J. W. Mayo
CONSULTING

jwmc-llc.com

J. W. Mayo CONSULTING

Quantify Risk to Guide Risk Policy

Joseph W. Mayo

CMMI Associate, PMP, PMI-RMP, CRISC, RIMS-CRMP

joseph.mayo@jwmc-llc.com

Learning Objectives

At the end of this session, you will:

- Understand how to use tolerance and appetite to shape ERM policy
- Learn tools and techniques that can be used to objectively quantify risk impact
- Understand the relationships between risk policy, tolerance, appetite, and reserve budgets
- Understand the impact of ineffective Enterprise Risk Management by reviewing two real-world case studies

joseph.mayo@jwmc-llc.com

Agenda

- Introduction
- Risk policy, risk appetite, risk tolerance, and reserve budgets
- Objectively quantify risk appetite and tolerance
- Tools and Techniques
- Case Studies
  - Deepwater Horizon
  - US Government
- High Reliability Organizations (HRO)
- Conclusion
- Q&A

joseph.mayo@jwmc-llc.com

J. W. Mayo CONSULTING

conferences i/o

We're going to be using a product called Conferences i/o that will allow you to engage with us during this session. **All responses are anonymous!**

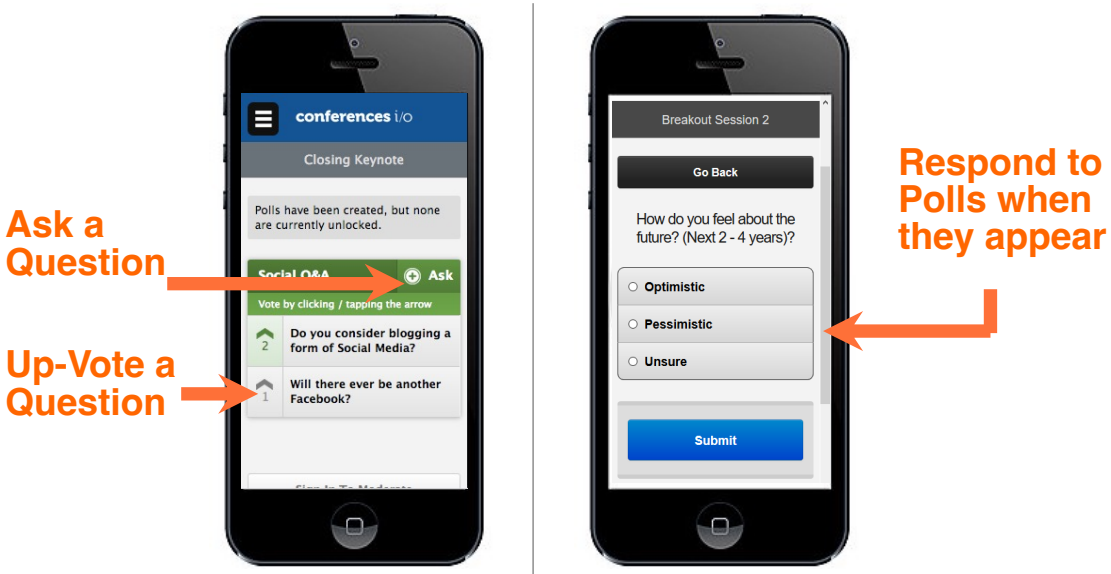
If you have a mobile device (smartphone, tablet, laptop, etc.) please take a moment now, and go to https://taoofrisk.cnf.io

The Conferences i/o app allows you to ask questions, up-vote questions other attendees asked and respond to polls when they appear on your device, all in real time!

joseph.mayo@jwmc-llc.com

J. W. Mayo CONSULTING

WEBSITE ADDRESS: **TaoOfRisk.cnf.io**



Note: Responses and submissions are anonymous

joseph.mayo@jwmc-llc.com

Policy, Appetite, and Tolerance

- Risk Policy or Risk Principles – a statement describing the types of risk and the amount of risk exposure an organization is willing to entertain
  - Policy statement
  - Risk appetite
  - Risk tolerance
  - Roles and responsibilities
  - Governance
- Risk Appetite – Desire or craving for taking risk
  - Risk appetite is conceptually similar to human appetite
  - Risk appetite cannot exceed the organization's risk capacity
  - Six risk contexts; Budget, Schedule, Quality, Mission, Reputation, and Safety
- Risk Tolerance – degree of variance from a stated appetite or threshold

joseph.mayo@jwmc-llc.com

Policy, Appetite, Tolerance, and Budgets

- Risk appetite, risk tolerance, and reserve budgets guide the development of risk policy or risk principles
  - These can and should change over time as market conditions change
- Appetite and tolerance drive all aspects of risk management including Governance, treatment strategies, prioritization, reserve budgets, and risk management processes
  - These are strategic risk management elements
- Mandating that project teams manage risk is insufficient and does not constitute ERM
- Effective risk management requires a risk policy or principles that clearly establishes appetite, tolerance, and waiver-ability

joseph.mayo@jwmc-llc.com

Risk Appetite and Tolerance

- Risk policy or principles must explicitly state appetite
  - Enterprise appetite
  - Project appetite
  - Regional/business line differences
- Risk policy or principles must state whether the organization allows waivers
  - Risk policy must define or reference pre-defined waiver and governance processes
  - Waivers and tolerance go hand-in-hand

joseph.mayo@jwmc-llc.com

Risk Appetite and Tolerance

- If possible, objectively quantify appetite and tolerance
  - Based on organizational goals and objectives
- Risk impact must be properly valued and may include impact bands

joseph.mayo@jwmc-llc.com

Risk Appetite and Tolerance

- **Excerpt from the University of Edinburgh Risk Policy**

The University's appetite for risk across its activities is provided in the following statements, and is illustrated diagrammatically.

