



"the consolidated technology services agency -RCW 43.105.006"

The Continuity Narrative

How it all comes together

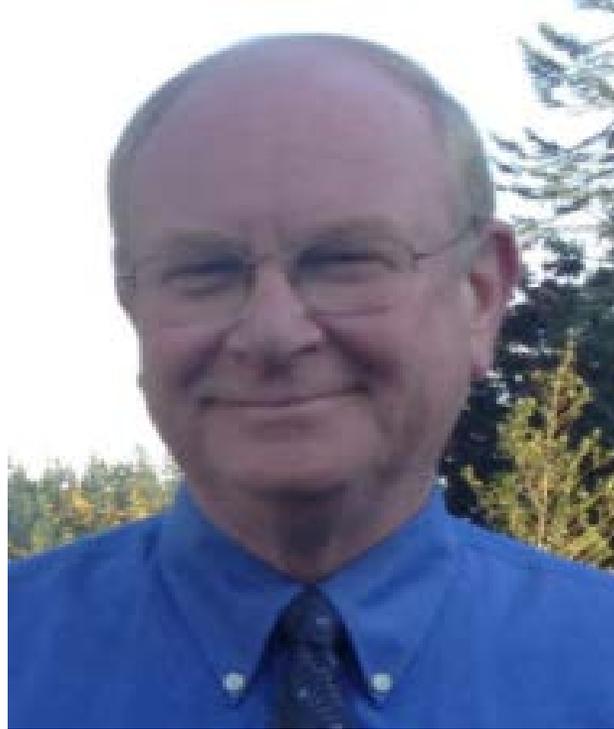


MEET THE TEAM: WaTech EMP



Alisha King

Emergency
Management /
Business Continuity
Specialist



Mark Donges

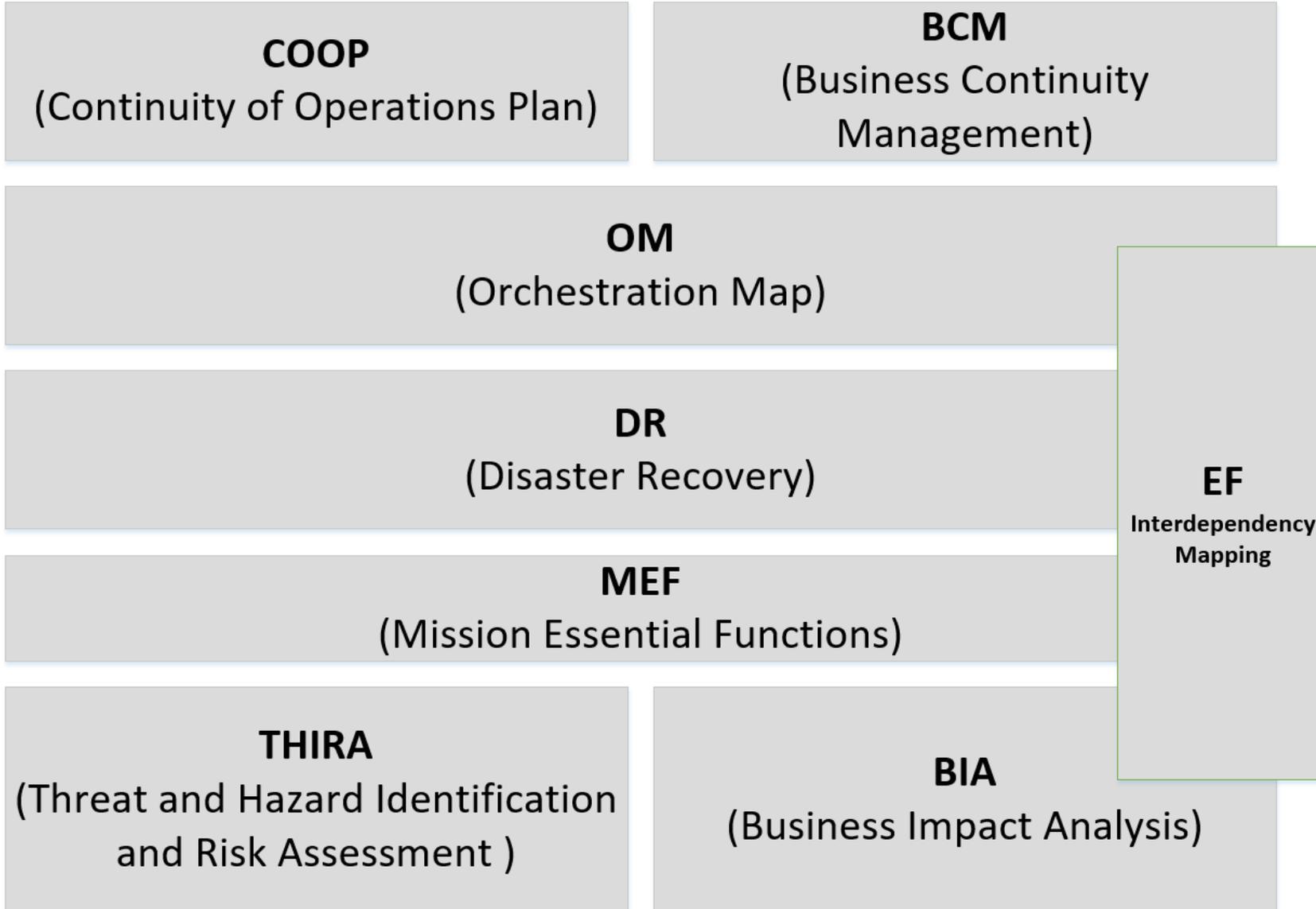
Emergency
Management Lead /
Business Continuity
Specialist



Wesley Chandler

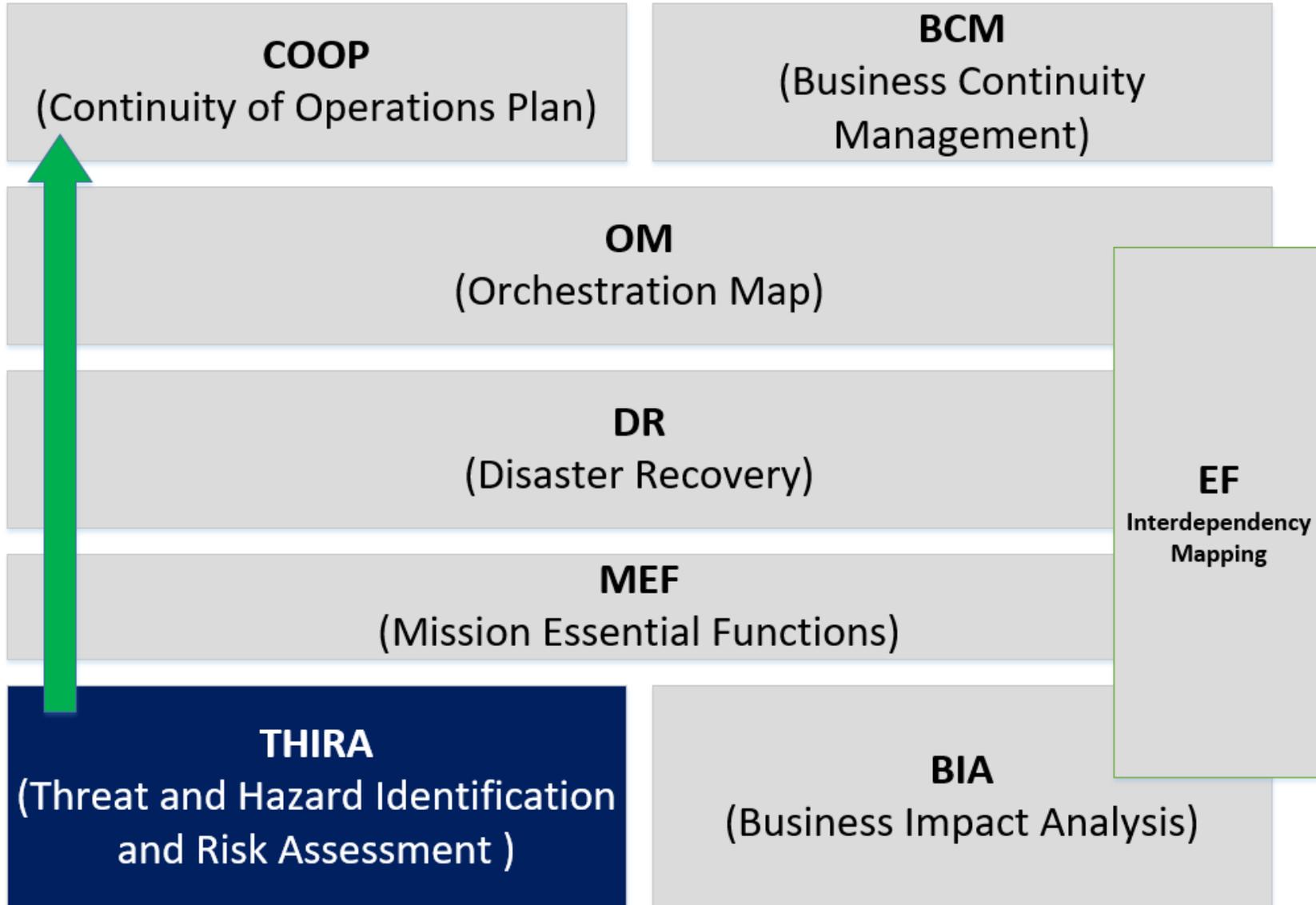
Disaster Recovery
Architect /
Information Systems
Auditor

CONTINUITY NARRATIVE



CONTINUITY NARRATIVE:

Threats and Hazards Identification and Risk Assessment



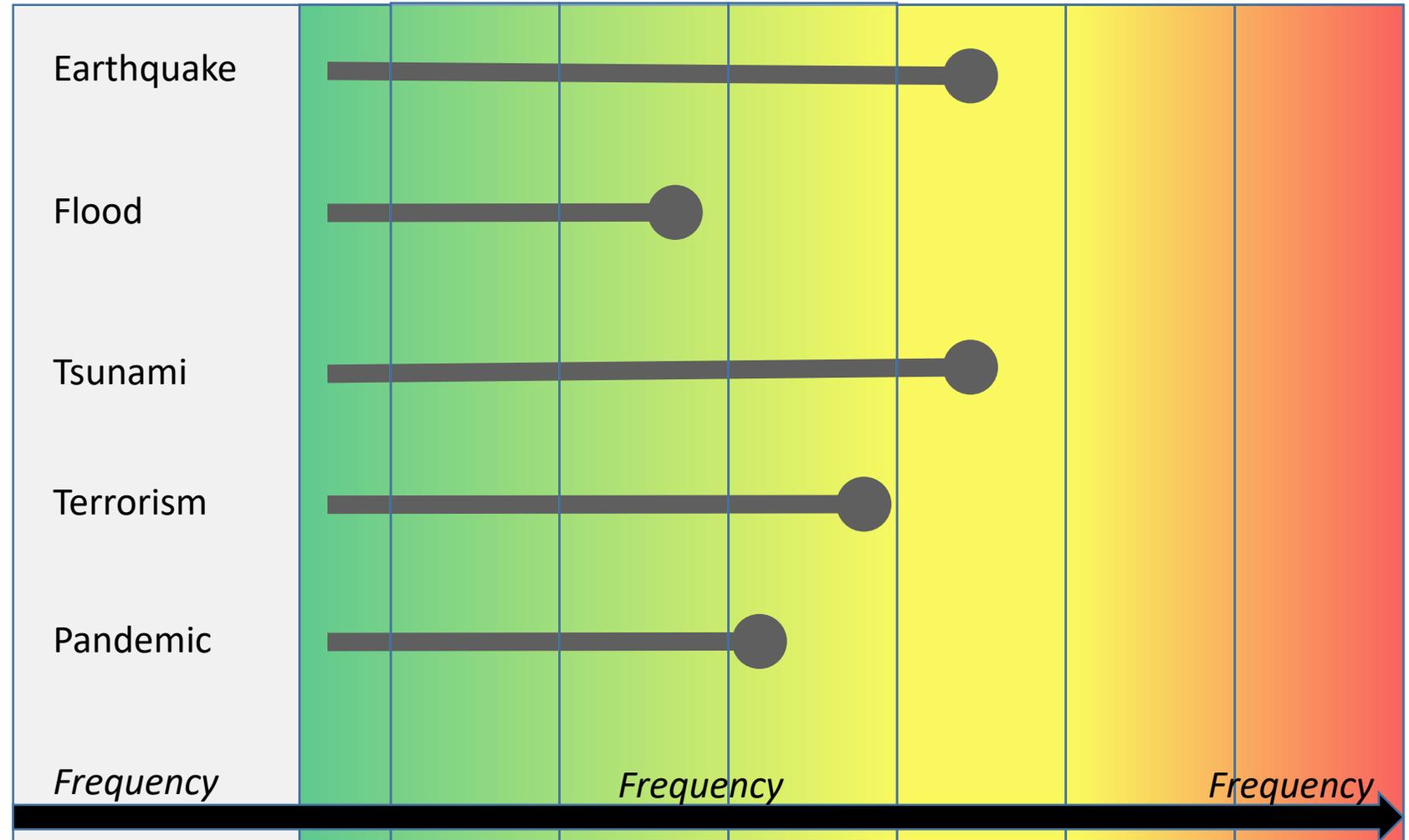
THIRA outputs inform a variety of emergency management efforts, including:

- Threats & Hazards Identification, Hazards, and Mitigation
- Emergency operations planning
- Mutual aid agreements

THIRA: Key Deliverables

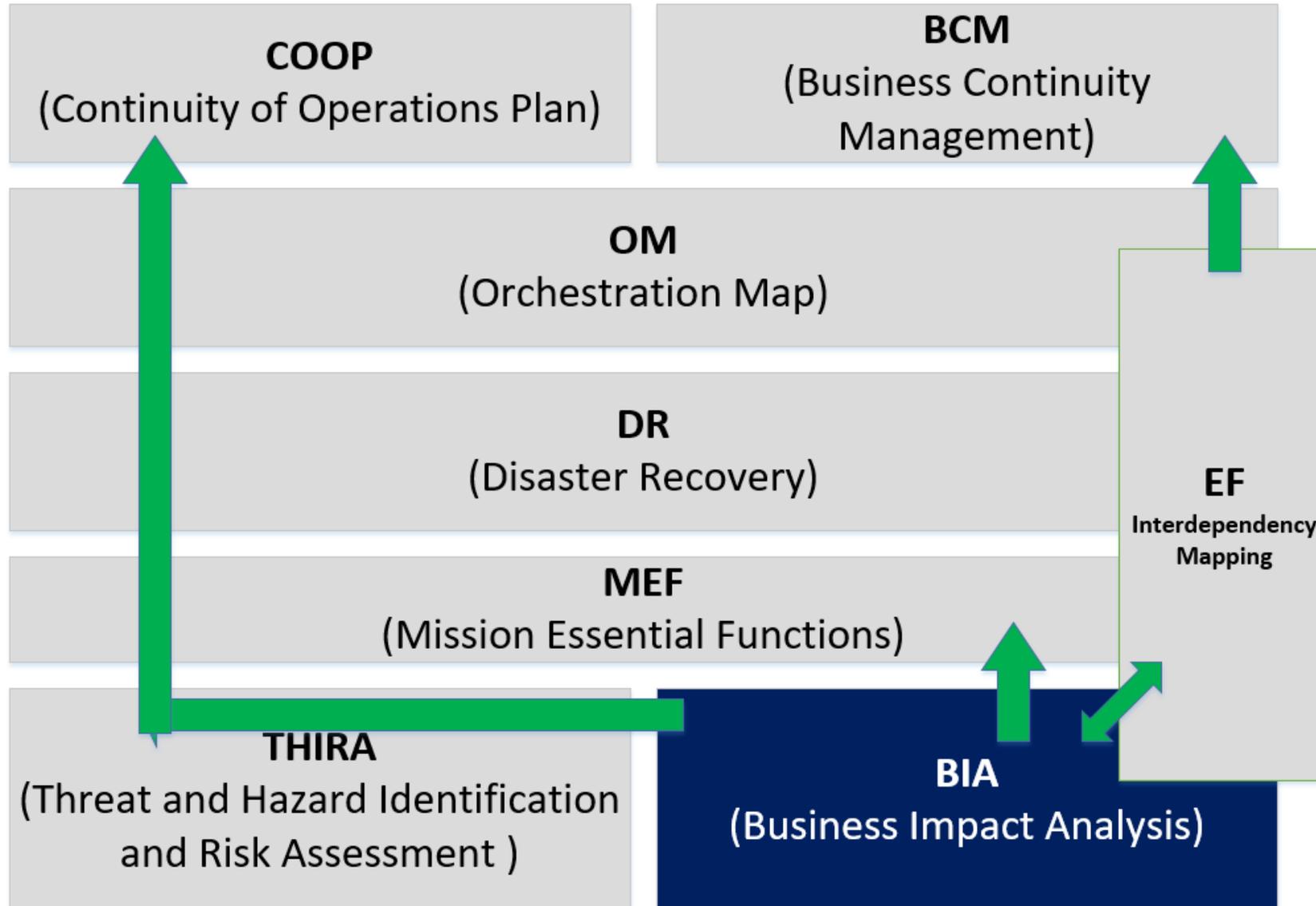
Assess probability of Threats and Hazards:

- Identification of Threats and Hazards
- Assess Probability
- Use above data to extrapolate impact to communities and facilities



NOTE: the above heat map is for illustrative purposes only and does not reflect collected data

CONTINUITY NARRATIVE: Business Impact Analysis

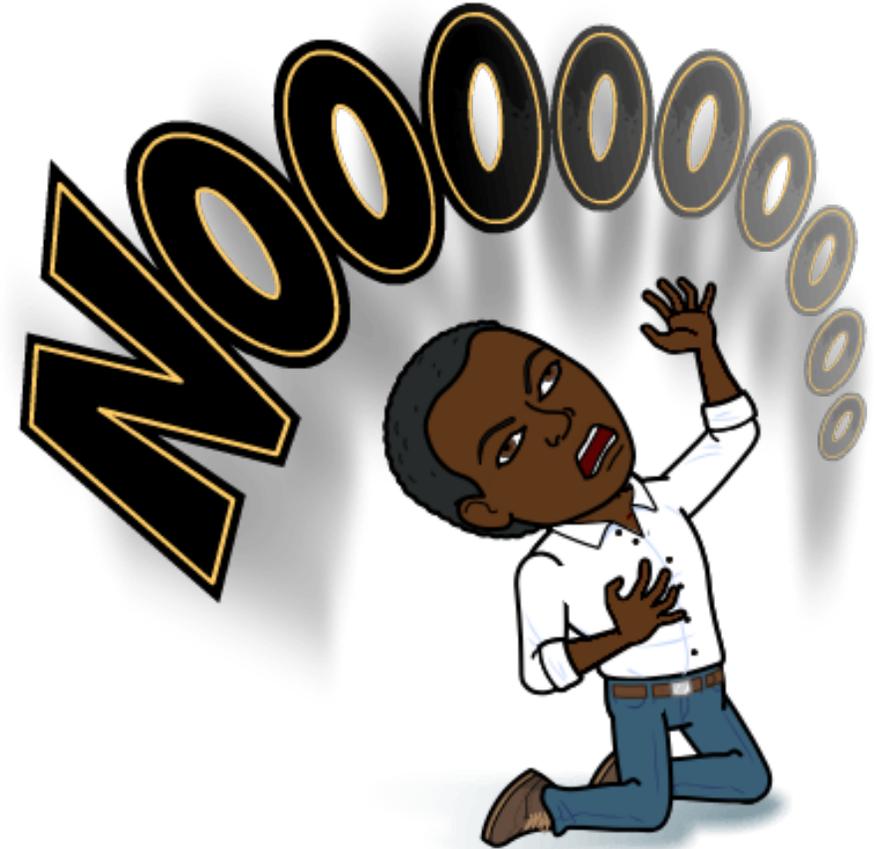


BIA outputs identify:

- An organization's Mission Essential Functions.
- Provides quantitative and qualitative impact measurements.
- Sets Tiers of Criticality
- Sets initial RTO, RPO, and Maximum Allowable Downtime

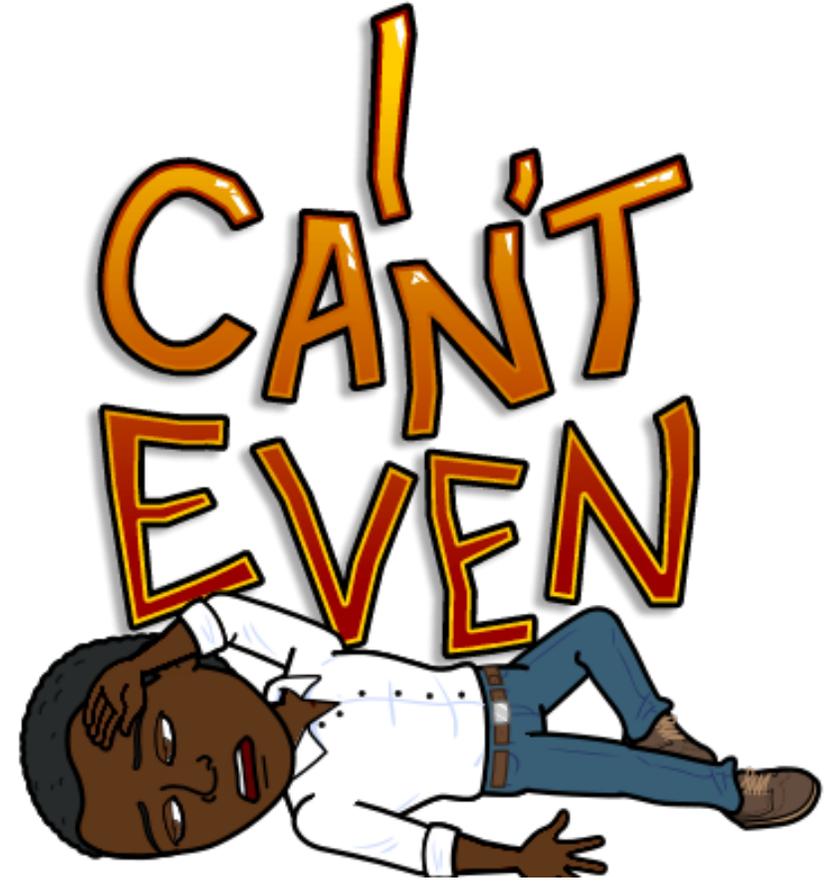
BUSINESS IMPACT ANALYSIS: Tangible Impacts

