



EFFECTIVE TECHNIQUES IN RISK MANAGEMENT

Joseph W. Mayo, PMP, RMP, CRISC

September 27, 2011

Effective Techniques in Risk Management

- Risk Management Overview
- Exercise #1
- Break
- Risk IT
- Exercise #2
- Break
- Risk Management Tools and Techniques
- Q&A



Risk Management Overview

Risk Management Standards

- Project Management Body of Knowledge (PMBOK)
- ISO/IEC 16085 – 2006 Systems and software engineering – Life cycle processes – Risk Management
- ISO 31000 Risk management – Principles and guidelines
- AS/NZS 4360:2004 Risk Management
- Information Systems Audit and Control Association (ISACA) Risk IT

Risk Management Fundamentals

1

- Risk Governance

2

- Risk Analysis

3

- Risk Response / Treatment

Risk Governance

	PMBOK	ANZ-4360	ISO 16085	ISO 31000	Risk IT
Align with Enterprise Risk Management (ERM)		✓	✓	✓	✓
Risk tolerance and risk appetite					✓
Risk policy			✓		✓
Risk management planning	✓	✓	✓	✓	✓

Risk Analysis

	PMBOK	ANZ-4360	ISO 16085	ISO 31000	Risk IT
Identify risks	✓	✓	✓	✓	✓
Maintain a risk register	✓	✓	✓	✓	✓
Estimate and quantify risk impact	✓	✓	✓	✓	✓
Prioritize risks	✓	✓	✓	✓	✓
Establish risk scenarios		✓	✓	✓	✓
Risk frequency		✓	✓		✓

Risk Treatment

	PMBOK	ANZ-4360	ISO 16085	ISO 31000	Risk IT
Risk strategies	✓	✓	✓	✓	✓
Risk treatment / response plan	✓	✓	✓	✓	✓
Monitor ERM alignment and risk tolerance thresholds					✓
Organization's ability to treat the risk					✓
Continuous improvement			✓	✓	✓

Risk Management Summary

1987

2004

2006

2009

Governance				Risk Analysis			Risk Treatment		Improvement	
PMBOK	Risk Management Planning			Risk Identification	Qualitative Analysis	Quantitative Analysis	Risk Response Planning			
ANZ-4360	Communicate & Consult	Establish Context	Identify Risks	Analyze Risks	Evaluate Risks		Treat Risks	Monitor & Review Risks		
ISO 16085	Plan & Implement Risk Management	Manage the Project Risk Profile		Risk Analysis				Treat Risks	Monitor Risks	Evaluate Risk Management Process
Risk IT	Define Risk Universe & Scope Risk Management	Risk Appetite & Risk Tolerance	Risk Awareness, Communication & Reporting		Expressing and Describing Risk		Risk Scenarios	Risk Response & Prioritization		Risk Awareness, Communication & Reporting



Risk Management Process

Governance

- Risk Management Plan (RMP)
 - Compliant with ISO 16085 or AS/NZS 4360
 - PMBOK is weak in governance (e.g. risk policy, risk tolerance, and risk appetite) and specific guidance
- Establish the context
 - Context should include at least schedule and budget
 - Mature organizations can include mission accomplishment

Governance

- Risk Appetite
 - The amount of risk an enterprise is prepared to accept
- Risk Tolerance
 - The amount of risk that an organization is willing to withstand

Governance

- Management Reserve
 - Unknown Unknowns
 - An unknown-unknown is also referred to as a Black Swan event. Black Swan theory is based on Nassim Nicholas Taleb's article describing extreme events that cannot be reasonably conceived to happen (Taleb, 2007).
 - Deepwater Horizon
 - 2004 Indonesian Tsunami
- Contingency Reserve
 - Known Knowns and Known Unknowns
 - Used to managed documented risks (including risks that are accepted)

Risk Analysis

- Identify risks
 - Not issues, conditions, symptoms, events, or opinions
 - Utilize industry accepted nomenclature
 - IF <bad thing> THEN <context> <impact>
 - IF the integration test environment is not complete by Oct 1 THEN <the scheduled implementation> <will be delayed by 2 months>
 - <something happens> LEADING TO <outcomes expressed in terms of impact on objectives>
- Update risk register
 - Document containing the results of risk analysis and planned responses

