



Module 1: Understanding Crisis Management

Module 2: Pre-Crisis activities

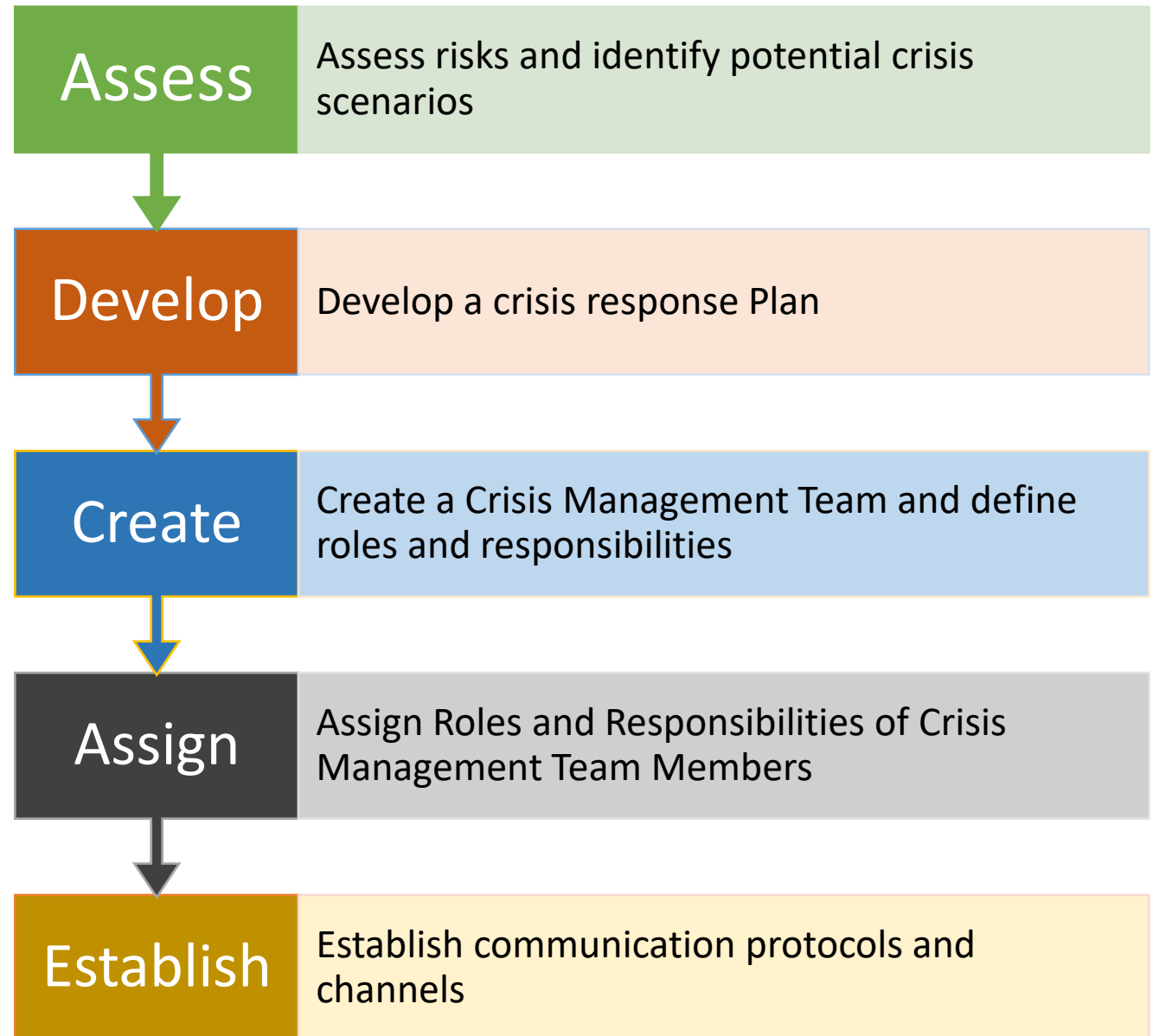
Module 3: During-Crisis activities

Module 4: Post-Crisis activities

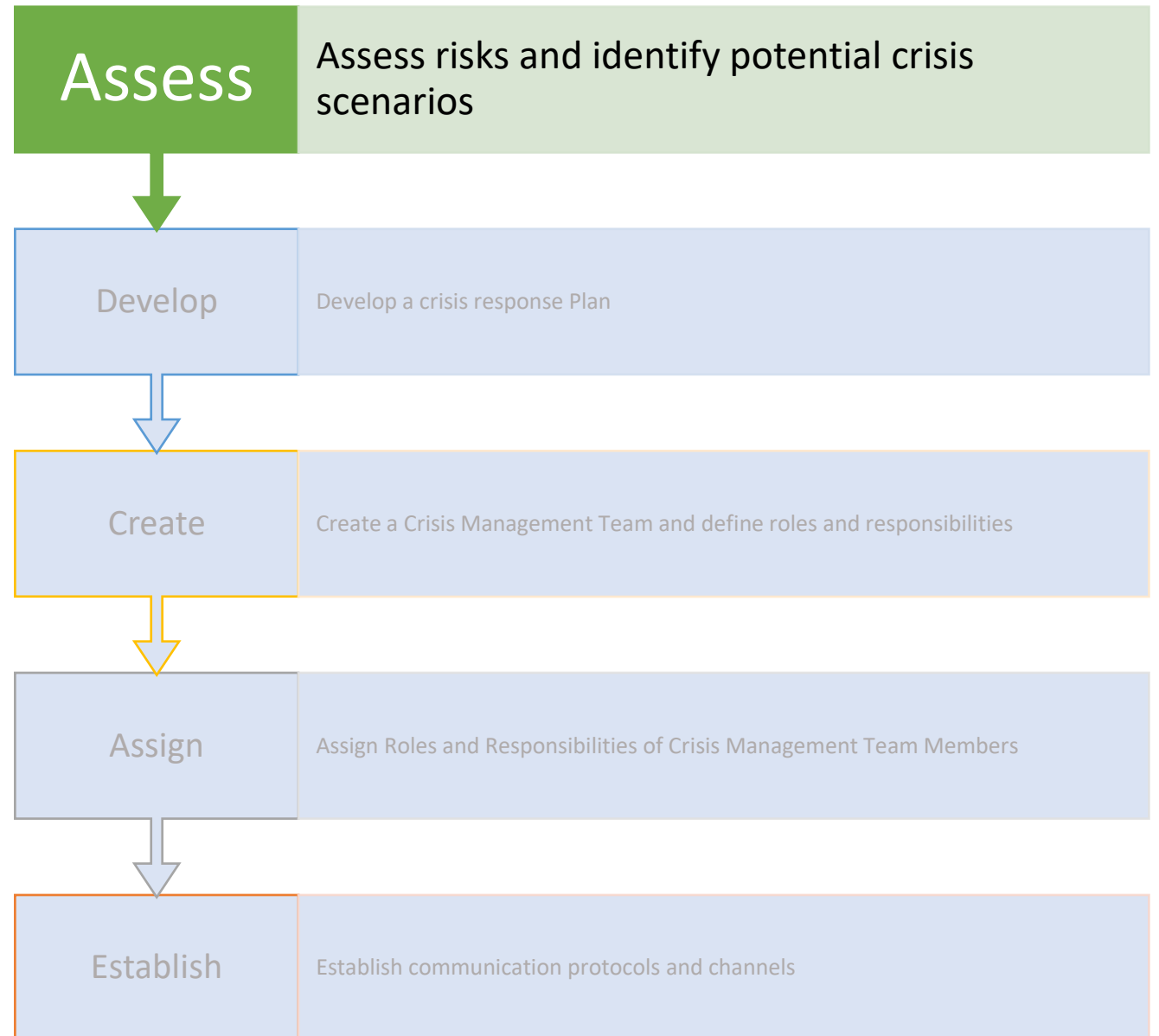
Module 5: Case studies


Module 6: Extra materials for your success

5 Key Pre-Crisis Activities:



5 Key Pre-Crisis Activities:



- 
- The first step in identifying the risks a company faces is to define the risk universe. The risk universe is simply a list of all possible risks that can potentially impact your organization.
 - During this step, you will brainstorm all the possible risks you can imagine across all of your systems, functions and processes and then prioritize them using different factors:
 - **Threats:** are events that could potentially harm the organization by intrusion, destruction, or disclosure.
 - **Impact:** is a measurement of how severe the harm to the organization would be if a particular vulnerability or threat is compromised.
 - **Likelihood:** is a measurement of the risk factor based on the probability of an attack on a specific vulnerability.



1. What could happen? (Risk/Threat)
2. How could it happen? (Cause/Trigger)
3. What is the Probability? (likelihood)
4. What could be the consequences? (Impact)
5. Is there anything that can reduce likelihood or consequences? (Controls)

Let's see some examples...

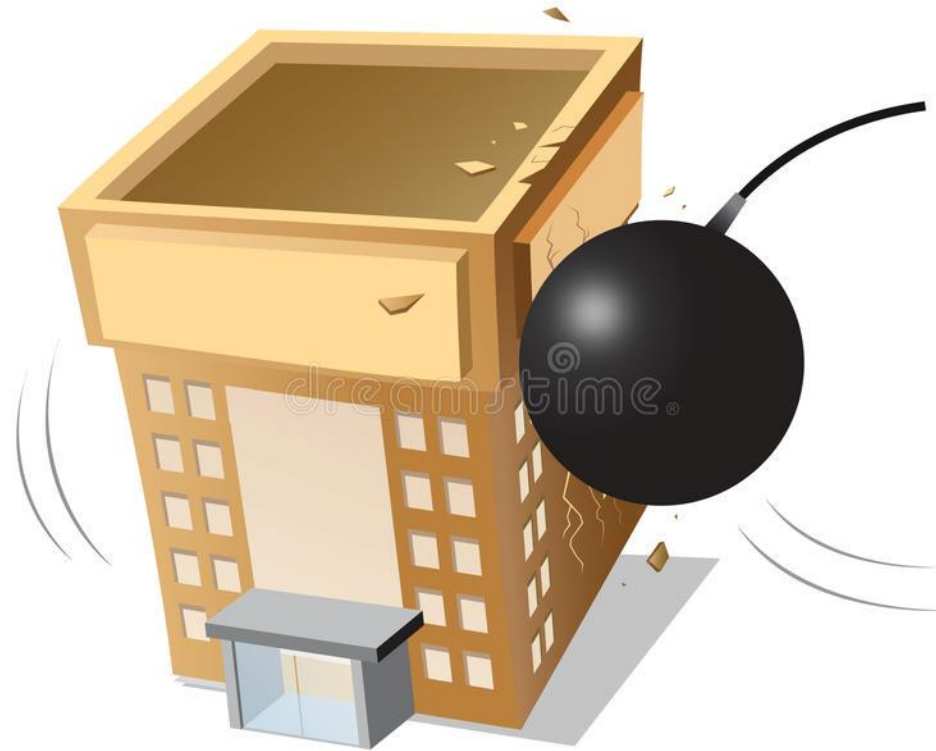


1. Natural Disasters

Examples:

- Earthquake
- Tornados
- Floods
- Severe Weather
- Wildfires
- Hurricanes





Example:

1	What could happen?	Risk	Office inaccessibility or unavailability Loss of staff Loss of/unavailability of key logistics or resources
2	How could it happen?	Cause	Hurricane, Flooding, Snow Storm, Wildfires, etc
3	What is the Probability?	likelihood	High, Medium, Low
4	What could be the consequences?	Impact	Operational: (operational downtime) Financial: (\$\$ loss of business) Reputational: customer complaints Legal/regulatory: contract breaches
5	Is there anything that can reduce likelihood or consequences?	Controls	Alternate location (Disaster recovery location) Standby outsource agreements Remote work

Activity (1):

	Cyberattack	Software Failure	Loss of Key employee	Data Theft
➤ What could happen? (Risk)				
➤ How could it happen? (Cause)				
➤ What is the likelihood? (Probability)				
➤ What could be the consequences? (Impact)				
➤ Is there anything that could to reduce likelihood or consequences? (Controls)				

