

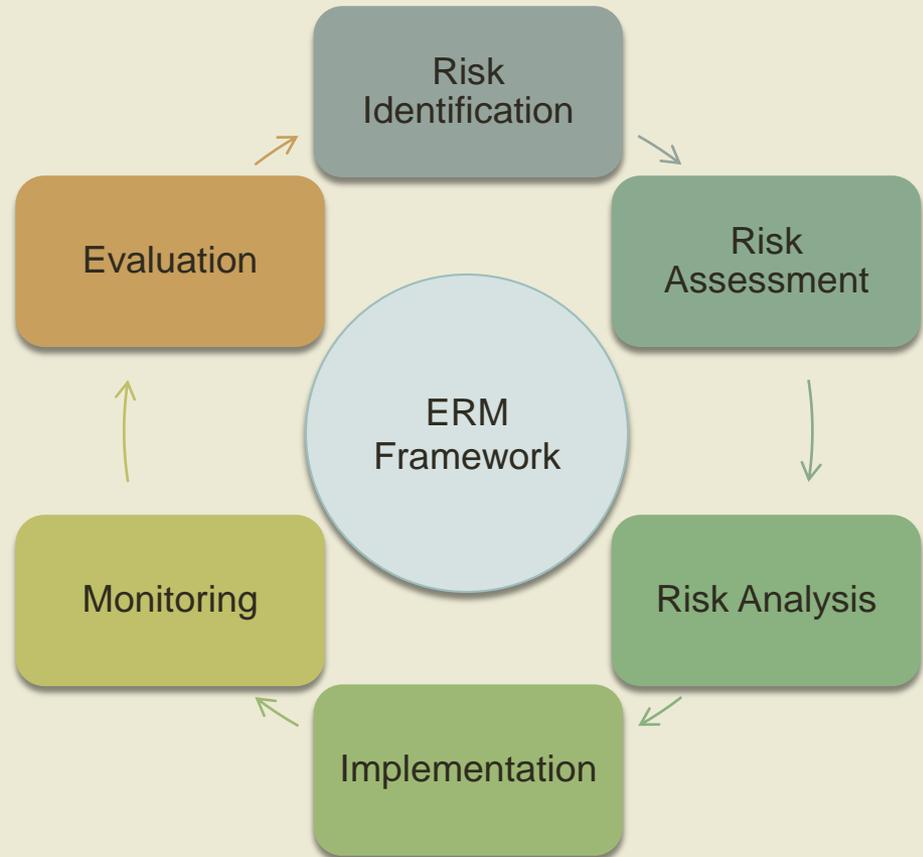
Enterprise Risk Management Application & Case Studies

Presented by Kristina Narvaez, MBA
President of ERM Strategies, LLC

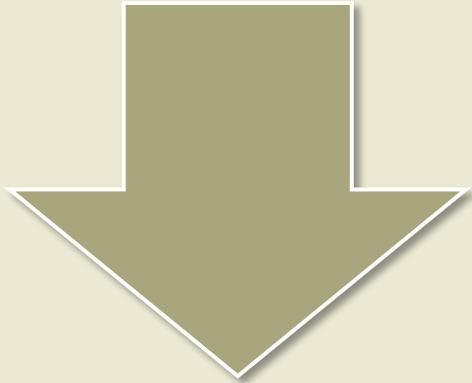
Enterprise Risk Management

ERM provides a framework for risk management, which typically involves identifying particular events or circumstances relevant to the organization's objectives (risks and opportunities), assessing them in terms of likelihood and magnitude of impact, determining a response strategy, and monitoring progress.

By identifying and proactively addressing risks and opportunities, business enterprises protect and create value for their stakeholders, including owners, employees, customers, regulators, and society overall.

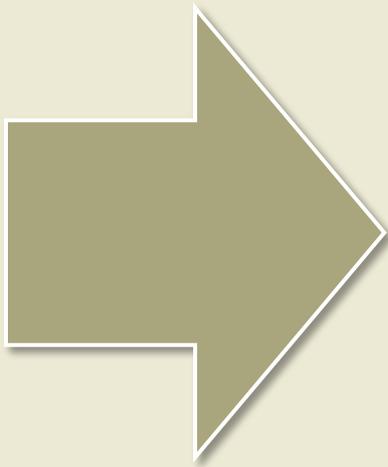


Difference Between GRC & ERM



Governance Risk and Compliance (GRC)

Embraces compliance as a separate activity for each business silo.



Enterprise Risk Management (ERM)

Is concerned with delivering measurable business value by tying front line operational activities to goals across all business units.

Burden of Compliance Suppresses Risk Taking Activities

Many organizations believe that they must continue to eliminate risk through compliance

Risk has not been eradicated by regulation instead it has been driven underground

Risk taking activities are not bad if an organization has established their risk appetite and risk tolerance levels and has the proper risk controls in place

Risk Appetite and Risk Tolerance

- **Risk Appetite** is the manner in which an organization and its stakeholders collectively perceive, assess and treat risk
- **Risk Tolerance** requires a company to consider in quantitative terms exactly how much of its capital it is prepared to put at risk



ERM Is Used for Risk Optimization

- Considering both the upside and downside outcomes of risk taking activities
- When threats and opportunities are better understood, risk taking is optimized and managers, in turn, will make more informed business decisions
- Improved decision making enables an organization to quickly meet emerging marketplace challenges



Six Step Approach to ERM



1. Risk Identification

- The process of taking inventory of all risks in an organization and defining the potential risk event, the causes to that risk event, and the potential outcome if that risk event were to occur
- Focus not only on hazard or operational risks, but also strategic, financial, reputational, compliance, environmental, human capital and technology, market, and supply chain risks



Scope of Risk Identification

1
Risk
Identification

Define where the source of a potential risk event is coming from; Inside or Outside the organization. Establishing risk categories helps to identify the sources of a risk event.



Strategic Risk Categories

1
Risk
Identification



Operational Risk Categories

1
Risk
Identification



Financial Risk Categories

1
Risk
Identification



Other Risk Categories



Identify Subcategories

1
Risk
Identification



Hazard Risk

Safety risk of increased slips, trips and falls accidents occurring in the organization



Operational Risk

Human capital risk of 25% of workforce is eligible for retirement in the next 5 years



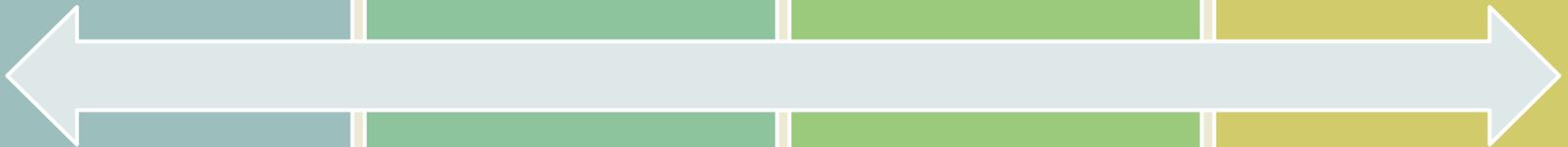
Financial Risk

Credit risk of 35% of commercial loans will default in the third quarter



Strategic Risk

Sole supplier of a raw material has been acquired by competitor



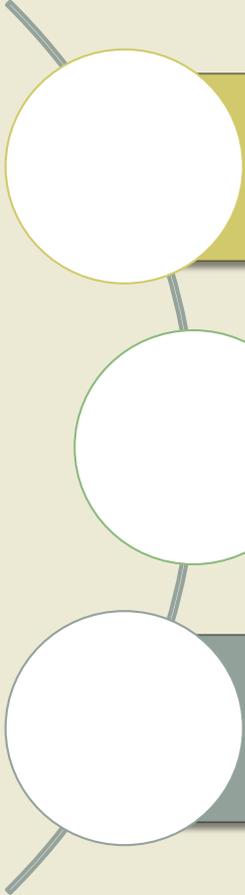
Existing & Emerging Risk

Look not only at existing risks, but also the emerging risks to the organization.

- What new business processes have been added to the organization?
- What changes have been made in the organizational chart?
- What are some external risks that could impact the organization like economic, environmental, societal, geopolitical, and technological?



Know Where You Stand



Meet with senior management to define the strategic goals of your organization

Review the mission and vision statements of the organization

Define the expectations of internal and external stakeholders

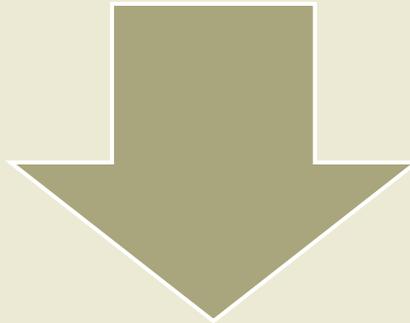
Don't Be Conflicted



GlaxoSmithKline – A study in conflicting strategic goals

This conflict caused the quality control of manufacturing to suffer.

Case in point – the Cidra Plant in Puerto Rico made 20 drugs under unhealthy conditions that lead to a \$750 million FDA fine

