



Resilience. Education. Credentialing.

**Embedding the Culture and Systems of Organizational Resilience**

# ICOR Webinar: Risk Management Principles & Practices



*Managing Risk Before, During, and After a Global Pandemic*

# Webinar: Risk Management Principles and Practices



Presented by Lynnda Nelson

ICOR President

April 29, 2020

Lynnda@theicor.org

- Expert in US TAG & ICOR Liaison for ISO TC 292 Security and Resilience
- Author of ICOR's NEW COR series
- Author of ICOR's ISO 22301:2019 series of courses

[Build-Resilience.org](http://Build-Resilience.org)

# Webinar Objectives

---

- 1. Understand how effectively managing risk is essential to increasing your organization's resilience.*
- 2. How to identify sources of risk.*
- 3. How to analyze and quantify risk impacts.*

The recording of the webinar will be available on the ICOR webinar page in 2 days.

If you have questions use the questions button. Questions will be answered either during the webinar or in an email after the webinar.



# Risk Defined

---



The effect of uncertainty on objectives.  
(ISO 31000)

Negative events = threats



Positive events = opportunities

# The Discipline of Risk Management

---

Managing risk is...



Dynamic



Setting Strategy

Part of Governance & Leadership

---

---

# POLL

//

*Who is responsible for managing risk at your organization?*

//

# Standards for Risk Management

---

- **Project Management Institute (PMI)** *Practice Standard for Project Risk Management* – focus on project and major program risk
- **National Institute for Standards and Technology (NIST)** *Guide for Conducting Risk Assessments (SP 800-30)* – focus is on federal information security systems (USA)
- **International Standards Institute (ISO)** *ISO 31000 Risk Management Principles and Guidelines: 2017*
- **Management System Standards** manage a specific type of risk.



# ISO 31000: Risk Management Principles

## Risk Management:



Creates & protects value



Is the responsibility of management



Is part of decision making



Addresses uncertainty



Is systematic and structured



Is based on the best available information

# ISO 31000: Risk Management Principles

---

## Risk Management:



Should be tailored to the needs of the organization



Is based on human and cultural factors



Is transparent and inclusive.



Is responsive to change in a timely manner



Facilitates continual improvement

# The Risk of Local Outbreaks Becoming Global Pandemics

---

Many challenges exist worldwide that increase the risk that outbreaks will occur and spread rapidly, including:

Increased risk of infectious pathogens “spilling over” from animals to humans

Development of antimicrobial resistance

Spread of infectious diseases through global travel and trade

Acts of bioterrorism

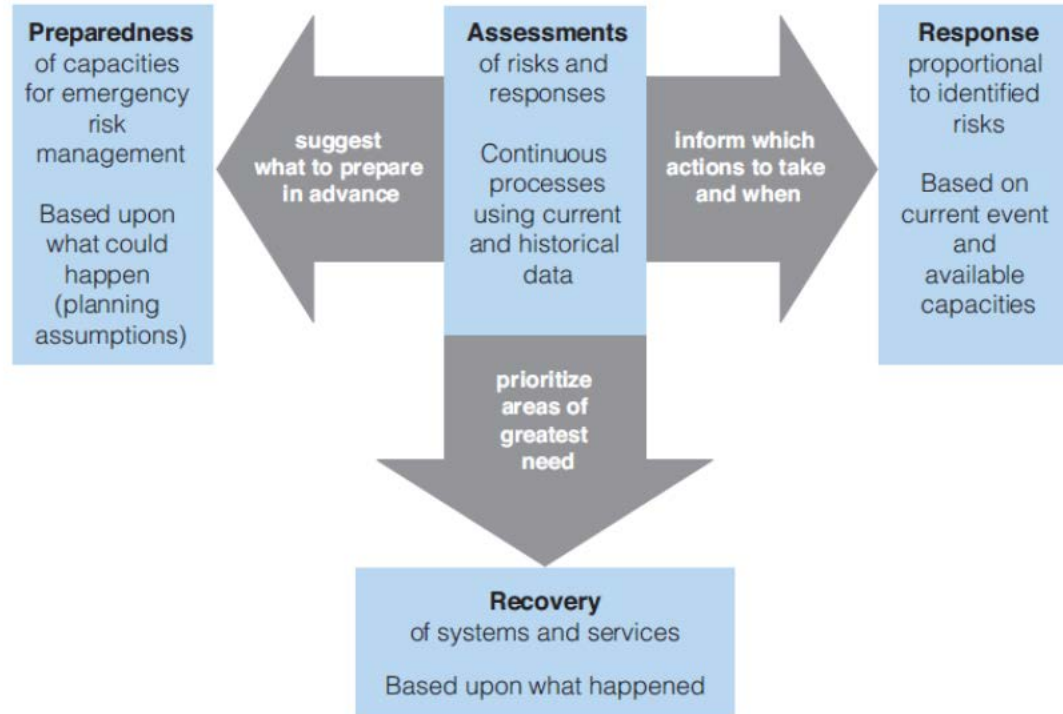
Weak public health infrastructures

**CDC 2017**

<https://www.cdc.gov/globalhealth/healthprotection/fieldupdates/winter-2017/why-it-matters.html>

# WHO: Pandemic Influenza Risk Management (May 2017)

Figure 4.1: Pivotal role of risk assessment in preparedness, response and recovery actions



[https://www.who.int/influenza/preparedness/pandemic/influenza\\_risk\\_management/en/](https://www.who.int/influenza/preparedness/pandemic/influenza_risk_management/en/)

# Pandemic Risk in the News – BEFORE 2020



By **Jessie Yeung**, CNN

Updated 8:57 AM ET, Wed September 18, 2019



**The Risk of a Global Pandemic is Growing –  
and the world isn't ready, experts say**

<https://www.cnn.com/2019/09/18/health/who-pandemic-report-intl-hnk-scli/index.html>



# Pandemic Risk in the News – BEFORE 2020

---

"The world is not prepared," the report from the Global Preparedness Monitoring Board (GPMB), co-convened by the World Bank and the World Health Organization (WHO), warned. "For too long, we have allowed a cycle of panic and neglect when it comes to **pandemics**: we ramp up efforts when there is a serious threat, then quickly forget about them when the threat subsides. It is well past time to act."

**WHO**  
**September**  
**2019**

The WHO called for world leaders to take seven concrete actions to lessen the risk, including monitoring progress during international summits, creating multi-year disaster plans, strengthening United Nations coordination, and building preparation systems across all sectors.


<https://www.cnn.com/2019/09/18/health/who-pandemic-report-intl-hnk-scli/index.html>

---

---

# POLL

**// To what extent do you feel your national and local government was prepared to handle the COVID-19 pandemic? //**

A man with dark hair and a beard, wearing a dark suit, white shirt, and patterned tie, is looking slightly to the right with a thoughtful expression. The background is a blurred indoor setting.

**The risk of a global  
pandemic has been  
realized.**

**What do we do now?**

**DO WE HAVE YOUR  
ATTENTION NOW?**



# Managing Risk – What are you waiting for?!?

---

**“By failing  
to prepare,  
you are  
preparing  
to fail.”**

Benjamin Franklin

*It is time to understand best  
practice for managing risk.*

# Risk Management Process

---

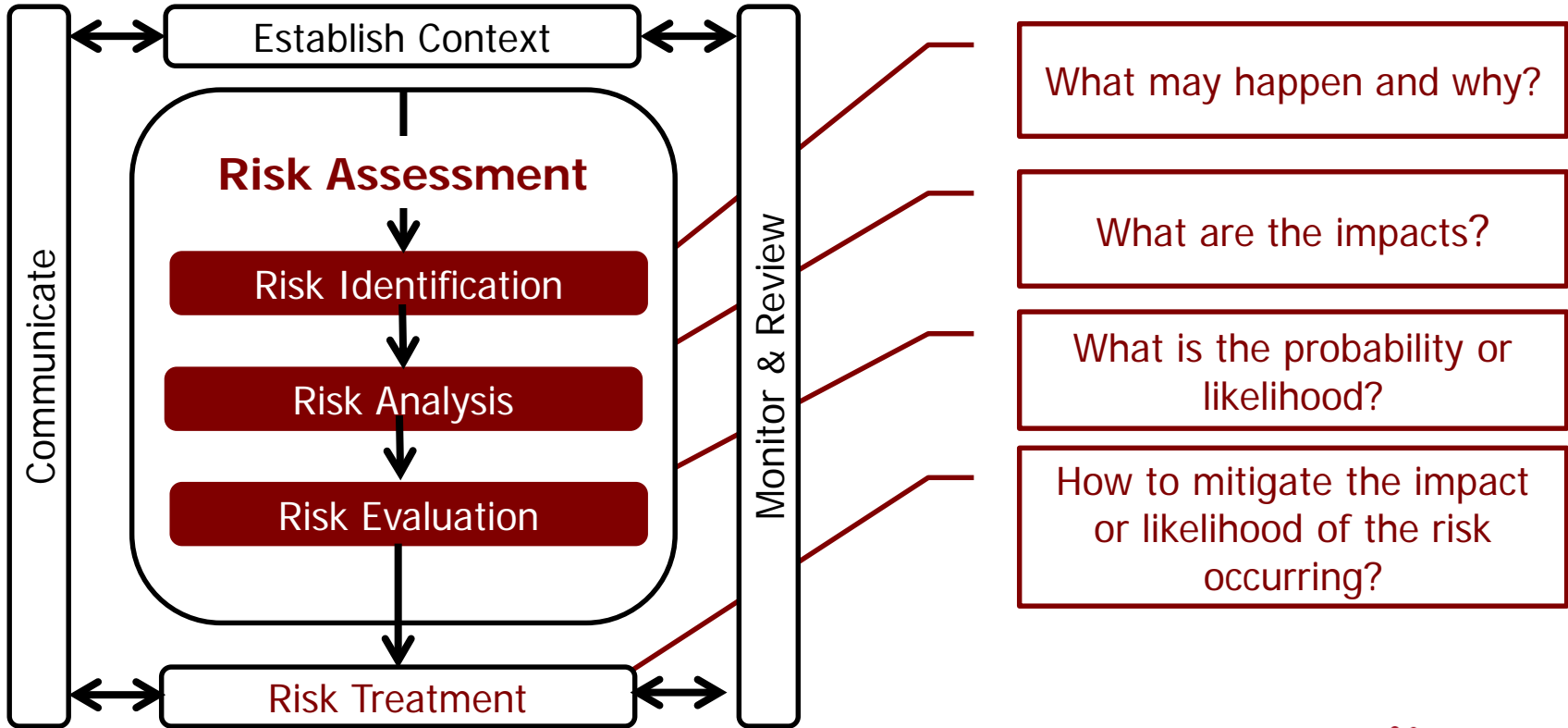


## Essential Aspects Include:

1. List of individual risks
2. Rating of each risk based on likelihood and impact
3. Assessment of current controls and vulnerabilities
4. Plan of action – treatment of risks

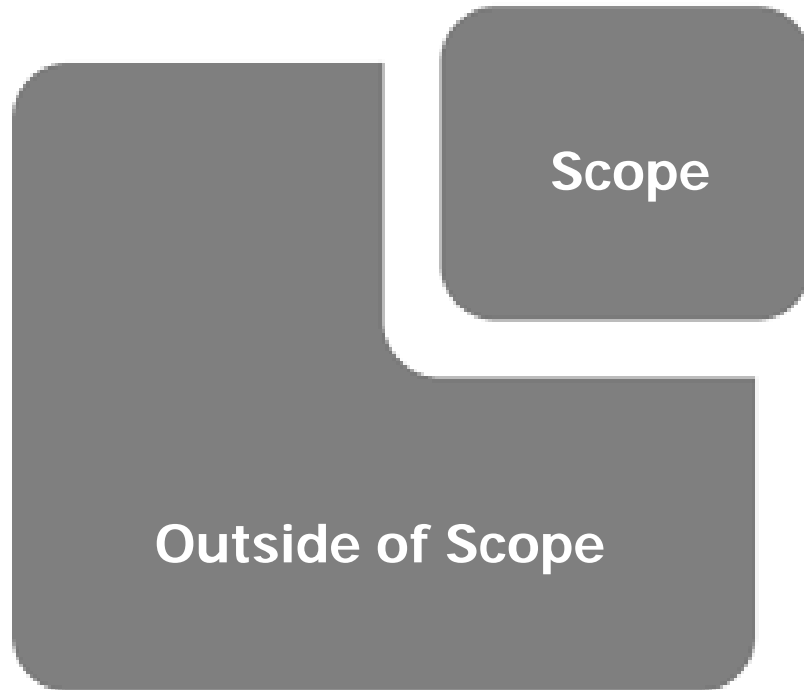
How can we be more prepared?

# ISO 31000 Risk Management Methodology



# Establish the Context

---



Define the scope of the risk assessment – is it based on the probability of a specific risk event, a specific risk category, or “all hazards”?

# Pandemic Risk Forecasting – AI (BlueDot)

---



<https://www.cbsnews.com/news/coronavirus-outbreak-computer-algorithm-artificial-intelligence/>

# Risk Identification - Sources / Types of Risk

---



Strategic  
Risk



Compliance  
Risk



Operational  
Risk



Financial  
Risk



Reputational  
Risk

*What might happen and why?*

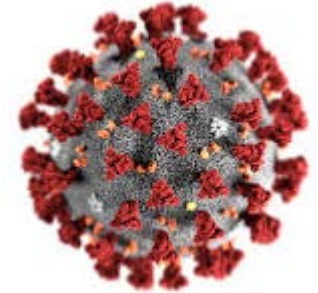
<https://business.tutsplus.com/series/managing-risk-in-your-business--cms-701>

# Business Risks Due to Pandemics

---

How will your organization generate revenue and execute operations with workplaces mostly either off-line or remote? For 18-24 months?

1. Disruption due to social distancing
2. Plummeting employee productivity (and deaths!)
3. Stressed supply chains
4. Recession, unemployment, and investment pull-back
5. Economic instability and civil unrest
6. Cybersecurity risk for remote working



---

---

# POLL

***“ Who is responsible for managing ‘pandemic’ risk at your organization? Choose all that apply. ”***



# Risk Identification Methodologies



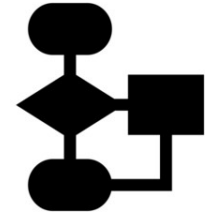
Brainstorming /  
Historical Records



Delphi



Interviews / Experience  
Judgment



Flow Charts



Bow Tie Analysis



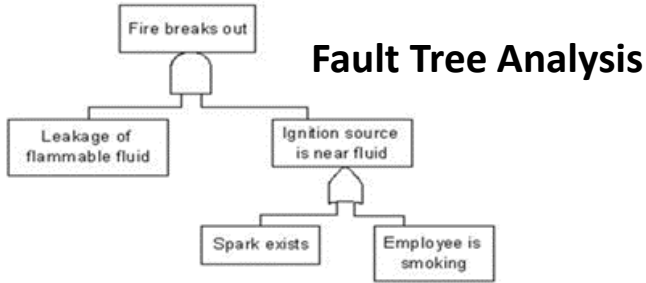
Audits



Scenario Building

[https://sielearning.tafensw.edu.au/toolboxes/toolbox904/toolbox904/resource\\_centre/r2\\_risk\\_assess/r206\\_identi\\_meth/r206\\_identi\\_meth.htm](https://sielearning.tafensw.edu.au/toolboxes/toolbox904/toolbox904/resource_centre/r2_risk_assess/r206_identi_meth/r206_identi_meth.htm)

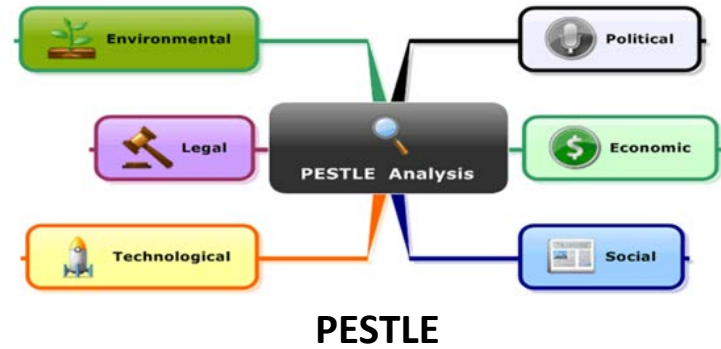
# Methods of Failure Analyses - Examples



## Failure Mode and Effects Analysis (FMEA)

## SWOT Analysis

<b>S</b>	<b>Strengths</b> <ul style="list-style-type: none"> <li>• Things you are good at</li> <li>• Experience, knowledge</li> <li>• Unique characteristics</li> <li>• Resources</li> <li>• Geographical location</li> <li>• Competence, capabilities</li> <li>• Quality, reputation</li> <li>• Flexibility on Product, Pricing, Distribution</li> </ul>	<b>W</b>	<b>Weaknesses</b> <ul style="list-style-type: none"> <li>• Things you need to improve</li> <li>• Gap in skills, knowledge</li> <li>• Financial issues</li> <li>• Market awareness and reputation</li> <li>• Right people doing the right job</li> <li>• Poor location</li> <li>• Leadership and Management issues</li> <li>• Staff motivation and involvement</li> </ul>
<b>O</b>	<b>Opportunities</b> <ul style="list-style-type: none"> <li>• Strategic alliances, acquisitions</li> <li>• Diversify the business</li> <li>• Take advantage of new trends (PESTLE)</li> <li>• New Product Development</li> <li>• Enter new markets</li> <li>• Reduce costs</li> <li>• Be faster, better, easier, more stylish,</li> <li>• Innovation in technology development</li> </ul>	<b>T</b>	<b>Threats</b> <ul style="list-style-type: none"> <li>• Change in the environment (PESTLE).</li> <li>• Loss of major customers.</li> <li>• Raw material, energy and transport costs</li> <li>• Strong competition</li> <li>• Competitors new products and innovation</li> <li>• Change in technology</li> <li>• Fashion</li> <li>• Seasonality</li> </ul>



# List Potential Risks

---



**Once you have identified all of the risks within your scope , list them in a simple manner as a starting point.**

<https://business.tutsplus.com/series/managing-risk-in-your-business--cms-701>

# Risk Analysis – Information to Collect

---

- **The nature of the risk** - how, when, why, and where the risk is likely to occur.
- **The source of the risk** - what aspects of the source put the elements at risk, any technical data available
- **The elements of the risk** – who or what is at risk, why they are vulnerable, technical data or background information.
- **Statistical or historical data** – if available

# Risk Analysis - Controls

---



During the risk identification process, information about how the risk is currently being controlled may become available.

Those current controls then become part of the data under analysis in determining if those controls are adequate to continue to manage the risk or, if not, whether the level of risk needs to be reduced further.

# Risk Analysis - Impact

---

WHAT IS THE...  
**Impact**

**You'll need some way of quantifying the impact the identified risks would have on your organization.**



# Risk Analysis – List by Greatest Impact

---

**High Impact**

**Medium Impact**

**Low Impact**

*List the risks in order from greatest impact to least impact.*

# Risk Analysis – List by Impact: Example

Scale	Impact	General Description	Example of Expected Loss
1	Extreme	Threatens survival of organization, major problems for stakeholders. Revenue loss greater than x%	Death or destruction Greater than \$500,000
2	Very High	Threatens survival of organization, requires top level intervention. Revenue loss greater than y%	Serious injury, loss or operational capacity Less than \$500,000
3	Moderate	Survival of organization would not be threatened, requires significant review of operations. Revenue loss greater than z%	Outside assistance required Less than \$50,000
4	Low	Threat to efficiency of some aspects of the organization, dealt with internally. Revenue loss below w%. Little or no effect on stakeholders	Immediately contained Less than \$5,000
5	Negligible	Dealt with by variation to routine operations. Minimal or no loss to organization or stakeholders	Disruption minimal Less than \$100



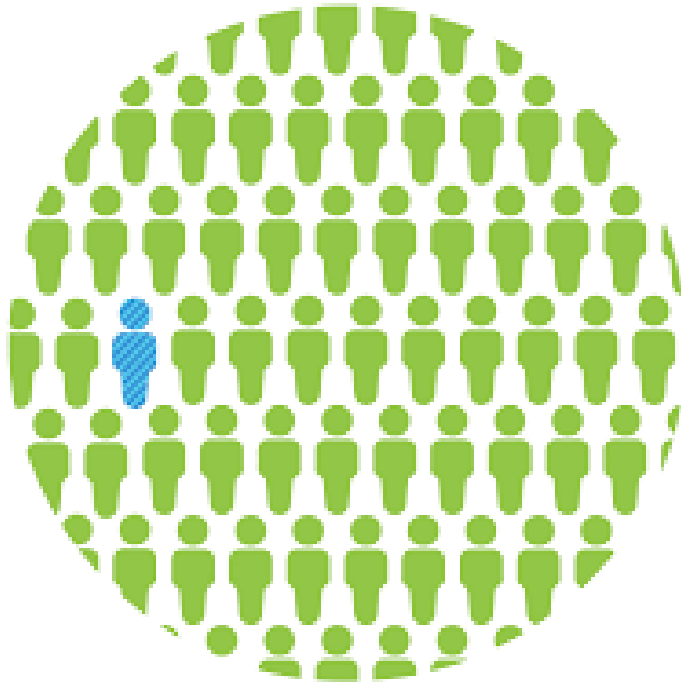
# Question from a Participant

---

*“Is it necessary to identify probability or could we just focus on the identification of the impacts of every threat?”*

# Risk Analysis – Likelihood

---



**Estimate the  
Likelihood of the  
Risk Occurring**

<https://business.tutsplus.com/tutorials/how-to-measure-risk-in-your-business--cms-22763>

# Risk Analysis – List by Likelihood

---

Scale	Likelihood	General Description
A	Very Likely	Is expected to occur in most circumstances
B	Likely	Will probably occur in most circumstances
C	Possible	Might occur at some time
D	Unlikely	Could occur at some time in particular circumstances
E	Rare	May occur only in exceptional circumstances

# Risk Evaluation Criteria - Example

---

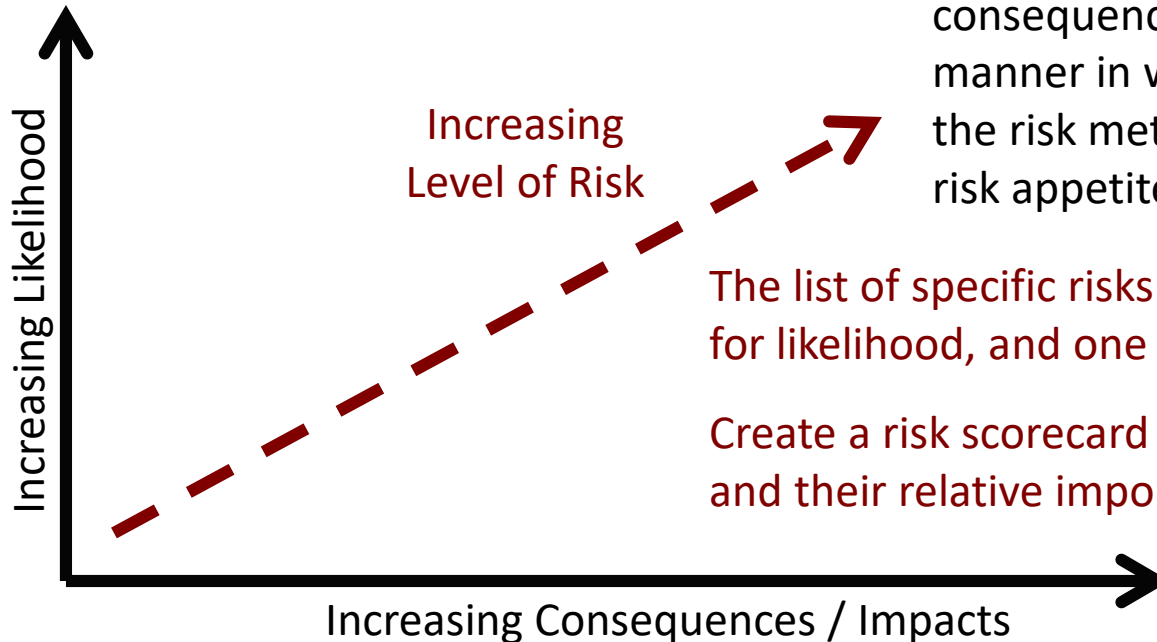
Level of Risk	Evaluation Criteria	Management Action Required
High	Almost certain to threaten the organization. Financial threat to survival of organization body or stakeholders.	Involvement of senior management of stakeholder organization. Eliminate risk or curtail activity.
Medium	Unlikely to threaten the organization. Stakeholder organizations may suffer some threat to financial security.	Manage by specific monitoring and response to risk. Risk should be reduced as much as possible.
Low	Unlikely to threaten the organization or stakeholders.	Monitor and manage as part of routine procedures. Accept risk.

# Risk Evaluation

---

- Compare the estimated risks against given risk criteria to determine significance of risk
- Use the risk evaluation to make decisions about the significance of risks and whether each risk should be accepted or treated
- Qualify risks by probability and loss enabling the organization to spend resources on those most likely to occur

# Characteristics of a Risk Metric



The scales for measuring the consequences and likelihoods and the manner in which they are combined in the risk metric reflect the risk attitude or risk appetite of the organization.

The list of specific risks should have two scores: one for likelihood, and one for impact.

Create a risk scorecard that summarizes these risks and their relative importance.

# Risk Evaluation Techniques

	Quantitative	Qualitative
<i>Advantages</i>	<ul style="list-style-type: none"><li>• Allows for definition of consequences of incidents and allows the identification of costs and benefits during selection of mitigation choices</li><li>• Provides a more accurate image of risk</li></ul>	<ul style="list-style-type: none"><li>• Allows for putting in order risks according to priority</li><li>• Allows for determination of areas of greater risk in a short time without bigger cost</li><li>• Analysis is relatively easy and cheap</li></ul>
<i>Disadvantages</i>	<ul style="list-style-type: none"><li>• Depend on scope and accuracy</li><li>• Must be enriched by qualitative descriptions</li><li>• More expensive requiring greater experience and advanced tools</li></ul>	<ul style="list-style-type: none"><li>• Does not allow for determination of probabilities and results using numerical measures</li><li>• Cost-benefit analysis is more difficult during selection of mitigation choices</li></ul>

**There are many different risk evaluation techniques.**

# Qualitative Evaluation Example

	<b>Likelihood</b>	<b>Insignificant</b> (incident but no injury)	<b>Minor</b> (first aid injury)	<b>Serious</b> (serious injury / lost time)	<b>Major Impact</b> (death / disability)
<b>PROBABILITY</b> ↑	<b>Very Likely</b> (will most certainly happen)	Medium	High	High	Extreme
	<b>Likely</b> (will probably happen at some time)	Medium	Medium	High	High
	<b>Unlikely</b> (could happen sometime)	Low	Medium	Medium	High
	<b>Very Unlikely</b> (might happen only rarely)	Low	Low	Medium	Medium
	<b>IMPACT</b> →				



# Qualitative Method: NIST Methodology

## Combining Qualitative with a Quantitative Measure

### Risk Scale:

High = 51 to 100

Medium = 11 to 50

Low = 1 to 10

	Likelihood of Risk	Low (10)	Medium (50)	High (100)
PROBABILITY ↑	High (1.0)	Low $10 \times 1.0 = 10$	Medium $50 \times 1.0 = 50$	High $100 \times 1.0 = 100$
	Medium (0.5)	Low $10 \times 0.5 = 5$	Medium $50 \times 0.5 = 25$	Medium $100 \times 0.5 = 50$
	Low (0.1)	Low $10 \times 0.1 = 1$	Low $50 \times 0.1 = 5$	Low $100 \times 0.1 = 10$
	IMPACT →			

# What is the Organization's Risk Appetite?

---

*What is the Amount of Risk your Organization May or May Not Take?*

Are they risk averse?



Or do they live on the edge – ready to try anything?

Risk appetite reflects the organization's risk management philosophy, and influences its culture and operating style.

Risk appetite guides resource allocation and is part of designing the infrastructure necessary to effectively respond to and monitor risks.

---

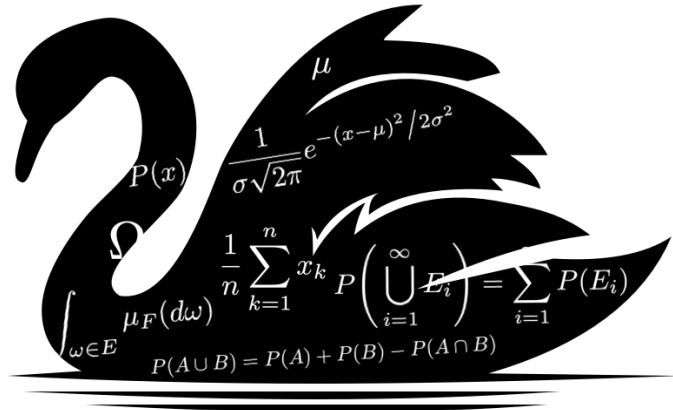
---

# POLL

**// To what extent has your organization's risk appetite "changed" as a result of the pandemic?  
Choose all that apply. //**

# Do you need to plan for everything?

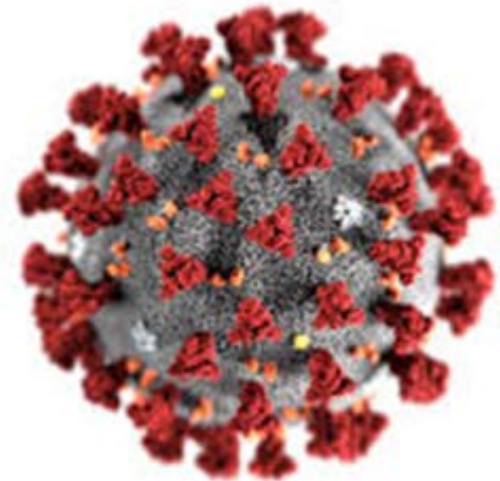
---



**Black Swan Events**

**High Impact**

**Low Probability**



# Risk Treatment / Mitigation Strategies

Options for risk treatment should be selected based on:



