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
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 part of decision making
- Is systematic and structured
- Is the responsibility of management
- Addresses uncertainty
- 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


©2020 ICOR ALL RIGHTS RESERVED
WHO: Pandemic Influenza Risk Management (May 2017)

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

- **Preparedness**
  - of capacities for emergency risk management
  - Based upon what could happen (planning assumptions)

- **Assessments**
  - of risks and responses
  - Continuous processes using current and historical data

- **Response**
  - proportional to identified risks
  - Based on current event and available capacities

- **Prioritize areas of greatest need**

- **Recovery**
  - of systems and services
  - Based upon what happened

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

"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.

To what extent do you feel your national and local government was prepared to handle the COVID-19 pandemic?
The risk of a global pandemic has been realized.

What do we do now?
Managing Risk – What are you waiting for?!?

“It is time to understand best practice for managing risk.”

Benjamin Franklin
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 Context
- Risk Assessment
  - Risk Identification
  - Risk Analysis
  - Risk Evaluation
- Risk Treatment
- Communicate
- Monitor & Review

What may happen and why?
What are the impacts?
What is the probability or likelihood?
How to mitigate the impact or likelihood of the risk occurring?
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)

Risk Identification - Sources / Types of Risk

Strategic Risk

Compliance Risk

Operational Risk

Financial Risk

Reputational Risk

What might happen and why?

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
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

Methods of Failure Analyses - Examples

Fault Tree Analysis

SWOT Analysis

Failure Mode and Effects Analysis (FMEA)

©2020 ICOR ALL RIGHTS RESERVED
List Potential Risks

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

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

You’ll need some way of quantifying the impact the identified risks would have on your organization.
List the risks in order from greatest impact to least impact.
## Risk Analysis – List by Impact: Example

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

# Risk Analysis – List by Likelihood

<table>
<thead>
<tr>
<th>Scale</th>
<th>Likelihood</th>
<th>General Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
<td>Very Likely</td>
<td>Is expected to occur in most circumstances</td>
</tr>
<tr>
<td>B</td>
<td>Likely</td>
<td>Will probably occur in most circumstances</td>
</tr>
<tr>
<td>C</td>
<td>Possible</td>
<td>Might occur at some time</td>
</tr>
<tr>
<td>D</td>
<td>Unlikely</td>
<td>Could occur at some time in particular circumstances</td>
</tr>
<tr>
<td>E</td>
<td>Rare</td>
<td>May occur only in exceptional circumstances</td>
</tr>
</tbody>
</table>
# Risk Evaluation Criteria - Example

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

Increasing Likelihood

Increasing Level of Risk

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

<table>
<thead>
<tr>
<th>Advantages</th>
<th>Quantitative</th>
<th>Qualitative</th>
</tr>
</thead>
</table>
|            | • Allows for definition of consequences of incidents and allows the identification of costs and benefits during selection of mitigation choices  
• Provides a more accurate image of risk | • Allows for putting in order risks according to priority  
• Allows for determination of areas of greater risk in a short time without bigger cost  
• Analysis is relatively easy and cheap | |
| Disadvantages | • Depend on scope and accuracy  
• Must be enriched by qualitative descriptions  
• More expensive requiring greater experience and advanced tools | • Does not allow for determination of probabilities and results using numerical measures  
• Cost-benefit analysis is more difficult during selection of mitigation choices | |

There are many different risk evaluation techniques.
Qualitative Evaluation Example

<table>
<thead>
<tr>
<th>Likelihood</th>
<th>Insignificant (incident but no injury)</th>
<th>Minor (first aid injury)</th>
<th>Serious (serious injury / lost time)</th>
<th>Major Impact (death / disability)</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Very Likely</strong> (will most certainly happen)</td>
<td>Medium</td>
<td>High</td>
<td>High</td>
<td>Extreme</td>
</tr>
<tr>
<td>** Likely** (will probably happen at some time)</td>
<td>Medium</td>
<td>Medium</td>
<td>High</td>
<td>High</td>
</tr>
<tr>
<td>** Unlikely** (could happen sometime)</td>
<td>Low</td>
<td>Medium</td>
<td>Medium</td>
<td>High</td>
</tr>
<tr>
<td>** Very Unlikely** (might happen only rarely)</td>
<td>Low</td>
<td>Low</td>
<td>Medium</td>
<td>Medium</td>
</tr>
</tbody>
</table>
### Qualitative Method: NIST Methodology