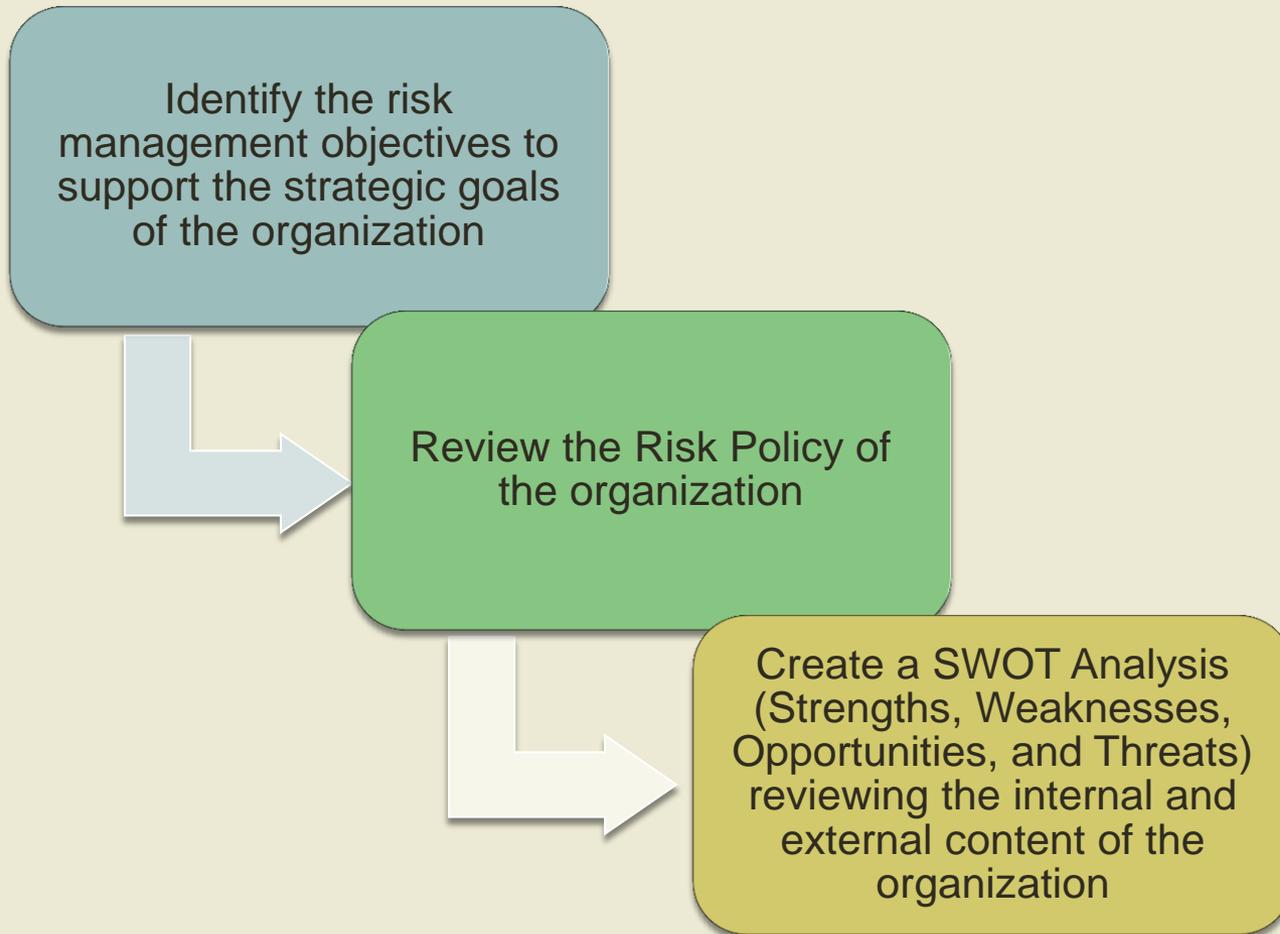


One of GSK's strategic goals was to sell safe and effective prescription medication

Another goal was to increase profitability by outsourcing manufacturing to other parts of the world



Next Steps



SWOT Analysis

1
Risk
Identification



Risk Identification Activities

1
Risk
Identification

Brainstorming

Can effectively generate lots of ideas of potential risk scenarios that could take place

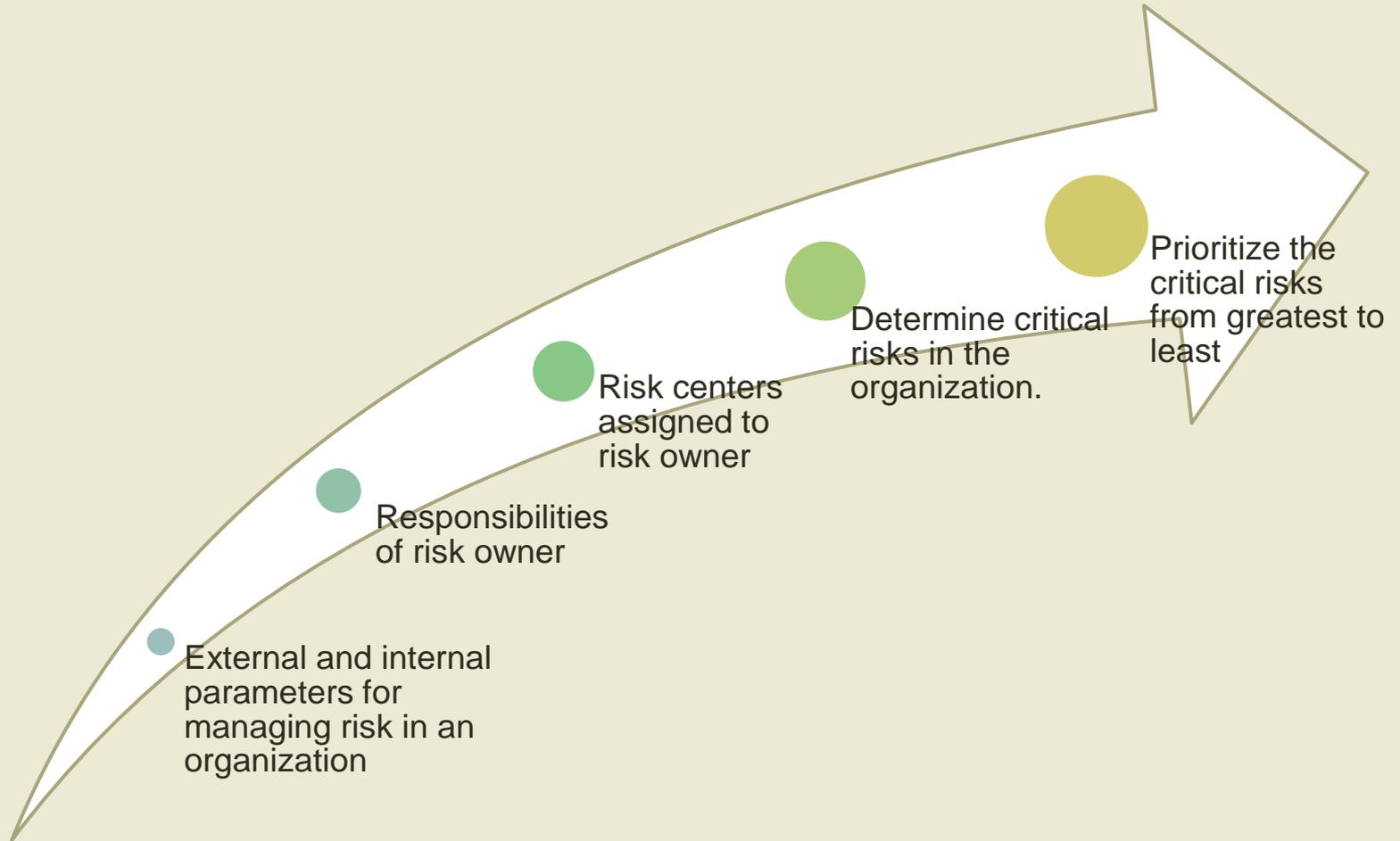
Structured Interviews

Uses a risk survey or questionnaire to ask specific questions related to different types of potential risk events facing a particular risk owner or risk center

Top Down / Bottom Up Approach

Establish Risk Criteria

1
Risk
Identification





UC's ERM Work Plan

1
Risk
Identification

University of California has developed an ERM Work Plan for its employees. Within the context of campus/medical center's mission, the management team establishes strategic goals, selects strategy and aligns ERM objectives to the strategic plan. The enterprise risk management framework is geared to achieving objectives in four categories:

Strategic

High-level goals, aligned with and supporting their mission

Operations

Effective and efficient use of their resources

Reporting

Reliability of reporting

Compliance

Compliance with applicable laws and regulations

Key Performance Indicators (KPI)

KPIs help you understand how well you are performing in relation to your strategic goals and objectives.

In order for KPIs to be effective, they need to be measurable.

- % of customer attrition
- % of employee turnover
- Rejection rate
- Meantime to repair IT problems
- Customer order waiting time
- Profitability of customers by demographic segments

Key Risk Indicators (KRIs)

KRIs are leading indicators of risk to business performance. They give us an early warning to identify a potential event that may harm continuity of the activity/project.

% of suppliers with no business continuity management

% of mission-critical recovery plans not exercised with the last 12 months

% turnover of mission-critical IT personnel

% of mission – critical business processes with a backup/recovery architecture

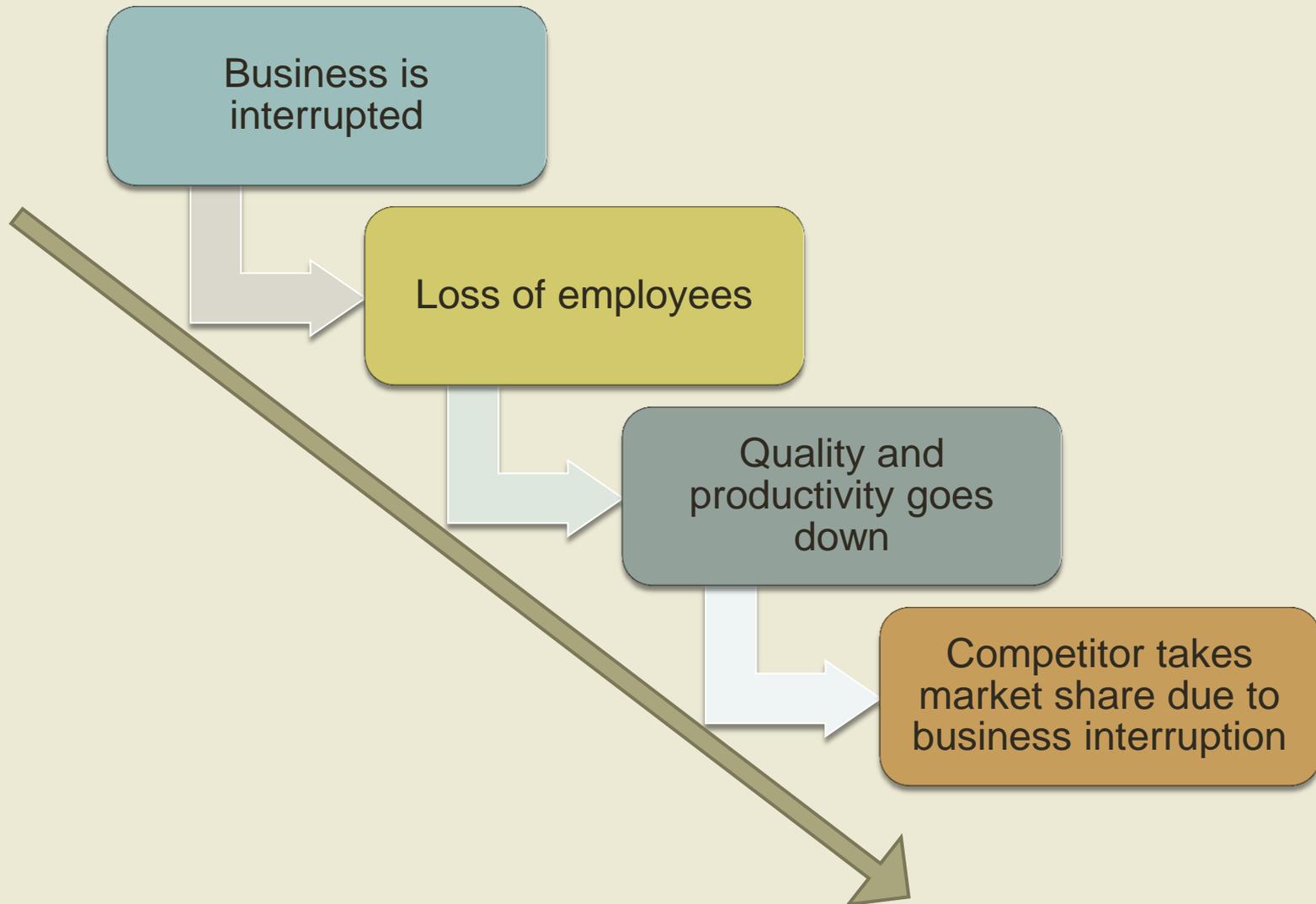
Supply Chain Disruption

1
Risk
Identification

Some sources of risk are not directly under the control of the organization, but are a part of their supply chain.