- Lost Productivity
- Loss of Core Functionality
- Supply Chain Disruptions
- Legal / Contractual / SLAs
- Regulatory
- Overtime Pay
- Delayed Processes / Executed Functions



BUSINESS IMPACT ANALYSIS: Intangible Impacts

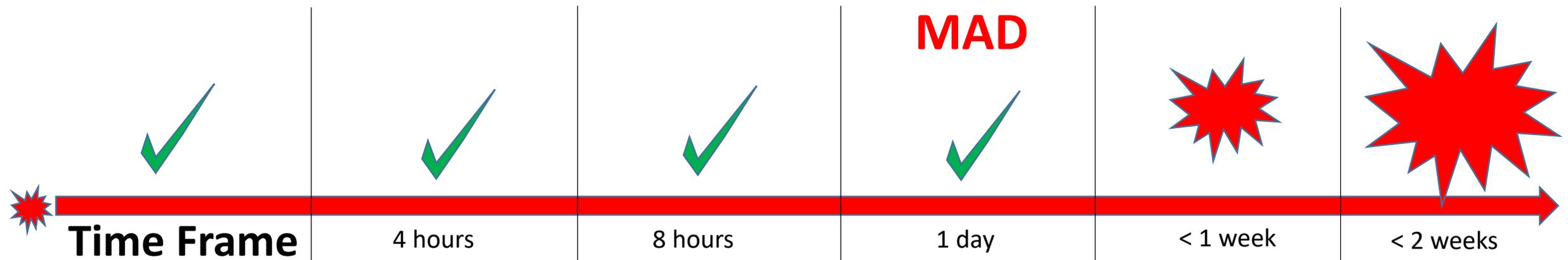
- Reputation/brand
- Loss of confidence
- Customer / Partner / Vendor dissatisfaction
- Increases in liability
- Exposure to lawsuits
- Personnel issues or losses (beyond loss of productive time)



BUSINESS IMPACT ANALYSIS: Analysis + Time

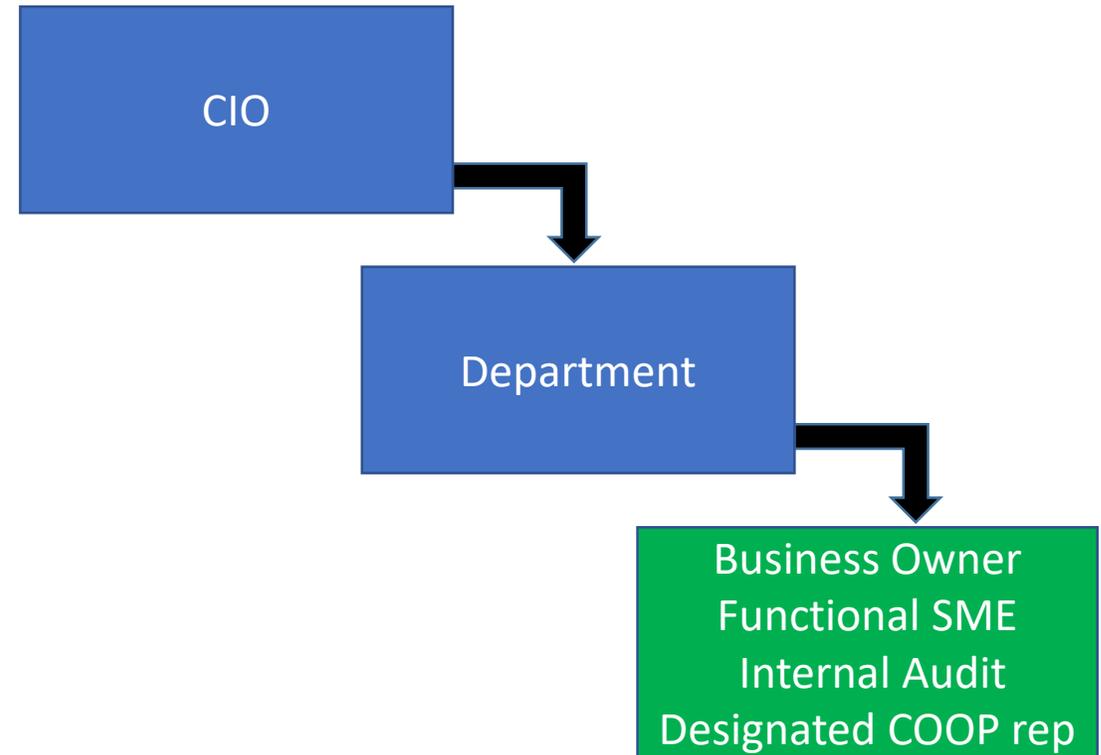
The BIA helps properly assess the impact of a service outage using time to forecast how tangible and potential intangible impacts evolve. Allowing for the development of MAD.

Degree of Impact	Description
0	Fines/Penalties/Lawsuits \leq \$1M
1	\$1M < Fines/Penalties/Lawsuits \leq \$5M
2	\$5M < Fines/Penalties/Lawsuits \leq \$10M
3	\$10M < Fines/Penalties/Lawsuits \leq \$50M
4	Revocation of License or Certificates; Fines/Penalties/Lawsuits > \$50M

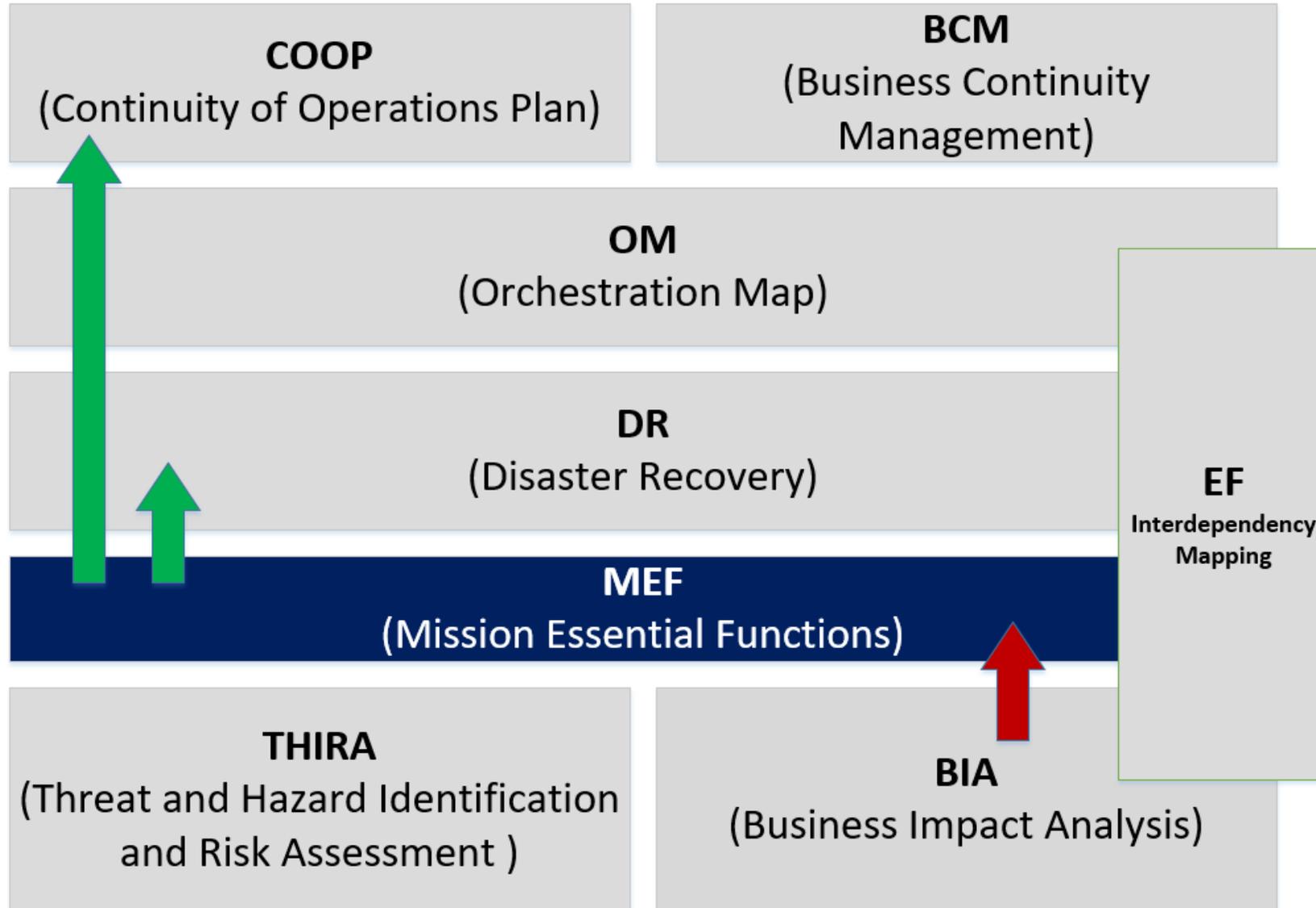


BUSINESS IMPACT ANALYSIS: Data Collection

- Impacts are collected at the functional level
- Process Dependencies:
 - Applications and Systems
 - Justifications
 - 3rd Party Providers (3PP)
 - Specialized Equipment
 - Type of Personnel (essential for defining resources needed for business processes and dependencies)



