

IT Risk Assessment Procedure

# Overview/Purpose

In accordance with the *IT Risk Management Policy*, the following procedure outlines the Risk Assessment (RA) process which will be followed by <**Utility Name**>.

# Scope

Risk assessments (RAs) can be conducted by any entity within <**Utility Name**> or any outside entity that has signed a Third Party Agreement with <**Utility Name**>. RAs can be conducted on any information system, including applications, servers, and networks, and any process or procedure by which these systems are administered and/or maintained.

# Procedure

## Risk Assessment Sequence

The RA process will be conducted using asset, threat, vulnerability model, in the following sequence:  
 Asset  →  Threat  →  Vulnerability  =  Risk

A mitigation plan will be developed for any risks with a score beyond a specified threshold. Risk Assessment can be conducted by using the *Risk Register Form*.

## Asset Identification

The data asset inventory maintained under the *Data Classification Policy* will be used for the RA.  Similar assets may be aggregated as appropriate for the RA process.

## Threat Identification

Threats may include people, the systems they use, and conditions that could cause harm to an organization. Personnel at different levels of the organization will have different perspectives and can provide information about the risk which was not previously considered.   
Some examples of threats include:

* Accidental data corruption
* Denial of service attack
* Physical theft

Threats should be related to the applicable assets and vulnerabilities.

## Vulnerabilities

A vulnerability is a weakness that can be exploited by a threat and may originate from technology, the organization, the environment, or a business process.  
Examples of vulnerabilities include:

* Backup restore failure
* Firewall rule error
* Not patched operating system
* Improper confidential waste disposal

Each vulnerability should be related to the impacting threat(s) and assets. Additionally, any controls that offer protection from a vulnerability should be noted.  The adequacy of the controls should be estimated for each vulnerability, and considered as part of the vulnerability score.

## Potential Outcome

Once the threat list has been established, each entry should have possible outcome/risk.  
Then risk can be scored in the following categories:

* **Asset Value** – Low (0) to Critical (4)
* **Likelihood of Threat** – Low (0) to High (2)
* **Ease of Exploitation** – Low (0) to High (2)

A total score should be produced for each threat, which is the sum of the scores given for each category.

## Existing Controls

This list will primarily consist of active policies and technologies such as:

* Password change policy
* Backup policy
* Firewall

## Mitigation Plan

Any vulnerabilities with a risk score of 6 or above should be listed on the mitigation plan.  For each entry, a mitigation strategy should be developed. In cases where no practical mitigation strategy can be found, the risk can be accepted.  If any mitigation is under way, the status of said mitigation should be shown.

The IT Manager will convene a meeting of appropriate personnel, and develop plans for mitigating risk of score 3 to 5. In the case of a temporary mitigation strategy, a long-term approach should be developed and listed as well.

# Compliance

## Compliance Measurement

The <**person or group responsible for policy**> will verify compliance to this policy through various methods, including but not limited to, business tool reports, internal and external audits, and feedback to the policy owner.

## Exceptions

Any exception to the policy must be approved by the <**person or group responsible for policy**> in advance.

## Non-Compliance

An employee found to have violated this policy may be subject to disciplinary action in accordance with **<Utility Name>** HR policies.

# Related Standards, Policies, and Processes

* PCI DSS Risk Assessment Guidelines
* Data Classification Policy
* Data Protection and Availability Standards

# Governance Responsibilities

The ISP uses the RACI model for assigning responsibility.

|  |  |  |  |
| --- | --- | --- | --- |
| Responsible | Accountable | Consulted | Informed |
| CIO | **CEO/GM** | **CFO**  **COO**  **Legal Department** | **All Employees** |

*[Explanatory Note: <Utility Name> should feel free to alter section to reflect the specific responsibility requirement determined by <Utility Name> management.]*

# Approval

\_

<**Insert title of Accountable**> Date

# Revision History

|  |  |  |
| --- | --- | --- |
| Date of Change(s) | Revised by | Summary of Change(s) |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |