**Understanding Likelihood and Impact Ratings**

**& Risk Responses**

Most of the information contained in this document is derived from the National Institute of Standards and TechnologyNIST Special Publications (800 Series): <http://csrc.nist.gov/publications/PubsSPs.html>

**Including:**

NIST\_sp800\_30\_New Version-r1.pdf:

<http://csrc.nist.gov/publications/nistpubs/800-30-rev1/sp800_30_r1.pdf>

NIST Special Publication 800-30(dated July 2002)

<http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf>

NIST Special Publication 800-37, revision 1

<http://csrc.nist.gov/publications/nistpubs/800-37-rev1/sp800-37-rev1-final.pdf>

NIST\_SP800-39-final.pdf:

<http://csrc.nist.gov/publications/nistpubs/800-39/SP800-39-final.pdf>

**Introduction**

Information Technology risk assessments are used to identify, characterize, and prioritize risk to organizational operations (i.e., mission, functions, image, and reputation), organizational assets, individuals, and other organizations, resulting from the operation and use of information systems. The purpose of an IT risk assessment is to inform decision makers and support risk responses by identifying: (i) relevant threats to organizations or threats directed through organizations against other organizations; (ii) vulnerabilities both internal and external to organizations; (iii) impact (i.e., harm) to organizations that may occur given the potential for threats exploiting vulnerabilities; and (iv) likelihood that harm will occur. The end result is a determination of risk (i.e., typically a function of the degree of harm and likelihood of harm occurring). IT Risk assessments are part of an overall risk management process—providing senior leaders/executives with the information needed to determine appropriate courses of action in response to identified risks.

A **threat** is the potential for a particular threat-source to successfully exercise a vulnerability. A **vulnerability** is a weakness that can be accidentally triggered or intentionally exploited.

A **threat source** can be either (1) intent or method targeted at the intentional exploitation of a vulnerability or (2) a circumstance, situation and/or method that may accidentally trigger a vulnerability. Threat sources include but are not limited to: (i) hostile cyber/physical attacks; (ii) human errors of omission or commission; or (iii) natural and man-made disasters. Threat sources cause events having undesirable consequences or adverse impacts on organizational operations and reputation, assets, and individuals, and/or other organizations.

**Likelihood**

To derive a likelihood rating that indicates the probability that a potential vulnerability may be exercised, the implementation of current or planned controls must be considered. For example, a vulnerability (e.g., system or procedural weakness) is not likely to be exercised or the likelihood is low if there is a low level of threat-source interest or capability or if there are effective security controls that can eliminate, or reduce the magnitude of, harm.

|  |  |
| --- | --- |
| **Likelihood Rating** | **Likelihood of Occurrence Definition** |
| High | The threat source exists, is highly motivated and sufficiently capable, or controls to prevent the vulnerability from being exercised are ineffective or no controls are currently in place. |
| Medium | The threat source exists, is motivated and capable, but controls are in place to impede successful exercise of the vulnerability. |
| Low | The threat source exists, but lacks motivation or capability or controls are in place to prevent or at least significantly impede the vulnerability from being exercised. |

**Impact**

**Impact Ratings:** The impact of a security event can be described in terms of loss or degradation of any 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 functions in support of 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.

**NOTE:** When assigning an impact rating to a risk, assign the rating corresponding to the most serious consequence that could result should the vulnerability be exploited.

|  |  |
| --- | --- |
| **Impact Rating** | **Impact Rating Definition** |
| High | The potential impact is **high** if 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 severe or catastrophic adverse effect could mean that the loss of confidentiality, integrity, or availability might:       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;       Result in major damage to organizational assets, major financial loss, or severe or catastrophic harm to individuals involving loss of life or serious life threatening injuries. |
| Medium | The potential impact is **medium** if the loss of confidentiality, integrity, or availability could be expected to have a *serious* adverse effect on organizational operations, organizational assets, or individuals. A serious adverse effect could mean that the loss of confidentiality, integrity, or availability might:       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;       Result in significant damage to organizational assets, significant financial loss, or significant harm to individuals, but not loss of life or serious life threatening injuries. |
| Low | The potential impact is **low** if the loss of confidentiality, integrity, or availability could be expected to have a *limited* adverse effect on organizational operations, organizational assets, or individuals. A limited adverse effect could mean that the loss of confidentiality, integrity, or availability might:       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;       Result in minor damage to organizational assets, minor financial loss, or minor harm to individuals. |

**Risk Response Strategies**

Once a risk has been identified, and the likelihood of the risk has been considered, there are five possible strategies for addressing the risk – these are *accept, avoid, mitigate, transfer*, or *share*.

|  |  |
| --- | --- |
| **Risk Response**  **Strategy** | **Risk Response Definition** |
| Accept | To explicitly accept any potential impact or consequence to organizational operations (including to mission, functions, image or reputation, or finances), organizational assets, individuals, other organizations etc., and continue with current activities or operating IT systems. To do nothing, as in cases where no resources are available (funding, personnel etc.) to implement any change |
| Avoid | To avoid the potential risk involves taking specific actions to eliminate the activities or technologies that are the basis for the risk or to revise or reposition these activities or technologies within organizational mission/business processes to avoid the potential for unacceptable risk. |
| Mitigate | To mitigate or reduce the potential risk can include implementation of common security controls and/or new or enhanced management, operational, organizational (e.g., policies) or technical safeguards or countermeasures that that eliminate or minimize the adverse impact of a vulnerability or threat (e.g., use of supporting, preventive, or detective controls). |
| Transfer | To transfer a potential risk shifts the entire risk responsibility or liability from one organization to another organization (e.g., using insurance to transfer risk from particular organizations to insurance companies). Risk transfer does not reduce the likelihood of harmful events occurring nor the impact or consequences in terms of harm to the organization, assets, operations, individuals, etc. |
| Share | To share a potential risk means that some portion of risk responsibility or liability is shifted to another organization, such as when one department is dependent on services provided by a different department. Risk sharing may be a sharing of liability or a sharing of responsibility for other, adequate risk responses such as mitigation. Risk sharing often occurs when organizations determine that addressing risk requires expertise or resources that are better provided by other organizations.  Example: Departments share risk when utilizing central services such as Banner systems, networked storage space, or web hosting service offered by another organizations or units within departments. For instance, data hosting or storage services may be responsible for providing secure hardware, software, access tools, and availability of services, but the responsibility for data integrity and user access may be the responsibility of the department that owns the data but relies on the service. In such cases certain risks are shared. For example, if systems or services are misconfigured, data could be lost or unauthorized individuals may gain access. If departmental data access is not managed, monitored, controlled and reviewed the same thing can happen. Risk is shared but the boundaries between security responsibilities are clear. |

(These definitions are taken or derived from: NIST\_SP800-39-final.pdf, available online at: <http://csrc.nist.gov/publications/nistpubs/800-39/SP800-39-final.pdf>)