	Unacceptable to take risks									Higher Willingness to take risks
	1	2	3	4	5	6	7	8	9	10
Reputation	<	>								
Compliance	<	>								
Financial			<		>					
Research						<				>
Education & Student Experience					<				>	
Knowledge Exchange						<				>
International Development				<			>			
Major change activities		<				>				
Environment and Social Responsibility					<			>		
People and culture		<			>					

University of Edinburgh Risk Policy and Risk Appetite. (20013). Retrieved from http://www.docs.sasg.ed.ac.uk/GaSP/Governance/RiskManagement/RiskAppetite.pdf

joseph.mayo@jwmc-llc.com

Risk Appetite and Tolerance

J. W. Mayo CONSULTING

Financial – The University aims to maintain its long term financial viability and its overall financial strength. Whilst targets for financial achievement will be higher, the University will aim to manage its financial risk by not breaching the following minimum criteria[1]:

It will

- achieve a surplus of a minimum of 2% of gross income over any 3 year period
- operate with a Staff Cost/Total Expenses ratio of less than 60%
- achieve a rate of return of at least 2% above inflation on its endowment investments over a 3 year period
- ensure long term borrowings never exceed 20% of net assets
- ensure its surplus before interest always exceeds 2 times net interest charge
- ensure that at least three months equivalent spend is held cash or cash equivalents or in negotiated bank facilities

University of Edinburgh Risk Policy and Risk Appetite. (20013). Retrieved from http://www.docs.sasg.ed.ac.uk/GaSP/Governance/RiskManagement/RiskAppetite.pdf

joseph.mayo@jwmc-llc.com

Why Quantify Objectively?

- A poll of random people revealed interesting answers to the following questions
  - What is a high budget amount?
  - What is a long duration?

High Budget	Long Duration
$1 Trillion	50 years
$50 Billion	5 years
$20 Million	10 years
$3.5 Million	5 years

joseph.mayo@jwmc-llc.com

Why Quantify Objectively?

- Large government agency normalizes risks using a concept called a Risk Adjusted Cost (RAC)
  - $225,000 impact and “High” probability yields the same RAC as $175,000 impact and “Very High” probability
  - The RACs are equal however, there is more than 20% difference in the impact
  - In this case, RAC causes equal treatment when in fact, the $175,000 risk should have a higher priority because of the higher probability of occurrence

joseph.mayo@jwmc-llc.com

Why Quantify Objectively?

- NASA normalized foam strikes as a simple ‘‘maintenance” issue, and not a concern for mission success of Space Shuttle Columbia[1]
  - Foam from the fuel tank had struck the wing on at least 12 previous shuttle flights, each time causing gouges or other damage
  - Acquiescence to recurring risks has been termed “normalized deviance”

joseph.mayo@jwmc-llc.com

[1]NORMALIZED DEVIANCE. (2003, May 24). *St.Louis Post - Dispatch* Retrieved from http://search.proquest.com/docview/402298524?accountid=458

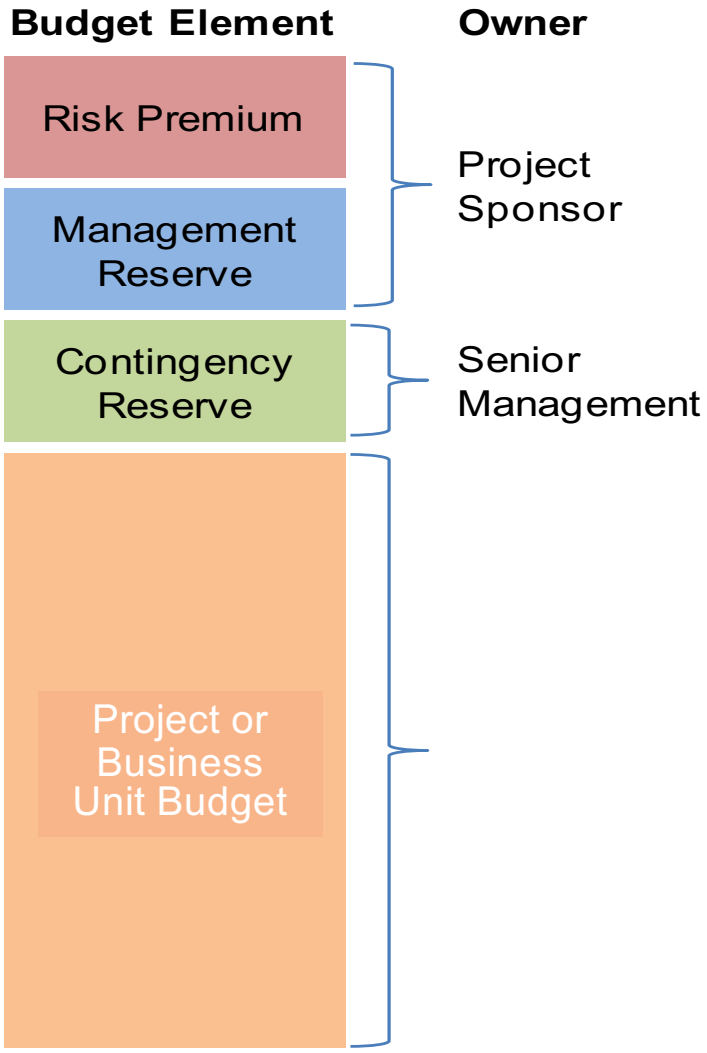
Why Quantify Objectively?

