restena

réseau · sécurité · .lu

Business Continuity Management

An introduction to BCM

Cynthia Wagner

What is BCM?

BCM : Business Continuity Management

- A lot of definitions exist:
  - BCM is "an organization's ability to maintain critical business functions during and after a disaster has occurred" (techtarget)
  - "Business continuity and resiliency planning is the process of creating systems of prevention and recovery to deal with potential threats to a company" (wikipedia)
  - "Business continuity management helps organisations reduce the likelihood and impact of disruption and downtime, protect assets if something does go wrong, continue operating through the disruption, and recover as quickly as possible from any incidents that do occur." (isms.online)
  - It provides a framework for organizations to plan, establish, implement, operate, monitor, review, maintain, and continually improve a documented management system to protect against, reduce the likelihood of, and ensure recovery from disruptive incidents. (ISO22301)

What is a BCMS?

- BCMS = Business Continuity Management System
- It is by far more than a Disaster Recovery plan
- It is a management system for business continuity , so a structured/documtented approach to achieve operational resilience and ensure to
  - Continue working within times of disrupted services
  - Have the necessary competences to manage the organisation in crisis/disruption scenarios
  - Safety, environment and health protection
- Being prepared

What does a BCMS?

- Disaster prevention
  - e.g. risk reduction
- Disaster preparedness
  - e.g. training programs
- Disaster response
  - e.g. plan for incident management/response
- Disaster recovery
  - E.g. long term plans

Source: unknown

Why a BCMS

Examples

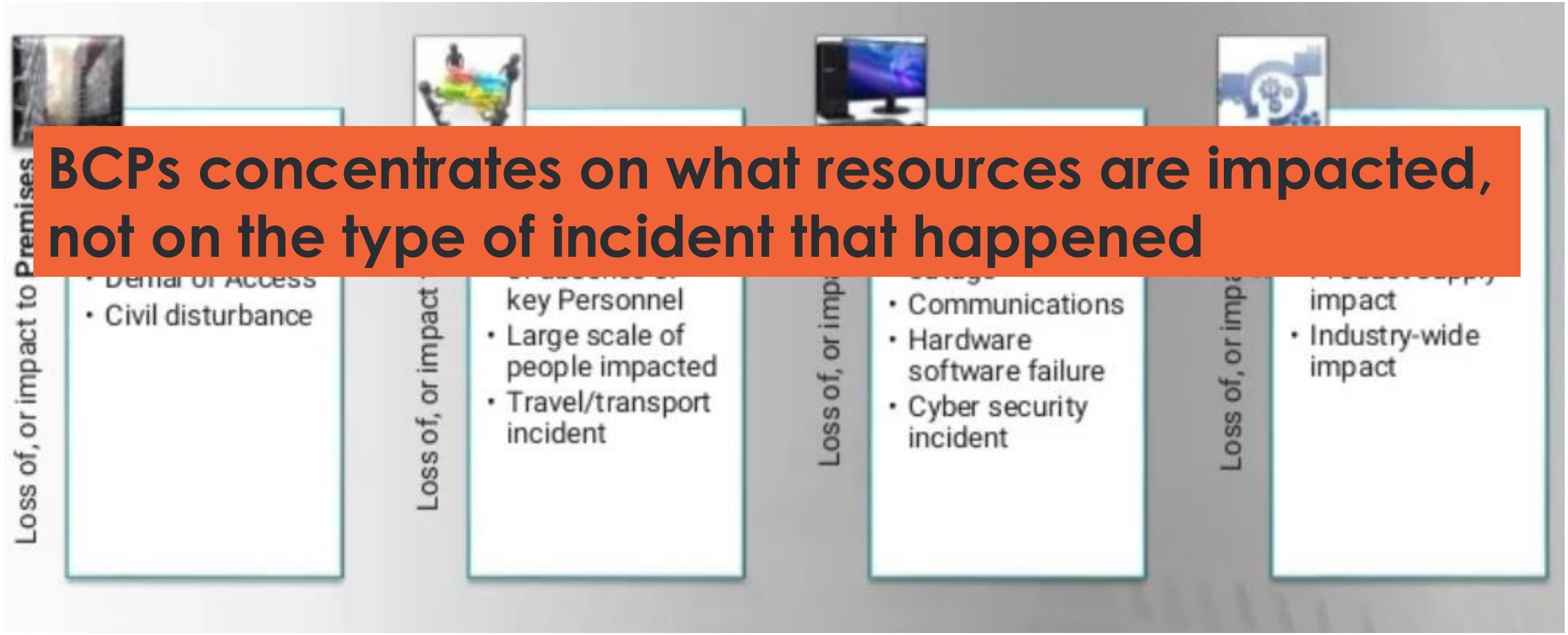
Loss of customer records

Failure of essential service to a large community

Large fire or flooding

Breakdown of supply chain

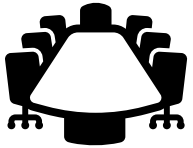
BCPs for Business disruption/incidents



BCPs concentrates on what resources are impacted, not on the type of incident that happened

Source: PECB

Who may be a BCMS driver



Board members / Strategic committee of organisation (internal)

Government (external)

Regulators (external)

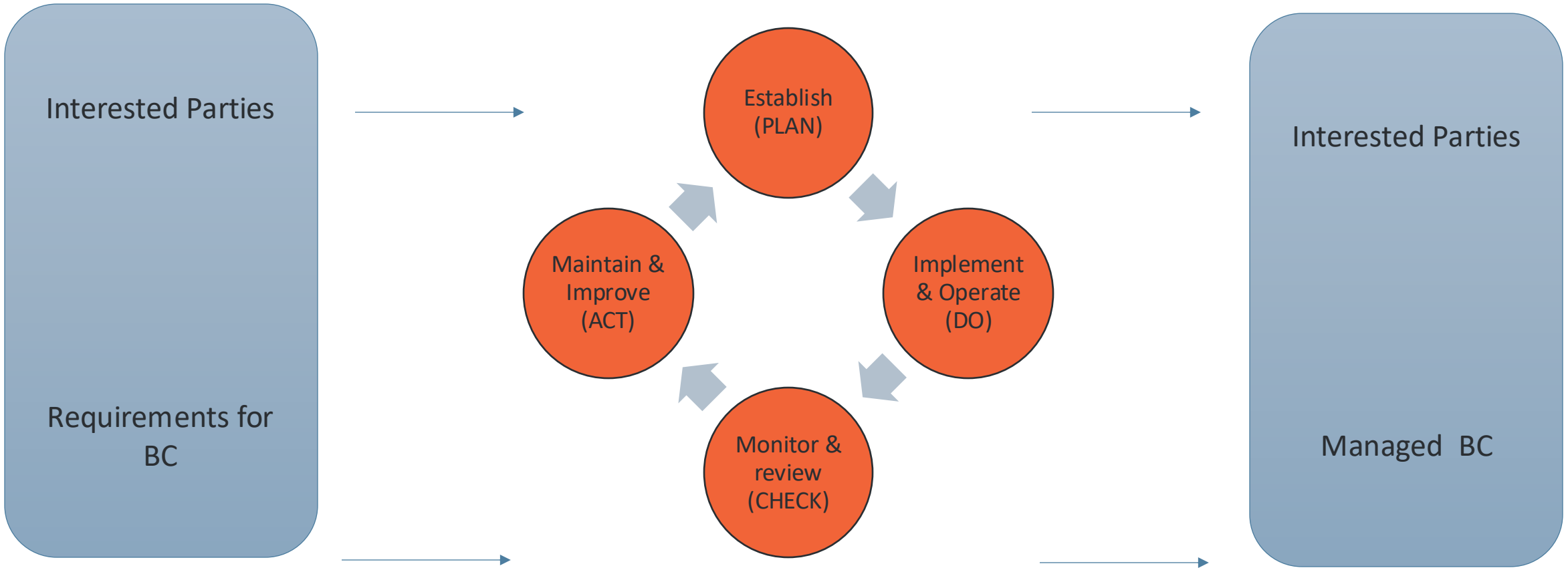
Insurances (external)

