Brian Sandoval
Governor

Jeff Mohlenkamp
Director

David Gustafson
Chief Information Officer

STATE OF NEVADA

DEPARTMENT OF ADMINISTRATION

Enterprise I.T. Services Division

A TECHNOLOGY INVESTMENT REQUEST (TIR) GUIDE:

Defining and Evaluating Risks

November 23, 2011

Version 3

Risk analysis is a critical part of any technology project. Risks determined during TIR phase of a project can be used in later phases of the project lifecycle, particularly during project management.

Definitions of terms:

Major Risk Categories

- **Risk of Doing Nothing** – This risk is specifically addressed in the Background section of the TIR business case (Section 4.3 Risk of Doing Nothing). This risk addresses the consequences of continuing on the same course without taking any intervention, technological or otherwise. It is extremely important for those business cases focused on problem resolution. This is not a risk area addressed in the TIR 's Risk Evaluation Table.

- **Project Specific Risks** – These risks exist for the TIR project irrespective of any specific IT alternative. These risks must be managed during all phases of project planning, implementation and ongoing support of the resulting technology solution. They should be addressed in the Risk Evaluation Table.

- **Alternative Specific Risks** – These risks consider issues encountered during the planning, implementation and support of a particular solution alternative. While other alternatives may share these risks, they differ from the project specific risks in that they do not occur for all viable alternatives. When there is more than one valid alternative solution, comparing alternative specific risks is an important part of a cost benefit analysis.

Types of Risk

- **Economic Risks** – These are risks related to adequate funding for project planning, implementation and ongoing support. It includes unfunded mandates and inadequate initial funding, as well as situations where grant funding starts a project but funding for ongoing support is in question. Another possibility is the potential loss of funding due to lack of compliance with stipulations from a funding authority. Component price changes from when the project was planned to when items are purchased is a risk. Other risk types can result in economic impact (ex. scope changes, a Business Risk, result in costly change orders).

- **Schedule Risks –**This relates to mandated timeframes, or a schedule that may be hard to accomplish considering particular project constraints. Project complexity, available resources, project staffing and management can all contribute to extending the project schedule and should be considered when evaluating schedule risks.

- **Business Risks –**This is the broadest category and incorporates all risks related to business environment and culture, stakeholder involvement and political issues. Primary among these are the risk of inadequately defining requirements, or not considering evolving or changing business requirements. Potential changes in business functions and process should also be considered here. Management and staff "stability" and having adequate project governance should also be considered

- **Technology Risks –**This addresses all of the potential technical barriers to completing the project and supporting the final solution. These include having poorly defined data interfaces, using new "bleeding edge" technology, and acquiring a complex solution that is technically difficult to manage. External contingencies and dependencies on technical components out of the control of the project should be considered.

- **Data Security Risks –** Three primary areas of security risk are addressed in the Risk Evaluation Table. These have been included in the table and should be addressed for each project:

    - Breach of confidentiality: Can the data be acquired by someone who is restricted form access?
    - Loss of data integrity: Can the data be corrupted or invalidated?
    - Loss of access: Can access to the data be disrupted, causing an unacceptable disruption or adverse impact?

  The level of concern you have for any of these issues depends on how you have classified your data. Some data is classified by statute, regulation, or a policy which establishes special requirements: security precautions, restricted access, etc. Other data may be classified as public information available for general access.

Another consideration in data classification is how dependent your critical business functions and applications are on this data. Also, the Maximum Acceptable Outage (MAO) or "downtime" if there were a serious system failure should be considered. If your agency participated in the business impact assessment used in the Critical Business Technology Assessment Program (CBTAP), these questions have probably been answered.

- The State security policies and procedures are available at: <http://infosec.intranet.nv.gov/Security PSPs.htm>. Also, if you have questions or need further information on IT security, contact the Office of Information Security (infosec@admin.nv.gov; 775-684-5800).

Risk Rating Factors

Risk can be rated base on three factors: Probability, Impact, and Control. Each of the three factors can be scored as High (3), Medium (2) or Low (1) in the Risk Evaluation Table.

Probability – What is the likelihood that this will occur?

Impact – If it does occur, what are the consequences? This considers the impact on all stakeholders, consequences on maintaining business service, the continuance of business functions, and the possibility of adverse political implications.

Control – What is your confidence in being able to adequately handle the risk if the situation occurs? This should consider your risk management plan and may include means of avoiding the risk ("dodging the bullet"), mitigating the risk, or in some other way managing the risk so that the effects are reduced to an acceptable level.

