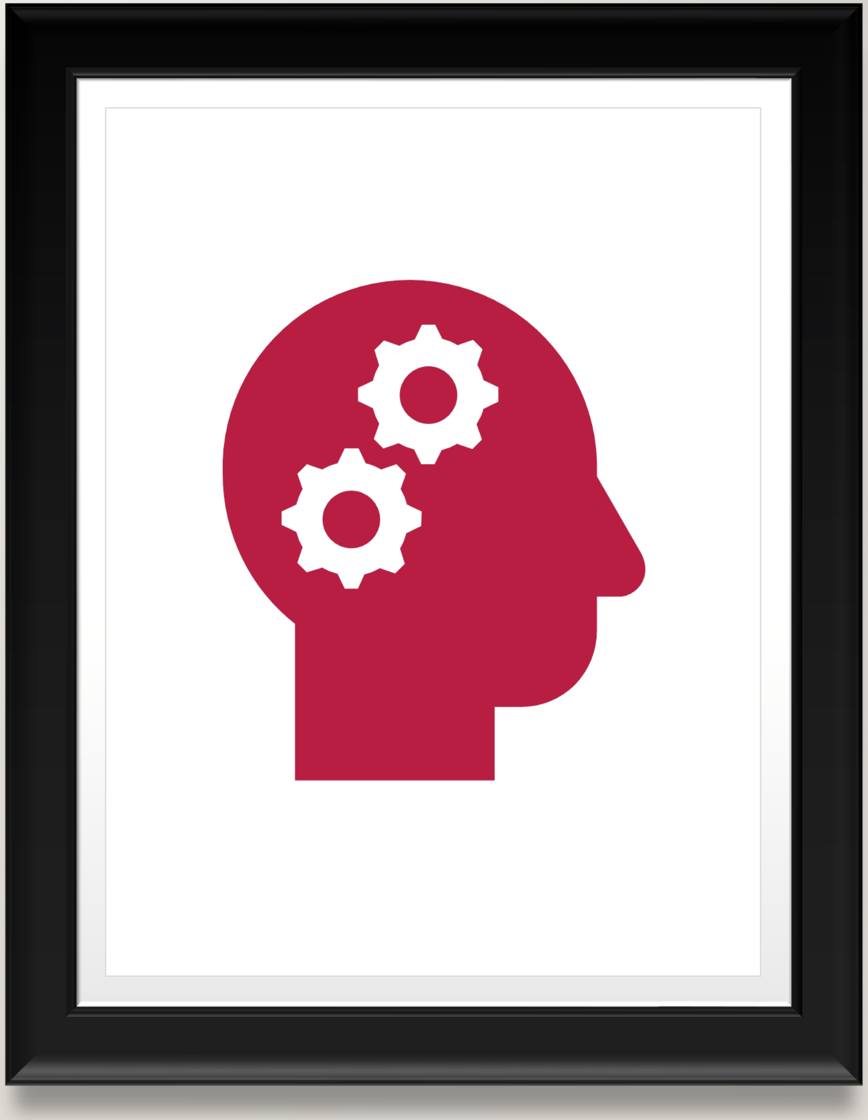
INTERSECTIONS OF RESILIENCE



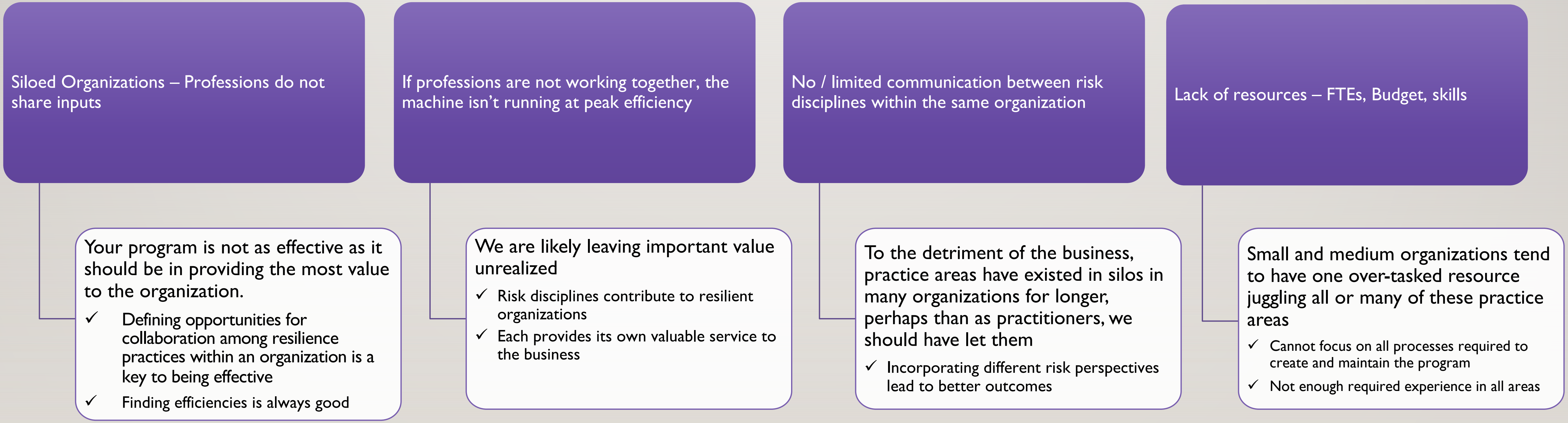
INTRODUCTIONS

DEFINING RESILIENCE

1. The capacity to recover quickly from difficulties; toughness
2. The ability of a substance or object to spring back into shape; elasticity

The ability to prepare for and adapt to changing conditions and recover rapidly from operational disruptions. Resilience includes the ability to withstand and recover from deliberate attacks, accidents, or naturally occurring threats or incidents. - DRI Glossary

THE PROBLEM(S)



Siloed Organizations – Professions do not share inputs

Your program is not as effective as it should be in providing the most value to the organization.

- ✓ Defining opportunities for collaboration among resilience practices within an organization is a key to being effective
- ✓ Finding efficiencies is always good

If professions are not working together, the machine isn’t running at peak efficiency

We are likely leaving important value unrealized

- ✓ Risk disciplines contribute to resilient organizations
- ✓ Each provides its own valuable service to the business

No / limited communication between risk disciplines within the same organization

To the detriment of the business, practice areas have existed in silos in many organizations for longer, perhaps than as practitioners, we should have let them

- ✓ Incorporating different risk perspectives lead to better outcomes

Lack of resources – FTEs, Budget, skills

Small and medium organizations tend to have one over-tasked resource juggling all or many of these practice areas

- ✓ Cannot focus on all processes required to create and maintain the program
- ✓ Not enough required experience in all areas

RESILIENCE PRACTICE AREAS

- Business Continuity / Disaster Recovery (BCDR)
- Enterprise Risk Management (ERM)
- Operational Risk Management (ORM)
- Security (Cyber & Facility)
- Emergency Management (EM)
- Occupational Health & Safety (OH&S)

SILOS IN RESILIENCE

Organisational Silos
EM
BC/DR
ERM
ETC.