J. W. Mayo CONSULTING

- Helps avoid personal perceptions influencing risk management actions
- Helps avoid normalized deviance
- Simplifies metrics collection and reporting

joseph.mayo@jwmc-llc.com

Risk Budgets



- Management reserve used to manage opportunities and Black Swan events
- Contingency reserve used for all risk management activities
- Project budget of for executing planned activities
- Reserve budgets are separate from project budgets
- Risk governance is the mechanism for transferring risk budget to project budget through RRB

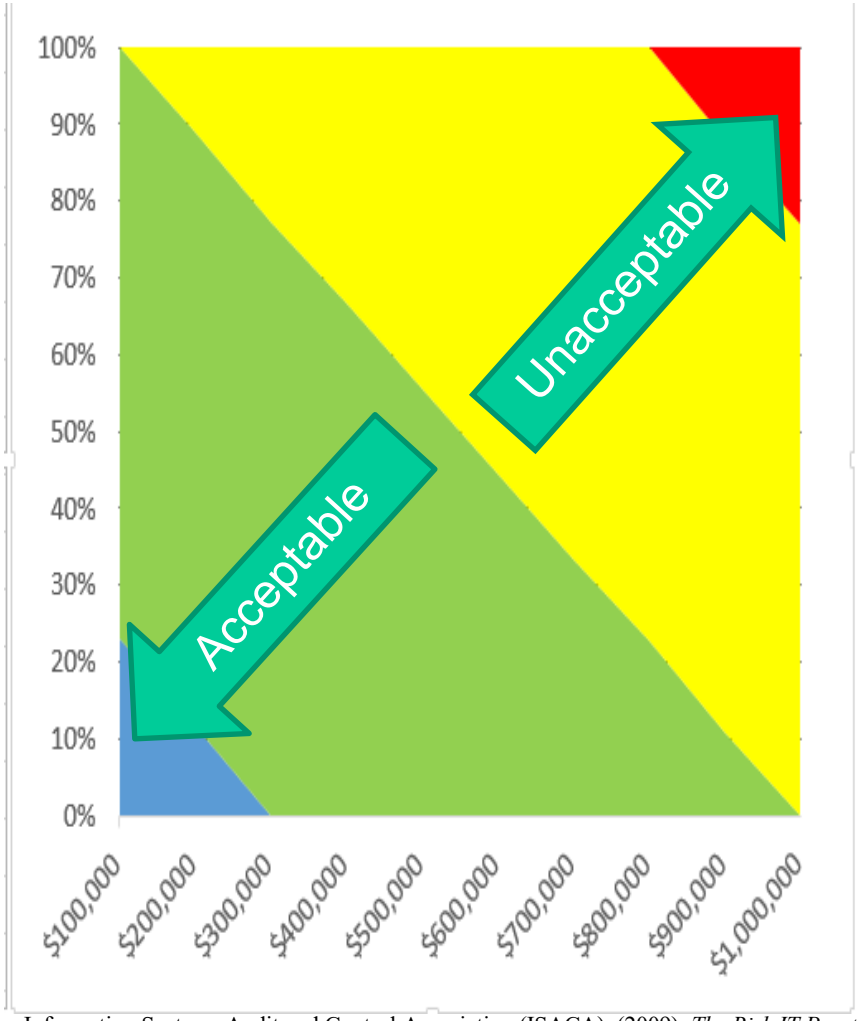
joseph.mayo@jwmc-llc.com

Tools for Quantifying Appetite & Tolerance

- Leveraging ISACA's Risk IT, Risk Appetite Risk Map
- Expected Monetary Value (EMV) Charts (aka Decision Tree)

joseph.mayo@jwmc-llc.com

Risk IT Risk Map

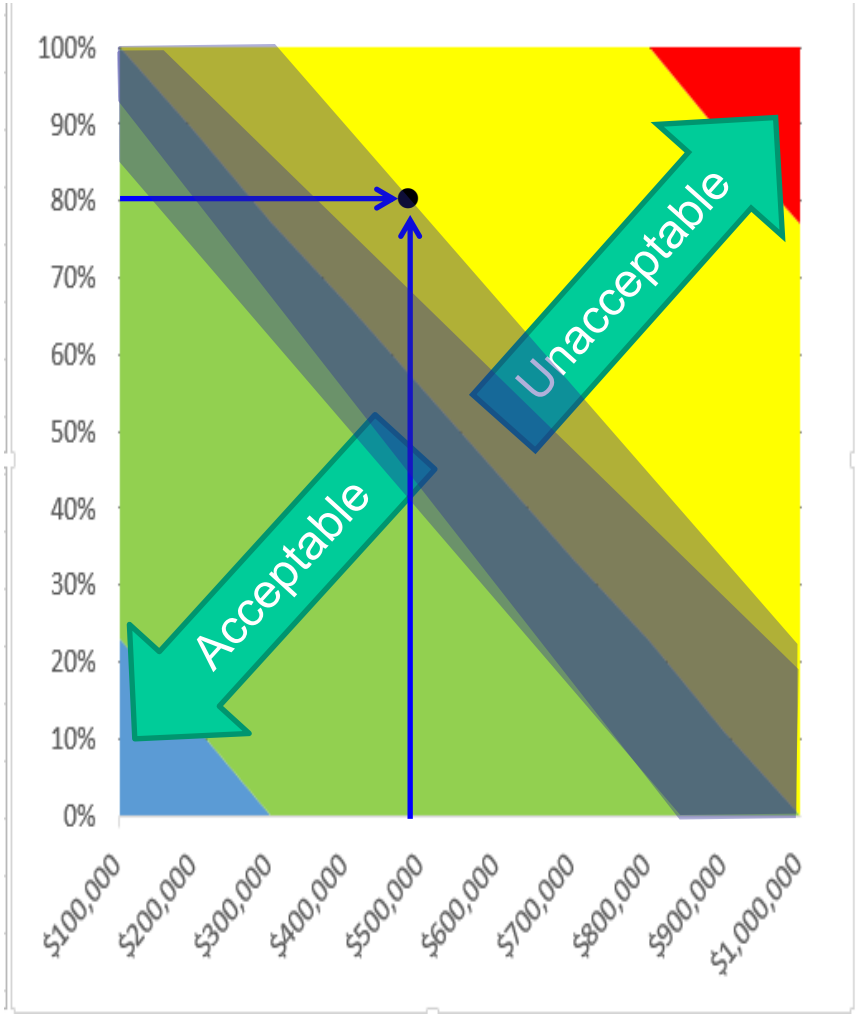


- ISACA's RiskIT is an excellent guide
- Understand what constitutes acceptable vs unacceptable risks