Sources of Risk Identification

1. Historical or evidence based method:

1. Audit or Incident reports
2. Public media (newspaper, TV, social media, etc)
3. Annual reports or press releases.

2. Systematic identification:

i.e Critical examination of business process to determine specific points of failure:

1. Vulnerability assessments
2. Review of existing process manual and recovery / continuity plans
3. Interviews and workshops with managers, SMEs customers, suppliers etc

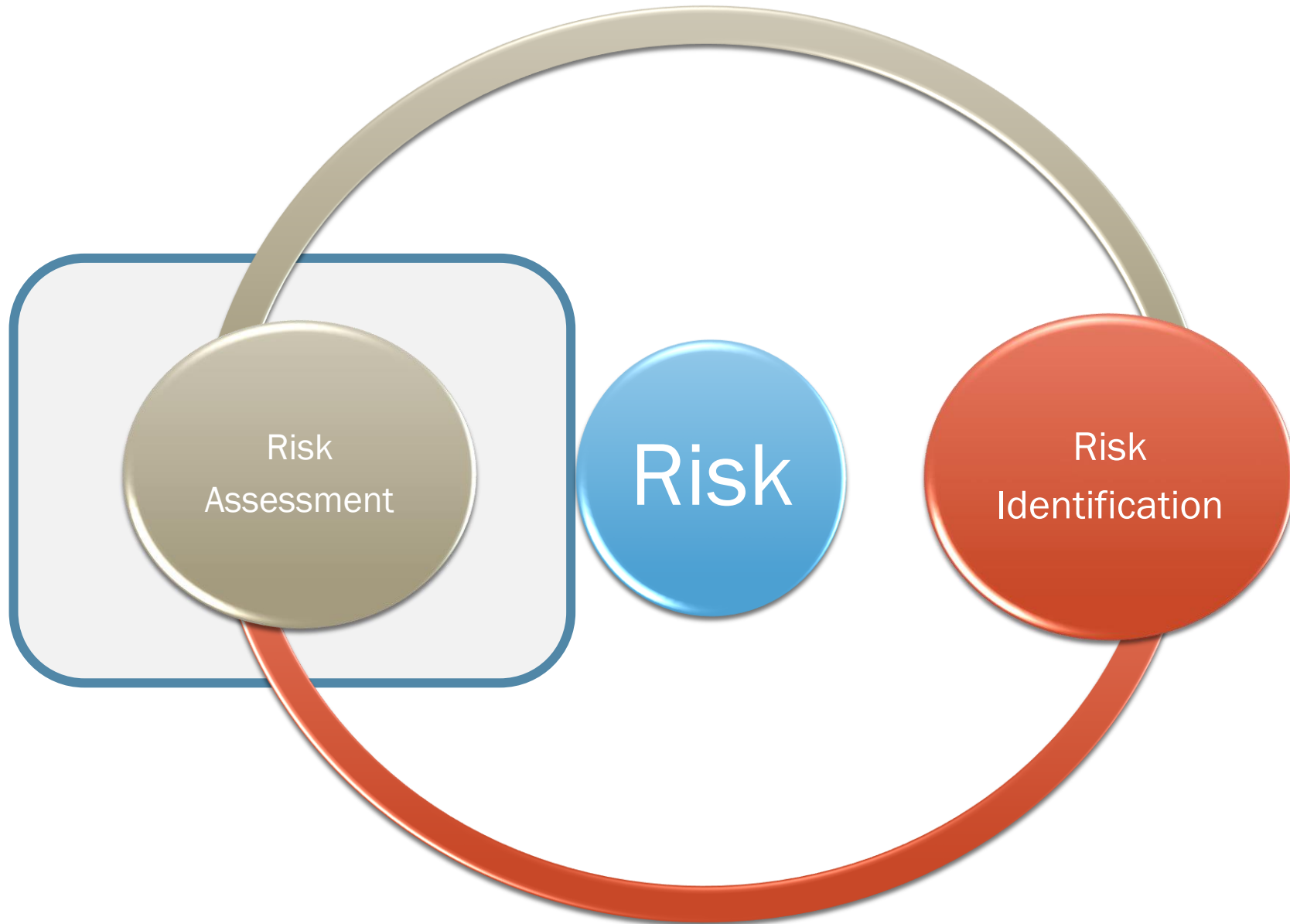
Sources of Risk Identification

Inductive methods (theoretical analysis)

