J. W. Mayo
CONSULTING

jwmc-llc.com

J. W. Mayo CONSULTING

How Culture Affects ERM

Joseph W. Mayo

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

joseph.mayo@jwmc-llc.com

Decisions, Decisions…

J. W. Mayo CONSULTING

I will do everything I can to save the company 57 cents including putting customer's lives at risk

I will lie to, deceive, and obstruct anyone who attempts to uncover product faults so our company can save $130 per unit

joseph.mayo@jwmc-llc.com

Top ERM Problems

J. W. Mayo CONSULTING

Organizational culture drives undesirable behavior

- "ERM's job is to protect the balance sheet"
- Normalized deviance is a warning sign of impending disaster
- Discourage risk reporting

Improper valuation of risk impact

- Monetizing risk impact
- Qualitative risk impact
- Ignoring risk impact

joseph.mayo@jwmc-llc.com

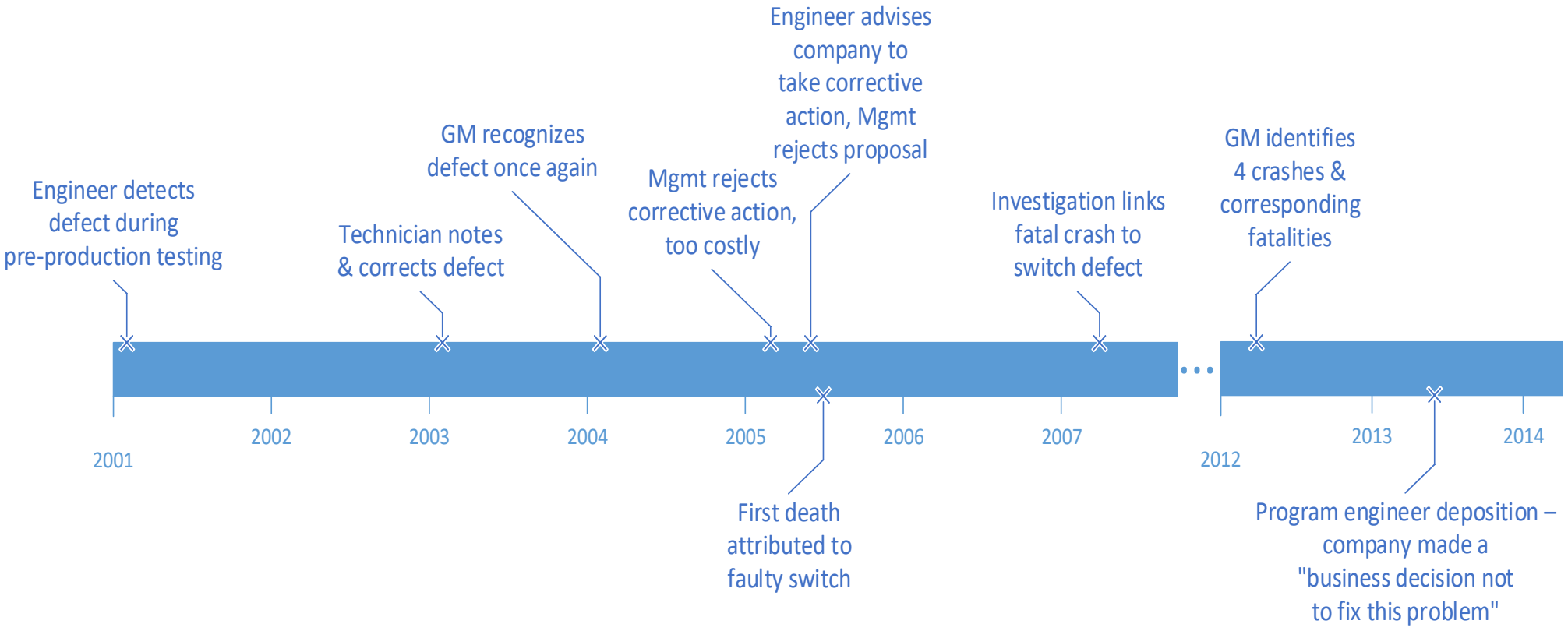
High Profile Risk Management Failures

J. W. Mayo CONSULTING

joseph.mayo@jwmc-llc.com

General Motors Ignition Switch Failure

J. W. Mayo CONSULTING



joseph.mayo@jwmc-llc.com

General Motors Ignition Switch Failure

J. W. Mayo CONSULTING

- By 2015 switch defect cost GM $4.1 billion
- Action prior 2004 would have avoided recall cost
- Action in 2004 could have been confined recalls to 4,100 Ions

