Health Service and Business Continuity Planning in Eastern Europe and Central Asia

Global Health Campus
Geneva, Switzerland
15-17 March 2023

Health Service and Business Continuity Planning in Eastern Europe and Central Asia

Goal: *To engage in structured service and business continuity planning for individual countries in EECA and for the regional 'Sustainability of Services' (SoS) program*

Supporting Objectives:

a. Understand business continuity management and disaster response
b. Identify major technical and programmatic risks to country health programs and SoS 2.0
c. Determine impacts on critical processes and services
d. Select solutions for critical processes and services
e. Develop planning timelines

Agenda

Day 1

1. Why and how the Global Fund achieved ISO 22301 certification for its Business Continuity Management System (BCMS)
2. Health service continuity planning as an essential component of an 'end to end' BCMS
3. Pandemic preparedness and workforce planning in EECA as a BC priority
4. The link (and difference) between business continuity and disaster recovery
5. Organizational priorities during the Global Fund's new round of funding

Day 2

1. Essential characteristics of a Business Continuity Management System
2. Business Impact and Risk Assessment (BIRA)
3. Business continuity solutions & strategies
4. Business continuity plans

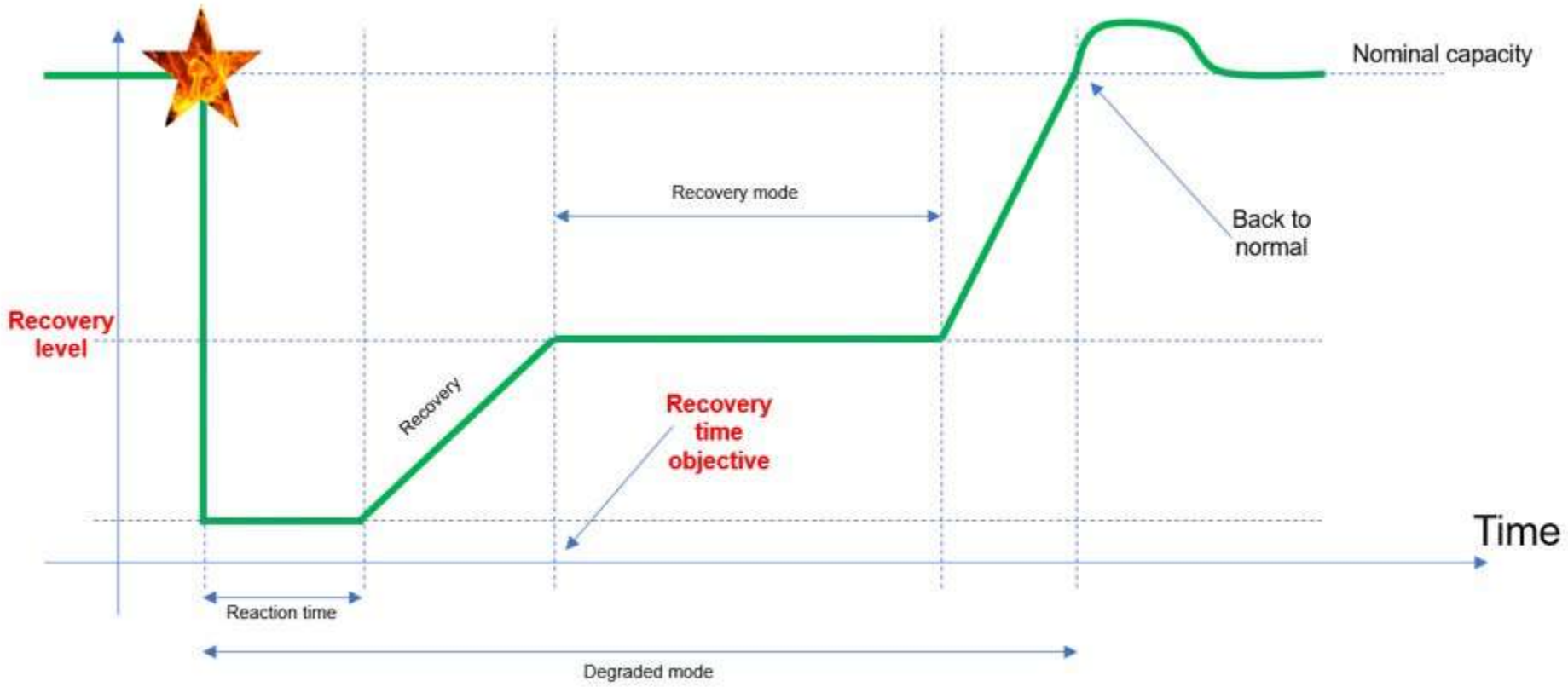
Day 3

1. How the region is dealing with pandemics and war-related disruptions today
2. Prioritizing actions/solutions in the EECA region and in individual countries
3. Defining technical assistance (TA) needs & aspects for inclusion into funding requests
4. Next steps

Day 1

Why and how the Global Fund achieved ISO 22301 certification for its Business Continuity Management System (BCMS)

Anatomy of a Disaster



Recovery Time Objective (RTO) : time after which the activities are resumed at least at the recovery level

Recovery Level : level (fraction of the nominal capacity) that the organization can sustain for an undefined period of time

Rationale for the Global Fund's Business Continuity Management System

In order to reach its strategic objectives, the Global Fund relies on key business processes supported by critical information systems.

Lack of preparation in the event of a disruption could interrupt these processes, preventing the Global Fund from performing its lifesaving mission and potentially threatening the existence of the organization.

Organizational resilience and business continuity management must ensure that the Global Fund's key business processes can recover to a pre-defined level.

For the Global Fund, business continuity and organizational resilience center on:

- identifying and anticipating possible threats to business activities
- defining the steps that the Global Fund can take to prevent these threats from occurring
- implementing and documenting these steps in a manner appropriate to the materiality of risks and proportionate to assets to be protected
- verifying on a regular basis that the steps are effective and adequate as the Global Fund evolves over time
- training, educating and informing staff and consultants about risks, threats and measures being put into place to ensure that the Global Fund can continue to operate in a business disruptive environment.

Organizational resilience is a product of preparedness and preparedness is best achieved in the absence (as opposed to in the course) of a business disruption. In this context, a timely investment in business continuity management can safeguard the Global Fund's mission, people, resources, and reputation in the years ahead.

Project risks & issues

Definition of the scope

- We must develop the BCMS on solid grounds
- Avoid scope ambiguity and changes
- Make clear definition on what is excluded

Top management buy-in and support

- Additional effort on communication

Contribution of Global Fund staff

- although minimal, there must be a validation effort to be provided by Global Fund staff and in some cases, direct contribution (tests & exercises)

Contribution to the BC/DR plans

- Global Fund personnel have already contributed to the development of the contingency plans, repetitive effort to be avoided

Project scope:

- The BCMS will be implemented across all Global Fund Secretariat divisions and processes, the Office of the Inspector General (OIG), Global Fund administration. It will cover all related IT operational management processes, IT systems/applications/ platforms and facilities of the Global Health Campus

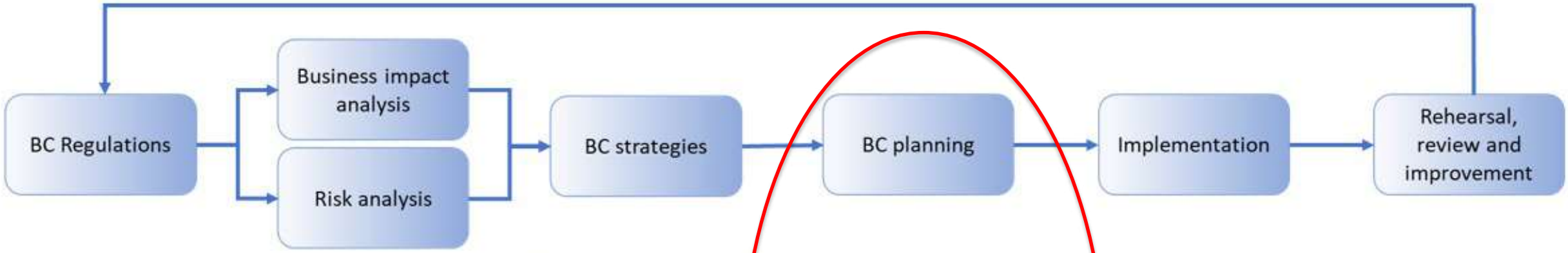
  => While the Secretariat falls within the scope of the effort, external partners do not

  => This holistic effort will include finalizing & adjusting IT and Business BCP documents, and developing detailed, integrated disaster recovery plans (DRPs) for all systems

Implementing a BCMS

Continual improvement cycle

«Covid led us to start here in 2020»



- Provide general BC principles, decisions and responsibilities
- Establish BC guidance or standard

- Assess impacts of business disruptions and RTOs
- Identify critical operations
- Identify and map BC risks

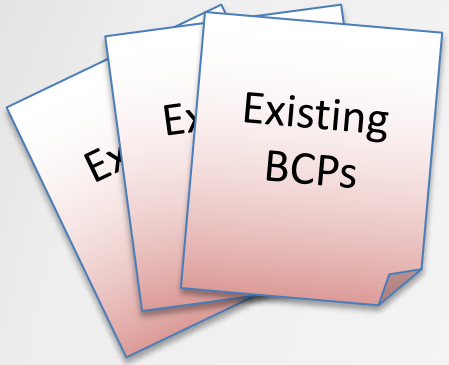
- Examine strategies to
  1. ensure continuity of critical operations
  2. recover critical resources
  3. maintain core services
- Design BC arrangements and risks reduction measures to implement

- Document BC/DR procedures based on BC/DR arrangements
- Develop education and practice plan
- Develop review and improvement plan
- Develop communication plan

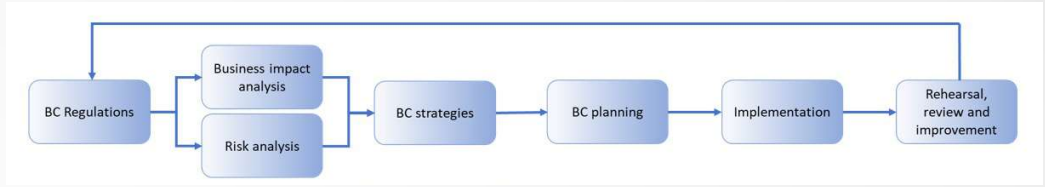
- Implement BC/DR arrangements
- Implement risk mitigation measures
- Implement education and practice

- Exercise BC/DR plans & procedures
- Tests BC/DR arrangements and risk mitigation measures
- Inspect & review BCM
- Correct & improve

Leveraging existing work into an ISO 22301 compliant BCMS

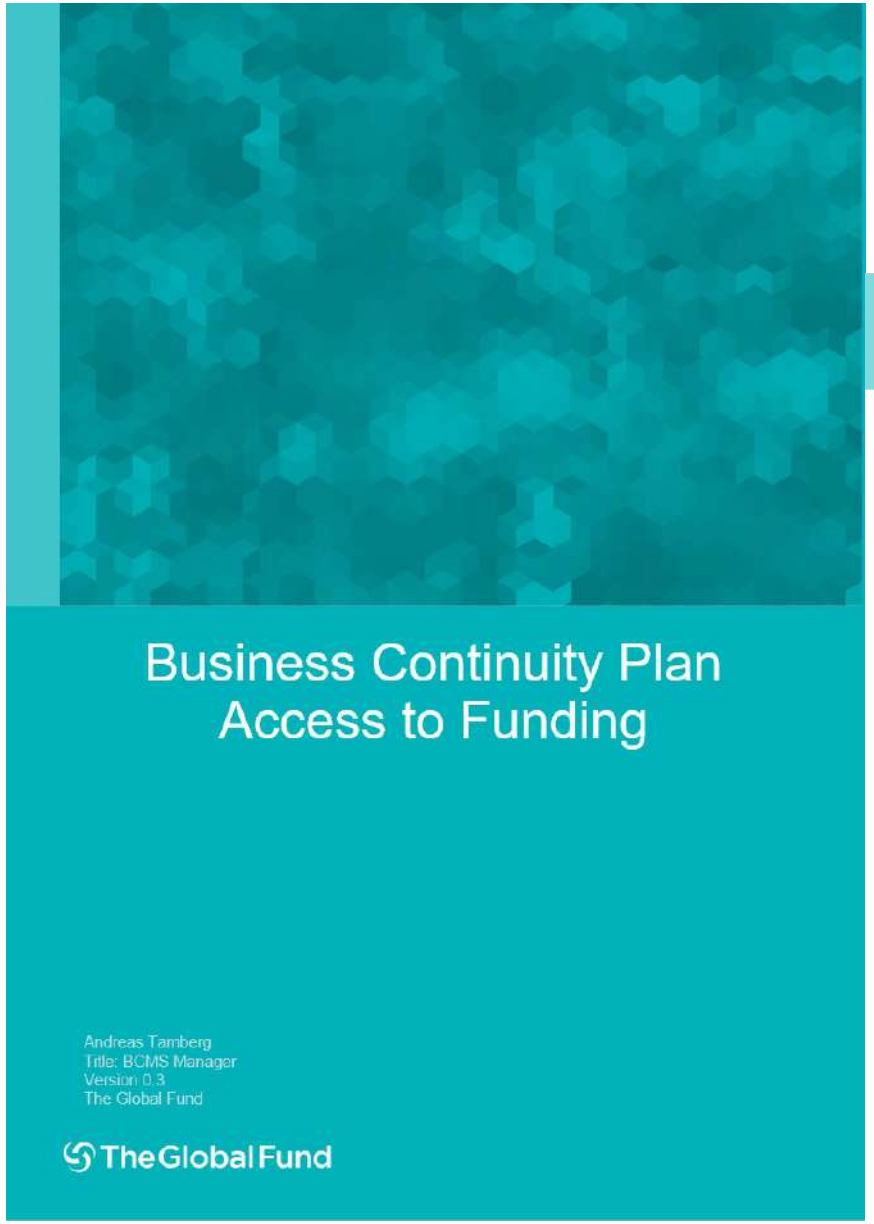


BCM lifecycle



Draft BCPs

(in conformity to ISO-22301)