Risk Analysis

- Objectively quantify impact
 - Based on context
 - Avoid risk normalization
 - A U.S. Government agency normalizes all risks using a Risk Adjusted Cost (RAC). Using the Risk Adjusted Cost calculation, a risk with a \$225,000 budget impact and a “High” probability of occurrence would have the same RAC (\$157,500) as a risk with a \$175,000 budget impact and a “Very High” probability of impact.
- Estimate probability or frequency

Risk Response

- Select treatment strategy
 - Accept, avoid, mitigate, or transfer
- Prioritize Risks
- Develop formal risk treatment / response plan
 - ISO 16085, ISO / IEC 31000, or AN/NZS 4360 compliant
 - Risk response is a weakness in the PMBOK
- Monitor progress against the response plan



EXERCISE #1

RISK MANAGEMENT

OVERVIEW

Fill in the blank

The four industry accepted risk management strategies are _____, _____, _____, and _____

Response, _____, and _____ are the three functional aspects of risk management.

Term Matching

Definition

Describes threats, events, assets, and timing

Document showing how the chosen options will be implemented

The results of risk analysis and response planning

The degree of risk that an entity is willing to withstand

Amount of risk an entity is prepared to accept

Term

Appetite

Risk Register

Scenarios

Tolerance

Treatment Plan

Word Search

G	X	R	X	P	X	B	X	G	B	Y	E	O	G	F	H	S	W	V	B
Q	F	R	K	D	B	H	D	O	W	I	J	Y	N	J	A	L	V	L	L
M	W	E	U	N	I	N	H	Q	C	B	J	C	A	K	Q	N	V	O	W
L	A	T	E	B	S	Y	C	C	D	R	K	N	L	P	G	E	O	Q	S
G	P	S	S	J	U	L	B	Y	E	Q	G	L	P	G	P	P	Y	A	G
H	P	I	C	V	R	G	N	F	V	Y	C	F	T	B	A	A	M	K	O
F	E	G	A	P	V	Y	S	F	A	Y	M	O	N	F	S	I	Q	J	V
Q	T	E	M	E	R	N	K	K	F	C	F	O	E	U	C	I	G	D	E
N	I	R	O	T	A	C	T	J	G	R	C	E	M	X	E	W	U	B	R
C	T	K	I	R	E	T	M	O	N	L	P	X	T	G	N	F	B	S	N
B	E	S	T	T	W	C	R	T	W	K	E	Q	A	U	A	D	F	R	A
Y	V	I	N	H	L	V	N	E	Y	T	W	Z	E	N	R	X	K	I	N
T	D	R	X	V	M	X	F	A	A	R	A	P	R	I	I	L	L	V	C
N	W	M	Q	E	F	Y	T	G	R	X	N	X	T	Q	O	L	P	N	E
F	M	G	U	U	E	P	I	U	T	E	A	G	C	B	S	I	U	N	L
W	C	Y	D	E	E	T	Q	I	W	L	L	I	N	L	H	A	L	W	S
L	Y	Y	G	C	I	V	C	J	K	Y	Y	O	P	L	R	E	A	U	T
P	W	X	C	M	C	E	K	T	E	K	S	T	T	T	B	O	F	F	E
A	Q	A	P	P	V	U	U	L	P	V	I	D	W	V	E	J	C	H	E
D	J	D	Y	R	V	J	Z	S	D	U	S	A	V	O	I	D	Q	F	X

ACCEPT
ANALYSIS
APPETITE
AVOID
GOVERNANCE
MITIGATE
RISK REGISTER
SCENARIOS
TOLERANCE
TRANSFER
TREATMENT PLAN



Break



ISACA's Risk IT

Risk IT at a Glance

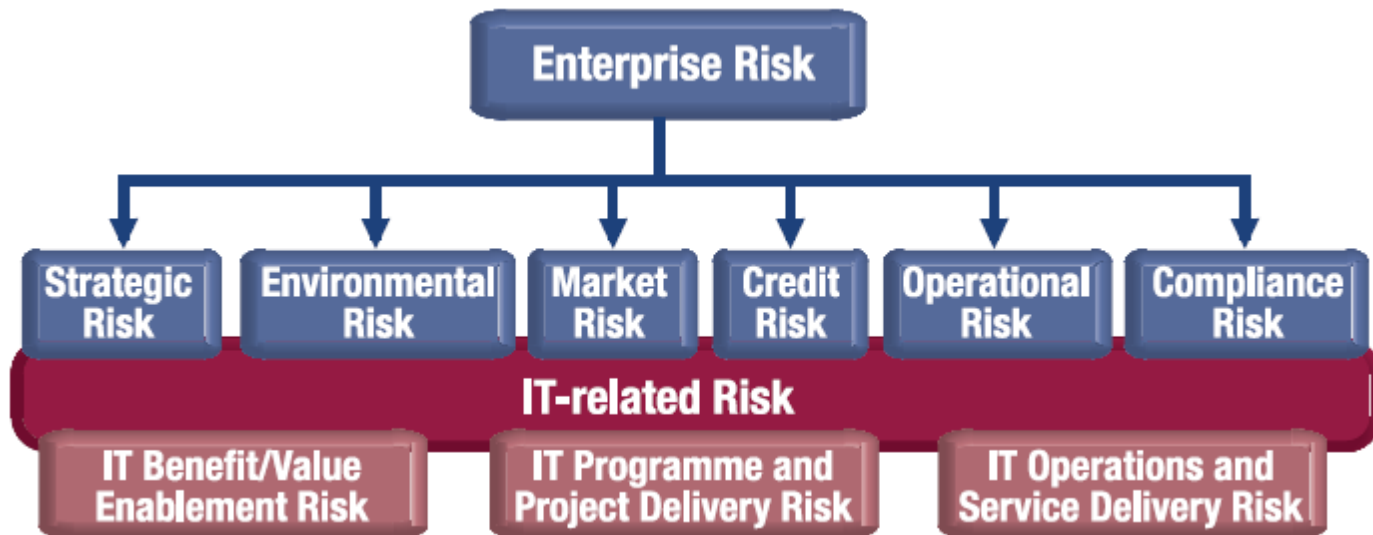


Risk IT

- Define Risk Universe and Scoping Risk Management
- Risk Appetite and Risk Tolerance
- Risk Awareness, Communications, and Reporting
- Expressing and Describing Risk
- Risk Scenarios
- Risk Response and Prioritization

Define Risk Universe and Scoping Risk Management

- Consider overall business objectives
- Establish risk context(s)
- Develop a risk management plan (RMP) that is ISO 16085 compliant

