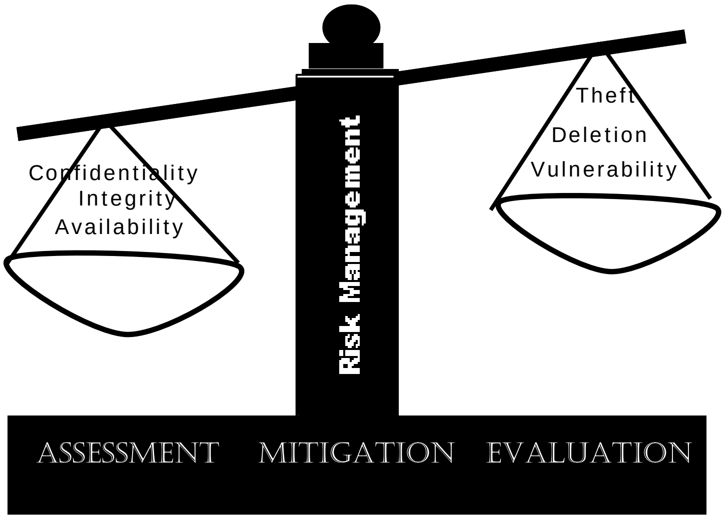
Cyber Security:

Risk Management

A Non-Technical Guide

Essential for
Business Managers
Office Managers
Operations Managers



Multi-State Information
Sharing and Analysis Center

NYS Office of Cyber Security

This appendix is a supplement to the Cyber Security: Getting Started Guide, a non-technical reference essential for business managers, office managers, and operations managers. This appendix is one of many which is being produced in conjunction with the Guide to help those in small business and agencies to further their knowledge and awareness regarding cyber security. For more information, visit: http://www.dhses.ny.gov/ocs/ .

Introduction

Risk Management is simply to look at what could go wrong - and then decide on ways to prevent - or minimize - these potential problems. It encompasses three processes – risk assessment, risk mitigation and evaluation.

We all carry out informal risk management numerous times in the course of a day without even realizing it. Every time we cross a street, we stop to weigh the risk of rushing in front of oncoming traffic, waiting for the light to change, using the crosswalk, etc. Our ability to analyze the consequences of each decision is risk assessment. What we decide to do after performing that quick analysis is risk mitigation based on proper early training and our experience of crossing a road. We may decide to wait for the traffic light and use the cross walk which greatly reduces the potential risk, we may follow someone else across the street allowing them to make the decision for us, or we may simply choose not to cross the street. These decisions are a result of our risk assessment of the situation. If you make it across the street you remember what worked. If anything went wrong such as a honked horn or brakes squealing, you should evaluate if another choice would have been better.

Below are important definitions for terms that are used in this Guide.

Risk: The probability of suffering harm or loss. It refers to an action, event or a natural occurrence that could cause an undesirable outcome, resulting in a negative impact or consequence.

Risk Assessment: The process of identifying *threats* to *information* or *information systems*, determining the likelihood of occurrence of the *threat*, and identifying *system vulnerabilities* that could be exploited by the *threat*.

Risk Management: The process of taking actions to assess *risks* and avoid or reduce *risk* to acceptable levels.

As a manager the issues of risk assessment may seem difficult and the right decisions for risk management challenging; but the principles remain the same. It is your responsibility to make the best decision based on the information at hand. A well-structured risk management methodology, when used effectively, can help. For instance, a citizen may report a pothole on a local road and you are obligated to determine an appropriate response. There are many factors to consider: what if a car gets damaged in the pothole? Is the cost to fix the pothole justified by the potential consequences? What if a citizen sues or seeks restitutions for damage caused by the pothole? You have to analyze the risk and then decide how to manage the problem. Is it best to put signs around the pothole warning citizens? Should you pay overtime to send a road crew out to fix it? Do you ignore the problem? Risk assessment allows managers to evaluate what needs to be protected relative to operational needs and financial resources. This is an ongoing process of evaluating threats and vulnerabilities, and then establishing an appropriate risk management program as part of your larger organization’s risk management program to mitigate potential monetary losses and harm to an organization's reputation. For information security, the program should be appropriate for the degree of risk associated with the organization's systems, networks, and information assets. For example, organizations accepting online payments are exposed to more risk than websites with only static information.

The Steps in Risk Management are

1. Risk Assessment
    - A. Classify information
    - B. Identify threats
    - C. Identify vulnerabilities
    - D. Analyze risk to information assets
    - E. Select a method
    - F. Summarize and communicate risk

2. Risk Mitigation
    A. Identify options
    B. Choose an option
    C. Implement
        - Accept the risk
        - Transfer the risk
        - Limit the risk: put control in place
        - Avoid the risk
3. Evaluation

Small businesses and agencies maintain information that is confidential and integral to the operation of their organization. Information is any representation of facts, concepts or instructions created, stored (in temporary or permanent form), filed, produced or reproduced, regardless of the form or media. This may include, but is not limited to the *data* contained in reports, files, folders, memoranda, statements, examinations, transcripts, images, and communications whether electronic or hard copy. For example, a computer in a business office may contain client social security numbers, financial records, health records and other personal, private, or sensitive information (PPSI).

An employee's decision to leave his computer unprotected for even a short time opens the risk to unauthorized physical access. Or, the organization's decision not to have a firewall or antivirus software installed to protect it leaves the computer at risk to someone who gains unauthorized access through the Internet. The management of these risks may be as simple as requiring employees to lock the computer every time they step away, installing anti virus, or the installation of firewalls.

1. Risk Assessment

Risk assessment is the first phase in the risk management process. Risk is assessed by identifying threats and vulnerabilities, and then determining the likelihood and impact for each risk.

It is important to designate an individual or a team, who understands the organization's mission, to periodically assess and manage information security risk. The designated individual will work with others from the organization to understand the business program component of information assets, the technology involved, and the impact as well as the costs of managing the risk.

1a. Classify Information

Before an organization can assess the risk it must first classify the information assets in the organization. Classification is the designation given to information from a defined category on the basis of its sensitivity. Information assets include all categories of *information* (automated and non-automated), including (but not limited to) *data* contained in records, files, and databases. Information assets usually include: public records mission-critical systems, customer interfaces, internal tools, source code, and confidential records. The organization is responsible for protecting the confidentiality, integrity and availability of the information assets. The value of an asset will be determined by the information owner - an individual or a group of individuals responsible for making classification and control decisions regarding use of information, especially PPSI.

An information asset can mean many different things depending on what the organization is trying to accomplish; therefore, it is important to identify each information asset. Information may be stored onsite or offsite, on hard drives, CDs and tapes. It is best to create a list of all information assets and classify each asset (e.g., confidential, restricted, public information). The classification of the information should be included on the information itself and on a central list. Policies and procedures regarding the classification of documents should be in place so all employees are aware and educated about them. A reference for information classification and control can be found in the references section at the end of this document.

1b. Identify Threats

A threat is a force, organization or person, which seeks to gain access to, or compromise, *information*. By looking at the nature of the *threat*, its capability and resources, one can assess it, and then determine the likelihood of occurrence, as in *risk assessment*. A *threat* can be assessed in terms of the probability of an attack.

There are many types of information security threats, some examples are listed below[1]:

- Internal (e.g., malicious or unaware employees);
- Mobile (e.g., attackers who steal remote systems which, in turn, provide access to information);
- Physical (e.g., attackers who steal computers or enter server rooms, file cabinets, or offices);
- Natural (e.g., fire, floods, and earthquakes resulting in electrical outages, equipment and hardware failures);
- Network (e.g., attackers who try to compromise systems exposed on a public network or try to spoof or imitate remote systems);
- Social (e.g., attackers who try to fool employees into revealing information through phishing);
- Malicious (e.g., viruses, worms, and Trojan horses, code that may damage, reveal, or capture information).

It is important to be aware of threats to your organization's information in order to prevent compromise to that information's confidentiality, integrity and availability. Information security threats must be identified at as many levels as possible.

1c. Identify Vulnerabilities

Vulnerabilities must be identified. Vulnerabilities are weaknesses, in a *system* or facility holding *information,* which can be exploited to gain access or violate *system integrity*. *Vulnerabilities* can be assessed in terms of the means by which the attack would be successful, such as,

- Tapes lost during transfer to a storage facility (availability issue).

- Information read by an unauthorized individual(s) (confidentiality issue).

- Software and hardware not maintained at current patch levels allow unauthorized access via the Internet resulting in a breach of confidential information (confidentiality, integrity and/or availability issues).

- Unintentional loss of data via theft resulting in identity theft (confidentiality issue).

- Accidental or intentional deletion or modification of information (availability and integrity issues).

- Unsecured computers and portable devices such as blackberries, laptops, or USB devices (confidentiality, integrity and availability issues).

