



# Business Continuity and the Business Impact Analysis

---

**Anthony Hurley**, MEP, CPP®, PCI®, PSP®, CPD  
Consultant, Critical Preparedness, LLC  
[www.CriticalPreparedness.com](http://www.CriticalPreparedness.com)



# Agenda



# Agenda

- Speakers / Abstract Introduction
- Terminology
- Business Continuity Overview
- Business Continuity Failures
- Business Impact Analysis (BIA)
- Plan Development
- Exercises



# Anthony Hurley, MEP, CPP®, PCI®, PSP®, CPD



- Thirty-seven (37) years in the electric utility industry (retired VP of Operations)
  - Post-retirement: Four (4) years as a Consultant
    - Worked with clients across Continental U.S., Alaska, Caribbean and the Middle East
- Former Vice-Chair, New Jersey Homeland Security and Preparedness, Infrastructure Advisory Committee (IAC)
- Adjunct Instructor, NYU, School of Professional Studies, Infrastructure Security and Resilience
- Adjunct Instructor, FEMA Emergency Management Institute (EMI)
  - *Master Exercise Practitioner (MEP)*
  - *Master Continuity Practitioner*
  - *Certified Instructor, Incident Command System (ICS)*
- American Society of Industrial Security (ASIS)
  - 'Triple Crown' Recipient (250 in the world as of 1Q 2021)
    - *Board certified as a Certified Protection Professional (CPP®)*
    - *Board certified as a Professional Certified Investigator (PCI®)*
    - *Board certified as a Physical Security Professional (PSP®)*
- Graduate, FBI Citizen's Academy (Cleveland Field Office)





# Session Abstract



# Session Abstract

“Business Continuity (BC) planning is the process of creating processes and systems to enable the recovery to a potential threat, or incident to an organization. The goal is to enable ongoing operations before and during the execution of disaster recovery.

Presenter will highlight the Business Continuity process, with emphasis on the Risk Assessment and the Business Impact Analysis (BIA).

Speaker will demonstrate the guidelines for Strategy & Plan Development, how to Test, Train & Maintain your Business Continuity plans.”





# What You'll Learn (Deliverables)



# What You'll Learn (Deliverables)

- Get a guideline(s) for Strategy & Plan Development
- Checklist to Test, Train & Maintain your Business Continuity plans
- Recordings of all sessions
- Transcripts of all sessions
- Directories of Vendors / Suppliers
- Speaker contact information
- AHC Membership





# Phases of Business Continuity

# Phases of Business Continuity

## Business Continuity Lifecycle

- **Risk Assessment** - A product or process which collects information and assigns values to risks for the purpose of informing priorities, developing or comparing courses of action, and informing decision making.
- **Business Impact Analysis** - A method of identifying the consequences of failing to perform a function or requirement.
- **Strategy & Plan Development** – Activity that evaluates the Risk Assessment and Business Impact Analysis to document actions that will be taken that support the resumption of normal functions.
- **Test, Train & Maintain** - Activities designed to familiarize, enhance skills, and ensure viability of continuity plans. Aids in verifying that an organization's continuity plan is capable of supporting the continued execution of the organization's essential functions throughout the duration of a continuity plan activation.







So why is Business  
Continuity important?

# POLL SLIDE

Per FEMA, what percentage of small businesses never reopen after a disaster?

- A: 5%
- B: 18%
- C: 25%
- D: 40%



# POLL SLIDE

Per FEMA, what percentage of small businesses never reopen after a disaster?

- A: 5%
- B: 18%
- C: 25%
- D: 40%



# Is Business Continuity Important?

According to **FEMA**;

- 40% of **small businesses** never reopen after a disaster, and another 25% that do reopen, will fail within a year. It is not only important to that business' bottom line and to its employees to get back in business, but it is also important to the community.
- Following a disaster, 90% of smaller companies fail within a year unless they can resume operations within 5 days.





What exactly is  
Business Continuity?

# What is Business Continuity Planning?

- Business Continuity Planning is the creation of processes and systems for the prevention and recovery to deal with potential threats to a company, and seeks to minimize business interruptions, both planned and unplanned. These threats can be natural, human-caused or malevolent acts.
- Business Continuity Plan (BCP) includes:
  - Risk Assessment (Hazard Vulnerability Assessment or HVA)
  - Business Impact Analysis (BIA) to identify staff analysis, essential business functions, and maximum tolerable downtime.
  - Recovery Strategies & Interim Processing procedures to guide the organization from minimal business functions back to resumption of normal business functions
  - Staff Roles, Functions, and Actions throughout the disaster recovery process



# TEMPLATE Risk Assessment

(Hazard Vulnerability Assessment or HVA)

- What are the components of an XXX?
- What's important
- Where do I start
- Where are some resources/tools I can learn more about XXX?
- Checklists, sample plans & approaches, etc....
- What groups can I join? (Internal and External)
- In future course, we will develop a deeper dive into these complex areas



# What is the goal of Business Continuity?

- To proactively plan to avoid and mitigate risks including:
  - Minimize the effect of a disruption on an organizations business operations
  - Reduce the revenue at risk
  - Safeguard organizations brand and image and give employees, customers, suppliers and shareholders confidence in the organization's services
  - Provide data to enable the recovery of critical systems within an agreed timeframe
  - Meet legal, regulatory, statutory requirements
  - Satisfy credit rating agencies
  - Prepare employees to respond effectively during a business interruption
  - Meet insurance requirements
  - Support the overall recovery of the community