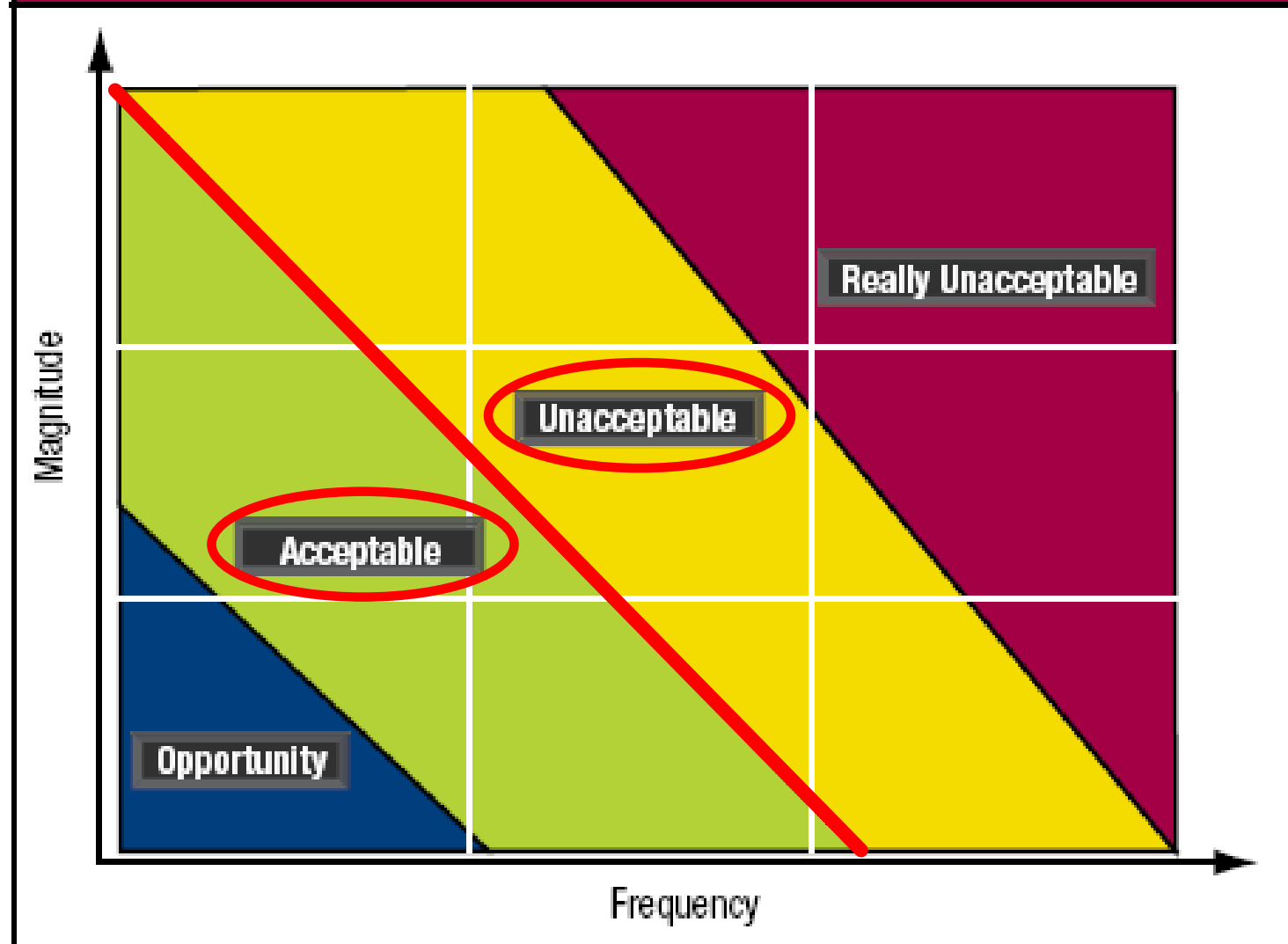


Risk Appetite and Risk Tolerance

- Risk appetite
 - The amount of risk an enterprise is prepared to accept
- Risk tolerance
 - The amount of risk that an organization is willing to withstand


Risk Appetite and Risk Tolerance

Figure 11—Risk Map Indicating Risk Appetite Bands



Risk Awareness, Communications, and Reporting

- Clear
- Concise
 - Consider using *Information Dashboard Design* by Stephen Few
- Useful
 - Avoid risk normalization
- Timely
- Adapt information for the intended audience



Risk Awareness, Communications, and Reporting

- Clear

Probability	Lvl	Your approach and processes	
	A	Not Likely	Will effectively avoid or mitigate this risk based on standard practices~10%
	B	Somewhat Likely	Have usually mitigated this type of risk with minimal oversight in similar cases~30%
	C	Likely	May mitigate this risk, but workarounds will be required~50%
	D	Highly Likely	Cannot mitigate this risk, but a different approach might ~70%
	E	Near Certainty	Cannot mitigate this type of risk; no known processes or workarounds are available~90%

Lvl	Technical Performance	Schedule	Cost
1	Minimal: Minimal or no consequence to technical performance impact	Minimal or no impact	Minimal or no impact
2	Some: minor reduction in technical performance or supportability, can be tolerated with little or no impact on program; same approach retained	Additional activities required, able to meet key dates	Budget increase or unit production cost increases
3	Medium: Moderate reduction in technical performance or supportability with limited impact on program objectives; workarounds available	Minor schedule slip, no impact to key milestones	Budget increase or unit production cost increases
4	High: Significant degradation in technical performance or major shortfall in supportability; may jeopardize program success; workarounds may not be available or may have negative consequences	Program critical path affected, all schedule float associated with key milestones exhausted	Budget increase or unit production cost increases
5	Critical: Severe degradation in technical performance; cannot meet key performance parameter or key technical/supportability threshold; will jeopardize program success; no workarounds available	Cannot meet key program milestones	Exceeds accepted standards/ requirements threshold