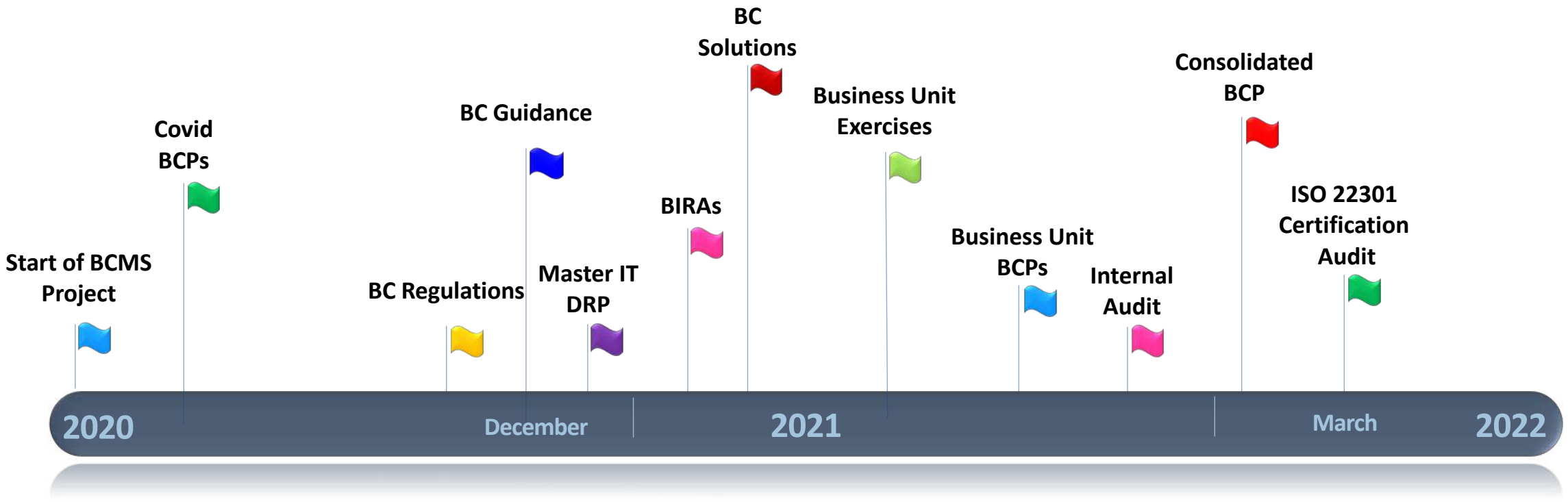


The Global Fund

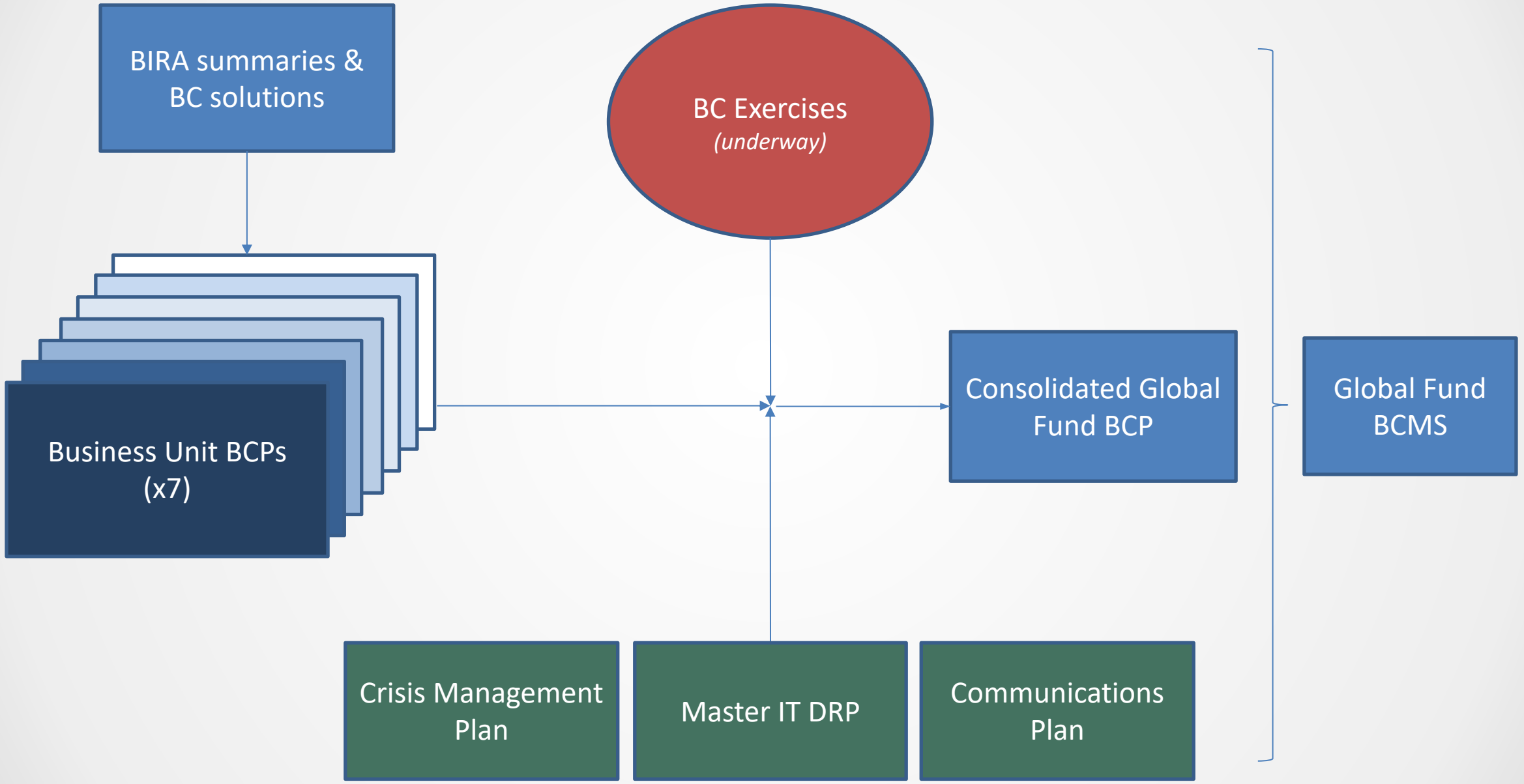
1 Contents

1 Contents 2
2 List of changes 3
3 Distribution list 4
4 Introduction 5
4.1 How to use this plan 5
4.2 Purpose and audience 5
4.3 Objectives 5
4.4 Assumptions 6
4.5 Duties & responsibilities 6
4.6 References 7
5 Roles, responsibilities and contact details 8
5.1 Business continuity team 8
5.2 From other services/units 8
5.3 External contacts 9
5.4 Specific responsibilities 10
6 Communication requirements and procedures 11
7 Resources required 12
8 Business Continuity Procedure 13
9 Validity and document management 15
10 Appendix : Forms & templates 16
10.1 Appendix A – Alternate site or work from home resource requirements 16
10.2 Appendix B – Emergency Operation Center location 16
10.3 Appendix C - Vital records 16
10.4 Forms 16
11 Document Control 17
11.1 Circulation Control 17
11.2 Sign-off 17
12 Document Issue Log 17
12.1 Open Issues 17
12.2 Closed Issues 17
13 Terms and Abbreviations 17

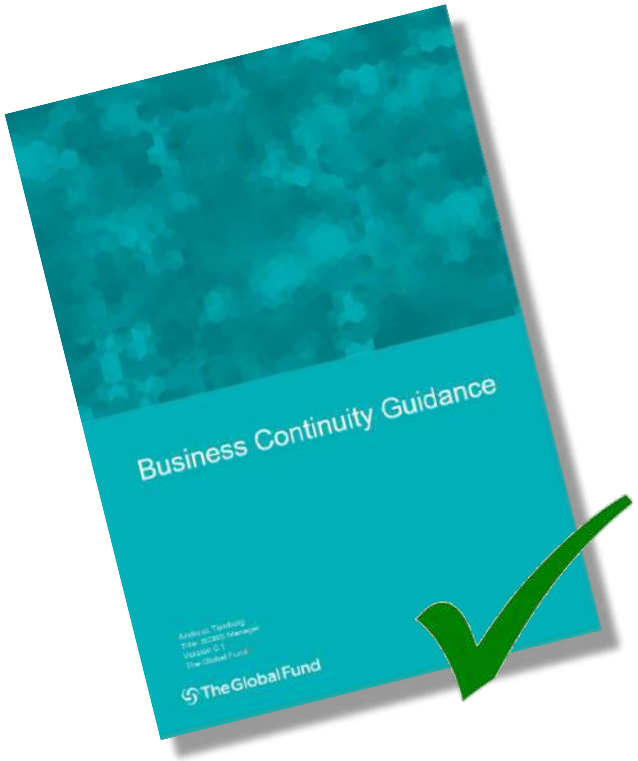
BCMS Milestones

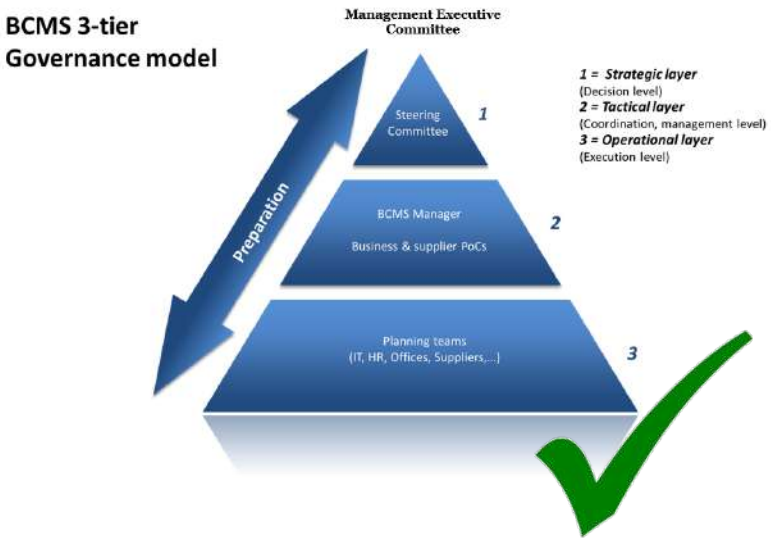


The Global Fund's BCMS Architecture



The Global Fund's BC Regulations, Guidance and Governance Model





Business Continuity Regulations

- States objectives, scope and governing principles of BC at the Global Fund
- Refers to the ISO 22301 standard
- Presents main BC roles and responsibilities
- Endorsed by the MEC

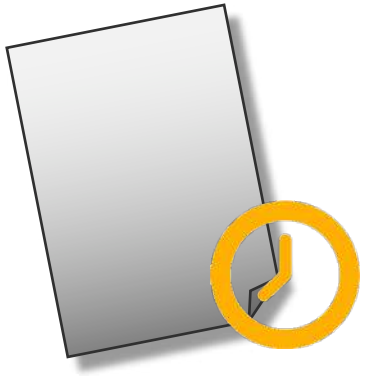
Business Continuity Guidance

- 60+ page "cookbook" to implement and maintain BC at the Global Fund
- Fully complies with the ISO 22301 standard
- Guarantees route to certification
- Describes precisely the entire BCM process to be performed at the Global Fund (processes, "how-to", expected outcomes, …)

BCM 3-tiers governance model

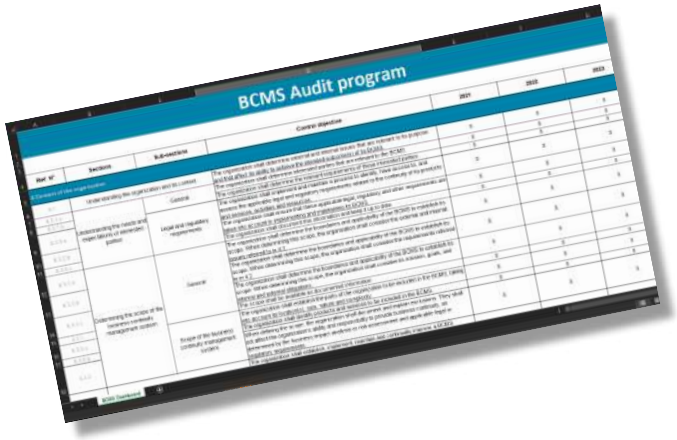
- Describes precisely the roles and responsibilities to run and maintain BCM within the Global Fund
- 3-tiers
  - Strategic – decision level
  - Tactical – management level
  - Operational –execution level

Exercises, Audit & Maintenance *(relative to the ISO 22301 Standard)*



BC/DR exercise program

- To be prepared & conducted once the BC plans are completed
- IT DR plans soon ready to be tested



Triannual internal audit program

- ISO 22301 compliant
- Required step prior to certification
- To be integrated in the general internal audit program
- Scheduled for summer 2021

External Certification Audit *(timing TBC)*

- Stage I: August 2021
- Stage II: September 2021
- Annual surveillance audits in 2022 & 2023

Health service continuity planning as an essential component of an ‘end to end’ BCMS

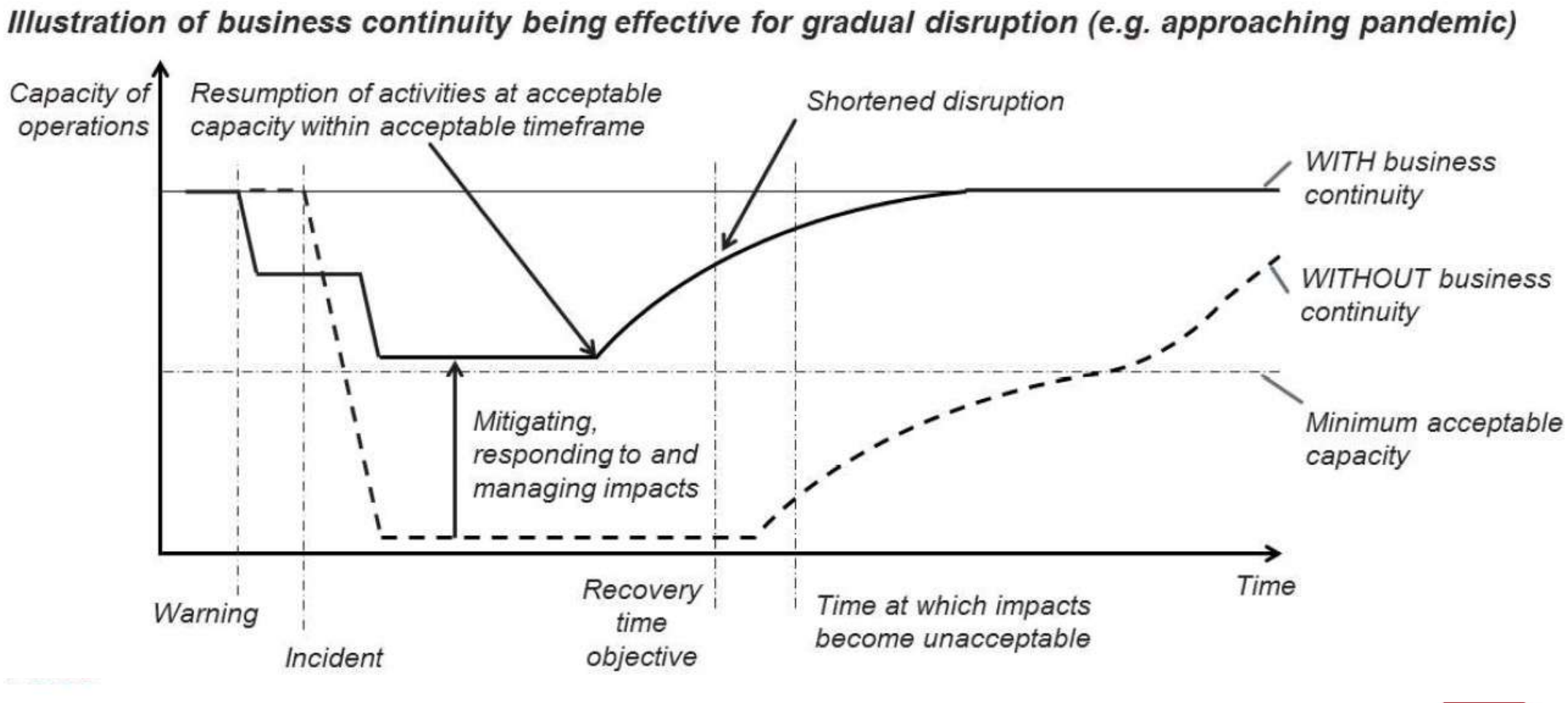
World Health Organization

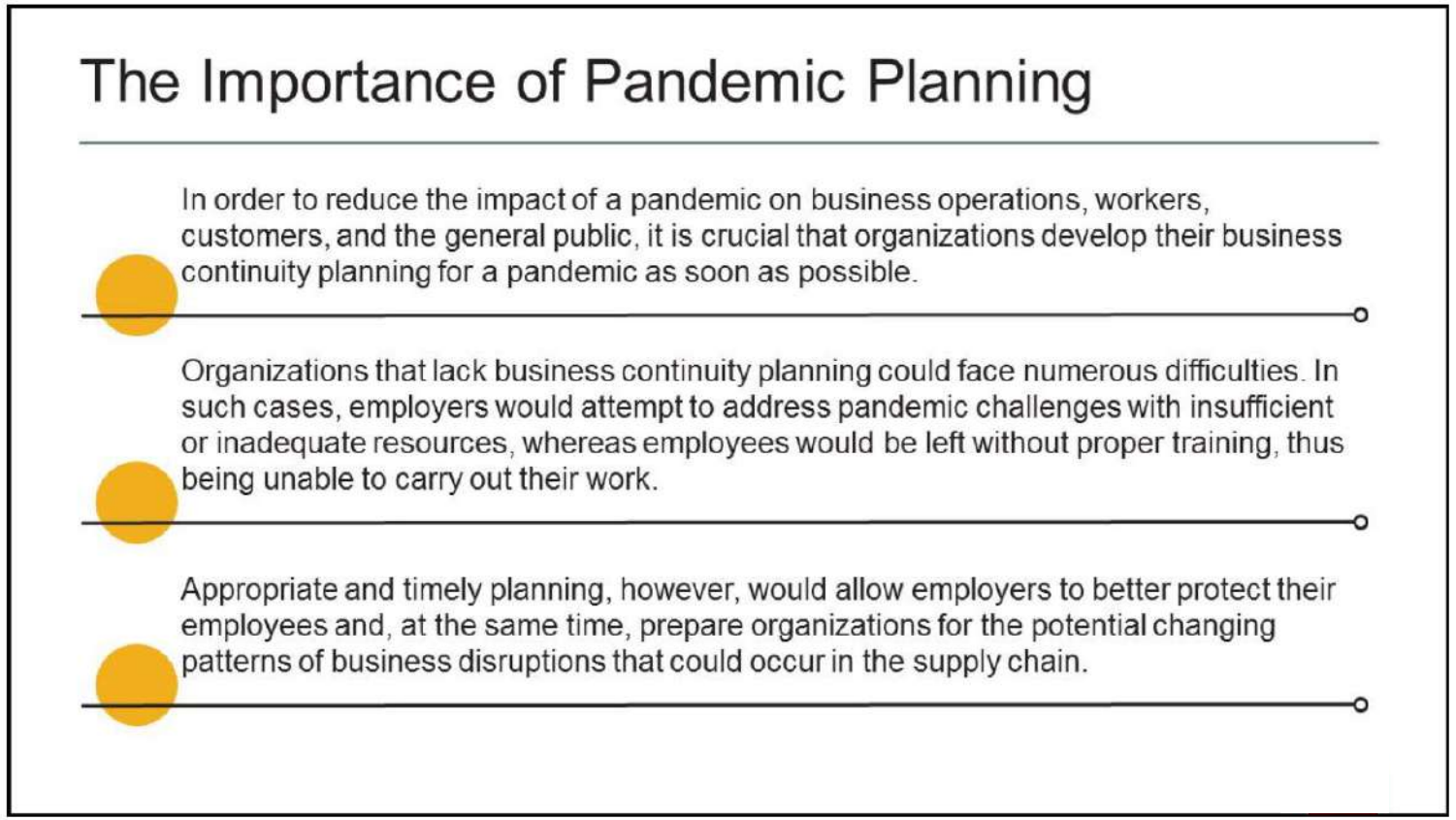
Health service continuity planning for public health emergencies

Sohel Saikat *(Technical specialist, team lead)*
Yu Zhang *(Consultant)*
Health Systems Resilience & Essential Public Health Functions team
World Health Organization

Pandemic preparedness and workforce planning in EECA as a BC priority

The importance of business continuity in pandemics





An organization's most important and valuable asset is its workers. They are well informed about their jobs and specifics, and often are more aware about the business than the employers themselves. Thus, it is crucial that they are involved in the planning phase of the business continuity plan. Including them from early on in the planning process will ensure that they are engaged and motivated, which can lead to a more effective emergency plan for the organization. Engaging workers will ensure that they understand the planning process and are able to help the organization in implementing it.

Source: Missouri Department Of Health And Senior Services. *Pandemic Influenza Business Planning Toolkit*. Accessed March 23, 2020.

US Centers for Disease Control and Prevention

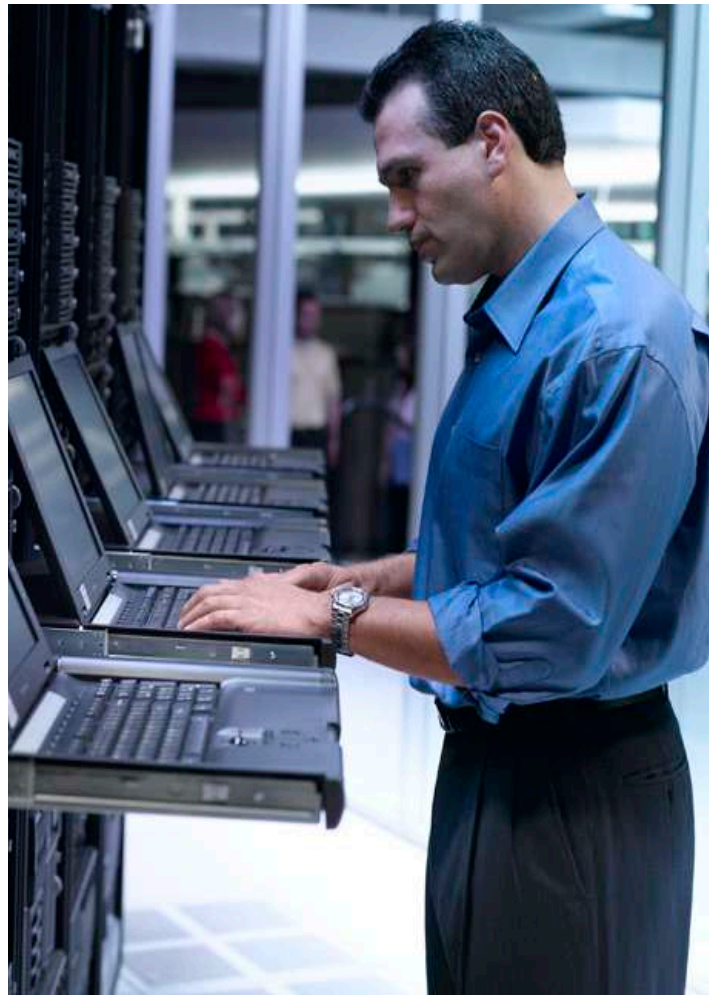
Regional Office for Eastern Europe and Central Asia

The link (and difference) between business continuity and disaster recovery

What is Business Continuity?

It is…

- A way of doing business and continuing to stay in business.
- A plan to assure business processes - including suppliers and service providers - are always available to meet critical needs.
- An integrated approach that links business continuity & recovery with IT availability management and security.
- An on-going management process to improve the operational resiliency of business processes and associated IT service levels.

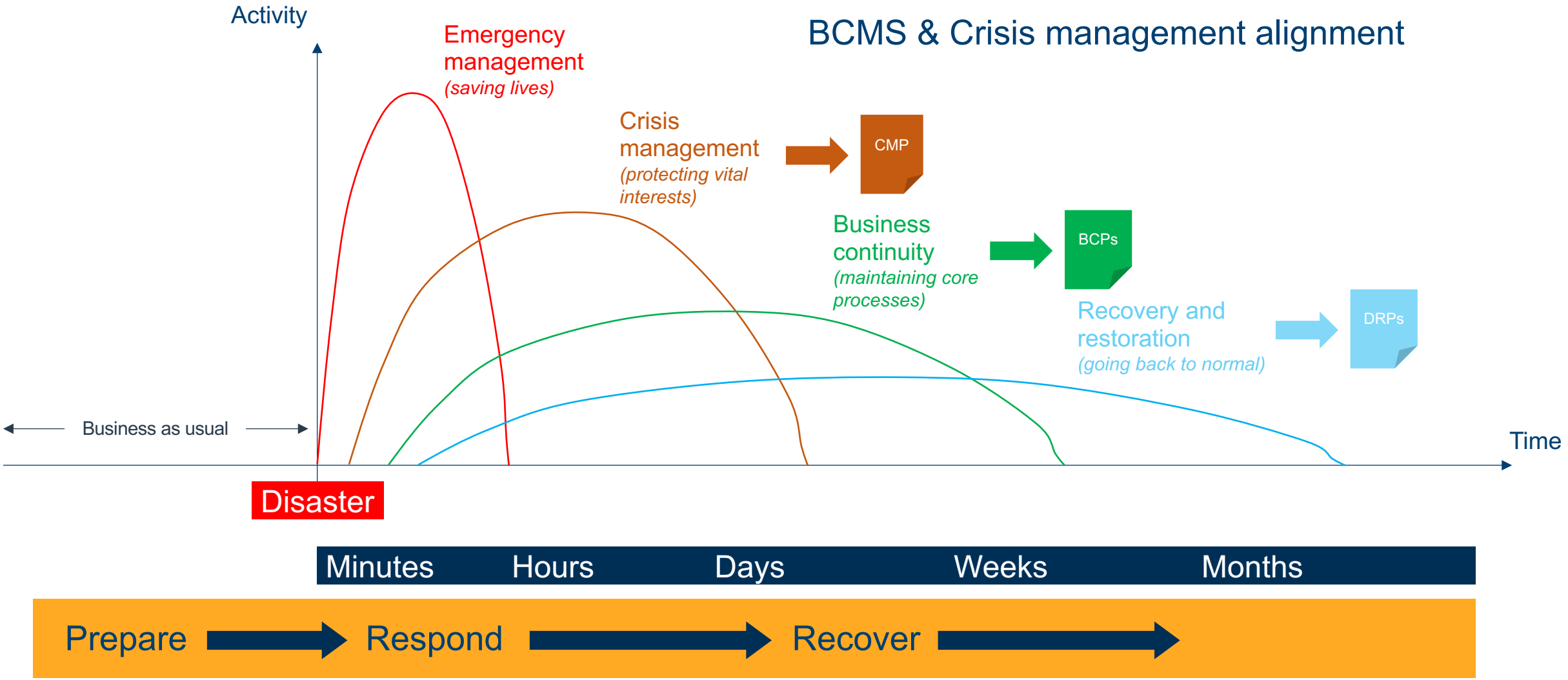


It isn't…

- A specific product, technology or service
- A "project" with a beginning and end
- Just disaster recovery or high availability

The BCM Continuum

(The BCMS links BCPs to Emergency Management, Crisis Management Plan and IT DRP)



Linking crisis management, business continuity and incident response

Senior Management Committee

Crisis Management

Lead : Situation Response Team

Focus : Strategic

- **Role** : strategic direction, communication
- Only activated in case of significant impact

Divisions & Departments

Business Continuity

Lead : Heads

Focus : Tactical

- **Role** : Ensures that core processes can be resumed through availability of key people and technologies
- Reports to SMC

IT/Admin/HR

Incident Management & Disaster Response

IT/Cyber incident response

Building/facilities incident management

HR personnel decisions

Focus : Operational

- **Role** : Problem solving and incident management
- Reports to SMC

Business Continuity Plans -- *Guides to alignment and action*

Organizational priorities during the Global Fund's new round of funding

Implementers

SoS Consortium

APH

100% Life

CPH

SEH

Regional networks

Technical agencies

WHO

UNAIDS

US CDC

USAID

EJF

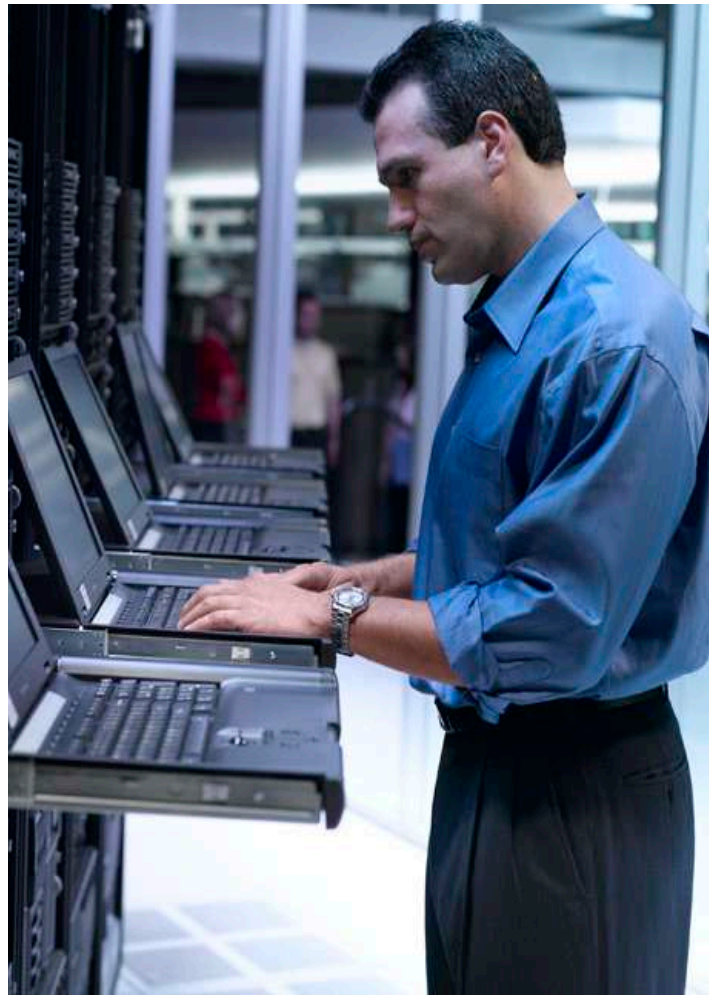
Day 2

Essential characteristics of a Business Continuity Management System

What is Business Continuity?

It is…

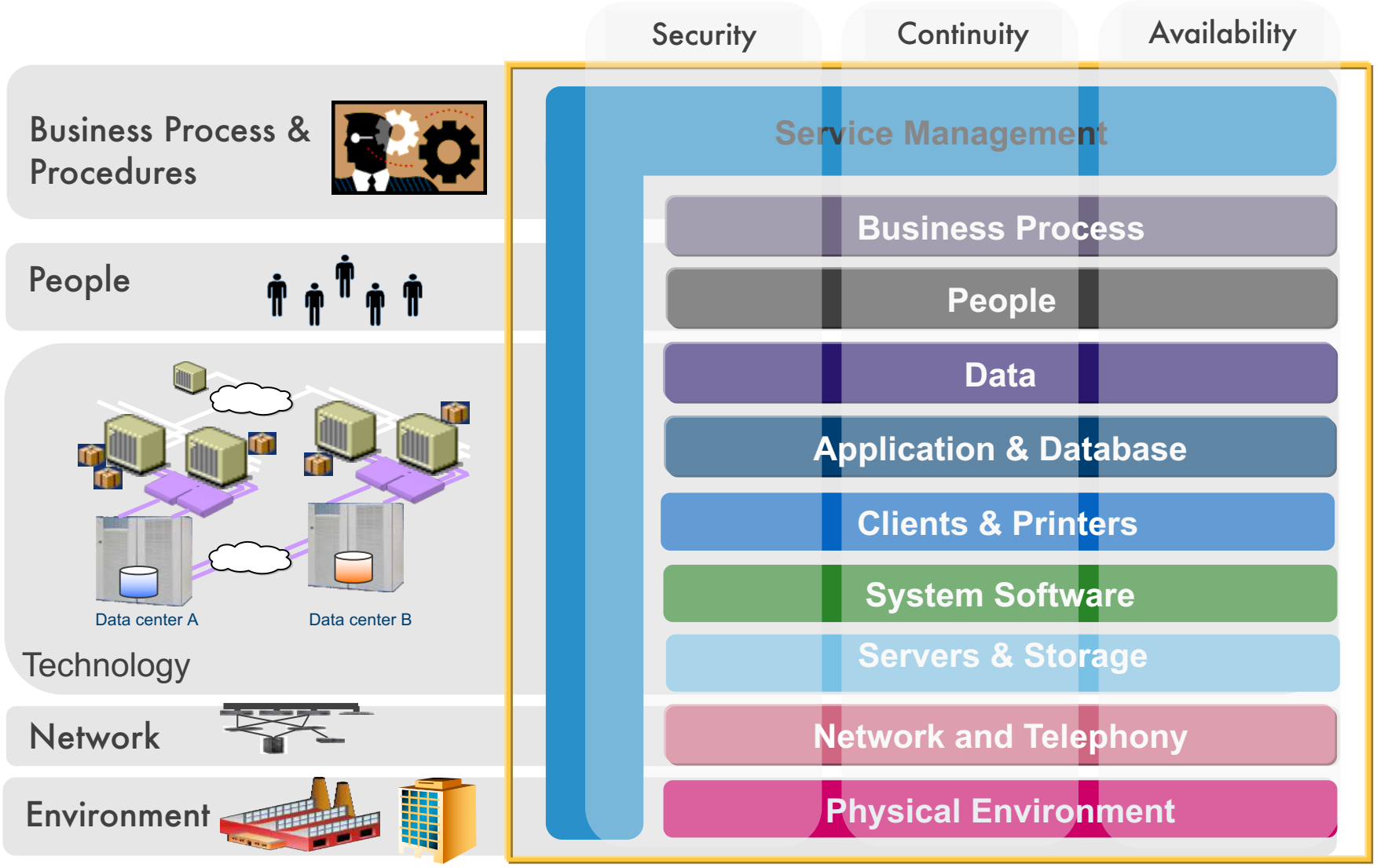
- A way of doing business and continuing to stay in business.
- A plan to assure business processes - including suppliers and service providers - are always available to meet critical needs.
- An integrated approach that links business continuity & recovery with IT availability management and security.
- An on-going management process to improve the operational resiliency of business processes and associated IT service levels.



It isn't…

- A specific product, technology or service
- A "project" with a beginning and end
- Just disaster recovery or high availability

Setting the stage for business continuity



BCM 101 – Basics

Definitions

- Business continuity
  - *“Capability of an organization to continue the delivery of products and services within acceptable timeframes at predefined capacity, during a disruption”*

- Business Continuity Management System
  - *“Part of the overall management system that establishes, implements, operates, monitors, reviews, maintains & improves business continuity”*

- Business Continuity Plan
  - *“Documented information that guides an organization to respond to a disruption and resume, recover, and restore the delivery of products and services consistent with its business continuity objectives”*

Key principles

A collective responsibility of the board of directors and the executive management

Readiness for all types of disruptive incidents, its consequences on the organization and on all its stakeholders

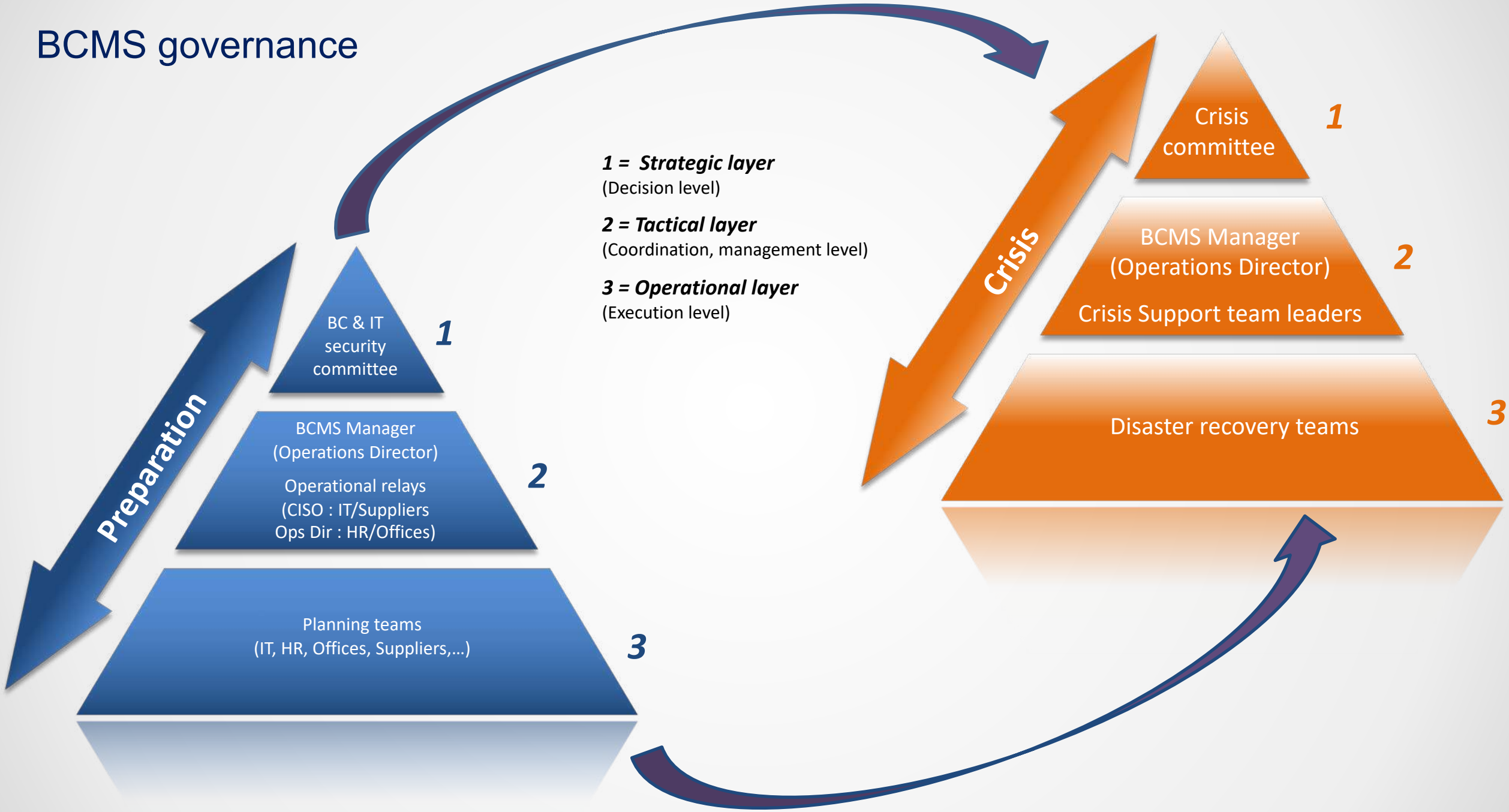
Recovery objectives commensurate to the relevant risks and their severity, and within the boundaries of the laws and regulations

A crisis communication, with internal and external stakeholders

Periodic tests and exercises to assess the effectiveness of the business continuity framework

A periodic review by an independant 3rd-party

BCMS governance



Business continuity management

Disaster recovery plan

HR

Premises

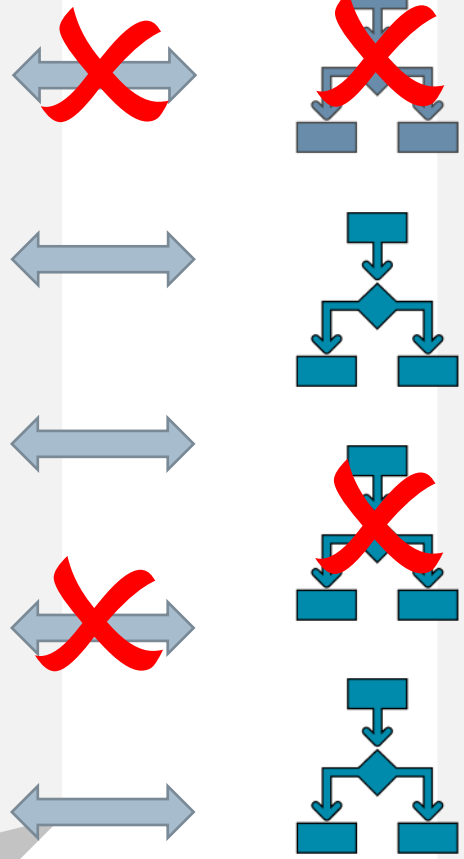
IT

Resources

nmunications

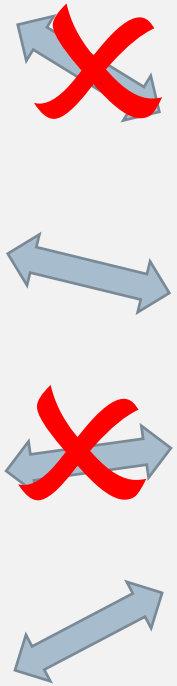
Suppliers

rastructures



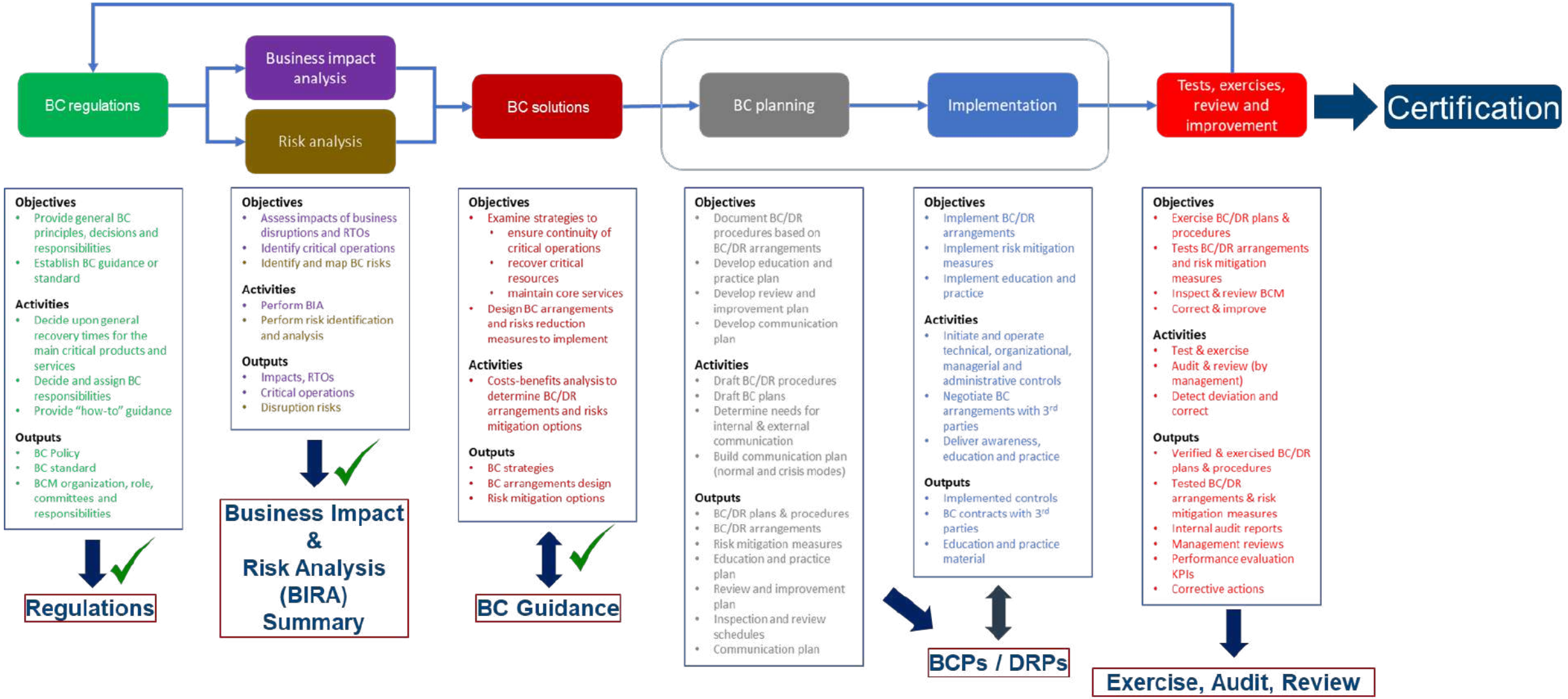
Processes

Business continuity plan



- Institutions
- Authorities
- Beneficiaries
- Donors
- ...

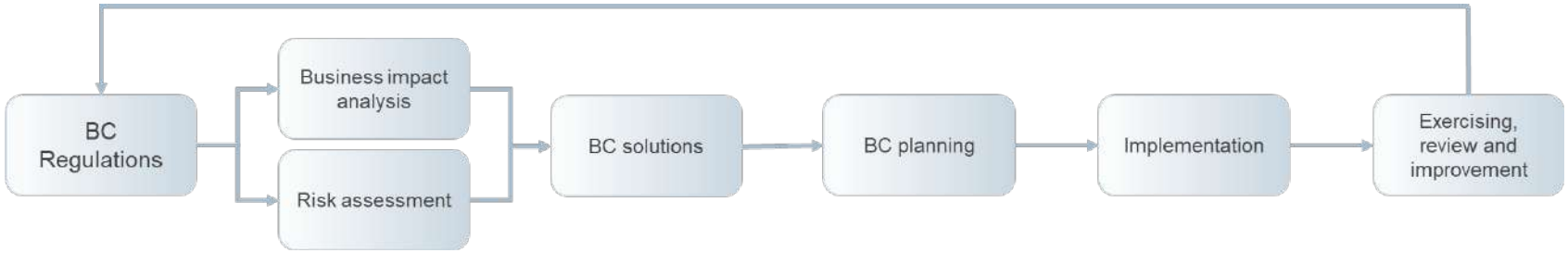
BCM process lifecycle *(per ISO 22301)*



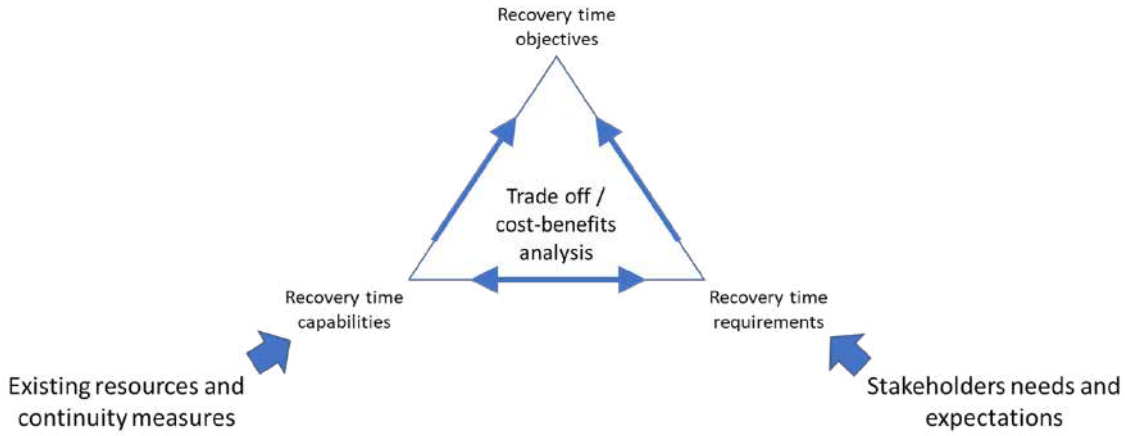
BCM continuum & process lifecycle

- The BCMS links BCPs, the Crisis Management Plan and IT DRP

- A proven method to develop exercised, tested and fit-for-purpose BC & DR plans



- Business continuity solution that takes in account Business continuity requirements & recovery capabilities of IT



BCMS deliverables

- **BCMS minimal set of documents required by the auditor**
  - Organizational context (from ISMS)
  - Register of regulatory and other requirements and evidence of compliance
  - Scope of the BCMS (derived and adapted from ISMS)
  - BC Policy & objectives
  - Evidence of BC competences
  - BIA & risk assessment process
  - BC & DR strategies considered and selected
  - BC/DR plans & crisis management plan (realized and under development)
  - Post-exercise reports
  - BCMS monitoring
  - Internal audit reports
  - Management review minutes
  - Nonconformities & corrective actions
- **Recommended BCMS documents**
  - SLA with main contractors (incl. response & notification procedures)
  - BIA & risk assessment results
  - Incident response process overview
  - Awareness & training programmers'
  - Communication plan (BCMS & in case of disruptions)
  - Exercise schedules
  - BCMS monitoring evidence

Key concepts

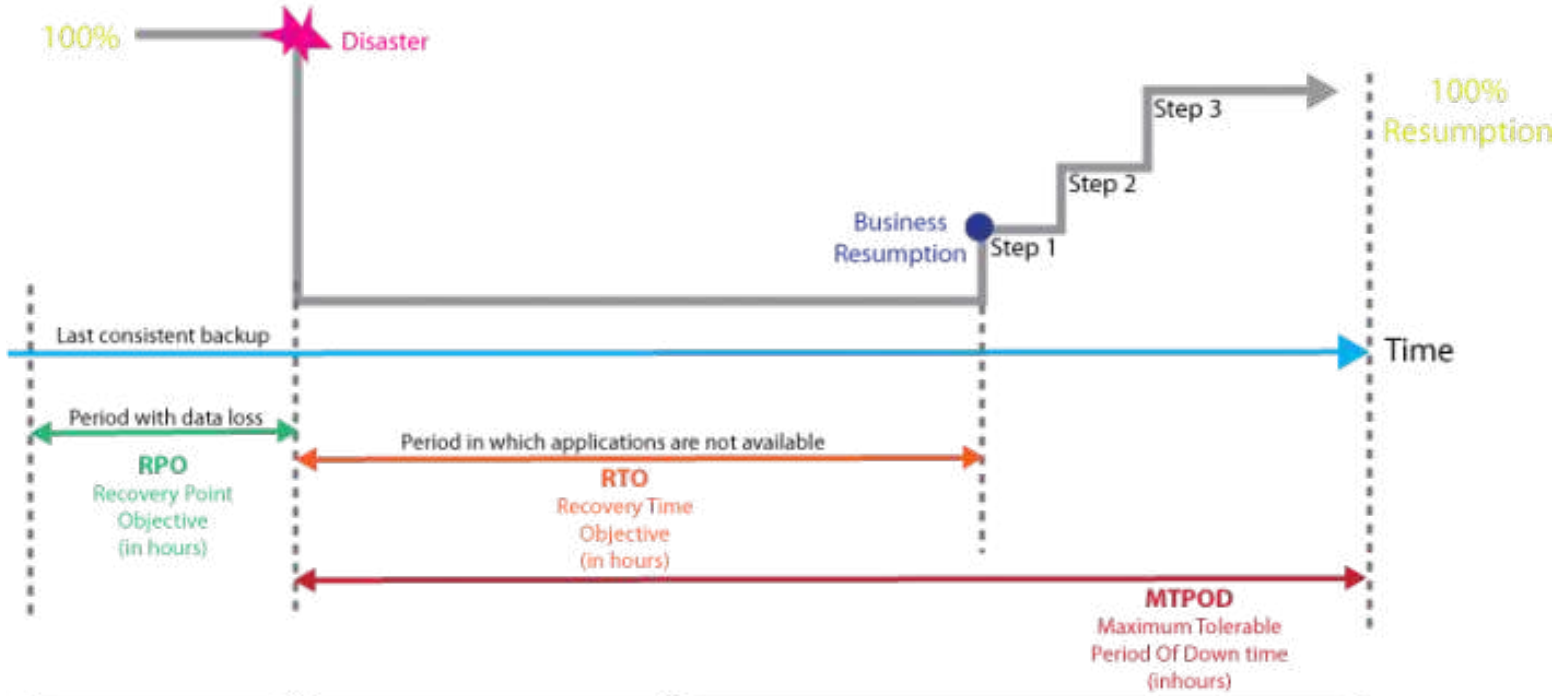
1. Recovery Time Objective (RTO)

2. Recovery Point Objective (RPO)

3. Maximum Tolerable Period of Down Time (MTPOD)

Because it has too many letters, MTPOD is also known as a 'Maximum Acceptable Outage' or MAO)

Defining RTO, RPO and MTPOD



RPO
is the maximum acceptable level of data loss following an unplanned "event".

RTO
is defined as the length of time that a business process could be unavailable before the business unit's operations are significantly impaired.

MTPOD
is defined as the "duration after which an organization's viability will be irrevocably threatened if product and service delivery cannot be resumed.".

MTPOD can be calculated on the following factors :

> The maximum time period after the start of a disruption within which each activity needs to be resumed
> The maximum level at which at which each activity needs to be performed after resumption
> The length of time within which normal level of operation need to be resumed

Business Impact and Risk Assessment (BIRA)

Business impact and risk analysis (“BIRA”)

- The Business Impact Analysis or BIA is a systematic and documented process aimed at assessing the potential effects of a disruption to critical business operations following a disaster. The BIA is complemented with a Risk assessment, the objective of which is to assess the risk that business activities will be disrupted, identify the risk that prioritized activities and related resources will be disrupted, establish a process to determine which business continuity risks require treatment and use this process to determine which continuity risks need to be treated.

- Questions are geared toward ***worst-case*** disruption scenarios form which the organization can reasonably expect to recover.

A BIRA frames the process context, priority, time sensitivity & disruption risk for business continuity solutions and plans based on defined scenarios

Detailed objectives

- Understand the department **context** / **organization** / **key processes**
- Understand what is the **Maximum Outage Acceptable for key processes** identified
- Understand what is **needed at minimum** to achieve **mandatory objectives** during **disruption**
- Understand **which disruption** could **strongly impact** key processes

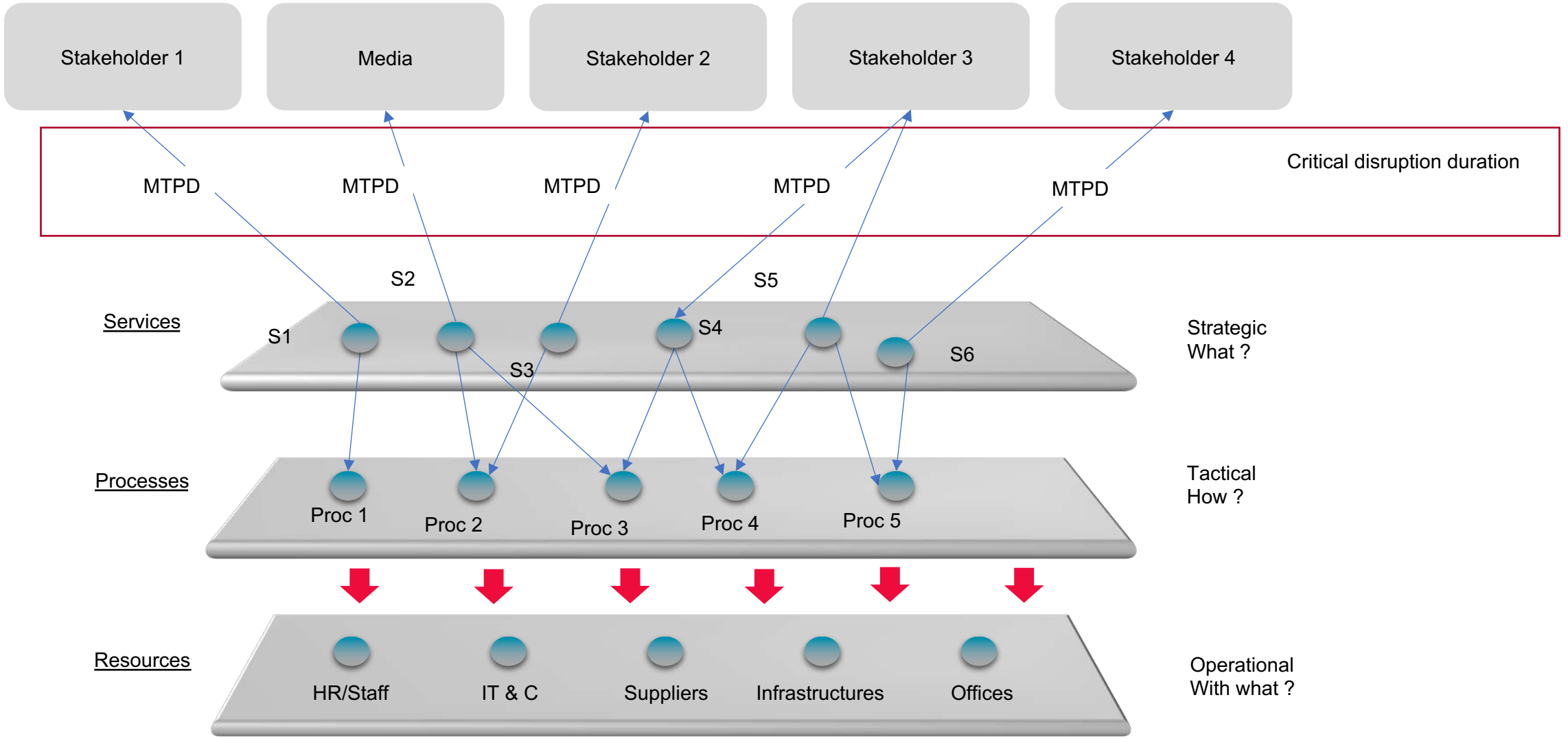
Workshops with business to get information complementary to existing BCPs

Scope

- ✓ OIG
- Finance
- ✓ Com
- GMD
- Supply Ops
- ✓ Admin
- ✓ IT
- ✓ Ethics
- ✓ HR

BIRA questionnaires

Business impact analysis - visualizing interdependencies



Risk analysis

- *Identifying threats (even emerging ones)*

Environmental threats

Related to natural events, floods, earthquake, electrical storms, volcanic activities, …

Human caused threats

Accidental or deliberate, it includes errors of use, theft, sabotage, violence, terrorism, war , …

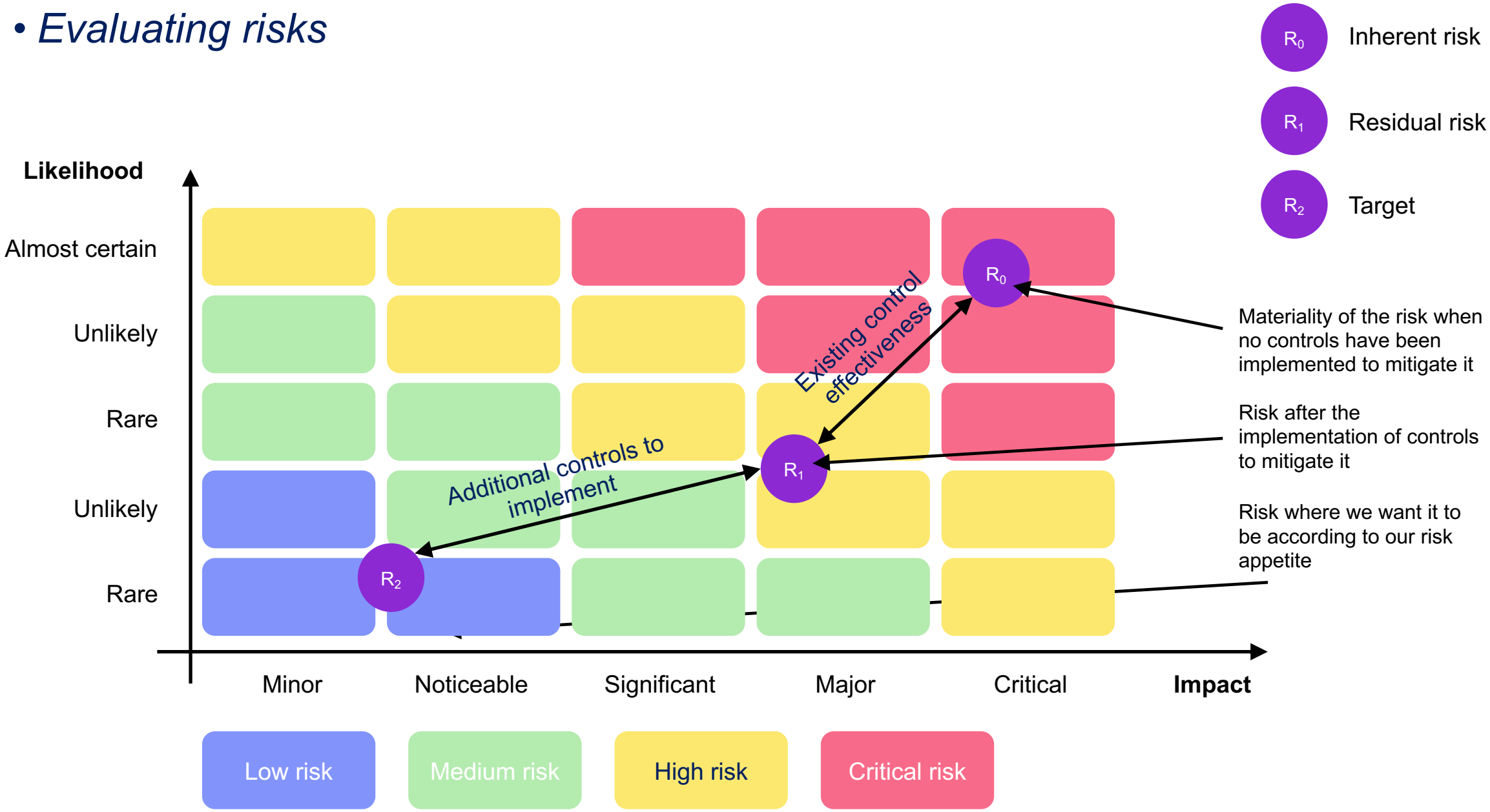
Infrastructure threats

Mostly related to critical infrastructure failure, it refers to problems with public transportation, loss of essential service, power supply disruptions, …

IT related threats

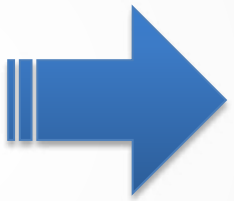
Threats having the potential to harm assets such as information, processes and systems, cyberattacks, massive system failures, …

• *Evaluating risks*



BIRA questionnaire

- **Business impact and risk analysis questionnaire**
  - **I. Introduction**
  - **II. Process description**
  - **III. Business Impact Analysis (BIA) for worst case disruption scenarios**
  - **IV. Dependencies, resources, data, and workarounds**
  - **V. Risk Analysis of various disruption scenarios**
  - **Annex 1: Risk Heat Map**
  - **Annex 2: Disruption examples**



A "BIRA" will set the stage for development of business continuity solutions and plans

BIRA Output *(Requirements that Link Process Criticality, Time Sensitivity and Recovery Complexity)*

Implement Market Shaping Strategy (Pooled Procurement Team) D2

Responsible manager(s): PR Services Manager ; Strategic Sourcing Manager

Business Impact Analysis

Timeline	<1d	1d - <1wk	1wk - <1mo	1mo - <6mo	>6m
Achievement of business objectives	Very low	Low	Medium	High	Very high
Reputational damage	Very low	Low	Medium	Very high	Very high
Stakeholder confidence	Very low	Low	Medium	Very high	Very high
Pledge and commitment exposure (income)	Very low	Low	Medium	Very high	Very high
Financial loss (resource efficiency)	Very low	Low	Medium	High	Very high

Process, Dependencies, Resources, Data and Workarounds

Process description

Process descriptions	Deliver strategic objectives of the Market Shaping Strategy through key tools, including the Pooled Procurement Mechanism (PPM), to leverage the Global Fund's health product spend to drive value. This includes managing health product demand for pooled volumes and strategic sourcing for timely delivery of quality-assured health products to the point of delivery in countries. This also includes managing the quality assurance policy.
General resources	50 people IT systems (GFS, O365, DataHub / GIS, Service Now, Website, Wambo (Coupa), GOS (Salesforce), PQR) GHC

Business Impact Analysis

Frequency	TBC
period sensitivity	January / February
MAO	1mo - <6mo

Dependencies, Resources, Data and Workarounds

Dependencies	Downstream: 'C2. Quality Grants: forward visibility of demand E1. Grant Implementation: Purchase Requisitions submissions and approvals H1. Info Systems: GFS, Coupa Upstream: 'E1. Grant Implementation: Receipt of deliveries by PRs J2. Manage Financial Transactions D5. Reconcile and Close Grants G1. Report Results
Resources	2 or 3 people IT systems (GFS, O365, DataHub / GIS, Service Now, Website) Key PPM Suppliers Key PSAs
Data	**Critical data** List of eligible suppliers (public domain – QA team), Wambo transaction data (savings) **Critical reporting** Annual Supplier Performance reports KPI 12a (product availability) & b (savings)
Workarounds	Remote WHO location Transfer to another department (GMD, TAP, FA)

Risk analysis

Scenarios	Likelihood	Impact	Risk rating	Recovery complexity
HR unavailability	High (4)	1 = Low	Medium	TBC
Supplier unavailability	TBC	TBC	TBC	TBC
IT system disruption	Low (1)	4 = Very High	Medium	TBC

The Global Fund

A “clean” BIRA

Business Impact Analysis					
Achievement of business objectives					
Reputational damage					
Stakeholder confidence					
Pledge and commitment exposure (income)					
Financial loss (resource efficiency)					
MAO	<1d	1d-1wk	1wk-1mo	1mo-6mo	6m-1yr

Business Impact Risk Analysis

Process description	Activity description	Description of your activity (subprocesses, main activities responsibilities) and general information of the department
	General resources	Business owner needs (HR, IT, building, etc.)
	Process descriptions	Description of key processes

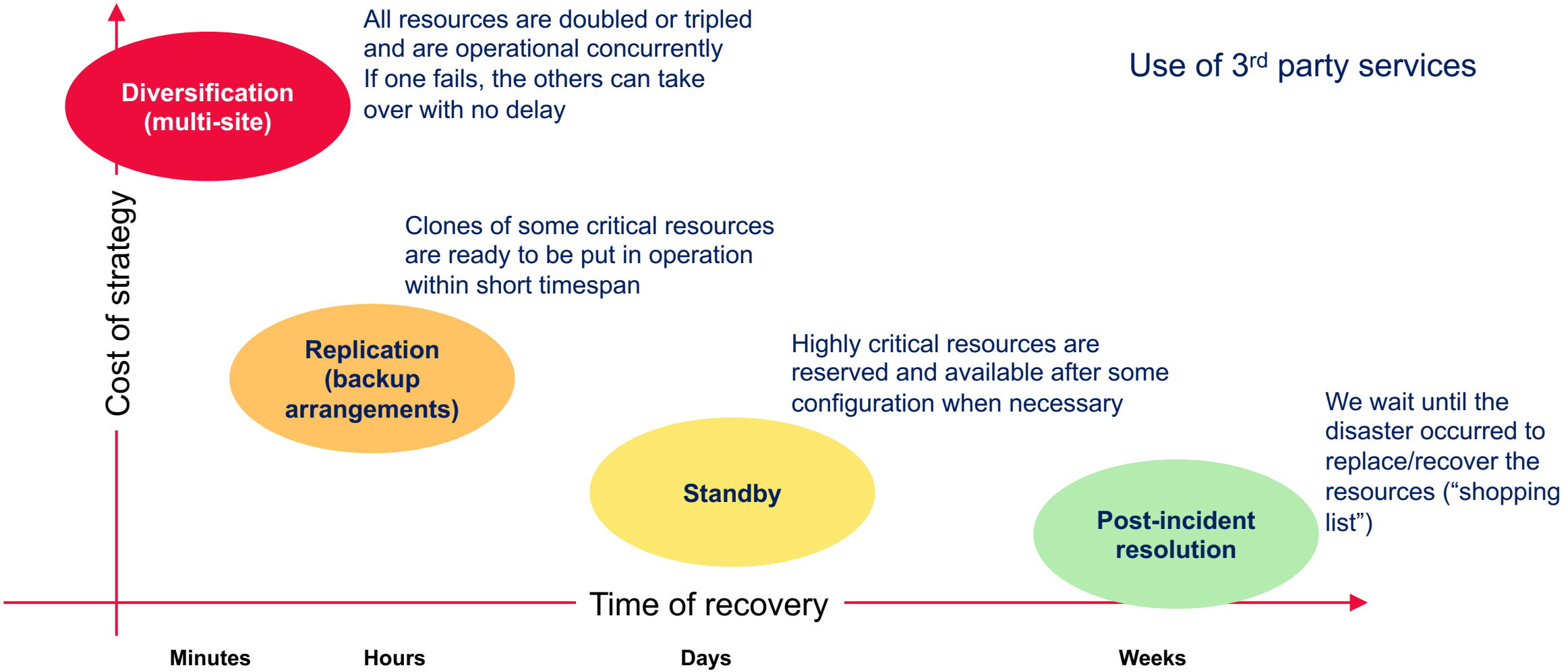
Business Impact Analysis	Frequency	Importance of key outputs over a calendar year (or longer if required). This will help identify the period of “Maximum Acceptable Outage (MAO)
	period sensitivity	
	BIA ratings	Impacts on time period sensitivities and previous variables on the 5 risk dimensions

Dependencies, Resources, Data and Workarounds	Dependencies	Which IT systems, critical providers, and internal resources (data received from another processes) are critical for completing the process
	Resources	Minimum resources would be needed in the case of a disruption
	Data	Processes require critical data (inputs) and/or critical reporting
	Workarounds	Information about workarounds for disrupted processes

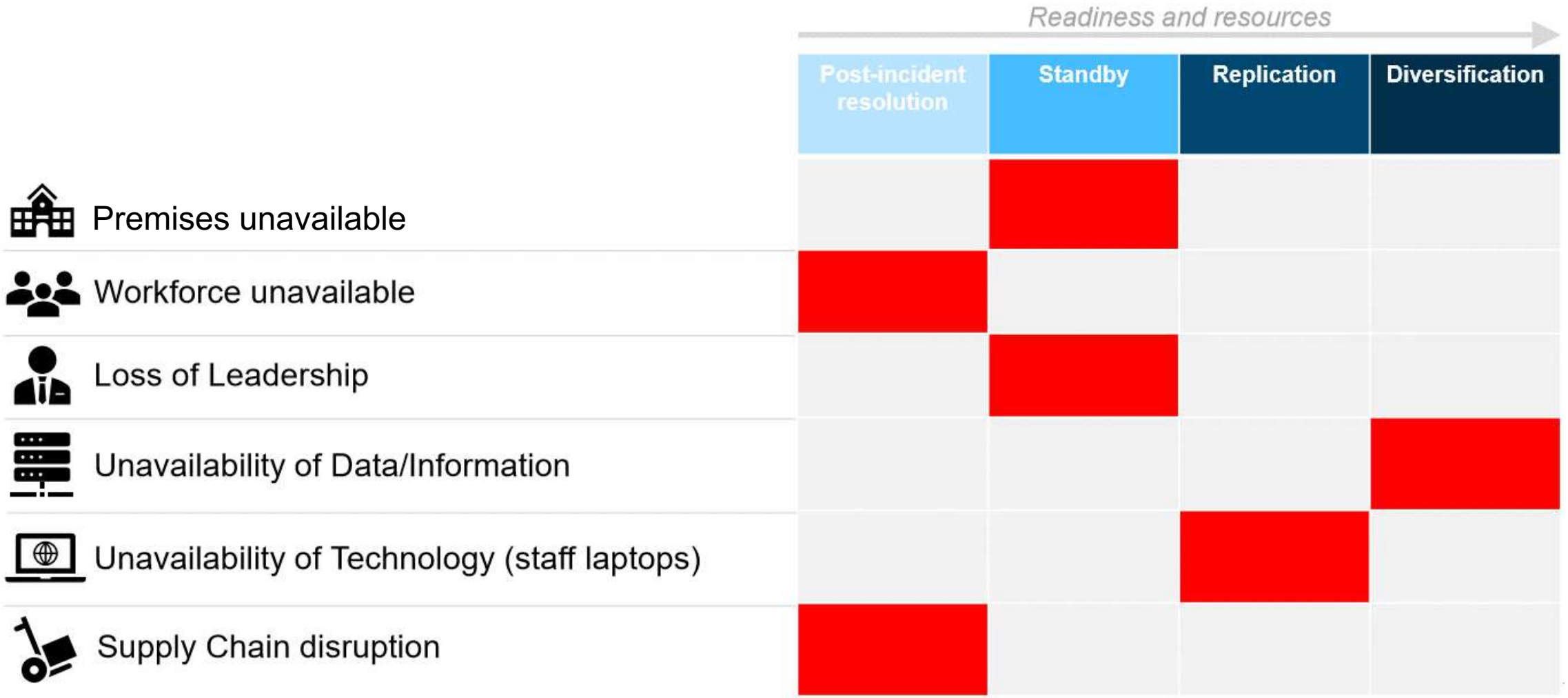
Risk analysis
Kind of outage which could strongly disrupt a process. Difficulty in case of outage to recover the service. Likelihood and impact of each type of outage. Rate the recovery complexity.

Business continuity solutions & strategies

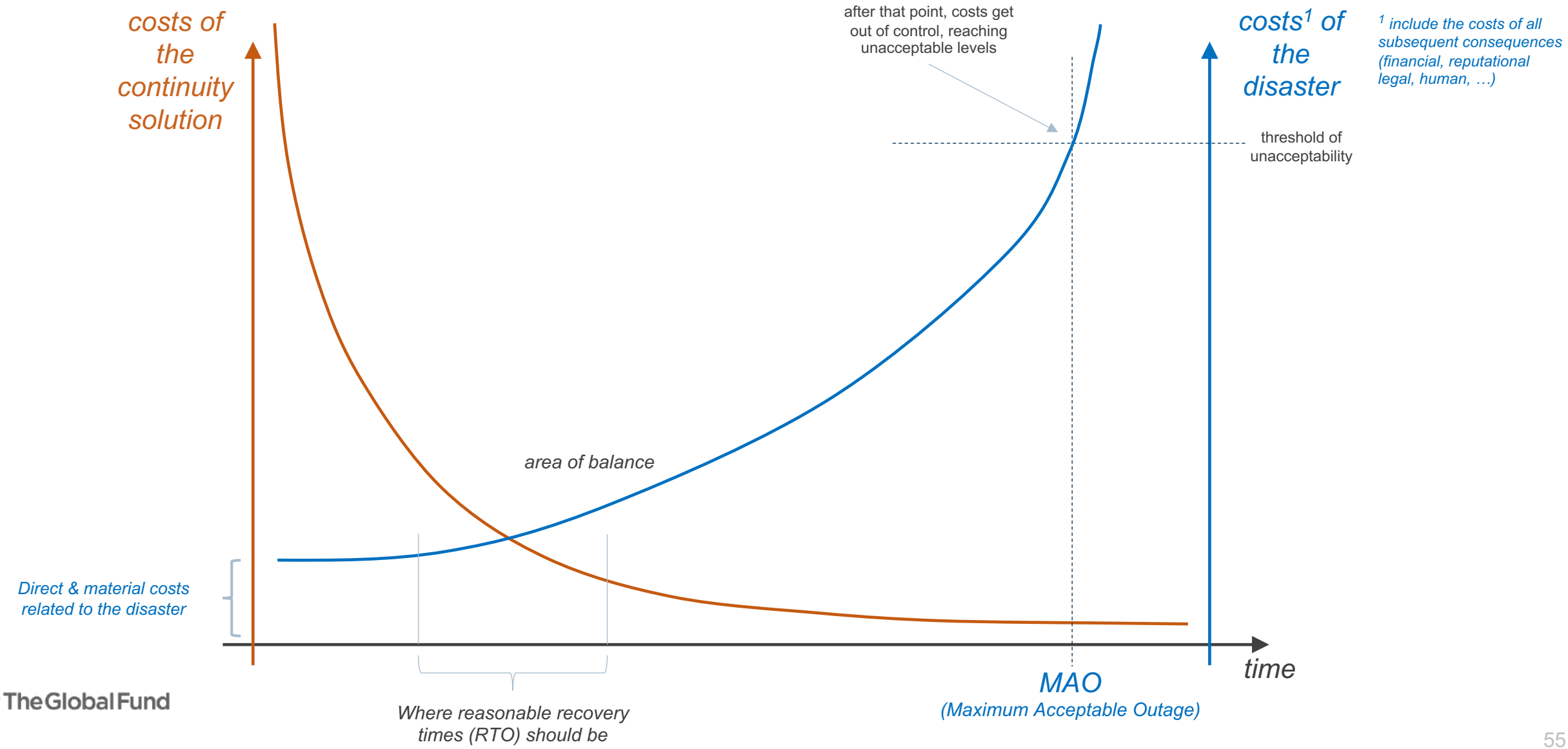
BC strategies and times for recovery



Disruption Scenarios and Response Models



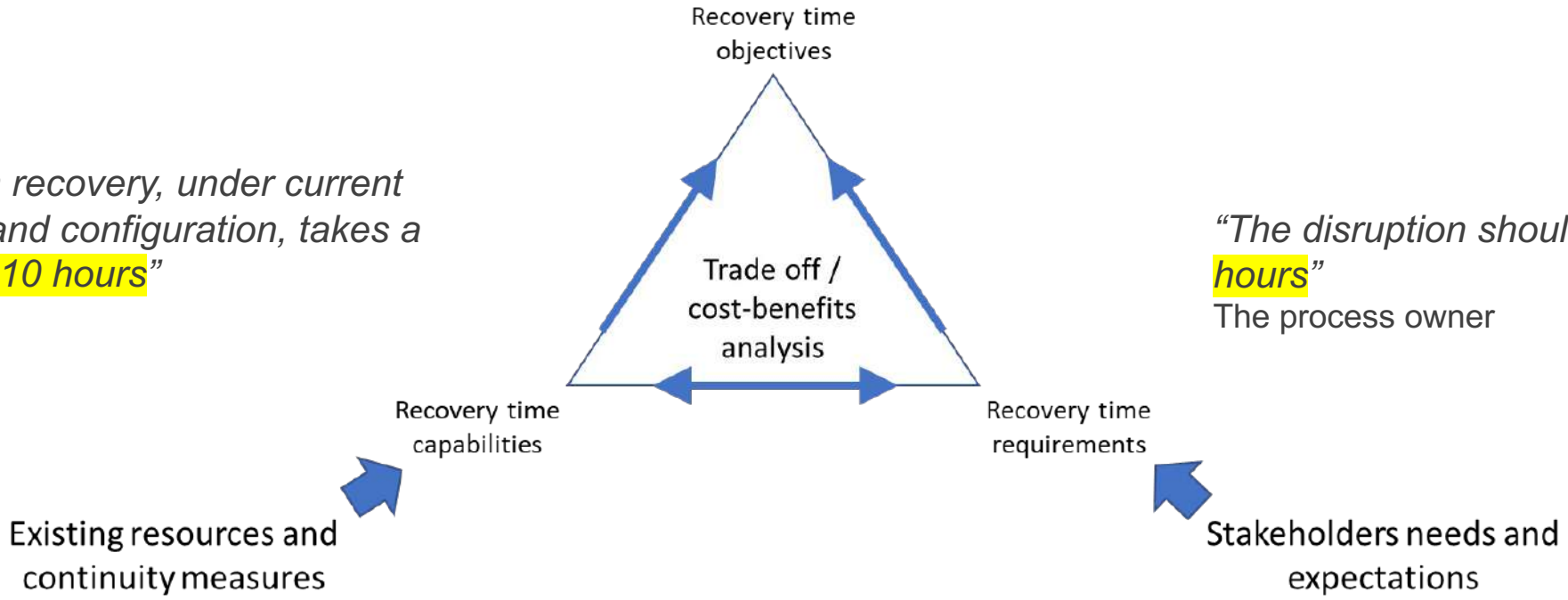
Cost-benefit analysis & business continuity solutions



The trade-off triangle

- **Recovery time requirements** (obtained from the needs and expectations of internal and external process stakeholders
- **Recovery time capabilities** (obtained from existing resources: sites; information systems, external suppliers -- and their current capacity to ensure recovery time objectives)

"The system recovery, under current technology and configuration, takes a minimum of 10 hours"
The CIO



"The disruption should not exceed 4 hours"
The process owner

Reducing this recovery time to match requirements represents a **total investment** of 2 million USD and 20% increase in the cost of maintenance.
A **cost-benefit analysis** will determine if the operational and reputational damages incurred from not meeting these requirements justify investment and additional recurring costs, leading to a negotiated RTO somewhere in-between 4 and 10 hours.

Business continuity plans

A key BCMS focus: *analysis to planning*

- Assess impacts of business disruptions and RTOs
- Identify critical operations
- Identify and map BC risks

- Examine strategies to:
  1. ensure continuity of critical operations
  2. recover critical resources
  3. maintain core services
- Design BC arrangements and risks reduction measures

- Document BC/DR procedures based on BC/DR arrangements
- Develop education and practice plan
- Develop review and improvement plan
- Develop communication plan

Leveraging existing plans to develop exercisable ISO 22301 compliant plans

Business Continuity Plans

Concise, clear and short

BCPs are to be used in stressful situations when individuals are overwhelmed by multiple events and often emotionally affected

BCPs are **action-oriented documents**

What is required for a Business Continuity Plan

ISO22301 requires several key elements: (BCPs & DRPs)

- Its purpose, the scope to which it applies and its objectives
- The roles & responsibilities of the team who will execute the plan
- A list of the actions to execute the solution
- The plan's activation criteria, who will activate and the activation procedure
- How the team's actions will be operated, coordinated, communicated
- The internal & external dependencies
- The resources requirements
- What to report, to whom, by whom, when and how
- What will be done to stand down

Business Continuity Plans: Context and Purpose

Plans designed to recover operations step by step; to be exercised and tested periodically

Crisis Management

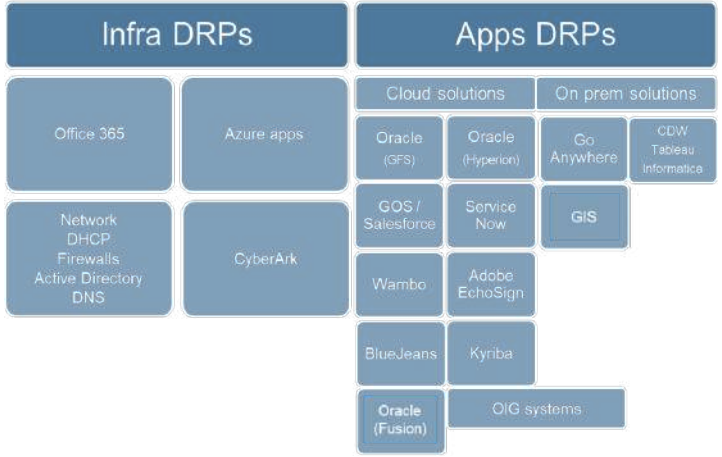
Business Continuity

Recovery and Restoration

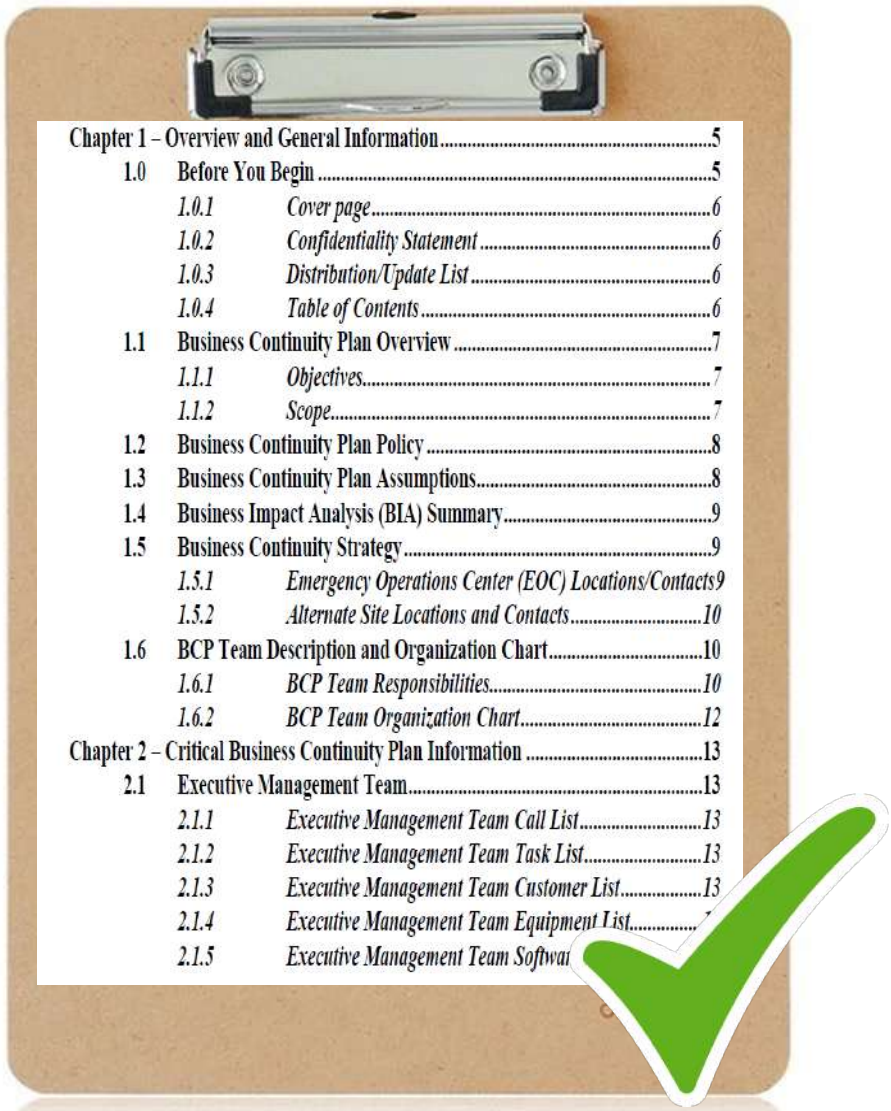
HR BCP | GMD BCP | Administration BCP

Ethics BCP | Finance BCP | OIG BCP

Communications BCP | Supply Operations BCP | Master IT DRP



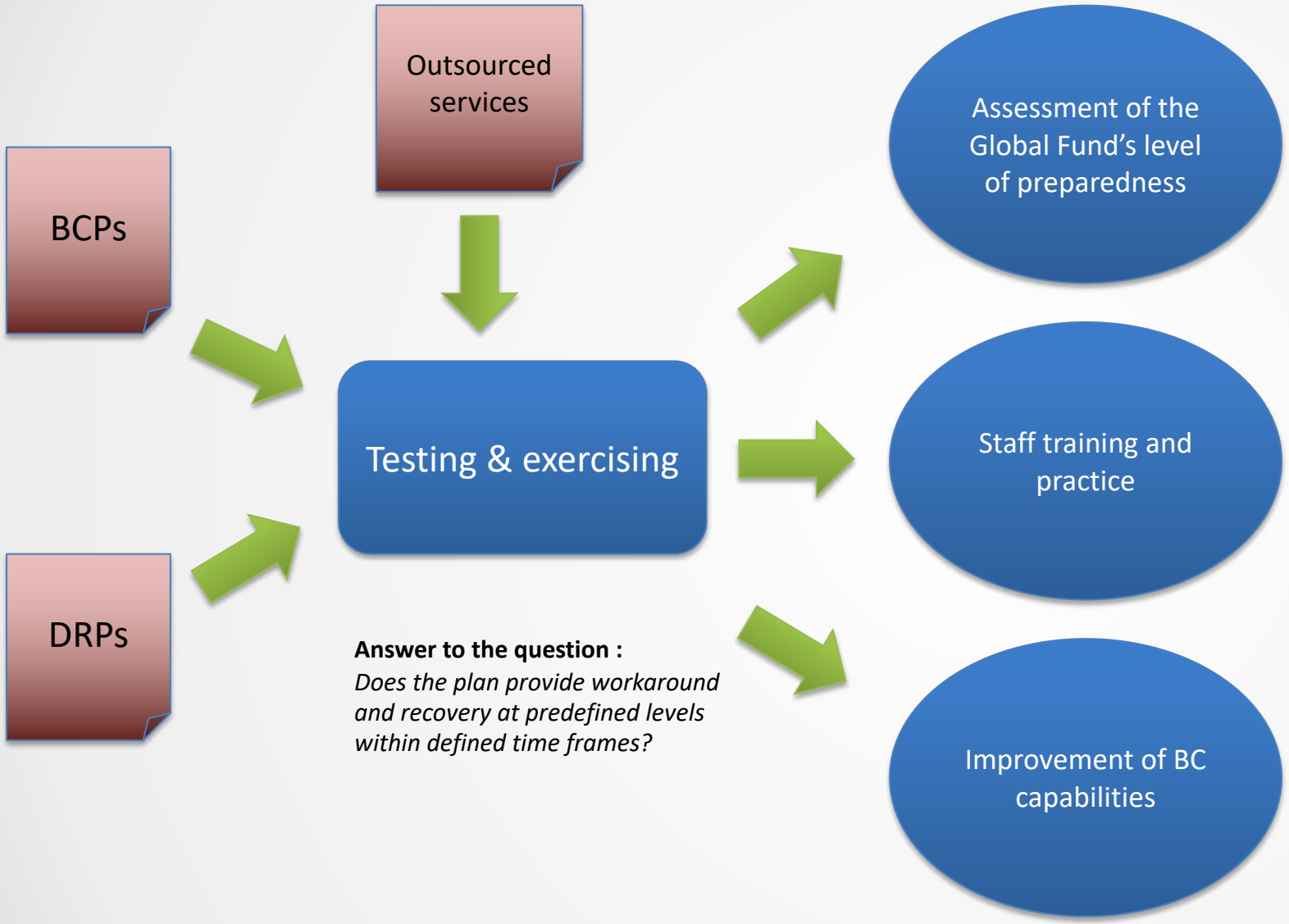
Structure of a Business Continuity Plan



Chapter 1 – Overview and General Information 5
1.0 Before You Begin 5
1.0.1 Cover page 6
1.0.2 Confidentiality Statement 6
1.0.3 Distribution/Update List 6
1.0.4 Table of Contents 6
1.1 Business Continuity Plan Overview 7
1.1.1 Objectives 7
1.1.2 Scope 7
1.2 Business Continuity Plan Policy 8
1.3 Business Continuity Plan Assumptions 8
1.4 Business Impact Analysis (BIA) Summary 9
1.5 Business Continuity Strategy 9
1.5.1 Emergency Operations Center (EOC) Locations/Contacts 9
1.5.2 Alternate Site Locations and Contacts 10
1.6 BCP Team Description and Organization Chart 10
1.6.1 BCP Team Responsibilities 10
1.6.2 BCP Team Organization Chart 12
Chapter 2 – Critical Business Continuity Plan Information 13
2.1 Executive Management Team 13
2.1.1 Executive Management Team Call List 13
2.1.2 Executive Management Team Task List 13
2.1.3 Executive Management Team Customer List 13
2.1.4 Executive Management Team Equipment List 1
2.1.5 Executive Management Team Softwa

- ***Introduction**, with distribution list, executive summary, objectives and glossary*
- *Critical business continuity **plan information***
- *Incident response **plan**, with **plan** activation, incident response team, communications and contact list*
- *Continuity and recovery **procedures***
- *Plan **administration and maintenance***

Proving the concept: exercises and tests



Answer to the question :
Does the plan provide workaround and recovery at predefined levels within defined time frames?

Realistic exercises should be used to help **identify issues** and **validate assumptions** that may require attention

Goal is **continuous improvement** of business continuity management capabilities and organizational readiness by ensuring that lessons learned are integrated into prevention, mitigation, planning, training, and future exercise activities.

Also necessary for outsourced services the responsibility for BC exercising remains with the owner of the service : the Global Fund must make sure, through exercises, that the **outsourced company can continue to meet its contractual obligations** in the event of a disruption.

BC exercise: "*the process to train for, assess, practice and improve performance [of the BCMS] in an organization.*"

BC test: "*a unique and particular type of exercise, which incorporates an expectation of pass or fail element within the goal or objectives of the exercise being planned.*"

Business Continuity Exercises

Exercises confirm that business continuity/disaster recovery (BC/DR) plans, are fit-for-purpose

They confirm whether a business continuity plan (BCP) provides recovery at predefined levels within defined timeframes. Exercises should be conducted on a regular, periodic basic basis and are observed, recorded and results documented as the exercise/test proceeds.

Exercises permit

- Confirmation that continuity objectives are met
- Evaluation of an organization's response to various disruptions
- Identification of gaps or weaknesses in BCPs
- System and process improvements
- BCP updates

Typical exercises or tests cover

- Data losses/
- Power outages
- Remote working
- Physical disruption while in the office
- Emergency communications

Steps to develop an exercise

1) Develop a narrative

- Using the results of the BIRA, develop a story of an event threatening the normal operation of the organization
- Decide what is (are) the objective (s) of the exercise/
- Prepare questions to the relevant team
  - What should be done
  - How to communicate internally
  - How to continue to perform tasks
  - What/when/how to communicate to external stakeholders

2) Inject realism

- Develop an evolving script, including additional disruptions and threat variations e.g.: key people on vacation; workarounds that do not work

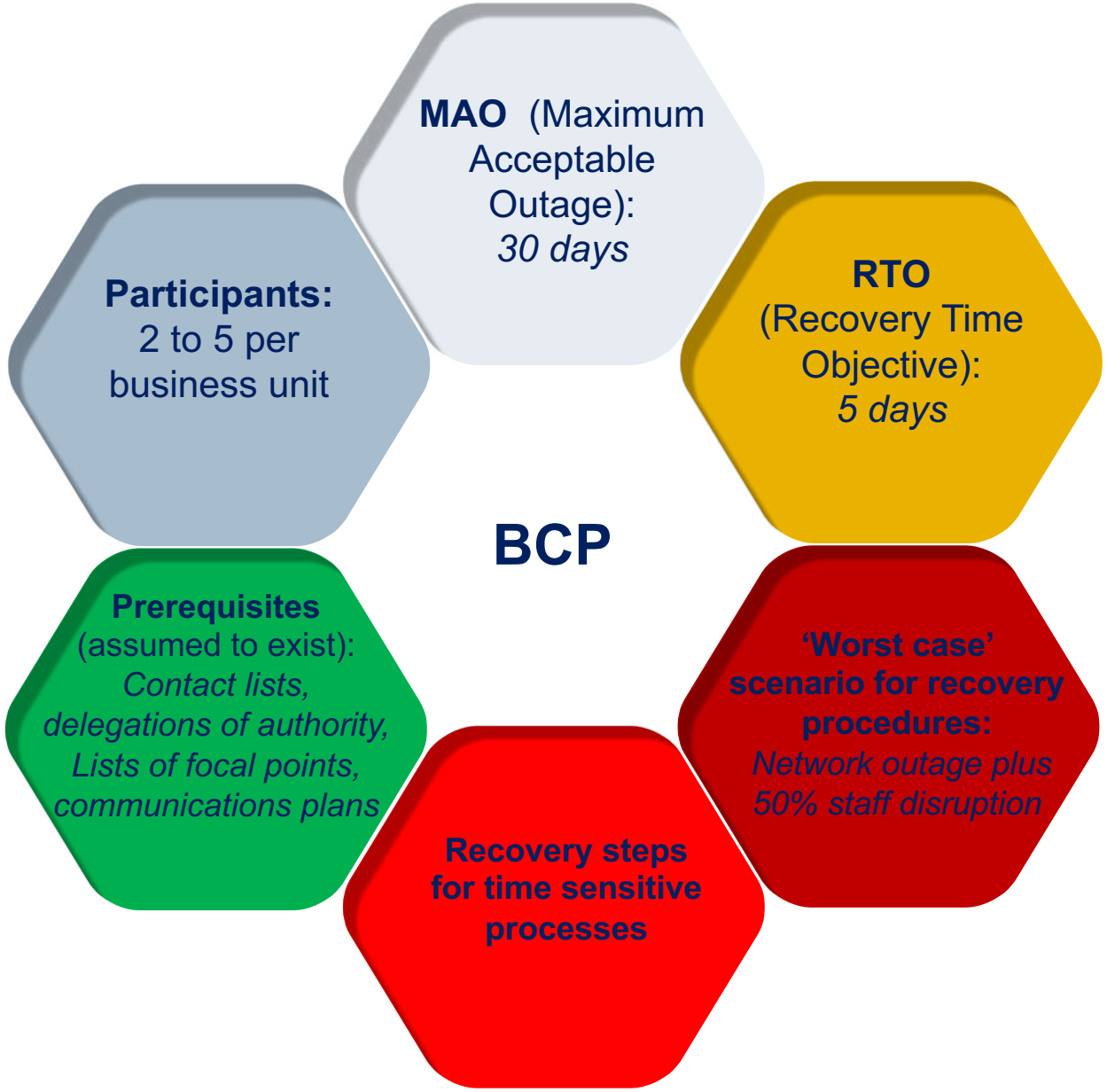
3) Decide upon the nature of the test or exercise

- •Table-top: from a simple distribution of the plan for review to a thorough examination of each step of the BCP
- •Simulation: the plan is played in a workshop enacting the procedures
- •Operational: life-like exercise to the extent that normal operations are stopped and the event/threat is fully simulated

Exercises validate Business Continuity Plans

IT system RTOs are shorter than business recovery requirements

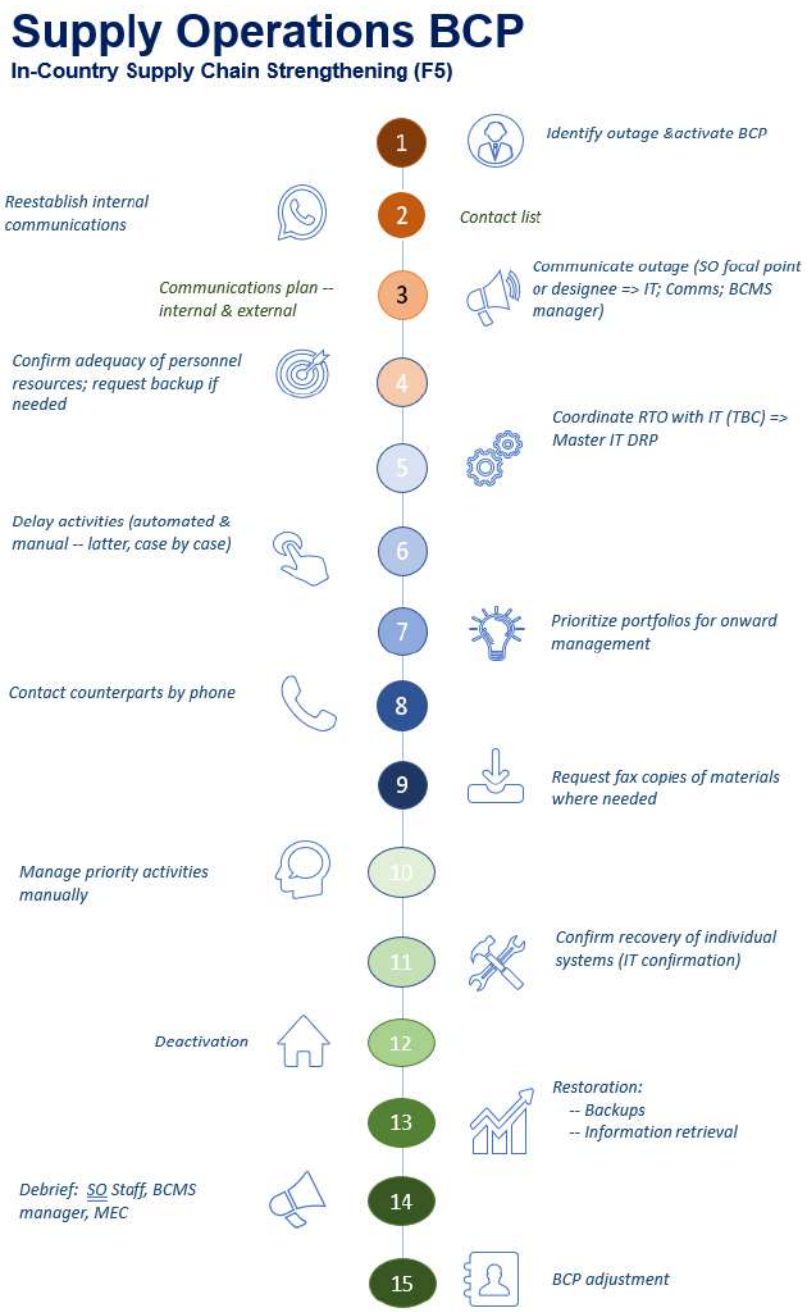
Maximum time for data loss (RPO) = 24hrs

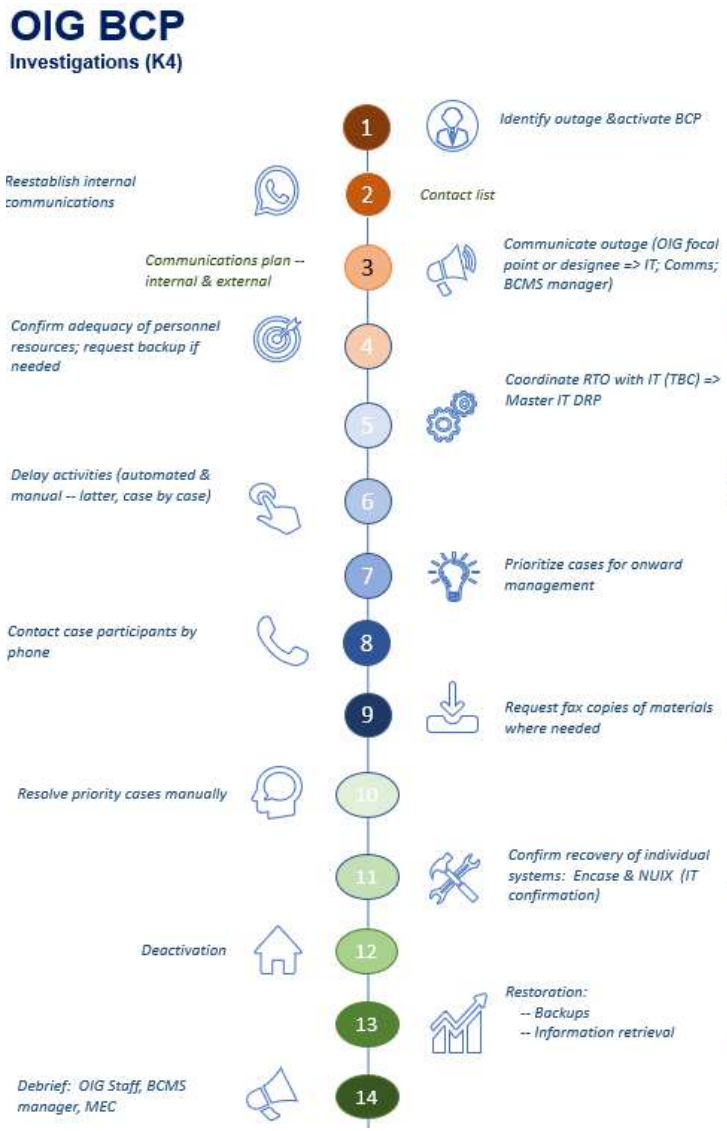


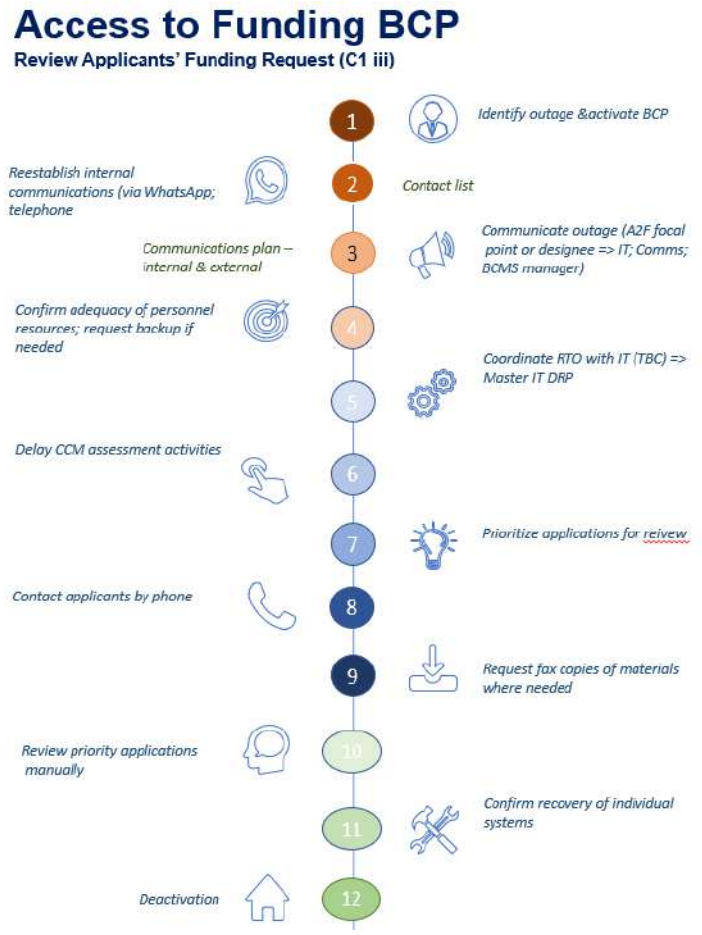
Departments share many steps especially those involving internal and interdepartmental communications

Business unit BC scripts

(illustrative)







BCMS continual improvement cycle

Illustrative Status

Not started | In progress | For approval | Completed

Day 3

How the region is dealing with pandemics and war-related disruptions today

Ukraine's Center for Public Health and the road to ISO 22301 certification

Alliance for Public Health

Other examples

Prioritizing actions/solutions in the EECA region and in individual countries

Group work

Challenges and solutions *(from Warsaw workshop)*

EECA Region & Ukraine

Challenges:

- **War**
  - **Nuclear attack**
  - **Nuclear power disaster**
  - **Biochemical attack**
  - **Renewed conventional attack on Kiev**
  - **Infrastructure damage**
  - **New unexpected migration**
  - **Energy cutoff/blackouts**
  - **Economic crisis**
  - **Computer/network outage**
  - **Supply chain disruption (procurement/transport/warehousing)**
  - **Donor withdrawal**
- **Covid or new pandemic**
- **Cyberattack (loss/leak of data)**

Solutions: **Focused on staff, logistics (PSM) & infrastructure (facilities) (72 hour – 2 week MAOs; < 72 hour – 1 month RTOs)**

- **Mobile health staff**
- **Mobile laboratories**
- **Evacuation of patients and hospitals**
- **Roll out of services at new sites**
- **Provision of humanitarian aide**
- **Remote work arrangements**
- **Stock redistribution**
- **Legislative changes**
- **New regimens**

Requirements: **key persons/teams; funds; data backups; alternate work locations; computers; internet/network access; funds; alternative suppliers; direct contracts**

Challenges and Solutions

Country xxxx

Challenges:

Solutions:

Requirements:

Defining technical assistance (TA) needs & aspects for inclusion into funding requests

Moderated discussion

Requirements

Per country and region

Next steps

BCMS self-assessment questionnaire

ISO 22301 compliant BCMS self-assessment questionnaire

How to use the questionnaire:
For each question, answer yes or no. If you answered positively, provide evidence.

1. The organization and its context

- Have the issues that will drive the BCMS been defined?
- Has the environment within which the BCMS will operate (interna
outcomes of the system, been identified?
- Has an appropriate and repeatable risk assessment method and th
defined and documented?

2. Needs and expectations of interested parties

- Is the scope of the BCMS clear and documented?
- Is there a procedure in place to identify, take into account, docum
applicable legal and regulatory requirements for the BCMS?
- Have these legal, regulatory and other requirements been commu
identified interested parties?

3. Scope of the BCMS

- Is the scope of the BCMS clear and documented?
- Have options for risk treatment been identified and evaluated?
- Does the scope define the BCMS in terms of its extent, purpose, d
in a way that is appropriate to the organization?

7. Business continuity objectives

- Have measurable business continuity (BC) objectives been established, documented and communicated throughout the organization?
- Is the achievement of these objectives evaluated by both internal audit and the management review?

8. BCMS resources and competence

- Are roles within the BCMS clearly defined?
- Is the BCMS adequately resourced?
- Is there a process defined and documented for determining competer
- Are those undertaking BC roles competent, and is this competence dc

9. Awareness and communication

- Is everyone within the organization's control aware of the importance involvement in implementing it and their role in a disruption?
- Has a communication needs analysis been conducted for the BCMS?
- Have procedures been confirmed and facilities made available for cor
- Are they regularly tested with results recorded?
- Is appropriate documentation created, maintained and controlled to the BCMS?

10. Operational planning and control

- Have you devised and implemented a program to ensure the BCMS ac
- Has there been analysis of the threats to any outsourced processes ar

12. Risk assessment and treatment

- Is there a formal risk assessment process for analyzing the risk of disruptive incidents?
- Does this risk assessment method identify risk treatments appropriate to BC objectives?
- Is there evidence of prioritizing risk treatments with costs identified?

13. Business continuity strategy

- Is the BC strategy based on the outputs of the BIA and risk assessment?
- Does the BC strategy protect prioritized activities and provide appropriate continuity and recovery of them, their dependencies and resources?
- Does the BC strategy provide for mitigating, responding to and managing impacts?
- Have prioritized time frames been set for the resumption of all activities?
- Have the BC capabilities of suppliers been evaluated?
- Have the resource requirements for the selected strategy options been determined, including people, information and data, infrastructure, facilities, consumables, IT, transport, finance and partner/supplier services?
- Have measures to reduce the likelihood, duration or impact of a disruption for identified risks been considered and implemented, and are these in accordance with the organization's risk appetite?

14. Establishing and implementing BC procedures

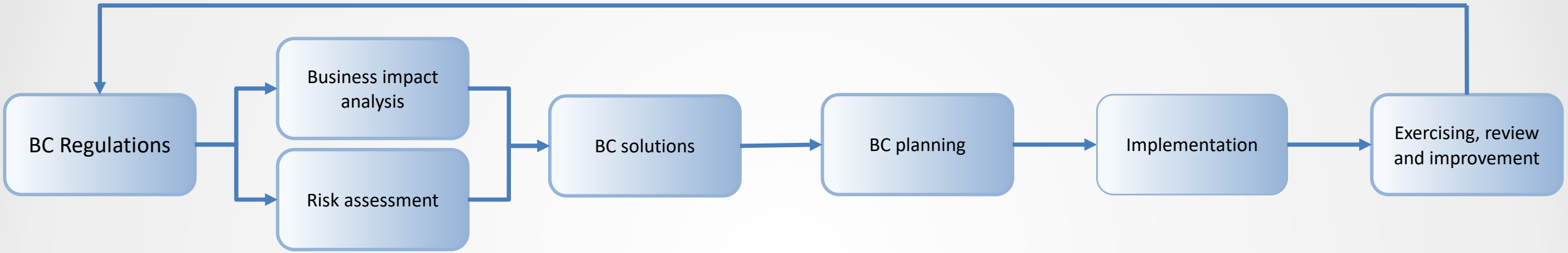
- Have BC procedures been put in place to manage a disruptive incident, and have continuity activities based on recovery objectives been identified in the BIA?
- Are the business continuity procedures documented?
- Have internal and external communication protocols been established as part of these procedures?

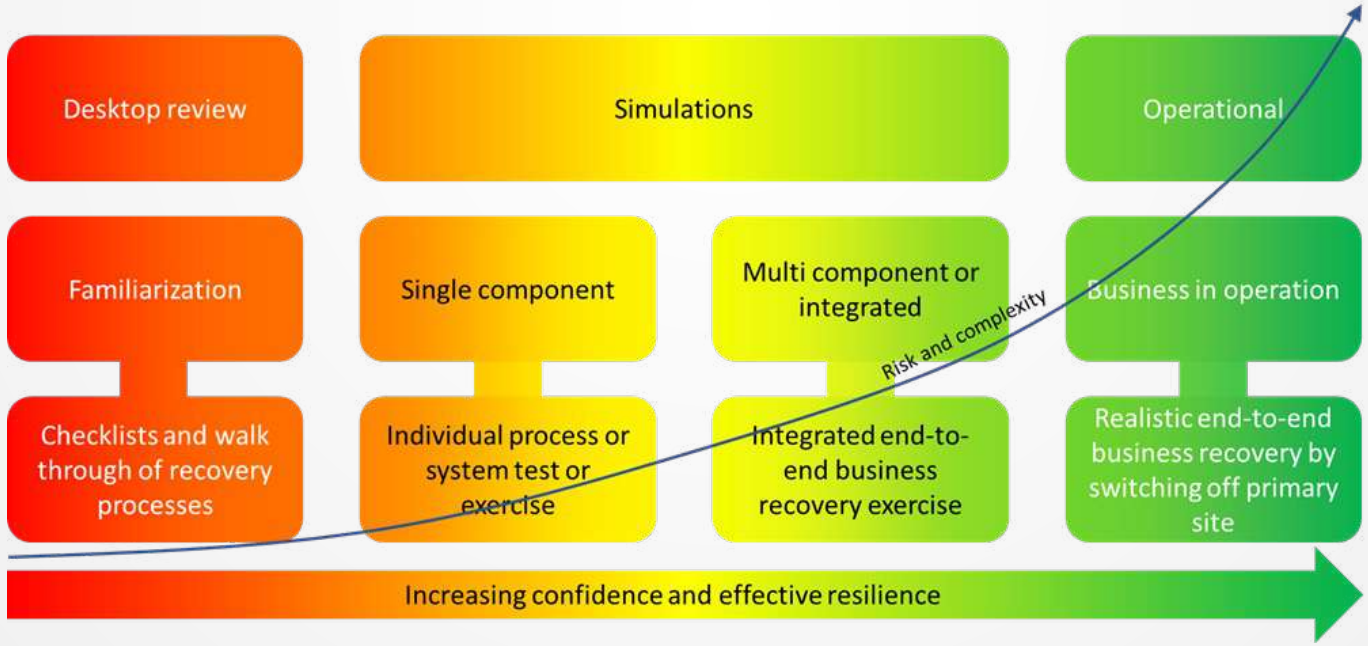
etc…

Some options

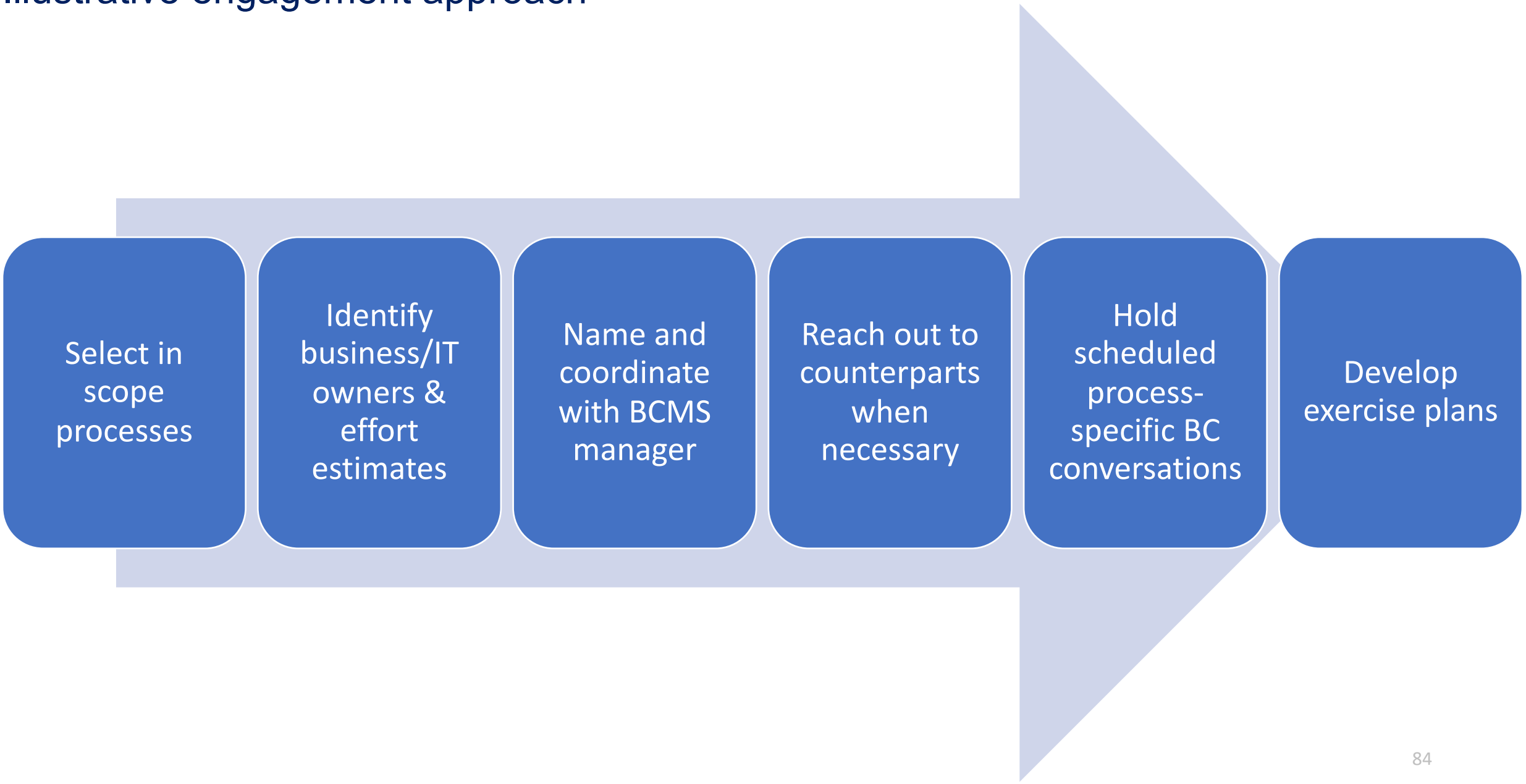
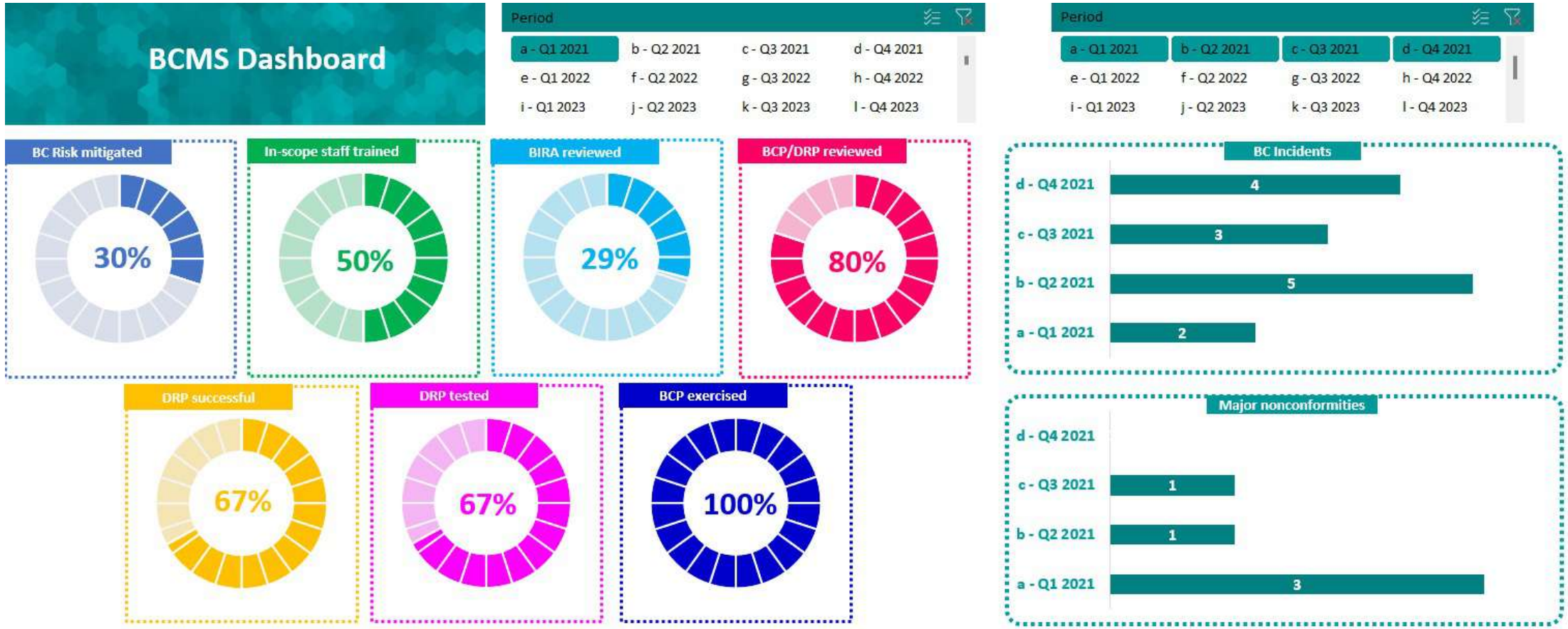
- Share relevant documentation
- Select services that would require a Business Continuity Plan(based on urgency and criticality)
- Develop individual Business impact and Risk Assessments (BIRAs)
- Develop Business Continuity Solutions
- Transform Solutions into Business Continuity & Disaster Recovery plans where necessary

BCM Process Lifecycle





Illustrative engagement approach



Performance improvement