# Terminology



# Terminology

- **Alternate Work site** – A location where you can work if your building is damaged and uninhabitable.
- **Business Continuity Planning** – Creation of processes and systems to enable the recovery to potential threats or incidents to an organization. The goal is to enable ongoing operations before and during the execution of disaster recovery.
- **Business Impact Analysis (BIA)** – An evaluation of how an organization's business functions and resources will be impacted by the various disaster scenarios identified in the Risk Assessment.
- **Business Interruption** – An event, whether anticipated (hurricane, protests), or unanticipated (outage, attack), which interrupts the normal course of business operations.
- **Crisis** – Unexpected, complex event, which has the potential to impact an organization. Requires cross-functional and senior management engagement.
- **Crisis Management** – A proactive operating capability to respond to and recover from an event, series of events, or circumstances that threaten to negatively impact an organization.
- **Enterprise Resiliency** – When a sudden disruption occurs, having the competence to react, respond and adjust to ensure that an organization survives, and ensures their ongoing success.
- **Essential business functions** – Critical business processes/work functions that are the core of running your organization (IT, Payroll, AR/AP, etc.)
- **Incident** – Localized event that has limited impact on an organization, and is managed locally, using established procedures (does not involve senior management).
- **Risk Assessment** - Process of evaluating potential hazards, identifying gaps and challenges, and prioritizing the outcomes (aka HVA)
- **Succession planning** - Process to identify which staff members are trained in positions to support staff redundancy.





Business Continuity  
Planning is NOT ...

# Business Continuity Planning is NOT ...

- A guide to operate your organization 'business-as-usual'
- A massive and cumbersome set of documents that is meant to be referenced to during a disaster
- A crystal ball that can identify every possible scenario





# Recovery Steps addressed by a BCP



# Recovery Steps addressed by a BCP

- **What** are we recovering?
- **Why** are we recovering?
- **Who** is responsible for recovery?
- **When** do / can we recover?
- **Where** will we recover?
- **How** will we recover?

*An organization's resistance to failure is "the ability to withstand changes in its environment and still function". Often called resilience, it is a capability that enables organizations to either endure environmental changes without having to permanently adapt, or the organization is forced to adapt a new way of working that better suits the new environmental conditions.*





# Challenges to Business Continuity



# Challenges to Business Continuity Implementation

- Lack of senior management support (commitment involvement)
- Incorrect assumptions in creating Business Continuity and Disaster Recovery plans
- Incorrect assumptions on organizations existing readiness status
- Budget restraints
- Lack of Business Continuity awareness
- Lack of time and resources
- Employee turnover
- Conflicting priorities
- Internal culture not focused on readiness
- No relationship with critical partners
- Tools and resources
- Attitude that *“it will never happen to us”*



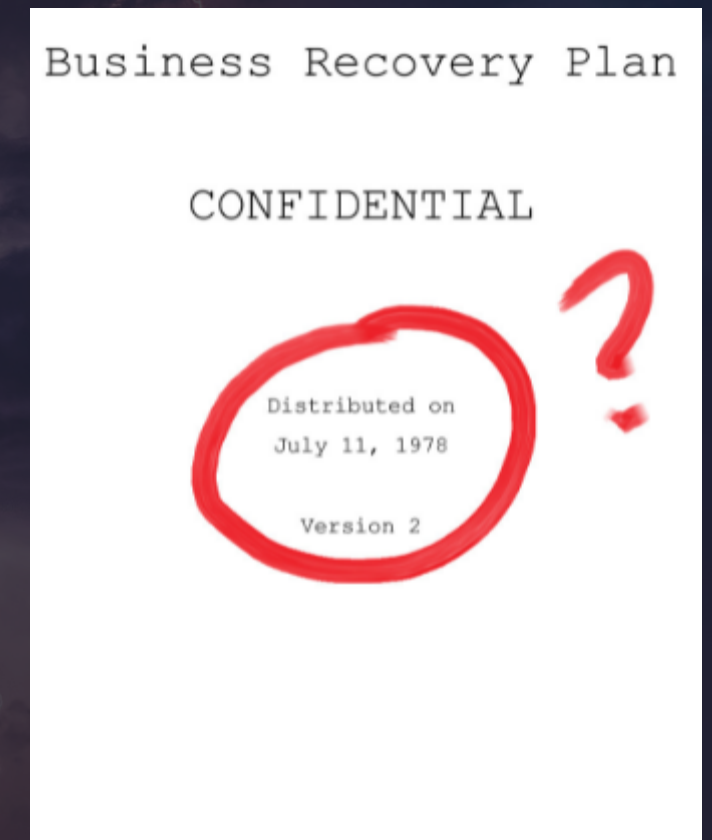


# Business Continuity Failures



# Traditional Reasons for Business Continuity Failures

- No Business Continuity plan developed
- No Business Impact Analysis conducted
  - Failure to develop a system or process recovery prioritization list
- No Risk Assessment conducted
- No Communications Plan created
- Existing Plan has incomplete list of Risks
- Existing Plans were never updated
- Failure to identify or fund mitigation projects
- Failure to communicate Business Continuity Plan
- Failure to train staff on the plan, expectations and their roles
- Failure to exercise plans





# Planning Failure – Facility Design

- Critical Infrastructure Owner/Operator
  - Constructed an EOC to be used for hurricane recovery operations
  - Building designed to withstand a specific Category of hurricane
  - Equipped each cubicle with a desktop computer and landline
  - Hardwired communications lines and had microwave backup communications
  - Installed a back generator in basement
  - Installed server room in basement
  - Created EOC Standard Operating Procedures (SOP)
  - Trained staff on their roles and responsibilities
- **First Event: EOC hit by a hurricane with winds higher than the design criteria. Windows were blown in, staff were injured, and water came into the building. Basement flooded, generator and servers failed.**
- **Failure: Reduced design criteria / critical equipment in basement**
- **Solution: Build to the maximum identified hazard / Consider all risk profiles**



# Planning Failure – Facility Selection

- Critical Infrastructure Owner/Operator
  - Identified a need to locate critical electrical / mechanical parts near the coast.
  - Selected a building that was central to their most vulnerable assets, where parts would most likely be needed after a hurricane.
  - Facility and storage building also housed specialized vehicles and personnel that were essential to the restoration of the electrical system.
- **Event:** Hurricane surge (saltwater) flooded the storage facility and grounds. Many critical spare parts (electrical) were underwater and would eventually corrode. Flooded facility made it difficult for staff to access the building that housed those parts not underwater.
- **Failure:** Planning never took the time to evaluate the selected location, which was later mapped using SLOSH (Sea, Land and Overland Surges from Hurricanes) modeling.
- **Solution:** Facility was later identified to be in a hurricane surge zone. Critical parts were relocated to other locations (risk spreading). An SOP was developed to close the facility and relocate all personnel and vehicles when a hurricane is approaching.



# Planning Failure – Incomplete SOP

- Critical Infrastructure Owner/Operator
  - Constructed an EOC to be used as a backup (alternate site)
  - Designed with a large-screen board, meeting rooms and a cubicle layout
  - Equipped each cubicle with a desktop computer and landline
  - Hardwired communications lines and had microwave backup communications
  - Installed a backup generator in case of a power outage
  - Created a partial EOC Standard Operating Procedures (SOP)
  - Trained staff on their roles and responsibilities
- **First Event: No one had visited the EOC in months, so as staff arrived, several versions of computer upgrades were 'stacked', crashing all of the computers**
- **Failure: No facility or IT maintenance plan for EOC while it sat idle**
- **Solution: SOP was revised to visit facility monthly, including turning on all computers to ensure all upgrades were loaded**



# Planning Failure - Technology

- Utility
  - Had implemented advanced technology to operate their various systems, including outage mapping using Advanced Metering technology
  - Crews had Mobile Data Terminals to receive outage orders and access maps and files
  - Network was dependent on a fiber-optic ring that was 100% redundant. Each ring was physically separated, and had a low probability of being impacted at the same time
- **Event:** During a high-wind event a fire broke out in a fiber-optics cabinet, rendering one ring unavailable. At the same time, a backhoe operator dug up the other ring.
- **Due to their dependance on this fiber-optics network, their systems were down, and they had no access to determine an outage footprint or to assign work.**
- **Failure: They had removed all paper processes and maps and were totally dependent on technology.**
- **Solution: Plan for catastrophic technology failures. Be able to revert to old processes. Total dependance on technology can be risky, so one must be able to pivot and be ready for 'the old way' of doing things (some organizations actually exercise this).**



# Planning Failure - Procurement

- Procurement
  - Utility reduced the number of wood pole suppliers during a 'cost-cutting' initiative. The selected pole supplier was actually located in a hurricane prone area and was impacted by a hurricane. Ironically, their ability to purchase wood poles during their hurricane restoration was severely impacted.
  - Organization reduced the number of cellular carriers from three to one during a 'cost-cutting' initiative. During a storm, their single carrier lost area service, so their mobile phones, iPads, hotspots, and mobile technology was inoperable.
  - Organization had emergency rental agreements in place with a single local Heavy Equipment rental company. Unfortunately, the rental company had the same agreement with others, so when they called, there was no more equipment left.



# Planning Failures - Honorable Mention

- Planning Failures
  - As part of hurricane preparedness, a transit authority developed an SOP that required that diesel locomotives be relocated to a specific railway yard. That yard was unfortunately in a flood zone, so when a hurricane impacted the area, the locomotives were damaged due to flooding. SOP was revised.
  - In one major city, due to space considerations, many buildings placed their backup generators in basements. When a hurricane hit, the basements and generators flooded. Many elevated their generators or relocated them to rooftops.
  - Utility brought in extra construction trucks and crews in advance. Staging site they had selected was in a floodwater zone and trucks were under 8' of water. Plan was revised.
  - Utility had contracts with area coastal hotels and private condos. Hurricane wiped out 90%+ of these, so crews had to travel two (2) hours to inland hotels. Plan revised to include building temporary staging sites closer to the damaged areas.