Real Risk Example

- Risk Description # 6-01:
 - Generation of the monthly Site/System Usage Report is not possible without the specific details of what metrics are to be reported. Additionally, the software required to capture the data and has not been defined. While Citrix has some capability the Enterprise version is the only one that has the software included. There are many Citrix servers that do not have the required reporting software. The Windows platform does not natively produce the data required. As the exact requirement is defined a Decision Analysis Resolution (DAR) should be completed to assist in the selection of the best product to support the report.

Real Risk Example

- Probability:
 - Near Certainty (Cannot mitigate this type of risk; no known processes or workarounds are available~90%)
- Impact
 - High

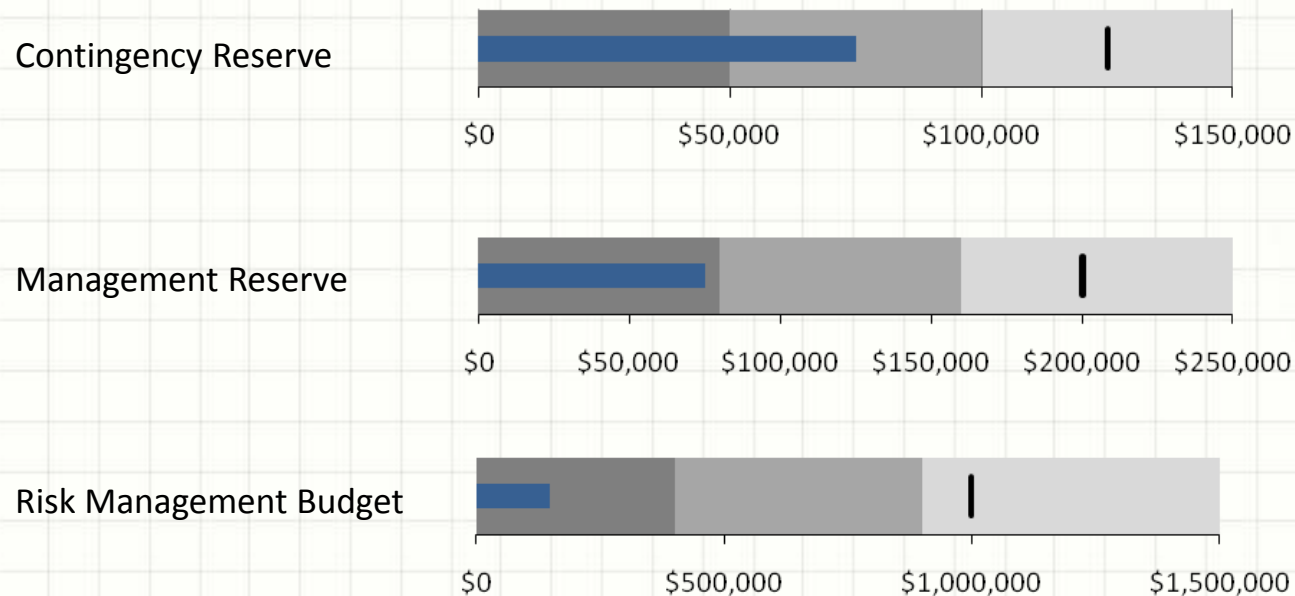
Level	Technical Performance	Schedule	Cost
4	High: Significant degradation in technical performance or major shortfall in supportability; may jeopardize program success; workarounds may not be available or may have negative consequences	Program critical path affected, all schedule float associated with key milestones exhausted	Budget increase or unit production cost increases

Real Risk Example

- Mitigation Plan:
 - System Administrators meet to brainstorm requirement
 - Products are evaluated that meet the requirement.
 - Perform a DAR to determine the ""best"" one.
 - Provide selected tool(s) to each site with guidance on usage.
 - Deploy solution and provide Site/System Usage Report monthly
- What is the real risk?
- What is the real impact?
- What is the context?
- What is the risk exposure to the Project? Sponsoring organization?