Information Systems Audit and Control Association (ISACA). (2009). *The Risk IT Practitioner Guide*. Rolling Meadows, IL: Information Systems and Control Association (ISACA).

joseph.mayo@jwmc-llc.com

Risk IT Risk Map

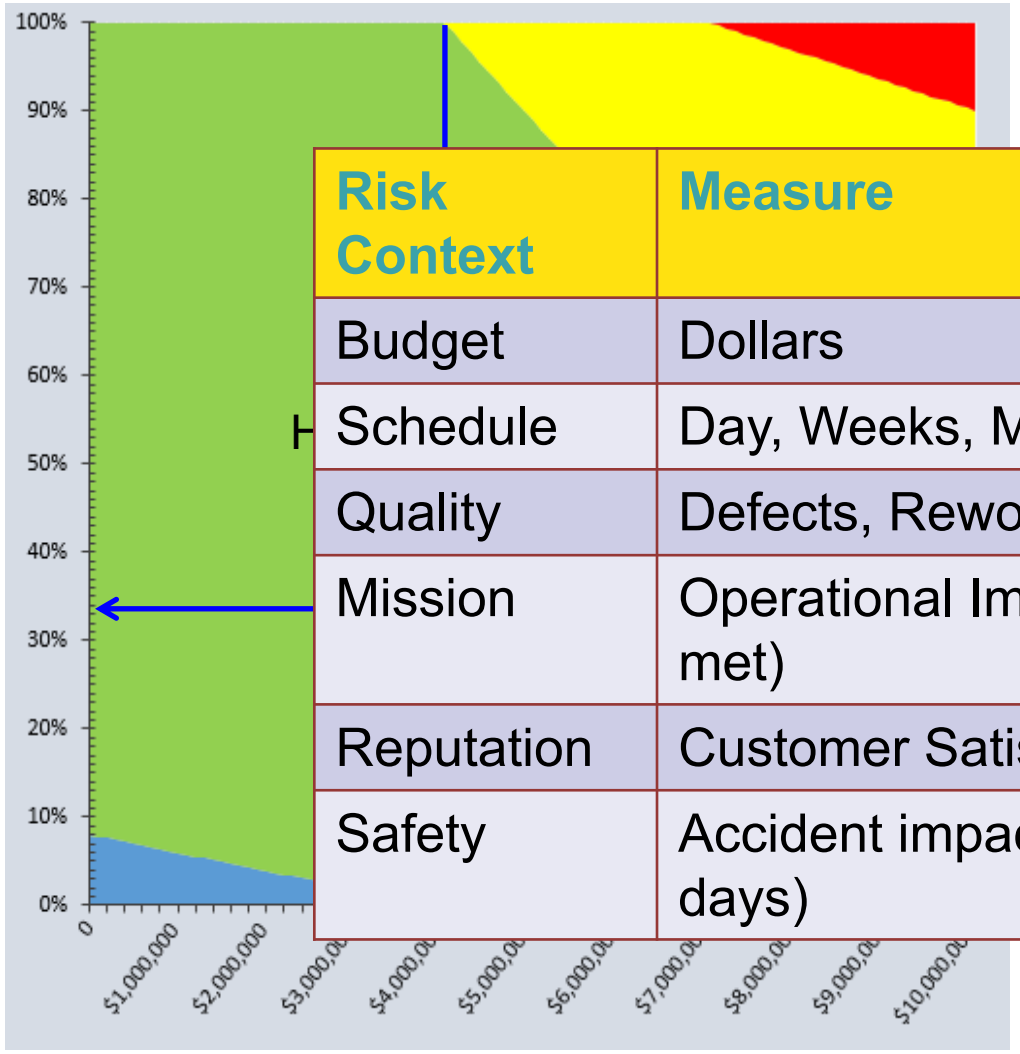


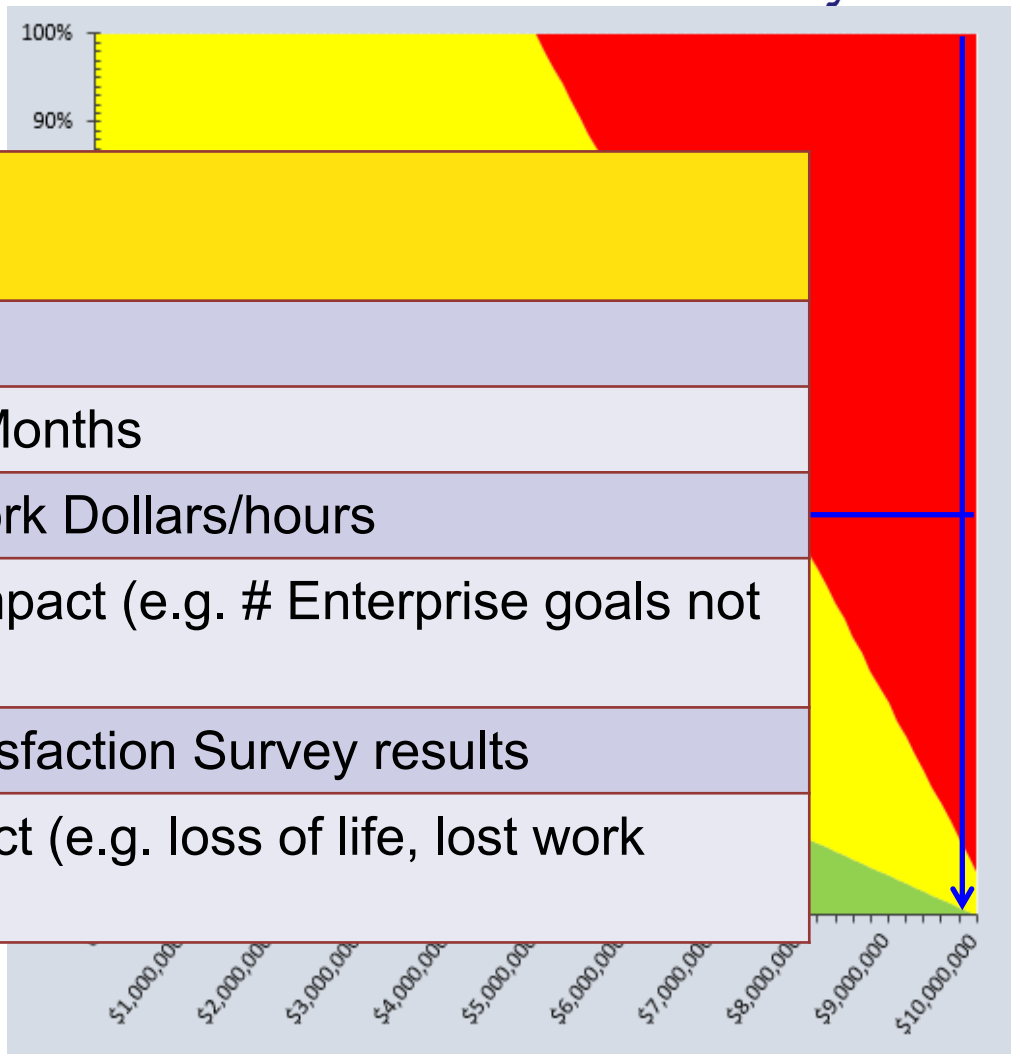
- ISACA's RiskIT is an excellent guide
- Understand what constitutes acceptable vs unacceptable risks
- Understand how much stakeholders are willing to spend for risk treatment
- Objectively quantify appetite
- Properly value risk impact
- Understand risk tolerance thresholds

joseph.mayo@jwmc-llc.com

Risk IT Risk Map

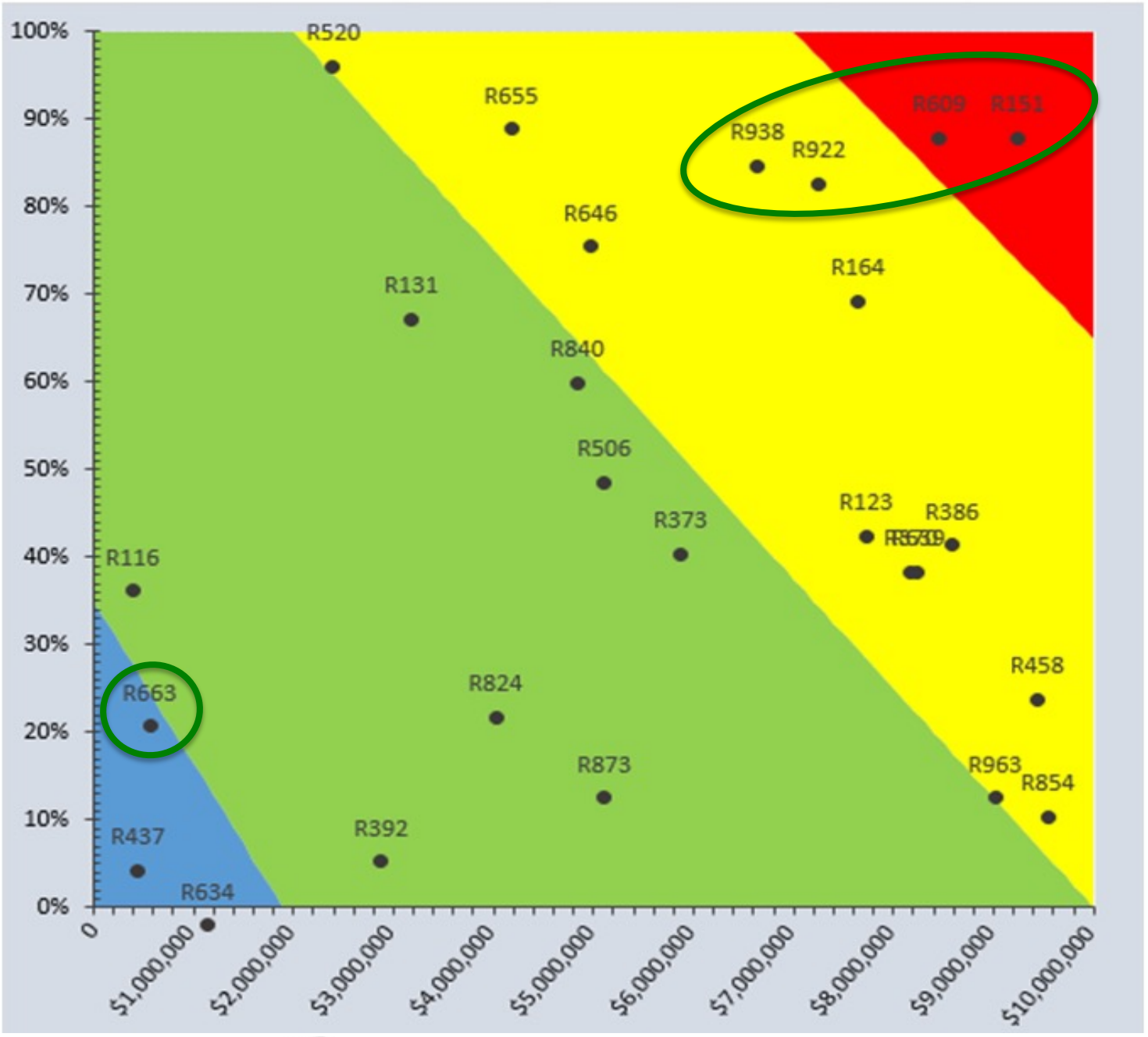
J. W. Mayo





Risk Context	Measure
Budget	Dollars
Schedule	Day, Weeks, Months
Quality	Defects, Rework Dollars/hours
Mission	Operational Impact (e.g. # Enterprise goals not met)
Reputation	Customer Satisfaction Survey results
Safety	Accident impact (e.g. loss of life, lost work days)

joseph.mayo@jwmc-llc.com



J. W. Mayo CONSULTING

- 26 risks represent a total risk exposure of $72M
- Highlighted risks represent 15% of the identified risks and 38% of total exposure

joseph.mayo@jwmc-llc.com

EMV Scenario

- Choose most cost effective travel from Boston to Chicago
- Risk statement: IF travel cost exceeds $350 THEN cancel trip
- EMV Charts are constructed left to right