Question

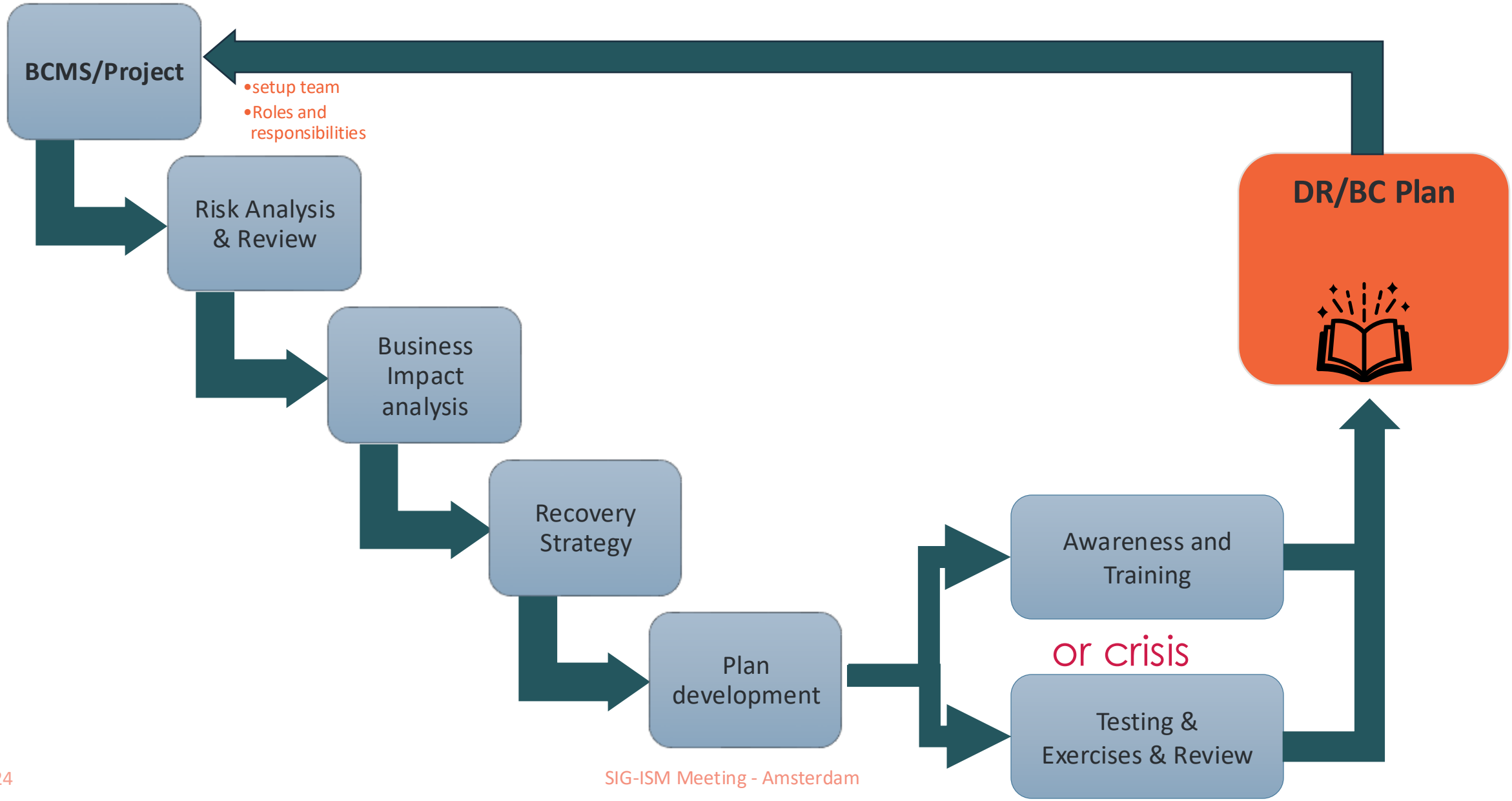
Who implemented an

- ISO 27001 certification? What is your scope?
- ISO 22301 certification? What is your scope?
- Who has a Business Continuity Process in place?

