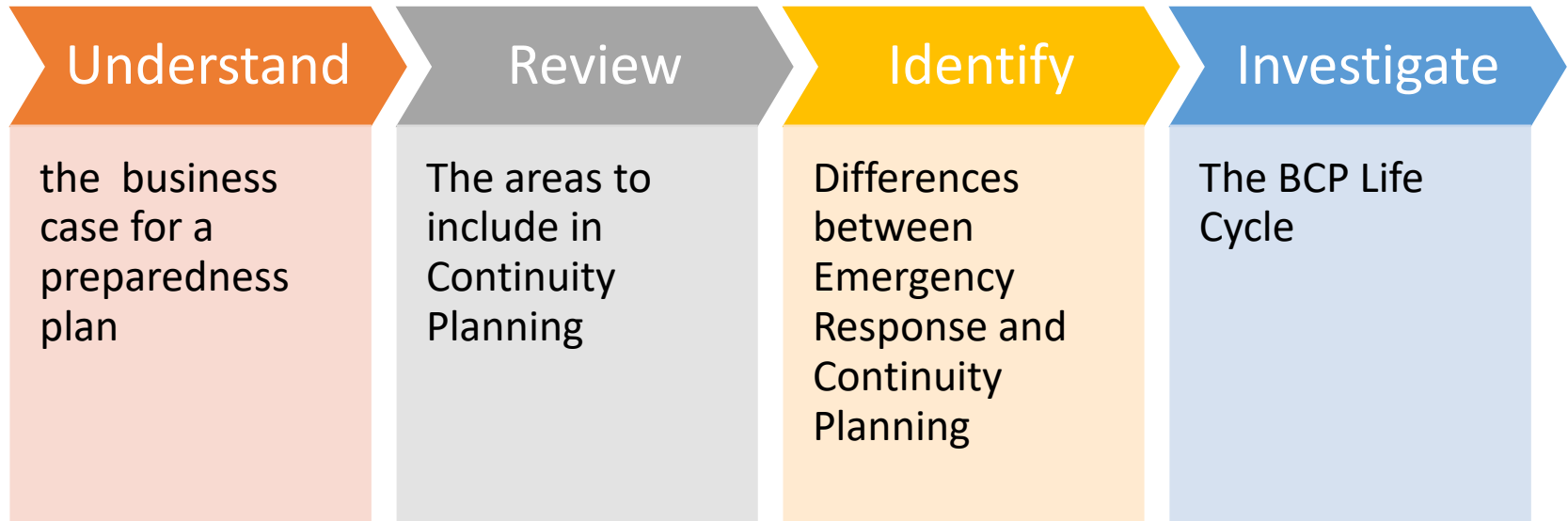


Business  
Continuity  
Planning and  
Risk Assessment  
Sharon Justice

---



# Objectives



---

# What is Business Continuity Planning?

---

It helps to

- anticipate,
- prepare for,
- prevent,
- respond to,
- recover
- survive

disruptive events affecting daily operations.

Think of all the things  
that can disrupt your  
business

---

Make a quick list

---



Why do we need BCP?



Make It Before  
You Need It

10% (or more) of businesses do not  
recover

It should include:

---

People

---

Facilities

---

Data

---

Suppliers

---

Policies and Procedures

---

Other unique areas







If you said “I wish I had...”





## ERP vs BCP

---

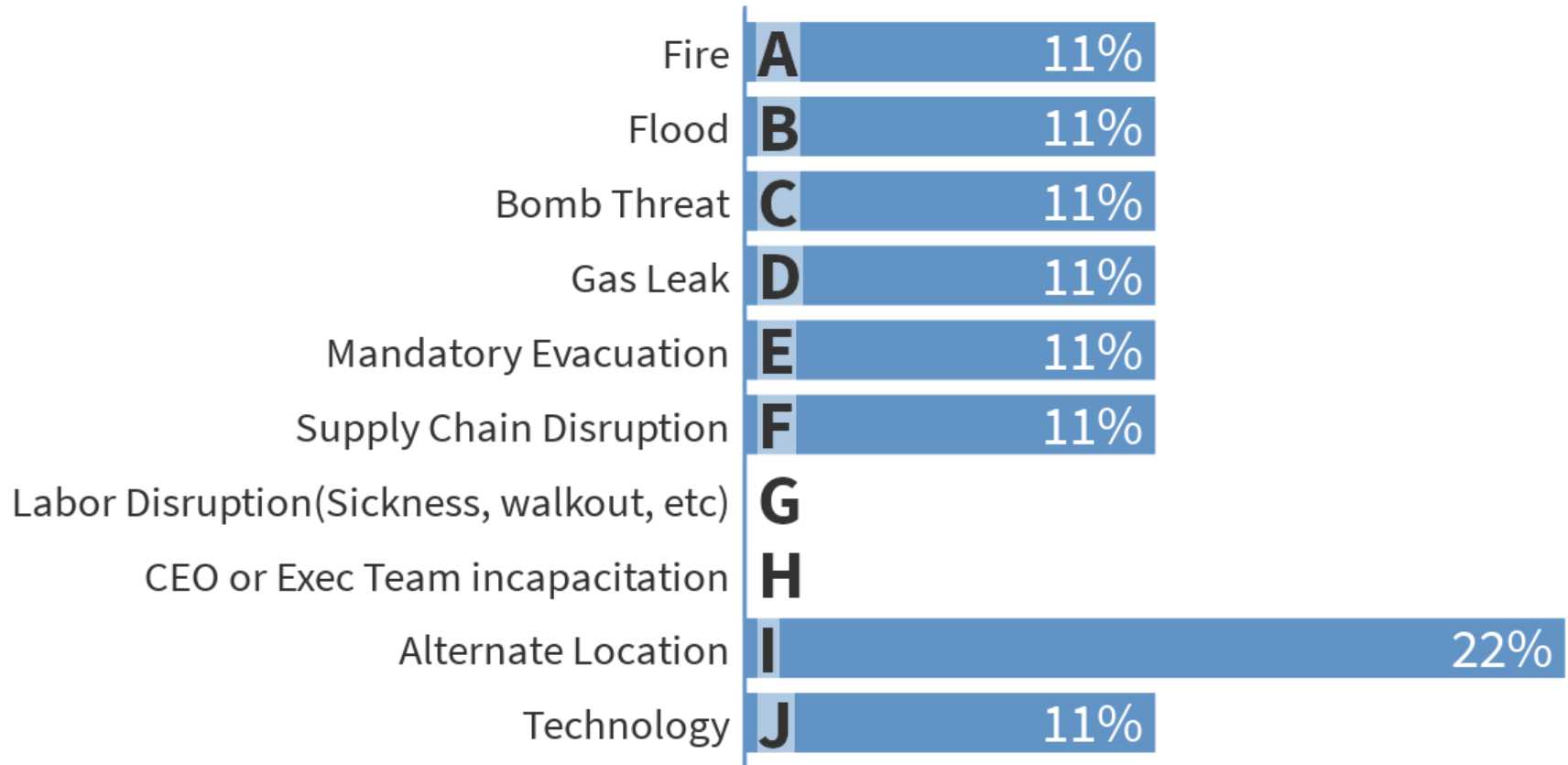
- Emergency Response: Focused on Preparedness and Response
- BCP: primarily a mitigation and recovery plan