$4.4M
2004 recall cost

$ .57
Cost of correct switch

51
Deaths

joseph.mayo@jwmc-llc.com

General Motors Ignition Switch Failure

J. W. Mayo CONSULTING

- ✓ Protect the balance sheet
- ✓ Normalized deviance
- ✓ Discourage risk reporting
- ✓ Monetizing risk impact
- Qualitative risk impact
- ✓ Ignoring risk impact

joseph.mayo@jwmc-llc.com

Toyota Accelerator Defect

- Toyota concealed defect information from consumers and government officials
- Faulty parts caused sudden, unintended acceleration in several models
- US attorney general, calls Toyota's behavior "shameful" and a "blatant disregard" for the law
- Toyota recalls 8.5 million cars with accelerator defect

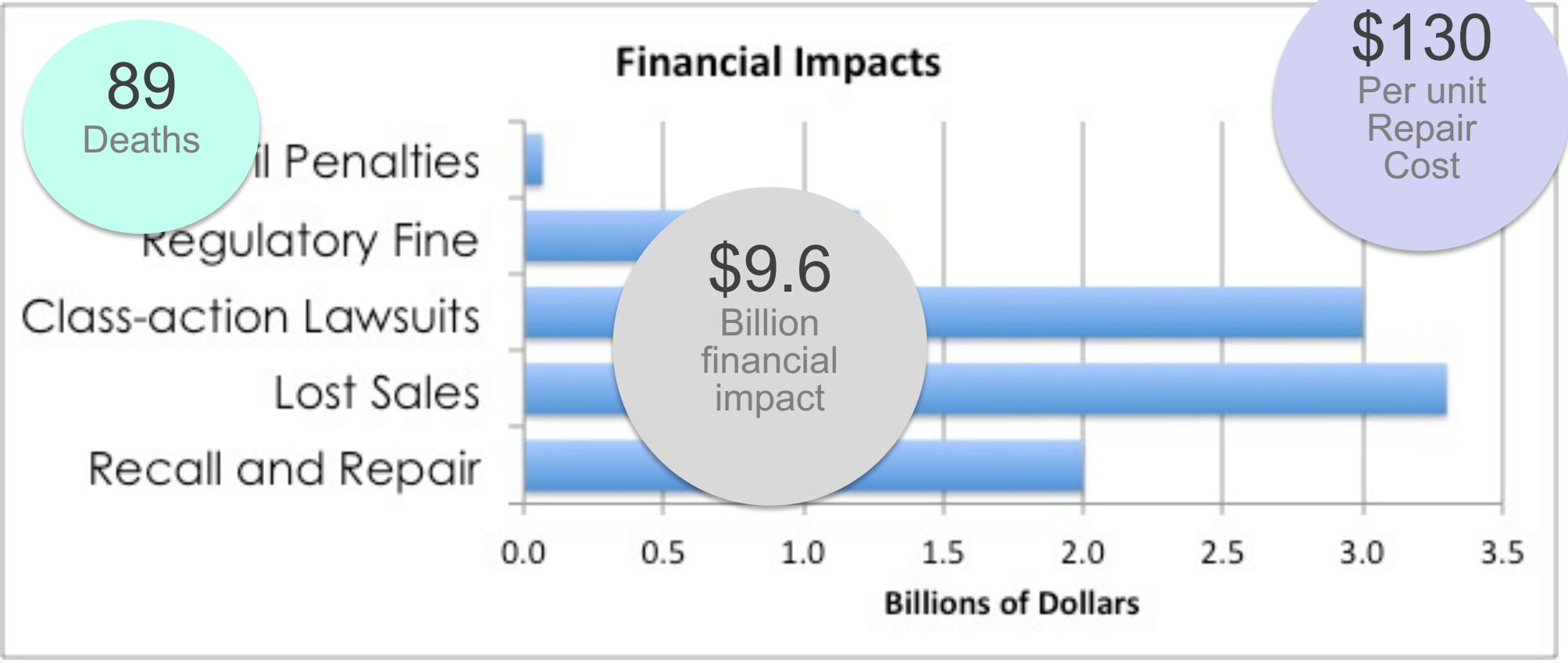
joseph.mayo@jwmc-llc.com

Toyota Accelerator Defect

J. W. Mayo CONSULTING

89
Deaths

$130
Per unit
Repair
Cost



joseph.mayo@jwmc-llc.com

Toyota Accelerator Defect

J. W. Mayo CONSULTING

- ✓ Protect the balance sheet
- Normalized deviance
- ✓ Discourage risk reporting
- ✓ Monetizing risk impact
- Qualitative risk impact
- ✓ Ignoring risk impact

joseph.mayo@jwmc-llc.com

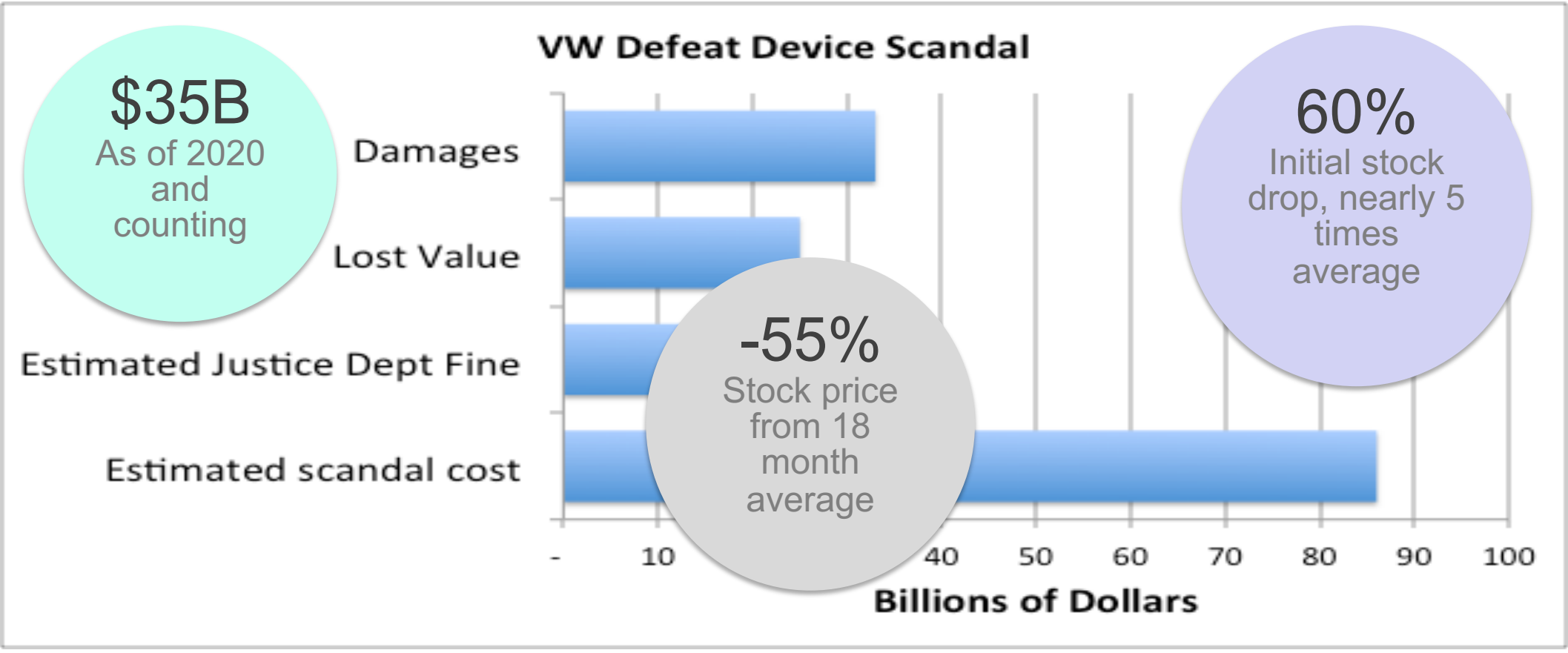
VW Defeat Device Scandal

- VW installed software on diesel vehicles that altered emissions during emission testing
- Defeat device software allowed engines to emit pollutants up to 40 times above allowable limits