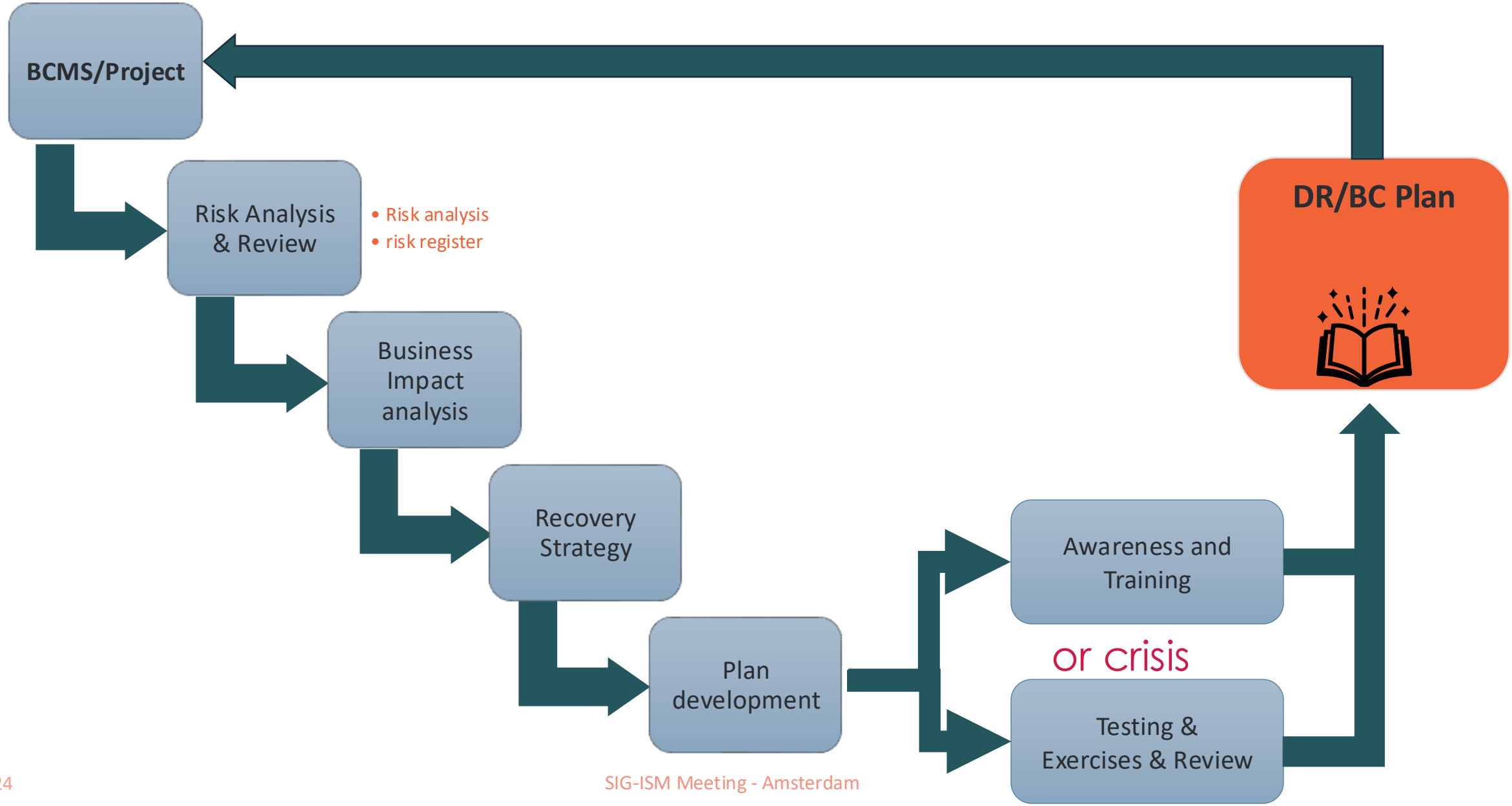
PDCA – Continual Improvement of BCMS



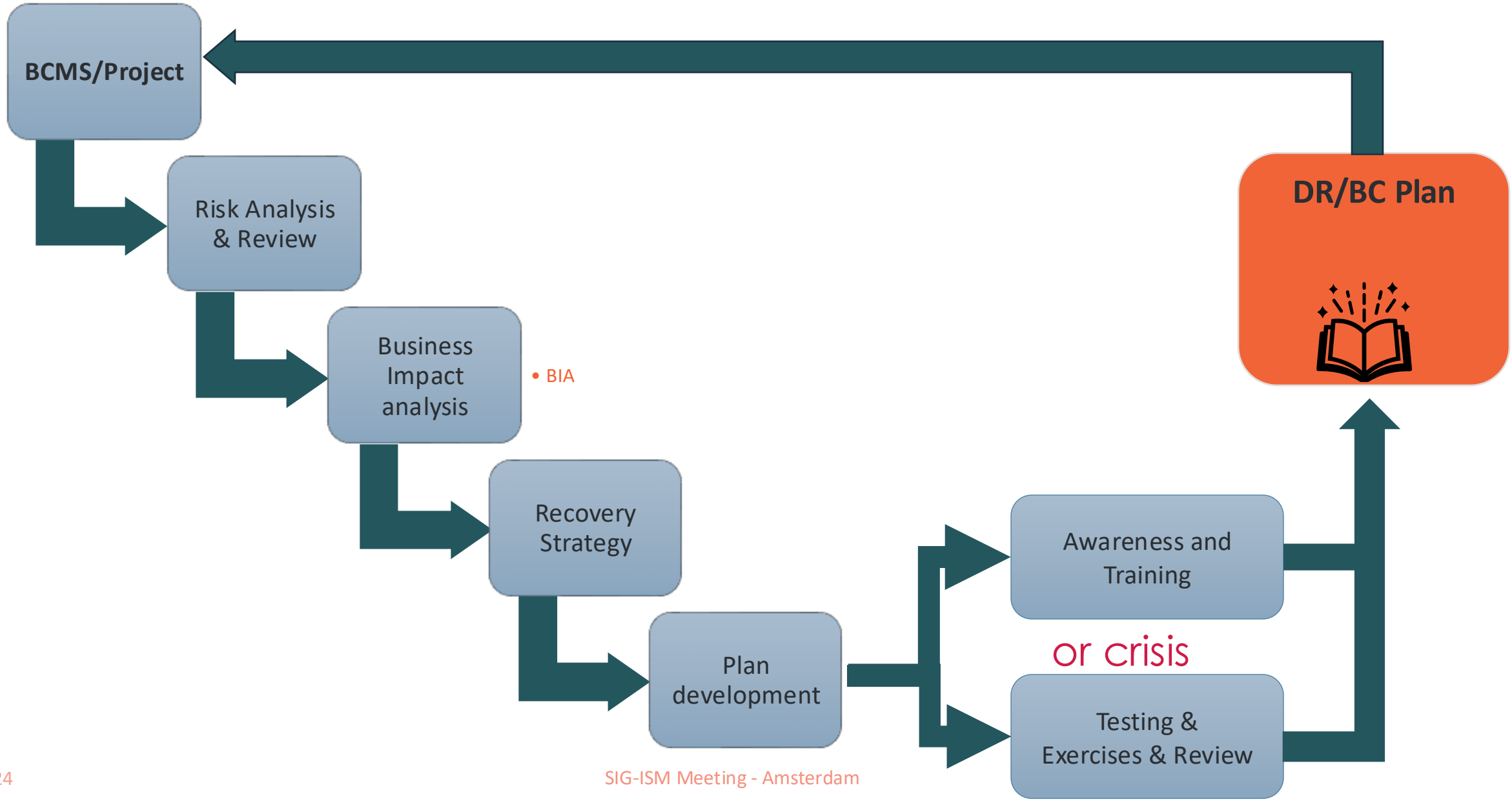
Phases of a BCMS - the Project



Phases of a BCMS: RA and review



Phases of a BCMS: BIA



Business Impact Analysis

BIA (also in ISO27001:2022)

- Evaluate to:
- Prioritize critical operations/processes/services for a business
- Determine tolerable downtimes (and the related RTOs/RPOs)
- Determine the resources for recovery