■ - Decision node

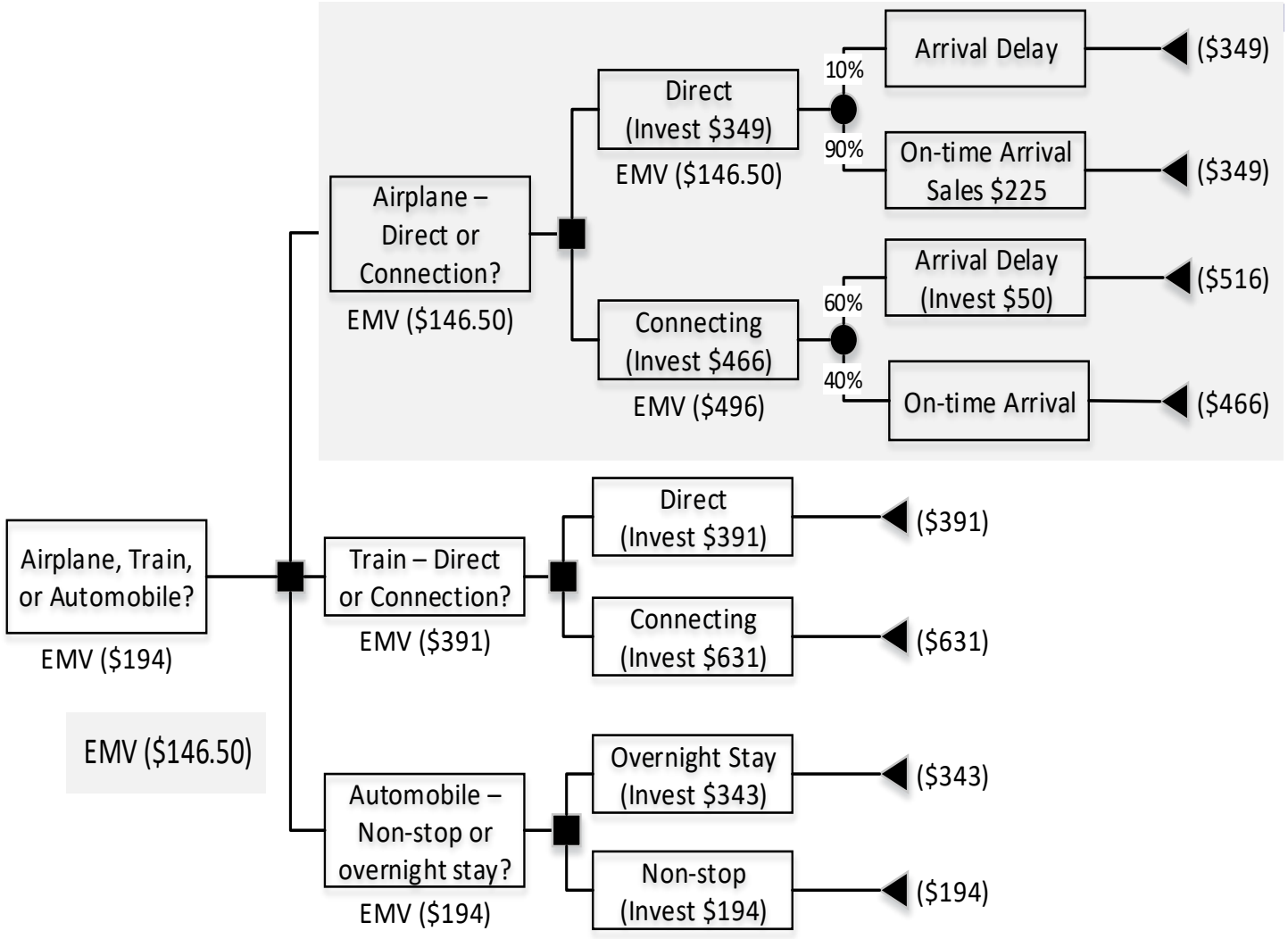
● - Chance node

The sum of all chance nodes on a branch must equal 100%

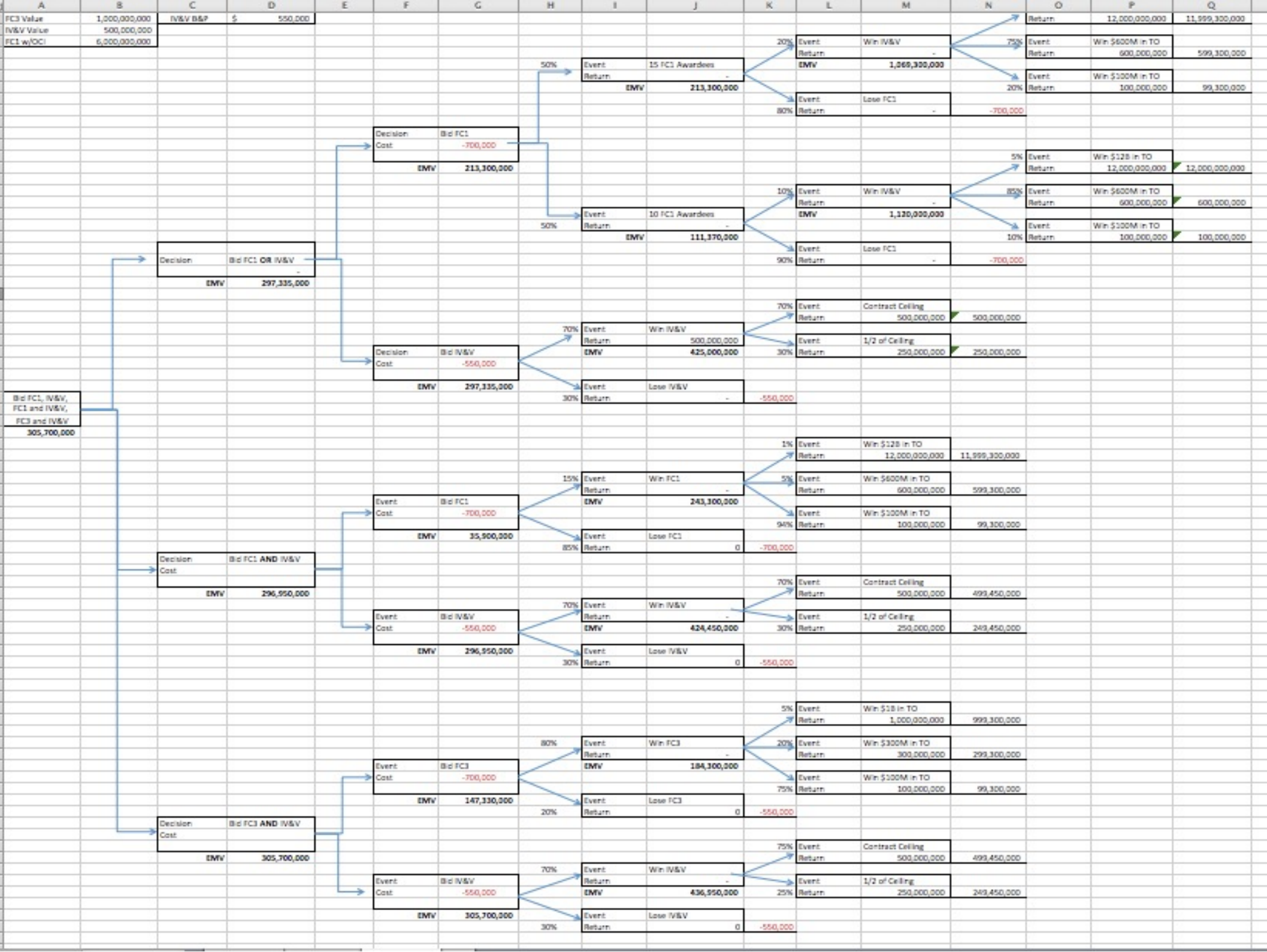
EMV values are computed right to left

joseph.mayo@jwmc-llc.com

EMV Diagram



joseph.mayo@jwmc-llc.com


FC3 Value 1,000,000,000
IV&V Value 500,000,000
FC1 w/OCI 6,000,000,000
IV&V B&P $ 550,000
Bid FC1, IV&V, FC1 and IV&V, FC3 and IV&V
305,700,000
Decision Bid FC1 OR IV&V
EMV 297,335,000
Decision Bid FC1
Cost -700,000
EMV 213,300,000
50% Event 15 FC1 Awardees
Return -
EMV 213,300,000
20% Event Win IV&V
Return -
EMV 1,060,300,000
75% Event Return
Win $600M in TO 600,000,000 599,300,000
20% Event Return
Win $100M in TO 100,000,000 99,300,000
80% Event Lose FC1
Return - -700,000
50% Event 10 FC1 Awardees
Return -
EMV 111,370,000
10% Event Win IV&V
Return -
EMV 1,130,000,000
5% Event Return
Win $12B in TO 12,000,000,000 12,000,000,000
85% Event Return
Win $600M in TO 600,000,000 600,000,000
10% Event Return
Win $100M in TO 100,000,000 100,000,000
90% Event Lose FC1
Return - -700,000
Decision Bid IV&V
Cost -550,000
EMV 297,335,000
70% Event Win IV&V
Return 500,000,000
EMV 425,000,000
70% Event Contract Ceiling
Return 500,000,000 500,000,000
30% Event 1/2 of Ceiling
Return 250,000,000 250,000,000
30% Event Lose IV&V
Return - -550,000
Decision Bid FC1 AND IV&V
Cost
EMV 296,950,000
Event Bid FC1
Cost -700,000
EMV 35,900,000
15% Event Win FC1
Return -
EMV 243,300,000
1% Event Return
Win $12B in TO 12,000,000,000 11,999,300,000
5% Event Return
Win $600M in TO 600,000,000 599,300,000