“ a course of action that your organization would take if an unexpected situation occurs”

Business Continuity Planning

# I have Business Continuity plans in place for:

## Choose as many as apply







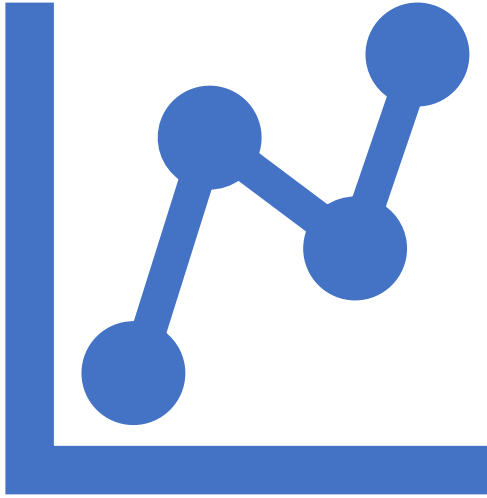
# Defining Business Continuity Planning Objectives

- What is the goal and focus of your BCP?
- What is the scope of your BCP?
  - Will it cover the entire company or organization or just one location?



# Defining Business Continuity Planning Objectives

- What kind of events will your BCP address?
  - Define each event and the projected impact
  - Identify any Assumptions that are made

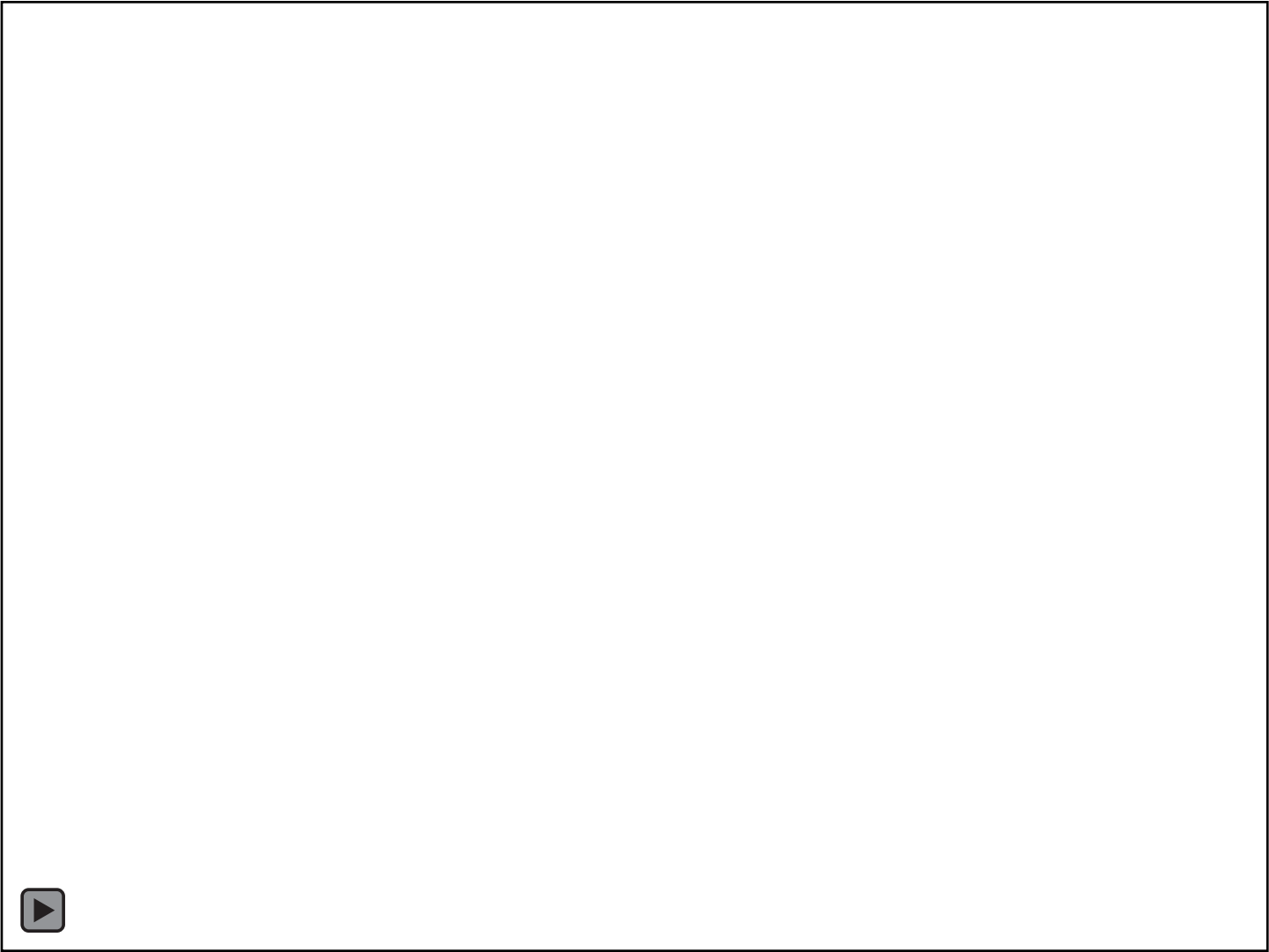


Analyze



# Business Impact Analysis

Analyzing your Business



### **Business Impact Analysis**

- Develop questionnaire
- Conduct workshop to instruct business function and process managers how to complete the BIA
- Receive completed BIA questionnaire forms
- Review BIA questionnaires
- Conduct follow-up interviews to validate information and fill any information gaps



