Auditing the Corporate Business Continuity and Disaster Recover Plan

IIA 16th Annual Conference

Transforming Internal Audit to Drive Value

Sarova Whitesands, Mombasa
June 2018

Antony Nzamu

Associate Director
KPMG East Africa

Antony is a technology risk and cyber security services director passionate about empowering boards and senior leadership on the right questions to ask in order to gain true value from their technology investments.

His work experience is drawn from 15+ years serving clients in financial services, manufacturing, telecoms and the public sector, among others.

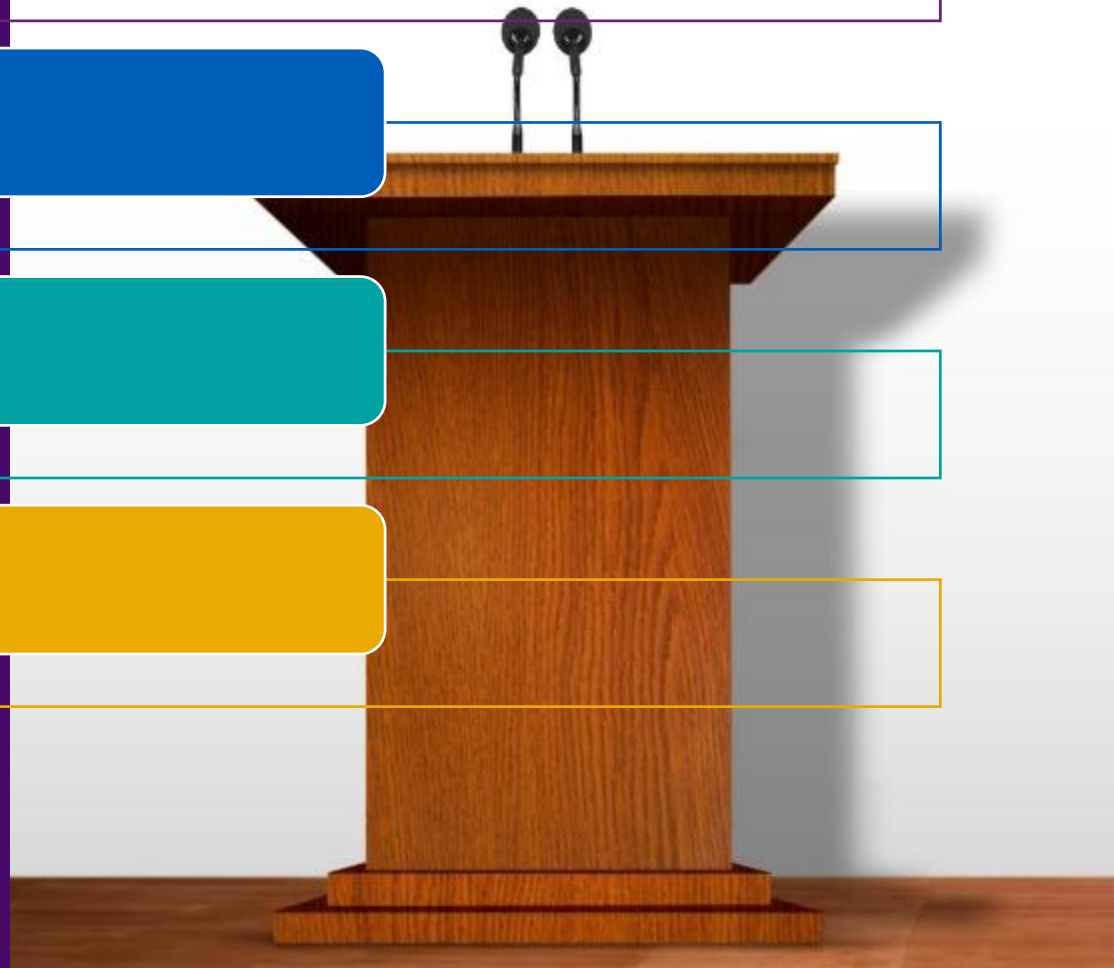
Nzamu's work has exposed him to the vast East Africa region and numerous African countries including Ethiopia, Malawi, Morocco, South Africa and Zimbabwe.

CIA, FCCA, CGEIT, CISA, ISO27001:2013, ISO22301:2012

KPMG

Agenda

- Why build Business Resilience?
- What does it entail?
- The role played by the Internal Auditor
- Auditing for Business Resilience



Top 5 Global Risks in Terms of Likelihood

2015	2016	2017	2018
Interstate conflict with regional consequences	Large-scale involuntary migration	Extreme weather events	Extreme weather events
Extreme weather events	Extreme weather events	Large-scale involuntary migration	Natural disasters
Failure of national governance	Failure of climate-change mitigation and adaptation	Major natural disasters	Cyberattacks
State collapse or crisis	Interstate conflict with regional consequences	Large-scale terrorist attacks	Data fraud or theft
High structural unemployment or underemployment	Major natural catastrophes	Massive incident of data fraud/theft	Failure of climate-change mitigation and adaptation

Economic Environmental Geopolitical Societal Technological

Source: 2018 the WEF Global Risks Landscape 2018

Top 5 Global Risks in Terms of Impact

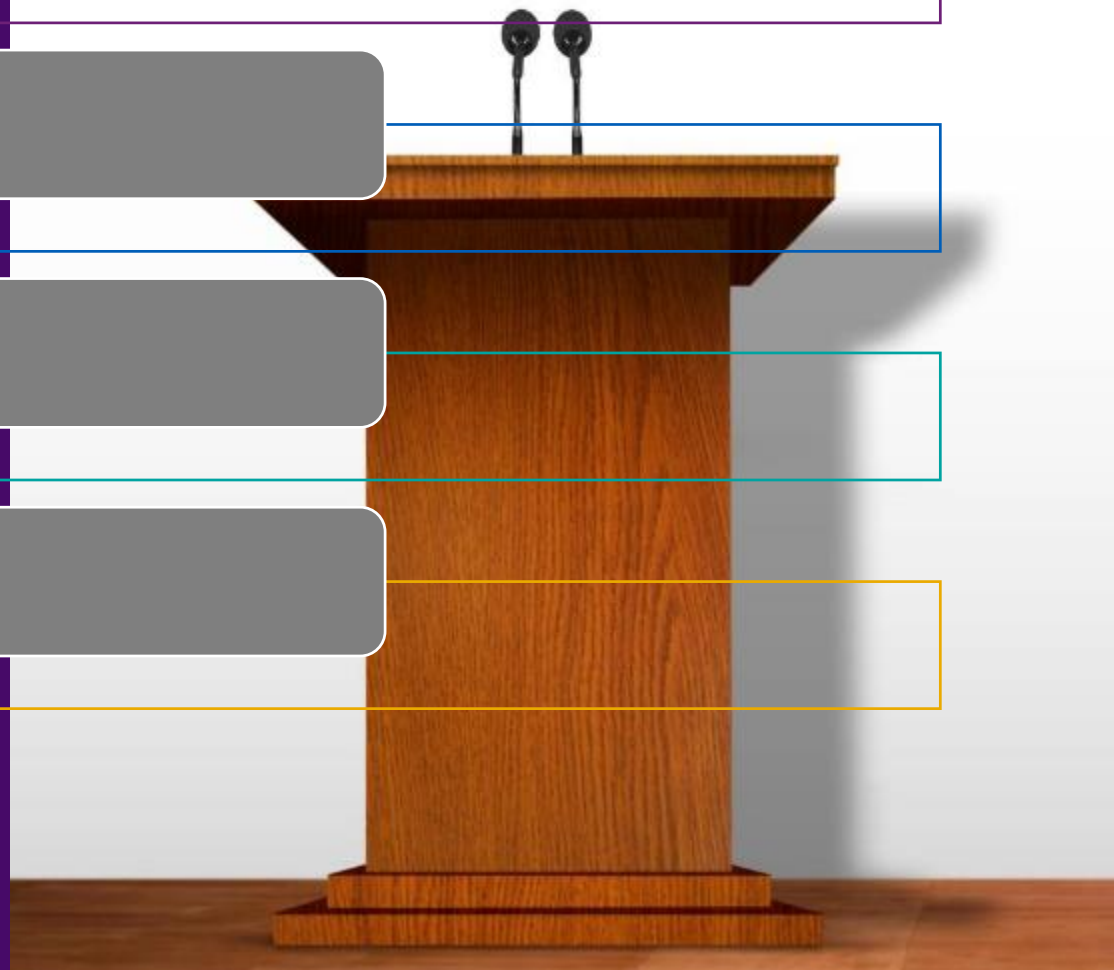
2015	2016	2017	2018
Water crises	Failure of climate-change mitigation and adaptation	Weapons of mass destruction	Weapons of mass destruction
Rapid and massive spread of infectious diseases	Weapons of mass destruction	Extreme weather events	Extreme weather events
Weapons of mass destruction	Water crises	Water crises	Natural disasters
Interstate conflict with regional consequences	Large-scale involuntary migration	Major natural disasters	Failure of climate-change mitigation and adaptation
Failure of climate-change mitigation and adaptation	Severe energy price shock	Failure of climate-change mitigation and adaptation	Water crises

