www.cvr-it.com
info@cvr-it.com

Overview

Standard Risk Register

CVR/IT Consulting LLC

Introduction

The Standard Risk Register is a full featured implementation of the risk register as commonly used in project management. Use this tool in any project where it is necessary to track identified threats and opportunities, information about analysis of those risks, and plans made to manage them. The Standard Risk Register**:**

- Supports proactive management of project risk
- Allows adjustment of risk priority thresholds
- Includes separate registers for Threats and Opportunities
- Is based on a spreadsheet format that is easy to use
- Is available at very low cost

Std Risk Register Features

1. Supports Risk Management activities described in the PMBOK®
2. Provides separate registers for threats and opportunities
3. Includes a Risk Ranking Matrix with customizable probability and impact values, and dynamic risk priority thresholds
4. Worksheet layout supports the natural flow of risk management work
5. Threat detectability chart reveals significant threats that could arrive without warning
6. Threat and Opportunity scores are color coded to indicate risk importance
7. Includes step by step instructions and extensive pop-up help
8. Includes customizable dropdown lists
9. Instructions are color-coded to relevant sections of the risk registers

Instructions

Instructions provide guidance on how to use the Standard Risk Register as part of your risk management practice.

1. Separate instructions are provided for Threat and Opportunity Management
2. Instructions point out the primary questions to be answered during each step of risk management
3. Color and number of each instruction heading map to risk register headings
4. Instructions are preformatted for easy printing
5. You can modify the instructions to fit your specific risk management methodology

Instructions

In this slide the first 4 of 7 sections are shown for Threat Management. Colors and numbers map to the risk register headings. Separate instructions are provided for Opportunity Management.

Engage in Threat Management

1. Threat Identification - What threats exist in the project? Which aspect of the project could each threat affect?

a. As threats are identified, enter information about them in the Risk Identification section of the Threat Register. Be certain to give every threat a unique I.D. as shown.
b. Be certain to use many risk identification tools and techniques such as Risk brainstorming, Risk Breakdown Structure, Risk checklists, etc.
c. Identify the Risk Type of each risk. By default a risk can be a project, business or business value risk, but you can modify that list.
d. Identify Impact Areas for each threat. Select from a list of Triple Constraint factors, and then select from a list of sources of risk that you create. That list could be derived from your Risk Breakdown Structure and could include, for example, technology, budget, staff and more.

2. Qualitative Risk Analysis - How severe are the threats? Which threats warrant further analysis?

a. For each threat fill in every field in the Qualitative Risk Analysis section
b. Be very clear about the root cause of any threat. You may not be able to manage the threat effectively if you do not know root cause.
c. When you finish this analysis unProtect the worksheet, select all rows with risk information, sort on the Status (= Observe) and Threat Score columns, then reProtect the worksheet. This will put all of the most important threats at the top of the worksheet.

3. Extended Risk Analysis - For each risk, what will you do if the event happens? When is it likely to happen? How urgent is the threat?

a. Perform extended threat analysis on any threat whose Threat Score is above your predetermined threshold.
b. Describe what actions you will take if the threat event happens.
c. Describe what impact the threat event could have on the project
d. Document the level of Risk Urgency and Risk Event Timing.

4. Proactive Threat Response Planning - How can you eliminate or minimize the threat?

a. For each risk above your threshold document your preferred proactive response strategy (if you have one).
b. Indicate the type of Response you will use, e.g. Avoid or Mitigate Impact.

Dynamic Priority Chart

The Priority Chart allows you to set the threshold for High and Medium risk to a level that fits the risk tolerance of your customer. Features include:

1. The default values for Impact (1 through 9) and Probability (0.1 to 0.9) can be changed
2. Threshold for Threat and Opportunity can be set independently
3. Threshold for High and Medium risk can be set independently
4. Scores in the priority grid change color to match thresholds
5. Settings in this chart determine numeric values and colors used in the Threat and Opportunity registers

Priority Chart - Overview

Priority Chart

Project Name: Your Project

Threat Priority Thresholds	
High	4.5
Medium	2

Opportunity Priority Thresholds	
High	4.5
Medium	2

Instructions: You can customize your Risk Score values by doing the following:

1. Enter Impact and Probability Scores (or use default provided)
2. Enter Priority Threshold scores for Threats
3. Enter Priority Threshold scores for Opportunities

Color coding indicates priority of Risks and Opportunities.
When you enter risk impact and probability values on the ThreatRegister and OpportunityRegister tabs, the scores and colors shown in the Risk Score columns will reflect the values you set on this page.