### **Recovery Strategies**

- Identify and document resource requirements based on BIAs
- Conduct gap analysis to determine gaps between recovery requirements and current capabilities
- Explore recovery strategy options
- Select recovery strategies with management approval
- Implement strategies



### **Plan Development**

- Develop plan framework
- Organize recovery teams
- Develop Relocation Plans
- Write business continuity and IT disaster recovery procedures
- Document manual workarounds
- Assemble plan; validate; gain management approval



### **Testing & Exercises**

- Develop testing, exercise and maintenance requirements
- Conduct training for business continuity team
- Conduct orientation exercises
- Conduct testing and document test results
- Update BCP to incorporate lessons learned from testing and exercises



# Getting Started: Risk Assessment and Management

Ignoring Risks=Disaster

---



Seek Out  
Problems  
Before  
They  
Happen

Prevent when  
possible

Be prepared to  
respond when  
they happen



# Key Risks

Human

Operational

Technical

Financial

Security

Communication



## Unique to Your Business

- Physical Risks
- Human Risks
- Technology Risks
- Location Risks

# Walk Around: Physical Risks

---

- How tools are used
  - Different methods used to complete tasks
  - Materials used
- 





## Human Risks

---

- Safety protocols
- Labor availability
- Sickness
- Walkout
- Changing Skills required
- Succession Planning





**Growth**

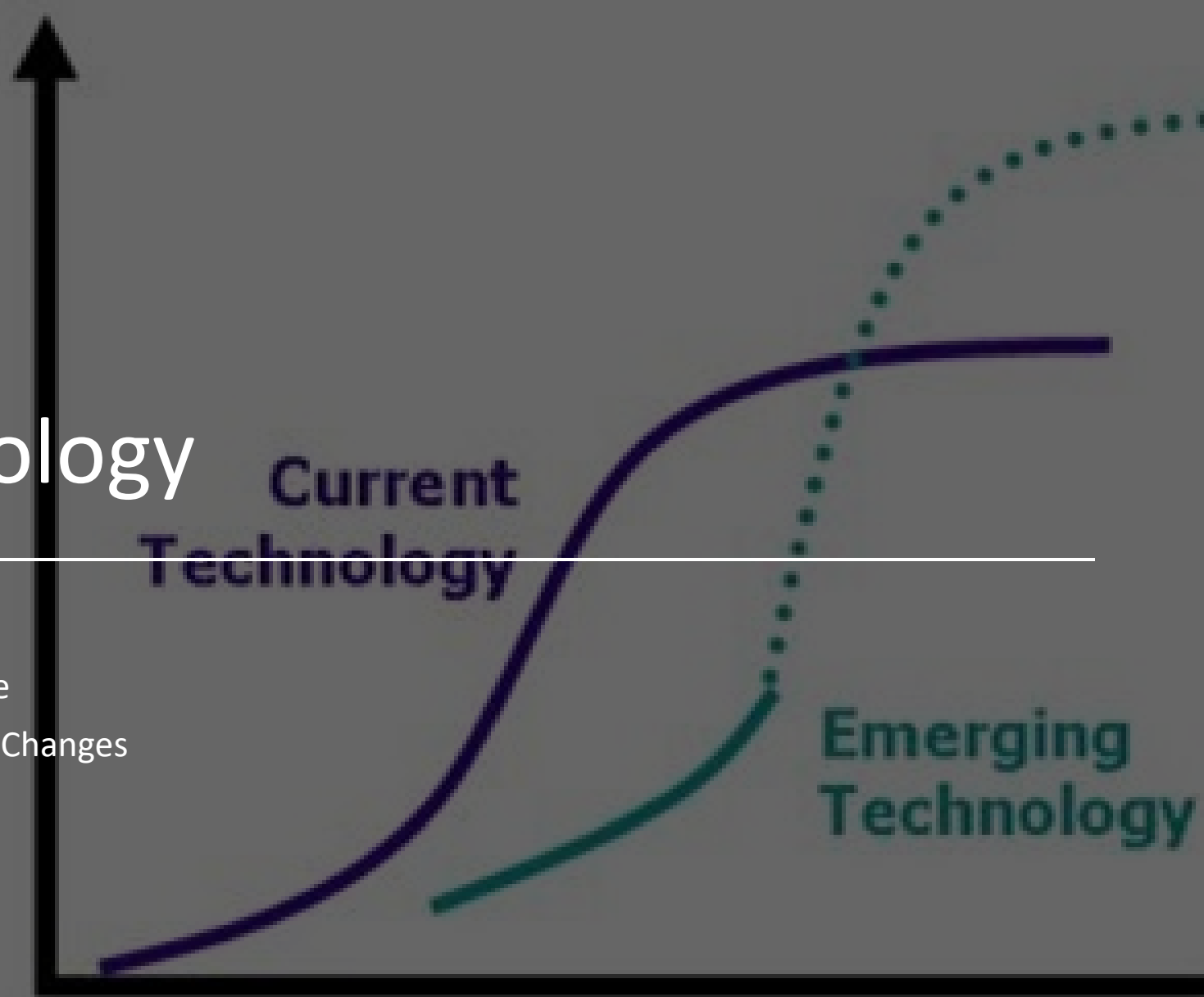
# Technology

- Hackers
- Ransomware
- Technology Changes

**Current  
Technology**

**Emerging  
Technology**

**Time**





---

## Location, Facility and Equipment

---


- Near a river or Coast/Hurricanes
- Fire Prone Area
- Snow, Power Outages
- Specialty Equipment, Ventilation
- Waste Disposal



# Beginning the Risk Assessment

---

- What is your “early warning system” for identifying business risks?
- What is your cross-business/cross-function risk assessment process to identify, assess, and prioritize events with consequences that impact operations?
- What is your process for making decisions regarding identified risks for recommended mitigation, and transferring or accepting risk (insurance – assess property risks, etc.)?
- How does the business report these risk assessment findings and plans to your senior leadership?