CONTINUITY NARRATIVE: Mission Essential Functions



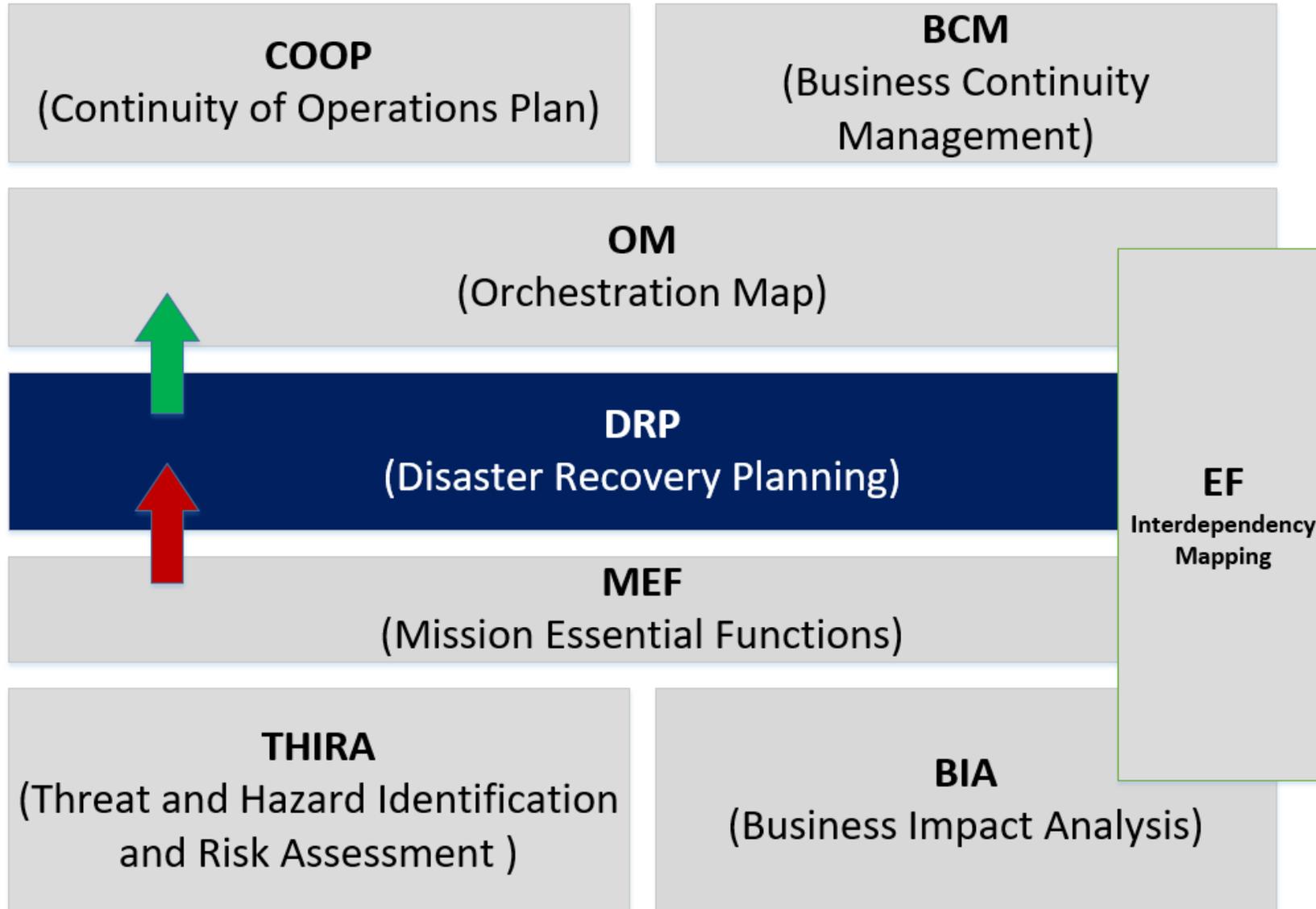
MEF outputs identify:

- The identified most essential functions of the organization; they also tend to be services of the greatest value and/or magnitude should they suffer an outage.

MISSION ESSENTIAL FUNCTIONS: Some MEFs for State Government

- Essential Websites
- Payroll
- Payee Payments
- Legislative and Budget
- Voice & Email Communications
- State Government Network
- Electronic Data Security
- Compute Hosting

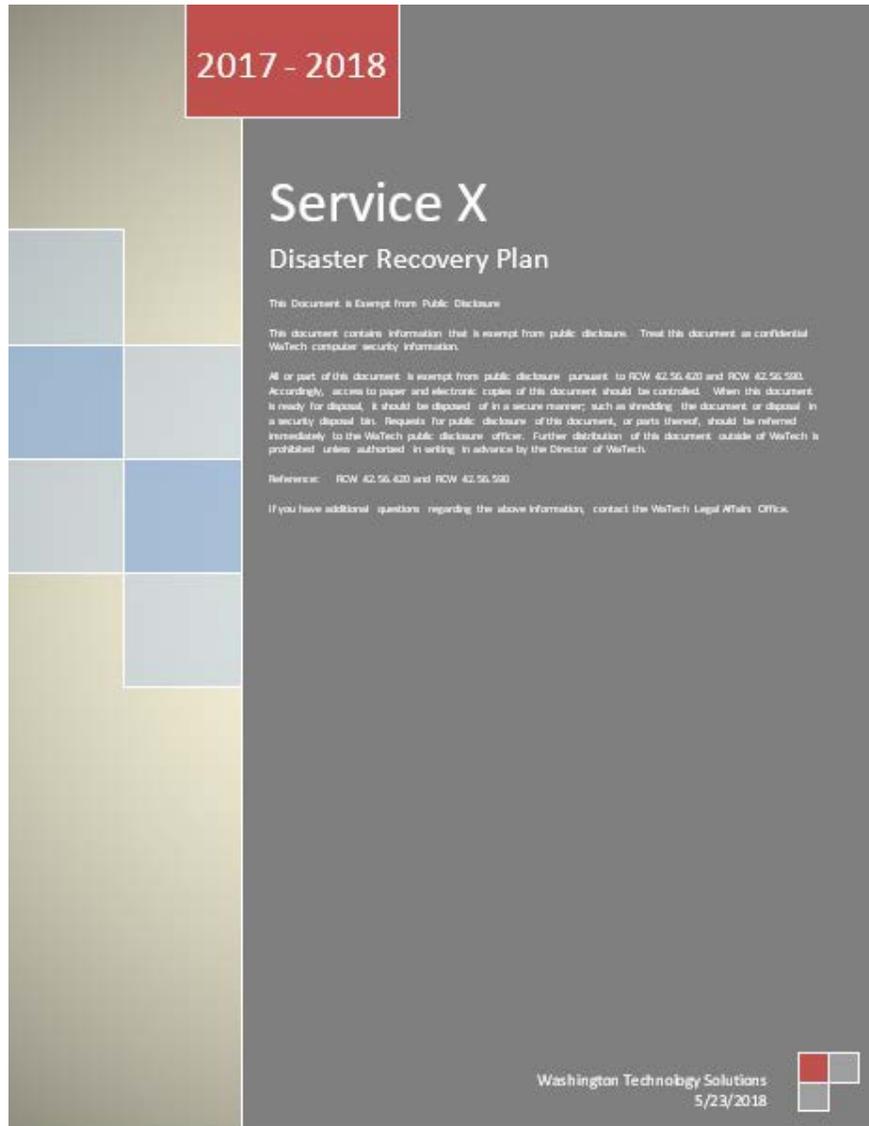
CONTINUITY NARRATIVE: Disaster Recovery Planning



DR Planning outputs identify:

- Applications, systems, and services that support MEFs
- The operational steps required to return systems to an acceptable level of service delivery
- Critical dependencies needed in order to execute DRP

DISASTER RECOVERY PLANNING: Parts of a Plan



- **Document Type**
 - Attestation (*can be leveraged to show compliance*)
 - Operational
 - *Illustrates process level granularity*
- **Security** (*contains CAT3 data*)
 - Integrity
 - Confidentiality
 - Availability
- **Distribution**
 - Onsite & Offsite copies
 - Accessible regardless of scale or magnitude of outage
- **Accountability**
 - Key stakeholders must sign-off on that they've reviewed and/or have been briefed before officiating the DRP as published.

DISASTER RECOVERY PLANNING: Parts of a Plan



Service Summary

<p>Description of Service: Click here to enter text.</p> <p>Impact: Should the Service X primary environment be subject to an outage; consumers of the service will experience a loss and/or impairment of the following features / applications / technology / business processes:</p> <ul style="list-style-type: none"> Impact 1 Impact 2 Impact 3 	Data Category	Choose an item. Comments: Click here to enter text.
	Recovery Time Objective (RTO)	Choose an item. Comments: Click here to enter text.
	Recovery Point Objective (RPO)	Choose an item. Comments: Click here to enter text.
	Maximum Down-Time (MDT)	Choose an item. Comments: Click here to enter text.

[\[Table of Contents\]](#)

[\[Checklist\]](#)

Scope

In-Scope / Out-of-Scope

Clearly define what the scope is for this document; what applications, systems, and services specifically will and will not be addressed for recovery.

This document will speak only to the recovery of the Service X environment in order to make available the following features / applications/ technology / business processes:

- Impact 1
- Impact 2
- Impact 3

The DR Plan will reference the critical dependencies required to stand up the Service X environment, the order in which those dependencies are needed, and who owns those dependencies; but will not speak to the recovery of such dependencies. For the recovery of critical dependencies, please reference their associated DR Plans.

[\[Table of Contents\]](#)

[\[Checklist\]](#)

Post Event Expectations

Will the system be operating in a degraded state, is there an expectation of limited functionality, capacity, or performance? In what way will the level of service be different than what consumers of the service are accustomed to?

- **Service Summary**

- What is the core functions / features that will be unavailable.
- Recovery Objectives
 - RTO, RPO, MAD

- **Scope**

- **IN** – Specifically what will be recovered and specifically what core functions / features will this document restore.
- **OUT** – What functions / features will this document not restore.

- **Expectations**

- Will the customer experience post-failover differ from production? If so explain how.

NOTE: “Document will identify critical dependencies, who owns them, and in what order they must be made available; but not their recovery.” See associated DRP for dependency for recovery as it is out of scope.

DISASTER RECOVERY PLANNING: Parts of a Plan

Roles and Responsibilities

List the the roles needed on the primary team responsible for the recovery of Service X of those on your team both internal and external to your team that are directly required to stand up this service, a description of the role , and mark the role as essential for recovery of the service to be successful.

Role	Responsibility
EXAMPLE SQL Database Administrator	Responsible for the recovery, configuration, and validation of SQL databases.

[\[Table of Contents\]](#)

[\[Checklist\]](#)

Dependencies

Provide a list of any and all dependencies: these include next hop dependencies such as services and applications not within the scope of this DR Plan. Dependencies include such things such as relay agents, load balancing equipment, DNS, other systems to which you pull or push data, software agents, etc. If external support agreements exist please list the vendor as well.

Dependency Name	Dependency Ownership	Contact Information
Post Declaration Communications	Emergency Coordination Center (ECC)	watechmiecc@watech.wa.gov
Service Desk	Service Desk	servicesdesk@watech.wa.gov / 855.928.3241
Workstation Tools	Desktop Support	
Network Core	NSD Network Control Center (NCC)	
Core / Edge Firewalls	NSD Firewall Team	
Secure Access Manager (SAM)		
Enterprise Active Directory (EAD)	Forest Enterprise Administrators	
Active Directory Federated Services (ADFS)		
Domain Name System (DNS) \wo.fc/		
O365 Authentication		
Shared Services Email (SSE)	Messaging Support Team	
Secure Email		
Secure Access Washington (SAW)	Secure Gateway Services Team	
Web Service Gateway (WSG)		
Secure Certificates		
Enterprise Forward Proxy (EFP)		
ADM-CTS	Enterprise Infrastructure Security Team	
ADM-GTM		
ADM-LTM1		
ADM-LTM2		
ADM-MSG		

- **Roles**
 - What personnel are required to execute the in-scope objectives of this DRP.
 - What is their role and responsibility in this activity.

- **Dependencies**
 - List the applications, systems, and services (out of scope) that must be available to restore service delivery.

NOTE: Personnel names are never to be used in a DRP; if possible refer to team names (ex. Data Admin Team) and/or required skillsets (ex. SQL DBA). The only departure from this maybe when referencing a 3PP resource.

