# RISK WORKSHEET

This worksheet has been created to help University of Washington (University) organizations identify information security risks. This document is intended to be a part of the security planning process and does not take the place of an in-depth risk assessment. Completion of this form does not imply approval from the Office of the CISO. Definitions can be found in [Administrative Policy Statement 2.4](http://www.washington.edu/admin/rules/policies/APS/02.04.html).

NOTE: When filled out, this document or information therein is classified as Restricted and may be exempted from a public records request on the basis of security; pursuant to RCW 42.56.420.

## INSTRUCTIONS

Follow the steps below to develop risk statements. Use the table at the end of the document. Copy the table if you need additional space.

1. Refer to your organization’s **Security Plan**, **Security** **Self-Assessment,** and **Controls Worksheet(s)** while writing risk statements
2. Write clear risk statements:

* **Do** name a specific compliance violation, financial loss or harm
* **Do** use plain language, but be specific enough to assess control options
* **Do** specify the asset or groups of assets if a risk statement is not generally applicable
* **Do** distinguish a risk from a breakdown in control
* **Do** keep in mind what is/is not in your control
* **Do** **not** over or underestimate a scenario without any logic or evidence to back it up
* **Do** **not** try to engineer a solution when thinking about addressing risks
* **Do** **not** blame a particular person, team, or organization

1. Revise, consolidate, or break-out risk statements as necessary
2. Use the **Impact Table** to determine the impact to the organization for each risk
3. Write option(s) for addressing risk for each risk statement
4. Use the **Effort** **Table** to rank the level of effort required to address each risk

## RISK

**Risk** is the combination of the **likelihood** that a threat will occur and the severity of the resulting **impact** on the organization and its business partners.

### THREATS

Threats can be targeted (deliberate, focused) or not targeted (opportunity based, not specific, accidental), and may be internal or external to your organization. Threat level can depend on the health and exposure of an asset. Is the asset portable? Then it is more likely to be lost or stolen. Is the asset a web service? Then you can surmise that there may be software vulnerabilities and automated tools to exploit them. The following is a list of example threats. It is in no way a complete list of possible threats but is presented to help you identify your organization’s own risks.

* Operational Management Threats
  + Unforeseen effect of changing or adding software without authorization or prior communication
  + Unforeseen effect of change to an application, operating system, or firmware
  + Vulnerabilities from malware (Trojan horse, spyware, BOTS, worms, and viruses)
  + Inability to regularly patch software
  + Business process/service disruption and/or loss of confidential/sensitive data
  + Malfunction of application or operating system and the inability to roll back to a known good state
  + Unauthorized disclosure of data
* Technical Security and Access Control Threats
  + Vulnerabilities of mobile computing
  + Vulnerabilities of Web 2.0
  + Destruction, misuse, or modification of information assets
  + Lack of traditional network boundaries
  + Unintended consequence of implemented information security controls
  + Unauthorized access to systems and/or data
* Monitoring Threats
  + Inability to adjust to changing technology environment
  + Inability to understand specific application or operating system threats
  + Unknown incidence of security breach
  + Ineffective identification of and response to incidents including communications
* Physical Threats
  + Loss of services
  + Theft or loss of systems/data
  + Injury to or loss of life
  + Unauthorized access to restricted areas
* Asset Identification Threats
  + No accountability for information assets
  + Loss of information assets due to misclassification and non-classification of data
  + Misclassification of data due to aggregation
* Account and Identity Management Threats
  + Unauthorized access to resources
  + Improper use of sensitive information
  + Lack of credential management after job role change or employee separation from the university

### LIKELIHOOD

Determining the likelihood of a threat occurring isn’t always a straight-forward process. It often involves assessing numerous variables that may be unique to a given threat and is therefore beyond the scope of this document. For this exercise, assume that a threat will occur and focus on what the impact would be to your organization.

### IMPACT

Use the table below to determine the potential impact to your organization for each risk.

|  |  |
| --- | --- |
| **IMPACT TABLE** | |
| **IMPACT** | **DESCRIPTION** |
| **HIGH** | Catastrophic data loss or corruption, catastrophic effect on annual budget, complete loss of primary services, high news coverage, brand damage |
| **MEDIUM** | Significant data disclosure or corruption, significant effect on annual budget, interruption of primary services, moderate news coverage, loss of goodwill |
| **LOW** | Minimal data disclosure or corruption, minor effect on annual budget, interruption of secondary services, low news coverage, minimal reputation damage |

## ADDRESSING RISK

There are four ways that you can address risks:

* **Avoid** the risk by discontinuing the activity or performing it in a different way
* **Transfer** the liability for the risk to someone else through insurance or contract
* **Accept** the risk
* **Reduce** the risk by creating, enhancing, or applying controls

The following table represents a simple way to estimate the level of effort required to avoid a risk by changing a business process, transfer a risk, or to implement a security control that reduces a risk. Specifics should be tailored to fit your organization. Refer to the [Information Security Guideline](http://ciso.washington.edu/site/files/Information_Security_Guideline.pdf) for more details on the controls outlined in [Administrative Policy Statement 2.6](http://www.washington.edu/admin/rules/policies/APS/02.06.html).

|  |  |
| --- | --- |
| **EFFORT TABLE** | |
| **EFFORT** | **DESCRIPTION** |
| **DIFFICULT** | $$$ - Project, RFP & contract, possible budget change, multiple people, more than 120 hours, new/complex system implementation |
| **MODERATE** | $$ - Purchase order, one or two people, up to 120 hours, new or modification of existing system |
| **EASY** | $ - Small purchase, one person, less than 40 hours, modification of existing system |

|  |
| --- |
| **BACKGROUND** |
| *Organization, Departmental Unit* |
| *Date* |
| *Author(s)* |
| *Assets, threats, assumptions...* |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| # | RISK STATEMENT | IMPACT | ADDRESSING THE RISK | EFFORT |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |