Risk Analysis Exercise

by [admin3](http://usaonlineessays.com/author/admin3/) · November 28, 2015

Perform a formal risk assessment for the three following assets and threats. Use the Risk Register table provided below for your answers. Justify your decisions.

1) As part of a formal risk assessment of desktop systems in a small accounting firm with limited IT support, you have identified the asset “integrity of customer and financial data file on the desktop systems” and the threat “corruption of the files due to import of a worm/virus on to system.” Suggest reasonable values for the items risk register (below) for this asset and threat, and provide justifications for your choices.

2) As part of formal risk assessment of the main file server for a small local police department, you have identified the asset “integrity of case investigation records on the server” and the threat of “accidental/intentional delete or altering of the records by an employee” as the threat. Suggest reasonable values for the items risk register (below) for this asset and threat, and provide justifications for your choices.

3) As part of a formal risk assessment on the use of laptops of a large government department, you have identified the asset “confidentiality of personnel information in a copy of a database stored unencrypted on the laptop” and the threat “theft of personal information, and its subsequent use in identity theft caused by the theft of the laptop.” Suggest reasonable values for the items risk register (below) for this asset and threat, and provide justifications for your choices.

Risk Register Table

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **S/No.** | **Threat**  **(Cause & Risk)** | **Asset Effected** | **Consequence** | **Existing Controls** | **Likelihood / Probability** | **Vulnerability / Impact** | **Level of Risk / Exposure** | **Risk Priority** | **Remarks** |
| 1 | **corruption of the files** due to import of a worm/virus on to system | Integrity of customer and financial data file on the desktop systems |  |  |  |  |  |  |  |
| 2 | accidental/intentional delete or **altering of the records** by an employee | Integrity of case investigation records on the server |  |  |  |  |  |  |  |
| 3 | **theft of personal information**, and its subsequent use in identity theft caused by the theft of the laptop | Confidentiality of personnel information in a copy of a database stored unencrypted on the laptop |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |

Risk Analysis Assignment

Perform the following tasks as specified.

### Analyze risks

Repeat the following tasks until you are satisified with the result:

### Analyze probability

|  |
| --- |
| For each threat, assess the probability that the function will fail to behave as required, based on your assessment of the technical difficulty of implementing the function.  Use the qualitative scale described in the risk analysis procedure. The probability is an assessment of the likelihood that the *product implementation* will fail to meet the requirement as specified, not that the user will make a mistake. In other words, we are interested in the probability that the product will fail to detect invalid input, or fail to correctly handle valid input, or otherwise behave incorrectly. We are not interested in the probability that a user will use a function incorrectly, or provide invalid input, or otherwise misuse the product. |

### Explain probablity

|  |
| --- |
| Explain the reason for your assessment. |

### Analyze impact

|  |
| --- |
| Assess the *impact* of a function's failure, based on your understanding of the product's purpose and your assessment of how a failure of that kind might affect the end user or customer, and/or the developer's bottom line. You should consult the project authority if you can't determine the impact with confidence. Again, use the qualitative scale described in the risk analysis procedure.  One way to do this is to identify the function(s) most and least likely to fail, then compare other functions to these. Determine the most severe failure in terms of impact, and assign this an impact of Definitely High. Then compare other functions to this ``benchmark.''  The customer's requirements list can give another clue, as these are ordered by importance: items at the bottom of the list are less important, and therefore would have lower impact if they fail. |

### Explain impact

|  |
| --- |
| Write a brief justification for the value you chose. |

### Document result

|  |
| --- |
| For each risk analysed, write a separate entry, including the following bulleted or numbered sub-sections:   * + 1. Function description.     2. Probability assignment and justification.     3. Impact assignment and justification.     4. Exposure calculation (value to be added later).   *Example Format*   * + 1. ...     2. ...     3. Function: File->Load        - Probability: definitely unlikely. Reason: this is a technically straightforward feature involving simply opening a file and reading its contents. Most of the hard work is done by the operating system.        - Impact: definitely high. Reason: if a file cannot be loaded the tool is useless.        - Exposure: 1 \* 9 = 9     4. ...     5. ...     6. ...   Note: You may find that many functions have the same justification for their probability or impact. If this is the case, write an introductory paragraph explaining the broader failure or impact categories into which groups of functions fall; then refer to these categories in your analysis. |

### Determine exposure

Repeat the following tasks until you are satisfied with the result:

### Calculate exposure

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| For each function analysed previously, calculate the *exposure* associated with the function, based on your quantitative assessment:  Exposure = Risk \* Impact    Where the values for Risk and Impact are obtained as follows:   |  |  |  | | --- | --- | --- | | **Assessment** | **Risk Value** | **Impact Value** | | Definitely High | 8 | 9 | | Somewhat High | 6 | 7 | | Somewhat Low | 3 | 4 | | Definitely Low | 1 | 1 | |

### Document exposure

|  |
| --- |
| Add the exposure calculation to the results.  Note: it's important to do the exposure calculation after you have done the qualitative assessment, so that the values for each level do not influence your assessment. |