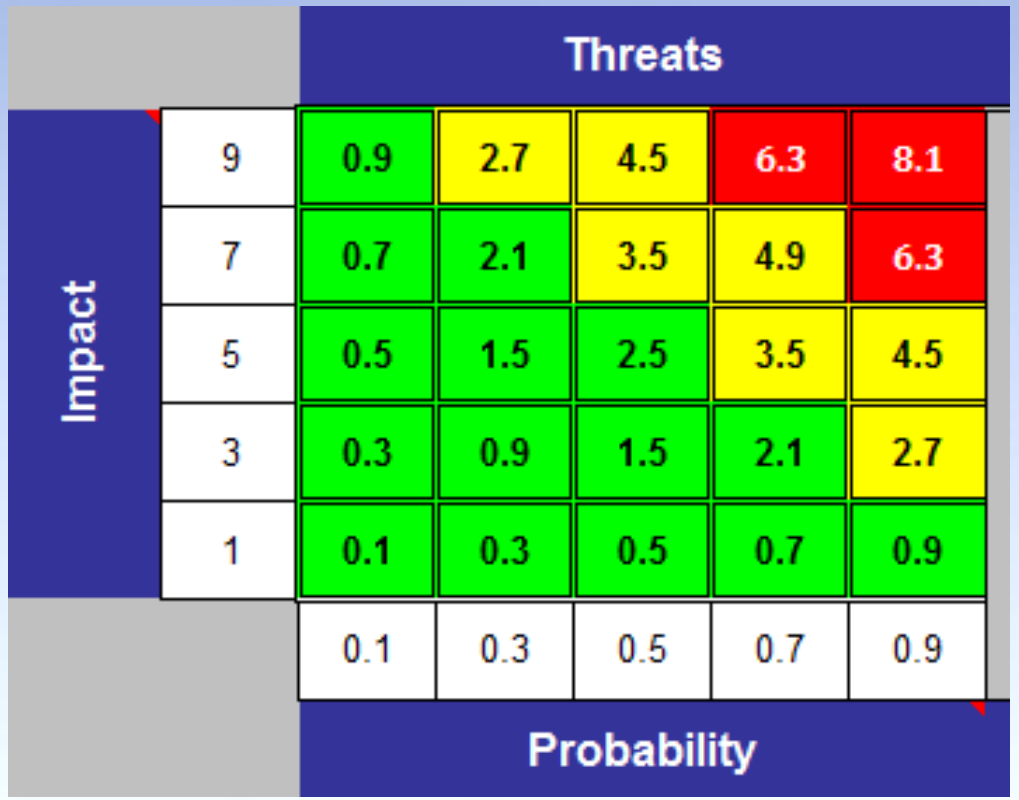
Threats		Opportunities	
	= High Priority		= High Priority
	= Medium Priority		= Medium Priority
	= Low Priority		= Low Priority

		Threats					Opportunities				
Impact	9	0.9	2.7	4.5	6.3	8.1	8.1	6.3	4.5	2.7	0.9
	7	0.7	2.1	3.5	4.9	6.3	6.3	4.9	3.5	2.1	0.7
	5	0.5	1.5	2.5	3.5	4.5	4.5	3.5	2.5	1.5	0.5
	3	0.3	0.9	1.5	2.1	2.7	2.7	2.1	1.5	0.9	0.3
	1	0.1	0.3	0.5	0.7	0.9	0.9	0.7	0.5	0.3	0.1
		0.1	0.3	0.5	0.7	0.9	0.9	0.7	0.5	0.3	0.1
		Probability									

The Priority Chart allows separate High and Med risk thresholds for Threats and Opportunities.

Values entered here are used in the Risk Registers.

Settings for High Risk Tolerance

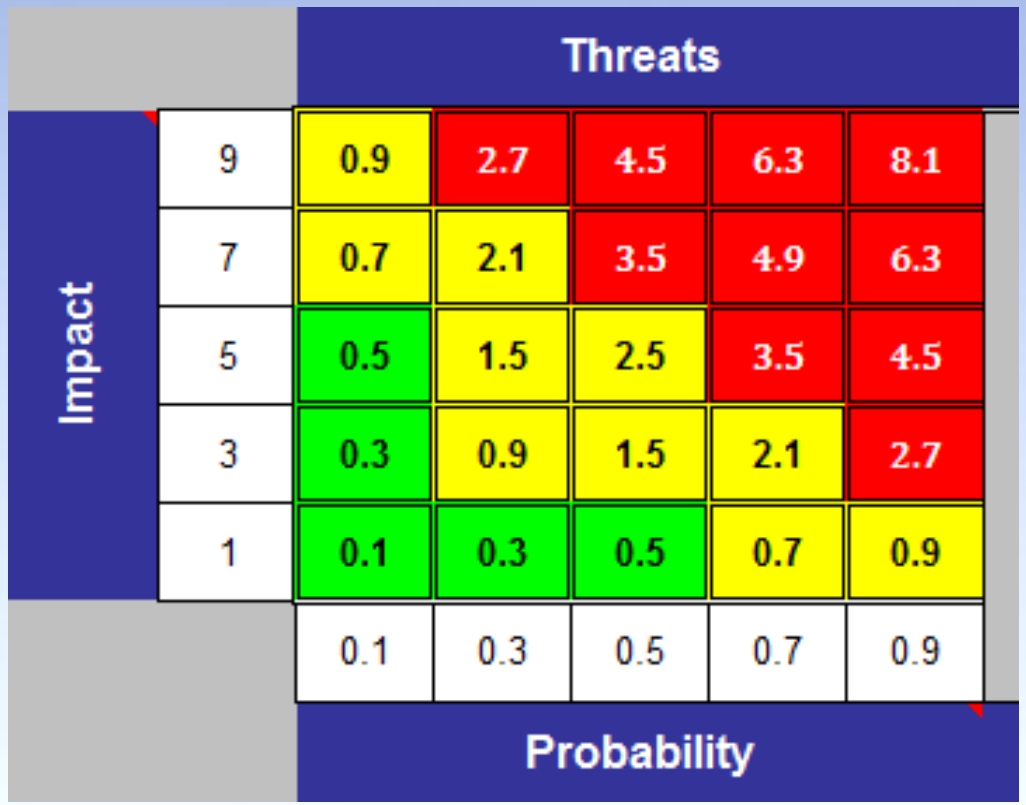


Threat Chart with threshold values set for high risk tolerance:

High = 6.3 and above

Medium = 2.7 to 4.9

Settings for Low Risk Tolerance



Threat Chart with threshold values set for low risk tolerance:

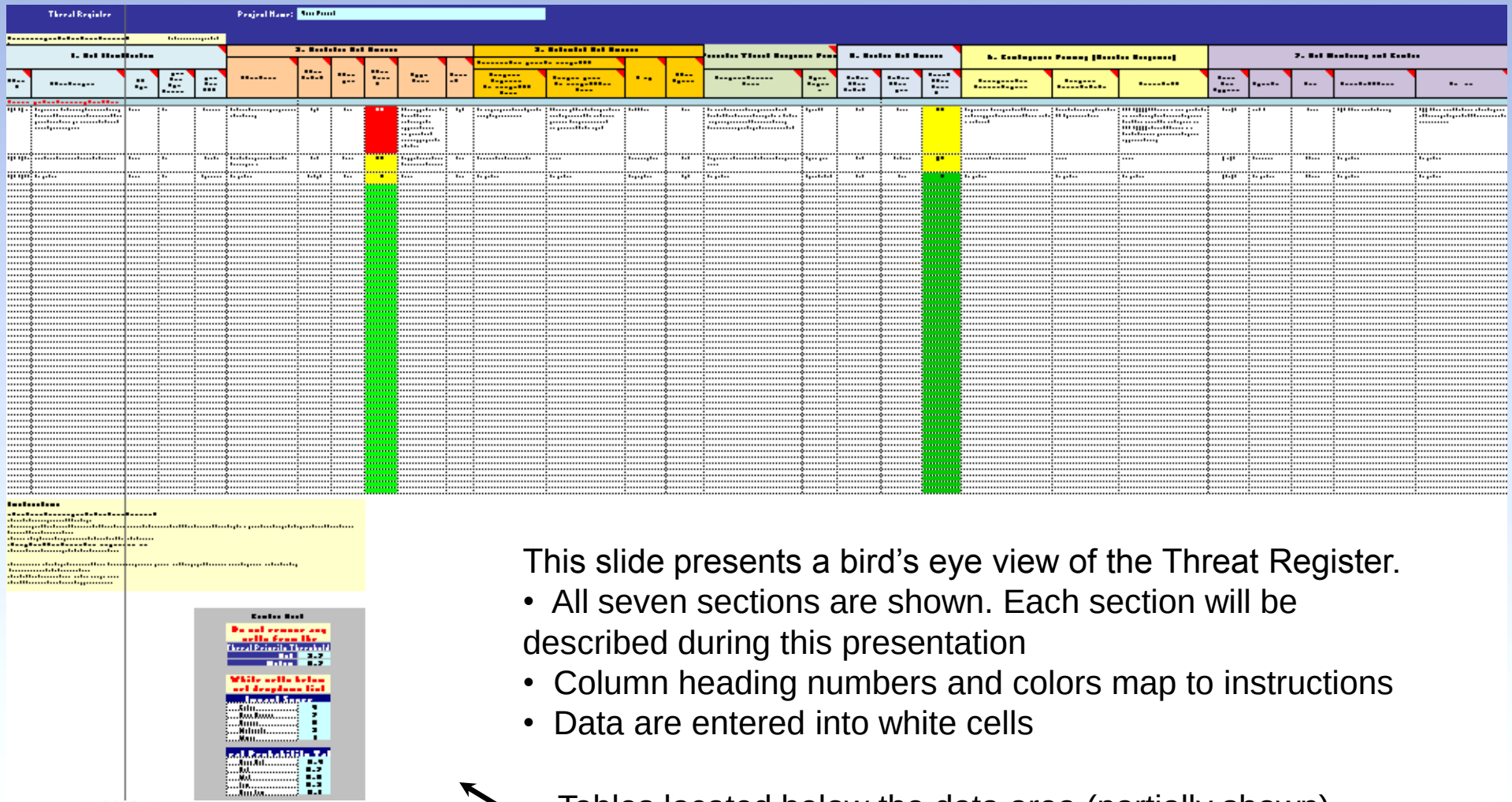
High = 2.7 and above

Medium = 0.7 to 2.5

Threat Register Features

1. A full complement of risk data can be recorded for each threat
2. Drop down lists are fully customizable
3. Records Residual Risk remaining after proactive actions have been taken
4. Every column heading provides mouse-over help
5. Cells with formulas are locked for protection. However, the spreadsheet can be unlocked as needed
6. Sections are color coded to match instructions

Threat Register - Overview



This slide presents a bird's eye view of the Threat Register.

- All seven sections are shown. Each section will be described during this presentation
- Column heading numbers and colors map to instructions
- Data are entered into white cells

Tables located below the data area (partially shown) control content of drop down lists in the worksheet

Risk Identification Features

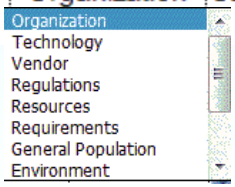
The Risk Identification section of the Threat Register is used to record basic information about each threat. It provides the following features:

1. Allows for each risk to have a unique ID
2. Provides guidance on how to write an effective risk description
3. Supports entry of Risk Type (e.g. Project risk, Business risk)
4. Supports entry of two views of Impact Area (i.e. impact on Triple Constraint; impact on aspects of the project)
5. Mouse over help is included in each column heading
6. Drop down lists are fully customizable
7. The color of column headings make clear which columns are used in Risk Identification
8. Risks may be sorted with active, most important risks at the top

Risk Identification (1)

1. Risk Identification					2. C
Threat ID	**Threat Description**	**Risk Type**	**Impact Area (Triple Constraint)**	**Impact Area (RBS)**	
Delete sample data before using this worksheet					
T120510a	If the project team has difficulty using the new technology, there could be a cost overrun due to extra work hours, plus a substantial delay in implementation which would result in a big financial penalty	Project	Cost	Resources	Staff do not have training or experience in this technology
T120615a	If vendor fails to deliver we will have to build it ourselves	Project	Cost	Vendor	Vendor has a poor track record for delivering on time
T120615b	Sample data	Business	Cost	Organization	Sample data

Impact Area (RBS) indicates the source of risk as defined by your Risk Breakdown Structure (RBS). Default values are provided but you can change these with your own by modifying the Control Block below the data area.



All risk identification data go here. Mouse over help for Impact Area is shown (upper right). The drop list for Impact Area (lower right) contains elements from a Risk Breakdown Structure.

Qualitative Analysis Features

The Qualitative Analysis section of the Threat Register examines the approximate level of risk in each threat. It provides the following features:

1. Probability, Impact and Detectability are all supported
2. Verbal measures are used (e.g. High, Medium, Low) rather than numbers; this is more intuitive for many stakeholders
3. Verbal measures are converted to numeric scores for calculation of Threat Score
4. Threat Score value and color are based on Priority Chart threshold settings
5. Entry of Root Cause and Trigger data are supported
6. Threat ID and Description are shown at all times even as the view of the spreadsheet scrolls to the right

Qualitative Analysis

2. Qualitative Risk Analysis						3.
Threat Cause	**Threat Probability**	**Threat Impact**	**Threat Score (P x I)**	**Trigger Event**	**Detecta - bility**	
Staff do not have training or experience in this technology	High	Critical	6.3	Obvious trigger. If the team has difficulty with the new technology it will be apparent by failure to complete tasks and constant slippage of the schedule	High	
Vendor has a poor track record for delivering on time	Med	Serious	2.5	No trigger. We won't know they are late until they are late.	Low	Do lots of work we don't want to do
Sample data	Very High	Minor	0.9	None	Low	Sample data
			0			
			0			

Detectability is a measure of how much advance warning you will have when the threat actually happens. Threats with low detectability are inherently more dangerous. Detectability scores are numeric as follows:

1 =High detectability
3 = Medium detectability
5 = Low detectability

All qualitative analysis data are entered here. Mouse over help for Detectability is shown (upper right). Verbal scores (e.g. High, Critical) are converted to numeric scores for computation of Threat Score.

Threat Detectability Chart (1)

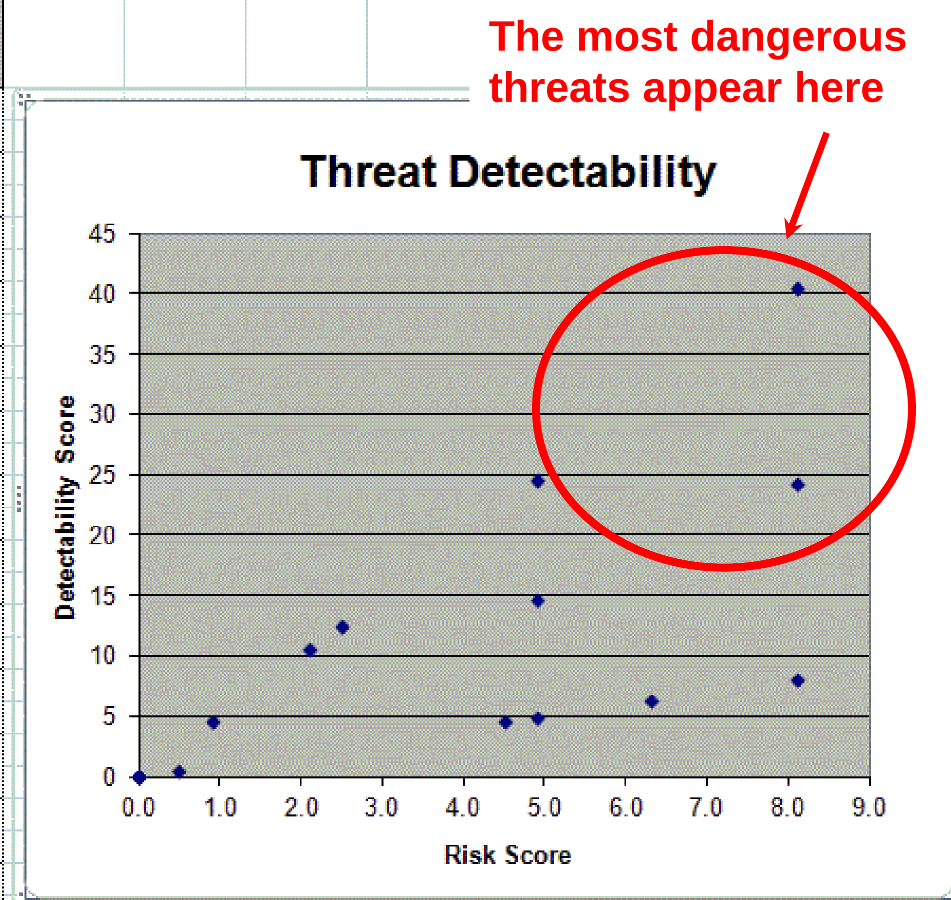
This chart plots threat detectability against Threat Score. It provides a means of identifying the truly dangerous threats, i.e. those high probability, high impact threats that give no warning before they actually occur. Features include:

1. Low Risk Scores are on the left; High Risk Scores are on the right
2. Highly detectable risks are at the bottom; Poorly detectable risks are at the top
3. Threats in the top right quadrant are the most dangerous, i.e. significant threats with low detectability.
4. Chart data are updated automatically as data in the Threat Register is changed

Threat Detectability Chart (2)

Threat Detectability Chart

Risk ID	Risk Score	Risk Score x Detectability	Risk Status
T120510a	6.3	6.3	Active
T120615a	2.5	12.5	Observe
T120615b	0.9	4.5	Observe
T120615c	8.1	8.1	Observe
T120615d	8.1	24.3	Observe
T120615e	8.1	40.5	Observe
T120615f	4.9	4.9	Observe
T120615g	4.9	14.7	Observe
T120615h	4.9	24.5	Observe
T120615i	4.5	4.5	Observe
T120617	2.1	10.5	Observe
T120620	0.5	0.5	Observe
0	0	0	0
0	0	0	0
0	0	0	0
0	0	0	0
0	0	0	0
0	0	0	0
0	0	0	0
0	0	0	0
0	0	0	0
0	0	0	0
0	0	0	0
0	0	0	0
0	0	0	0
0	0	0	0



Extended Analysis Features

The Extended Analysis section of the Threat Register focuses on the likely impact of unmanaged risk. It provides the following features:

1. A full description of the expected response to the unmanaged threat event is captured (i.e. no proactive action was taken)
2. A full description of the impact of the unmanaged threat event is captured
3. Entry of risk urgency and timing is supported

Extended Analysis

3. Extended Risk Analysis			
Quantitative Analysis: Impact of Unmanaged Risk		Timing	Threat Urgency
Description of Response to Unmanaged Risk Event	Description: Impact of Unmanaged Threat Event		
Put more people on the work; provide training; bring in a consultant	The client might decide the assigned staff are not adequate and demand a new project team. Our reputation as a tech company could be damaged.	Build Phase	Low
Do lots of work we don't want to do	none	Execution phase	Med
Sample data	Sample data	Design phase	High

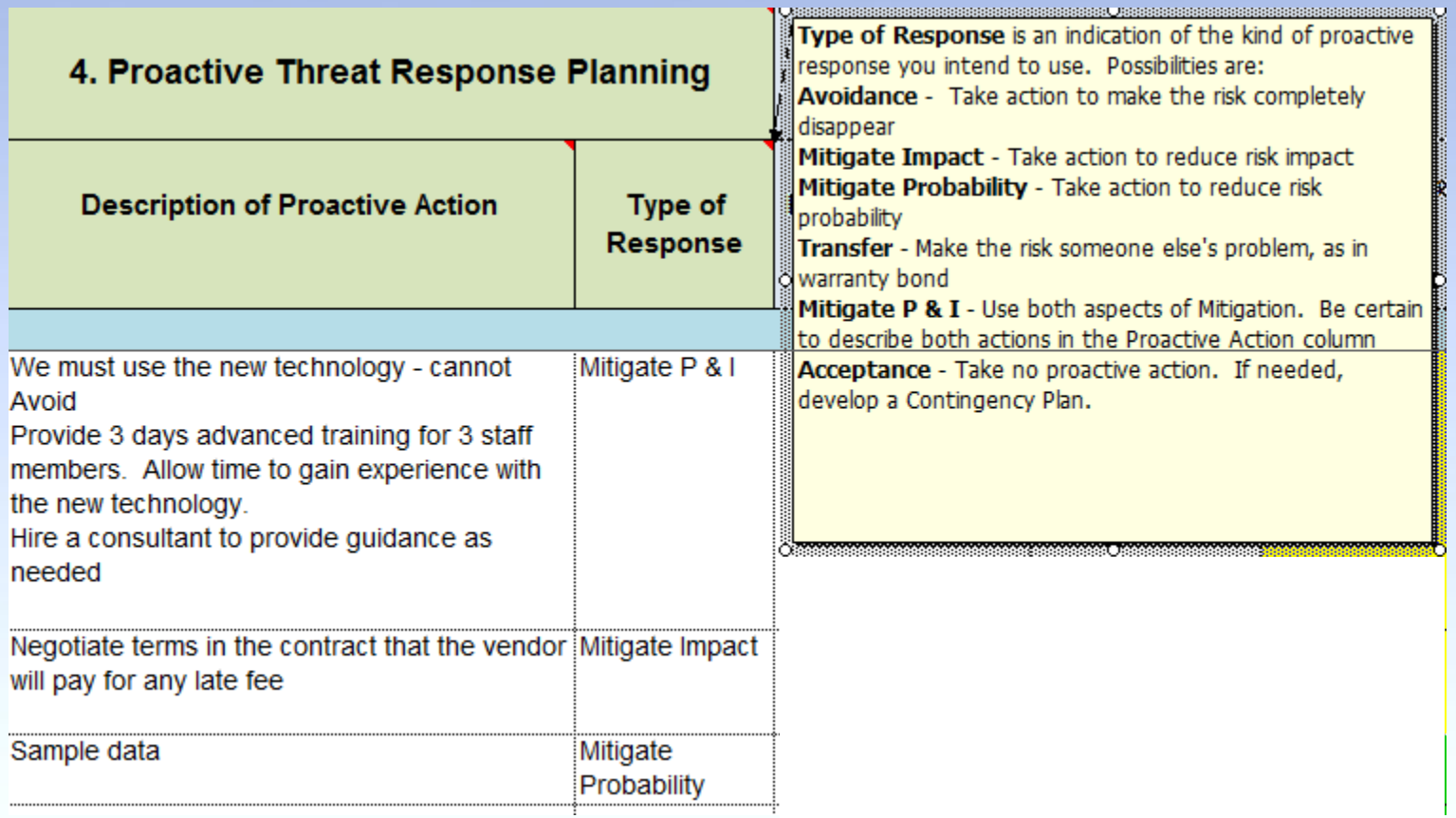
Extended analysis data are entered here. Focus is on the response to and consequences of unmanaged risk..

Proactive Planning Features

The Proactive Threat Response section of the Threat Register records risk management actions that can be taken BEFORE the threat event occurs. It provides the following features:

1. Details of one or more proposed proactive action(s) are recorded
2. Type of response (i.e. Avoidance; Mitigation; Transfer; Acceptance) is captured
3. Drop list for Type of Response contains standard threat response strategies, but these can be customized.

Proactive Planning



4. Proactive Threat Response Planning

Description of Proactive Action	Type of Response
We must use the new technology - cannot Avoid Provide 3 days advanced training for 3 staff members. Allow time to gain experience with the new technology. Hire a consultant to provide guidance as needed	Mitigate P & I
Negotiate terms in the contract that the vendor will pay for any late fee	Mitigate Impact
Sample data	Mitigate Probability

Type of Response is an indication of the kind of proactive response you intend to use. Possibilities are:
Avoidance - Take action to make the risk completely disappear
Mitigate Impact - Take action to reduce risk impact
Mitigate Probability - Take action to reduce risk probability
Transfer - Make the risk someone else's problem, as in warranty bond
Mitigate P & I - Use both aspects of Mitigation. Be certain to describe both actions in the Proactive Action column
Acceptance - Take no proactive action. If needed, develop a Contingency Plan.