#### Combining Qualitative with a Quantitative Measure

<table>
<thead>
<tr>
<th>Likelihood of Risk</th>
<th>Low (10)</th>
<th>Medium (50)</th>
<th>High (100)</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>High (1.0)</strong></td>
<td>Low 10 x 1.0 = 10</td>
<td>Medium 50 x 1.0 = 50</td>
<td>High 100 x 1.0 = 100</td>
</tr>
<tr>
<td><strong>Medium (0.5)</strong></td>
<td>Low 10 x 0.5 = 5</td>
<td>Medium 50 x 0.5 = 25</td>
<td>Medium 100 x 0.5 = 50</td>
</tr>
<tr>
<td><strong>Low (0.1)</strong></td>
<td>Low 10 x 0.1 = 1</td>
<td>Low 50 x 0.1 = 5</td>
<td>Low 100 x 0.1 = 10</td>
</tr>
</tbody>
</table>

#### Risk Scale:
- High = 51 to 100
- Medium = 11 to 50
- Low = 1 to 10
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**

Low Probability

High Impact
Options for risk treatment should be selected based on:

- Perceived vulnerability of the organization
- The urgency of the activity
- The cost of measures compared to benefits
- Overall feasibility and suitability of the option
- Risk Appetite
Types of Risk Treatment or Mitigation

- **Acceptance**: Leave the risk as it is.
- **Avoidance**: Cease or change the activity.
- **Transfer Risk to another part of the Organization or a Third Party**
- **Reduce: Control or mitigate**
- **Transfer - Financing / Insurance**
- **Remove Risk to Activity**

©2020 ICOR ALL RIGHTS RESERVED ICOR Webinar.46
Effectiveness of Controls

A control is anything that modifies risk.

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

Effectiveness of Controls

- **Most Effective**
  - Eliminate
    - Physically remove the hazard (can’t eliminate COVID-19)
  - Substitute
    - Replace the hazard (vaccination)
  - Engineering Controls
    - Isolate people from the hazard (social distancing)
  - Administrative Controls
    - Change the way people work (6 feet apart, scheduling, remote work)
  - PPE
    - Protect the worker with Personal Protective Equipment

## Control Effectiveness & Risk Levels

<table>
<thead>
<tr>
<th>Control Effectiveness</th>
<th>Level of Risk</th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Low</td>
<td>Medium</td>
<td>High</td>
<td>Extreme</td>
</tr>
<tr>
<td>Fully effective</td>
<td>9</td>
<td>8</td>
<td>2</td>
<td></td>
</tr>
<tr>
<td>Substantially effective</td>
<td>22</td>
<td>44</td>
<td>12</td>
<td></td>
</tr>
<tr>
<td>Partially effective</td>
<td>9</td>
<td>42</td>
<td>22</td>
<td></td>
</tr>
<tr>
<td>Largely ineffective</td>
<td>4</td>
<td>12</td>
<td>15</td>
<td></td>
</tr>
<tr>
<td>Totally ineffective</td>
<td>5</td>
<td>5</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Priority area for control improvement**


©2020 ICOR ALL RIGHTS RESERVED
Potential Exposure Measures

- Maximum monetary loss
- Impact to life safety / safety outcomes
- Impact to company brand and reputation

<table>
<thead>
<tr>
<th>Level of Risk</th>
<th>Potential Exposure</th>
<th>Control Effectiveness</th>
<th>Priority for Treatment</th>
</tr>
</thead>
<tbody>
<tr>
<td>High</td>
<td>High</td>
<td>Low</td>
<td>1</td>
</tr>
<tr>
<td>High</td>
<td>High</td>
<td></td>
<td>4</td>
</tr>
<tr>
<td>Low</td>
<td>Low</td>
<td>Low</td>
<td>2</td>
</tr>
<tr>
<td>Low</td>
<td>Low</td>
<td>Low</td>
<td>5</td>
</tr>
<tr>
<td>Low</td>
<td>High</td>
<td>Low</td>
<td>3</td>
</tr>
<tr>
<td>Low</td>
<td>High</td>
<td>High</td>
<td>6</td>
</tr>
<tr>
<td>Low</td>
<td>Low</td>
<td>Low</td>
<td>7</td>
</tr>
<tr>
<td>Low</td>
<td>High</td>
<td>High</td>
<td>8</td>
</tr>
</tbody>
</table>
# Risk Description Ties to Risk Strategy

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

©2020 ICOR ALL RIGHTS RESERVED

ICOR.Webinar.52
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 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

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.
   a. Fundamental design changes to accommodate for social distancing
   b. What travel modes and facilities are acceptable?
   c. Impact to commuting, car-pooling and ride sharing?

6. **Prepared.** Time to get prepared – finally?
   a. Planning, training, and practice required – including supply chains
   b. New / updated policies and practices
   c. Robust IT systems
   d. Stockpiles of PPE and other essentials
   e. 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

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

Build-Resilience.org
ICOR 2020 Webinar Series

May 27: Insights from an ISO 22301 3rd 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

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

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