Risk Rating

The Risk Evaluation Table calculates Risk Ratings based on the evaluation of these three factors. The Risk Rating is calculated using the formula: Probability + Impact – Control.

Risk Classification Categories

Minimal Risk– Agencies should not spend much effort defining and tracking risks that are not likely to happen and have little consequence. However, the Risk Evaluation Ta-

ble allows low level risks to be recorded, especially since three security categories have been pre-established in the template. One or more of these may result in a very low risk score, but still should be shown as having been considered. For instance, if all of the data is public and open access, the Breach of Confidentiality risk will be marked as "Low" Impact, "Low Probability" and easily managed ("High" Control). The resulting Risk Rating would be a negative score (1+1-3 = -1). The Risk Evaluation Table has been set up to convert all Risk Ratings below "1" to a value of "1." The Minimal Risk Classification applies to Risk Rating scores less than 1.5.

Low Risk – These risks have low to moderate values of Probability and Impact, and are pretty easy to control. The Low Risk Classification occurs for Risk Ratings between1.5 - 2.5.

Medium Risk – This category captures most risks. It covers risks with moderate Probability and/or Impact, as well as those with slightly higher risk evaluations that can be easily managed. This Risk Classification covers values from 2.5 to 3.5

High Risk – This covers risks that are quite likely and may have a severe impact, as well as moderate risks that cannot be easily managed. Risk Ratings between 3.5 and 4.5 are included in this Risk Classification.

Dangerous Risk – These are dangerous risks with a good chance of happening resulting in dire consequences which cannot be managed. Ratings greater than 4.5 are included here. If any of these occur in your Risk Evaluation Table, a warning "Reconsider Validity" shows next to the risk classification. You may wish to readdress your risk assessment in the Alternatives Evaluation Matrix and fail this as a valid alternative.

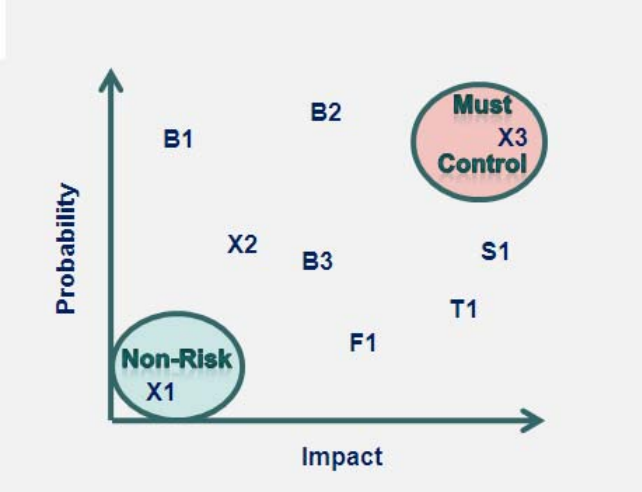


Figure 1.*Example Ranges in Risk Scores*

The above figure, *Example Ranges in Risk Scores*, characterizes most risks as occurring in the middle range of Likelihood and/or Consequence. Things that are of little consequence, such as “1” above, beg the definition of Risk. Things that have little likelihood of happening and are of little consequence (number “3”) may be considered Non-Risks. Things with high ratings on both accounts must be able to be controlled and managed. If this is not possible, the project’s validity should be re-evaluated. If the project is mandated and all viable alternatives have a High or Dangerous risk rating, an intensive Risk Management Plan must be put in place and active for the project to move forward.

Risk Evaluation and Cost Benefit Analysis: The cost benefit analysis workbook includes Risk Evaluation Tables for up to three different alternatives. The results are used along with benefit, cost and functional fit information in a comparative Cost Benefit Analysis: Alternative Comparison Summary

Entering Data into the Risk Evaluation Table:

Risks should be grouped and listed by type. Each risk should be assigned a unique Risk ID starting with a designation of Risk Type ("X"=Security; "B" = Business; "T" = Technical; "F" = Funding; "S" = Schedule), followed by a sequence number. For instance, the first three security risks (X1-X3) have been preloaded into the template for the Risk Evaluation Table. Explanations of what goes into each of the table’s sections are shown in the example on the following page. This is followed by an example of the complete Excel worksheet used as the Risk Evaluation Table.

Example Risk Evaluation Table:

Unique **Risk ID** consisting of Risk Type and Sequence Number

What is the **Impact** of this happening?

