Risk Management

Paul Dagger & Kris Bubendorfer

ENGR 401 Professional Practice

Life is Inherently Risky (whether professional or personal)

- *I get out of bed …. and the cat doesn't trip me up*
- *I start the car … and it doesn't explode*
- *I drive into the office … and no one crashes into me*
- *I go up the elevator … which doesn't fall to bottom of the lift shaft*
- *I make my cup of tea … and the milk doesn't poison me*
- *I head back to the house … pleasantly surprised I didn't spontaneously combust*

Life is Inherently Risky (whether professional or personal)

Life is Inherently Risky (whether professional or personal)

- We all encounter risk every day
- Most people already understand the general concept of “risk”
- Most people already have approaches for managing risk
  - *Civil Defence kits of canned food and fresh water*
  - *Wearing seatbelts*
  - *Paying for insurance we hope will never be needed*

Risk Management – Learning to Identify & Accepting Risk

- Its inevitable that you may choose to accept some degree of risk.
- You need to be able to identify and properly define the risk in order for you or someone else to accept it from an informed position.
- Risk Management is a formalised approach to defining and classifying risk
- You may choose to try and do something to treat and reduce a risk …..
- …. But its entirely OK to do nothing and just accept a risk once you understand what you are accepting.

Overview

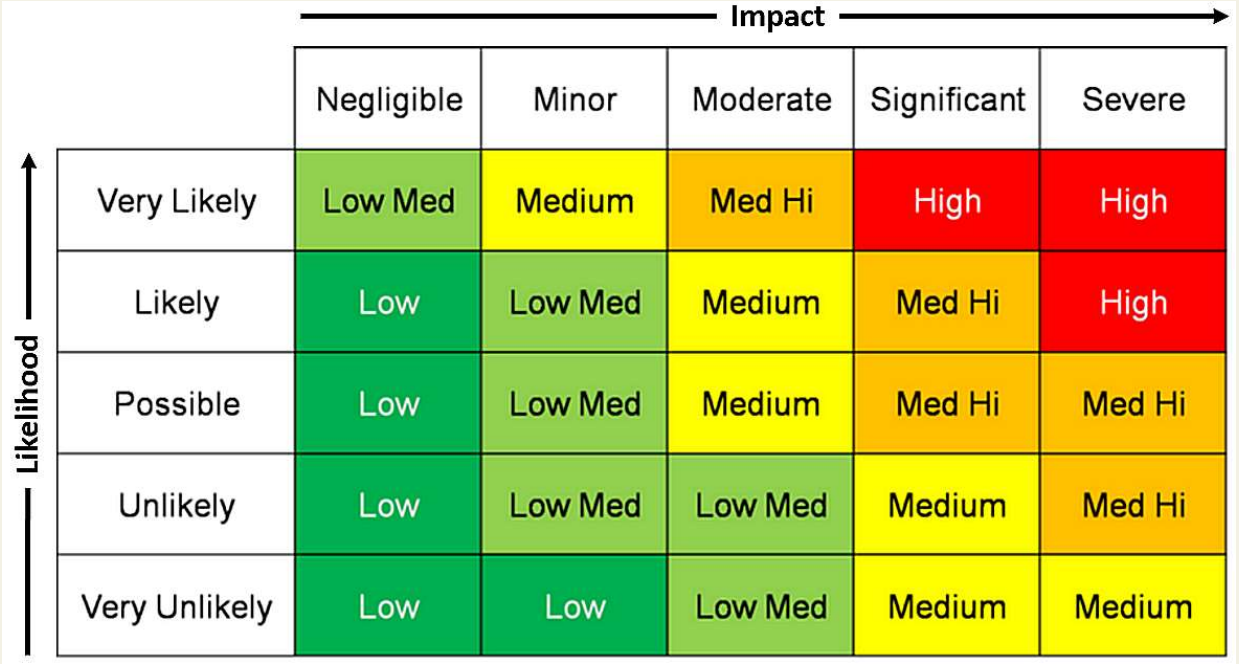
- Fundamentals of Risk
  - *Hazard, Likelihood, Impact, Treatment*
  - *Importance of regular risk re-evaluation*
- Differing Views of Risk
  - *Business Continuity Planning / Management*
  - *Enterprise Risk*
  - *Health & Safety Risk*
- Core Concepts of Risk Management