Economic Environmental Geopolitical Societal Technological

Source: 2018 the WEF Global Risks Landscape 2018

Agenda

- Why build Business Resilience?
- What does it entail?
- The role played by the Internal Auditor
- Auditing for Business Resilience



The need for resilience

Today's highly connected and global organizations are facing countless threats of disruptions to business operations. While some risks can be monitored and mitigated, high-impact, hard-to-predict events are occurring more often than ever.

Natural disaster

Drought

Ebola

Flooding

Earthquake

Landslides

Human error

2010 Deepwater Horizon oil spill

Building collapse

1986 Space Shuttle Challenger disaster

IT failure

Source: 2016 Technology Risk Radar, KPMG International

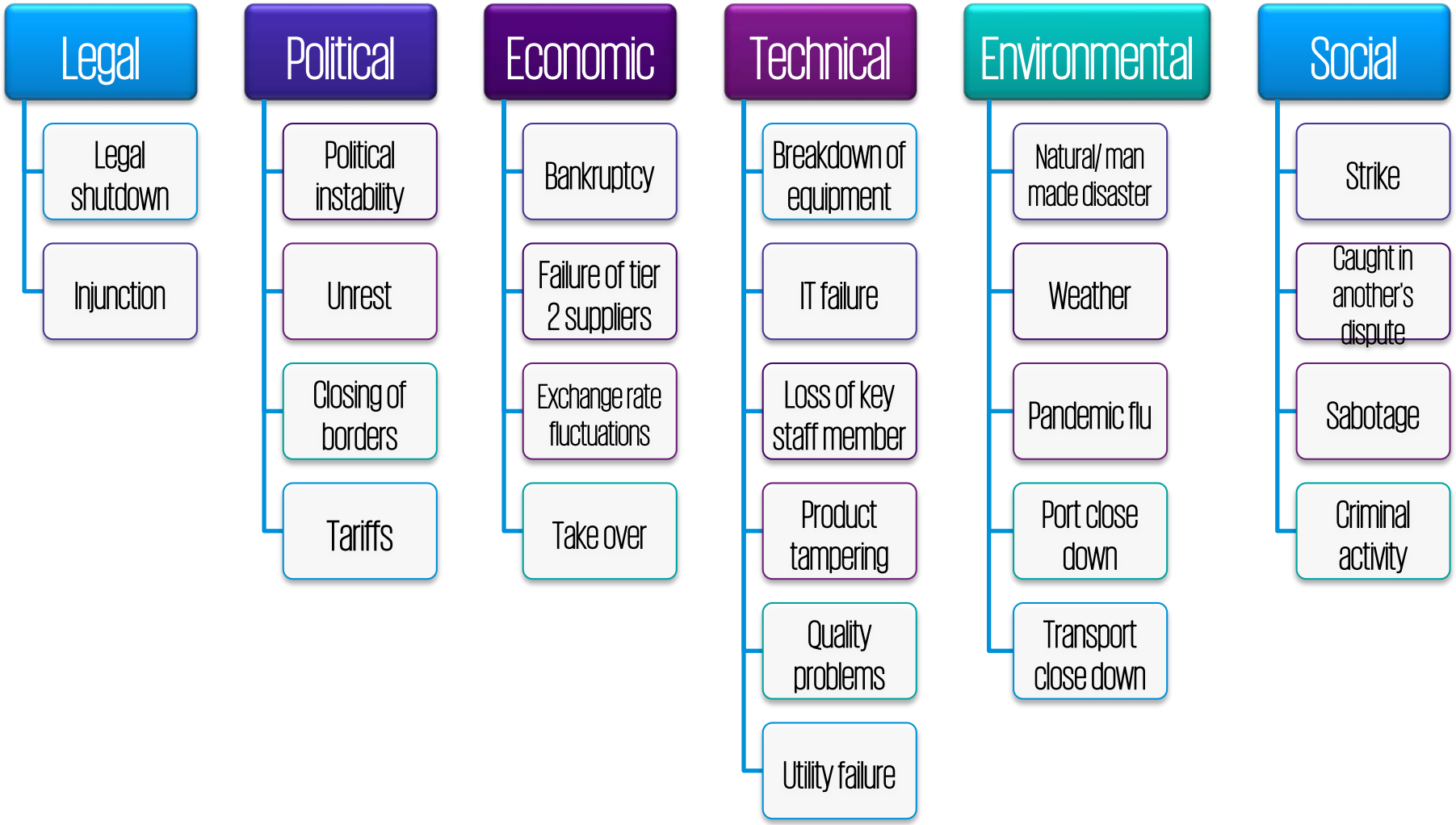
Adversary (terrorism)

2013 Westgate Attack

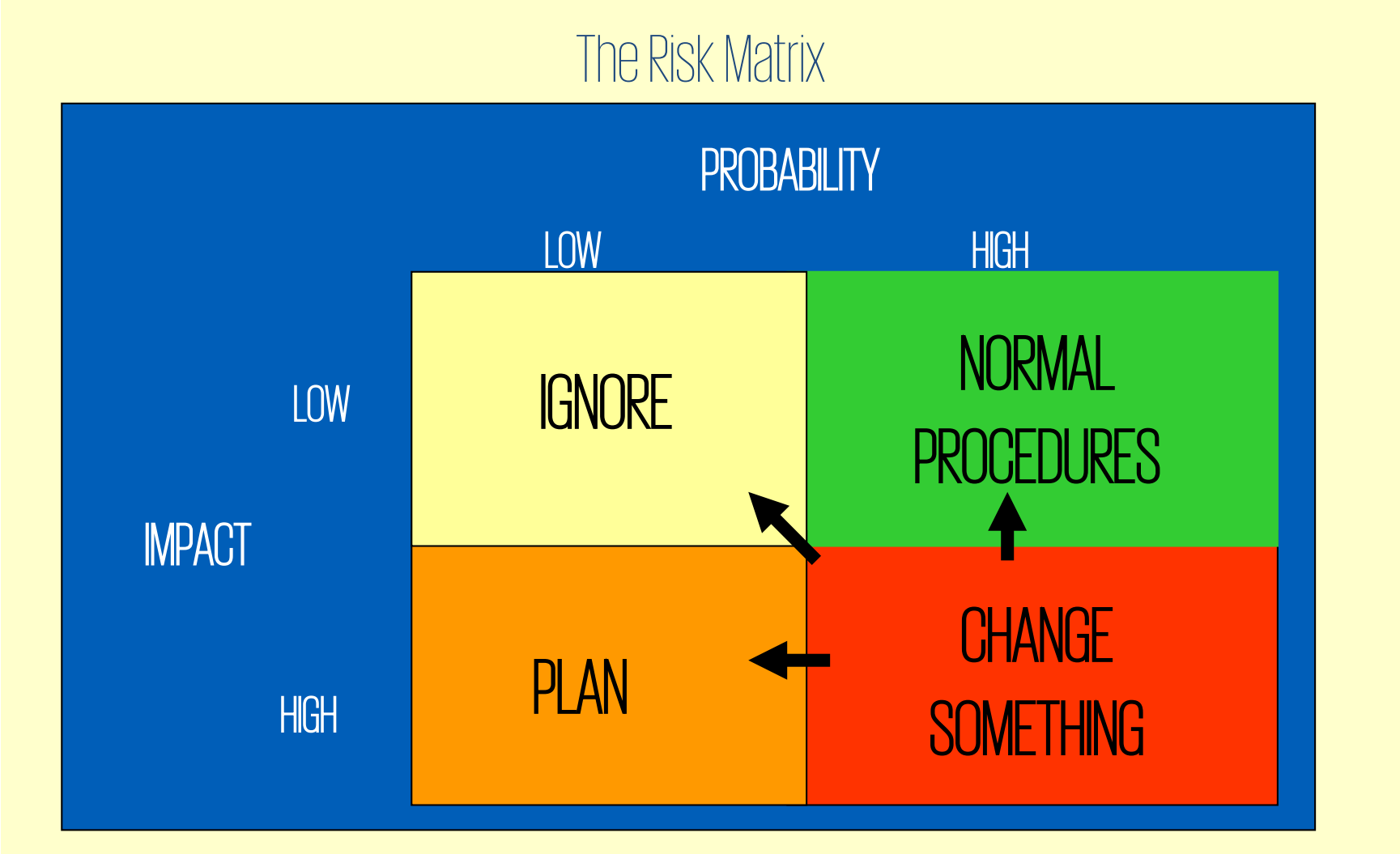
2015 Garissa Attack

1998 US Embassy Bomb Attack

The need for resilience

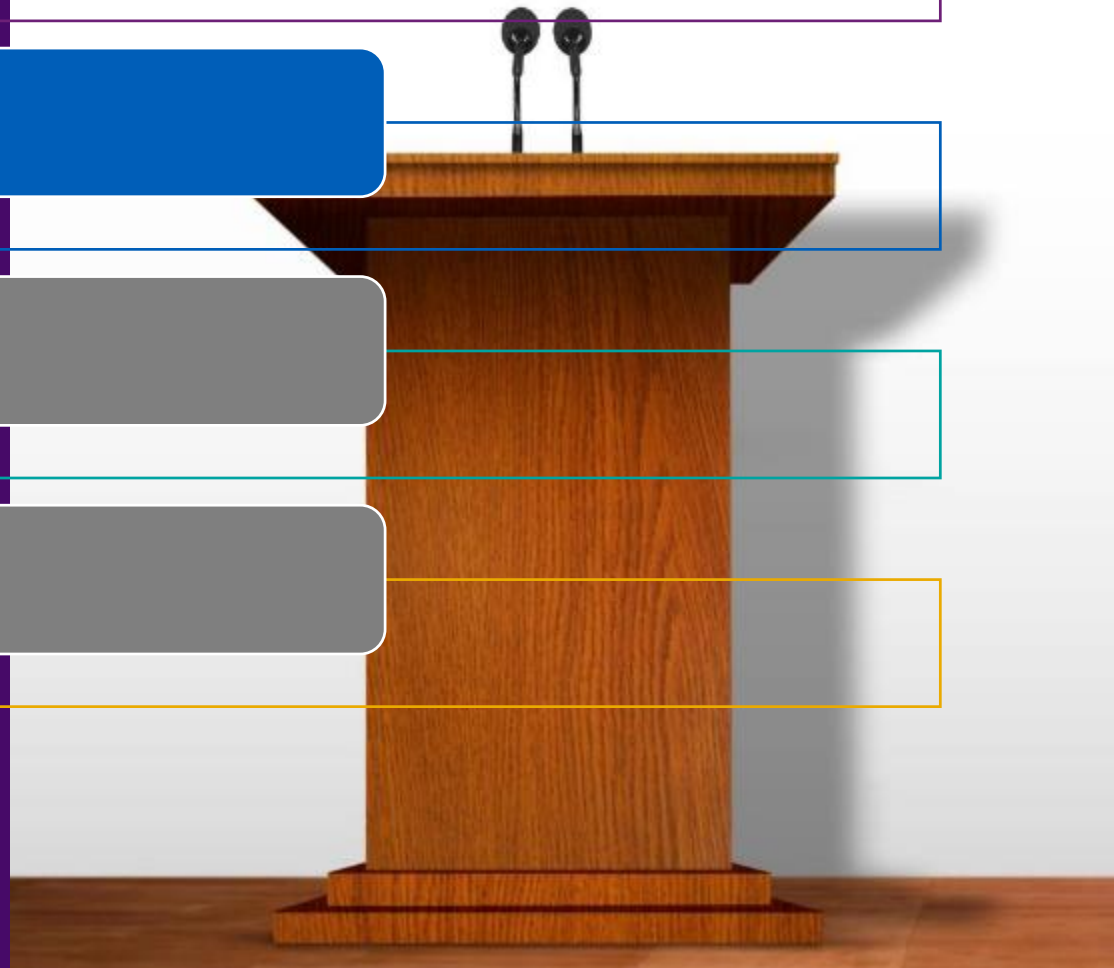


The need for resilience



Agenda

- Why build Business Resilience?
- What does it entail?
- The role played by the Internal Auditor
- Auditing for Business Resilience



Business Continuity defined...

Business Continuity is:

The capability of an organization to continue delivery of products or services at acceptable predefined levels following disruptive incidents.

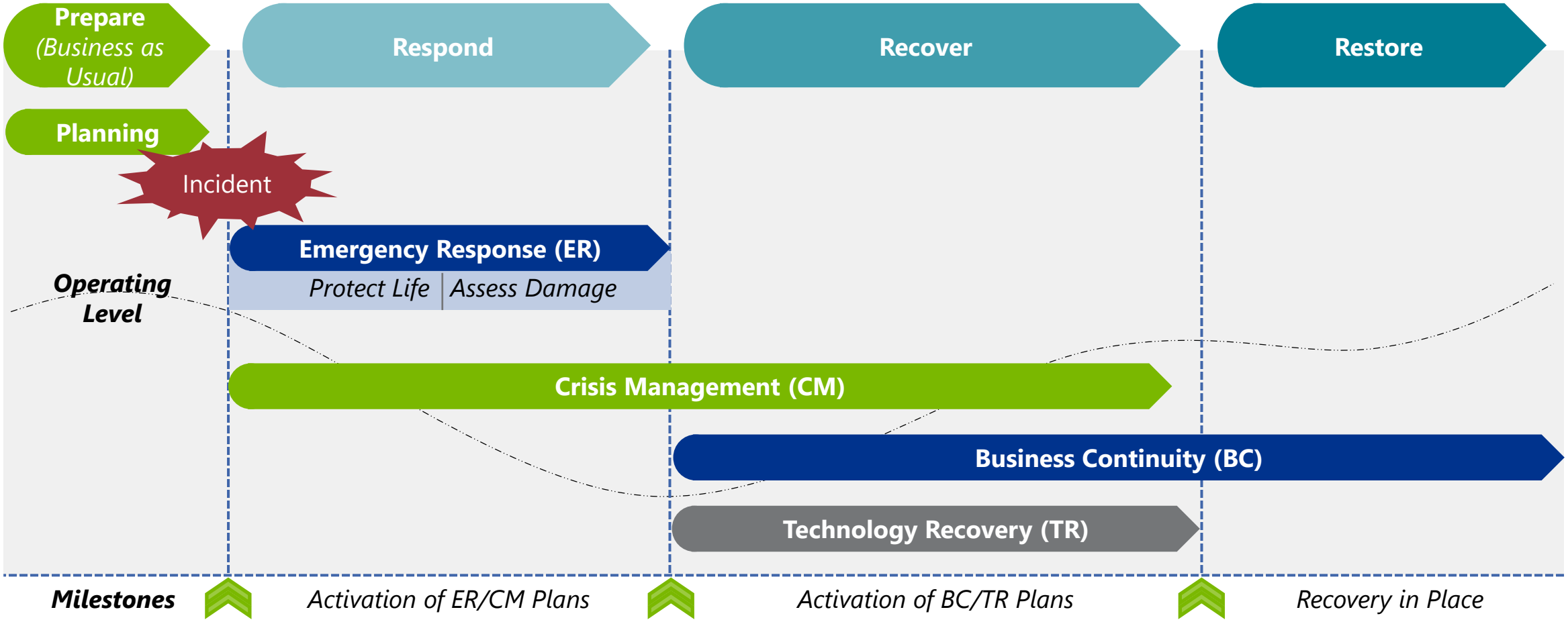
Source: *ISO 22301:2012 Clause 3.3*

BCM capabilities

BCM is a holistic process that must focus on all aspects of the Organization. The BCM capabilities that must be put in place comprise:

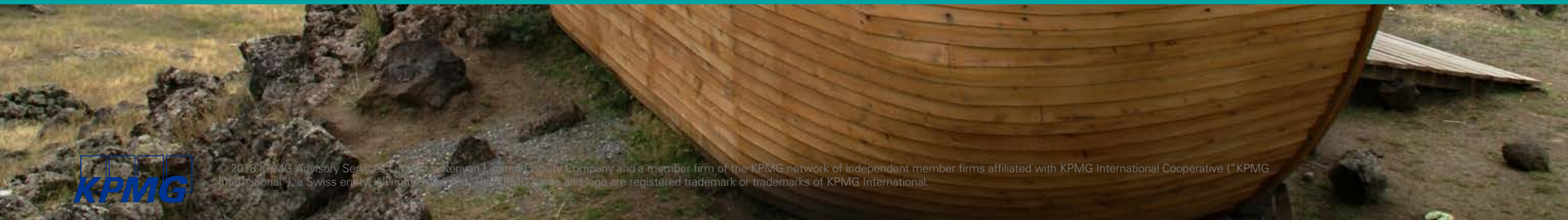
Recovery event time line

An effective resilience program must include an integrated and coordinated approach among all aspects of the recovery event time line.



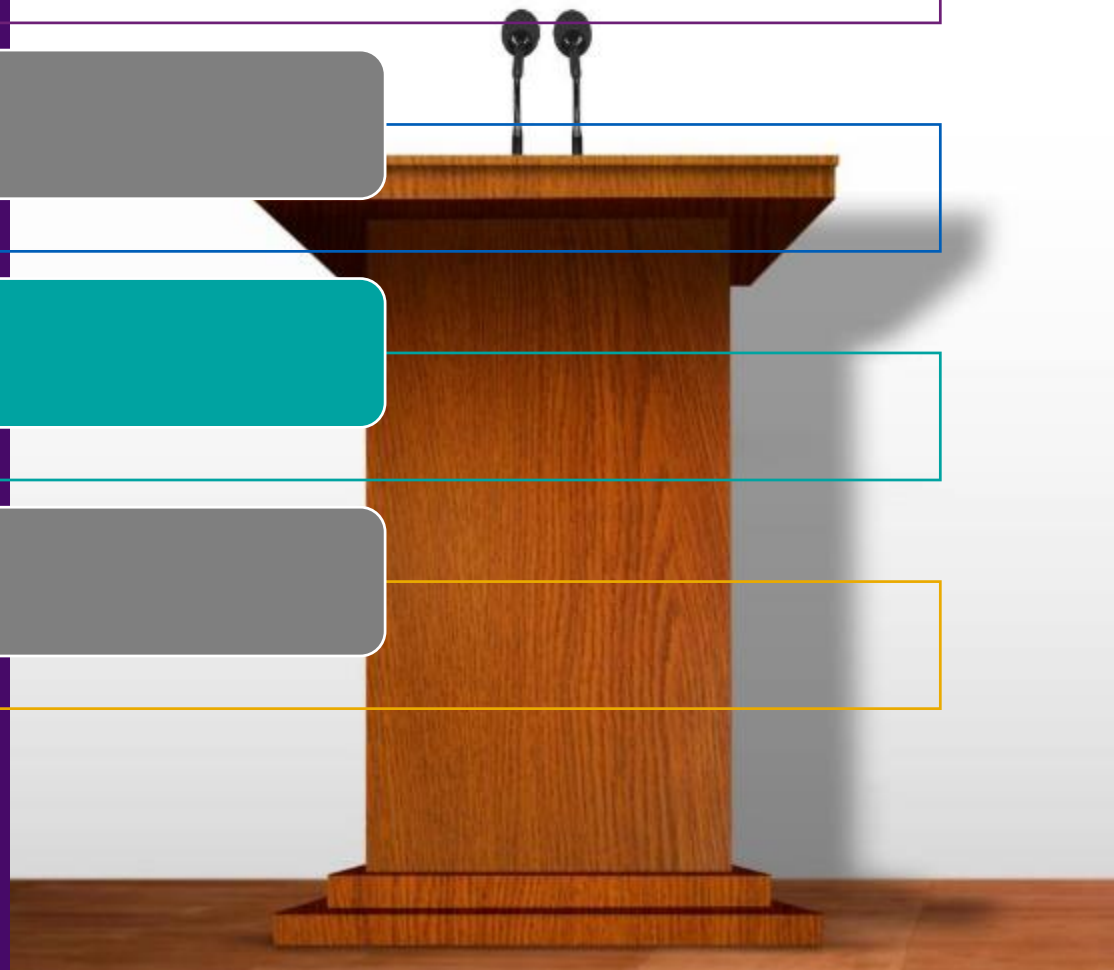
Business Continuity Planning

"It is **NOT** about trying to avoid bad things from happening to your business, but having a plan if they do"



Agenda

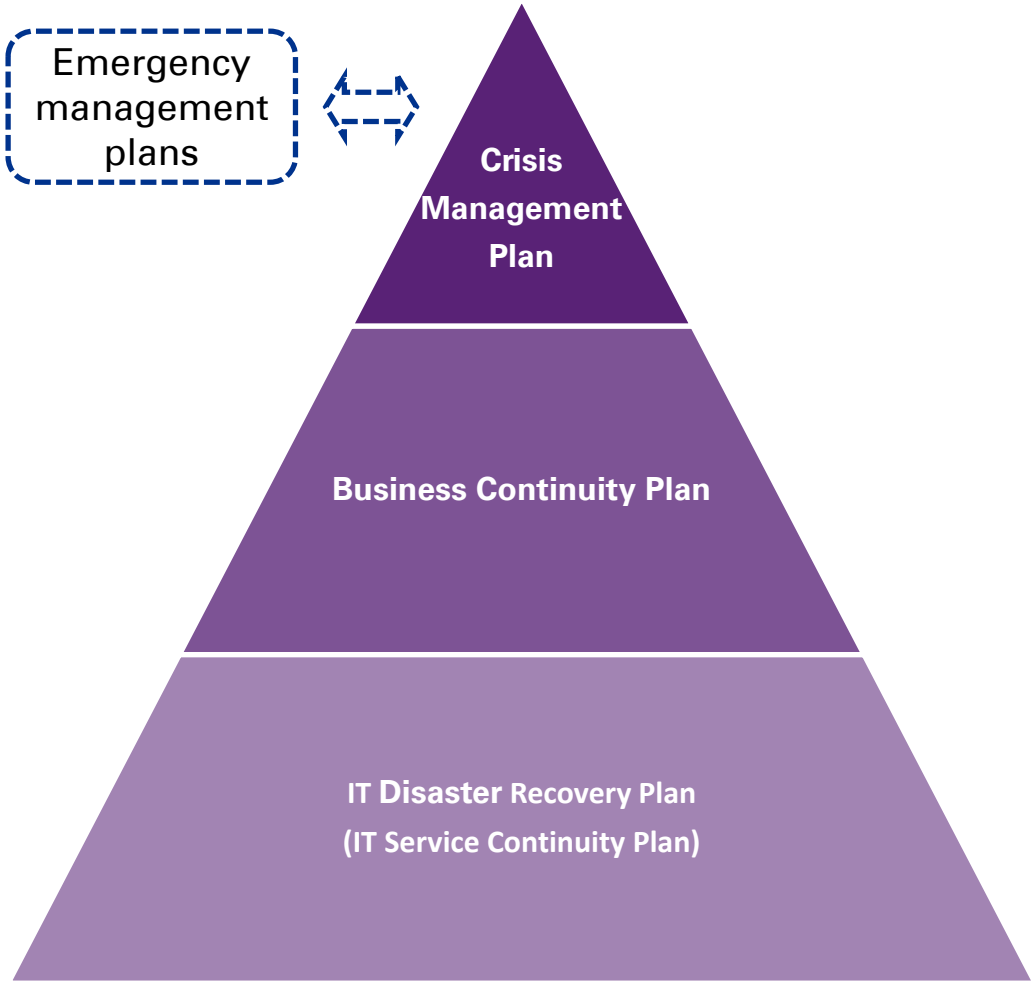
- Why build Business Resilience?
- What does it entail?
- The role played by the Internal Auditor
- Auditing for Business Resilience



BCM Framework

A BCM Framework comprises:

Emergency management plans



A **Crisis Management Plan (CMP)** outlines the immediate management level response to manage a crisis situation and recover critical operations. CMPs may include:

- Management roles and responsibilities, including escalation procedures
- Internal and external communication strategies, including stakeholder management
- Coordination with external recovery agencies
- Coordination with internal business continuity and recovery teams.

A **Business Continuity Plan (BCP)** outlines the procedures to follow during a major unanticipated disruptive event. BCPs may include:

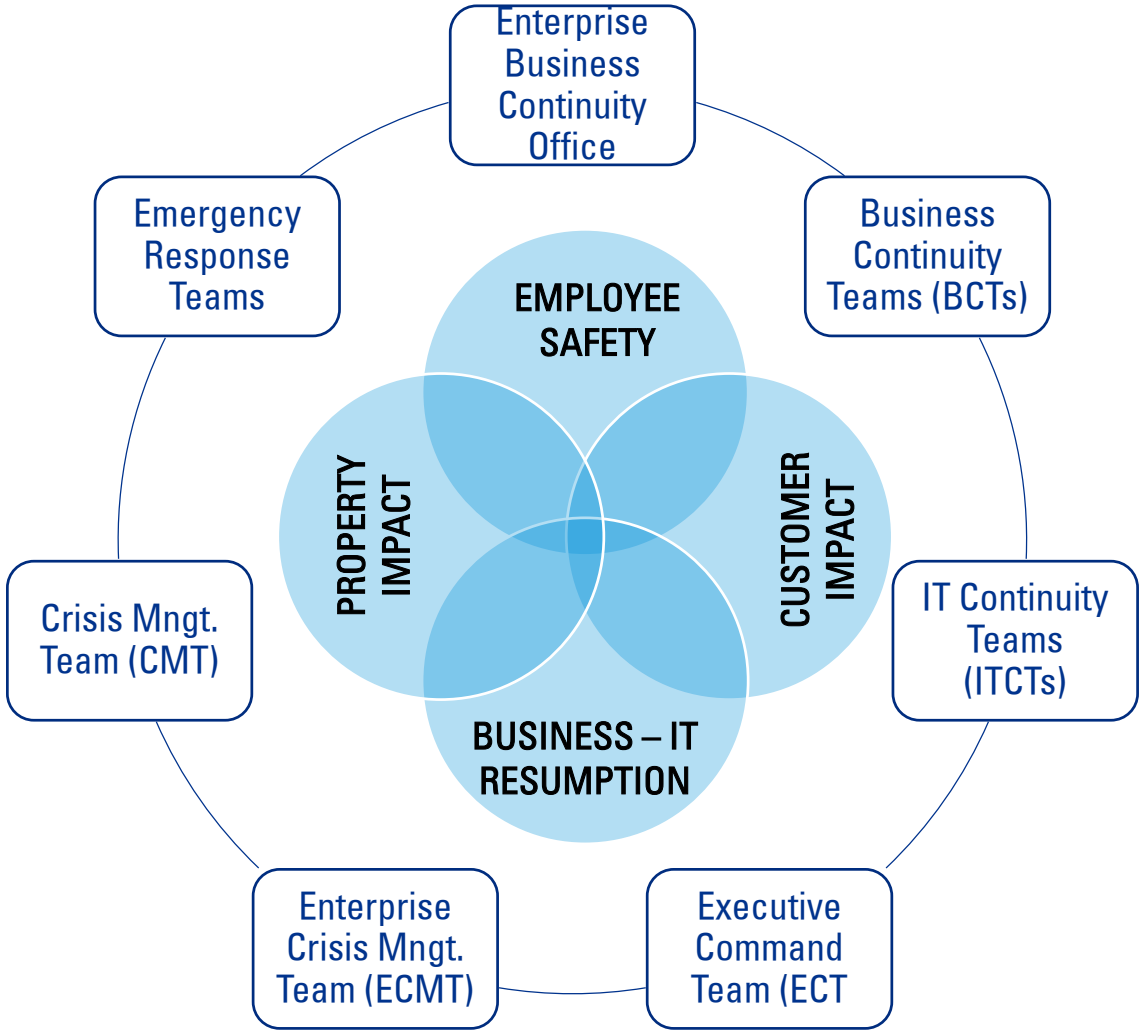
- Business recovery strategies (what needs to be performed to continue critical operations)
- Contact lists
- Equipment requirements
- Personnel requirements.

An **IT Disaster Recovery Plan (DRP)** outlines the specific procedures required to recover or restore critical IT systems. A DRP can be incorporated either as part of a BCP, or more commonly is a separate document.

KPMG

Understand what BCM is about

PLAN	Policy
ASSESS	Risk Assessment
	Business Impact Analysis
DESIGN	Risk Reduction Strategies
IMPLEMENT	Plan Development
EXERCISE	Test
MONITOR	Maintenance
	Awareness
	Measure