joseph.mayo@jwmc-llc.com

VW Defeat Device Scandal

J. W. Mayo CONSULTING



joseph.mayo@jwmc-llc.com

VW Defeat Device Scandal

J. W. Mayo CONSULTING

- ✓ Protect the balance sheet
- TBD Normalized deviance
- ✓ Discourage risk reporting
- Monetizing risk impact
- TBD Qualitative risk impact
- ✓ Ignoring risk impact

joseph.mayo@jwmc-llc.com

J. W. Mayo CONSULTING

What Now?

joseph.mayo@jwmc-llc.com

What Now?

Change organizational culture

Employ risk scenarios

- Facilitates classification of risk to highlight safety and reputational risk
- Clarifies risk ownership

Re-evaluate organizational structure

Embrace the tenants of High Reliability Organizations (HRO)

joseph.mayo@jwmc-llc.com

Change Organizational Culture

J. W. Mayo CONSULTING

Risk Policy

- Set quantitative appetite thresholds
- Include six risk contexts; schedule, budget, quality, mission, safety, and reputation
- Don’t monetize quality, mission, safety, and reputation risk

Properly value risk impact

joseph.mayo@jwmc-llc.com

Change Organizational Culture

J. W. Mayo CONSULTING

Use six risk contexts

- Schedule risk – days, weeks, months, years
- Budget risk – $$
- Quality risk – defect density, warranty claims
- Mission risk – organizational objectives not achieved
- Safety risk – loss of life, lost work days from injury
- Reputation risk – customer satisfaction ratings, focus group results, independent assessment results

joseph.mayo@jwmc-llc.com

Change Organizational Culture

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

Change Organizational Culture

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

Risk Scenarios

J. W. Mayo CONSULTING

A way to conceptualize risk to aid in the identification of risk events

Entity that generates the threat

Nature of threat event

Entity affected by risk event

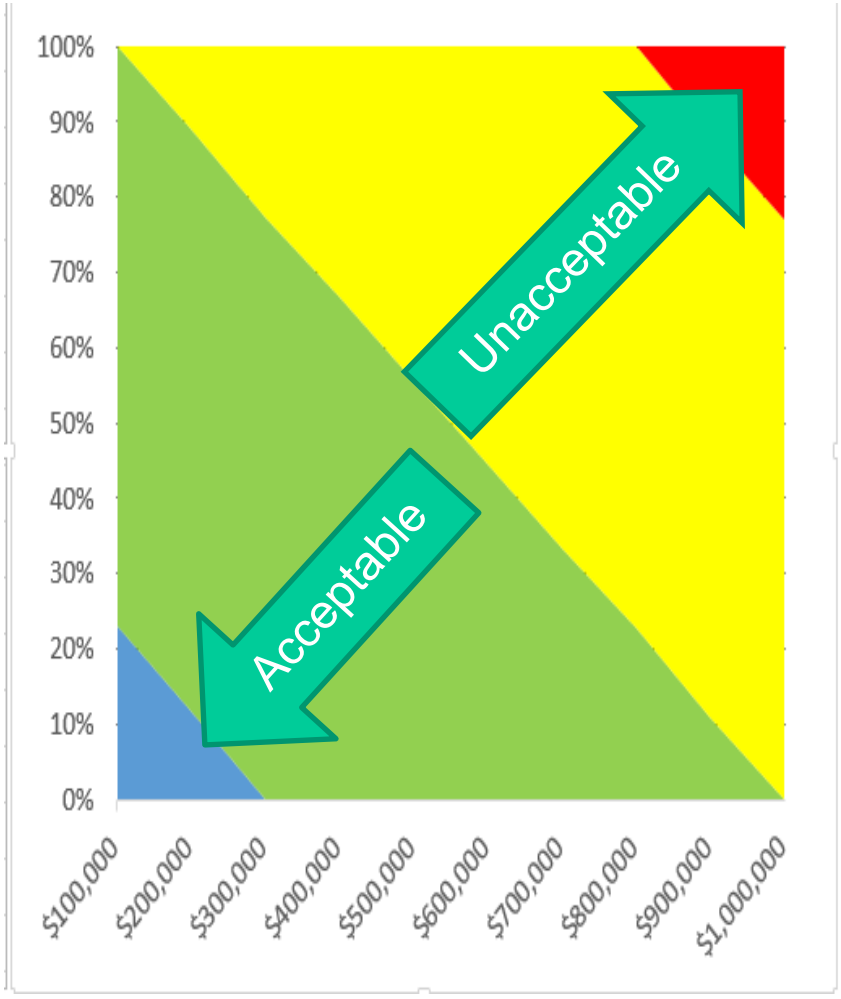
Risk Scenario

Actors	Threat Type		Risk Event		Assets	Time
Internal	Malicious	Failure	Disclosure	Ineffective Design	People	Duration
External	Accidental	Nature	Interruption	Ineffective Execution	Org Structure	Timing
	External Requirement	Error	Modification	Rules & Regulations	Process	Detection
			Theft	Inappropriate Use	Infrastructure	Time Lag
			Destruction		Information	
					Applications	

joseph.mayo@jwmc-llc.com

Risk Heat Maps

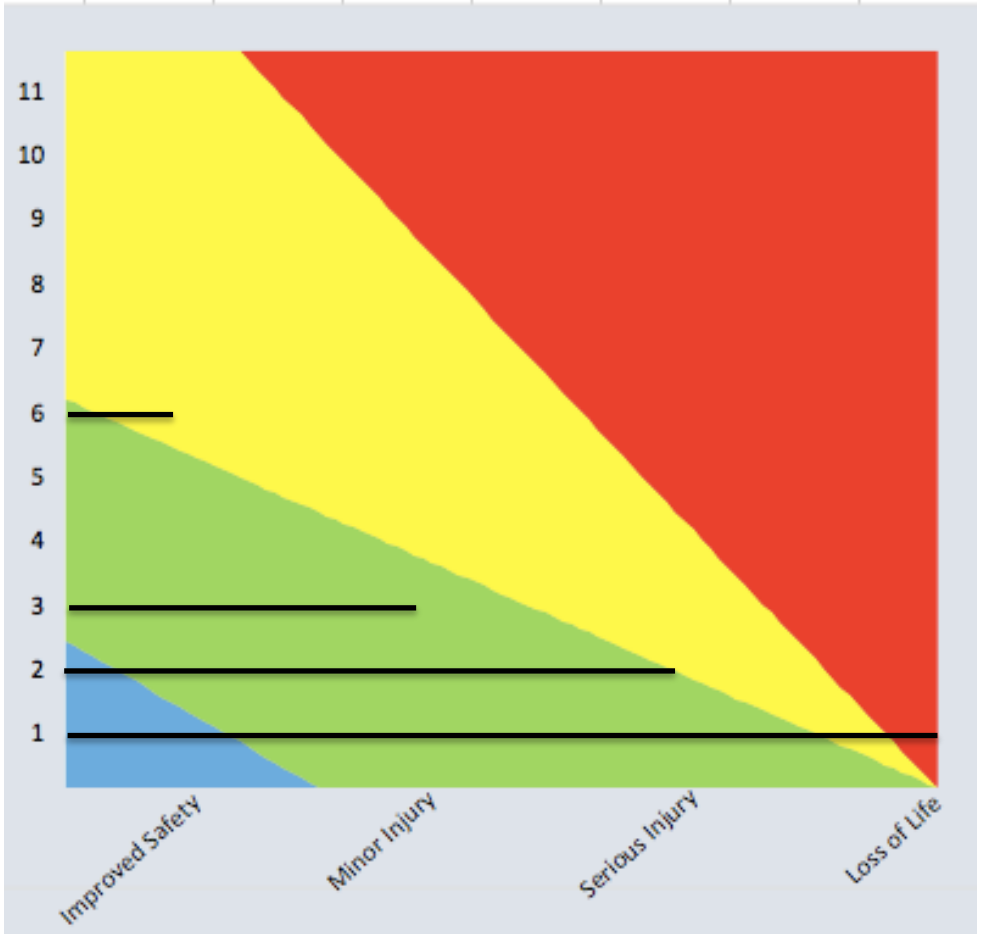
- ISACA's COBIT for Risk is an excellent guide
- Clarifies what constitutes acceptable vs unacceptable risks
- Understand risk tolerance thresholds



