employs continuous, coordinated attacks, potentially using all three attack vectors for the purpose of impeding organizational operations.

Table 6: Adversarial Threat Events e [Table E2 from SP800-30]

Threat Event	Description
Spill sensitive information	Authorized user erroneously contaminates a device, information system, or network by placing on it or sending to it information of a classification/sensitivity which it has not been authorized to handle. The information is exposed to access by unauthorized individuals, and as a result, the device, system, or network is unavailable while the spill is investigated and mitigated.
Mishandling of critical and/or sensitive information by authorized users	Authorized privileged user inadvertently exposes critical/sensitive information.
Incorrect privilege settings	Authorized privileged user or administrator erroneously assigns a user exceptional privileges or sets privilege requirements on a resource too low.
Communications contention	Degraded communications performance due to contention.
Unreadable display	Display unreadable due to aging equipment.
Earthquake at primary facility	Earthquake of organization-defined magnitude at primary facility makes facility inoperable.
Fire at primary facility	Fire (not due to adversarial activity) at primary facility makes facility inoperable.
Fire at backup facility	Fire (not due to adversarial activity) at backup facility makes facility inoperable or destroys backups of software, configurations, data, and/or logs.
Flood at primary facility	Flood (not due to adversarial activity) at primary facility makes facility inoperable.
Flood at backup facility	Flood (not due to adversarial activity) at backup facility makes facility inoperable or destroys backups of software, configurations, data, and/or logs.
Hurricane at primary facility	Hurricane of organization-defined strength at primary facility makes facility inoperable.
Hurricane at backup facility	Hurricane of organization-defined strength at backup facility makes facility inoperable or destroys backups of software, configurations, data, and/or logs.
Resource depletion	Degraded processing performance due to resource depletion.
Introduction of vulnerabilities into software products	Due to inherent weaknesses in programming languages and software development environments, errors and vulnerabilities are introduced into commonly used software products.
Disk error	Corrupted storage due to a disk error.
Pervasive disk error	Multiple disk errors due to aging of a set of devices all acquired at the same time, from the same supplier.
Windstorm/tornado at primary facility	Windstorm/tornado of organization-defined strength at primary facility makes facility inoperable.
Windstorm/tornado at backup facility	Windstorm/tornado of organization-defined strength at backup facility makes facility inoperable or destroys backups of software, configurations, data, and/or logs.

Table 7: Non-Adversarial Threat Events [Table E3 from SP800-30]

Qualitative Values	Semi-Quantitative Values		Description
Very High	96-100	10	Adversary is **almost certain** to initiate the threat event.
High	80-95	8	Adversary is **highly likely** to initiate the threat event.
Moderate	21-79	5	Adversary is **somewhat likely** to initiate the treat event.
Low	5-20	2	Adversary is **unlikely** to initiate the threat event.
Very Low	0-4	0	Adversary is **highly unlikely** to initiate the threat event.

Table 8: Likelihood of Threat Event Initiation [Table G2 from SP800-30]

Qualitative Values	Semi-Quantitative Values		Description
Very High	96-100	10	Error, accident, or act of nature is **almost certain** to occur; or occurs **more than 100 times a year**.
High	80-95	8	Error, accident, or act of nature is **highly likely** to occur; or occurs **between 10-100 times a year**.
Moderate	21-79	5	Error, accident, or act of nature is **somewhat likely** to occur; or occurs **between 1-10 times a year**.
Low	5-20	2	Error, accident, or act of nature is **unlikely** to occur; or occurs **less than once a year**, but **more than once every 10 years**.
Very Low	0-4	0	Error, accident, or act of nature is **highly unlikely** to occur; or occurs **less than once every 10 years**.

Table 9: Likelihood of Threat Event Occurrence [Table G3 from SP800-30]

Qualitative Values	Semi-Quantitative Values		Description
Very High	96-100	10	If the threat event is initiated or occurs, it is **almost certain** to have adverse impacts.
High	80-95	8	If the threat event is initiated or occurs, it is **highly likely** to have adverse impacts.
Moderate	21-79	5	If the threat event is initiated or occurs, it is **somewhat likely** to have adverse impacts.
Low	5-20	2	If the threat event is initiated or occurs, it is **unlikely** to have adverse impacts.
Very Low	0-4	0	If the threat event is initiated or occurs, it is **highly unlikely** to have adverse impacts.

Table 10: Likelihood of Threat Event Resulting in Overall Impact [Table G4 from SP800-30]

Likelihood of Threat Event Initiation or Occurrence	Likelihood Threat Events Result in Adverse Impacts				
	Very Low	**Low**	**Moderate**	**High**	**Very High**
Very High	Low	Moderate	High	Very High	Very High
High	Low	Moderate	Moderate	High	Very High
Moderate	Low	Low	Moderate	Moderate	High
Low	Very Low	Low	Low	Moderate	Moderate
Very Low	Very Low	Very Low	Low	Low	Low

Table 11: Overall Likelihood [Table G5 from SP800-30]

Type of Impact	Impact

HARM TO OPERATIONS	- Inability to perform current missions/business functions.
	  - In a sufficiently timely manner.
	  - With sufficient confidence and/or correctness.
	  - Within planned resource constraints.
	- Inability, or limited ability, to perform missions/business functions in the future.
	  - Inability to restore missions/business functions.
	  - In a sufficiently timely manner.
	  - With sufficient confidence and/or correctness.
	  - Within planned resource constraints.
	- Harms (e.g., financial costs, sanctions) due to noncompliance.
	  - With applicable laws or regulations.
	  - With contractual requirements or other requirements in other binding agreements (e.g., liability).
	- Direct financial costs.
	- Relational harms.
	  - Damage to trust relationships.
	  - Damage to image or reputation (and hence future or potential trust relationships).

HARM TO ASSETS	- Damage to or loss of physical facilities. - Damage to or loss of information systems or networks. - Damage to or loss of information technology or equipment. - Damage to or loss of component parts or supplies. - Damage to or of loss of information assets. - Loss of intellectual property.
HARM TO INDIVIDUALS	- Injury or loss of life. - Physical or psychological mistreatment. - Identity theft. - Loss of Personally Identifiable Information. - Damage to image or reputation.

HARM TO OTHER ORGANIZATIONS	- Harms (e.g., financial costs, sanctions) due to noncompliance.
	  - With applicable laws or regulations.
	  - With contractual requirements or other requirements in other binding agreements.
	- Direct financial costs.
	- Relational harms.
	  - Damage to trust relationships.
	  - Damage to reputation (and hence future or potential trust relationships).

HARM TO THE NATION	- Damage to or incapacitation of a critical infrastructure sector.
	- Loss of government continuity of operations.
	- Relational harms.
	  - Damage to trust relationships with other governments or with nongovernmental entities.
	  - Damage to national reputation (and hence future or potential trust relationships).
	- Damage to current or future ability to achieve national objectives.
	  - Harm to national security.

Table 12: Examples of Adverse Impacts [Table H2 from SP800-30]

Qualitative Values	Semi-Quantitative Values		Description
Very High	96-100	10	The threat event could be expected to have **multiple severe or catastrophic** adverse effects on organizational operations, organizational assets, individuals, other organizations, or the Nation.
High	80-95	8	The threat event could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, individuals, other organizations, or the Nation. A severe or catastrophic adverse effect means that, for example, the threat event might: (i) cause a severe degradation in or loss of mission capability to an extent and duration that the organization is not able to perform one or more of its primary functions; (ii) result in major damage to organizational assets; (iii) result in major financial loss; or (iv) result in severe or catastrophic harm to individuals involving loss of life or serious life-threatening injuries.
Moderate	21-79	5	The threat event could be expected to have a **serious** adverse effect on organizational operations, organizational assets, individuals other organizations, or the Nation. A serious adverse effect means that, for example, the threat event might: (i) cause a significant degradation in mission capability to an extent and duration that the organization is able to perform its primary functions, but the effectiveness of the functions is significantly reduced; (ii) result in significant damage to organizational assets; (iii) result in significant financial loss; or (iv) result in significant harm to individuals that does not involve loss of life or serious life-threatening injuries.
Low	5-20	2	The threat event could be expected to have a **limited** adverse effect on organizational operations, organizational assets, individuals other organizations, or the Nation. A limited adverse effect means that, for example, the threat event might: (i) cause a degradation in mission capability to an extent and duration that the organization is able to perform its primary functions, but the effectiveness of the functions is noticeably reduced; (ii) result in minor damage to organizational assets; (iii) result in minor financial loss; or (iv) result in minor harm to individuals.
Very Low	0-4	0	The threat event could be expected to have a **negligible** adverse effect on organizational operations, organizational assets, individuals other organizations, or the Nation.