1d. Analyze Risk to Information Assets

There are inherent risks involved in containing and transferring information. Information is subject to intentional and unintentional actions by other people or systems. If information is confidential, there may be unauthorized people who want to see it, such as competitors or disgruntled or curious employees. People may try to break into the devices containing the information or try to intercept the information during transfer. People may also receive confidential information unknowingly and completely by accident. Furthermore, information systems can be maliciously or accidentally damaged. Information security breaches like these can seriously hurt an organization.

Risk for a given asset can be provided in the most general form using the following equation:

Risk = (Probability of a threat occurring against an asset) x (Value of asset)

In other words, the higher the likelihood of a threat occurring and affecting an asset and the higher the value of that asset, the higher the risk. If a threat has little or no chance of occurring, or if the asset has no value, the risk is either very low or zero. Since information assets within an organization most likely hold some level of value, risk management will involve reducing the likelihood of threats from occurring[2].

1e. Select a Method

In order to quantify risk in some fashion, an organization will need to develop a method of measuring risk so that this information can be communicated with others. There are many methodologies to pick from; each organization will need to determine which is best. Ultimately, the organization will need to understand its information security risks. The question "What information assets are most at risk to compromise or damage and what can happen to these assets?" needs to be answered.

The question may best be answered by assigning a value and acceptable risk level to each asset. The value of an asset varies from asset to asset and from organization to organization. The level of risk depends on actions taken by the organization. For example if backups are done and secured, the loss (unavailability) of an electronic copy may be a low risk. One way that you might measure risk is shown in the following illustration, while presented as a methodology, can be modified to meet your needs. We will expand this illustration later in this document.

Information Asset	**Value** (High/Low/Medium)	**Risk Level** (High/Low/Medium)	**Notes** (explain major risks and or costs)
Board Minutes	High	Low	Expectation is these are highly protected
Personnel Records	High	High (Identity Theft)	Have a high value to the organization for reporting, retiring, payroll, etc.

To assist the organization in making information security risk assessment decisions it will help to ask some questions based on confidentiality, integrity and availability. Additional resource information is found at the end of this document.

1. Negative effects on credibility

Will an organization's actions, process, program or procedure negatively affect its credibility?

Ex: Imagine if health information, probation or social services information were posted publicly on the Internet. (Confidentiality)

2. Health, welfare and detriment to the community

Will an organization's actions, process, program or procedure affect the health, safety and welfare of another?

Ex: If information is corrupted, drug-testing results for school bus drivers changed, bridge height specifications altered, or a computer system slowdown delays updated information about a stolen car from reaching law enforcement, citizens' health and safety may be at risk. (Availability)

3. Violation of the right to informational privacy or confidentiality

Will an organization's actions, process, program or procedure result in the breach of informational privacy or confidentiality?

Ex: If unauthorized release of personal information, Social Security number, health information, drug testing results, etc. occurs, it may result in identity theft.

4. Accessibility and integrity of public records

Will an organization's actions, process, program or procedure prevent access to necessary records or result in changes to data in them?

Ex: If vital records are stored on a computer but are not backed up and a natural disaster destroys the computer, the records are no longer available.

Ex: If tax records are accessed by an unauthorized individual, the records could be modified and the integrity of the information lost.

5. Violation of laws, regulations or contracts

Will an organization's actions, process, program or procedure result in the breach of any law, regulation or contract?

Ex: If a breach of information occurs, for example where a law is in place, the result may be: "if client information is exposed or divulged inappropriately, individuals can be financially accountable with personal financial liability upwards of $5,000."

6. Operational impact

Will an organization's actions, process, program or procedure result in impacting operations in a negative way?

Ex: If systems are unavailable, information systems crash, or email is not available, chaos can ensue, or, at best, jobs cannot be completed.

7. Financial consequences

Will an organization's actions, process, program or procedure result in the loss of revenue, workforce downtime, litigation, or increased resource expenditure?

Ex: If information is destroyed due to a virus or catastrophe, how could it be restored? What is the cost to reproduce or recreate it?

Additional questions that may be asked during a risk assessment include:

- Who has a need to access this information?
- What happens if the application, program, or website is not available to those who need the information?
- Are there any security risks associated with the proposed software?

- To whom or what other organizations will this information be connected?
- Will this information be connected to the Internet?

Total risk to an organization’s information assets is the aggregation of all risks to all information assets, and can be calculated using a specific model, added together, or averaged, depending on how the quantified risk is to be communicated. For each risk a control may be available to manage to the risk. These will be discussed in the risk mitigation section of this guide.