joseph.mayo@jwmc-llc.com

Risk Heat Maps

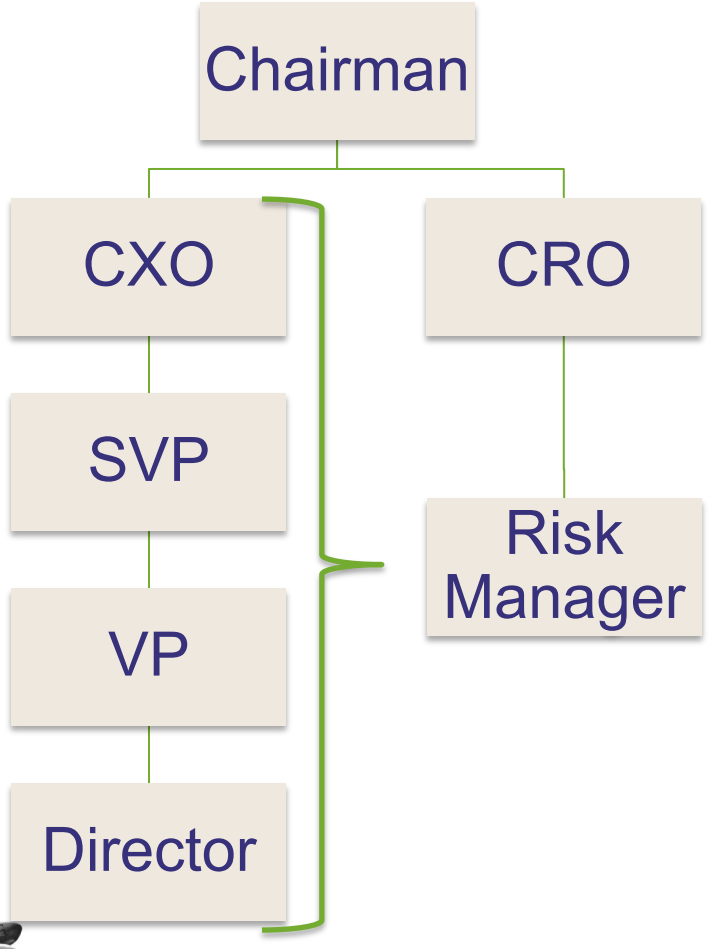
J. W. Mayo CONSULTING

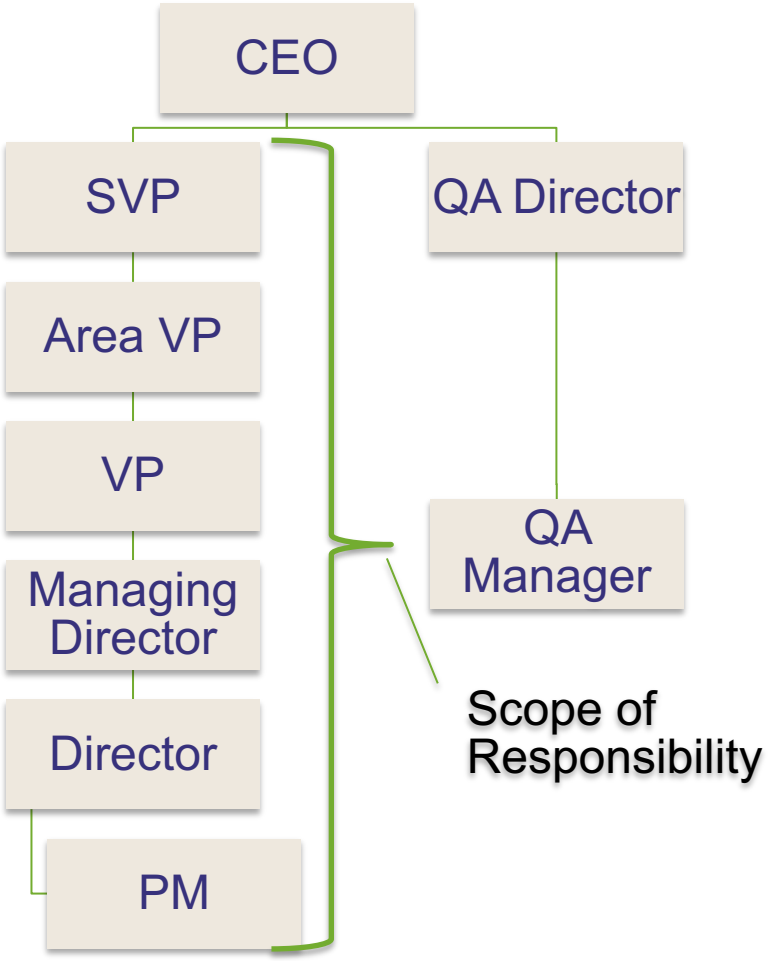


joseph.mayo@jwmc-llc.com

Re-evaluate Organizational Structure

J. W. Mayo CONSULTING





joseph.mayo@jwmc-llc.com

Re-evaluate Organizational Structure

Risk owner – person who writes the check to cover the impact resulting from a loss event

- Schedule Risk and Safety Risk – COO
- Budget Risk – CFO
- Mission Risk – CEO
- Quality Risk – CQO
- Reputation Risk – Chairman of the Board

joseph.mayo@jwmc-llc.com

High Reliability Organization (HRO)

J. W. Mayo CONSULTING

- Operate in environments where potential for disaster is high
- Very high risk appetite and tolerance
- Top priority is effective performance
- Avoid disasters through collective learning
- Develop a culture of reliability
- Extensive process auditing exists

- Reward system that rewards risk-mitigating behavior
- Quality standards that exceed referent standards
- Correctly assess risk impact
- Strong command and control system that includes migrating decision making, redundancy, decision makers have “big picture” perspective, and formal rules and procedures

joseph.mayo@jwmc-llc.com

Conclusion

- Is protecting the balance sheet enough?
- Establish and foster a risk aware culture
- Improper impact valuation can lead to astronomical financial impacts
  - Toyota, VW, Takata
- Normalized deviance can be catastrophic
  - GM, Columbia Shuttle, Deepwater Horizon
- Consider all risk contexts, not just financial risk
- Embrace tenants of HROs
  - Effectiveness, reliability, collective learning, and proper risk valuation

joseph.mayo@jwmc-llc.com

Basu, T. (2014, March). Timeline: A History Of GM's Ignition Switch Defect. *National Public Radio*, ().

CBS News. (2010). Toyota "Unintended Acceleration" Has Killed 89. Retrieved from http://www.cbsnews.com/news/toyota-unintended-acceleration-has-killed-89/

etkin, D. S. (1999). ESTIMATING CLEANUP COSTS FOR OIL SPILLS. *1999 International Oil Spill Conference*, (168).

Isidore, C. (2015, February). GM's Total Recall Cost: $4.1 billion. *CNN Money,* (), . Retrieved from http://money.cnn.com/2015/02/04/news/companies/gm-earnings-recall-costs/

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).

Morgan, D., & Klayman, B. (2015, May 20). UPDATE 8-Takata doubling U.S. recall for defective air bags to 34 mln vehicles. *Reuters*, p. 1.

Robertson, C., Schwartz, J., & PÉREZ-PEÑA, R. (2015, July 2). BP to Pay $18.7 Billion for Deepwater Horizon Oil Spill. *The New York Times*, p. 1.

Stapleton, T. (2012). *Data Breach Cost - Risks, costs and mitigation strategies for data breaches*. Schaumburg, IL: Zurich American Insurance Corporation.

Ponemon Institute. (2015). *2015 Cost of Data Breach Study: Global Analysis*. Traverse City, MI: Ponemon Institute LLC.

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