Risk Awareness, Communications, and Reporting

- Concise
 - Consider using *Information Dashboard Design* by Stephen Few
- Useful



Expressing and Describing Risk

- Risk Analysis
 - Impact
 - Probability or Frequency
- Qualitative risk analysis
 - For use in situations where limited information is available
 - Less complex therefore, less expensive
- Quantitative risk analysis
 - Objective, empirical data is available
 - More complex and expensive than qualitative risk analysis

Expressing and Describing Risk

- Highly mature organizations tend to move towards probabilistic risk assessment
 - Involves complex mathematical models (e.g. Monte Carlo simulation)

Expressing and Describing Risk

- A number of industry models exist for expressing business impact
 - Balanced Scorecard (BSC)
 - Westerman 4 “A”
 - Agility, Accuracy, Access, Availability
 - COSO ERM
 - Strategic, Operations, Reporting, Compliance
 - FAIR
 - Productivity, Responses, Replacement, Competitive Advantage, Legal, Reputation

Risk Scenarios

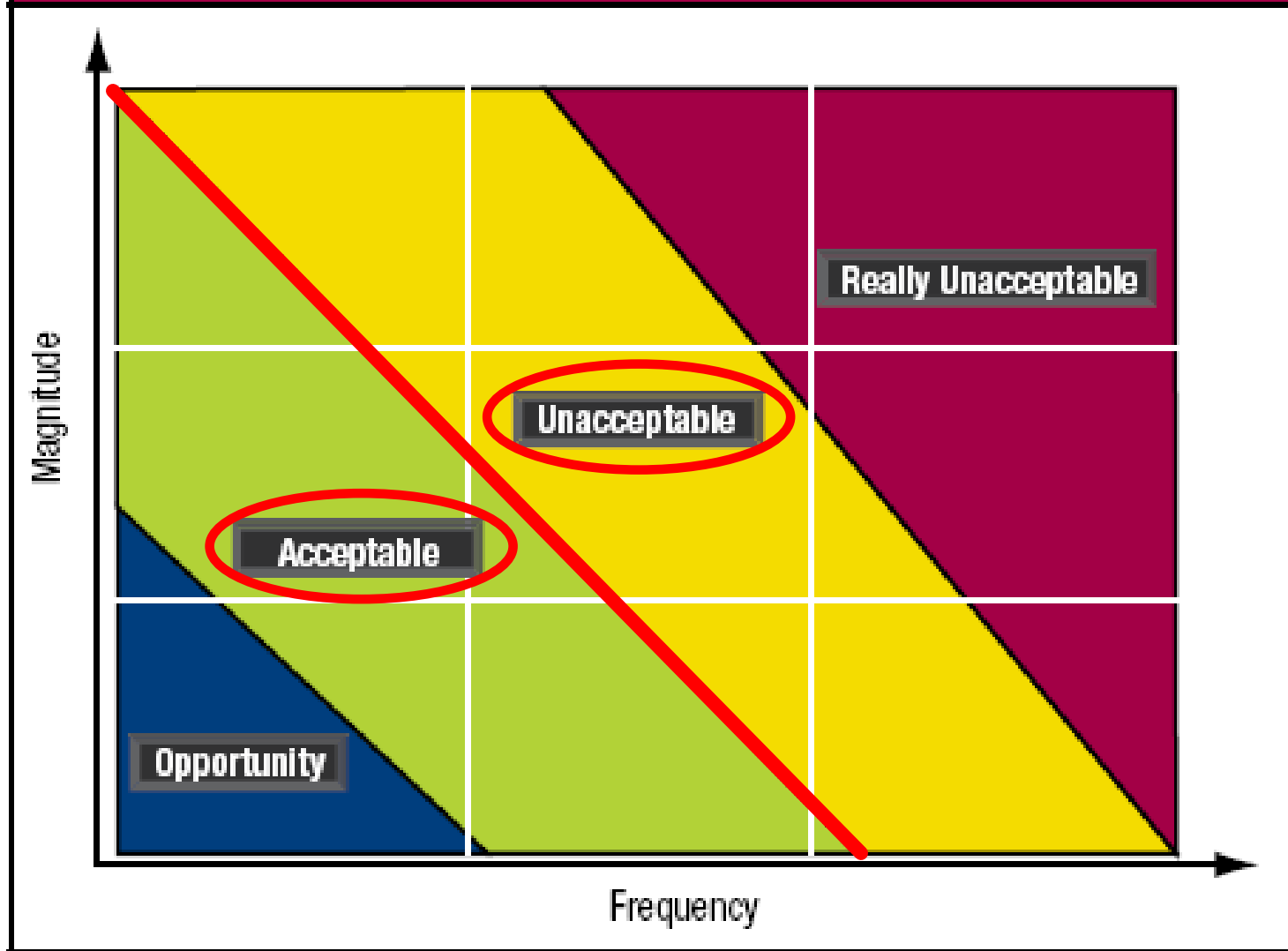


Risk Response and Prioritization

- Select treatment strategy
 - Accept, avoid, mitigate, or transfer
- Prioritize Risks

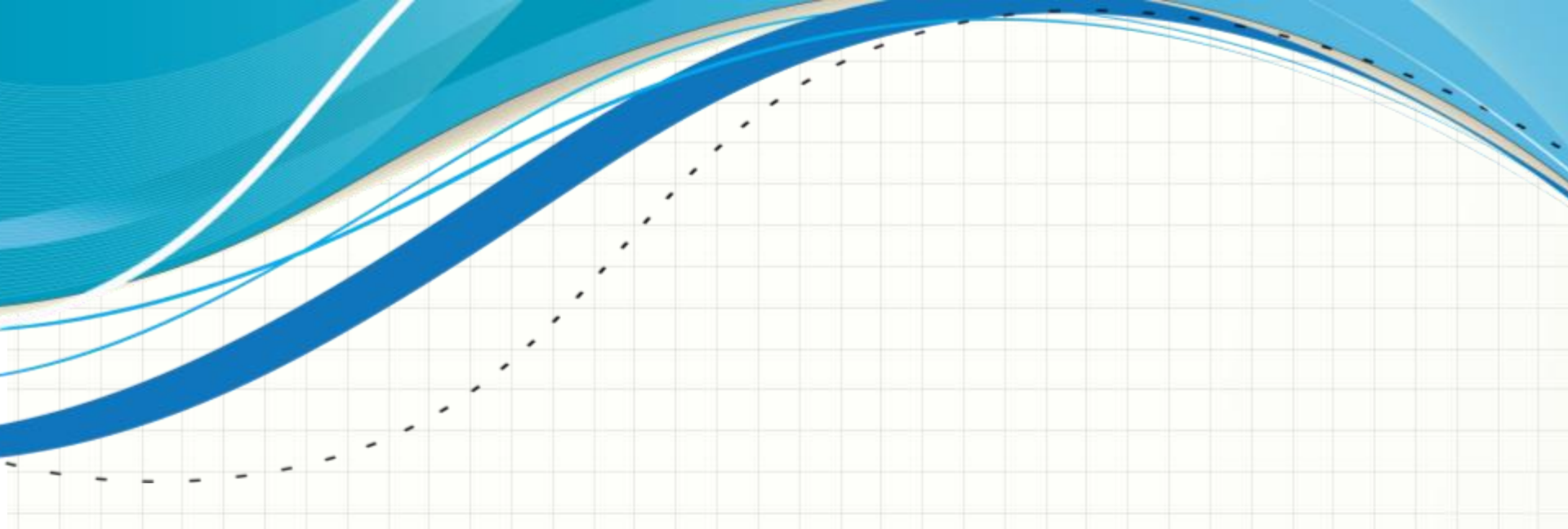
Risk Response and Prioritization

Figure 11—Risk Map Indicating Risk Appetite Bands



Risk Response and Prioritization

- Develop formal risk treatment / response plan
 - ISO 16085, ISO / IEC 31000, or AN/NZS 4360 compliant
 - Risk response is a weakness in the PMBOK
- Monitor progress against the response plan



EXERCISE #2

RISK SCENARIOS

Warwickshire Community

- Multiple vehicle incident causing up to 10 fatalities and up to 20 casualties (internal injuries, fractures, possible burns); closure of lanes or carriageways causing major disruption and delays.

