

Risk Analysis Survey

BASELINE DEVELOPMENT

The initial phase of the overall Risk Analysis project can be divided into two primary phases. This is done not only to identify risk and threats to the organization, but also to help determine value of identified assets. Depending upon the size of the organization, the tasks involved in analysis may be divided among many resources. The second phase consists primarily of a checklist type document that can be used to help assess where each agency is as far as risk/threat readiness.

The two primary core steps involved in Risk Analysis are:

1. **Identifying Risks:** Your baseline and information gathering phase of the overall Risk Assessment is to qualify what assets and resources your organization currently has and quantify the threats and risks to them. The first component of the risk analysis process is to gather documentation related to the current processes safeguarding electronic protected health information. This includes an inventory of existing policies, procedures, agreements, related documentation and/or mechanisms relating to overall business continuity. This is addressed in the attached DRAFT Risk Analysis Checklist.
2. **Analyzing Risks:** Once the information identifying potential risks/threats to be addressed is collected, the next step is to analyze and understand what are the costs associated. Outlined below are two matrices to help with the process of evaluating the overall risk factors.

The first example will assist in determining the appropriate general landscape your organization's IT environment. By determining these occurrences and effects, the agency creates a baseline of risk.

The first step is the compilation of a comprehensive list of the information the organization works with on a daily basis. Using this list, the Failure Mode, Effects, and Criticality Analysis process identifies the following:

- (1) *Application.* Identify the applications or processes in place at the site along with the data associated with the application, (e.g., patient registration database/patient intake data).
- (2) *Potential Failure.* List the known and potential failures that could occur at the location(s) (e.g., incorrect data input, loss of data).
- (3) *Failure Effect.* Identify the known and potential failure effects that would result from an occurrence of each failure: that is, list the consequence of the failure and the specific effect to the

environment (e.g., incorrect information on record, misidentification).

- (4) *Cause*. List the known and potential causes for each failure (e.g., poor data entry).
- (5) *Mitigation*. Examine the control mechanisms that are in place to eliminate or mitigate the failure (e.g., no mechanism to check accuracy).
- (6) *Required Action*. Determine actions needed to mitigate the risks identified to minimize or eliminate application or critical data failures (e.g., staff education).

With this you can next compile a comprehensive list of the functions performed at the organization and list the types of failures that could occur. Again evaluate the causes and effects of the different failures and establish techniques to minimize or eliminate the risk. Such as:

Application/ Critical Data (PHI)Processed	Potential Failure	Failure Effect	Cause	Mitigation	Required Action
Telephone inquiries	Inadvertent disclosure of PHI to incorrect recipient	Improper disclosure of PHI	Lack of employee training	Train staff on proper disclosure processes	Establish employee training program
Recordkeeping of patient information	Loss of electronic data	Loss of patient data	Intentional vandalism, i.e., deletion of records	System input logging	Ensure logging is enabled
Information that is transmitted electronically to a payer or other outside entity	Use of incorrect code set	Request rejected	Employee fatigue	Establish training and regular breaks	Establish work standards and policies

In addition, the table below is a list of information failures and their possible cause that may be appropriate for evaluation in the work area environment.

Information Failure	Possible Cause
Inadvertent deletion of information	Operator error
Intentional deletion of information	Internal vandalism, hacking
Incorrect receipt of electronic data from outside source	Information distribution error
Incorrect distribution of data to an outside source	Misdirected information
Date file corruption	Application failure

Hardware failure	Physical damage or obsolescence
Virus, Trojan, worm	Introduction of an electronic foreign agent

The second chart to assist in the process of assessment is illustrated below. This chart takes the identified assets as detailed above and places them in a matrix to help determine the key factors of priority/criticality.

To help in establishing **Confidentiality**, **Integrity** and **Availability**; we have included a few examples along with method used to determine each.

Overall System Criticality

System	Confidentiality	Integrity	Availability
Example 1	High	High	High
Example 2	Low	Medium	High
Example 3	Medium	Medium	Low
Overall	High	High	High

Systems Information Criticality

A. Example 1

1. Impact Definitions

a. High

- (1) *Public disclosure of personal medical history*
- (2) *Inability to make payments to providers*
- (3) *Safety of staff*

b. Medium

- (1) *Significant delay in payments to providers*
- (2) *Loss of productivity*

c. Low

- (1) *Minor delay in payments to providers*

2. System Criticality

Confidentiality	Integrity	Availability
High	High	High

B. Example 2

1. Impact Definitions

a. High

- (1) *Data integrity is compromised*

- (2) *Sustained inability to access/use resources*
- b. Medium
 - (1) *Minor delay in access/use resources*
 - (2) *Loss of productivity, re entry of data*
- c. Low
 - (1) *N/A*

2. System Criticality

Confidentiality	Integrity	Availability
Low	Medium	High

Systems Information Criticality

A. Example 3

Impact Definitions

- b. High
 - (1) *N/A*
- b. Medium
 - (1) *Loss of productivity, re entry of data*
- c. Low
 - (1) *Loss of productivity*

2. System Criticality

Confidentiality	Integrity	Availability
Medium	Medium	Low