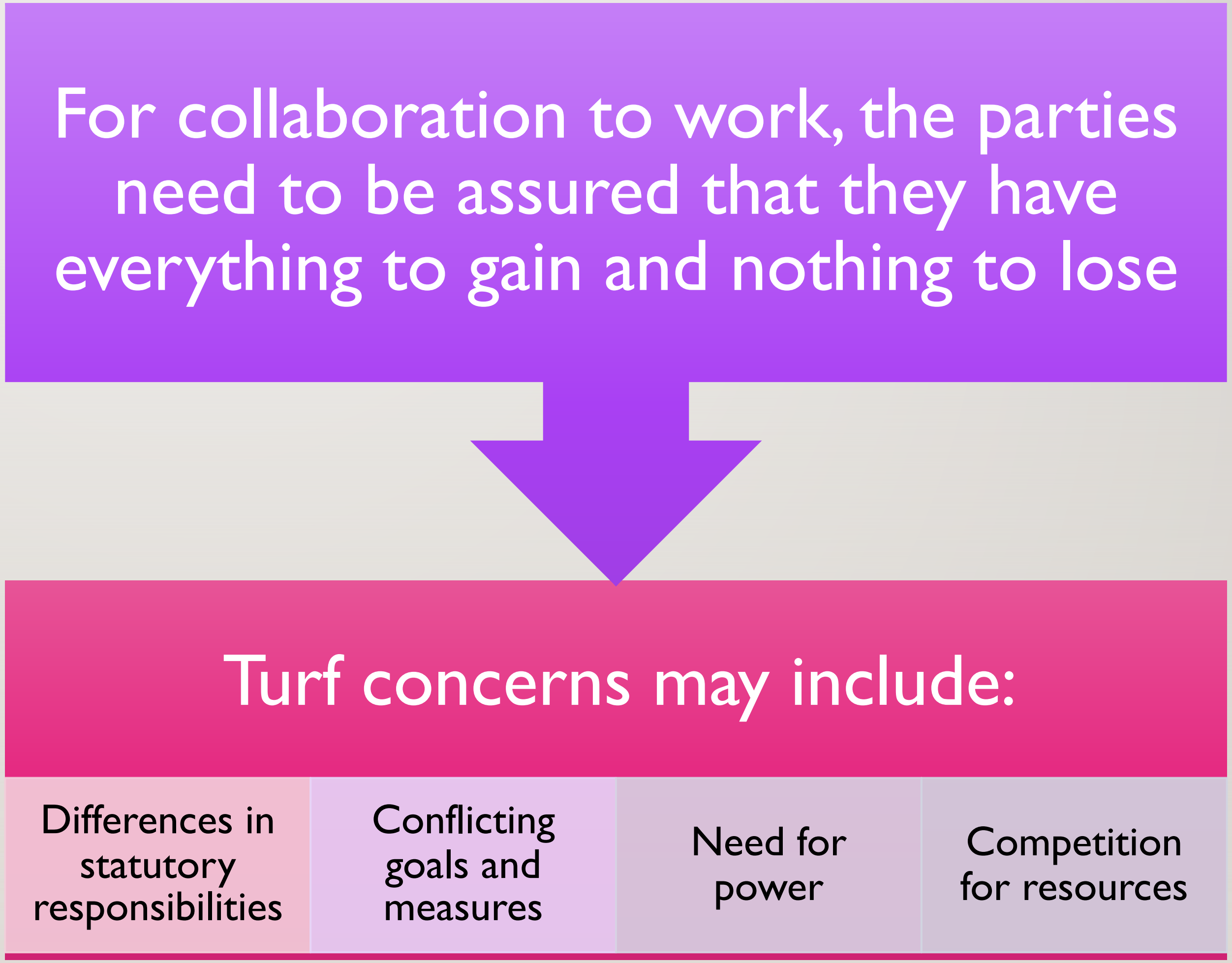
ROOT CAUSE ANALYSIS OF RESILIENCE SILOS

- In some practice areas, the problem starts right from the outset
  - No standardized curriculum in colleges or universities around BCDR
  - Courses typically offered as introductory courses as part of an EM degree or as certificates, not majors
  - Many courses assume, or require, a level of advanced knowledge
- Resilience Professions often don't understand their counterparts which leads to silos
  - Not enough understanding of the unique perspectives & contributions of various risk disciplines

MISTRUST

- Mistrust of fellow team members can get in the way of collaboration
- Mistrust can have a variety of causes, such as:
  - Different rules, organizational cultures, and values
  - Using different terminology
  - Unfamiliarity or lack of prior relationships among key players
  - Withholding information
  - Budget/Resource concerns
  - Internal corporate politics

TERRITORY CONCERNS



For collaboration to work, the parties need to be assured that they have everything to gain and nothing to lose

Turf concerns may include:

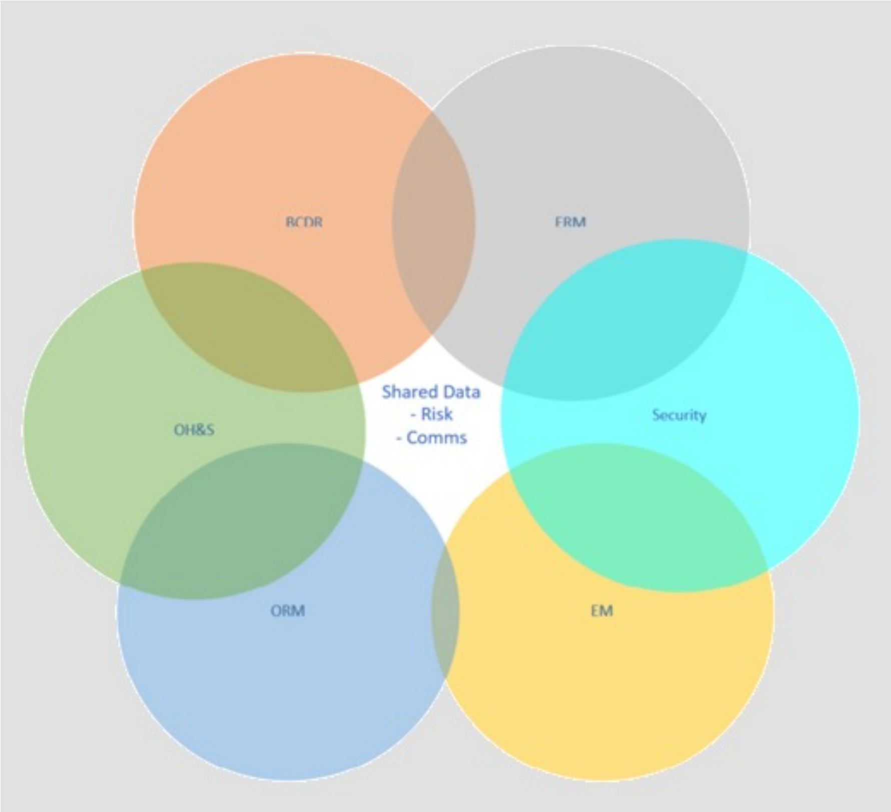
- Differences in statutory responsibilities
- Conflicting goals and measures
- Need for power
- Competition for resources

WHY FORM A COLLABORATIVE TEAM?

- People working together accomplish more than individuals working separately. Or as the author Ken Blanchard put it, “None of us is as smart as all of us.”
    - Significant results can be achieved through collaboration; the process of shared creation that occurs when people produce something by:
        - Combining efforts
        - Sharing ownership of the outcome
        - Making joint decisions
        - Exchanging expertise, information, and resources
        - There is nothing routine about this process. When collaboration occurs, something is there that wasn’t there before

PRACTICE AREA FUNCTIONS

	Disaster Recovery	Business Continuity	Enterprise Risk Management & Other Second Line	Emergency Management	Security	Operational Risk Management	OH&S
Functions	IT continuity	Business process resilience	Privacy	Life safety	Crisis Response & Management	Risk Identification	Life safety
	Information leakage and handling	Risk assessment & management	Strategic corporate planning	Major crisis	Threat & Risk Assessment	Risk Assessment	Pandemic/Infection awareness and procedures
	Cyber-threats	Advance planning completed prior to crisis events	Inputs into Internal audit	Vulnerability management	Mitigation	Measurement & Mitigation	Maintenance and promotion of workers’ health and working capacity
	Identification of efficiencies in IT operations	Business Impact Analysis. Defines critical processes to plan, resource, educate, and audit	Compliance & Ethics	Asset protection	Cyber-threat identification	Monitoring & Reporting	Improvement of working environment and work to become conducive to safety and health
	Definition and management of data	Business process continuity planning focused on stakeholder impact	Accounting / Financial compliance	Environmental protection	Physical safety & security		Development of work organizations and working cultures in a direction which supports health and safety at work
	Documentation of systems and network infrastructure / topology	Pandemic planning	Insurance	Crisis management			Identification of workplace hazards
	IT systems/data security	Crisis Management & Communication (Some will state this is a discipline of its own)	Credit	Risk Assessment (All Hazards)			Risk / Threat assessment and management
	Risk / Threat assessment	Alternate site planning	Risk assessment & management				



COMMONALITIES (CORE FUNCTIONS)

- Let's call certain functions, core, as they overlap between all resilience practices
  - Risk identification & management
  - Compliance to published/recognized standards
  - Audit of programs/plans, etc.
- Rather than identify who "owns" what, perhaps we can find a way to agree on how to share responsibility for the various resilience functions and allow the program to benefit from seeing all sides of the process
  - ✓ Incorporating different risk perspectives lead to better outcomes

HOW DOES THIS WORK FOR OUR INDUSTRY

COMMON DATA

- All resilience professions use common threat / risk data, and it makes sense to share this
  - Risk registers must be aligned
- Business functions

PLANS WHICH SHARE RESPONSES

- Incident Response / Management
- Crisis Management
- Communications
- Facility
- Etc.

COMMON FRAMEWORK

In IT, "A software framework provides a standard way to build and deploy applications. A software framework is a universal, reusable, software environment that provides functionality as part of a larger software platform to facilitate development of software applications, products, and solutions.“

https://en.wikipedia.org/wiki/Software_framework

SHARED DATA

- Business Functions
  - All practice areas require an understanding of the functions that the organization's business units perform, the most complete documentation of these functions is developed during the BIA and should be shared with all practice areas
- Risk
  - The impact may affect one practice area more than another, but the threats / risks for the organization are still the same
  - Rather than having 7 different risk assessment processes, which may provide different outputs, and create confusion, in addition to costing far more to produce, we have one set of clean data outputs that all can draw from
  - From there, specific discipline mitigation/treatment/transfer may vary, but the starting data to operate from will be richer

SHARED PLANS

- We do not require different plans from BCDR, EM, Security, or OH&S, for the same threats
  - Evacuating a building for a flood, fire, explosion, or gas leak is evacuating a building, regardless of the threat which is driving the response
  - These plans should be developed as a Resilience group and shared with the organization
    - Not separate plans from EM, BCDR, OH&S, etc. for the same outcome
    - Plans would include specific discipline roles or skills where required
- Communications
  - All resilience practitioners require internal and external communication, with one another and with stakeholders
  - In our experience, utilizing your communications dept (or HR if no formal communications dept exists) is the best way to ensure concise, accurate messaging and sharing this rather than having several different types of messaging is critical
- Incident / Crisis response & management
  - A collaborative approach (such as Incident Command System (ICS) or Ontario's Incident Management System (IMS)) is a good starting point to develop your framework
  - Standards (such as NIST) provide a great approach to cyber threats
- ERM and ORM do not have 'plans' as such
  - Every practice area has its own processes that make it distinct from the others, but we should focus on the common areas

STARTING POINT

- Risk
  - The one area we can all agree that the various practice areas share common ground is Threat / Risk
    - How we utilize this data (how we treat the risk) varies between each discipline, but the threats and risks for the organization should be the focus
  - This is where we should begin to align our organizational resilience
    - The following slides outline the risk register process, and we'll discuss, with audience participation, on how we could integrate this into the various disciplines

ARE RISK REGISTERS NECESSARY?

Standard Reasons;

- Provides a baseline
- Documents real or perceived risks to help ground alignment
- Helps track compliance
- Enables better communication
- Allows evaluation of risk for better treatment decision for each discipline

The question for debate:

- *Does the perspective from each discipline add value?*

A NEUTRAL PERSPECTIVE?

Full PMBOK Definition on Risk Register

“The risk register captures details of identified individual project risks. The results of Perform Qualitative Risk Analysis, Plan Risk Responses, Implement Risk Responses, and Monitor Risks are recorded in the risk register as those processes are conducted throughout the project. The risk register may contain limited or extensive risk information depending on project variables such as size and complexity.”

11.2.3.1 PMBOK

HOW TO CREATE A RISK REGISTER

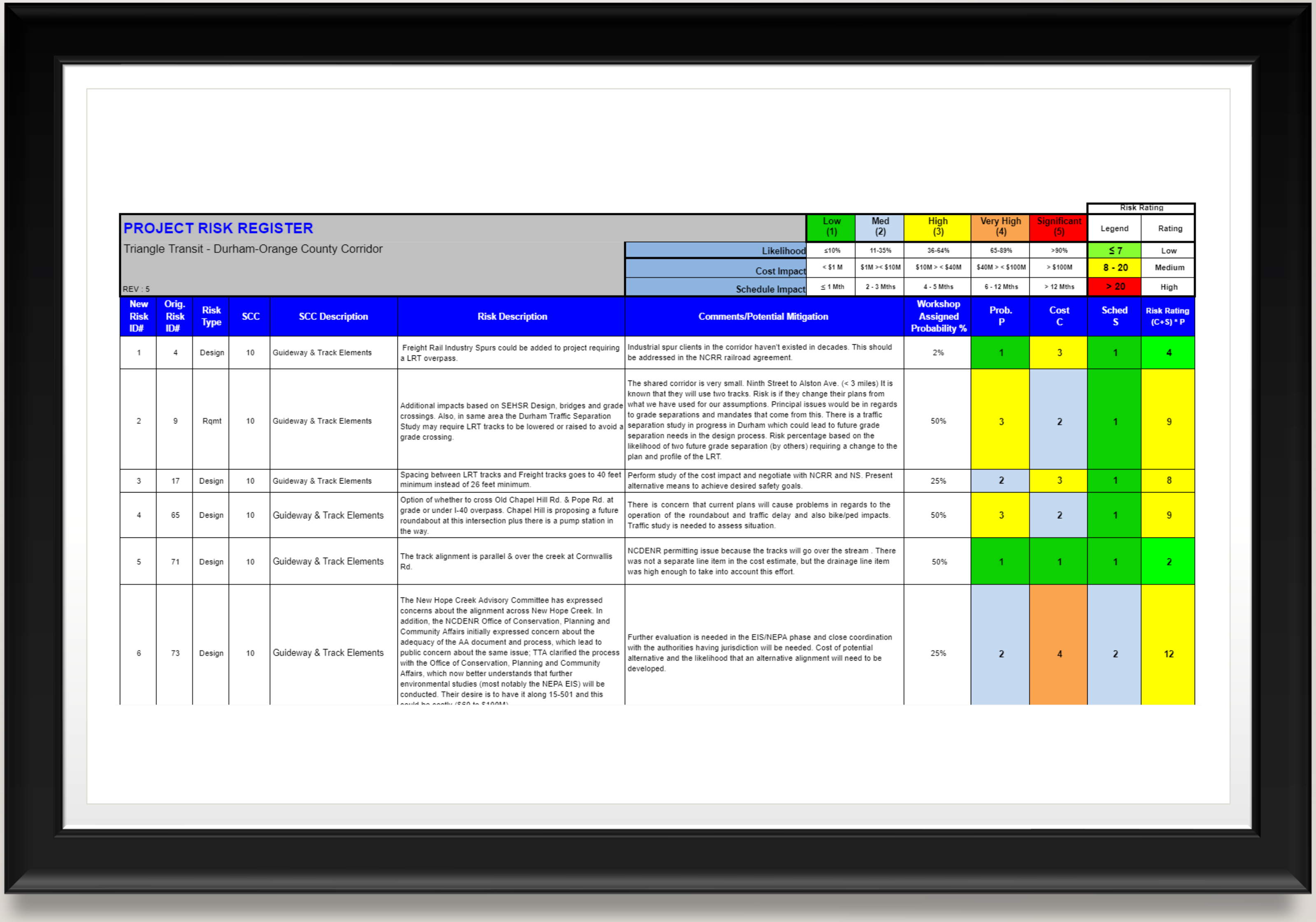
“Because risks change throughout the course of a project, a risk register is a *dynamic* document. Project and team leaders must continually evaluate total risk to adapt their register to the circumstances of each stage of a project.

At minimum, your risk register should have the following elements:

- a way to quickly identify each risk, such as an ID number
- a description of each risk
- a *breakdown structure* allowing you to sort risks into categories
- a space to list each risk’s probability of occurring using numerical or qualitative rankings
- a *priority score,* which is equal to the qualitative impact of the risk times its probability
- a list of mitigation steps, usually copied from a separate document
- a list of *risk owners*, who execute and oversee mitigation steps for a single risk”

Source: https://pm-training.net/risk-register-template/

SAMPLE PROJECT MANAGEMENT RISK REGISTER



PROJECT RISK REGISTER

Triangle Transit - Durham-Orange County Corridor

REV : 5

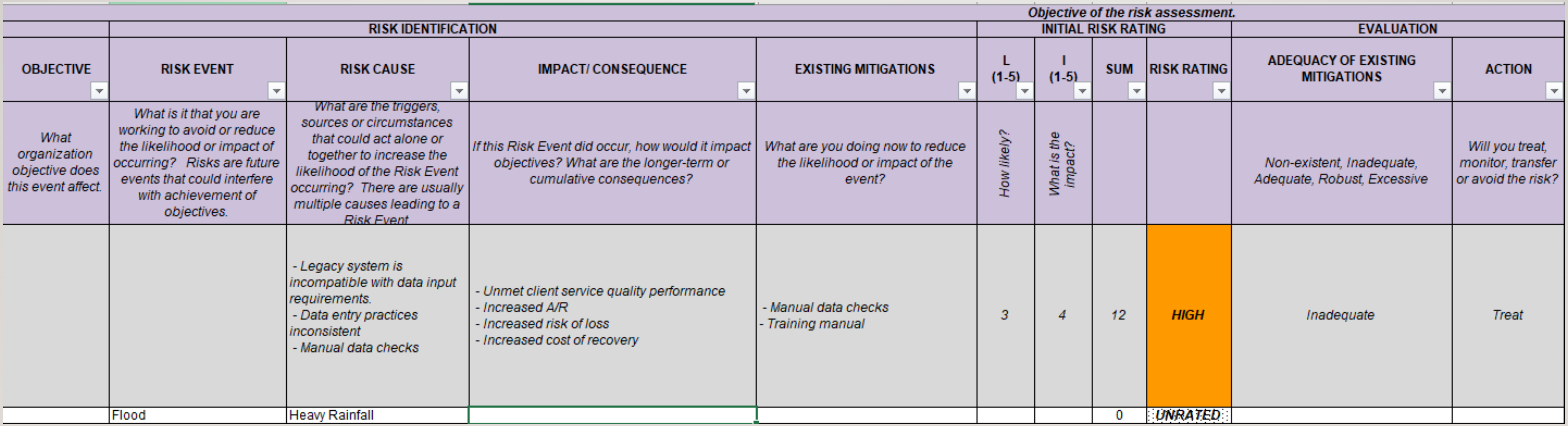
	Low (1)	Med (2)	High (3)	Very High (4)	Significant (5)	Risk Rating	
						Legend	Rating
Likelihood	≤10%	11-35%	36-64%	65-89%	>90%	≤ 7	Low
Cost Impact	< $1 M	$1M >< $10M	$10M > < $40M	$40M > < $100M	> $100M	8 - 20	Medium
Schedule Impact	≤ 1 Mth	2 - 3 Mths	4 - 5 Mths	6 - 12 Mths	> 12 Mths	> 20	High

New Risk ID#	Orig. Risk ID#	Risk Type	SCC	SCC Description	Risk Description	Comments/Potential Mitigation	Workshop Assigned Probability %	Prob. P	Cost C	Sched S	Risk Rating (C+S) * P
1	4	Design	10	Guideway & Track Elements	Freight Rail Industry Spurs could be added to project requiring a LRT overpass.	Industrial spur clients in the corridor haven't existed in decades. This should be addressed in the NCRR railroad agreement.	2%	1	3	1	4
2	9	Rqmt	10	Guideway & Track Elements	Additional impacts based on SEHSR Design, bridges and grade crossings. Also, in same area the Durham Traffic Separation Study may require LRT tracks to be lowered or raised to avoid a grade crossing.	The shared corridor is very small. Ninth Street to Alston Ave. (< 3 miles) It is known that they will use two tracks. Risk is if they change their plans from what we have used for our assumptions. Principal issues would be in regards to grade separations and mandates that come from this. There is a traffic separation study in progress in Durham which could lead to future grade separation needs in the design process. Risk percentage based on the likelihood of two future grade separation (by others) requiring a change to the plan and profile of the LRT.	50%	3	2	1	9
3	17	Design	10	Guideway & Track Elements	Spacing between LRT tracks and Freight tracks goes to 40 feet minimum instead of 26 feet minimum.	Perform study of the cost impact and negotiate with NCRR and NS. Present alternative means to achieve desired safety goals.	25%	2	3	1	8
4	65	Design	10	Guideway & Track Elements	Option of whether to cross Old Chapel Hill Rd. & Pope Rd. at grade or under I-40 overpass. Chapel Hill is proposing a future roundabout at this intersection plus there is a pump station in the way.	There is concern that current plans will cause problems in regards to the operation of the roundabout and traffic delay and also bike/ped impacts. Traffic study is needed to assess situation.	50%	3	2	1	9
5	71	Design	10	Guideway & Track Elements	The track alignment is parallel & over the creek at Cornwallis Rd.	NCDENR permitting issue because the tracks will go over the stream . There was not a separate line item in the cost estimate, but the drainage line item was high enough to take into account this effort.	50%	1	1	1	2
6	73	Design	10	Guideway & Track Elements	The New Hope Creek Advisory Committee has expressed concerns about the alignment across New Hope Creek. In addition, the NCDENR Office of Conservation, Planning and Community Affairs initially expressed concern about the adequacy of the AA document and process, which lead to public concern about the same issue; TTA clarified the process with the Office of Conservation, Planning and Community Affairs, which now better understands that further environmental studies (most notably the NEPA EIS) will be conducted. Their desire is to have it along 15-501 and this could be costly ($60 to $100M).	Further evaluation is needed in the EIS/NEPA phase and close coordination with the authorities having jurisdiction will be needed. Cost of potential alternative and the likelihood that an alternative alignment will need to be developed.	25%	2	4	2	12

THE RISK FORMULA

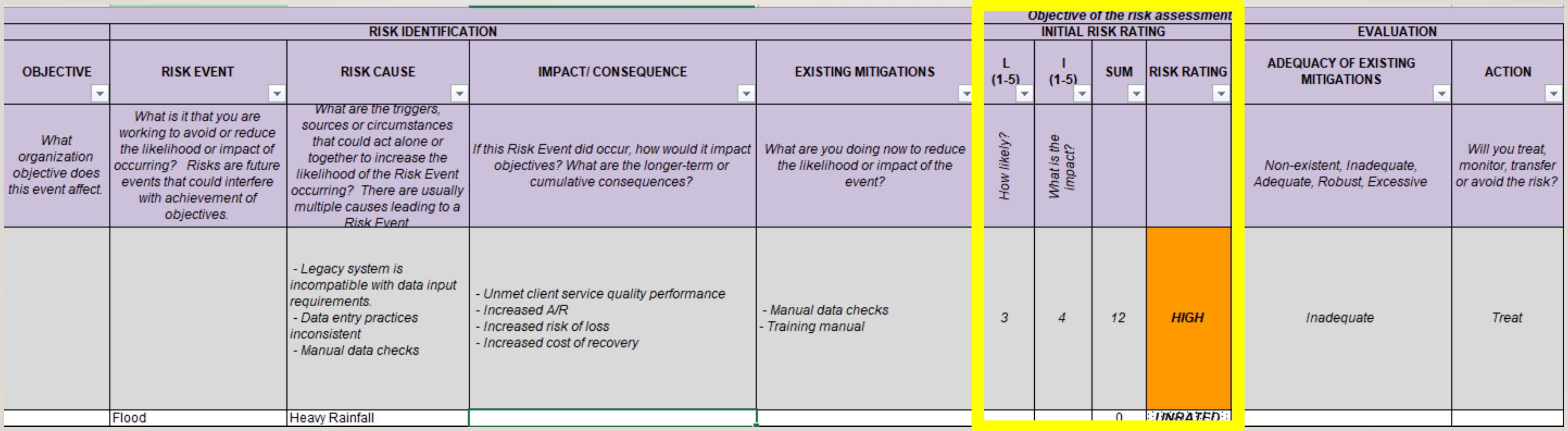
- Risk = Likelihood x Impact
  - Consequence?
    - Severity?

CAN WE START SMALL TOGETHER?



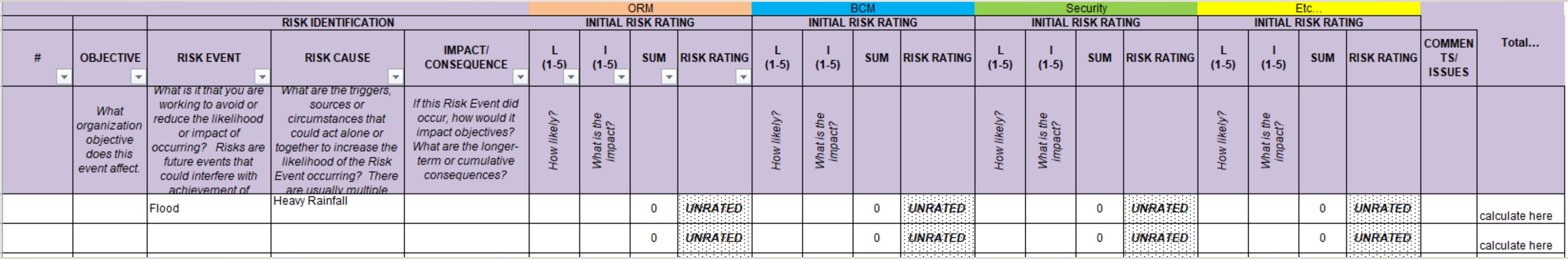
					Objective of the risk assessment.					
	RISK IDENTIFICATION				INITIAL RISK RATING				EVALUATION	
OBJECTIVE	RISK EVENT	RISK CAUSE	IMPACT/ CONSEQUENCE	EXISTING MITIGATIONS	L (1-5)	I (1-5)	SUM	RISK RATING	ADEQUACY OF EXISTING MITIGATIONS	ACTION
What organization objective does this event affect.	*What is it that you are working to avoid or reduce the likelihood or impact of occurring? Risks are future events that could interfere with achievement of objectives.*	*What are the triggers, sources or circumstances that could act alone or together to increase the likelihood of the Risk Event occurring? There are usually multiple causes leading to a Risk Event*	*If this Risk Event did occur, how would it impact objectives? What are the longer-term or cumulative consequences?*	*What are you doing now to reduce the likelihood or impact of the event?*	*How likely?*	*What is the impact?*			*Non-existent, Inadequate, Adequate, Robust, Excessive*	*Will you treat, monitor, transfer or avoid the risk?*
		- Legacy system is incompatible with data input requirements. *- Data entry practices inconsistent* *- Manual data checks*	*- Unmet client service quality performance* *- Increased A/R* *- Increased risk of loss* *- Increased cost of recovery*	*- Manual data checks* *- Training manual*	*3*	*4*	*12*	***HIGH***	*Inadequate*	*Treat*
	Flood	Heavy Rainfall					0	*UNRATED*		

CAN WE START SMALL TOGETHER?