Perceived vulnerability of the organization



The cost of measures compared to benefits



The urgency of the activity

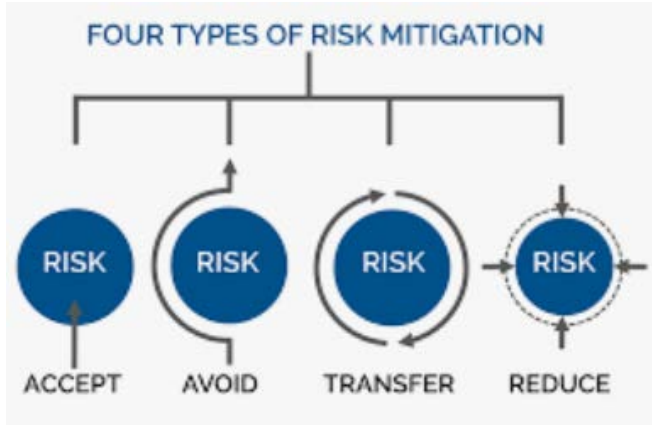


Overall feasibility and suitability of the option

Risk Appetite



# Types of Risk Treatment or Mitigation



Acceptance



Avoidance



Cease or Change the Activity



Transfer Risk to another part of the Organization or a Third Party



Transfer - Financing / Insurance



Reduce: Control or mitigate

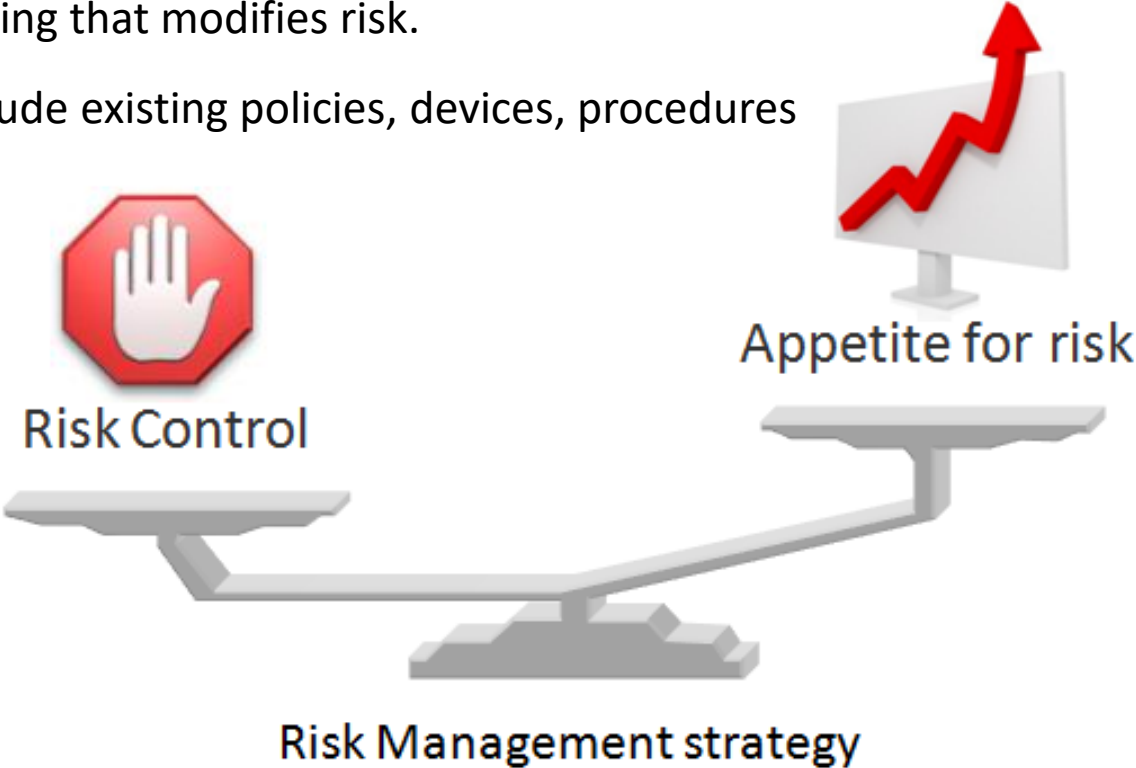


Remove Risk to Activity

# Effectiveness of Controls

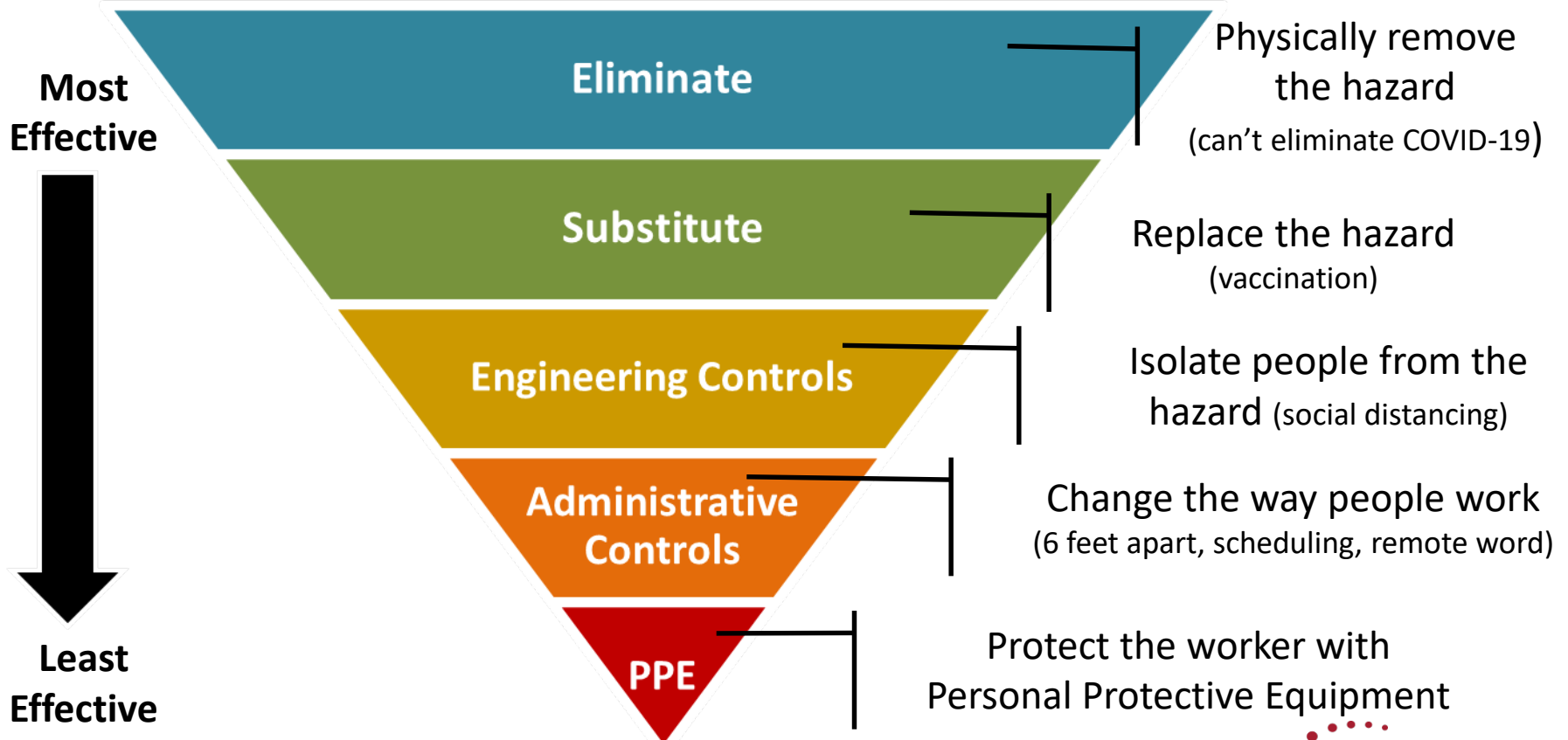
A control is anything that modifies risk.

Controls may include existing policies, devices, procedures and practices.