Table 13: Impact of Threat Events [Table H3 from SP800-30]

Likelihood (Threat Event Occurs and Results in Adverse Impact)	Level of Impact				
	Very Low	**Low**	**Moderate**	**High**	**Very High**
Very High	Very Low	Low	Moderate	High	Very High
High	Very Low	Low	Moderate	High	Very High
Moderate	Very Low	Low	Moderate	Moderate	High
Low	Very Low	Low	Low	Low	Moderate
Very Low	Very Low	Very Low	Very Low	Low	Low

Table 14: Level of Risk [Table I2 from SP800-30]

Qualitative Values	Semi-Quantitative Values		Description
Very High	96-100	10	**Very high risk** means that a threat event could be expected to have **multiple severe or catastrophic** adverse effects on organizational operations, organizational assets, individuals, other organizations, or the Nation.
High	80-95	8	**High risk** means that a threat event could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, individuals, other organizations, or the Nation.
Moderate	21-79	5	**Moderate risk** means that a threat event could be expected to have a **serious** adverse effect on organizational operations, organizational assets, individuals, other organizations, or the Nation.
Low	5-20	2	**Low risk** means that a threat event could be expected to have a **limited** adverse effect on organizational operations, organizational assets, individuals, other organizations, or the Nation.
Very Low	0-4	0	**Very low risk** means that a threat event could be expected to have a **negligible** adverse effect on organizational operations, organizational assets, individuals, other organizations, or the Nation.

Table 15: Description of Levels of Risk [Table I3 from SP800-30]

5 Security Controls

From SP800-53 (page 1): "Security controls are the safeguards/countermeasures prescribed for information systems or organizations that are designed to: (i) protect the confidentiality, integrity, and availability of information that is processed, stored, and transmitted by those systems/organizations; and (ii) satisfy a set of defined security requirements. "

A risk analysis identifies areas that need fixing and should select suitable controls to address the problems. In SP800-53 NIST list a set of security controls classified into 18 families as shown in Table 16. The controls in each family are summarised in Appendix D of SP800-53, and then further demcomposed into the specific controls. Appendix F of SP800-53 provides a catalog of the controls, covering about 300 pages. The approach is an organisation should choose from the controls in the catalog; guidance is given as to which controls are more appropriate depending on the level of protection required (low, moderate, high). Consult Appendix D and Appendix F of SP800-53 for the details

ID	Family	ID	Family
AC	Access Control	MP	Media Protection
AT	Awareness and Training	PE	Physical and Environmental Protection
AU	Audit and Accountability	PL	Planning
CA	Security Assessment and Authorization	PS	Personnel Security
CM	Configuration Management	RA	Risk Assessment
CP	Contingency Planning	SA	System and Services Acquisition
IA	Identification and Authentication	SC	System and Communications Protection
IR	Incident Response	SI	System and Information Integrity
MA	Maintenance	PM	Program Management

Table 16: Security Control Identifiers and Family Values [Table 1 from SP800-53]

6 Documenting Risks and Controls

The results of a risk analysis should be documented, e.g. in a *risk register*. A plan for selecting and implementing security controls should also be developed, e.g. a *security implementation plan*. Table 14.5 from Stallings and Brown gives an example risk register with the following fields:

Asset: name or description of the item/information that is of value to the organisation

Threat/Vulnerability: description of the threat/vulnerability of the asset, examples are in Tables 2 to 7.

Existing Controls: security controls that are currently used (Section 5).

Likelihood: A rating from Very Low, Low, Moderate, High, Very High of the overall likelihood of the threat. This is determined by first determining the likelihood of occurrence (Tables 8 and 9), then the level of impact (Table 10), and finally looking up Table 11.

Consequence: A rating from Very Low, Low, Moderate, High, Very High of the impact on the organisation if the threat event occurs. See Table 13.

Level of Risk: A rating from Very Low, Low, Moderate, High, Very High of the level of risk, determine using the likelihood and consequence using Table 14.

Risk Priority: A ranking of the risk (integer) that considers both the risk level and the cost of treatment.

Table 15.4 from Stallings and Brown gives an example implementation plan with the following fields:

Risk: Name/description of the asset and threat

Level of Risk: From the risk register

Recommended Controls: A set of security controls that ideally would be used to reduce the risk

Priority: From the risk register

Selected Controls: A set of security controls selected to reduce the risk. The selection of the recommended controls needs to take into account the cost of implementing the controls and the benefit they bring.

Required Resources: The resources (personnel, time, financial, equipment) required to implement the selected controls.

Responsible Persons: List of people responsible for this risk item.

Start to End Date: Dates for when the controls will be implemented.