- Building plausible risk scenarios and challenge response plans
- Example: IT penetration testing (simulating a threat actor's behavior)

Existing taxonomy:

- Using existing risk library of relevant risks



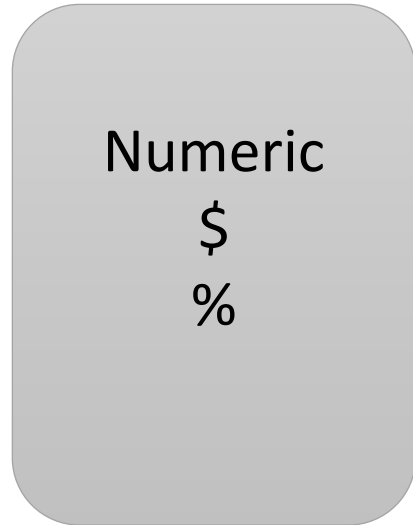
A} Identify **probability** limits/thresholds:

Probability / Likelihood / Frequency		
Probability	Description	Score
Rare	Once in > 20 years	1
Infrequent	Once in 10-20 years	2
Decade	At least once every 10 years	3
Annual	Once/Year	4
Frequent	More than once/year	5



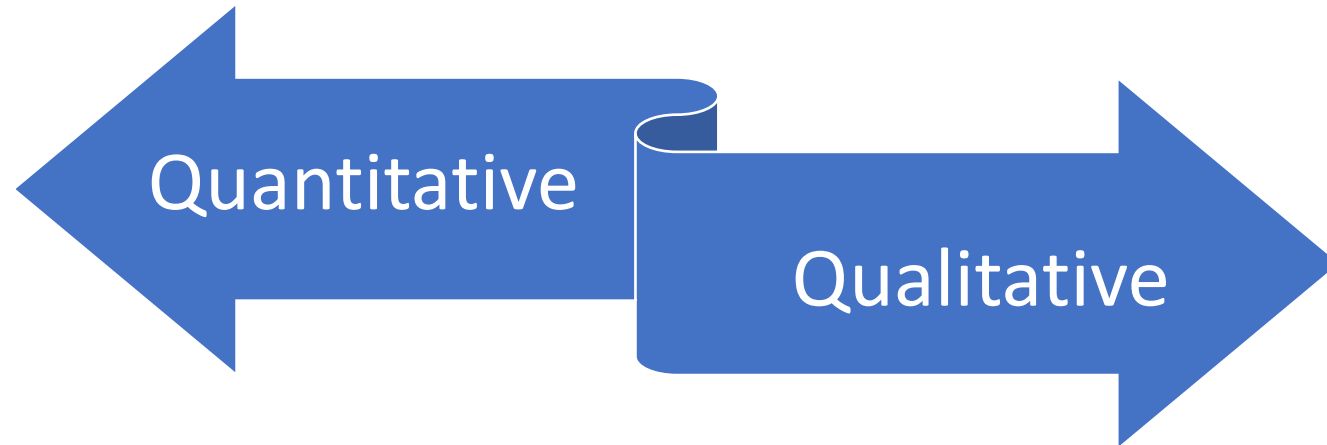
B} Identify **Impact** and assessment Criteria

Financial



Examples:

- Profit \$\$
- Losses \$\$
- Expenses \$\$
- Profit %



Non-Financial



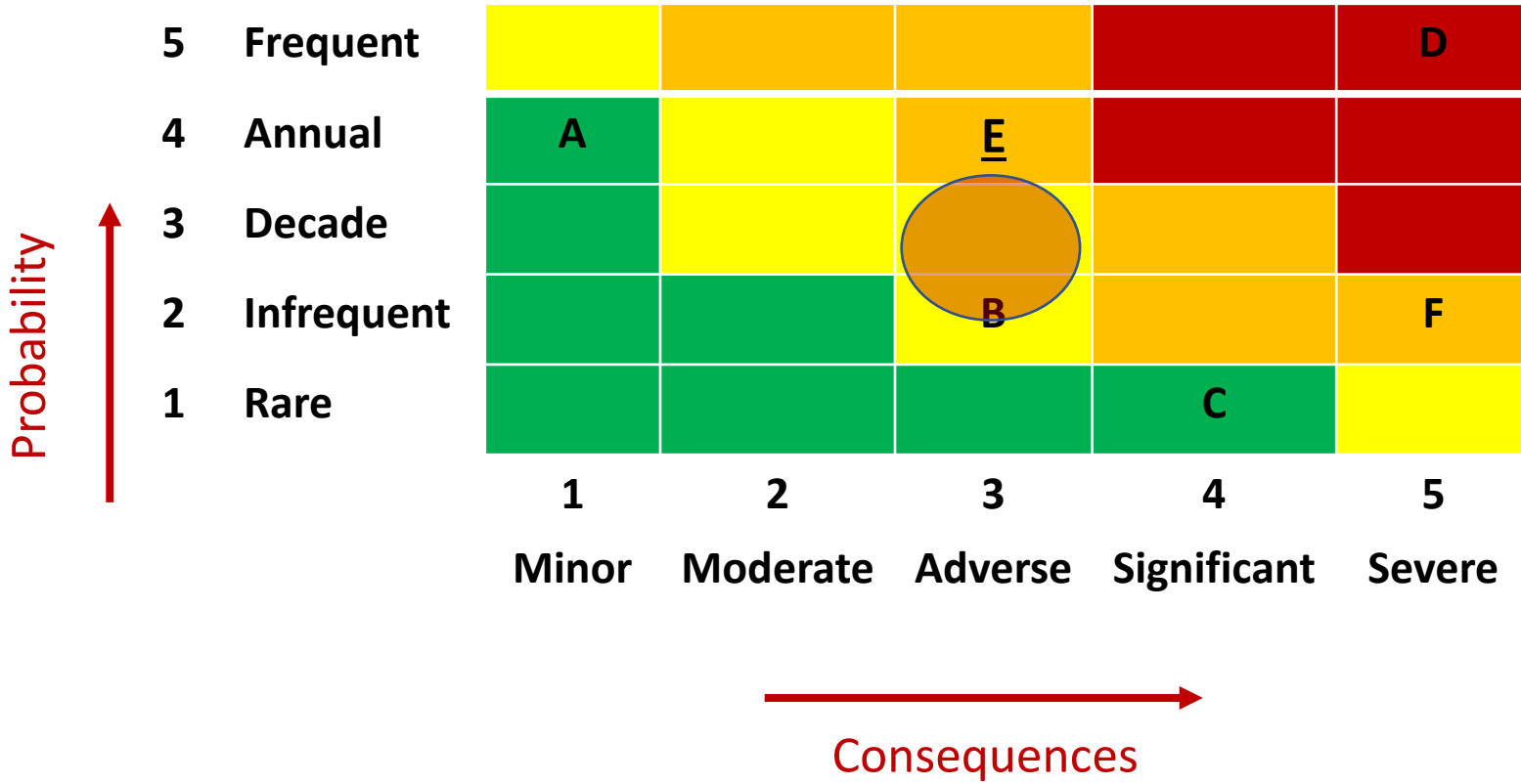
Examples:

- Reputational risk

Identify impact limits/thresholds:

Consequences (12 months)					
Impact	Score	Financial	Non-Financial		
			Customer/Operational	Reputational	Legal/Regulatory
Minor	1	< \$100K	Risk confined to 1 customer	Minor impact (client complains)	Requires regulatory notification only
Moderate	2	\$101 - 500M			Minor fine
Adverse	3	\$ 501 - 1 M	Risk affects a specific group	Mass social media spread	Risk can result in substantial regulatory fine
Significant	4	\$ 1.1 - 3 M			Regulatory breach, substantial fine is inevitable
Severe	5	\$ 3M	Risk impacts all customers	Global wide-spread scandal	Risk can result in license suspension