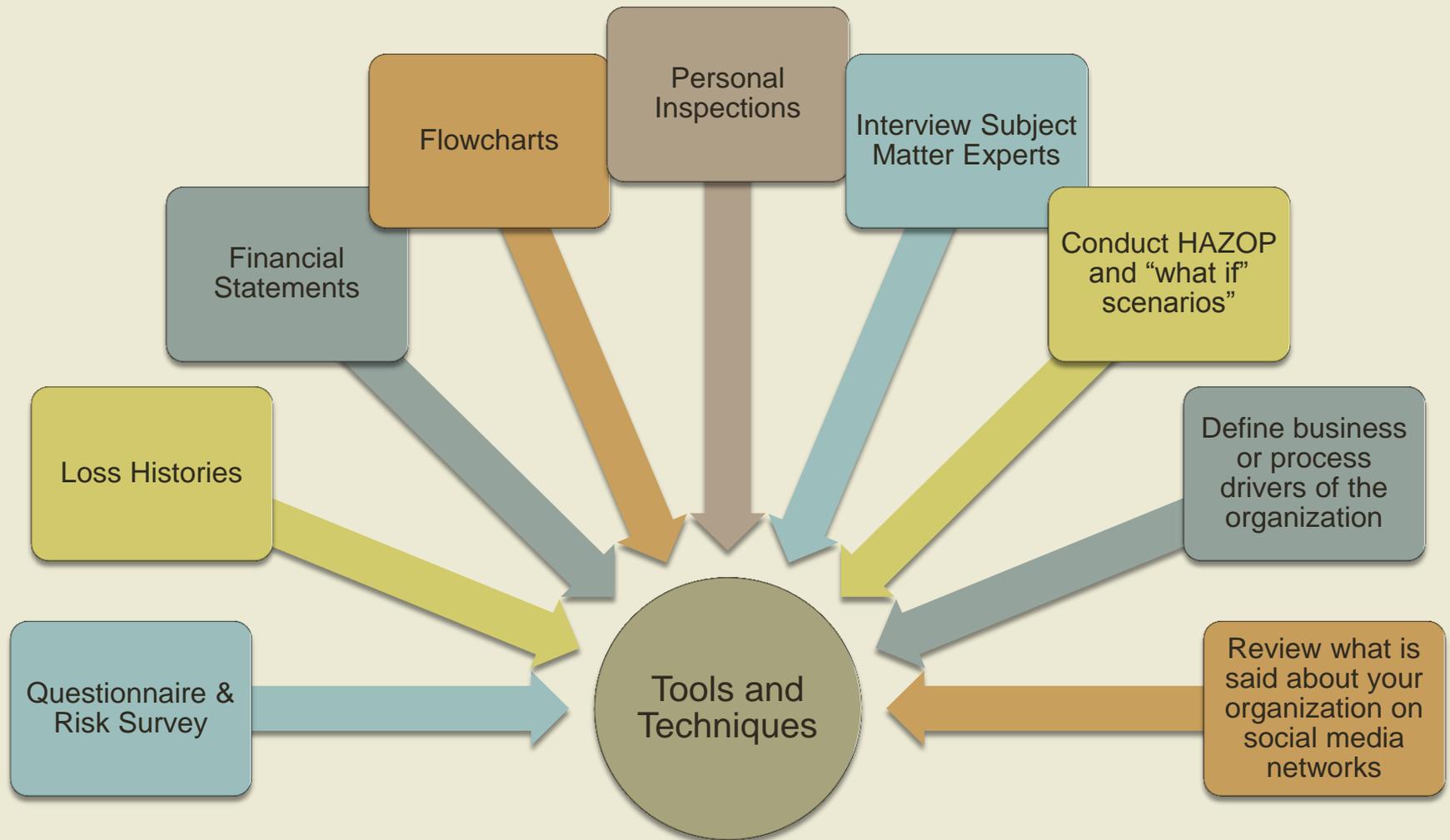
March 11, 2011 - A massive tsunami devastated the coastline of Japan. GM, who might had a competitive advantage to their Japanese competitors, had a transmission that was manufactured in Japan for its Chevy Volt

Cascading Effects



Tools and Techniques

1
Risk
Identification



Create A Risk Register

1
Risk
Identification



Sample Risk Register

1
Risk
Identification

Risk Register

File Edit View Tools Reports Help

Qualitative Quantitative

Risk		Pre-Mitigation (Data Date = 25 Oct 07)							Mitigation		Post-mitigation					
ID	T/O	Title	Probability	Schedule	C...	Sco...	Quality	Score	Response	Title	Probability	Schedule	C...	Sco...	Quality	Score
1	T	Number of rigs just 31 against 54 agreed	VH (90%)	VH (60)	L (...)	VL	L	72	Avoid	Additional rigs (threat)	L (15%)	VH (60)	L (...)	VL	L	24
49	T	Dosing skids	VH (90%)	VL (2)	VL ...	H	H	36	Reduce		VH (90%)	VL (2)	VL ...	L	L	12
3	T	Tubing tongs	VH (90%)	VH (60)	VL ...	VL	M	72	Transfer	Provide tubing tongues	L (15%)	VH (60)	VL ...	VL	M	24
4	T	Organizational changes	VH (90%)	L (7)	L (...)	L	M	18	Reduce	Program organization	VL (5%)	VL (2)	VL ...	VL	VL	1
5	T	Supplies	L (15%)	H (30)	VL ...	VL	VL	12	Transfer	Sub-supplier	VL (5%)	H (30)	VL ...	VL	VL	4
6	T	Review and Approvals	H (60%)	H (30)	VL ...	L	VL	28	Avoid	Update review and approval pro...	L (15%)	H (30)	VL ...	L	VL	12
7	T	Maintenance	VH (90%)	N (0)	N (...)	VL	VH	72	Avoid	Rod Pump Manual	VL (5%)	VL (2)	VL ...	VL	VH	8
X1	O	Shift rigs	M (30%)	VH (120)	L (...)	L	L	40	Exploit		H (60%)	VH (120)	L (...)	L	L	56
8	T	Weather	H (60%)	H (30)	L (...)	L	L	28	Avoid	Prepare for bad weather	H (60%)	L (7)	L (...)	L	L	7
9	T	Injuries	L (15%)	L (7)	VL ...	VH	VL	24	Avoid	Hazards identification	VL (5%)	VL (2)	VL ...	VH	VL	8
10	T	Information and communication	VH (90%)	VH (60)	L (...)	L	L	72	Avoid	Data planning	L (15%)	VH (60)	L (...)	L	L	24
11	T	Equipment availability	M (30%)	VH (60)	L (...)	L	L	40	Reduce	Procurement planning	L (15%)	L (7)	VL ...	VL	VL	3
12	T	Material, Equipment performance reliabil...	VL (5%)	N (0)	N (...)	M	H	4	Transfer		VL (5%)	L (7)	VL ...	VL	VL	1
13	T	Service, Technical performance reliability	L (15%)	H (30)	M ...	M	H	12	Reduce		VL (5%)	L (7)	VL ...	VL	VL	1
14	T	Environment exposure	H (60%)	H (30)	M ...	L	L	28	Avoid		L (15%)	L (7)	L (...)	VL	VL	3
16	T	Maintenance training	VL (5%)	VL (2)	VL ...	VH	VL	8	Avoid	New team trainings	VL (5%)	VL (2)	VL ...	VL	VL	1

Risk Details User Defined Mitigation Waterfall Chart Notes Risk History

ID: 1 Title: Number of rigs just 31 against 54 agreed

RBS Resources: ...

Cause: 1) operating areas claim that they have production losses and that wells are waiting for intervention or that other work over jobs are in progress and so they cannot provide additional rigs

Description: During a presentation on 22nd of March to the Management it has been agreed that the project will get 54 rigs, approximately 45 would work on new completions and 9 rigs would have to go back and perform interventions on wells

Effect: 1st delay of schedule in September expected, effect on project total 4 - 6 month

Threat / Opportunity: Threat Manageability: Difficult

Owner: Unassigned Status: Open

Exposure (Entered):

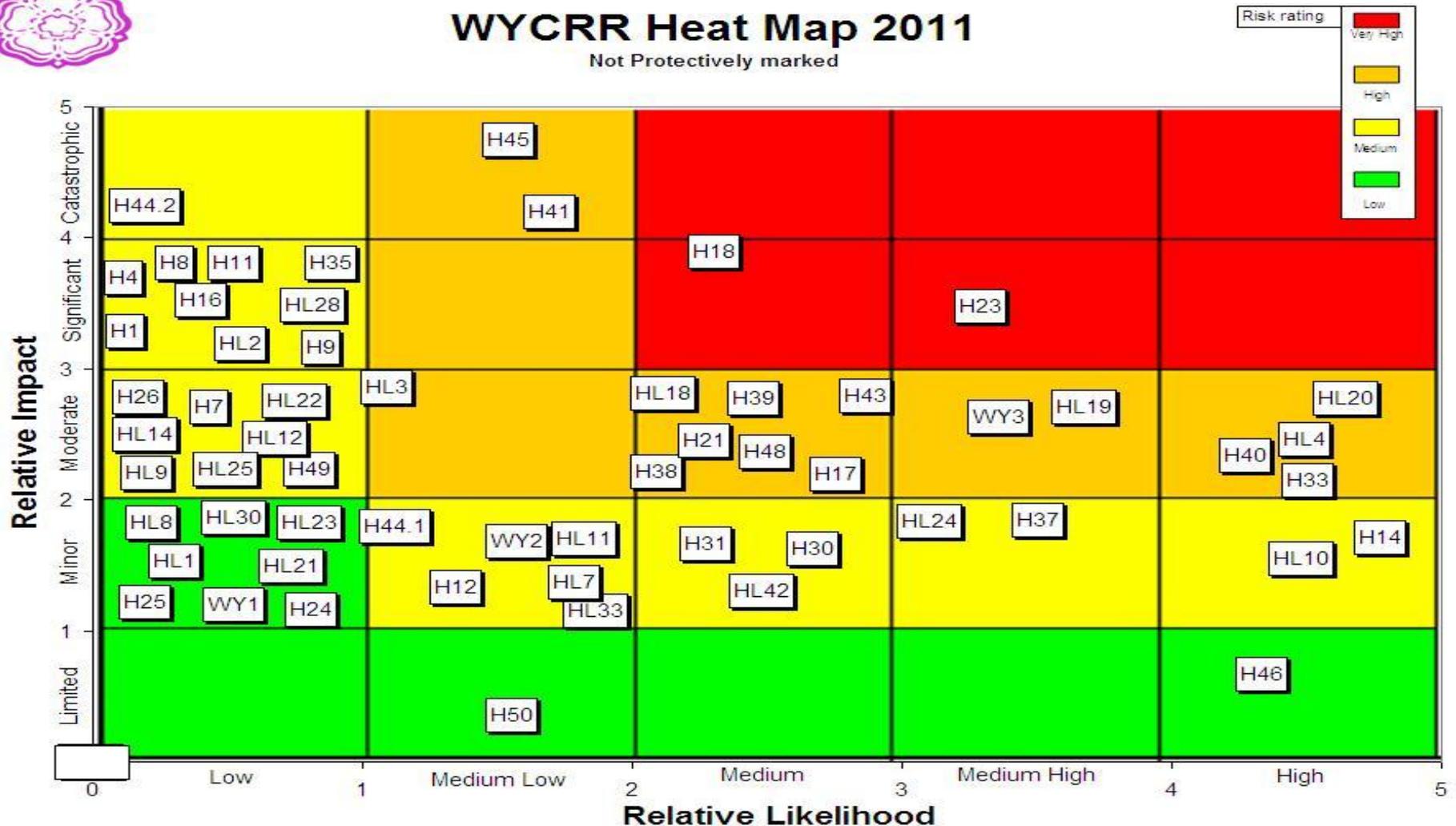
Selected risk: 1 - Number of rigs just 31 against 54 agreed

Sample Risk Heat Map

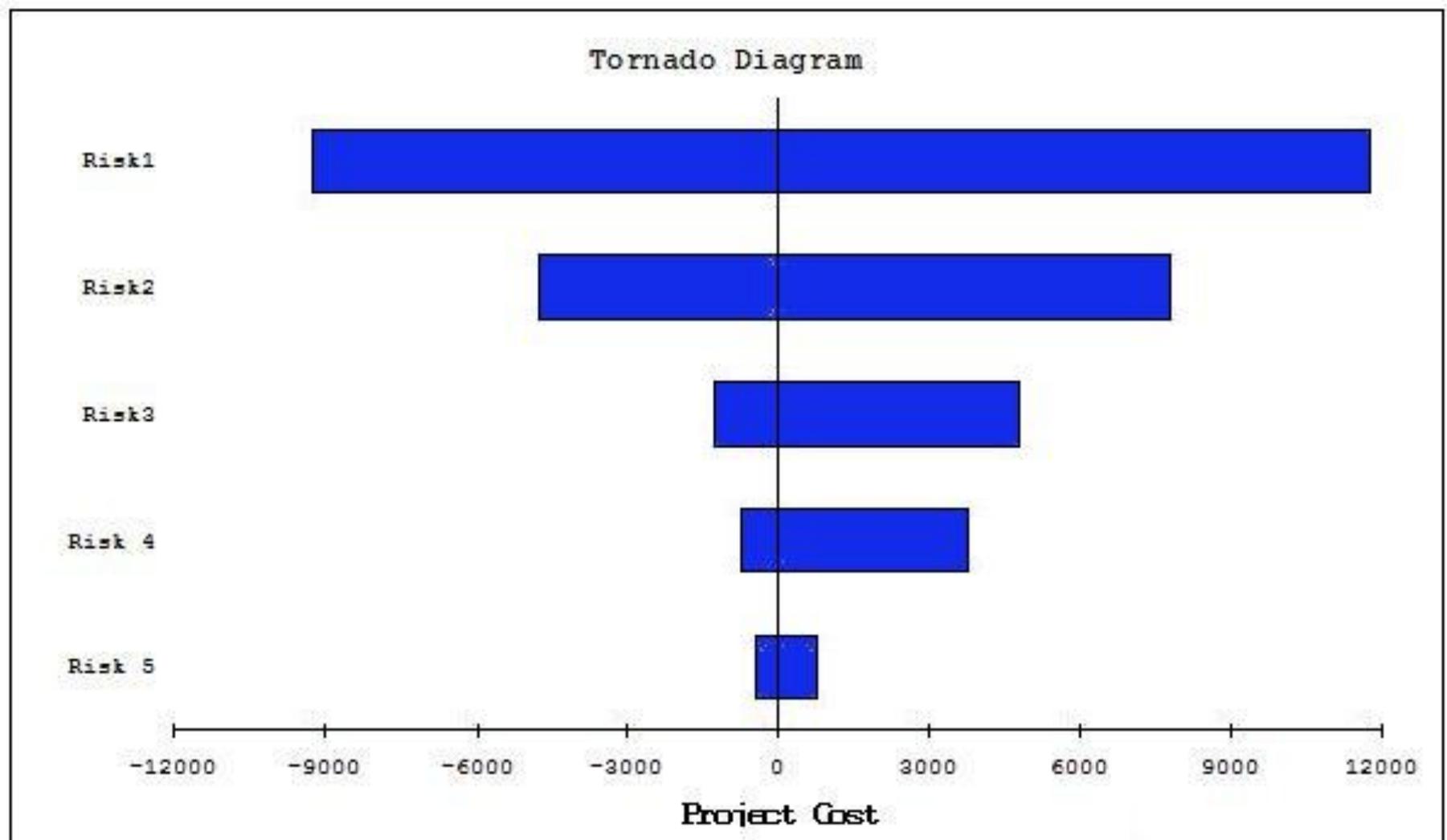


WYCRR Heat Map 2011

Not Protectively marked

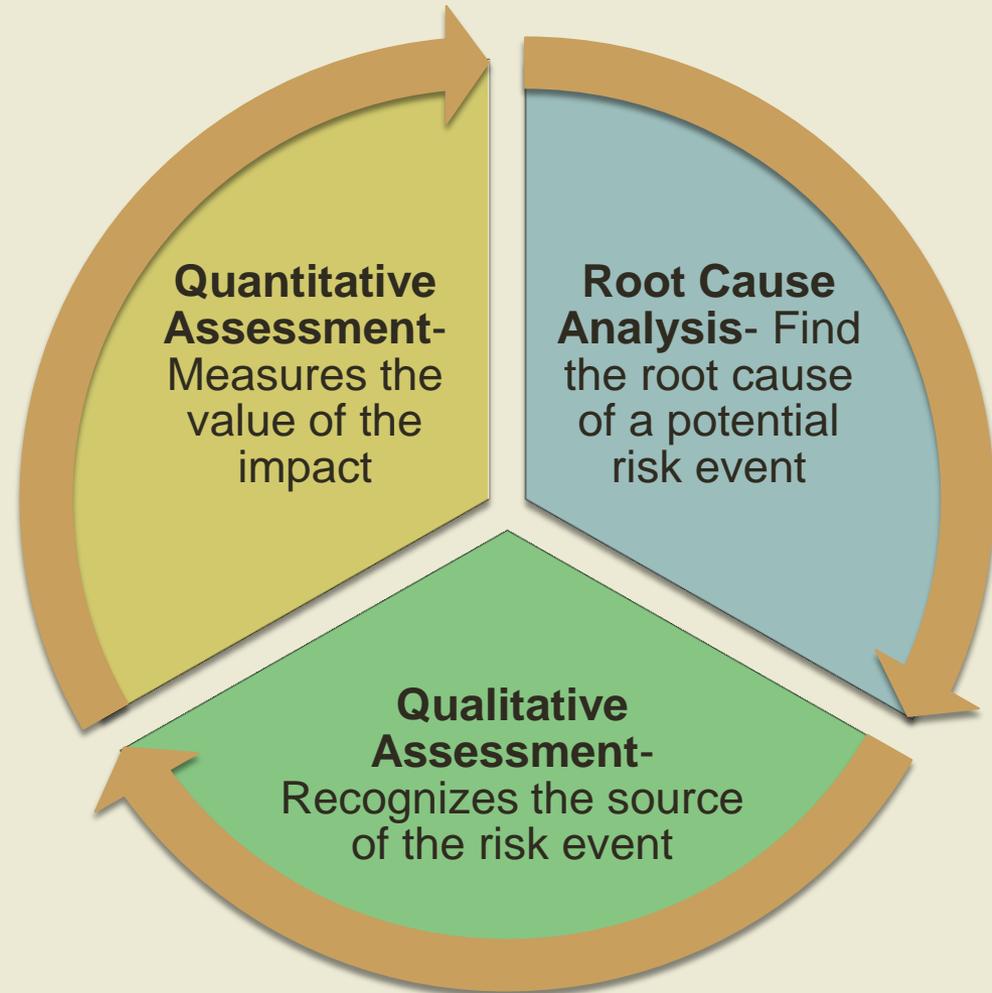


Risk Tornado Diagram



2. Risk Assessment

Risk Assessment is a process to determine the cause of the risk event, the risk event itself, and the impact and the velocity of the risk event.



Three Basic Causes

Physical causes

A tangible or material item failed in some way.

Brakes stop working on a car

Human causes

People did something wrong or did not do something required.

No one check the condition of the brakes

Organization causes

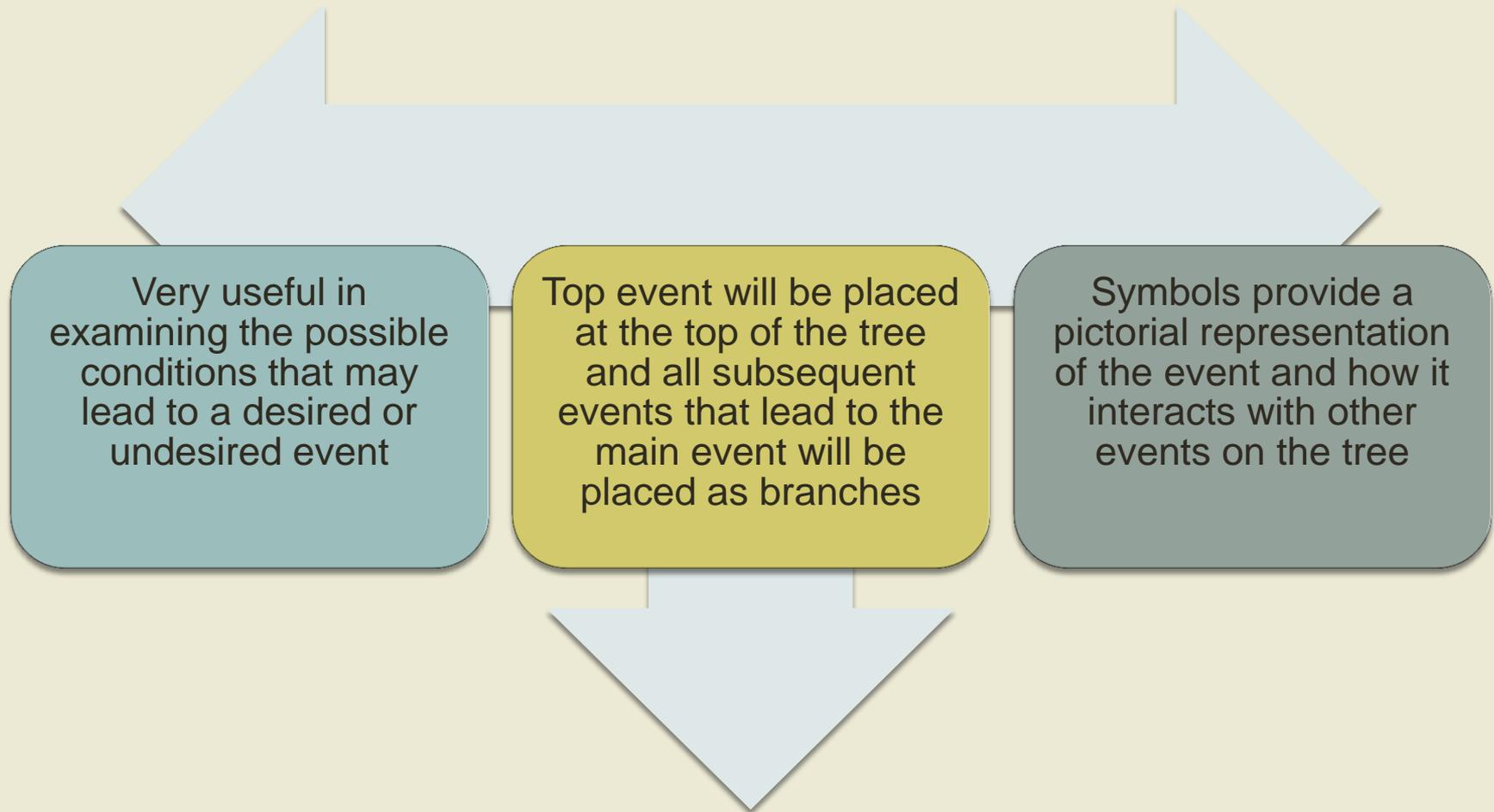
A system, process or policy that people use to make decisions in doing their work is faulty.