The role of the Internal Auditor

Keep pace with the business

Involvement with BCP/DRP during formulation and/or update

Evaluate business continuity **readiness** and report this

Highlight the risk of a 'lacking' BCMS

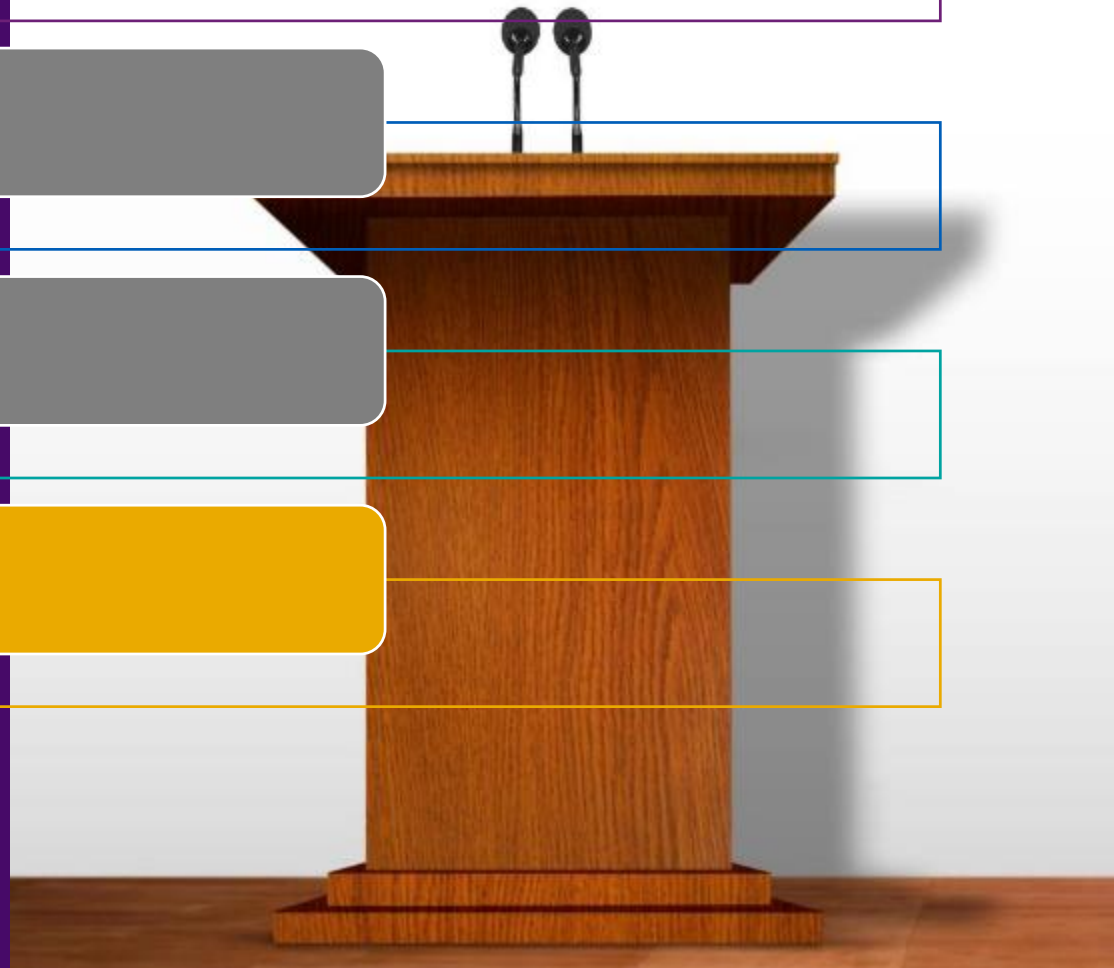
Focus on "does the BCMS **work**" and not on existence

KPMG

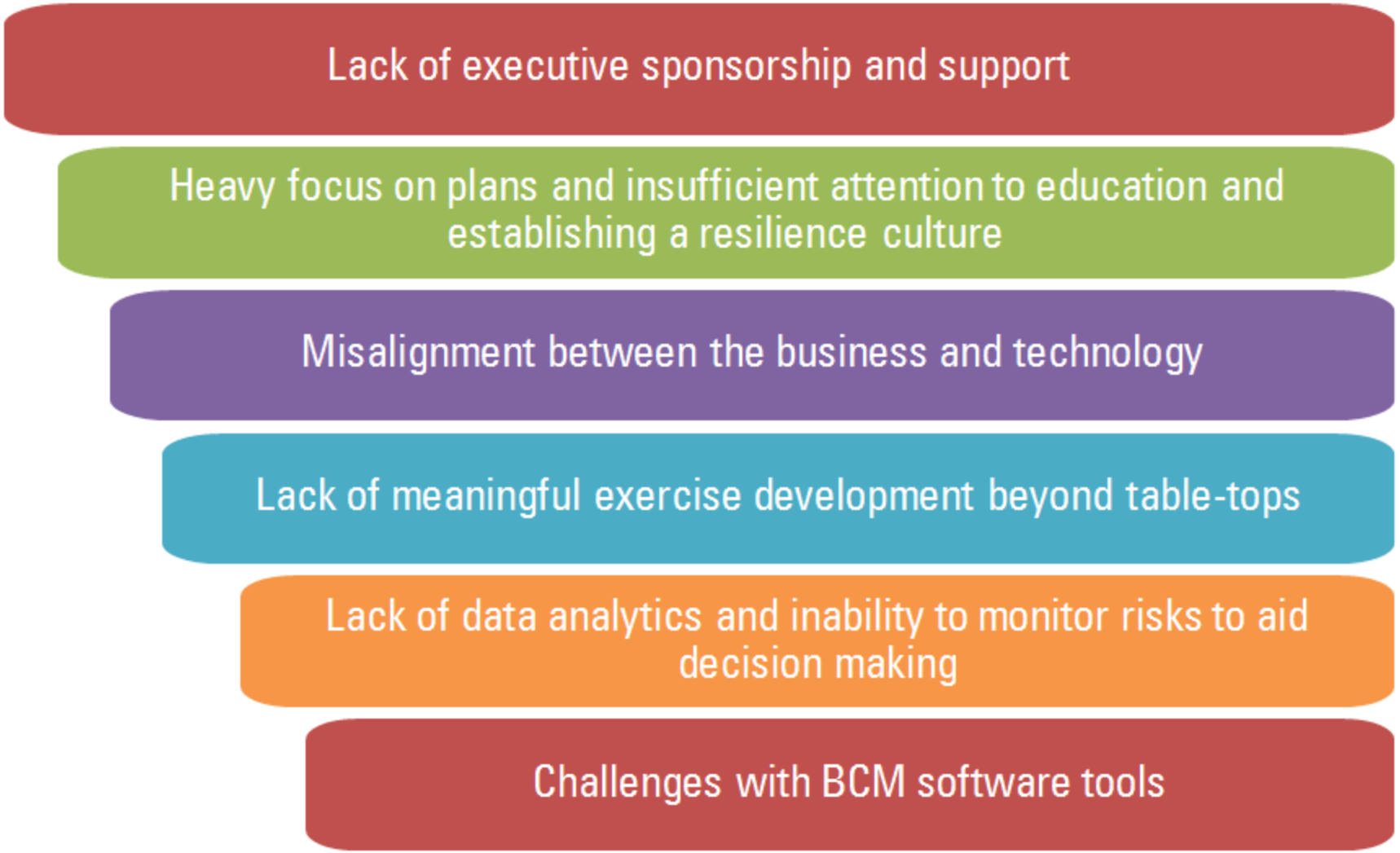
A resilience culture – what does it mean to you?