94% Event Return
Win $100M in TO 100,000,000 99,300,000
85% Event Lose FC1
Return 0 -700,000
Event Bid IV&V
Cost -550,000
EMV 296,950,000
70% Event Win IV&V
Return -
EMV 424,450,000
70% Event Contract Ceiling
Return 500,000,000 499,450,000
30% Event 1/2 of Ceiling
Return 250,000,000 249,450,000
30% Event Lose IV&V
Return 0 -550,000
Decision Bid FC3 AND IV&V
Cost
EMV 305,700,000
Event Bid FC3
Cost -700,000
EMV 147,330,000
80% Event Win FC3
Return -
EMV 184,300,000
5% Event Return
Win $1B in TO 1,000,000,000 999,300,000
20% Event Return
Win $300M in TO 300,000,000 299,300,000
75% Event Return
Win $100M in TO 100,000,000 99,300,000
20% Event Lose FC3
Return 0 -550,000
Event Bid IV&V
Cost -550,000
EMV 305,700,000
75% Event Contract Ceiling
Return 500,000,000 499,450,000
70% Event Win IV&V
Return -
EMV 436,950,000
25% Event 1/2 of Ceiling
Return 250,000,000 249,450,000
30% Event Lose IV&V
Return 0 -550,000

Deepwater Horizon

- Deepest oil well in history at more than 35,000 feet
- Spill cleanup procedures and technology in 2009 were essentially unchanged since the 1960s
- Prior to the Deepwater Horizon disaster, BP considered deep water blowouts in the Gulf of Mexico a high-level risk

joseph.mayo@jwmc-llc.com

Davis, M. (2012). Lessons Unlearned: The Legal and Policy Legacy of the BP Deepwater Horizon Spill. *Washington and Lee Journal of Energy, Climate, and the Environment*, *3*(2), 155-170

Eilperin, J. (2010). "U.S. exempted BP's Gulf of Mexico drilling from environmental impact study". The Washington Post (The Washington Post Company)..