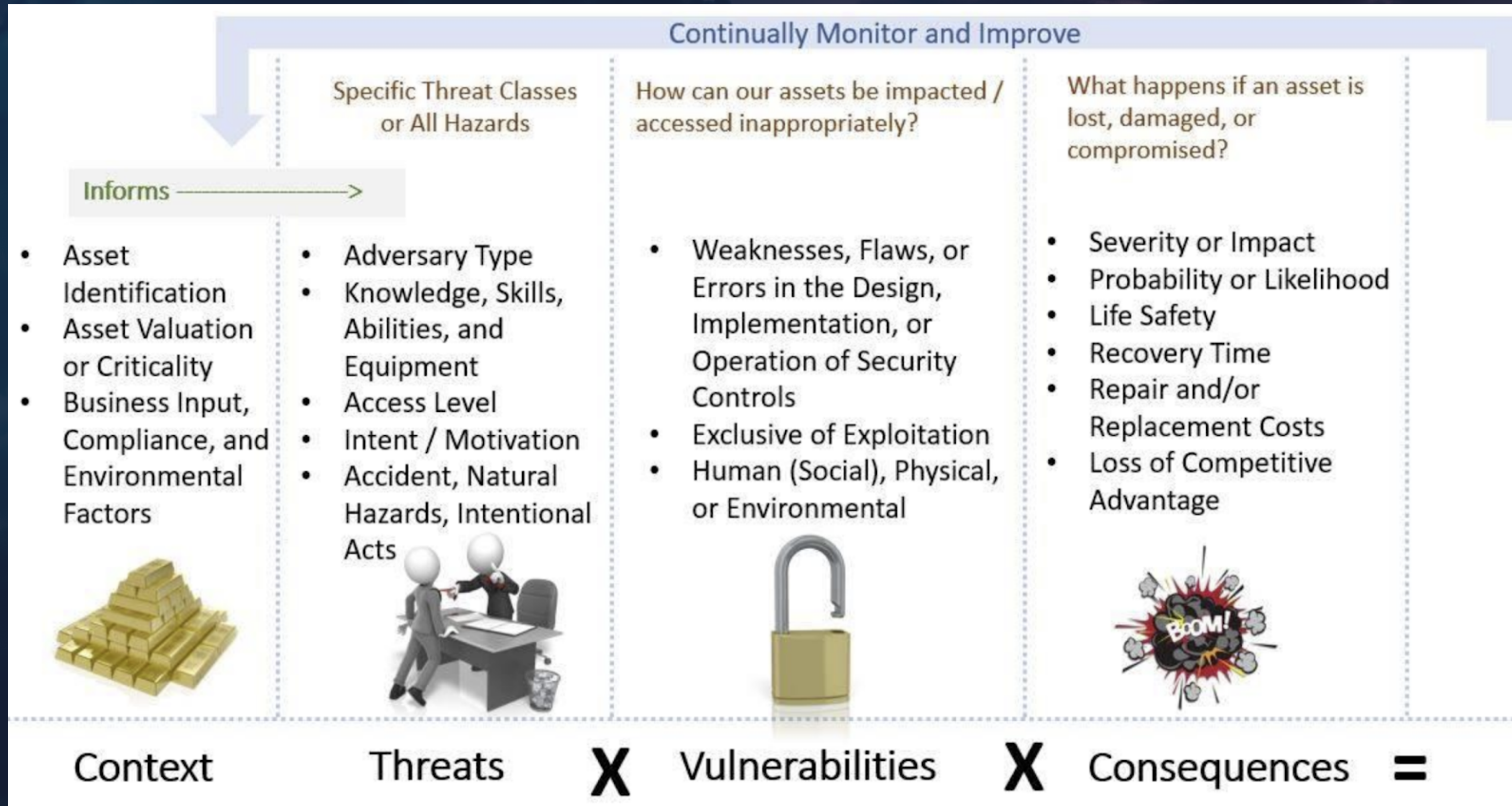


# Risk Assessment



# Risk Assessment

Matthew R. Dimmick, CPP®, PCI®, PSP®, CPD





# Risk Assessment

- Risk assessment identifies and minimizes key risks/threats
  - Control weaknesses and/or points of failure
  - Mitigation/corrective(s) measure to address
  - Select, implement, and document mitigation/corrective measure(s)
  - Ensure facility personnel awareness of risks



# Risk Assessment Considerations

- Risk Considerations for Business Continuity Planning
  - People
  - Process
  - Equipment
  - Technology
  - Facility
  - Supply Chain



A dramatic, dark sky filled with heavy, dark clouds. A bright light source, possibly the sun or moon, is partially obscured by the clouds, creating a strong backlight effect. Several bright, jagged lightning bolts are visible, striking down from the clouds. The overall color palette is dominated by deep blues, purples, and greys, with the white text providing a sharp contrast.

# **Room Assignment**

What are your organizations  
greatest risks?



# Survey Results (2019)

1. Major IT disruption (cyber attack)
2. Data Breach
3. Extreme Natural Disaster
4. Major IT disruption (accidental)
5. State sponsored cyber attack
6. Cyber terrorism
7. Critical Infrastructure Failure
8. Supply Chain Disruption
9. Human-caused major disaster
10. Global Financial Crash

*This survey among Business Continuity professionals was in 2019. Do you see anything missing?*



# Survey Results (2019)

1. Major IT disruption (cyber attack)
2. Data Breach
3. Extreme Natural Disaster
4. Major IT disruption (accidental)
5. State sponsored cyber attack
6. Cyber terrorism
7. Critical Infrastructure Failure
8. Supply Chain Disruption
9. Human-caused major disaster
10. Global Financial Crash

*This survey among Business Continuity professionals was in 2019. Do you see anything missing?*

**How would COVID-19 rank today?**

**Risks can change year to year**



# Risk Matrix / HVA Tool

RISK ASSESSMENT MATRIX				
SEVERITY PROBABILITY	Catastrophic (1)	Critical (2)	Marginal (3)	Negligible (4)
Frequent (A)	High	High	Serious	Medium
Probable (B)	High	High	Serious	Medium
Occasional (C)	High	Serious	Medium	Low
Remote (D)	Serious	Medium	Medium	Low
Improbable (E)	Medium	Medium	Medium	Low
Eliminated (F)	Eliminated			

HAZARD AND VULNERABILITY ASSESSMENT TOOL NATURALLY OCCURRING EVENTS								
EVENT	PROBABILITY	SEVERITY = (MAGNITUDE - MITIGATION)						RISK
		HUMAN IMPACT	PROPERTY IMPACT	BUSINESS IMPACT	PREPARED-NESS	INTERNAL RESPONSE	EXTERNAL RESPONSE	
	Likelihood this will occur	Possibility of death or injury	Physical losses and damages	Interruption of services	Preplanning	Time, effectiveness, resources	Community/ Mutual Aid staff and supplies	Relative threat*
SCORE	0 = Nil 1 = Low 2 = Moderate 3 = High	0 = Nil 1 = Low 2 = Moderate 3 = High	0 = Nil 1 = Low 2 = Moderate 3 = High	0 = Nil 1 = Low 2 = Moderate 3 = High	0 = Nil 1 = High 2 = Moderate 3 = Low or none	0 = Nil 1 = High 2 = Moderate 3 = Low or none	0 = Nil 1 = High 2 = Moderate 3 = Low or none	0 - 100%
Tornado								0%
Thunderstorm								0%
Snow Fall								0%
Blizzard								0%
Ice Storm								0%
Earthquake								0%
Heat/Humidity								0%
Drought								0%
Flood, External								0%
Wild Fire								0%
Landslide								0%
Dam Inundation								0%
Subsidence								0%
Epidemic								0%
AVERAGE SCORE								0%
*Threat increases with percentage.								
	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0%