No procedure for checking the maintenance of the cars

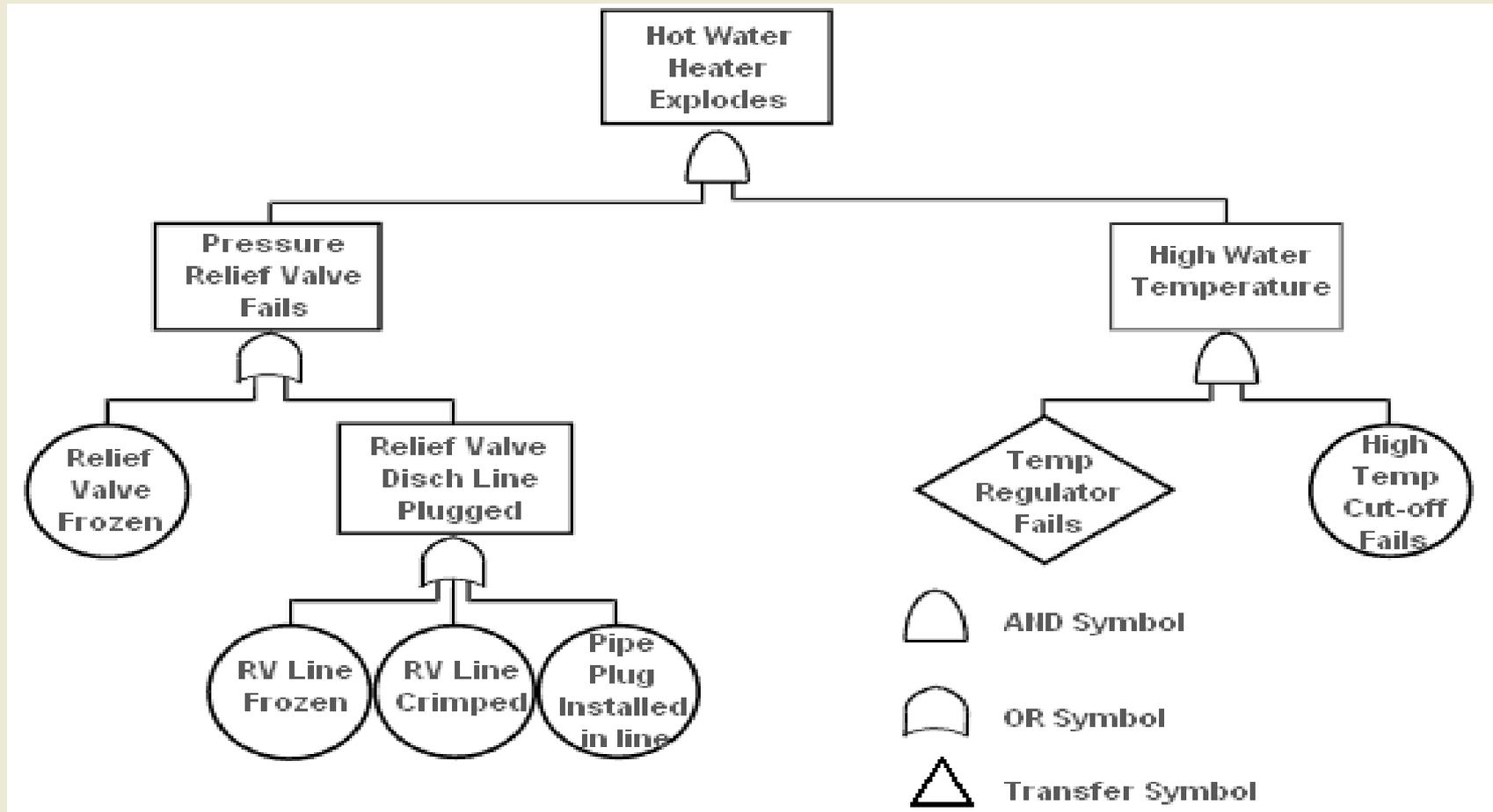
Root Cause Analysis



Fault Tree Analysis



Example Fault Tree



Qualitative Analysis

Positive Fault Tree Analysis

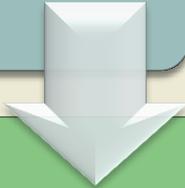
Will identify the events necessary to achieve a top desired event for example no accident in manufacturing facility

Negative Fault Tree Analysis

Constructed to show those events or conditions that will lead to a top undesired risk event such as a fire in the manufacturing facility

Quantitative Analysis

When the likelihood of an event is known and a probability value has been assigned, then analysis of these events on a fault tree will also yield quantitative results.



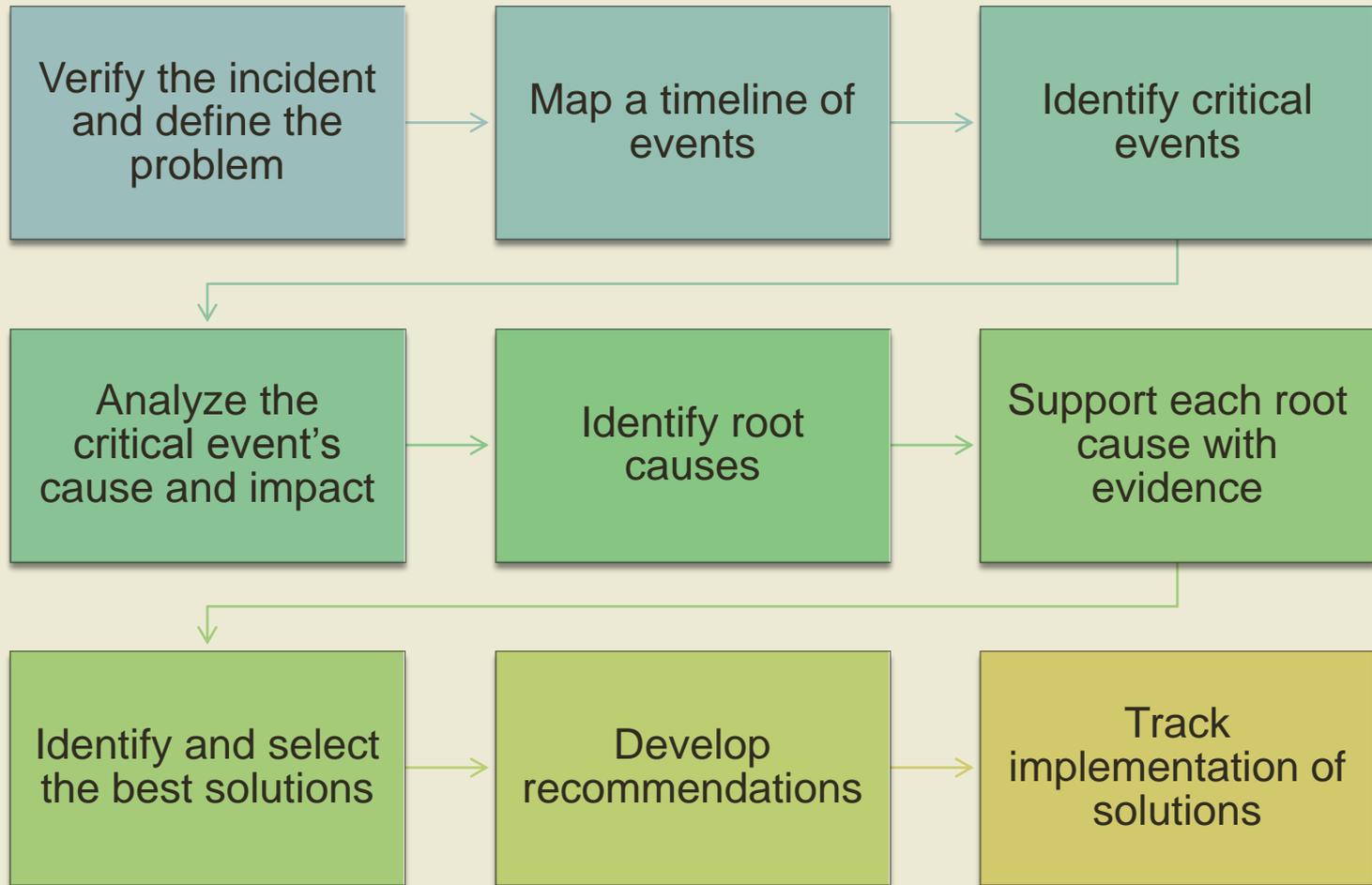
Financial impact can be added to each stage of the Fault Tree Analysis.