1f. Summarize and Communicate Risk

Risk has to be measured for each information asset, and for the organization as a whole, and then communicated so decisions can be made to manage the risk.

2. *Risk Mitigation*

Risk Mitigation is the process of taking actions to eliminate or reduce the probability of compromising the confidentiality, integrity, and availability of valued information assets to acceptable levels. There are three steps to risk mitigation: identify, choose and implement options.

2a. Identify Options

It is up to the organization to mitigate risks so that assets are protected. Once the risk to information assets has been measured, a decision must be made about how to mitigate that risk. There are four options available for mitigating risk:

1. accept the risk
2. transfer the risk
3. limit the risk
4. avoid the risk

Accept the Risk

An organization may choose to simply accept risk under these scenarios:

- The risk is considered low (e.g., the value of an asset is low and the probability of threats affecting the asset are acceptable).
- The cost of accepting the risk is found to be lower than the cost of transferring or limiting the risk.

If the cost of accepting the risk is high or more than the cost of transfer or limiting it, then the organization should not accept the risk. The organization should then look at transferring or limiting the risk[3].

Transfer the Risk

When the risk is transferred, the risk is shared with a third party in part or in whole. This is typically seen in the use of insurance. Third party insurance organizations, for a fee, agree to accept the risk and compensate the information owner for the full damage of a particular risk[4]. This is appropriate for hardware or when the recoup value is received if the asset is destroyed or where an organization wants to limit liability. In some cases, transferring risk may not be available. In other cases, the risk may be too high and too costly to insure.

An everyday example of transferring risk is with car insurance. Through the use of insurance, the car owner is transferring the risk of vehicle loss due to an accident to the insurance company.

Another example can be seen with third party web site hosting. If an organization utilizes a third party vendor to host their website they are transferring some of the risk to the vendor. The vendor is responsible for the availability and integrity of the information supplied by the organization to be posted. Vendor contracts and agreements should list the roles and responsibilities of the vendor.

Limit the Risk

When a risk is high for a particular asset, and the risk cannot be transferred (i.e., not practical or cost-effective), then the risk should be limited in part or in full. The process includes identifying the most probable threats to a given asset and identifying, researching, or developing an acceptable control to that threat.

In the case of limiting risks such as a virus infection, spam and unauthorized Internet access, the organization may decide to order the purchase of software for all computer devices to reduce the impact of those risks. Limiting risk will mean controlling access to the network, by installing antivirus, spamware and a firewall where none exists. Training employees, interns and contractors to be aware of information security will also help reduce the risks.

In some cases, limiting the risk can be fast, inexpensive and sometimes free. Information systems suppliers may provide free security patches and may even provide mechanisms that perform automatic updates to these systems. Applying security updates or bug fixes may simply involve the time and skills of the internal staff. Keeping software updated is a critical defense to recently discovered vulnerabilities.

In other cases, limiting risk can be very expensive. For example, if buildings housing computers that contain vital information are at risk to natural disasters, the organization may have to consider moving to a different location or providing redundancy by adding buildings.

There may be different levels of controls that can be applied to one threat that may only reduce the risk to an acceptable level to the organization. There may be certain aspects of a threat that can be reduced by implementing controls and some other aspects that may be covered by transferring the risk. Taking the example of the development of a new building – costs may be incurred to purchase new, redundant hardware while insurance may be purchased to cover the building itself. When processes are identified to incorporate threats, this may involve restructuring the process and re-training the people involved[5].

Avoid the Risk

Risk avoidance is natural for some of us; but for others risk taking is part of the thrill of life. When it comes to your responsibility as a manager you have to know when it is appropriate to avoid the risk altogether. There is no universal answer to when risk avoidance will be appropriate because every circumstance is different. Risk avoidance may be used to protect those assets which are at high risk. Some examples of this option include:

- Building a facility outside a flood zone
- Keeping computers systems with confidential information or PPSI on them disconnected from the Internet

2b. Choose an Option

Once the organization has identified the various options for mitigating risk, one must be selected. The team or individual designated to handle risk management will need to work with the appropriate individuals and make a recommendation to management. Keep in mind the decision will need to be reviewed whenever the information asset changes since the classification of the information asset may change or the threats and risks change. The illustration from the previous section can be updated in this manner:

Information Asset	Value High/ Low/ medium	Risk High/ Low/ medium	Recovery Mitigation Cost	Priority	Options
Board minutes	High	Low	Low	Medium	Accept: no new control Transfer: store with a vendor offsite Limit: save to microfilm, purchase fireproof cabinet Avoid: N/A
Personnel records	High	High (Identity Theft)	High	High	Accept: no new controls Transfer: store with a vendor offsite Limit: encrypt information Avoid: disconnect computer from the Internet