**RISK = PROBABILITY \* SEVERITY**

0.00      0.00      0.00





# Business Impact Analysis



# Benefits of Performing a BIA

Business Impact Assessment will help you:

- Identify essential business functions, dependencies, and requirements
- Measure effects of business functions and resource losses over time
- Provide crucial data for development of the Business Continuity Plan
- Identify business process gaps / weaknesses and improvement opportunities
- Identify IT Recovery Requirements
  - Recovery Time Objective (RTO)
  - Recovery Point Objective (RPO)
- Identify and Prioritize Business Recovery Workarounds and Strategies



# Recovery Definitions

## Essential Functions:

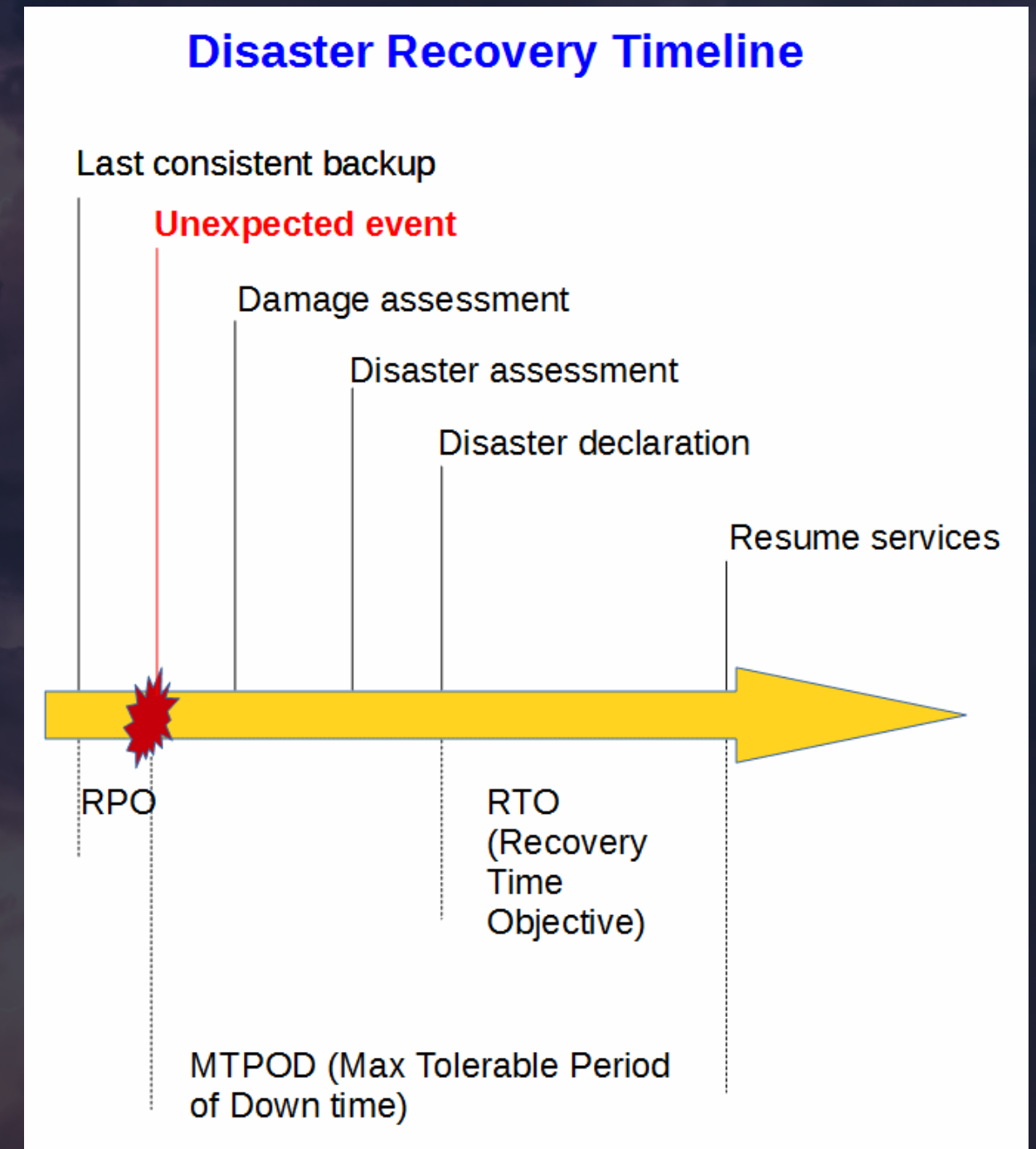
**Maximum Tolerable Downtime (MTD)** for each Essential Function. How long can an essential function be down before the identified impacts begin to escalate?

## IT Systems:

**Recovery Time Objectives (RTO)** maximum expected recovery time for each IT system or application after an outage

**Recovery Time Actual (RTA)** actual recovery time for each IT system

**Recovery Point Objectives (RPO)** maximum amount of expected data loss for each IT application after an outage





# Business Impact Analysis Considerations

## - Impact Considerations for the BIA

- Life Safety
- Revenue
- Customers / Clients
- Operating Costs
- Compliance/ Regulatory / Legal / Rating Agencies
- Brand Reputation
- Internal Staff Impacts



# Key Components - BIA

- Detailed study of all the business processes within the organization, department by department:
  - Critical processes - essential business functions
  - Non-critical processes - important functions, but not critical



# Mitigation Strategy

- Strategy to address identified risks
  - Critical equipment inventory
  - Maintain adequate supplies of water and non-perishable food
  - Items such as batteries, medical supplies, clothes, etc.
  - Have offsite backup systems for data, records and critical softwares
  - Have alternate facilities to relocate operations if necessary
  - Develop disruption alternatives for key essential utilities



# Recovery Strategy

- Developed for identified risks
  - Determine maximum tolerable downtime
  - Identify recovery strategies and courses of action
  - Determine and document reimbursement and cost recovery strategies



# Business Continuity Methods

Interviewing and information mining

## Traditional Method

- Process to have each department complete a BIA worksheet. A member of the BCP Team interviews each department individually to validate the worksheet information.

## Combination Method

- A combination of approaches may be useful and more effective for your facility to initially develop and/or update BCPs.

## Group Method

- Representatives from similar departments are brought together in workshops to complete the worksheet or BCP template. May save time and provide more details with the group thinking together.



# Assessment Topics

- Delegation of Authority
  - Decisions to be made
  - Triggers
  - Position holding Authority
  - Delegated Authority
- Staffing Analysis
  - Role
  - Number of staff
  - Can they work remotely
  - Staff needed
  - Staff available for reassignment
- Essential Business Functions
  - Department
  - Essential Function
  - Maximum Tolerable Downtime
- Maximum Tolerable Downtime
  - Essential Function
  - Dependency
  - Department Responsible
  - Alternate if unavailable
  - Maximum Tolerable Downtime



# Assessment Topics

- Essential Equipment & Supplies
  - Description
  - Normal Quantity
  - Alternate if unavailable
  - Maximum Tolerable Downtime
- Essential Vital Records
  - Description
  - Copy format (hard, electronic)
- Contact List
  - Name
  - Department
  - Point of Contact
    - Normal
    - Emergency



# Assessment Topics Ranked

Recovery Tiers	RTO Values	RPO Values	Impact Categories	Incident Outcome	Recovery Strategies	Recovery Time Frame
Tier 0	0	0	Human Impact	No Impact:	Implement Workaround	for up to 1 hour
Tier 1	0 - 1	4	Life Safety Impact	Minor Impact:	Delay / Defer Process	for up to 2 hours
Tier 2	0 - 4	8	Patient Care Impact	Moderate Impact:	Telecommute / Telecompute	for up to 4 hours
Tier 3	0 - 8	24	Business Impact	Major Impact:	Transfer Process to Alternate Location:	for up to 8 hours
Tier 4	0 - 24					
Tier 5	2 - 4					
Tier 6	4 - 8					
Tier 7	8 - 24					
	24 - 48					
	72 - 120					
	120 - 240					
	> 240					
	TBD					
	TBD					
	TBD					
	TBD					
	TBD					

		Recovery Objectives		Maximum Tolerable Downtime	Emergency Management Function?	Workaround Available?	Recovery Strategy 1	Time Frame	People:	Technology:	Facility:	Supply Chain:	Other:
Department	Essential Function	RTO (hours)	RPO (hours)	MTD	Y / N	Y / N			Staffing Levels	Software, Systems, etc	Location, # seats etc)	Vendors, Supplies, etc	Vital Records, Other Dept's Process, etc
Finance	Payroll									2 laptops			

Essential Functions, Business Impacts & Mitigation Strategies											
Essential Business Functions		Recovery Objectives (Select from Drop Down)	Maximum Tolerable Downtime (Select from Drop Down)	Emergency Management Function	Workaround Available?	Essential Business Function Dependencies				Impact Scale: 0 = N/A 1 = Low 2 = Moderate 3 = High (Note: Select Impact Categories from Drop Down before Scoring)	
										Impact Justification	
Department	Essential Functions	RTO (hours)	RPO (hours)	MTD	Y / N	Y / N	People Dependencies: Normal staffing (N) vs Disaster staffing (D)	Technology Dependencies: Software, Systems, etc	Other Process/		
Finance	Payroll	0 - 24	8	0 - 24	N	Y / N	N = 12 D = 4	ADP Internet RSA Token Employee Portal			

Recovery Tier	Recovery Time Objective (RTO)	Description	Recovery Point Objective (RPO)
	Max Downtime		Max Data Loss
Tier 0	0 - 1	<b>Emergency Management &amp; Recovery (Always Available Functions)</b> Emergency Management and Business Recovery Essential Functions that are required to be available all the time.	0 hours
Tier 1	0 - 4	<b>Mission Critical (Workaround not available)</b> Essential Functions supporting vital business activities and processes. Workarounds are not adequate to provide necessary level of continuity. The loss of these essential business functions could result in impact to patient safety and direct operations impact.	< 24 Hours
Tier 2	0 - 8	<b>Critical (Workaround available)</b> Essential Functions supporting critical business activities and processes. Manual workarounds exist, are in place. Loss of these functions would result in degradation of services and a possible risk to patient safety.	< 24 Hours
Tier 3	0 - 24	<b>Non Mission Critical</b> Functions supporting non-mission critical business activities and processes. Manual workarounds are in place and could be used with only minor patient safety and/or operational impact.	> 24 Hours
Tier 4	24 - 48	<b>Non Mission Critical</b> Functions supporting non-mission critical business activities and processes. Manual workarounds are in place and could be used with only minor patient safety and/or operational impact.	> 24 Hours
Tier 5	72 - 120	<b>Non Mission Critical</b> Functions supporting non-mission critical business activities and processes. Manual workarounds are in place and could be used with only minor patient safety and/or operational impact.	> 24 Hours
Tier 6	> 240	<b>Non Mission Critical</b> Functions supporting non-mission critical business activities and processes. Manual workarounds are in place and could be used with only minor patient safety and/or operational impact.	> 24 Hours

Recovery Strategy 2	Time Frame
Transfer Process to Alternate Location:	after 24 h