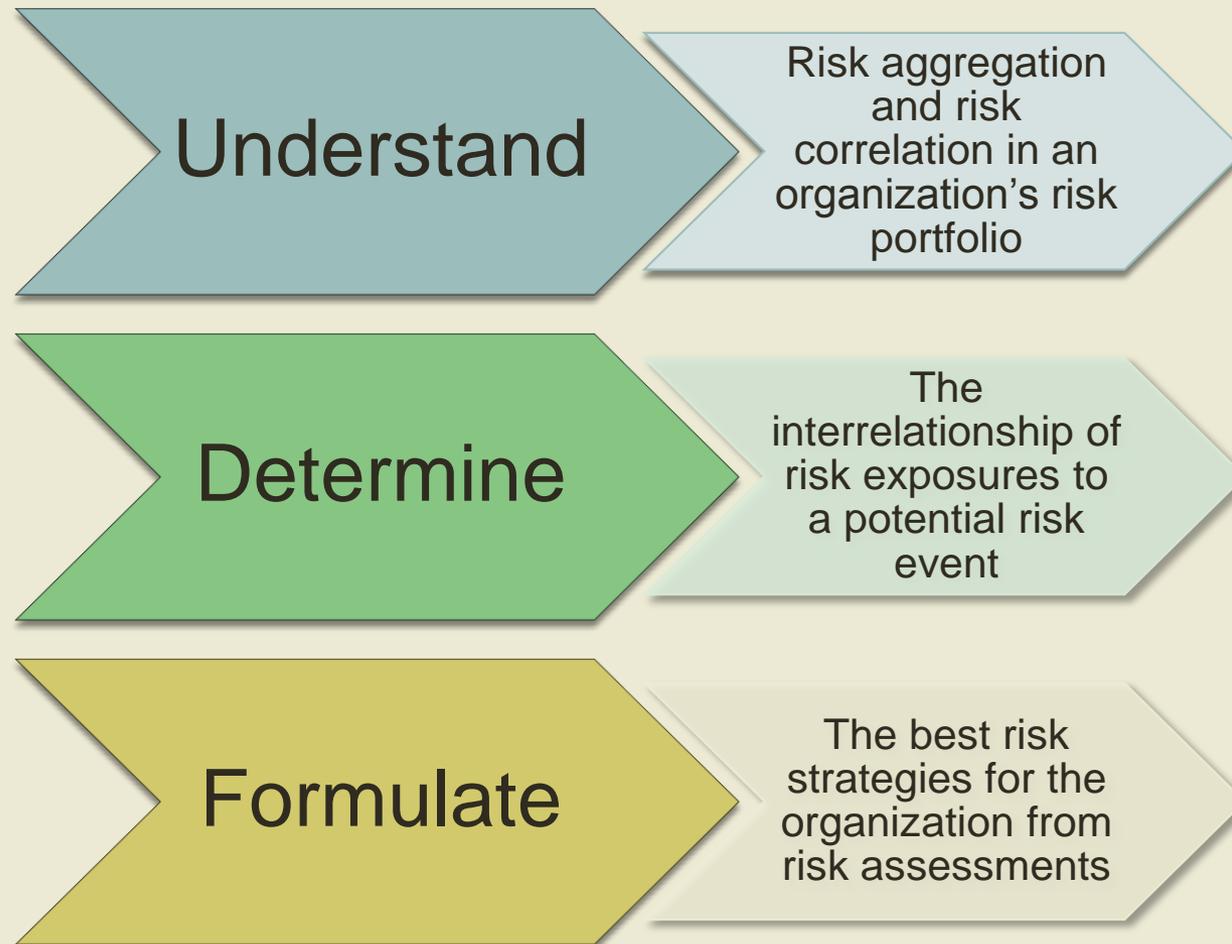
Risk correlation can be demonstrated.

State of Washington's Nine Step Approach to Root Cause Analysis

2
Risk
Assessment



3. Risk Analysis



Department of Homeland Security

3

Risk Analysis

DHS plays a leadership role in the Nation's unified effort to manage risk working across the homeland security enterprise which includes Federal, state, local, tribal, territorial, non-governmental and private sector entities.

As part of the analysis in their ERM program, DHS used an integrated risk management structure to share risk information and analysis.

The goal of using integrated risk management structure is to be able to work with its partners to address uncertainty inherent in their complex mission space, and help make the tough decisions necessary to keep the nation resilient and secure with limited resources.



DHS Analysis Tools

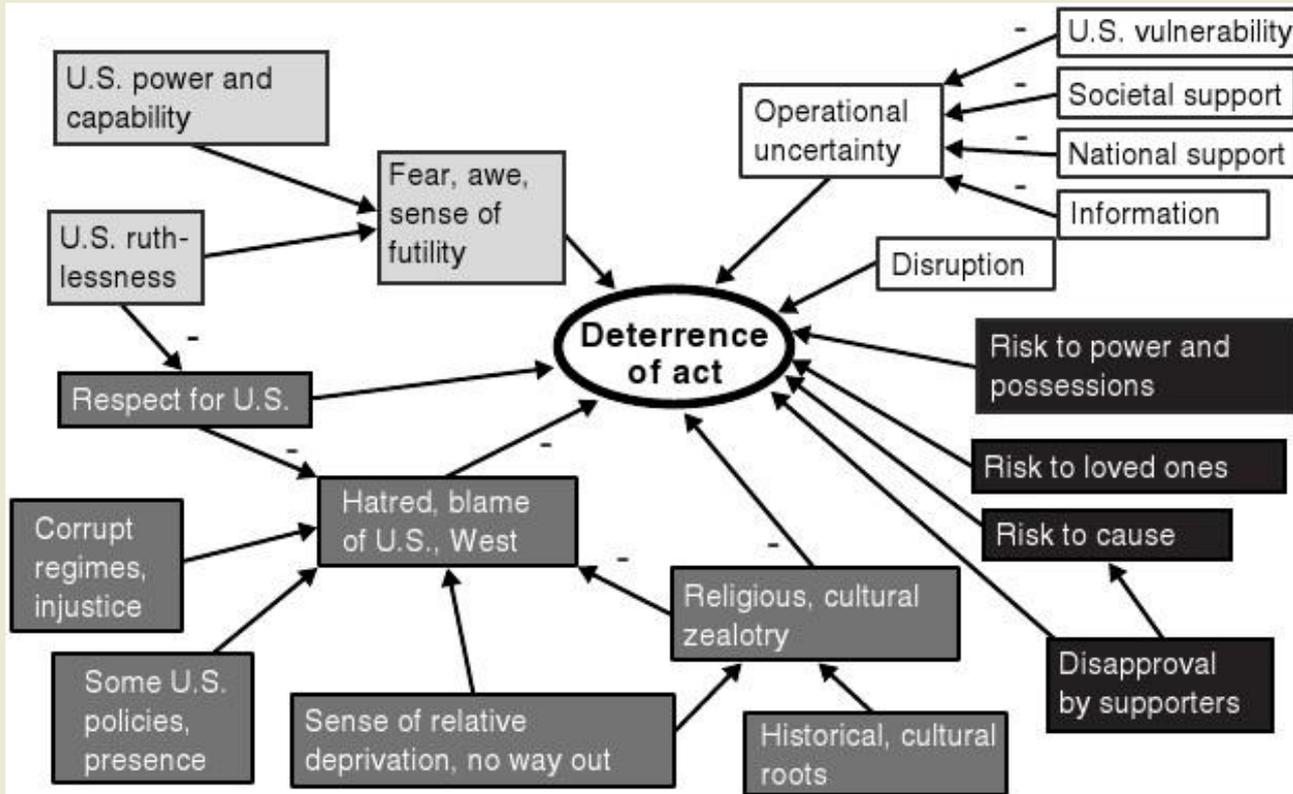
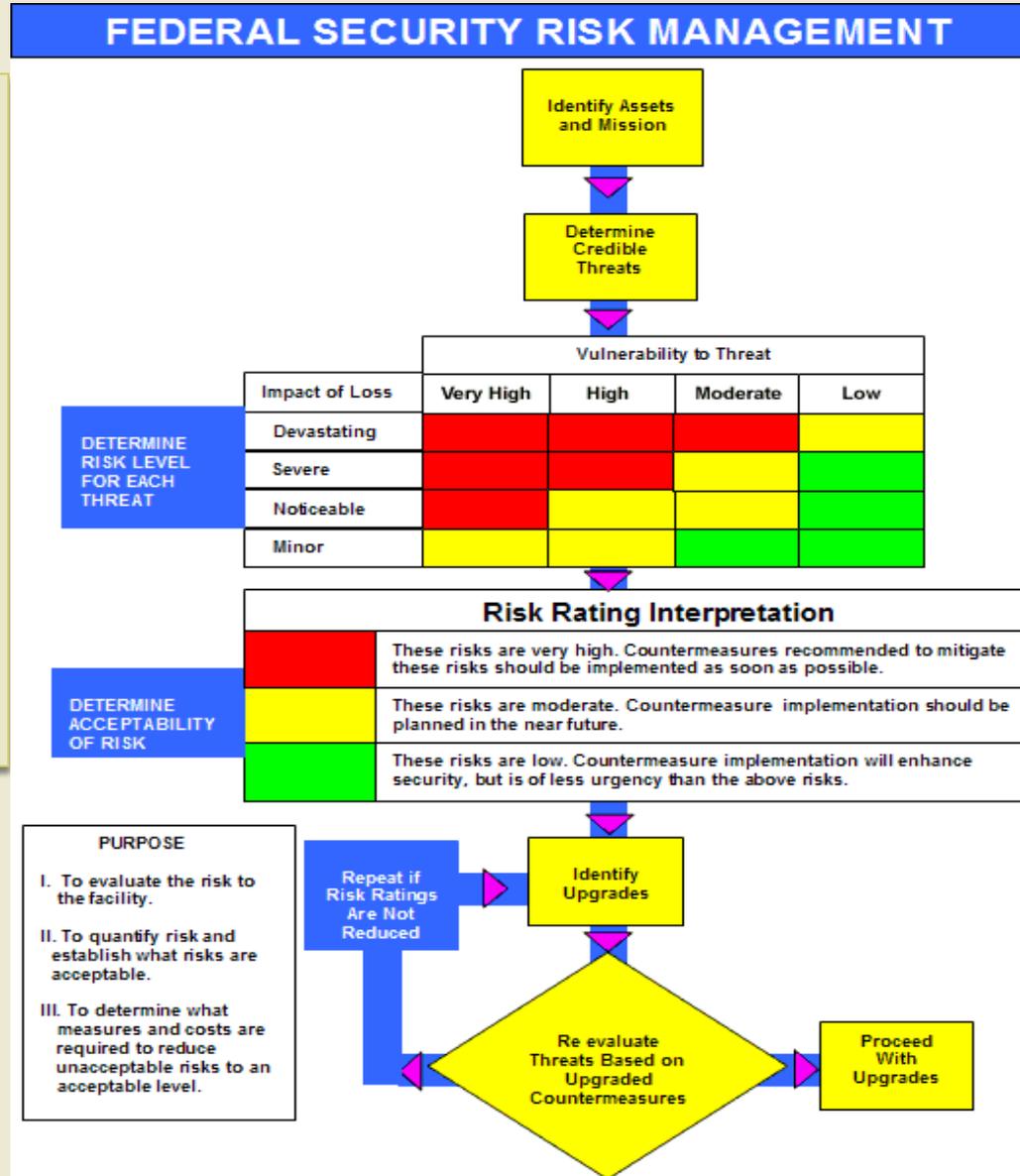