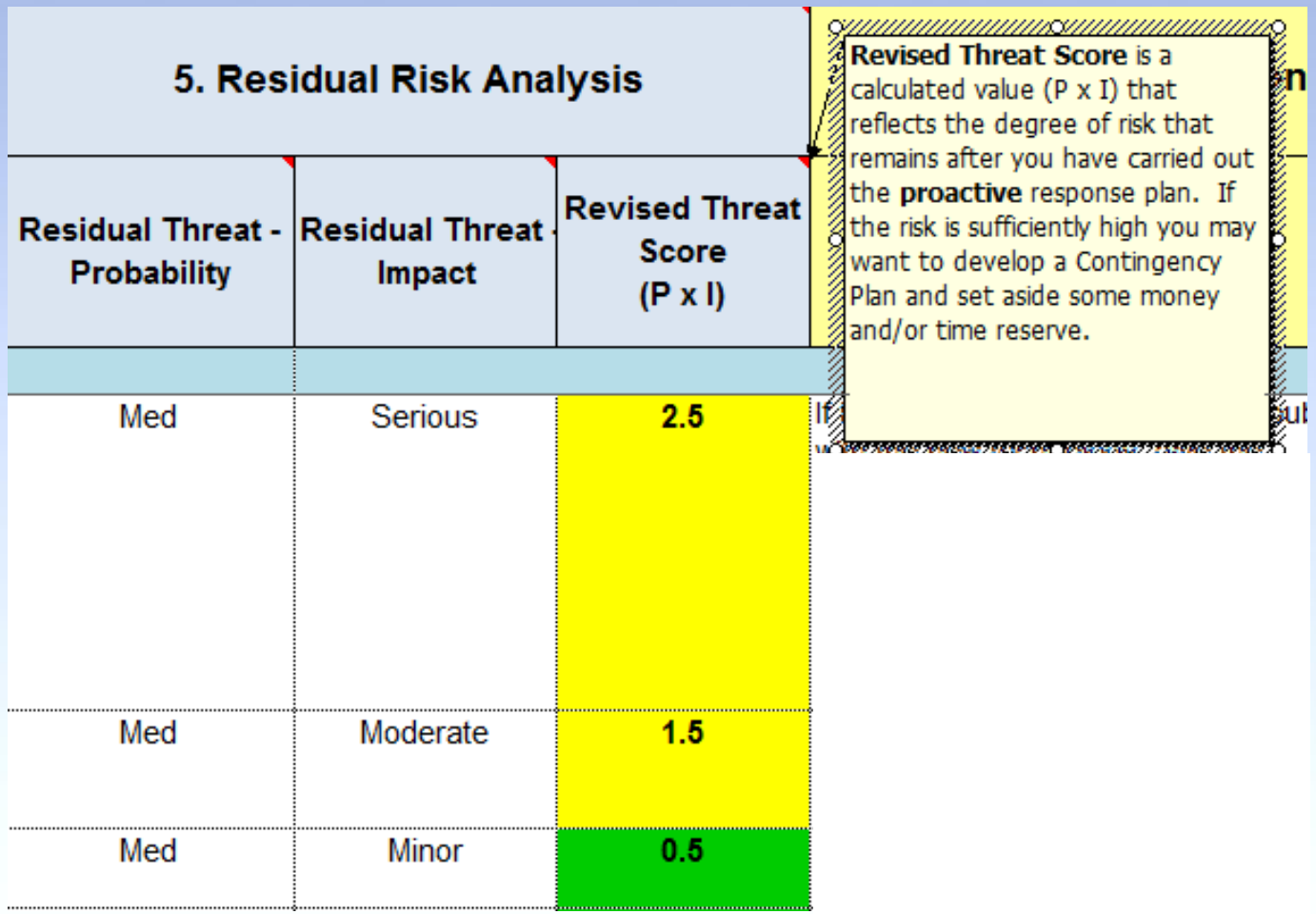
Proactive Response Planning data are entered here. Focus here is on what can be done BEFORE the threat materializes. Mouse-over help for Type of Response is shown.

Residual Risk Analysis Features

The Residual Risk Analysis section of the Threat Register analyses any risk that remains after proactive actions have been taken. It provides the following features:

1. Measures of the risk that remains after proactive actions are taken are entered here
2. Revised estimates of Probability and Impact are used to calculate a Revised Threat Score
3. Revised Threat Score is one indicator of the effectiveness of proactive action (e.g. score is reduced from 6.3 to 2.5; color changes from red to yellow)
4. Revised Threat probability score can be used in Contingency Reserve calculations

Residual Risk Analysis



5. Residual Risk Analysis

Residual Threat - Probability	Residual Threat - Impact	Revised Threat Score (P x I)
Med	Serious	2.5
Med	Moderate	1.5
Med	Minor	0.5

Revised Threat Score is a calculated value (P x I) that reflects the degree of risk that remains after you have carried out the **proactive** response plan. If the risk is sufficiently high you may want to develop a Contingency Plan and set aside some money and/or time reserve.