---

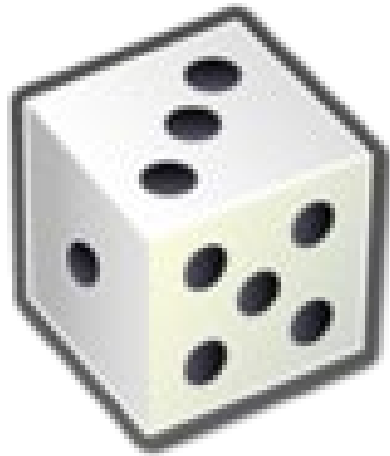
## Ask “What would happen if ... ?” Impact Scale

---

- Low Impact
- Medium Impact
- High Impact



# Probability Scale



- 0 – Impossible
- 1 – Remote possibility
- 2 – Medium possibility
- 3 – Probable



## Control Scale

---

- 1 – Total control
- 3 – Some Control
- 5 – Total Control

A close-up, black and white photograph of a computer keyboard. The focus is on a key labeled 'control'. The background is dark and blurred, showing other keys like 'on' and 'off'.

control



- **Probability Scale:** The likelihood that an event will occur.
- **Business Impact Scale:** The degree to which the event will affect your business
- **Control Scale:** How much control you have in preventing the event.

### Probability Scale

1 – 2 – 3 – 4 – 5

Low.....High

### Business Impact Scale

1 – 2 – 3 – 4 – 5

No Impact.....High  
Impact

### Control Scale

1 – 2 – 3 – 4 – 5

Good.....Poor



Create a threat matrix to identify possible risks.

Use this information to populate your risk assessment table.

<b>NATURAL THREATS</b>	<b>MAN MADE THREATS</b>	<b>TECHNOLOGICAL THREATS</b>
<b>TORNADO</b>	<b>SABOTAGE</b>	<b>POWER FLUCTUATION/OUTAGES</b>
<b>HURRICANE</b>	<b>RIOT/CIVIL DISTURBANCE</b>	<b>EQUIPMENT FAILURE</b>
<b>SEVERE THUNDERSTORMS</b>	<b>THEFT/VANDALISM</b>	<b>HVAC FAILURE</b>
<b>BLIZZARDS/ICE STORMS</b>	<b>TERRORISM</b>	<b>LOSS OF COMMUNICATIONS</b>
<b>TSUNAMI</b>	<b>BOMB</b>	<b>LOSS OF DATA</b>
<b>DROUGHT</b>	<b>PRODUCT TAMPERING</b>	<b>VIRUSES, MALWARE, HACKER ATTACK</b>
<b>HEAT</b>	<b>WORKPLACE VIOLENCE</b>	<b>LOSS OF INSTITUTIONAL KNOWLEDGE</b>
<b>PANDEMIC</b>	<b>UNAUTHORIZED RELEASE OF CONFIDENTIAL INFORMATION</b>	
<b>EARTHQUAKE</b>	<b>FIRE</b>	
<b>FLOODING</b>	<b>DISGRUNTLED EMPLOYEE</b>	

# Threat Matrix

Threat	Probability Scale	Business Impact	Control Scale	Ideas for mitigation



# Developing the BIA



Determine mission/business processes and Recovery criticality.



Identify resource requirements.



Identify recovery priorities for system or business resources.

# RTO: Recovery time Objective

Business Unit	Manager	Process	RTO	Daily Loss	Function	Risks	Comments

Department / Function / Process \_\_\_\_\_

### Operational & Financial Impacts

Timing / Duration	Operation Impacts	Financial Impact

**Timing:** Identify point in time when interruption would have greater impact (e.g., season, end of month/quarter, etc.)

**Duration:** Identify the duration of the interruption or point in time when the operational and or financial impact(s) will occur.

- < 1 hour
- >1 hr. < 8 hours
- > 8 hrs. <24 hours
- > 24 hrs. < 72 hrs.
- > 72 hrs.
- > 1 week
- > 1 month

Considerations (customize for your business)

**Operational Impacts**

- Lost sales and income
- Negative cash flow resulting from delayed sales or income
- Increased expenses (e.g., overtime labor, outsourcing, expediting costs, etc.)
- Regulatory fines
- Contractual penalties or loss of contractual bonuses
- Customer dissatisfaction or defection
- Delay executing business plan or strategic initiative

**Financial Impact**

Quantify operational impacts in financial terms.

Business Unit	Manager	Process	RTO	Daily Loss	Function	Risks	Comment
Finance	Joe	A/P	>48	\$1237	Pay Bills	1, 3, 4, 7, 8	Discuss telework policy & VPN solution, online banking?
Finance	Pete	A/P	>48	\$1275	Invoice	1, 3, 4, 7, 8	Discuss telework policy & VPN solution, online banking?
Finance	Erika	Payroll	>72	\$943	Payroll	1, 3, 4, 7, 8, 9	Discuss potential manual work-around procedures/paper check supplies and timesheets
HR	Mary Sue	Recruitment	>72	\$847	New Hires	1, 8, 9	Discuss possibility of contract with temp agency
Production	Fred	Widget Mfg	>60	\$10500	Product Assembly	1, 3, 4, 7, 8, 9	Discuss alternate supplier, surplus inventory
Production	Sara	Paintshop	>72	\$2345	Finishing	1, 3, 4, 7, 8, 9	Discuss piecework contract with Paintco. Surplus inventory?
<Enter your BIA Information here>							

# Address the following basic components of BCP

Triggers: what would set your plan in motion

Leadership: Who is in charge and how do they interact

People: Org charts, contact info, critical information

IT: What will it take to keep or recover critical functions

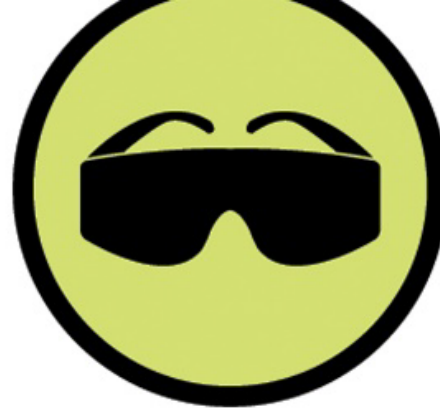
Customers

Vendors: Disruptions on their end

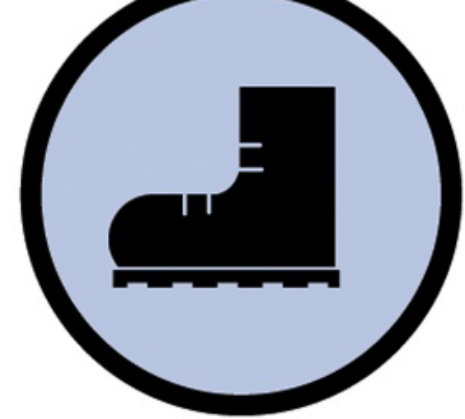
Communication: How, when, to whom



Gloves



Glasses



Closed-Toe  
Shoes

## Long Term and Short Term

- Immediate consequences
- Long term can be easy to miss
- Develop over time





# Fire claims supplier of Bill's Hot Dogs

HOW HAVE  
YOUR PLANS  
CHANGED?