DISASTER RECOVERY PLANNING: Parts of a Plan



Inventory

Servers / Appliances

Provide a list of all equipment within the scope of the DR Plan for your environment.

Server / Appliance Name / Role	Type	Manufacturer	Cluster	Host	Site (ex. SDC, SPD, QDC)	Row / Rack / U
EXAMPLE: SSVDBSDC/ HCM – Database / Database Server	Virtual Server	VMAX	HRMS SQL Cluster	ctsdchr001.ssv.wa.icl	SDC	
	Choose an item.					
	Choose an item.					
	Choose an item.					
	Choose an item.					
	Choose an item.					
	Choose an item.					

For Server / Appliance Configuration see [Appendix B](#) for additional details.

For Network Configuration see [Appendix C](#) for additional details.

[\[Table of Contents\]](#)

[\[Checklist\]](#)

- **Inventory (in scope for this DRP)**

- All hardware
- All Software

NOTE: The HW and SW inventory should include the logical and physical locations of assets, additionally should include version info should client / server side software require reinstallation.

DISASTER RECOVERY PLANNING: Parts of a Plan



Recovery Steps

List in as granular detail as possible the recovery steps required to recover the service. The steps should include the following:

- List of steps
- Order of operations
- What steps can be done in parallel?
- Who performs the task?
- How long should it approximately take to perform each step?
- Be sure to hyperlink any section requiring extensive additional detail to an appendice in order to preserve formatting and readability.
- For an example please see Appendix X.

Step # and Name	Task Detail / Task Dependency	Task Ownership (see dependencies for details)	Execution Time
Outage Notification Mechanism	<ul style="list-style-type: none"> • vendor phone home • ORION • Help Desk • Direct customer feedback • Local system self-monitoring 		
Skip to step xx if Declaration to execute the DR Plan has already been issued.			
Step xx: Validate Tools	Task xx: The following must be provided to the administrators to perform any sort of initial troubleshooting and/or recovery of the DNS environment: <ul style="list-style-type: none"> • Tools for remote administration: <ul style="list-style-type: none"> ○ RSA Secure ID ○ BIGIP EDGE client ○ Forticlient (For additional details regarding client side software inventory see section Software Inventory)		
Step xx: Initiate Connection to SDC instance to Administer Environment	Task xx: To connect to the environment you must be on one of the supported WaTech VLANs. Remotely you will have to use the SDC or QDC User VPN instance (whichever is available during the event). (For User VPN see Appendix BB , for additional details.) Restricted Network Access Task xx: This environment accepts connection requests from a restricted subnet. Connect to SAM1 or SAM2 (whichever is available during the event) using Forticlient. (For directions on using Forticlient to connect to the SAM2 instance see Appendix CC , for additional details)		

• Recovery Steps

• Steps

- Breaks up the phases of a recovery effort into manageable components.

• Tasks

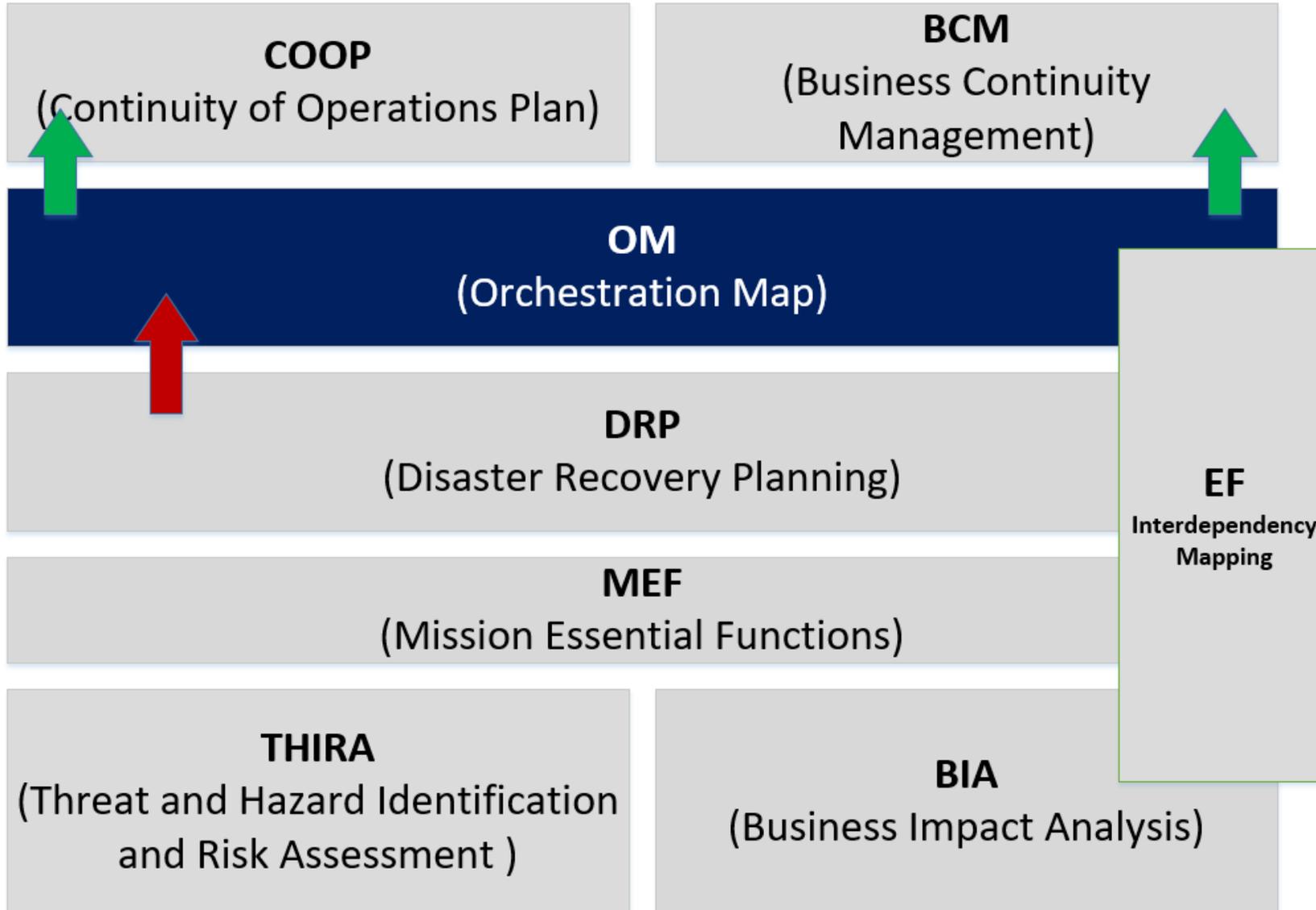
- individual process oriented actions taken to complete a step

• Ownership

- Which designated **Role** or **Dependency Owner** is responsible for executing this **Task**?

• Time

CONTINUITY NARRATIVE: Orchestration Mapping



Orchestration Mapping outputs identify:

- Consolidates MEFs list and DRPs by showing in which DRPs must be executed in chronological order to resuscitate the overall MEF

ORCHESTRATION MAPPING: Ordering and the Role Indexing

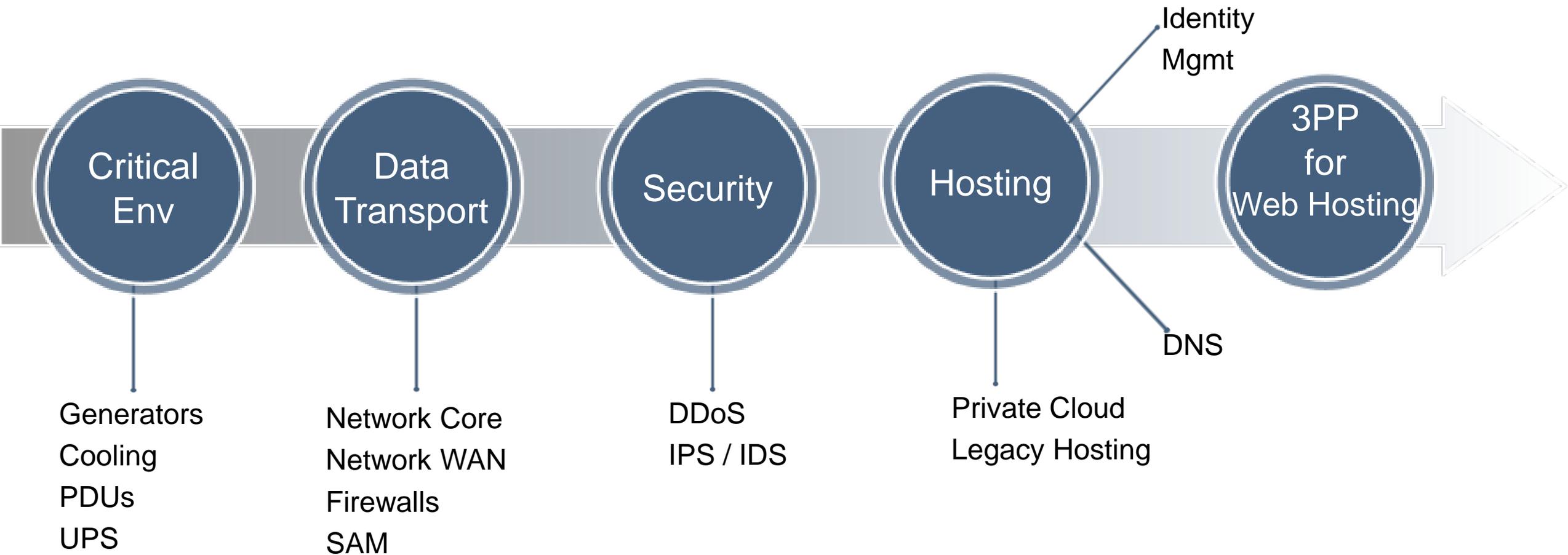


An Orchestration Map of a particular MEF is not only the order in which DRPs must be executed; but should also display when DRPs can be executed in parallel . Always be sure to include the **Roles** needed to execute the DRP so preparations can be streamlined.

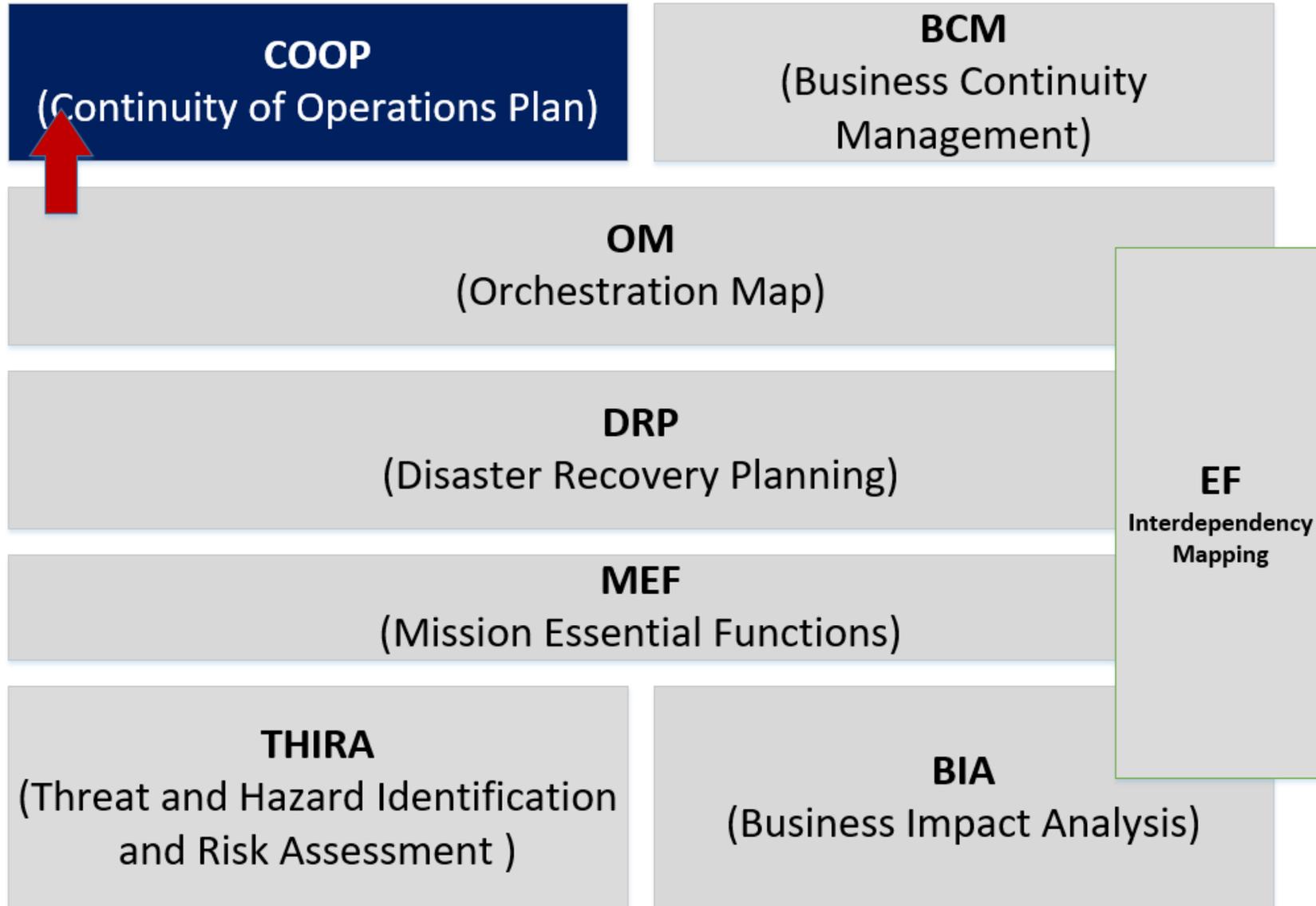
1	Generators	<ul style="list-style-type: none">• Engineer• Contractor• Analyst
2	Cooling	
3	Power Distribution Units	
3	Uninterruptible Power Supply	

ORCHESTRATION MAPPING: The Holistic View

ex. Essential Websites



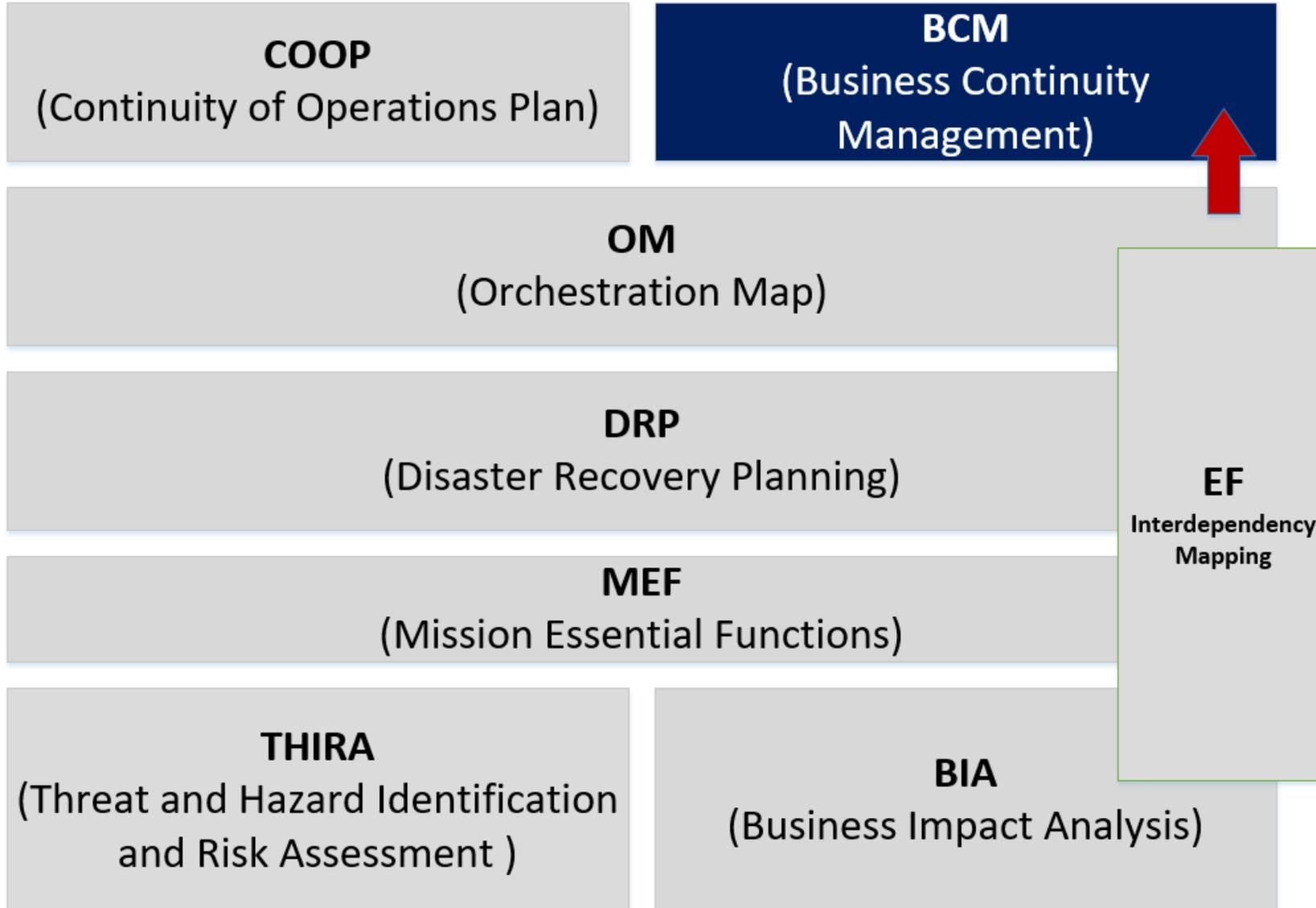
CONTINUITY NARRATIVE: Continuity of Operations Planning



COOP outputs identify:

- Communicates what core functions are needed to be resuscitated.
- Succession Planning
- Delegated authorities
- Emergency Coordination Center controls

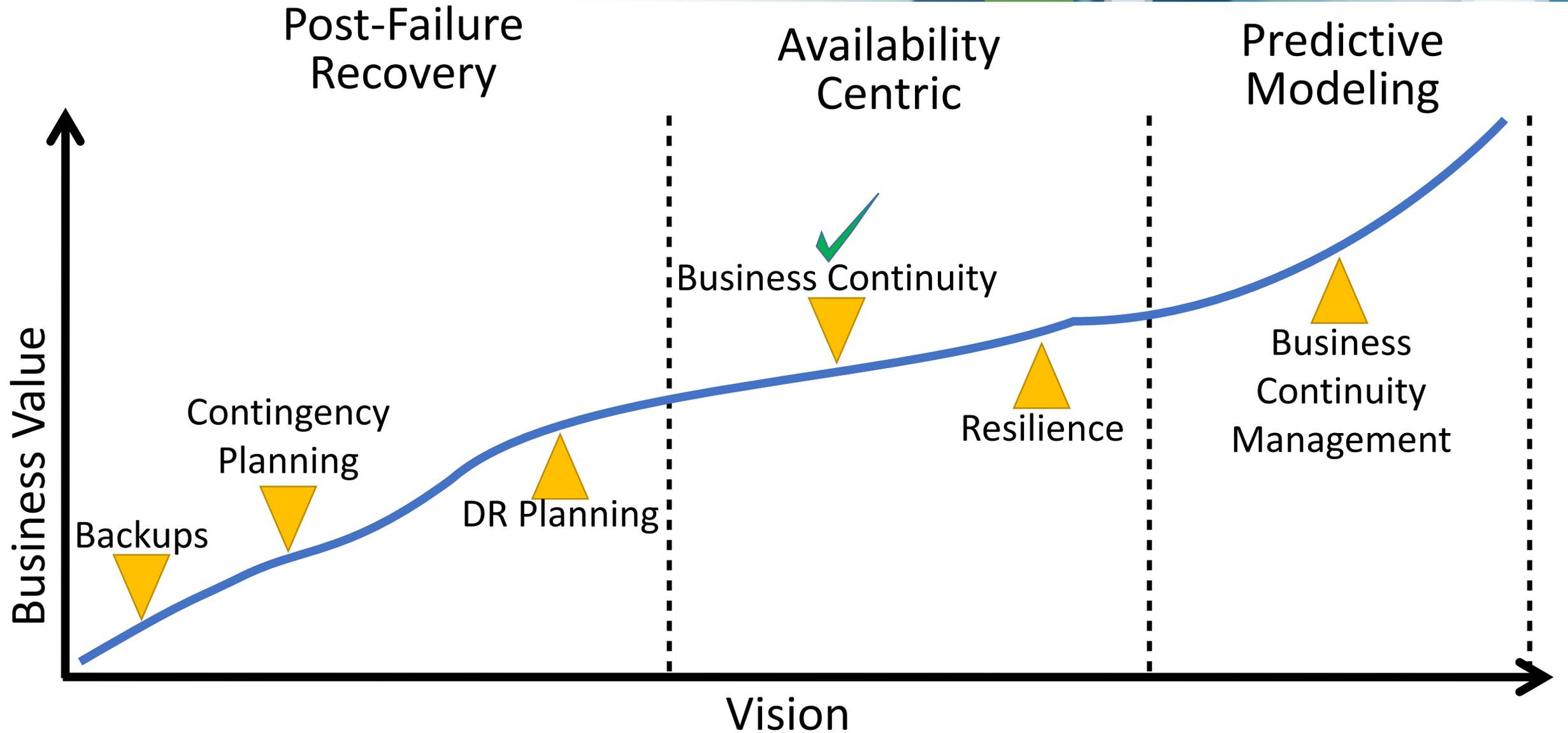
CONTINUITY NARRATIVE: Business Continuity Management



BCM outputs identify:

- Programmatic approaches to prevent service outages.
- Forecast challenges
- Operations integrations
- Data-driven decision making
- Proactive incident management

BUSINESS CONTINUITY MANAGEMENT: Achieving BC



BUSINESS CONTINUITY MANAGEMENT: ReThinking Continuity

“A ‘DR Only’ strategy, is a failure-first strategy.” *~Forrester*

Typical outcomes:

- Resource Intensive
- Extended Downtime
- Costly



BUSINESS CONTINUITY MANAGEMENT: ReThinking Continuity

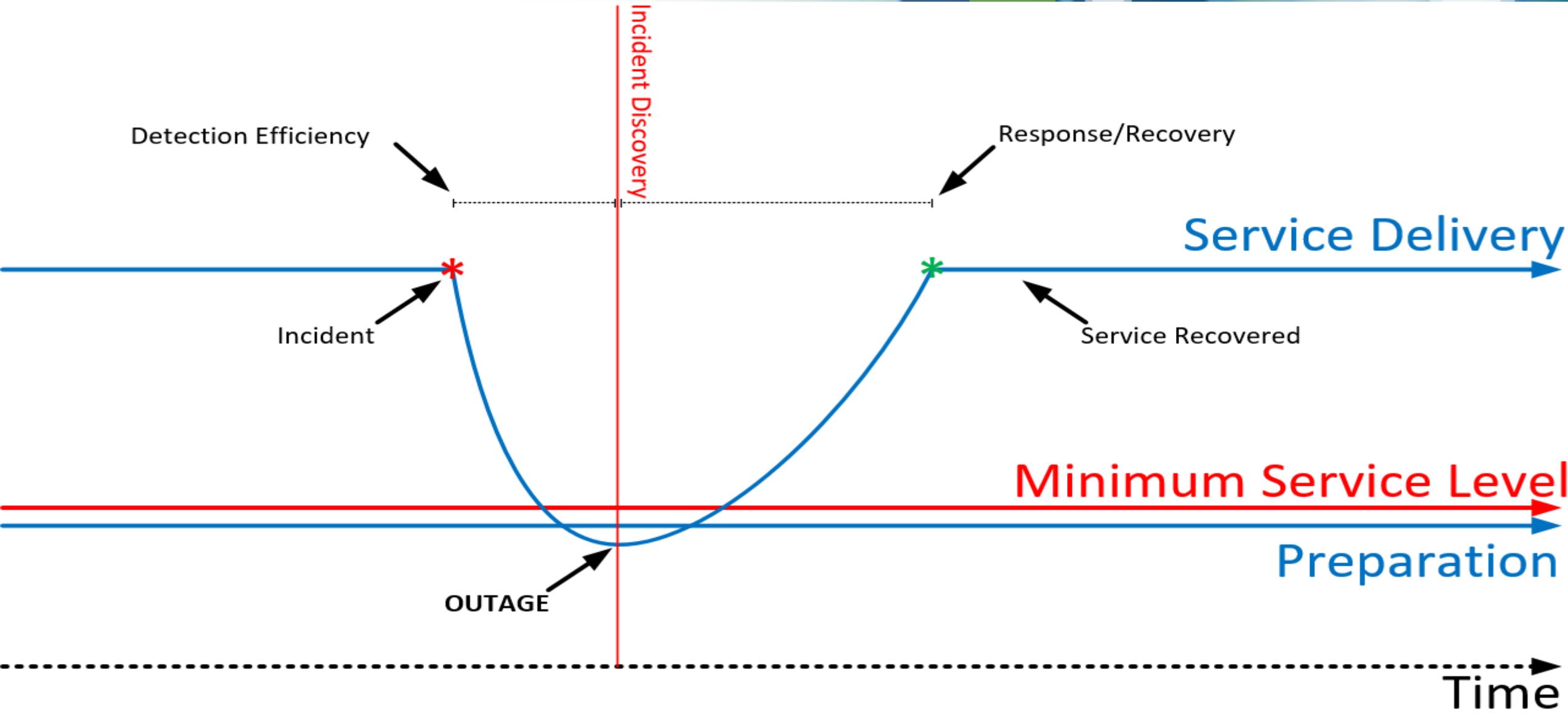
“Reliance on a “failure first” strategy by its very nature does not provide service availability, and should be reserved as a last resort for more extreme circumstances.”

Typical Outcomes:

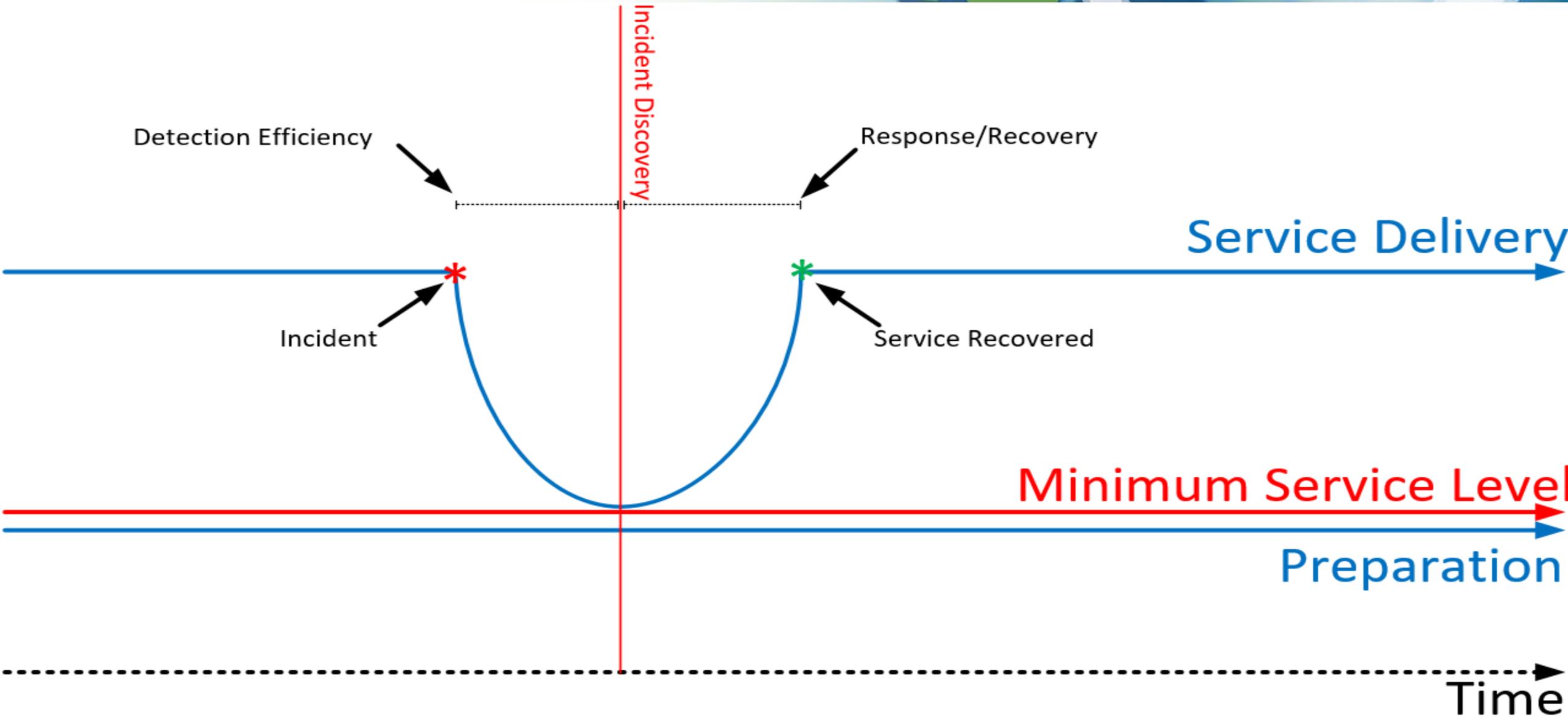
- Disruptive testing
- Security Gaps
- Functionality Gaps



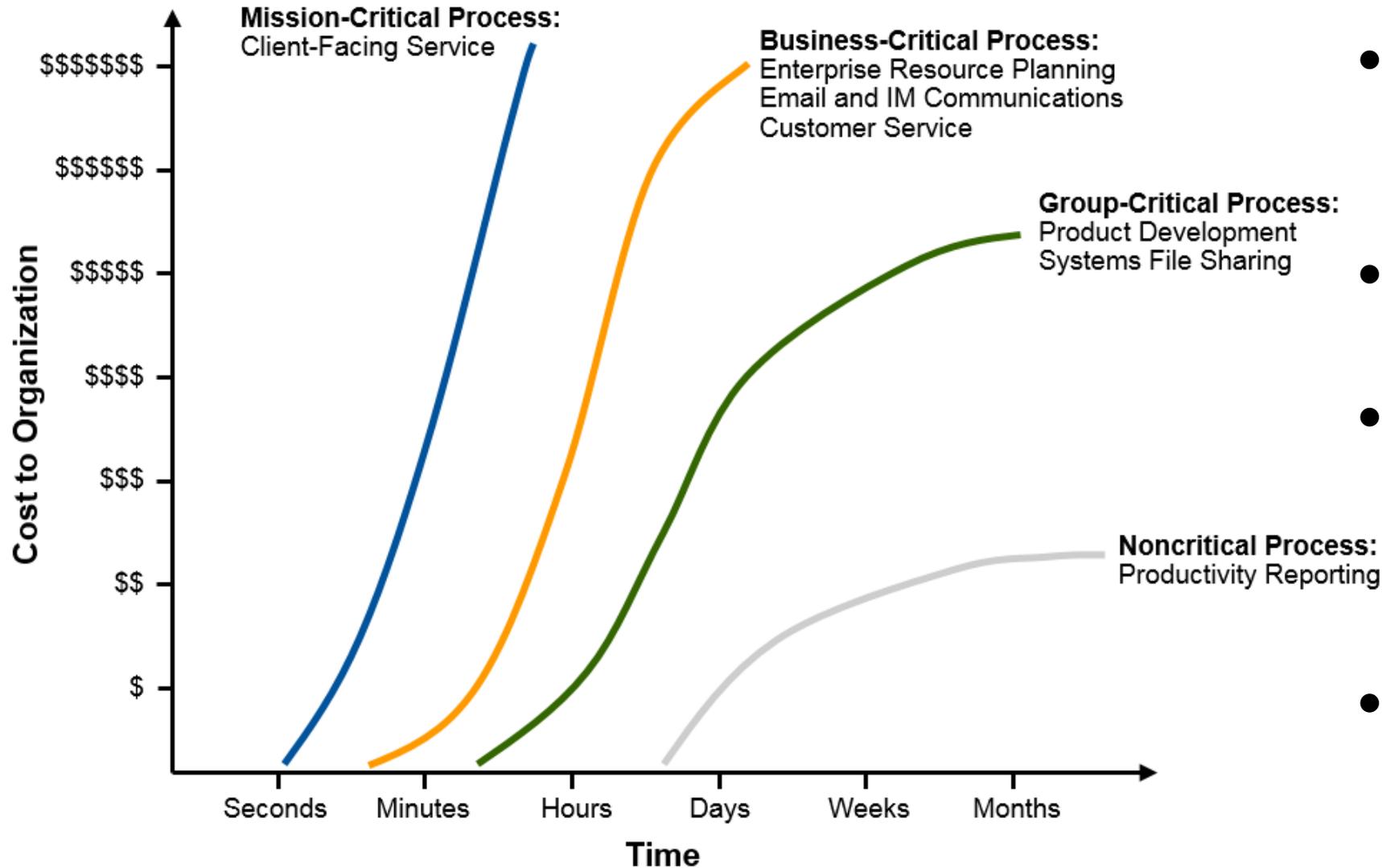
BUSINESS CONTINUITY MANAGEMENT: Typical Disaster Recovery Outcomes



BUSINESS CONTINUITY MANAGEMENT : Proactive Approach to Continuity



BUSINESS CONTINUITY MANAGEMENT: Regarding Resilience Solutions



- Not all solutions are created equally
- Think end-to-end
- Every layer of service delivery must be reviewed
- You can outsource responsibility, but not liability

BUSINESS CONTINUITY MANAGEMENT: Always-On, Always Available

Continuous Availability

- High-levels of Resilience
- Service Availability for Planned outages
- Service Availability for Unplanned outages



✓ Always Available

BUSINESS CONTINUITY MANAGEMENT: Continuity Profiles

Recovery Objectives	< 1min	< 30min	Hours to Days
Continuous Availability	●		
High-Availability	●	●	
Post-Failure Recovery		●	●

The 'Always-On, Always Available' strategy was never meant to be a one shoe fits all approach.

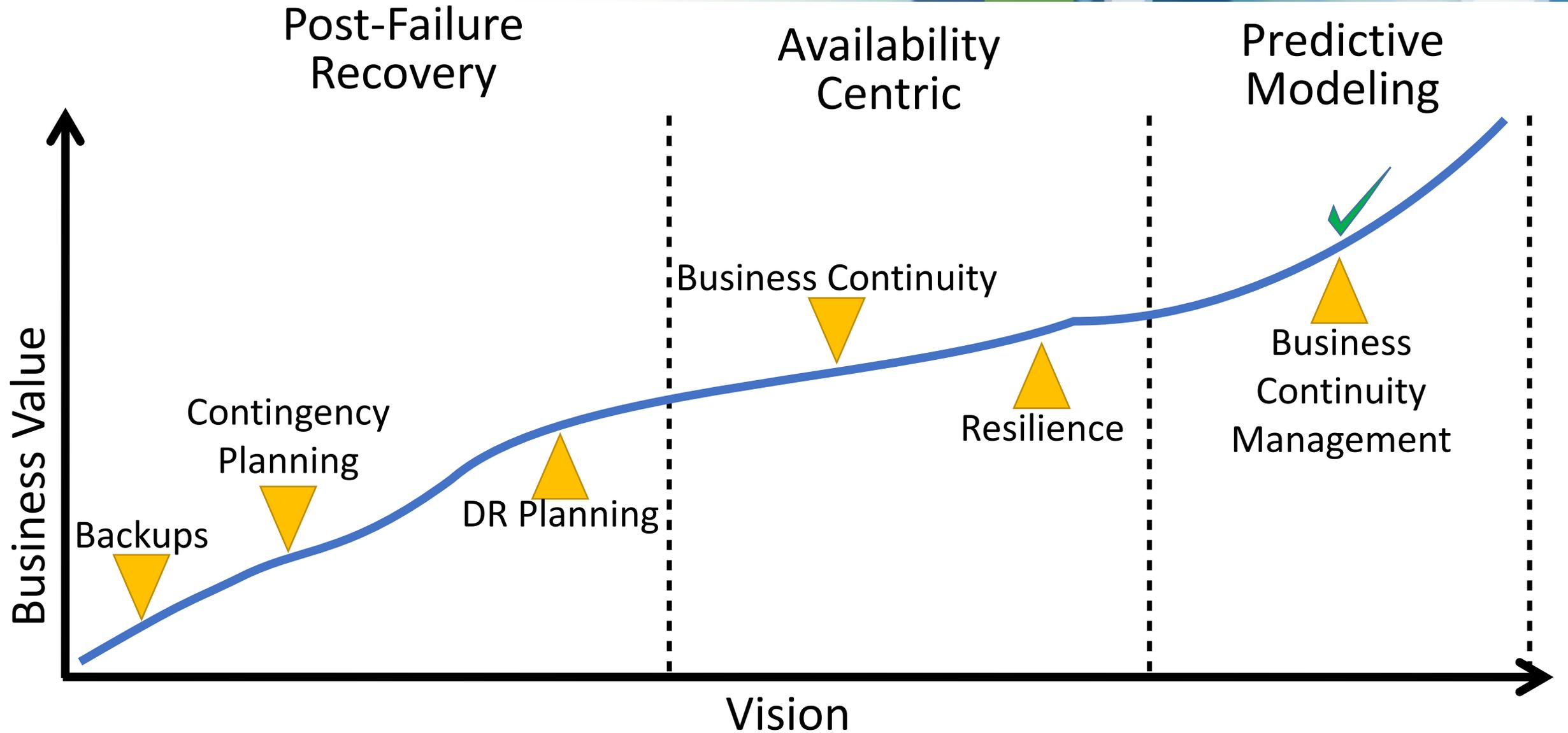
Rather it is but one of three Continuity Profiles that empowers the business unit with service delivery oriented options based on the business requirements, rather than leading with a inundated technical solution that is not sustainable long term.

Business Continuity Management



"the consolidated technology services agency -RCW 43.105.006"

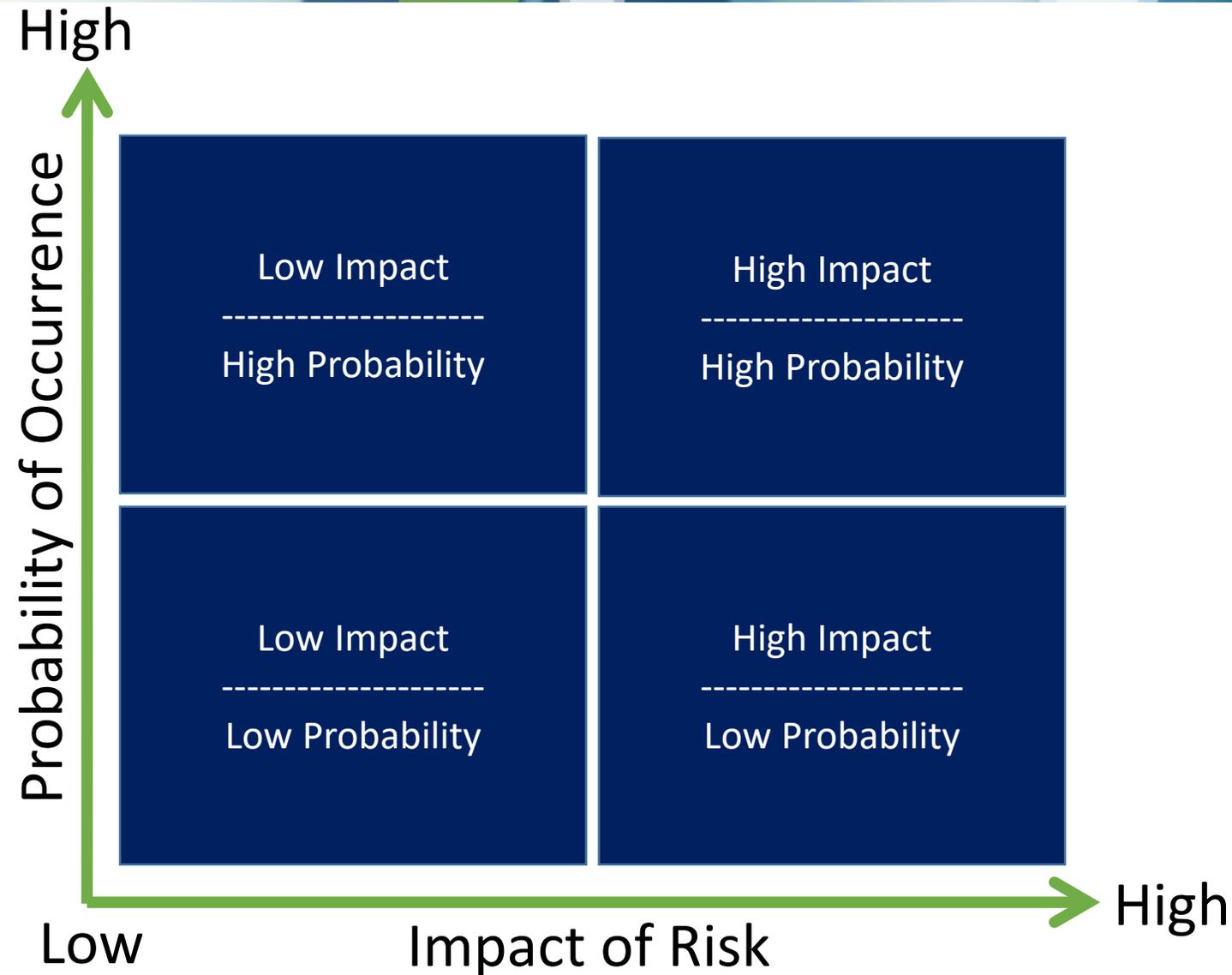
BUSINESS CONTINUITY MANAGEMENT: Achieving BCM



BUSINESS CONTINUITY MANAGEMENT:

Dimensions to Holistic Risk Assessment in BCM:

- List of Threat Vectors
- Vulnerability Footprint
- Geography and Probability of Hazards
- Impact and Time
- Weight and Context



ANY QUESTIONS ???

Alisha.King@watech.wa.gov

Mark.Donges@watech.wa.gov

Wesley.Chandler@watech.wa.gov



DEFINITIONS and other RESOURCES

- **MEF (Mission Essential Function)** – a function provided by an agent of state government that in of itself, or operates in support of 1) preservation of life and public safety, 2) sustaining civil authority, 3) the first responder community, and/or 4) another agency’s essential function.
- **Resilience** – The ability of a service, system, or application to provide and maintain an acceptable level of service in the face of various faults and challenges to normal operation. Rather than refer to applications, systems, and services as resilient or **not** resilient; understand that all services have levels of resilience and should more accurately be referenced as having **low** or **high** levels of resilience.
- **RTO (Recovery Time Objective)** – A point in time indicating the elapsed time between a service disrupting outage and recovery of an acceptable level of service. This is not reflective of actual performance, but an objective the organization targets to achieve.
- **RPO (Recovery Point Objective)** – A point in time indicating the maximum amount of data loss post service disrupting event. Determined from the point at which data can be made available and retrievable from an offsite location. This is not reflective of actual performance, but an objective the organization targets to achieve.
- **DRP (Disaster Recovery)** – A detailed set of instructions that, when followed, can be used to resuscitate or make available a service, system, and/or application after experiencing an outage. Additionally, should describe its resilient measures being taken if applicable and define the mechanisms and instruments used to employ this resilience to protect against service outages.
- **MAD (Maximum Allowable Downtime)** – Maximum Allowable Downtime or MAD is the absolute maximum time that the system can be unavailable without direct or indirect ramifications to the organization
- **3PP (3rd Party Providers)** – any external entity or organization that is relied upon to provide services that have been identified as mission essential or critical to supporting a mission essential function.

Download
Template



[https://
wa.gov/emp/DRA](https://wa.gov/emp/DRA)