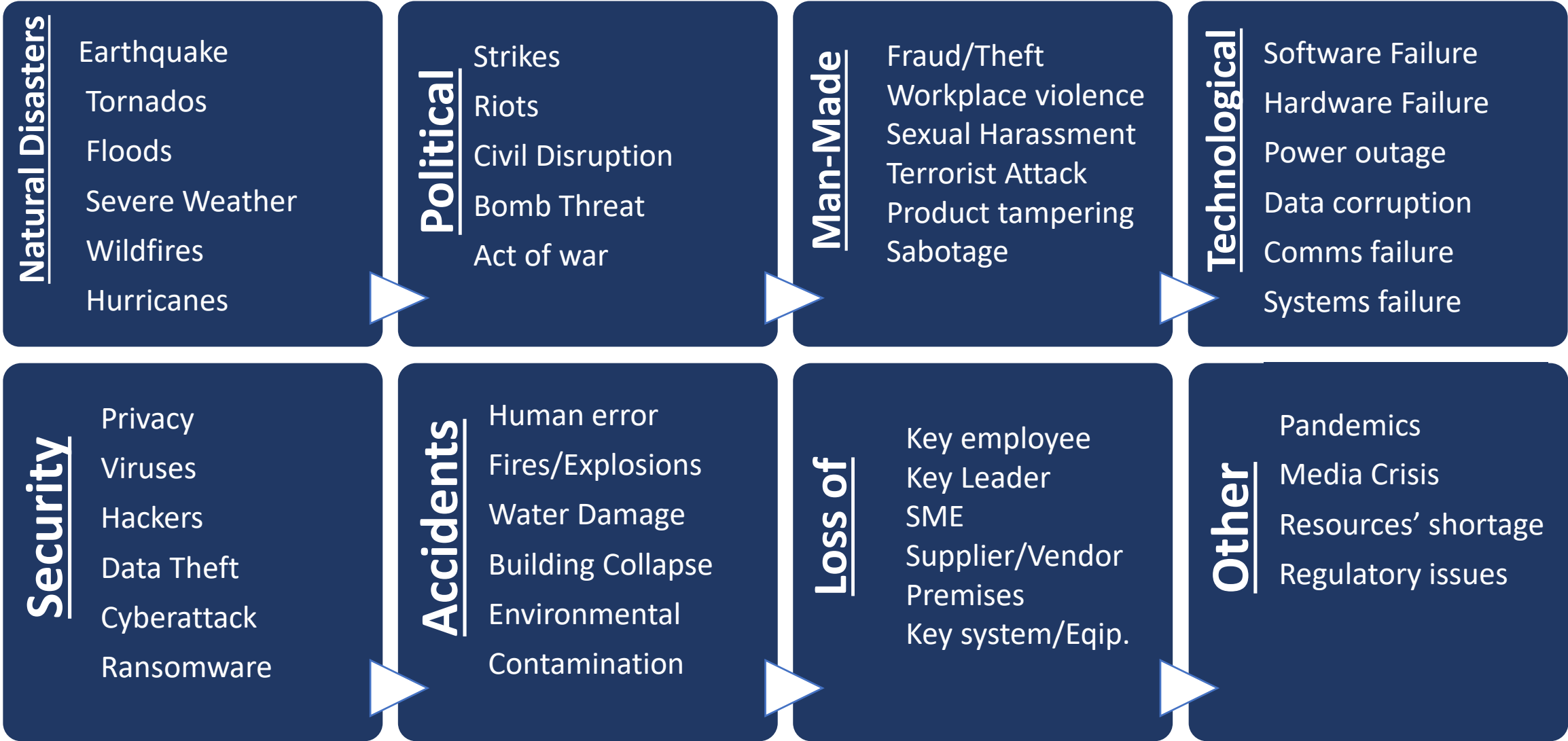


Low	Medium	High	Critical
1-4	5-9	10-15	16-25

Inherent Risk

Risk	Prob.	Impact	Risk Score
A	4	1	4
B	2	3	6
C	1	4	4
D	5	5	25
E	4	3	12
F	2	5	10

Operational Risk Universe:



Activity



List your top 5 key risks that represent a threat to your organization, arrange them in order of highest priority or highest perceived impact.

Across each risk, describe how it would impact your business



NEXT LECTURE..

Step 2: Develop a crisis response Plan