By Vail Stewart Rumley  
Email the author

Published 8:17 pm Friday, June 1, 2012





HOME

HAPPENINGS

NEED2KNOW

OUR PEOPLE

PROJECTS

SAFETY



**Crystal:** I started Sept 27, 1999: I couldn't get past the national guard. My supervisor made me a temporary badge by taking a photo of me standing outside the entrance of the plant, laminating it, and somehow putting a GUC logo on it. I still have that makeshift badge today and will probably always keep it.

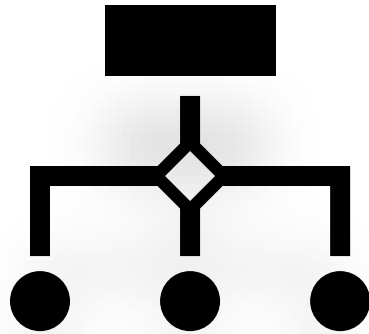
- **Randy Emory, Director of Water Resources** (*Assistant Director during Floyd*):
  - “Most of us here at the time were veterans of dealing with hurricanes, so we were pretty in tune with what to do. But it turned out to be something none of us had ever seen.



# External Events

- Suppliers
- Customers
- Visitors
- Traffic, Transportation
- Environment
- Others?





Identify  
the right  
people



# Key Roles

---

CEO

COO

CTO/CIO

CFO

CHRO

Marketing

Communication

Security



# Disaster Recovery Plan

- Unique to each process (and type of event)
- Outlines Procedures in event of disaster and loss mitigation

What one word describes  
your overall preparedness if  
a disaster were to hit today?