The resulting Risk Rating is automatically calculated based on the input for Probability, Impact and Control. The rating is calculated as:
(**Probability + Impact – Control)**

How much **Control** do you have in managing this level of risk?

What is the **Probability** of this occurring?

Identify the **Risk**

Describe the **risk management plan** to deal with the risk.

Risk Type* and #	Risk Factor	Probability 3=High 2=Medium 1=Low	Impact 3=High 2= Moderate 1=Low	Control 3=High 2=Medium 1=Low	How Risk will be Managed	Risk Rating
X1	Breach of Confidentiality	1	1	3	Define and build access controls in parallel w/business functionality.	1
X2	Loss of Critical Data	2	1	3	Develop contingency plans and capabilities in parallel with business functionality.	1
X3	Inability to Access Data	3	3	2	Reduce/eliminate single points of failure.	4
B1	Other conflicting commitment	3	1	2	Acquire management champion; Get commitments	2
B2	Stakeholder issues	3	2	2	Iinclude stakeholders in communication plan.Add peer pressure.	3
B3	Management Changing Mind	2	2	1	Communication plan	3
T1	Hazardous Facility Condition	1	3	1	Increasing leaks in computer area; move computers	3
S1	Mandated Timeframe	2	3	1	Incorporate strick change and scope control.	4
F1	Questionble Funding	1	2	2	Seek secondary grant funding	1
	Average	**2.00**	**2.00**	**1.89**	**Average Risk Rating**	**2.44**

* Key to Types: "X"=Security; "B" = Business; "T" = Technical; "F" = Funding; "S" = Schedule

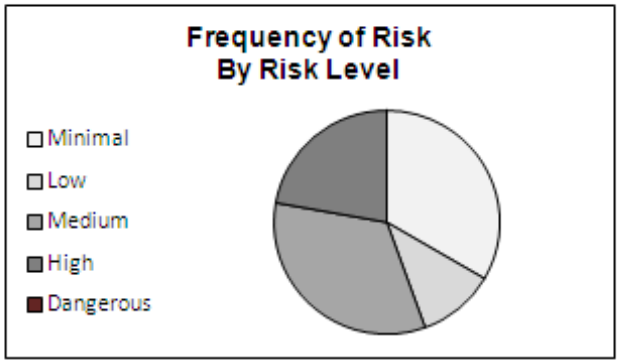
Calculated **Average Risk**

TIR Risk Worksheet: The example below represents the Excel worksheet used as the Risk Evaluation Table <hyper-link>. As previously indicated, the **Risk Rating** is automatically calculated, as are the Frequency Table and Chart.

					For Fiscal Year	*20xx*
	TIR Name:	*Large Example Project*				
	Agency Name:	*Division of xyz, Department of zyx*				
	Budget Account:	*$$$$*		**Decision Unit:**	*E-582*	
	Alternative 1:					

Risk Value	Risk Level	Frequency	Cumulative
1	Minimal	3	3
2	Low	1	4
3	Medium	3	7
4	High	2	9
5	Dangerous	0	9

Average Risk	**2.44**
Risk Classification	**Low**



Risk Type* and #	Risk Factor	Probability 3=High 2=Medium 1=Low	Impact 3=High 2=Moderate 1=Low	Control 3=High 2=Medium 1=Low	How Risk will be Managed	Risk Rating
X1	Breach of Confidentiality	1	1	3	Define and build access controls in parallel w/business functionality.	1
X2	Loss of Critical Data	2	1	3	Develop contingency plans and capabilities in parallel with business functionality.	1
X3	Inability to Access Data	3	3	2	Reduce/eliminate single points of failure.	4
B1	Other conflicting commitment	3	1	2	Acquire management champion; Get commitments	2
B2	Stakeholder issues	3	2	2	Iinclude stakeholders in communication plan.Add peer pressure.	3
B3	Management Changing Mind	2	2	1	Communication plan	3
T1	Hazardous Facility Condition	1	3	1	Increasing leaks in computer area; move computers	3
S1	Mandated Timeframe	2	3	1	Incorporate strick change and scope control.	4
F1	Questionble Funding	1	2	2	Seek secondary grant funding	1
	Average	**2.00**	**2.00**	**1.89**	**Average Risk Rating**	**2.44**

* Key to Types: "X"=Security; "B" = Business; "T" = Technical; "F" = Funding; "S" = Schedule