Fundamentals of Risk || Hazard, Likelihood, Impact, and Treatment

- Risks are caused by Hazards – *'There is a live sparking wire hanging in front of the doorway'*
- Risks are defined by two independent factors
  - *Impact – What is the bad outcome that potentially could happen?*
  - *Likelihood – What is the probability that the bad outcome is going to happen?*
- Each of the two aspects are normally assigned relative ratings for comparison
  - *Risk of spontaneous human combustion – 'Very Unlikely' / 'Extreme Impact'*
  - *Risk of the office milk being rancid – 'Possible' / 'Low Impact'*
  - *Risk of Paul paying for coffee at next PhD meeting – 'Definite' / 'Very Low Impact'*

Fundamentals of Risk || Likelihood, Impact, and Treatment

- Risk Matrix
  - *Normally organisational specific*
  - *Defines the range of Likelihood and Impacts*
  - *Combines to give Risk an overall classification to help guide treatment*
  - *E.g. – High & Very High risks must be treated*



https://2.bp.blogspot.com/-McErl5J1EK0/Vd3bB1Jg5GI/AAAAAAAAHwg/w-7KoUDzmyc/s1600/Typical%2BRisk%2BMatrix.png

Fundamentals of Risk || Likelihood, Impact, and Treatment

- Risk Treatments are the mitigation plans or steps put in place to reduce the Impact or reduce the Likelihood.
  - Risks before treatment are described as “Raw Risk”
  - Risks after treatment are described as “Residual Risk”
- Raw Risk Summary
  - *“The milk may be rancid and make Paul sick” / **“Likely”** / “Severe”*
- Risk Treatment & Residual Risk
  - *“Kris will check the milk every morning and tip out rancid milk” / **“Very unlikely”** / “Severe”*

Fundamentals of Risk || The Importance of Regular Risk Re-evaluation

- Conditions may change the Impact or Likelihood of Risks over time
  - *The wood on the bridge slowly rots, increasing the Likelihood of collapse*

https://youtu.be/uYufFUuTxMA

Differing Views of Risk || Business Continuity Planning/Management

- Business Continuity Planning is how to ensure business processes continue despite impacts of risks.
- Business Continuity Planning IS NOT the same as IT Disaster Recovery
  - *Its what the **business does** to handle when **IT fails** or is being repaired*
  - *Example – When the mainframe at a bank failed, the Bank ATMs would automatically hand out up to $800 whether you had it or not, as would the tellers. The tellers would write deposits and transfers in a book and enter them when the mainframe came back up.*
  - *The untreated risk impact of the mainframe going offline is the Bank couldn't provide any services to the customers. The likelihood of this was low, but the impact was unacceptably high (potentially also in breach of banking legislation).*
  - *The treatment of handing out up to $800 regardless of whether the customer had it or not left a residual risk of debt collection or having to write it off (which was an acceptable impact)*

Differing Views of Risk || Enterprise Risk

- A structured organisation wide review of serious risks the organisation is exposed to
  - *Financial Risk*
  - *Security Risk*
  - *Legal & Compliance Risk*
  - *Operational Risks*
- Ensures Senior leaders hold a common unified view of risks and treatment decisions
- Avoids risks that could bring down the organisation being lost within departmental ‘silos’

Differing Views of Risk || Health & Safety Risk

- Risks involving the health and safety of your workers, customers, and the public
- Risks that may be created by the work your organisation is carrying out
  - *Heavy machinery digging deep holes that are filled with explosives*
- Risks that may be created by your staff and customers being in your offices
  - *Someone spills their cup of tea on the kitchen floor just before a person running with scissors sprints through the puddle toward a customer*
- Like many areas of risk, there is specific legislation that every organisation needs to be aware of regarding Workplace Health & Safety - https://www.worksafe.govt.nz/

Differing Views of Risk || Operational Change Control

- Part of making changes to existing systems normally involves completing ‘Change Control’ that gets formally assessed and approved.
- Major part of a ‘Change Control’ involves explaining what you plan to do, how you plan to do it, and seeking peer review for errors in your plan.
- Another key purpose is to communicate the risks associated with your change
  - *What could be the worst-case outcome if your change goes wrong?*
- Communicating this clearly is important to allow others to potentially prepare for the worst case.
- *“You only need a change control for a failed change” – My Lead Engineer Mentor*