Recovery Strategy 4	Time Frame
Return to Normal Operations	after 24 h





# Strategy & Plan Development



# Example of BC Plan Table of Contents

Introduction

Approval Page

Revision Page

Section 1 – BC Management Teams

Section 2 – Emergency Action & Response Plan

Section 3 – Crisis Communications

Section 4 – Damage & Hazard Assessment

Section 5 – Disaster Declaration Procedures & Authority

Section 6 – Responding to a Disaster Declaration

Section 7 – Implementation of BC Procedures

Section 8 – Human Resource Management

Section 9 – Facility Recovery / Relocation

Section 10 – IT System & Data Recovery

Section 11 – Return to Normal Operations

Section 12 – BC Plan Governance, Maintenance & Testing

Appendix A – Contact Lists

Appendix B – Crisis Communications Plan

Appendix C – General Emergency Procedures


Appendix D – Departmental Recovery

Procedures

Appendix E – Incident Management Documents

Appendix F – Alternate Office Locations





Test, Train & Maintain



# Training – Building Block Approach





# Discussion-based Exercises

## Seminars, Workshops, Tabletop Exercises and Games

**Discussion-based exercises** familiarize participants with current plans, policies, agreements, and procedures, or may be used to develop new plans, policies, agreements, and procedures. Discussion-based exercises include **seminars, workshops, tabletop exercises, and games.**

These types of exercises are used:

- As a starting point in the building-block approach of escalating exercise complexity.
- To highlight new and existing plans, policies, interagency/interjurisdictional agreements, and procedures.
- As valuable tools for familiarizing agencies and personnel with current or expected capabilities of an entity.
- To focus on strategic, policy-oriented issues.





# Discussion-based Exercises

## Seminars, Workshops, Tabletop Exercises and Games

**Seminar:** An exercise designed to orient participants to new or updated plans, policies, or procedures through informal discussions.

**Workshop:** An exercise focused on increased participant interaction and focusing on achieving or building a product, such as plans and policies. A workshop is typically used to test new ideas, processes, or procedures; train groups in coordinated activities; and obtain consensus.

**Tabletop Exercise (TTX):** An exercise intended to stimulate discussion of various issues regarding a hypothetical situation. Tabletop exercises can be used to assess plans, policies, and procedures or to assess types of systems needed to guide the prevention of, response to, or recovery from a defined incident. Participants are encouraged to discuss issues in depth and develop decisions through slow-paced problem-solving rather than the rapid and spontaneous decision-making that occurs under actual conditions.

**Game:** A type of discussion-based exercise that simulates operations that often involve two or more teams, usually in a competitive environment, using rules, data, and procedures designed to depict an actual or assumed real-life situation.



# Operations-based Exercises

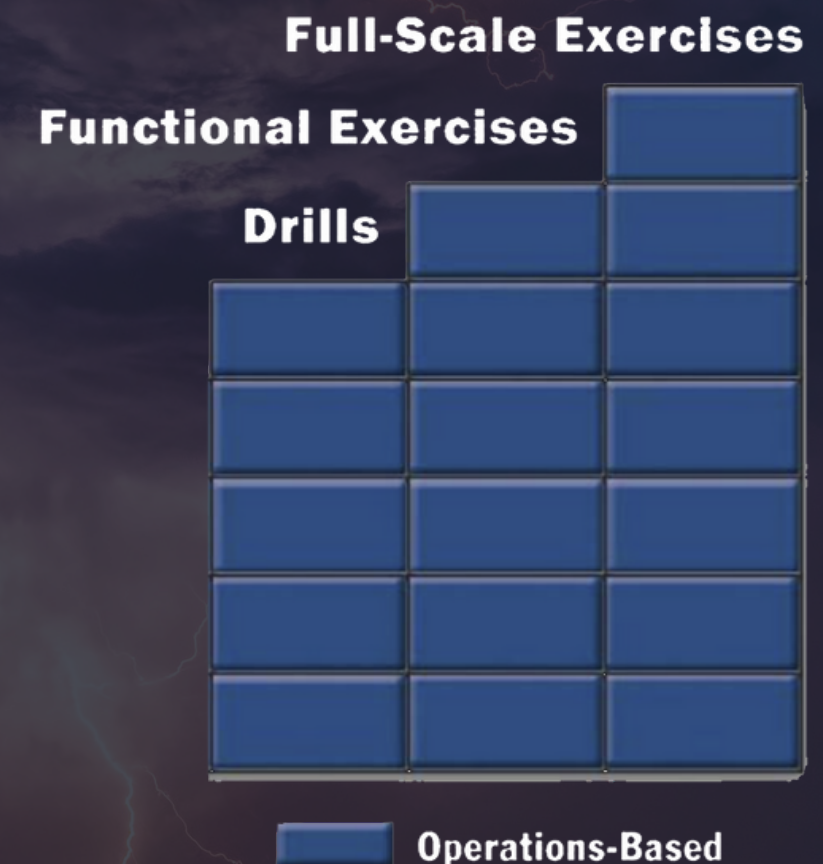
## Drills, Functional Exercises and Full-Scale Exercises

**Operations-based exercises** validate plans, policies, agreements, and procedures; clarify roles and responsibilities; and identify resource gaps in an operational environment.

Operations-based exercises include **drills, functional exercises, and full-scale exercises.**

Operations-based exercises are:

- Used to validate the plans, policies, agreements, and procedures solidified in discussion-based exercises.
- Used to clarify roles and responsibilities, identify gaps in resources needed to implement plans and procedures, and improve individual and team performance.
- Characterized by actual reaction to simulated intelligence; response to emergency conditions; mobilization of apparatus, resources, and/or networks; and commitment of personnel, usually over an extended period of time.





# Operations-based Exercises

## Drills, Functional Exercises and Full-Scale Exercises

**Drill:** An exercise that is a coordinated, supervised activity usually employed to test a single specific operation or function in a single agency. Drills are commonly used to provide training on new equipment, develop or test new policies or procedures, or practice and maintain current skills.

**Functional Exercise (FE):** A single- or multi-agency exercise designed to evaluate capabilities and multiple functions using a simulated response. Characteristics of a functional exercise include simulated deployment of resources and personnel, rapid problem solving, and a highly stressful environment.

**Full-Scale Exercise (FSE):** A multi-agency, multi-jurisdictional exercise involving actual deployment of resources in a coordinated response as if a real incident had occurred. A full-scale exercise tests many components of one or more capabilities within emergency response and recovery. It typically used to assess plans and procedures under crisis conditions and assess coordinated response under crisis conditions.



# Homeland Security Exercise & Evaluation Program (HSEEP)

Continuous Process Enhancement through Improvement Planning

- **Exercise Design and Development**
- **Conduct Exercise**
- **Exercise Evaluation** – Conduct post-exercise ‘hotwash’ to capture feedback on your response actions during a real event or an exercise, documenting an After-Action Report (AAR).
- **Improvement Planning (IP)** - Improvement Planning activities can help shape a jurisdiction’s/organization’s preparedness priorities and support continuous improvement. Actions identified during Improvement Planning help to strengthen elements of a jurisdiction’s / organization’s capability to plan, organize, equip, train, and exercise.





# After-Action Report / Improvement Plan

<div>&lt;Insert Facility Name&gt; &lt;Insert Exercise Name&gt; After Action Review and Improvement Plan</div>		
Section 1: Exercise Overview		
Client: <Insert Facility Name> Exercise Name: <Insert Exercise Name> Begin: <Insert Date>      Time: <Insert Time> End: <Insert Date>      Time: <Insert Time>		
Program: <input type="checkbox"/> CDC/HHS Public Health Emergency Preparedness (PHEP) Grant <input type="checkbox"/> CMS Requirement <input type="checkbox"/> Emergency Management Performance Grant (EMPG) <input type="checkbox"/> Hospital Preparedness Program (HPP) <input type="checkbox"/> Local Emergency Planning Committee <input type="checkbox"/> None (Not required by a Grant or Program)	Type of Event <input type="checkbox"/> Actual/Real Event <input type="checkbox"/> Drill <input type="checkbox"/> Full-Scale Exercise (FSE) <input type="checkbox"/> Functional/Command Post <input type="checkbox"/> Seminar/Workshop <input type="checkbox"/> Tabletop Exercise (TTX)	Mission Focus of Exercise <input type="checkbox"/> Continuity <input type="checkbox"/> Mitigate <input type="checkbox"/> Prevent <input type="checkbox"/> Protect <input type="checkbox"/> Recover <input type="checkbox"/> Respond
Exercise Scenario: (Mark appropriate blocks)		Core Capability
<b>Natural</b> <input type="checkbox"/> Earthquake <input type="checkbox"/> Flood <input type="checkbox"/> Landslide <input type="checkbox"/> Severe Weather	<b>Technological</b> <input type="checkbox"/> Communications (internet, cell tower) <input type="checkbox"/> Contamination <input type="checkbox"/> Dam Failure <input type="checkbox"/> Disease Outbreak	<input type="checkbox"/> Bomb Threat <input type="checkbox"/> Cybersecurity <input type="checkbox"/> Evacuation <input type="checkbox"/> Health & Social Services

2.
Rating:
• Critical Task:
o Task Met: Yes/No
o Analysis: <Insert evaluation/analysis of why/why not the Critical Task was achieved>
• Critical Task:
o Task Met: Yes/No
o Analysis: <Insert evaluation/analysis of why/why not the Critical Task was achieved>
3.
Rating:
• Critical Task:
o Task Met: Yes/No
o Analysis: <Insert evaluation/analysis of why/why not the Critical Task was achieved>
• Critical Task:
o Task Met: Yes/No
o Analysis: <Insert evaluation/analysis of why/why not the Critical Task was achieved>

<div>&lt;Insert Organization's Name&gt; After Action Report and Improvement Plan &lt;INSERT EXERCISE NAME HERE&gt;</div>		<div>Insert Logo Here</div>																																				
< Insert exercise related information in all areas marked in GREY. Delete these instructions in RED.>																																						
Exercise start date and time: <insert here>		Exercise end date and time: <insert here>																																				
Summary of exercise activities: <insert here>																																						
Participating agencies: <insert here>																																						
Resources needed/requested/deployed: <insert here>																																						
Exercise strengths: <insert here>																																						
Areas for improvement: <insert here>																																						
Improvement Plan Table																																						
<table><tr><th>Observation</th><th>Recommendation/ Area(s) for Improvement</th><th>Tasks to Complete Recommendations</th><th>Staff Assigned</th><th>Start Date</th><th>Completion Date</th></tr><tr><td>1</td><td></td><td></td><td></td><td></td><td></td></tr><tr><td>2</td><td></td><td></td><td></td><td></td><td></td></tr><tr><td>3</td><td></td><td></td><td></td><td></td><td></td></tr><tr><td>4</td><td></td><td></td><td></td><td></td><td></td></tr><tr><td>5</td><td></td><td></td><td></td><td></td><td></td></tr></table>			Observation	Recommendation/ Area(s) for Improvement	Tasks to Complete Recommendations	Staff Assigned	Start Date	Completion Date	1						2						3						4						5					
Observation	Recommendation/ Area(s) for Improvement	Tasks to Complete Recommendations	Staff Assigned	Start Date	Completion Date																																	
1																																						
2																																						
3																																						
4																																						
5																																						
<div>&lt;Insert Signature&gt; Print Name Incident Commander</div>				Date																																		
<div>&lt;Insert Signature&gt; Print Name Planning Section Chief</div>				Date																																		



# ***Thank you for Attending!!!***



## ***CRITICAL PREPAREDNESS, LLC***

**Anthony Hurley, MEP, CPP®, PCI®, PSP®, CPD**

Consultant, Critical Preparedness, LLC

Mobile: (216) 554-0558

Email: [Tony@CriticalPreparedness.com](mailto:Tony@CriticalPreparedness.com)

Website: [www.CriticalPreparedness.com](http://www.CriticalPreparedness.com)

LinkedIn: <https://www.linkedin.com/in/aenergyman/>

Twitter: <https://twitter.com/consulthurley>