2c. Implement the Option

Implementing the option involves putting into action the choice that has been made for mitigating the risk. As previously defined, the possible actions are to accept the risk, transfer the risk, limit the risk, or avoid the risk. Each information asset now has an assigned risk and the option for mitigating the risk has been chosen. Implementing the chosen option will result in certain procedures being followed and/or new controls put in place. Limiting the risk by putting a control in place will be the most commonly chosen option to protect your information assets and systems. Continual monitoring and regular updating is part of the implementation to keep the risk at an acceptable level.

Consider for example, the organization's operating system. Vulnerabilities are continually being discovered and exploited in operating systems. You can limit the risk by performing updates to patch your system. You can accomplish this by scheduling automatic updates. Additionally, most application software currently marketed has some mechanism to keep it updated to current levels. These updates are primarily distributed for security and functionality.

Antivirus software is another way to limit the risk to your computer and information assets. It is one thing to install the antivirus software but to continually limit the risk to your machine you must maintain the software and update it frequently. This would involve the purchase of a subscription to the service to receive daily updates, scheduling the daily updates, and the scheduling of frequent and regular scans of your computer.

3. Evaluation

A designated team or individual should follow through to ensure that the option chosen to mitigate the risk for each identified information asset has been implemented. At a minimum, an annual review must also be performed to ensure that the controls put in place are still functional and viable to protect a given information asset.

A technical security review would consist of reviewing the *controls* built into a system or application to ensure they still perform as designed and are in compliance with documented security policies and procedures. It would also include reviewing security patches to ensure they have been installed and are operational, reviewing security rules such as access control lists for currency, testing of firewall rules, etc. This type of testing includes intrusion and/or penetration testing of controls.

The evaluation step in the Risk Management process consists of two components

The review itself and recording of the review.

3a. Review and Record

After implementation, you must evaluate what was done through the classifying the assets, selecting an option and implementing the actions taken. It is time to record and document lessons learned. A group should be organized including the original team to discuss and evaluate the process and document any issues and lessons learned.

3b. Tools to Help with the Process

Also important is the use of tools, auditing, and policies. Tools such as dedicated risk management systems can be used to assess risk. Some tools can also help limit risk for the long term. Auditing allows the organization over time to identify the possible threats and risks and implement future risk assessment and management. Policies enable an organization to define how to prevent the exploitation of information assets and discipline those people who compromise the information. Policies, whether procedural-based or system based, should be used to minimize risk.

Leveraging tools (software, procedural, etc.) can help in the assessment and management of risk, and so, should be examined. These tools, if applied and used properly, will usually speed-up the assessment process or ease the management process. Freeware and shareware-based tools are available for multiple types of systems (although great care should be taken when using these tools and support is typically limited). Tools can be purchased, such as dedicated information risk management systems, and usually offer greater reliability and much-needed support services. Examples include tools that help identify and inventory information assets, assess security configurations, measure performance and availability, and implement “emergency” patches quickly[6].

Auditing tools are often available or integrated within systems that contain or transfer information assets. Consider installing and enabling these tools to help manage risk continually. Although not a replacement for risk management, these tools can help identify events that compromise the confidentiality, integrity, and availability of information assets[7].

Policy management tools also may be available or integrated into systems. Policies typically help prevent possible compromise. Policy management tools can limit what people do or see on systems. For example, a user policy can be enforced to allow certain users access to only the programs they need to use and prevent access to other programs, enforcing confidentiality. Some policy management tools can see that certain people or processes receive maximum bandwidth to critical systems, such as with Quality of Service, enforcing availability. Other policies help in sending data in a highly reliable format, enforcing integrity[8].

Conclusion

In most organizations the network itself will continually be expanded and updated; its components changed; and its software applications replaced or updated with newer versions. In addition, personnel changes will occur and security policies are likely to change over time. These changes mean that new risks will surface and risks previously mitigated may again become a concern. Thus, the risk management process is ongoing and evolving.

Once your organization has conducted a risk assessment and made decisions about how to mitigate those risks, a regular review should be scheduled at least annually. To help keep the cost down, the risk assessment should occur whenever an information asset is classified, purchased or a new project is developed. A security review is often helpful.

Risk management must be fully understood by any organization that seeks long-term success[9]. It includes risk assessment, risk mitigation, and evaluation. Proper risk management ensures that confidential information is not breached, data integrity is retained, and information remains available.