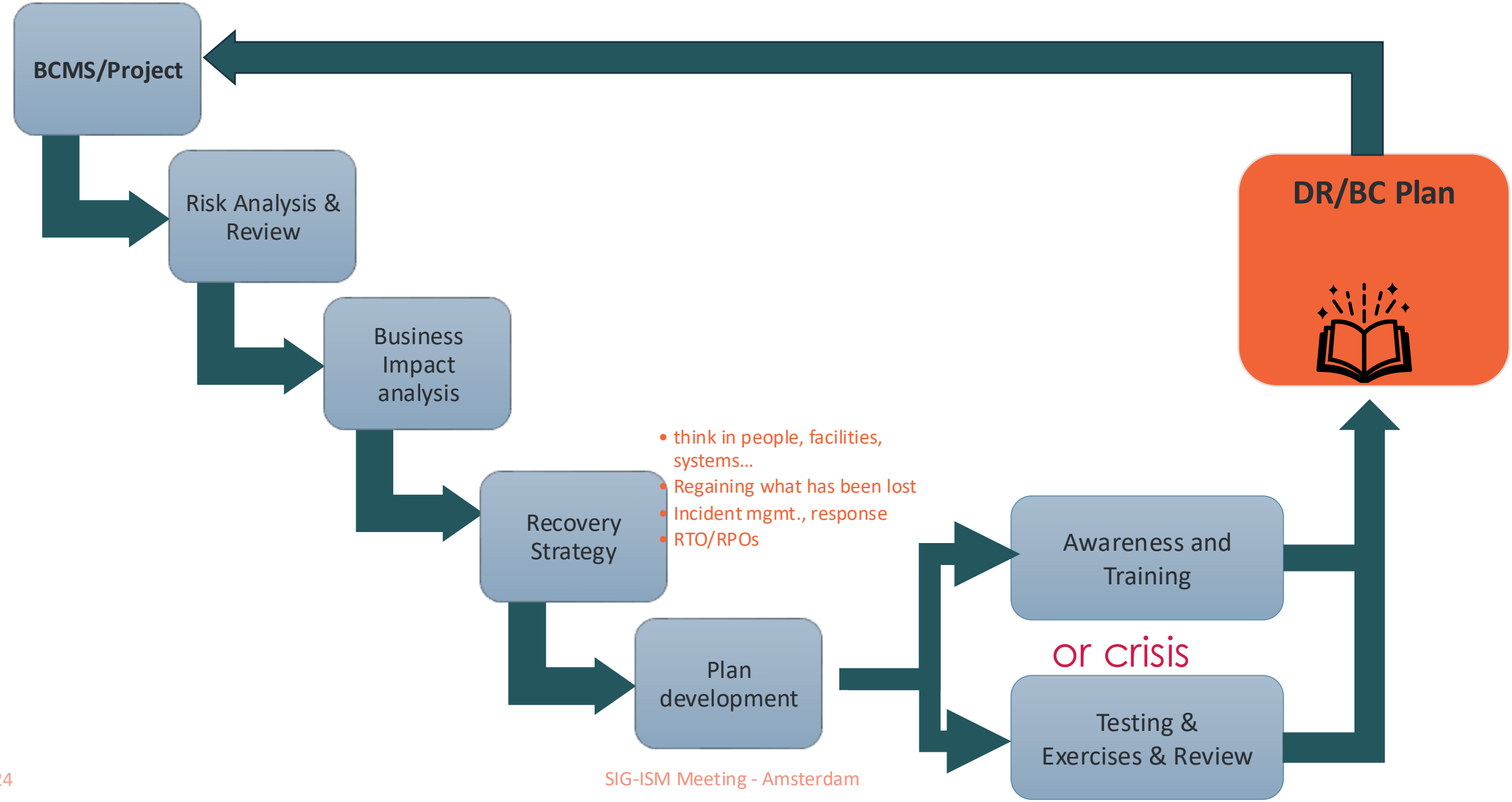
BIA examples

- People
  - Identify key staff / minimal staff
- Premises
  - Facility /Equipment/Resources
- Processes
  - Documentation / Systems / Communication
- Providers
  - Reciprocal arrangements / Contractors/Exernals/Suppliers
- Profile
  - Reputation/Legal constraints/Impacted customers, suppliers,…