R<sub>1</sub>

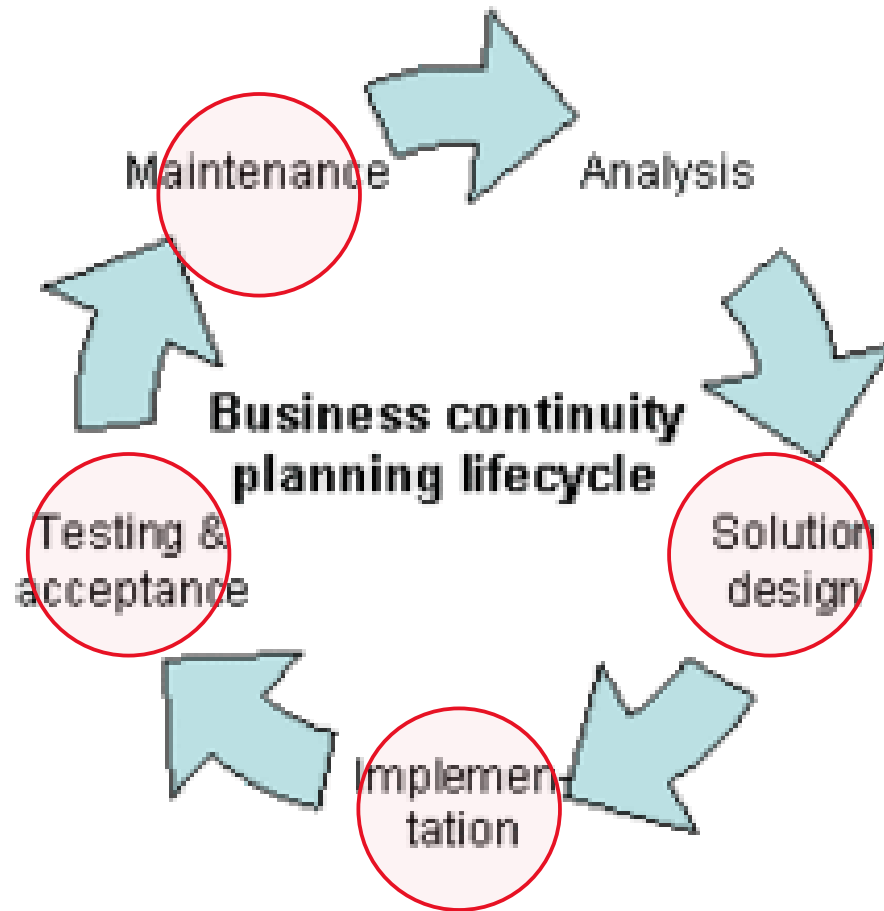
E<sub>1</sub>

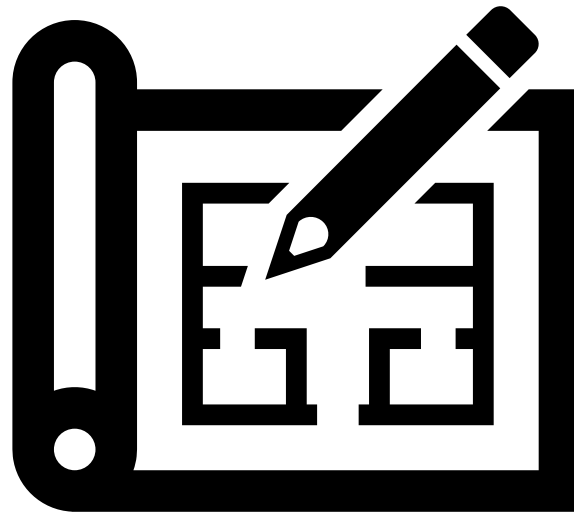
A<sub>1</sub>

D<sub>2</sub>

Y<sub>4</sub>







# Solution Design



# Define your objective for Business Continuity planning



ENSURE CONTINUITY  
OF OPERATIONS  
DURING CRISIS



ENSURE EMPLOYEE  
SAFETY DURING CRISIS



ENSURE CONTINUITY  
OF KEY IT SYSTEMS



MINIMIZE CUSTOMER  
IMPACTS FROM  
BUSINESS DISRUPTION



MINIMIZE REPUTATION  
DAMAGE FROM AN  
INCIDENT



# Planning for Success

---



ORGANIZATIONAL  
ENGAGEMENT



EXECUTIVE  
SUPPORT



ADEQUATE  
RESOURCES



TEAM  
DEDICATION



# Solution Design

7 Mistakes to Avoid

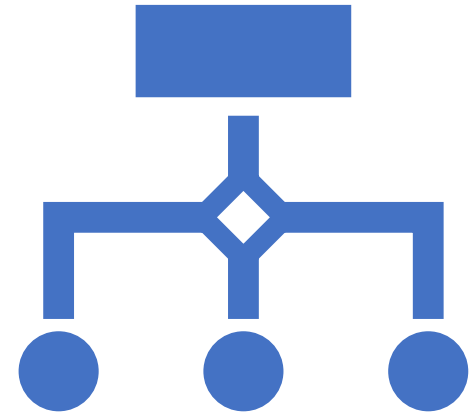


## #1 Overlooking Essential business functions and failing to identify associated risks

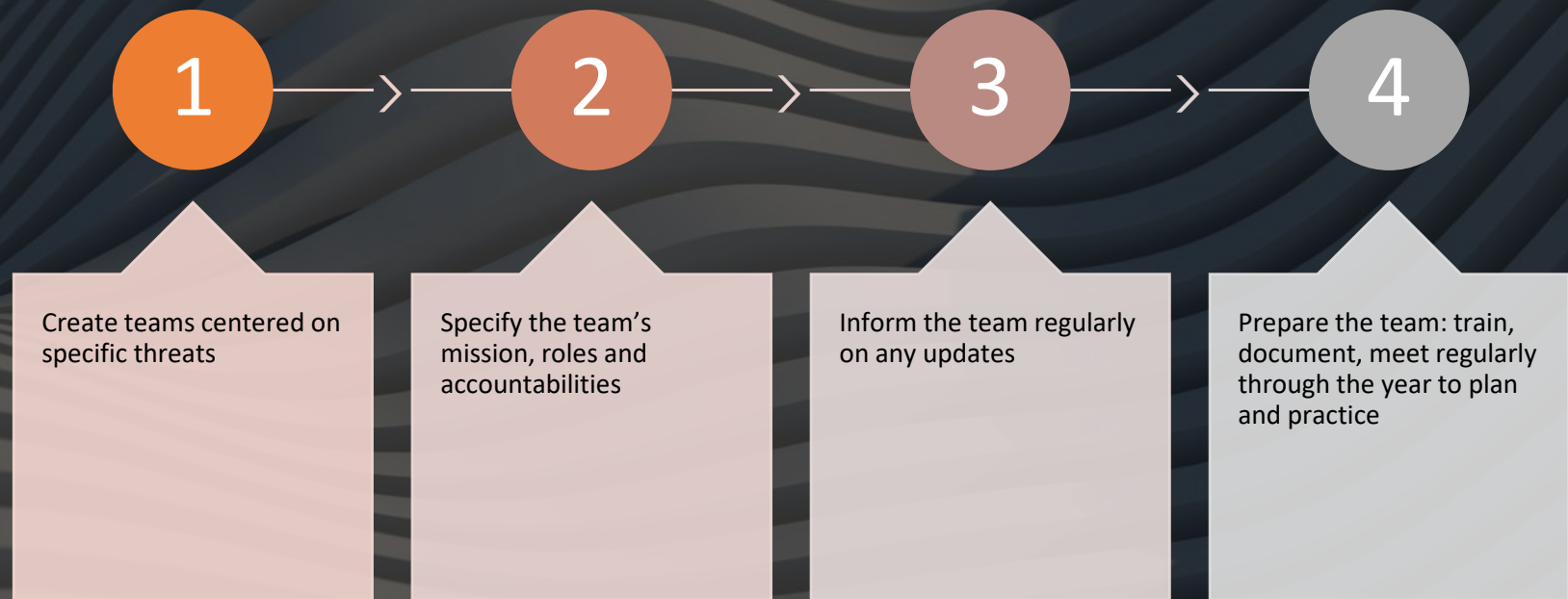
- Get Buy in from the top
- Incorporate feedback from multiple sources
- Document the details in your Threat matrix
- Make all solutions actionable: Provide clear steps of action to take

## #2 Failing to implement a process for accurate and reliable contact info

- Everything starts with people
  - Develop a consistent process to allow workers to validate and update information
  - Capture external information too! Don't forget vendors, key partners, stakeholders, board members, and others.



# #3 Failing to clearly define key teams and communicate assigned roles and duties







# Business Continuity Plan Generator

Help Resources Sitemap Print

Chapter 3 of 4, Section 1 of 7, Page 9 of 9

0% Complete

Back Forward Mark Complete and Forward

## Chapter 3 - Plan Administration and Maintenance

### 3.1 Functional Teams and Responsibilities (page 9)

#### Pre-disaster responsibilities

	Human Resources Team Responsibilities
<Insert N...	<Insert Team Responsibilities here>

#### Post-disaster responsibilities

	Human Resources Team Responsibilities
<Insert N...	<Insert Team Responsibilities here>

## #4 Insufficient orders of succession and lack of clear delegations of authority

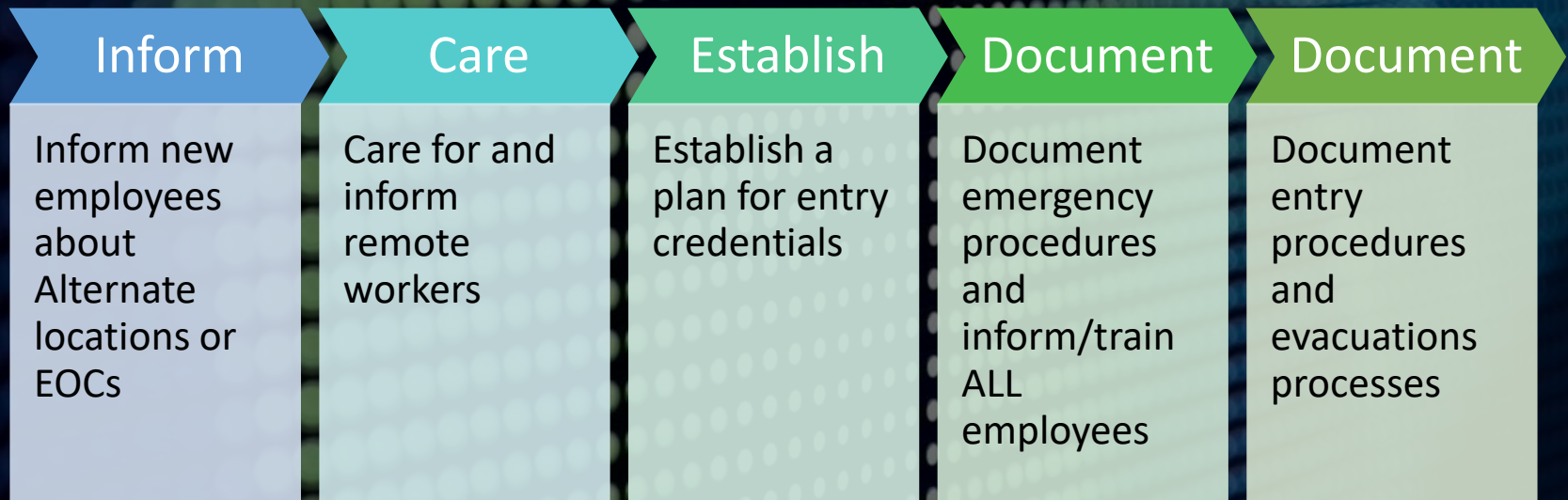
- Define and Document orders of succession.
  - Key leaders can be unavailable or incapacitated
  - Go at least 3 levels deep (more is advisable)
    - Use titles, and not employee names in the succession document.
  - Document Delegations of Authority