Deepwater Horizon

- BP's Oil Spill Response Plan presented worst case spill scenarios ranging from 28,033 to 250,000 barrels (Davis, 2012)
- Between 1937 and 2010 there were at least 59 oil spills ranging from 29,000 barrels to 6 million barrels.
- BP's spill scenarios undervalued spill risk by more than 2,400%
  - Average spill size of 59 spills was 741,000 barrels
  - Top 10 of 59 spills ranged from 1 - 6 million barrels and averaged 2.3 million barrels

joseph.mayo@jwmc-llc.com

Davis, M. (2012). Lessons Unlearned: The Legal and Policy Legacy of the BP Deepwater Horizon Spill. *Washington and Lee Journal of Energy, Climate, and the Environment*, *3*(2), 155-170

Eilperin, J. (2010). "U.S. exempted BP's Gulf of Mexico drilling from environmental impact study". The Washington Post (The Washington Post Company)..

Deepwater Horizon

- U.S. DOI exempted BP's drilling operation from a detailed environmental impact analysis
  - Three reviews of the area concluded a massive oil spill was unlikely (Eilperin, 2010)
- U.S. Minerals Management Service (MMS) approved the spill response plan

Davis, M. (2012). Lessons Unlearned: The Legal and Policy Legacy of the BP Deepwater Horizon Spill. *Washington and Lee Journal of Energy, Climate, and the Environment*, *3*(2), 155-170
Eilperin, J. (2010). "U.S. exempted BP's Gulf of Mexico drilling from environmental impact study". The Washington Post (The Washington Post Company)..

joseph.mayo@jwmc-llc.com

Government Agency

- 2,229 software defects identified through tool-based code analysis
- 142.7 hours * 2,229 defects = 318,078 hours of effort to correct all of the unreported defect
  - 142.7 - Average effort over hundreds of defect remediation efforts spanning more than 2 years
- Multiplying $95 per hour times 318,078 yields a total risk exposure of $30.2 million

joseph.mayo@jwmc-llc.com

Government Agency

- Customer could not accept the fact that there was $30M risk exposure
- Boehm and Basili's research shows a defect that gets deployed costs $14,102 to correct
- Multiplying the 2,229 defects by $14,102 equals $31,433,358

joseph.mayo@jwmc-llc.com

High reliability Organizations (HRO)

- Operate in environments where potential for disaster is high
- Very high risk tolerance
- Top priority is effective performance
- Avoid disasters through collective learning
- Develop a culture of reliability
- Even firms without such catastrophic outcomes from risk events can leverage the models used by HROs

joseph.mayo@jwmc-llc.com

Sullivan, J., & Beach, R. (2009, February). Improving project outcomes through operational reliability: A conceptual model. *International Journal of Project Management*, (27), 765-775.

High reliability Organizations (HRO)

J. W. Mayo CONSULTING

Five characteristics of a high reliability organization (HRO)

1. extensive process auditing procedures
2. reward system that rewards risk mitigating behavior
3. quality standards that exceed referent industry standards
4. correctly assess risks and their associated impact
5. strong command and control structure consisting of
   - migrating decision making
   - redundancy
   - rules and procedures
   - Training
   - situational awareness

joseph.mayo@jwmc-llc.com

Libuser, C. B. (1994). *Organizational structure and risk mitigation.* (Order No. 9427348, University of California, Los Angeles). *ProQuest Dissertations and Theses,* , Retrieved from http://search.proquest.com/docview/304083303?accountid=458. (304083303).

Compare and Contrast HRO w/Case Studies

J. W. Mayo CONSULTING

		Deepwater Horizon	Government
Strategic	Extensive process auditing procedures awareness	○	○
	Reward system that rewards risk mitigating behavior	○	○
Tactical	Quality standards exceed referent industry standards	○	○
	Correctly assess risks and their associated impact	○	◗
	Migrating decision making	○	●
	Redundancy	●	◗
	Rules and procedures	◗	◗
	Training	◗	◗
	Situational	○	○

● - Fully implemented ◗ - Partially implemented ○ - Not implemented

Conclusion

- Quantifying risk elements does not require sophisticated tools
  - Effective process and disciplined execution are critical success factors
- If possible, quantitative appetite, tolerance, and impact help avoid normalized deviance (lean toward science and away from art)
  - Imitate HROs (e.g. effective performance, collective learning, culture of reliability)
- Proper risk valuation can avoid catastrophic risk impacts
  - Imitate HROs (e.g. reward risk mitigating behavior, correctly assess risks and their associated impact)
- Effective ERM requires strategic and tactical elements that are complementary

joseph.mayo@jwmc-llc.com

Live Content Slide

When playing as a slideshow, this slide will display live content

Social Q&A for ISACA Maryland Chapter Virtual Conference

joseph.mayo@jwmc-llc.com

J. W. Mayo CONSULTING

Thank You!

• • •

Joseph W. Mayo

CMMI Associate, PMP, PMI-RMP, CRISC, RIMS-CRMP

joseph.mayo@jwmc-llc.com

@TaoOfRisk