Agenda

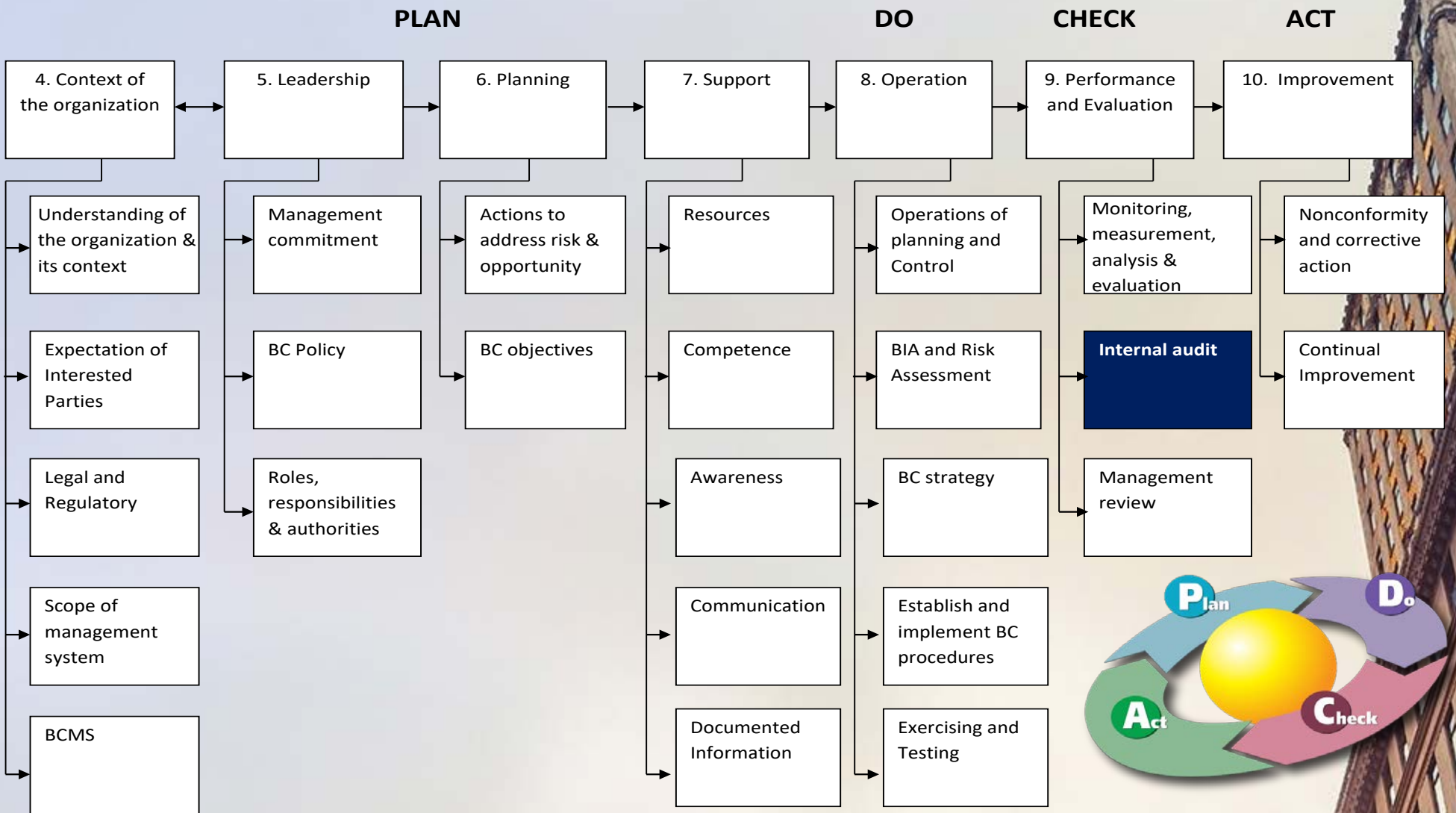
- Why build Business Resilience?
- What does it entail?
- The role played by the Internal Auditor
- Auditing for Business Resilience



Challenges to resilience



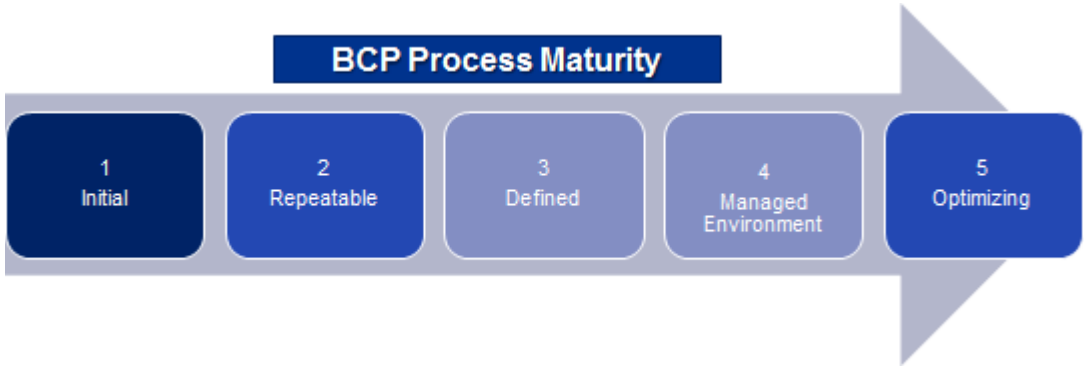
BS ISO 22301:2012 standard



Typical IA work-plan for BCM – high level

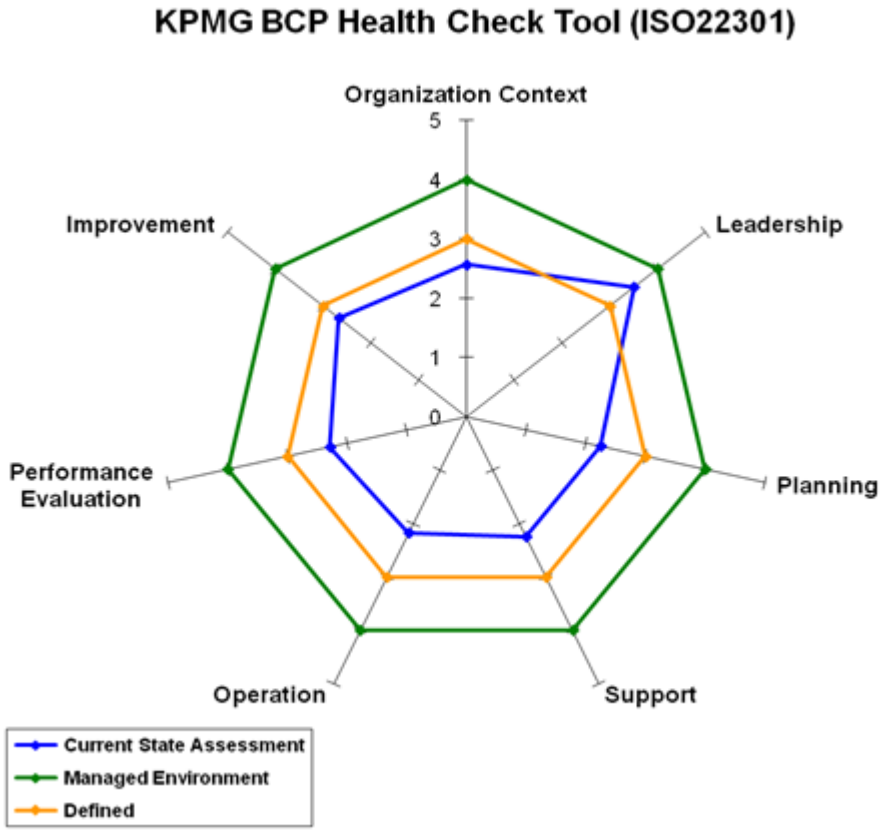
Scope/Area
Year One
Management has recognized the need for business continuity planning (BCP) program and has taken steps to establish and maintain such a program
Interim business continuity plans are sufficient to meet critical requirements should a disaster occur in the short-term
Business continuity plans are tested regularly and updated to reflect lessons learned and to address gaps and deficiencies identified in the tests
Documentation of business continuity plans is kept current
Overall BCP roles and responsibilities are clear
Reporting processes
Year Two
Business continuity plans are based on a thorough business impact analysis (BIA)
Critical business partners have appropriate business continuity plans
Business continuity plans consider and are linked to business planning processes.
Business continuity plans consider and are integrated with technology disaster recovery plans