Residual Risk data are entered here. Mouse over help for Residual Threat Score is shown (upper right)

Contingency Planning Features

The Contingency Planning section of the Threat Register focuses on development of a plan that will be implemented if the threat event actually occurs. It provides the following features:

1. Details of contingency action(s) (i.e. actions to be taken after the threat event has occurred) are recorded
2. A description of any cost in time or money that cannot be avoided by proactive and contingency actions is entered here (e.g. you have mitigated the amount of delay and your contingency response minimized monetary cost, but there is still a delay)
3. A description of any cost in time or money associated with secondary risks is also entered here (i.e. risks that arise as an unplanned consequence of proactive or contingency actions)

Contingency Planning

6. Contingency Planning (Reactive Response)		
Contingency Plan (Reactive Response)	**Description of Unavoidable Cost**	**Secondary Risks**
If the project team is still having trouble with the new technology, give the consultant additional time to do some of the work.	If the work takes too long there wil be a $50k penalty for late delivery	Risk ID 071111b: The customer may complain that if the team needs training, then they are inadequate for the job. Customer could demand replacements. Risk ID 071111c: Business risk: The customer may decide that our company is not an adequate supplier of technology.
Invoice vendor for amount of late fee	none	none
Sample data	Sample data	Sample data

Contingency Planning data are entered here. In addition, information about any unavoidable costs and secondary risks is entered in this section of the Threat Register.

Risk Monitoring and Control (1)

The Risk Monitoring section of the Threat Register focuses on recording metadata about identified risks (e.g. date recorded; assigned to) and tracking risk actions actually taken. It provides the following features:

1. Date that each risk plan is approved is recorded
2. Each risk can be assigned to an individual
3. The status of the risk can change over time. Default statuses include Observe, Active, Closed and Workaround
4. Risk actions can be recorded as they are taken
5. Additional information can be included in the Comments section

Risk Monitoring and Control (2)

7. Risk Monitoring and Control

Date of Plan Approval	Assigned to	Status	Record of Risk Actions	Comments
03-Jun-12	Joe Smith	Active	6/15/08: Team attended training	5/11/08: Customer is satisfied that the team will be adequate with the training to be provided. They will also cover the cost of a consultant.
10-Jul-12	Laura Jones	Observe	Sample data	Sample data
15-Jul-12	Sample data	Observe	Sample data	Sample data

Active
Observe
Closed
Workaround
blank
blank

All Risk Monitoring information is recorded here. The drop down list for risk Status is shown.

Opportunity Register Features

The Opportunity Register is specifically designed to support the management of opportunities. It complies fully with PMBOK response strategies for opportunity.

Features of the Opportunity Register include:

1. A full complement of risk data can be recorded for each opportunity
2. The language of all column headings, mouse-over help, etc. is focused on management of opportunity, rather than threat
3. Drop down lists are fully customizable
4. Records Residual Risk remaining after proactive actions are taken
5. Every column heading provides mouse-over help
6. Cells with formulas are locked for protection. However, the spreadsheet can be unlocked as needed
7. Sections are color coded to match instructions

Opportunity Register

4. Risk Response Planning (Proactive Response)				
Proactive Action (Response Strategy)	Potential Financial Benefit	Potential Labor Hours Benefit	Potential Beneficial Impact on Project Duration (Days)	Other Beneficial Impact
Get approval from the manager of the other department to use the software. Get approval from the vendor.	$100,000.00	1000	10.0	Could improve collaboration with the other department
Sign agreement with vendor to be an "early adopter". This will allow a substantial discount.	$200,000.00	2000	20.0	Test
Sample data	$50,000.00	500	5.0	Sample data

This screen shot highlights the difference in Proactive Response planning between threat and opportunity. Compare this with the earlier slide for Threat Proactive Planning.

Summary

The **Standard Risk Register** is a robust risk management tool that can be used to record identified risks, manage your risk response plans and track risk actions.

The Standard Risk Register is part of a package of risk management tools available at very low cost from this source:

http://www.cvr-it.com/PM_Templates/

Other templates in this set include:

- Comprehensive Risk Register with Cost Analysis (CRRCA®)
- Quick IT Project Risk Evaluator
- Opportunity Discovery template
- Risk Management Plan
- Much more…

About CVR/IT Consulting LLC

CVR/IT Consulting, established in 2002, provides guidance and support in the effective use of Project, Program, Portfolio Management and Business Analysis Technologies. The company provides professional consultation, training and tools in all matters related to Project Management and Business Analysis, such as:

- Implementation of governance structures and processes essential to effective Portfolio Management
- Establishment of a Project Management Office that finds its own success solely in the success of its customers
- Delivery of flexible, customized PM and BA Methodologies and tools
- Assessment of organizational project, program, portfolio management and business analysis practice
- Training (or re-training) of the project workforce
- Implementation of Organizational Change to make it all work

www.cvr-it.com
info@cvr-it.com

Overview

Standard Risk Register

CVR/IT Consulting LLC