Figure 3.4—A Systemic Perspective

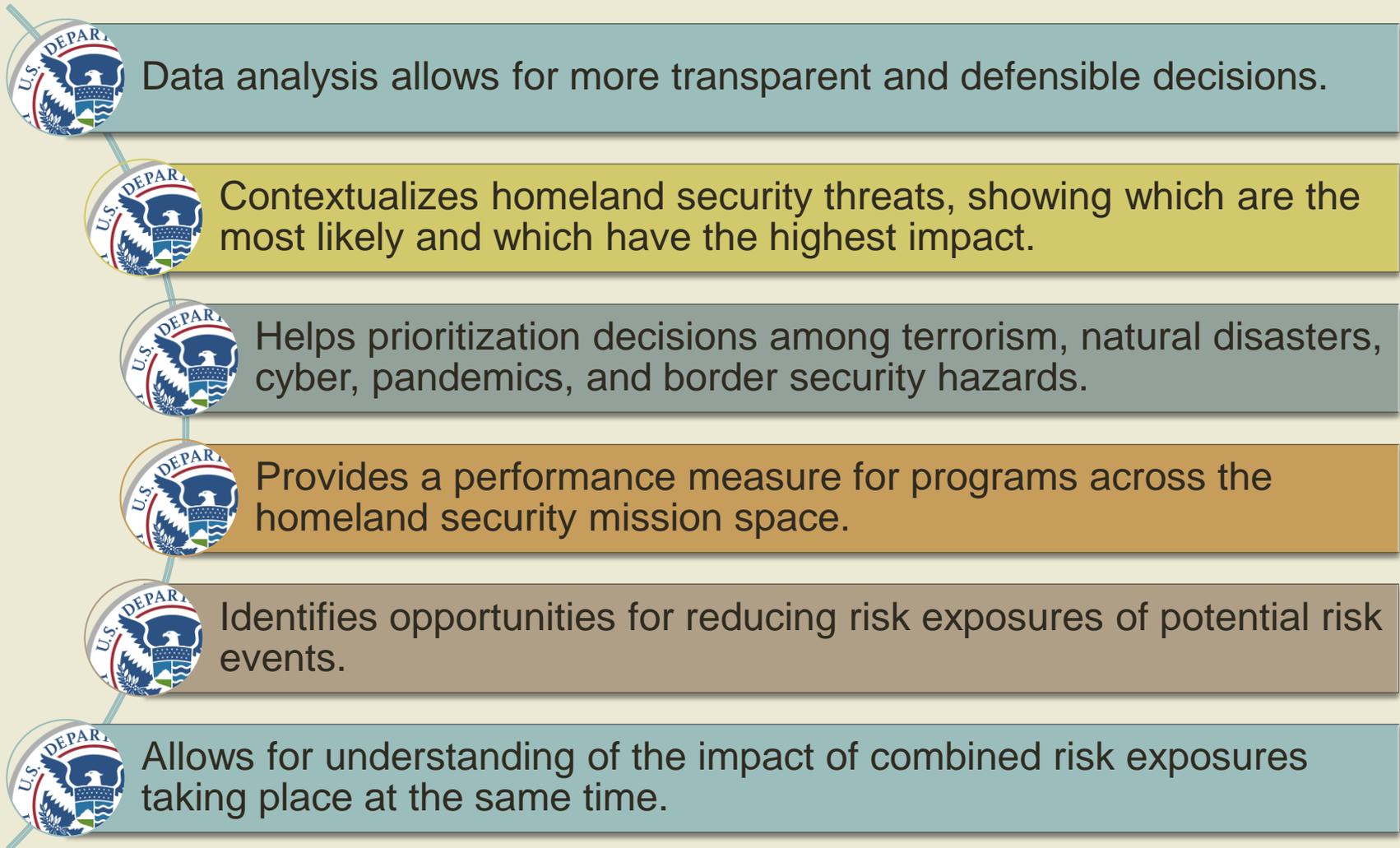
DHS uses Influence Diagrams to analyze the interrelationships and interdependencies of risks across the enterprise.

DHS Analysis Tools

DHS uses analytic tools like RAPID-Risk Assessment Process for Informed Decision-Making to manage risks associated with their strategic goals.



Value of Data Analysis to DHS



4. Implementation

Implementation - incorporating an ERM structure, practices, and strategies to fulfill the goals of the organization.

ERM framework

Risk controls

Risk champions and risk centers

Risk communication structure

Crisis management protocol

Business Continuity

ERM Frameworks

COSO II

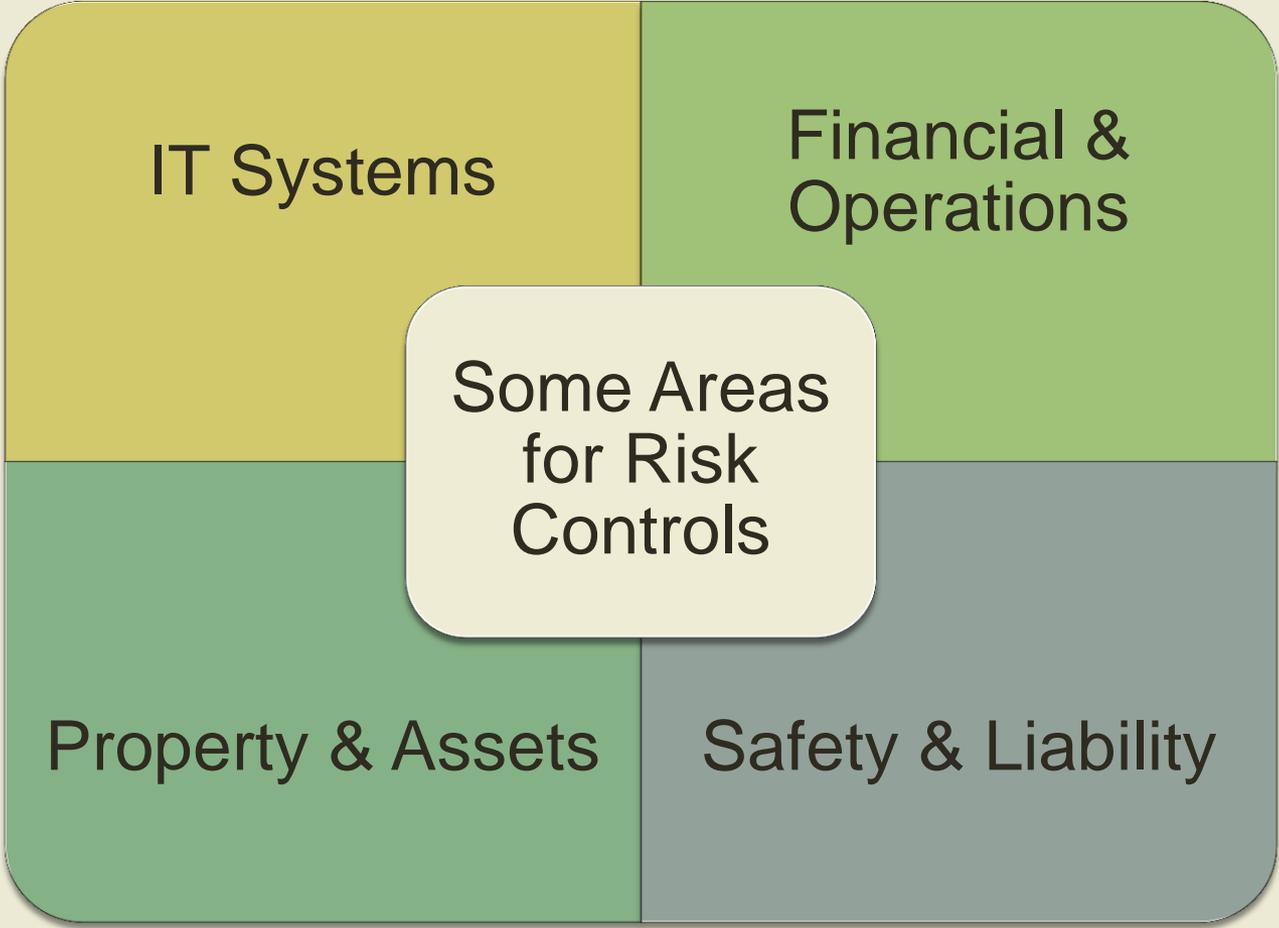
- Focus is to establish ERM goals as part of the strategic management process. It does not dive into the details of risk management approaches and process, but addresses threats to the organization and the need for proper controls.

ISO 31000

- Rooted in risk management principles and designed to provide an organized methodology to evaluate risk exposures and react to the environment.

Risk Controls

Management is responsible for implementing appropriate controls to reduce risk and to achieve operational objectives.



Risk Champions and Risk Centers

Risk Champions

- Accountable for ensuring accuracy within their department or business unit around the identification, assessment, management and monitoring of risk
- They are the eyes and ears of risk information for the risk manager who is in charge of assessing risk across the enterprise
- Not necessarily responsible for performing the actual risk management activities

Risk Center

- A department or unit within the organization charged with the risk exposures that are related to their duties and responsibilities

Intuit Case Study

4
Implementation

“When we talk about growth strategies for the company, we talk deliberately about both risks and opportunities”

Janet Nasburg,
Chief Risk Officer
at Intuit

CRO and ERM program office have ownership and accountability for Intuit’s ERM program and drive Intuit’s ERM capabilities

Ownership and accountability for identified risks are shared by executive and business unit level leaders

Risk communication is not only to report progress, but also so that business units can share and leverage risk knowledge