# #5 Failing to maintain accurate and detailed facility information

---



## #6 Failing to document vital records and critical systems

---



**Determine what is “vital”**



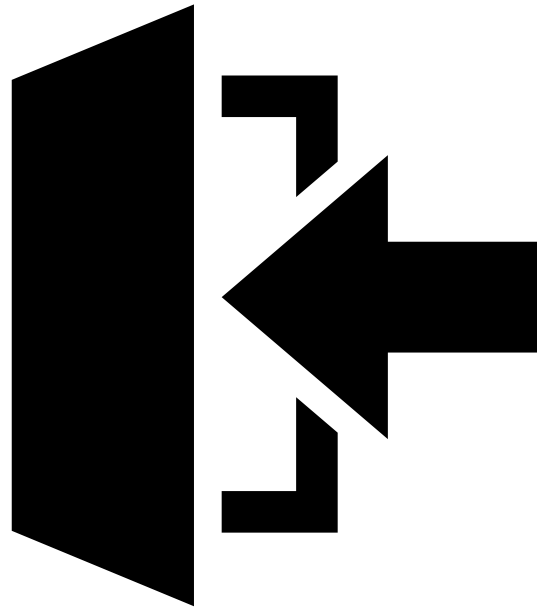
**Capture relevant details about the critical data source and storage**

Identify:

- Physical location for hard copies
- Share drive locations
- Local software applications
- Software service solutions—Administrator/Vendor information
- Network resources (printers, fax, etc)

# #7 Failing to make your BCP data accessible, editable and secure

- Avoid Binders on a shelf
- Consider online planning and Cloud storage and accessibility
- Maintain Security



Implement Plans



# Executive Support

Identify an Executive Sponsor

# Build employee awareness

01

Include in employee on-boarding or new hire training

02

Post information, boards, intranet,

03

Create campaigns

04

Design training events, lunch and learn





Evaluate  
Resources

---

People

---

Time

---

Money

---

Resources

---

Tools

# Establish Accountability

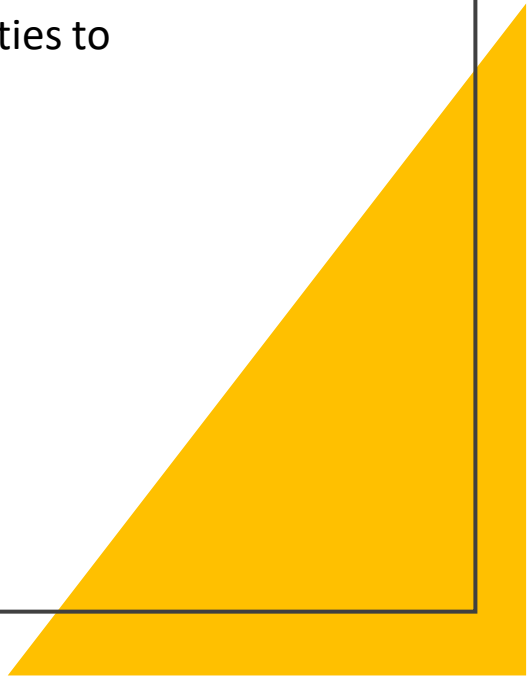
Dedicated Team

Decentralized,  
part time  
accountability



# Design Solutions for Recovery Plans



- Long Process
  - Identify short term activities to show progress
- 



## Keep Documentation Simple and Clear

---

- Keep it simple
- Roles and responsibilities
- Contingency/Redundancy procedures

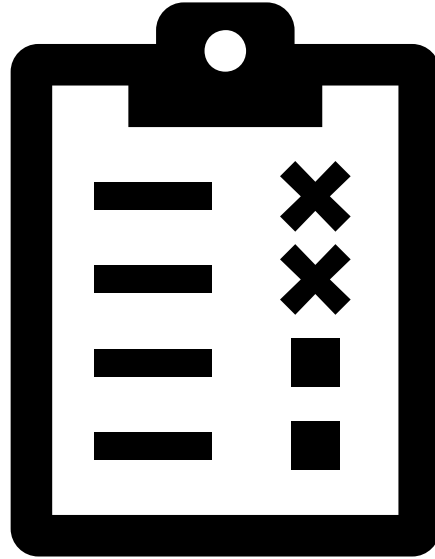




# Implement Recommendations

- Review recommendations
- Confirm commitment from participants
- Schedule the implementation process





Testing



## Test, Update, and Repeat

- Determine objectives
- Collect results
- Evaluate results
- Update the plan

# TRAINING



This Photo by Unknown Author is licensed under [CC BY-SA](#)

Train on the plan





College of Business - Home  
<https://collab.ecu.edu/sites/PRODCOB/SitePages/Home.aspx>