Some Resources

- Information Classification documents located at http://www.dhses.ny.gov/ocs/resources/ developed by NYS provide not only information classification guidance but contain a complete package of charts, questions, roles and responsibilities, and a matrix of controls for confidentiality, integrity and availability. It may be used by any organization.

- NIST Special Publications http://csrc.nist.gov/publications/PubsSPs.html. Some include the following:
  - 800-30 Risk Management Guide for Information Technology Systems
  - 800-37 Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach
  - 800-39 Managing Risk from Information Systems: An Organizational Perspective
  - 800-53 Rev. 3 Recommended Security Controls for Federal Information Systems and Organizations
  - 800-70 Security Configuration Checklists Program for IT Products: Guidance for Checklists Users and Developer

- NIST National Vulnerability Database Version 2.2 http://nvd.nist.gov/

- Open Web Application Security Project (OWASP) OWASP Top 10 www.owasp.org

- Cyber Security Evaluation Tool (CSET) U.S. Department of Homeland Security (DHS) product that assists organizations in protecting their key national cyber assets www.us-cert.gov/control_systems/satool.html

- 2009 CWE/SANS Top 25 Most Dangerous Programming Errors http://cwe.mitre.org/top25/

Definitions in this Guide are found in the NYS Information Classification documents. Thanks to the California Counties Information Services Directors Association for permission to use some excerpts from their California Counties “California Counties ‘Best Practices’ Information Security Program” document www.ccisda.org/docs/index.cfm?DocumentScreen=Detail&ccs=240&cl=4

Endnotes

[1] California County Information Services Directors Association, “California Counties ‘Best Practices’ Information Security Program” March 2002, page 36

[2] Ibid., page 37
[3] Ibid., page 38
[4] Ibid., page 38
[5] Ibid., page 39
[6] Ibid., page 39
[7] Ibid., page 39
[8] Ibid., page 39
[9] Ibid., page 40

Glossary

Availability: The extent to which information is operational, accessible, functional and usable upon demand by the authorized entity (e.g., a system or user).

Classification: The designation given to information from a defined category on the basis of its sensitivity.

Confidentiality: The property that information is not made available or disclosed to unauthorized individuals, entities, or processes.

Controls: Countermeasures or safeguards that are the devices or mechanisms that are needed to meet the requirements of policy.

Information: Any representation of facts, concepts or instructions created, stored (in temporary or permanent form), filed, produced or reproduced, regardless of the form or media. This may include, but is not limited to the data contained in reports, files, folders, memoranda, statements, examinations, transcripts, images, communications, electronic or hard copy.

Information Asset: All categories of information (automated and non-automated), including (but not limited to) data contained in records, files, and databases.

Information Owner: An individual or a group of individuals that has responsibility for making classification and control decisions regarding use of information.

Integrity: The property that data has not been altered or destroyed from its intended form or content in an unintentional or an unauthorized manner.

Personal, Private or Sensitive Information (PPSI): Any information where unauthorized access, disclosure, modification, destruction or disruption of access to or use of such information could severely impact the organization, its critical functions, its employees, its customers, third parties or citizens.

Physical Security: The protection of information processing equipment from damage, destruction or theft; information processing facilities from damage, destruction or unauthorized entry; and personnel from potentially harmful situations.

Risk: The probability of suffering harm or loss. It refers to an action, event or a natural occurrence that could cause an undesirable outcome, resulting in a negative impact or consequence.

Risk Assessment: The process of identifying threats to information or information systems, determining the likelihood of occurrence of the threat, and identifying system vulnerabilities that could be exploited by the threat.

Risk Management: The process of taking actions to assess risks and avoid or reduce risk to acceptable levels.

Technical Security Review: A technical security review would consist of reviewing the controls built into a system or application to ensure they still perform as designed and are in compliance with documented security policies and procedures. It would also include reviewing security patches to ensure they have been installed and are operational, reviewing security rules such as access control lists for currency, testing of firewall rules, etc. This type of testing includes intrusion and/or penetration testing of controls.

Threat: A force, organization or person, which seeks to gain access to, or compromise, information. A threat can be assessed in terms of the probability of an attack. Looking at the nature of the threat, its capability and resources, one can assess it, and then determine the likelihood of occurrence, as in risk assessment.

Vulnerability: A weakness of a system or facility holding information which can be exploited to gain access or violate system integrity. Vulnerability can be assessed in terms of the means by which the attack would be successful.