Risk Scenario

- Actor:

- Threat:

- Event:

- Asset(s):

- Timing:

Team Scenario

Risk Scenario

- Actor:

- Threat:

- Event:

- Asset(s):

- Timing:



WARWICKSHIRE CASE STUDY

References

- Information Systems Audit and Control Association. (2009). *The Risk IT Practitioner Guide*. Rolling Meadows, IL: Information Systems Audit and Control Association.
- A to Z Teacher Stuff, L.L.C. . (2010). *Word Search Generator*. Retrieved from <http://tools.atozteacherstuff.com/word-search-maker/wordsearch.php>
- Taleb, N. (2007, April 22). The Black Swan: The Impact of the Highly Improbable. *The New York Times*. Retrieved from http://www.nytimes.com/2007/04/22/books/chapters/0422-1st-tale.html?_r=1&ex=1178769600&en=bdae1078f2b4a98c&ei=5070
-



QUESTIONS?



THANK YOU!

JOSEPH W. MAYO, PMP, RMP, CRISC
JOSEPH.MAYO@KEANE.COM



BACKUP SLIDES

ISO 16085 RMP Outline

- Overview
 - Date of Issue and Status
 - Issuing Organization
 - Approval Authority
 - Updates
- Scope
 - [Define the boundaries and limitations of risk on the project]
- Reference Documents
- Glossary
- Risk Management Overview
 - [Describe the specifics of risk management for this project or organization's situation.]

ISO 16085 RMP Outline

- Risk Management Policies
 - [Describe the guidelines by which risk management will be conducted.]
- Risk Management Process Overview
- Risk Management Responsibilities
 - [Define the parties responsible for performing risk management.]
- Risk Management Organization
 - [Describe the function or organization assigned responsibility for risk management within the organizational unit.]
- Risk Management Orientation and Training
- Risk Management Costs and Schedules

ISO 16085 RMP Outline

- Risk Management Process Description
 - [If there is an organizational risk management process that is being used for this project or situation, refer to it. If adaptation of the process is appropriate, describe the adaptations made. Describe the procedures that implement the risk management process. If no organizational process exists, describe the risk management process and procedures to be used for the project or situation.]
 - Risk Management Context
 - Risk Analysis
 - Risk Monitoring
 - Risk Treatment
 - [Describe how risks are to be treated. If a standard management process exists for handling deviations or problems, refer to this process. If risks require a separate risk treatment activity due to specific circumstance, describe this activity.]

ISO 16085 RMP Outline

- Risk Management Process Evaluation
 - [Describe how this project or organization will gather and use measurement information to help improve the risk management process for the project and/or for the organization.]
 - Capturing Risk Information
 - Assessing the Risk Management Process
 - Generating Lessons Learned

ISO 16085 RMP Outline

- Risk Communication
 - [Describe how risk management information will be coordinated and communicated among stakeholders and interested parties (i.e., those who are interested in the performance or success of the project or product, but not necessarily of the organization) such as what risks need reporting to which management level.]
 - Process Documentation and Reporting
 - Coordinating Risk Management with Stakeholders
 - Coordinating Risk Management with Interested Parties
- Risk Management Plan Change Procedures and History

Risk Response Plans

ISO 16085	ISO/IEC 31000	AN/NZS 4360
Overview	Reasons for selection of treatment options, including expected benefits to be gained	Summary (Recommended Response and Impact)
Scope, reference documents, Glossary		
Planned Risk Treatment Activities and Tasks	Proposed actions	Proposed Actions
Treatment Resources and their Allocation	Resource requirements including contingencies	Resource Requirement(s)
Responsibilities and Authority	Individuals accountable for approving the plan and those responsible for implementing the plan	Responsibility
Treatment Schedule	Timing and schedule	Timing
	Performance measures and constraints	
Treatment Control Measures	Reporting and monitoring requirements	Reporting and monitoring required
Treatment Cost		
Interfaces among Parties Involved		
Risk Treatment Plan Change Procedures and History		