<http://broadleaf.com.au/wp-content/uploads/2014/07/Broadleaf-tutorial-Setting-priorities-for-risk-treatment-and-assurance-of-controls-v9.pdf>

# Effectiveness of Controls



<http://broadleaf.com.au/wp-content/uploads/2014/07/Broadleaf-tutorial-Setting-priorities-for-risk-treatment-and-assurance-of-controls-v9.pdf>





# Control Effectiveness & Risk Levels

		Level of Risk			
		Low	Medium	High	Extreme
Control Effectiveness	Fully effective		9	8	2
	Substantially effective		22	44	12
	Partially effective		9	42	22
	Largely ineffective		4	12	15
	Totally ineffective			5	5

**Priority area for control improvement**

<http://broadleaf.com.au/wp-content/uploads/2014/07/Broadleaf-tutorial-Setting-priorities-for-risk-treatment-and-assurance-of-controls-v9.pdf>

# Potential Exposure Measures

---



Maximum  
monetary loss



Impact to life safety /  
safety outcomes



Impact to company  
brand and reputation

<http://broadleaf.com.au/wp-content/uploads/2014/07/Broadleaf-tutorial-Setting-priorities-for-risk-treatment-and-assurance-of-controls-v9.pdf>

# Potential Exposure & Control Effectiveness

Level of Risk	Potential Exposure	Control Effectiveness	Priority for Treatment
High	High	Low	①
		High	4
	Low	Low	②
		High	5
Low	High	Low	③
		High	6
	Low	Low	7
		High	8

<http://broadleaf.com.au/wp-content/uploads/2014/07/Broadleaf-tutorial-Setting-priorities-for-risk-treatment-and-assurance-of-controls-v9.pdf>

# Risk Description Ties to Risk Strategy

---

---

<b>Name of the Risk</b>	<b>Unique identifier</b>
Risk Scope	Details of possible incidents, including size, type & number
Risk Nature	Timescale of potential impact
Stakeholders	Internal & external - expectations
Risk evaluation	Likelihood and magnitude and possible impact
Loss experience	Previous incidents and prior losses
Risk appetite	Risk attitude, tolerance, target for control of risk
Risk treatment	Existing controls, implementation of new controls
Potential for improvement	Recommendations for cost effective risk improvement
Risk strategy	Assignment of responsibility for implementation

# Risk Register

---

1. The Risk – what can happen and how it can happen
2. Consequences/impact of it happening
3. Likelihood of it happening
4. Adequacy of current controls
5. Consequence / impact rating
6. Likelihood rating
7. Level of risk
8. Risk priority

A risk register consolidates all of the risk information and decisions made.

# Risk Reporting & Communication

---



**Risk communication is an open, two-way exchange of information.**

# Reopening for Business-as-“new” usual

---

1. **Cleanliness is next to godliness – is required.** Implementation of rigorous cleaning procedures.
  - a. Define and distribute new cleanliness metrics and inspection
  - b. PPEs
  - c. HVAC and air filtration
  - d. Hazard analysis of critical control points – HACCP
  
2. **What is “healthy” and who can work?** Implementation of regular testing and screening for COVID-19 symptoms.
  - a. Impact of privacy and employment law issues
  - b. Isolation rooms for employees who experience symptoms while at work
  - c. Quarantine policies – time off policies
  - d. Mental health support

<https://www.marsh.com/us/insights/research/reopening-for-business-in-a-post-coronavirus-world.html>

# Reopening for Business-as-“new” usual

---

## 3. **Monitored.** Classified based on health standards

- a. Active monitoring of health and symptoms
- b. Screening for viruses
- c. Temperature monitoring
- d. Wristbands that allow access to transport, employment and commerce?

## 4. **Individualized.** No more shared office equipment or close quarters for seating.

- a. No or limited shared computers, printers, PDAs and phones
- b. How to implement non-touch control systems for fixed equipment?
- c. Use of shift schedules, rotations, start times
- d. No / limited large employee meetings



# Reopening for Business-as-“new” usual

---

- 5. Isolated.** Remote working will grow in popularity – become permanent.
- Fundamental design changes to accommodate for social distancing
  - What travel modes and facilities are acceptable?
  - Impact to commuting, car-pooling and ride sharing?

**6. Prepared.** Time to get prepared – finally?

- Planning, training, and practice required – including supply chains
- New / updated policies and practices
- Robust IT systems
- Stockpiles of PPE and other essentials
- Clear behavioral expectations, review, and feedback

---

---

***// Please share strategies your organization has already implemented or will implement soon in the post webinar survey. //***

***// ICOR will share your responses anonymously to the webinar attendees. //***

# In Conclusion

---

1. Risk should be managed at the “enterprise” or organization-wide level.
2. The Risk Assessment process methodically addresses the identification and treatment of risks that may harm the organization’s operating efficiency.
3. Risk management must be integrated into the culture of the organization by assigning responsibility for risk mitigation to each member of the organization.
4. Risk impact, probability, adequacy of controls, and risk appetite should inform an organization’s risk strategy.

# ICOR Education & Credentialing

**Organizational Resilience  
Professional Development &  
Credentialing Program**

**ICOR** **ICOR** **ICOR**

**CORM CORP CORE**

Certified Organizational Resilience Manager   Certified Organizational Resilience Professional   Certified Organizational Resilience Executive

*Required Competencies to be a Leader in Organizational Resilience*

**ICOR Competency Model**

- Continual Improvement
- Organizational Behavior
- Organizational Infrastructure
- Preparedness & Managing Risk
- Technology Infrastructure

Resilience.  
Education.  
Credentialing. **ICOR**

The International Consortium  
For Organizational Resilience

**Offered Globally –  
Instructor-led, Blended  
Learning, and eLearning**

[Build-Resilience.org](http://Build-Resilience.org)

# ICOR 2020 Webinar Series



Offered live and On Demand for 30 days to the public.

After 30 days available for ICOR members in the ICOR Resilience Research Center.

© 2020 ICOR ALL RIGHTS RESERVED

**May 27:** Insights from an ISO 22301 3<sup>rd</sup> Party Auditor

**June 10:** Hurricanes, Hackers, and #Hashtags

**July 15:** Strategies to Increase Supply Chain Resilience

**August 19:** Understanding the Facility Operations Maturity Model for Data Centers

**September 16:** Putting Agile into Performance Management

**October 14:** Crisis Management

**November 18:** Measuring Organizational Resilience