					Objective of the risk assessment					
	RISK IDENTIFICATION				INITIAL RISK RATING				EVALUATION	
OBJECTIVE	RISK EVENT	RISK CAUSE	IMPACT/ CONSEQUENCE	EXISTING MITIGATIONS	L (1-5)	I (1-5)	SUM	RISK RATING	ADEQUACY OF EXISTING MITIGATIONS	ACTION
What organization objective does this event affect.	What is it that you are working to avoid or reduce the likelihood or impact of occurring? Risks are future events that could interfere with achievement of objectives.	What are the triggers, sources or circumstances that could act alone or together to increase the likelihood of the Risk Event occurring? There are usually multiple causes leading to a Risk Event	If this Risk Event did occur, how would it impact objectives? What are the longer-term or cumulative consequences?	What are you doing now to reduce the likelihood or impact of the event?	How likely?	What is the impact?			Non-existent, Inadequate, Adequate, Robust, Excessive	Will you treat, monitor, transfer or avoid the risk?
		- Legacy system is incompatible with data input requirements. - Data entry practices inconsistent - Manual data checks	- Unmet client service quality performance - Increased A/R - Increased risk of loss - Increased cost of recovery	- Manual data checks - Training manual	3	4	12	HIGH	Inadequate	Treat
	Flood	Heavy Rainfall					0	UNRATED		

BLOWOUT OF INITIAL RISK RATING



					ORM				BCM				Security				Etc...					
		RISK IDENTIFICATION			INITIAL RISK RATING				INITIAL RISK RATING				INITIAL RISK RATING				INITIAL RISK RATING					
#	OBJECTIVE	RISK EVENT	RISK CAUSE	IMPACT/ CONSEQUENCE	L (1-5)	I (1-5)	SUM	RISK RATING	L (1-5)	I (1-5)	SUM	RISK RATING	L (1-5)	I (1-5)	SUM	RISK RATING	L (1-5)	I (1-5)	SUM	RISK RATING	COMMENTS/ ISSUES	Total...
	What organization objective does this event affect.	*What is it that you are working to avoid or reduce the likelihood or impact of occurring? Risks are future events that could interfere with achievement of*	*What are the triggers, sources or circumstances that could act alone or together to increase the likelihood of the Risk Event occurring? There are usually multiple*	*If this Risk Event did occur, how would it impact objectives? What are the longer-term or cumulative consequences?*	*How likely?*	*What is the impact?*			*How likely?*	*What is the impact?*			*How likely?*	*What is the impact?*			*How likely?*	*What is the impact?*				
		Flood	Heavy Rainfall				0	***UNRATED***			0	***UNRATED***			0	***UNRATED***			0	***UNRATED***		calculate here
							0	***UNRATED***			0	***UNRATED***			0	***UNRATED***			0	***UNRATED***		calculate here

WHO LEADS THE CHARGE?

- Not sure we'll ever have a single right answer to that question
  - It will likely depend on your organization's current structure
    - In public sector, the EM folks often have the task fall to them to ensure BC, but from experience, DR, OH&S, and ERM are silos, independent of other resilience functions
    - In private sector, experience shows that BCDR, OH&S, and ERM rarely take advantage of the synergy between these paradigms

WHO SHOULD YOU TRUST?

- The Resilience industry has several groups that provide guidelines, oversight, certification, and education to the various disciplines, but these groups are not tightly integrated and, in some cases, are business rivals
  - The International Association of Emergency Managers (IAEM) provides Certified Emergency Manager (CEM) credentials (most recognized EM credential to our knowledge)
  - The Disaster Recovery Institute (DRI https://www.dri.ca or https://www.dri.com) provides ABCP/CBCP/MBCP/etc. credentials to BC practitioners and have strict requirements for certification and a defined, industry accepted approach to BC planning (the Professional Practices)
  - Several organizations exist that promote their own flavour of ERM certification, but a degree in risk, math, modelling or significant experience is not something that can be faked
  - Operational Risk Management designations are available through RIMS, https://www.rims.org/, in Canada and through PRMIA, https://prmia.org//, in the US. In addition, many accredited universities and colleges offer courses and certificates in ORM
  - You can find many options for DR certification that vary greatly in what is covered within the certification. Some are skewed towards traditional backup & recovery, some are cloud based, some are cyber focused, and some are totally worthless
  - OH&S is regulated by the Canada Labour Code which requires training, as do some provinces. You can find a good list of the various OH&S certifications and designations on the Canadian Society of Safety Engineering (CSSE) website, https://www.csse.org/

SUMMATION

- Organizations must require that all disciplines agree that it’s an Organization-Focused Resilience Program
  - Not a BC, DR, Security, ERM, EM, ORM, or OH&S Program
  - Take the focus away from who is in charge and identify how we can build a program that allows us to work together effectively and efficiently to provide the best value for the organization

QUESTION FOR THE AUDIENCE

SHOULD ORGANIZATIONS HAVE A CHIEF RESILIENCE OFFICER (CRO)?

WHAT RISK FORMULA WOULD YOU USE?

RISK = LIKELIHOOD X IMPACT

QUESTIONS