Core Concepts of Risk Management || Your Thought Processes

- Be proactive in seeking and communicating risks to appropriate risk owners
  - *Adopt a risk seeking mindset*
  - *If someone else has accepted ownership of the risk, you aren't responsible for it anymore*
  - *"Crying Wolf" is normally not the way people think about risk management. There is nothing wrong with erring on the side of caution*
  - *Telling someone about a risk is not the same as them confirming they are now taking ownership of the risk*
- Have a documented and agreed process, and ensure people are aware of it and their obligations
- Don't be scared to put down "High-Severity" / "Very Low Probability" risks
  - *They may not ever happen, but if they do then its better you have a plan*

Core Concepts of Risk Management || Common Stages

- Stage 1 - Hazard & Risk Identification
  - *What hazards exist and how could they lead to risks?*
- Stage 2 - Risk Assessment
  - *What is the Likelihood & Impact, and what category of risk (finance, HR, etc)*
- Stage 3 - Risk Response
  - *What treatment is applied, and then what is the residual risk*
  - *Avoid the risk? Reduce the risk? Share a risk (e.g. – insurance)? Accept the risk?*
- Stage 4 - Monitor the Risk ongoing

Real World Example - Knight Capital Group || The Ask

- Imagine that you are from another Capital Group – *"Dagger Rocks Capital"*
- Your handsome, talented, amazing, and forward-thinking management has asked you to look into what happened at Knight Capital.
- The ask is to identify what risks that organisation didn't think about so your employer can learn from their mistakes.
- While you are watching this video make notes covering:
  - *Hazard, Risk Impact & Likelihood, Area of Risk (financial, compliance, etc)*
  - *Response or Treatment, Residual Risk Impact & Likelihood*

Real World Example - Knight Capital Group || Lets Watch

https://www.youtube.com/watch?v=263CooDJZCY

Real World Example - Knight Capital Group || Suggested Answers

- The following are a subset of potential answers, also only my potential answers
  - *Risk Assessment and Management is never an absolutely precise science*
  - *Remember that once potential risks are identified, the next step is to review and validate them (often in a group, agreeing risks and ratings), then determine treatment.*
  - *There will no doubt be more, you may have some of the same but have different ratings – this is all absolutely fine and correct.*
- I've listed almost the same risk multiple times in some cases, the scenario being the same and only the outcome different – thereby different consequences.
  - *Its better to start with a larger set of potential risks, then with stakeholders decide which to keep versus, which can be summarised, or which are ostensibly duplicates.*

Real World Example - Knight Capital Group || Suggested Answers

- Business Continuity – Key executive staff unavailable during product launches delays response and affects service or profit – Possible / Significant
- Tech DR – Lack of regular testing of technical DR plans (e.g. – “kill switch” activation”) affects business continuity in event of major incidents – Very Likely / Significant *(Very likely as the video proved they hadn’t done technical DR testing)*
- Compliance – Knight Capital technology systems and policies non-compliance with regulator policies may affect regulator support during crisis events – Very Likely / Significant
- Compliance – Knight Capital technology systems and policies non-compliance with regulator policies may incur fine, deregistration, or other regulator penalties - Likely / Moderate *(we will assume the regulator wouldn’t ‘bar them’ but may impose fines)*
- IT Change Management – Lack of formal change management process for modifications to key business applications allows unexpected, unsupported, or incorrect system changes that render Knight Capital unable to trade – Unlikely / Significant
- IT Change Management – Lack of formal change management process for modifications to key business applications allows unexpected, unsupported, or incorrect system changes that cause outages that affects service or profit – Unlikely / Moderate
- IT Change Management – Lack of formal change management processes for modifications to key business applications allows unexpected, unsupported, or incorrect system changes that cause customer confusion and negative perception of Knight Capital – Unlikely / Minor

Real World Example - Knight Capital Group || Suggested Answers

- Health & Safety – Inadequate project planning results in compressed delivery timelines which overwork staff and cause mental health or physical injury – Possible / Moderate
- Health & Safety – Inadequate project planning results in compressed delivery timelines which due to overworked staff introduces errors into key business applications that destroy Knight Capital financial stability – Possible / Severe
- Enterprise Risk – Lack of safety checks to match trades against available capital may cause Knight Capital automated trading to bankrupt the company in the event of coding error or malicious actor – Possible / Severe
- Technology – Incomplete business application performance and functional monitoring delays resolution of business impacting errors or outages to core financial systems – Likely / Severe
- Technology – Poor source-code version control and application development standard results in software development errors introducing business impacting errors or outages to core financial systems – Possible / Severe
- Technology – Incorrect error handling may allow error messages that should only occur in test environments to fail to trigger appropriate escalation if seen in PROD (indicating release management issues) – Unlikely / Moderate