## Business Continuity Plan Test

Exercise Planner Instructions

Facilitator & Evaluator Handbook

Situation Manual

Presentation

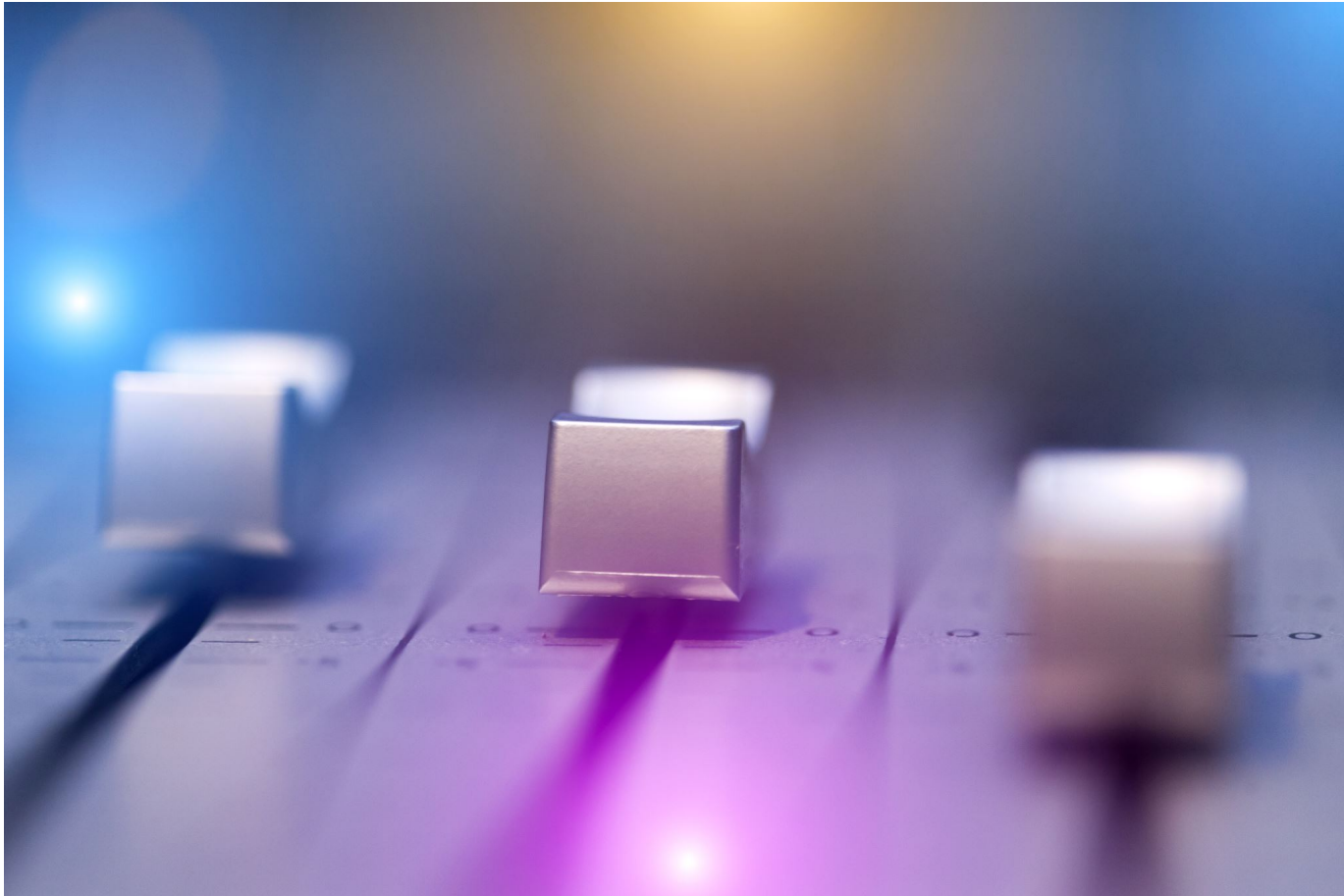
Participant Feedback Form

[Return to Main Menu](#)



Maintenance

# Maintenance: Learn and Adjust

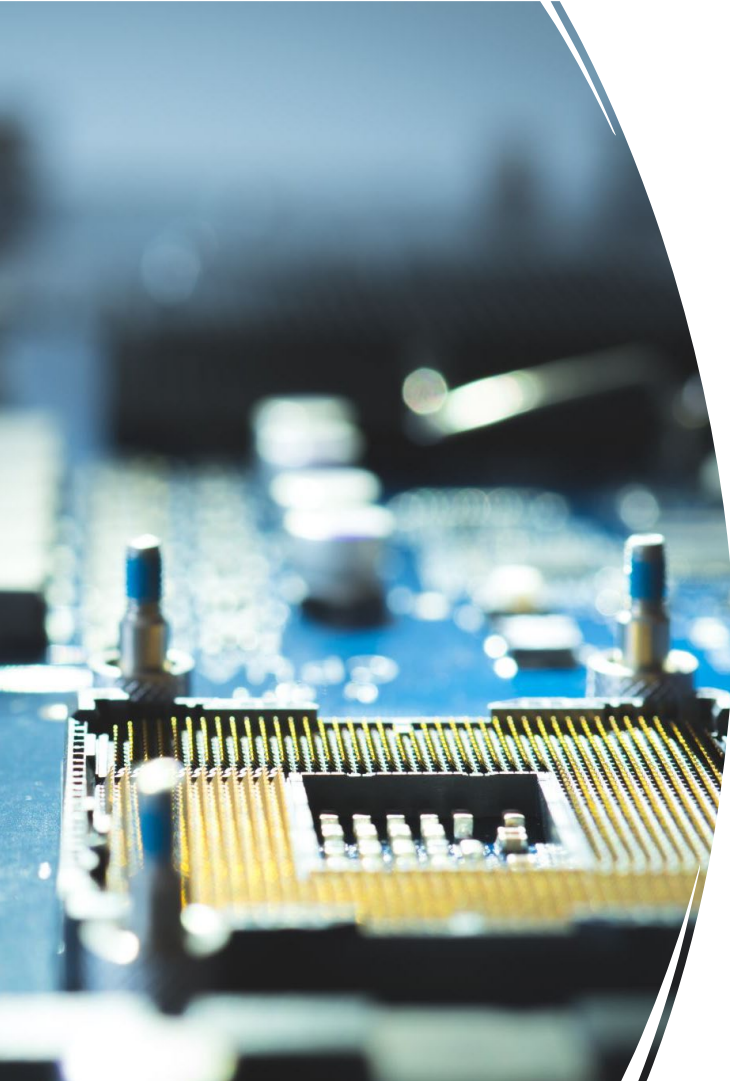




# Success Factors

---

- Include Risk assessments and review and update annually
- Utilize the Business Impact analysis as a key element of BCP
- Review BCP plans annually
- Conduct frequent simulation and testing



# Utilize Tools and resources

---

- Online tools or systems
- Consultants or Advisors
- Industry Experts and Associations
- Ready.gov
- Insurance Advisor or Agents
- Software or Business solutions vendors

What vulnerabilities  
have you thought  
about today?