intuit

Risk Communication Structure

4
Implementation

Simple State System

The event can be resolved through routine decisions

Complicated State System

The event is more difficult to resolve than a simple system, but it not unusual

Complex State System

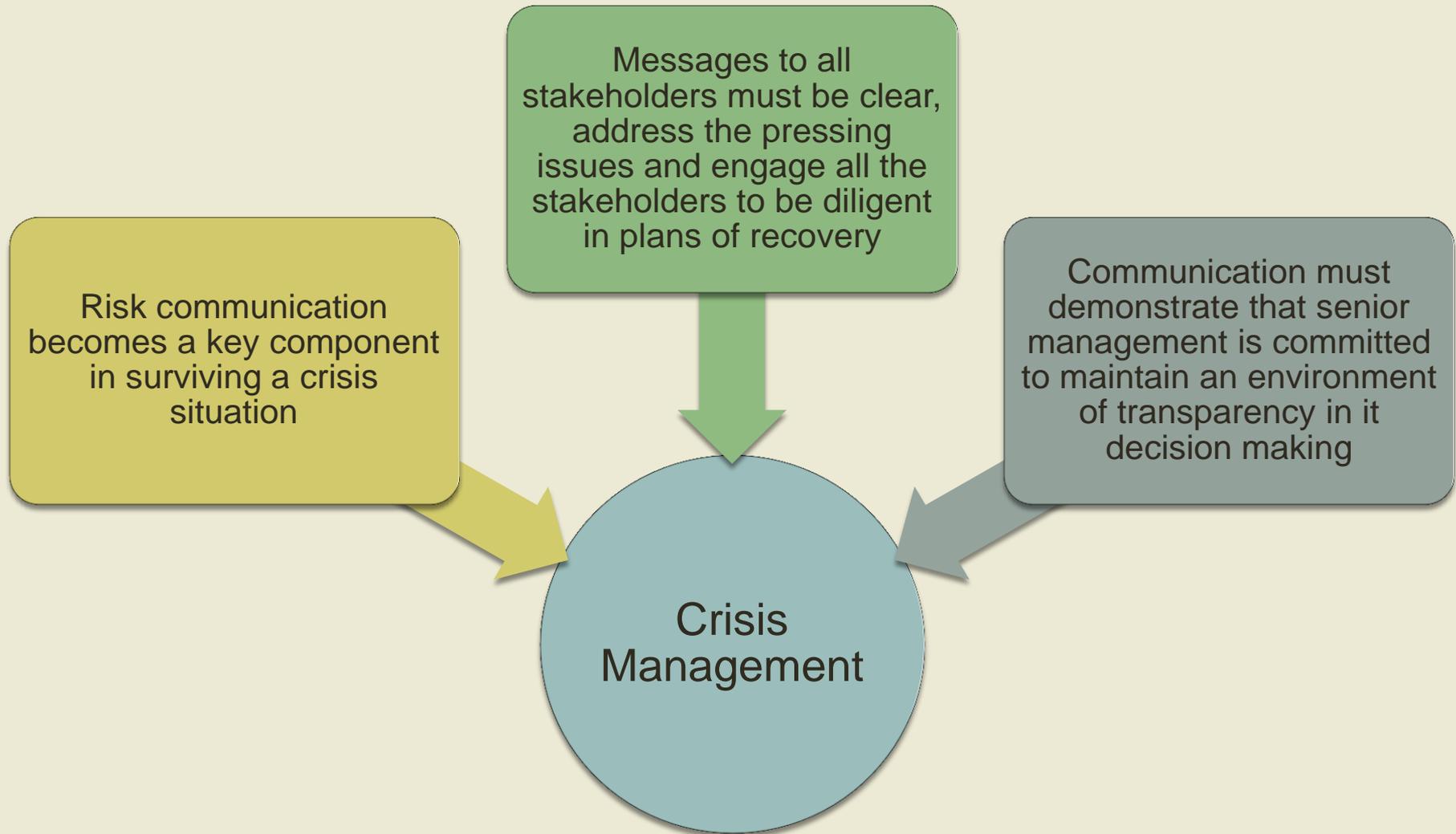
The event is unusual, and potentially critical to the organization

Chaotic State System

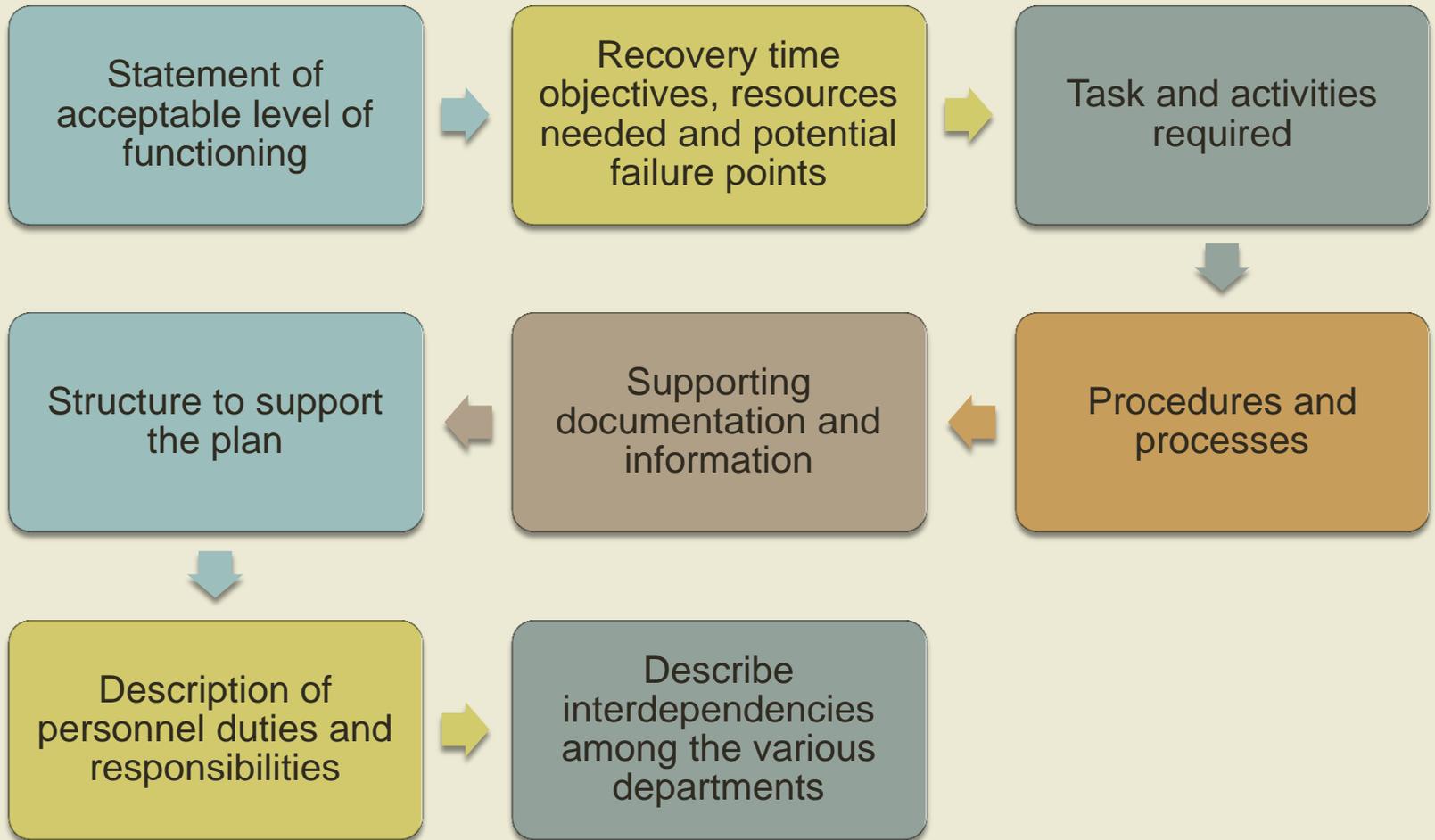
The event is a dramatic, unforeseen situation that threatens the organization's survival

Crisis Management

4
Implementation



Elements of Continuity Plan



5. Monitoring

Monitoring involves communication of risk both upstream and downstream across the organization. It includes periodic reporting and follow-up on the risks by various levels of management, risk committees, and internal auditors

KPIs and KRIs are a valuable way to monitor key risks linked to improved cash flows and earnings

Tools Used for Monitoring

5
Monitoring

Spreadsheets

Like risk registers

Balanced Scorecards

Captures company's strategy by

- Customer
- Internal Processes
- Innovation and Learning
- Financial

Dashboards

Pictorial reporting of risks

Governance Risk and Compliance Software

Focus on audit and compliance

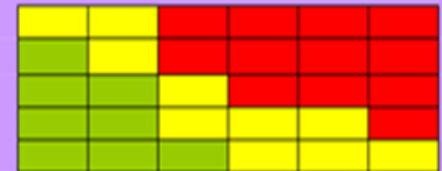
Enterprise Risk Management Software

ERM focus on software solutions

Critical Risk: Mitigation Plan

Critical Risk: Mitigation Plan

Project name				Project Impact Phase	
RISK Identified by		PM		Impact/Trigger Date	
Risk type/source		Risk Coordinator			
Risk No.		Risk owner		Max Cost	
Open date		Risk Score		Min Cost	
Risk Statement	(3 C's format - Condition, Cause, Consequence)			Most likely Cost	
Closure Criteria/ Closure Statement		Closure Date			
				Change Control Approved	Yes or No (circle one)
Mitigation action (Preventive)	Actionee	Action Deadline date	Action Deadline phase	Use the chart below to show the risk score before and after mitigation	
Contingency action					



Case Study: Walmart

Developed KPI and KRI metrics incorporated in a balanced scorecard.



Metrics used to track performance on risk and to determine the company's progress in managing the risk.



Walmart also uses these metrics to determine the value added by the ERM process.

KPI Selector				
	Metric #1 Reduce supply chain response time	Metric #2 Improve visibility of products in pipeline	Metric #3 Increase employee productivity	Metric #4 Reduce product shrinkage
Characteristic	Response Time Metric	Visibility Metric	Productivity Metric	Shrinkage Metric
Strategic value driver	x	function driven	x	function driven
Executive defined	x	function defined	x	function defined
Organization cascade	x	no	x	no
Enterprise standard	x	function specific	x	function specific
Quantifiable metric	x	x	x	x
Based on valid data	x	x	x	x
Easy to comprehend	x	x	x	x
Relevant over time	x	x	x	x
Provide context	x	x	x	x
Empower user	x	x	x	x
Promote positive action	x	x	x	x
KPI Status	KPI	Metric	KPI	Metric



6. Evaluation

6

Evaluation

Ascertaining the strengths and weaknesses of the ERM program with regard to the organization's strategic goals

Risk Optimization / Value Creation

Evaluation

Return on Investment

ERM's Role in Governance

Risk Optimization

6

Evaluation

Balance between taking on too much risk and not taking on enough risk to explore opportunities for growth

Explore various risk-return outcomes

Evaluate risk controls in place and decide the best use of financial resources to provide needed protection

Cost of Risk

6

Evaluation



Each year University of California holds an Annual ERM Summit focused on their continuous effort in improving their ERM program by reducing their Cost of Risk.

Case Study: University of California

Since 2003-2004 fiscal year, they have reduced Cost of Risk by \$493 million dollars

Reduced the Cost of Risk from \$18.46 per \$1,000 of operating budget to \$13.31 per \$1,000 of operating budget

Risk Governance

6

Evaluation

Key drivers of success and risks in the company's strategy

Crafting the right relationship between the board and its standing committees as to risk oversight

Establishing and providing appropriate resources to support risk management systems

Monitoring potential risks in the company's culture and incentive systems

Developing an effective risk dialogue with management

Guidance principles for board risk oversight

National Association of Corporate Directors
report, "Risk Governance: Balancing Risk and Reward"

Executive Risk Committee

The Executive Risk Committee Provides the Board of Directors with:



A structure that provides the board with the appropriate information that defines the firm's risk profile



A system that provides an audit of the effectiveness of the risk management process



A system that affords an evolving understanding of key risks to the company

“Boards are now finally asking management about the nature of the risk information process in place. Boards want to gather information about new or emerging risks and the extent to which these risks require a more in-depth analysis. This is being done to ensure future opportunities and threats to the company's performance are appropriately managed”.- John Bugalla, James Kallman, Chris Mandel and Kristina Narvaez in *The Corporate Board*

Thank you. Questions?

Presented by
Kristina Narvaez
President & CEO
ERM Strategies
www.erm-strategies.com