### Sort results

|  |
| --- |
| Sort the analysed functions by exposure, from highest to lowest. |
|  |

### Create report

|  |
| --- |
| Submit a formatted document, in 12pt type, *stapled* in the upper left hand corner with a *single* sturdy staple. Include a cover page with the document title (name of this exercise), your name and student ID, the name of this course, and the date.  The entries should be ordered by exposure, from highest to lowest.  If for some reason you cannot attend class on the due date, notify me via email ahead of time, and submit your results via email as a PDF attachment (do NOT send Word *doc* files or other formats). When printed, your attachment must conform to the requirements listed above.  The final document is due April 23, 2016, at the beginning of class. |

## 3. Assessment

This exercise will be assessed on the following criteria:

1. Completeness: are all functions covered?
2. Correctness: is the analysis plausible? Are the failures associated with the product, not its users? Are the calculations correct?
3. Presentation: is the writing clear? Is the formatting professional?

Risk Analysis Procedure

## 1. Overview

Risk analysis can help prioritize verification and validation activities by ranking potential problems according to the probability and consequence of their occurring.

We define these concepts as follows:

**Risk**

``The probabilty that undesirable things will happen'' (Kit).  
The chance of failure (Ottevanger).

Example: the system crashes, causing an airplane crash.

**Impact**

The consequence (usually expressed as cost) of an adverse event occurring.

Example: the cost of the lost airplane, plus the compensation to the families of each of the passengers, plus lost future customers.

**Exposure**

A measure of the ``importance'' of the risk, expressed as the risk impact multiplied by the probability:

Exposure = Risk \* Impact

By calculating the exposure associated with each risk, we gain a number by which risks can be ranked, and thus our activities prioritized.

## 2. Addressing Risk

There are X strategies for dealing with risks (threats):

* **Strategies for negative risk or threats** are
  + Avoidance "[...] which naturally involves changing the project management plan..."
  + Transfer the risk effects "to a third party", what naturally does not eliminate the risk
  + Mitigation which "[...] implies a reduction of probability and/or impact of an adverse risk event to an acceptable threshold"
* **Strategies for positive risk or threats** are
  + Exploiting which is a collection of positive effects
  + Sharing by which benefits will be (partially) given to "third parties"
  + Enhancing for getting more of the benefits
* **Strategy for both threats and opportunities** is
  + Acceptance because one cannot change the situation
* **Contingent response strategy** tries to combine risk responses and conditions under which the risk shall be responded

## 3. A Qualitative Technique

The problem with this approach is that it is frequently difficult to accurately estimate risk probability and impact. Insurance companies maintain voluminous records of historical data to aid in making these estimates. We, however, don't have such resources, and fortunately don't need them: since we are mainly interested in ranking risks to prioritize our activities, we only need to establish the relative impact among risks.

This allows you to do a qualitative risk analysis on your chosen product, as follows:

1. Identify product requirements from the specification, feature list, user interviews, etc. State each requirement as concisely and unambiguously as possible.
2. For each requirement or feature, identify potential ways in which the product can fail to meet the requirement.
3. Assign a probability to each potential failure, using the following subjective scale:
   * Definitely likely.
   * Somewhat likely.
   * Somewhat unlikely.
   * Definitely unlikely.
4. Assign an impact to the the risk, using the following subjective scale:
   * Definitely high impact.
   * Somewhat high impact.
   * Somewhat low impact.
   * Definitely low impact.
5. Calculate the risk exposure for each risk, by assigning the following arbitrary values to your subjective evaluations:
   * Definitely likely: 8
   * Somewhat likely: 6
   * Somewhat unlikely: 3
   * Definitely unlikely: 1
   * Definitely high impact: 9
   * Somewhat high impact: 7
   * Somewhat low impact: 4
   * Definitely low impact: 1
6. Order the risks from highest to lowest exposure. This gives you a priority list for your verification and validation activities, based on the risks associated with the product.

This technique exploits a simple two step qualitative analysis to produce a quantifiable risk ordering. For each risk, you must establish

1. Is it likely or not?
2. How likely or not likely is it?

and

1. Is the impact high or low?
2. How high or low is it?

Thus we reduce the risk analysis to a series of binary decisions, which are fairly easy for humans to make.

## 

## 4. Notes

* Events resulting in injury or loss of life are definitely high impact.
* Events resulting in direct financial loss have impact in proportion to the projected loss.
* Events resulting in loss of data are high impact, unless the data can be easily recovered.
* Impact must be considered in the context of the product under consideration. Some products have no financial impact or potential for injury or loss of life. High impact for these products is determined by how the failure affects the usefulness of the product. For example, a word processor can't kill someone, and doesn't do financial calculations, so it won't result directly in financial loss. So, high impact events are things like crashes that result in lost work, corruption of files, etc.
* Don't confuse user error with product failure. User's will make mistakes, but this is not an adverse event unless the product handles the mistake incorrectly.

## 5. Chance of Failure

The chance a product feature will fail is related to how often it's used and how likely it is that mistakes were made in its implementation.