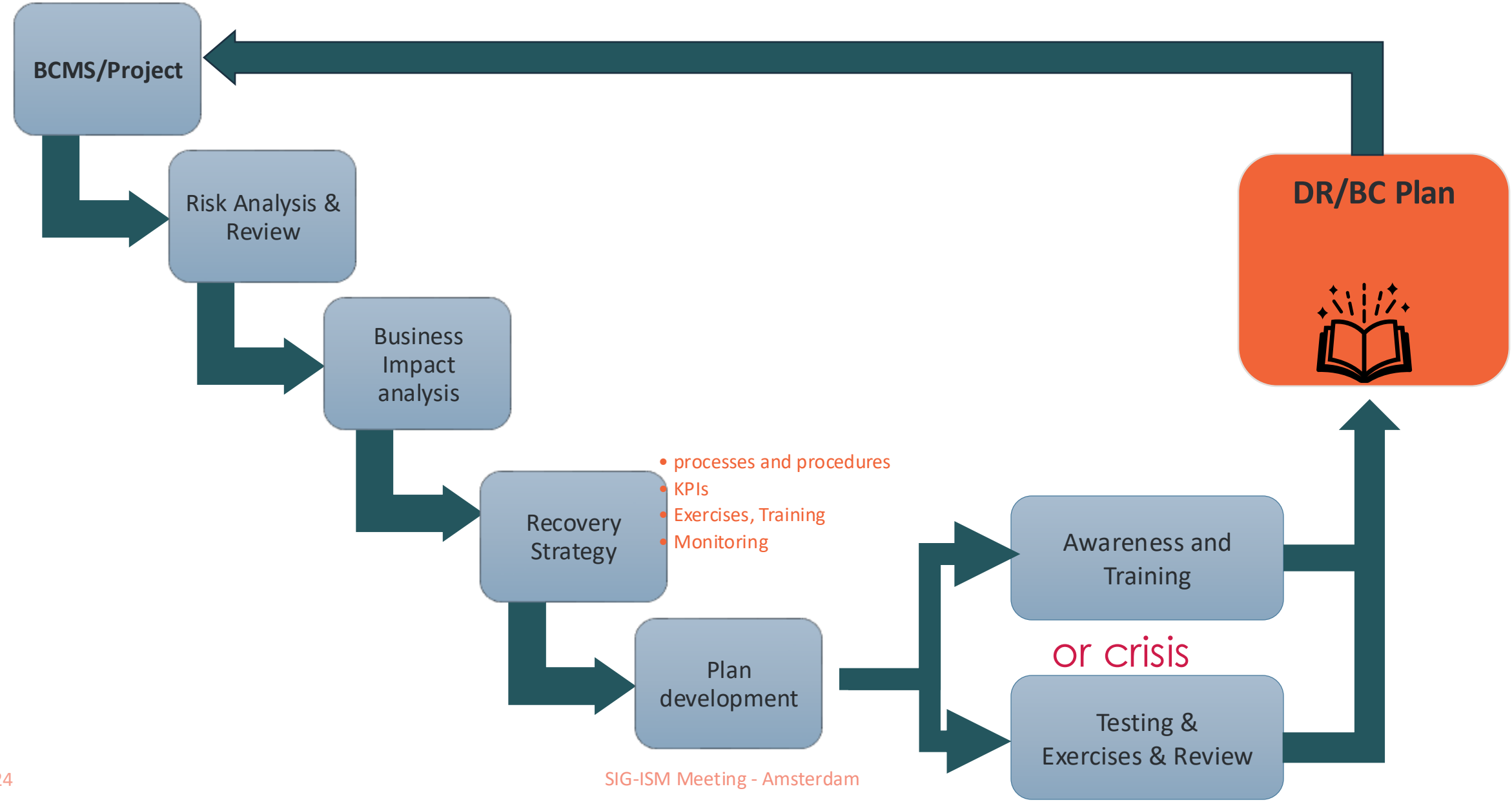
BIA challenges

- Sometimes difficult to estimate the long-term effects of a disruption
  - Impact may be on different levels (financial, reputation, growth…)
- Risk assessment (RA) and BIA are different
  - RA id the identification of inherent business risks and the “how to reduce the impact of these risks” on business operations, describing the key vulnerabilities and weak points
  - BIA identifies the organization's critical business processes, and the resources needed to support them
- But after all both provide valuable input for a BC/DR plan

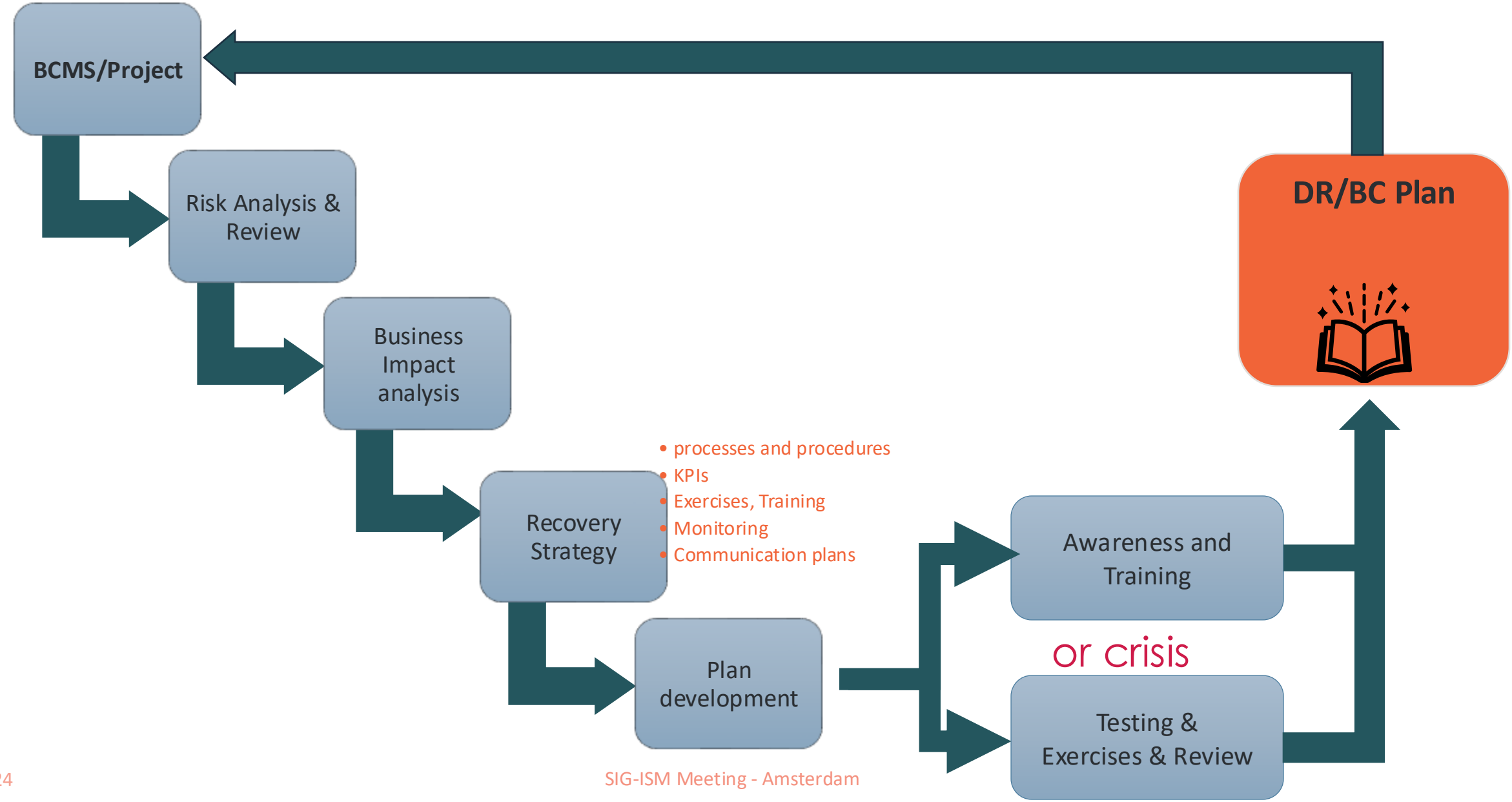
Phases of a BCMS: Recovery strategy



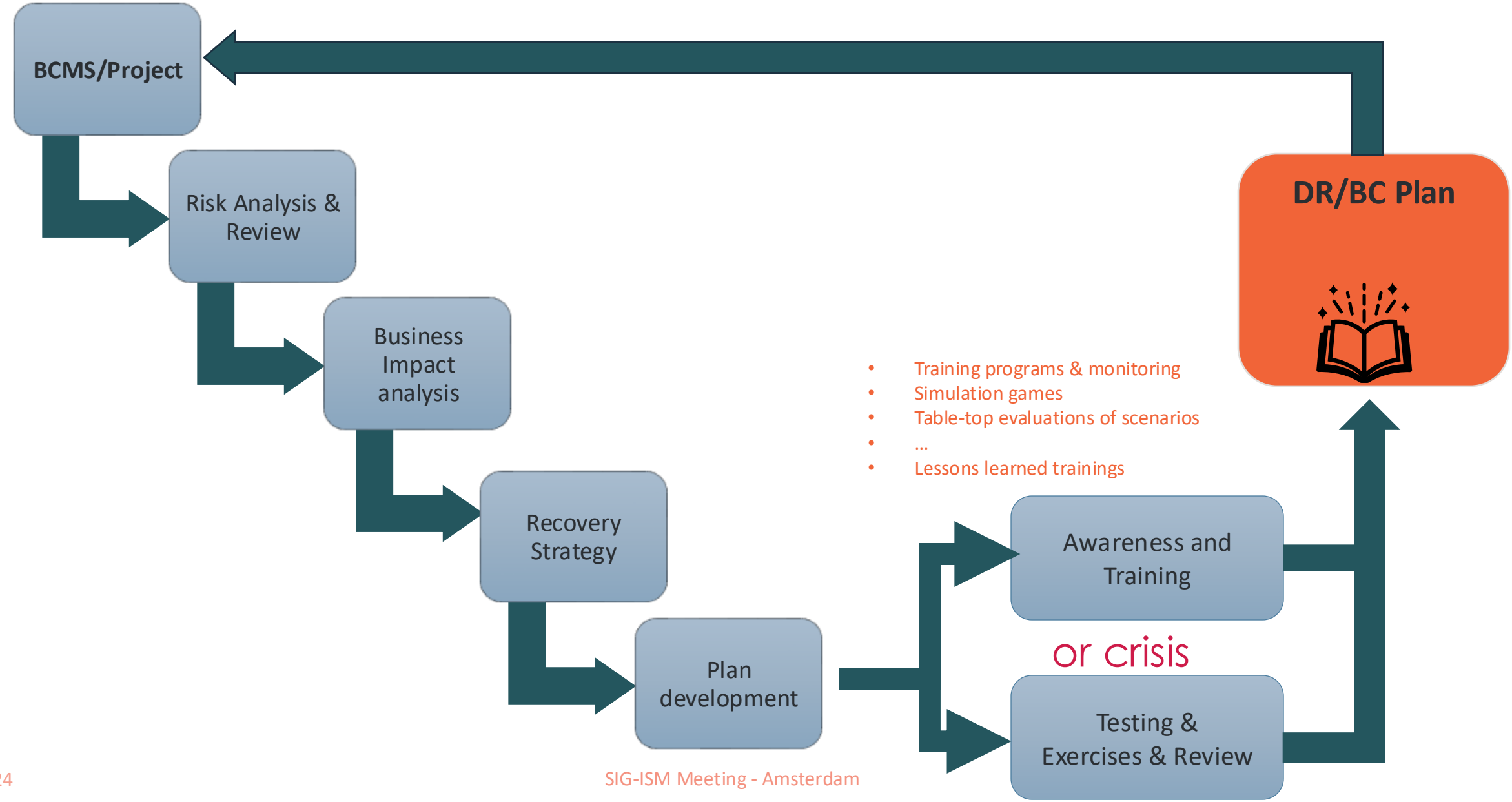
Phases of a BCMS: Plan development



Phases of a BCMS: Plan development



Phases of a BCMS: Training, Testing, Exercises



ISO 27001 vs ISO22301

Differences

- ISO27001 implements the information technologies continuity plan supporting business continuities activities in case of disruption
  - DRP
  - Focus on infrastructure and information security
  - Assets supporting products/services processes

- → achieving resilience requires more

ISO 27001 vs ISO22301

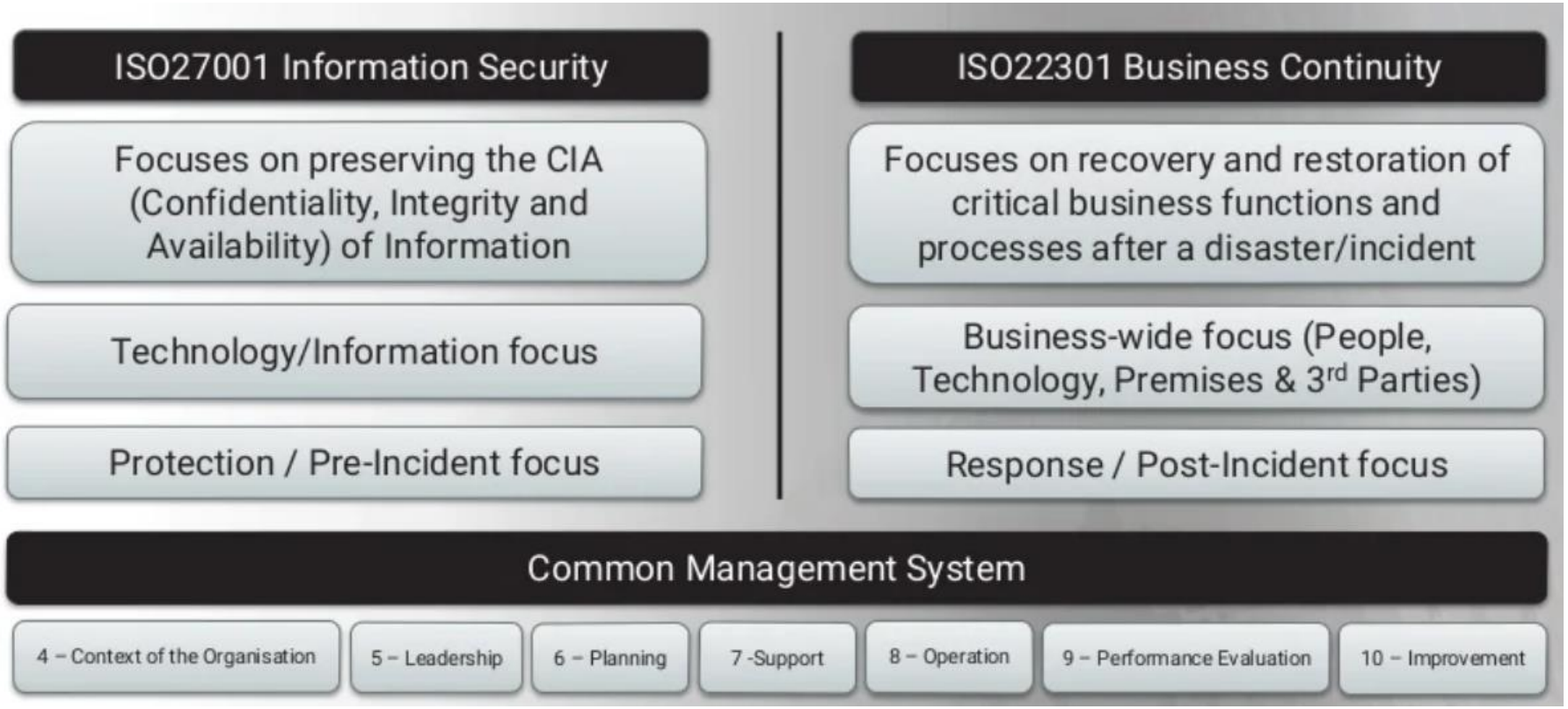
Differences

- ISO22301 ensures critical business, of all kind, are managed in case of disruptions
  - To reduce downtimes
  - Protect people
  - ….
  - The goal is to protect against, reduce the likelihood of occurrence, prepare for, respond to, and recover from disruptive incidents when they arise."(ISO22301)

  → Resilience aimed

→ But both deal with Business continuity

ISO27001 vs ISO22301 differences



Information Security Continuity
2013: A17.2 -- 2022: 5.30, 5.29, 8.14

ISO22301 provides guidelines for implementation of those

Source: PECB

ISO27001 vs ISO22301

Examples how they differ

- In ISO27001 an organisation should enable its information security to continue after an incident → DRP
- ISO22301 describes this more to develop a set of documents and processes including Business Impact analyses, plans, tests and exercises

- ISO27001 focuses on removing vulnerabilities before an incident may occur
- ISO22301 focuses on Business risks and opportunities evaluation

Outcomes of an effective BCM

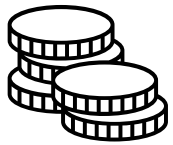
- Critical activities are identified and protected (BIA)

- Incident management

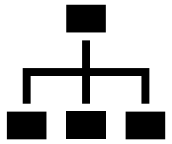
- Staff is trained on incidents and disruptions

- In line with compliance management and reputation is protected

Challenges

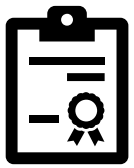


- Need a budget and resources



- Need support from management/board

- Plans must be rehearsed to work (exercise plans and controls)



- Regular assessments / audits

What we changed with the insights into ISO22301

Do we go for a ISO22301 certification? NO!

- ISO22301 was not on our radar as such
  - Training was provided by government
  - Critical infrastructure training program
- BIA was a new approach to us, also for ISO27001:2022 compliance
  - We are in the process right now
- We added new KPIs to our Management System → IS/BCMS combined
- We added a section to our Annual ISMS Management review that deals with BCM
- We want to be prepared for future requirements…

Personal challenge

Stay on right track

- A personal challenge for me was

  - Do not fall back into ISO27001
  - The processes and implementation are similar
  - The documentation is similar
  - The monitoring is similar
  - The review is similar
  - ….tricky to keep both apart in practice!

Thank you!

Questions?

www.restena.lu