Reporting on BCM review - a health-check approach

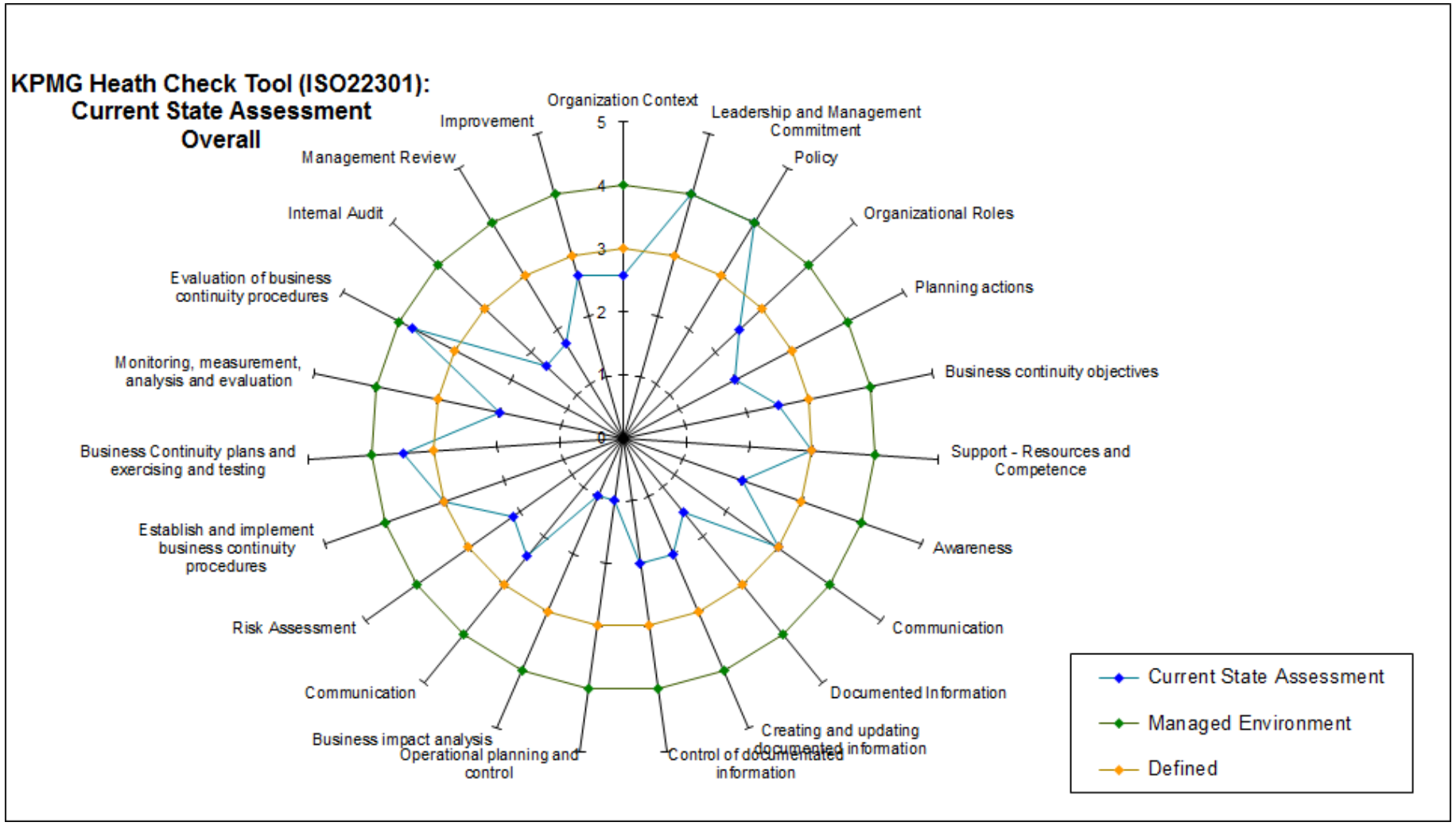


Rating scale

1. **Initial** – Ad hoc processes exist
2. **Repeatable** – Not documented but structured
3. **Defined** – Formalized and documented
4. **Managed** – Integrated with other organizational processes
5. **Optimized** – Defined KPI's with monitoring mechanisms for continuous improvement and enhancement



Reporting on BCM review - a health-check approach (cont'd)



Understand stakeholder concerns

Board's perspective

Strategic objectives

- Do we have a BCM plan that can withstand any disruption?
- Is the BCM program adding value?
- Are BCM objectives consistent with Organisation objectives?
- Is the BCM strategy aligned to the organisation strategy?

CEO's perspective

Gaining competitive advantage

- Can I be in business without a tested plan?
- Can my business withstand a breakdown in processes?
- How would it impact corporate value? Our people? Reputation?
- What happens if we don't deliver on our service promise?

CIO's perspective

Delivering IT value

- Is the role of IT in business continuity management (BCM) clear?
- Are IT recovery requirements determined by the business?
- Am I confident we can withstand or respond to a cyber attack?
- Can we support the discovery process for intensive litigation?

CFO's perspective

Cost effectiveness

- Do I understand the cost of a business disruption?
- What is the right balance between purchasing business disruption insurance and building our own processes and tools?
- How do I know we have made cost-effective BCM choices?

KPMG

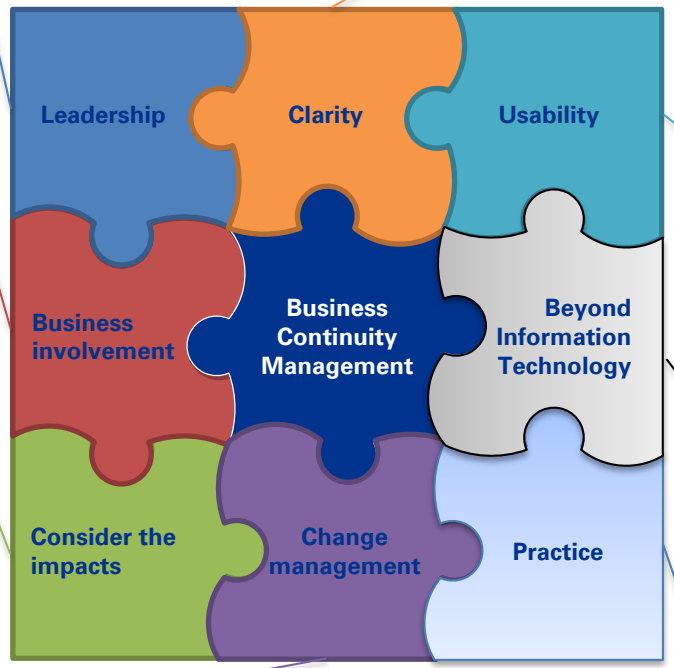
Key Success Factors of BCM

Effective BCM programmes require executive management support.

BCM should be driven from business units.

BCM focuses on the impact of major disruption even when it is difficult to accept the scenario.

BCM should be embedded as part of the change management process to build resilience in the organisation.



Plans must be written clear ly and consider the capabilities of team members during significant business disruption.

Plans must be simple, usable and effective. Staff should be able to pick up a plan and understand what they need to do.

IT is critical but is just one part of a BCM framework.

To be good at BCM requires a lot of practice.

Critical Success Factors

An informed perspective

The internal auditor must bring to bear a perspective on BCM that transcends surface-level issues and speaks to an integrated view – encompassing global best practices, emerging practices, an understanding of "common" practices in the industry yet also pinned to a maturity model which outlines the range of possibilities. IA should bring an understanding of the people, process, technology and governance dimensions critical to your success.

An understanding of your business

While no one will know the business better than management and employees, in conducting an IA review of your BCM program, you will be best served by an internal auditor that can rapidly understand the business, one that has some key relationships that will facilitate information gathering and the overall achievement of your objectives. The internal auditor must possess this understanding yet still retains the independence required to dutifully conduct this assessment.

Stakeholder involvement

Reviews of this nature will invariably lead to conclusions that validate the status quo in certain areas and recommend improvements in others. Active engagement with key stakeholders throughout the assessment will be required to ensure that consensus is built as the groundwork for change. The internal auditor must provide an approach that includes stakeholder involvement and alignment from day one.

Audit Program for a BCM

Key BCP Criteria - Plan and Foundations

1. Critical operational areas have been defined.
2. Key people critical to the operations of the business/department have been defined.
3. Critical skillset necessary to support the operational activities of the business have been defined.
4. Equipment needs of the business/department have been defined.
5. Adequate recovery work space has been defined and is available.
6. Key assumptions used as a basis for the plan have been defined.
7. Key objectives of the plan have been defined and communicated.
8. A documented business resumption plan(s) exist covering the entire enterprise.
9. Key timeframes within the recovery process have been defined, approved, and communicated.
10. System needs that support the business have been defined.

KPMG

Audit Program for a BCM

Key BCP Criteria - Management Support

1. Senior management support for the resumption plan and related process exist.
2. Senior Management reviews and approves Recovery Time Objectives (recovery windows 0-48, etc.) on a regular basis.
3. Budget shillings and FTE's are specifically allocated to the business resumption process.
4. A defined sponsor for the resumption plan has been established.
5. A dedicated person has been assigned responsibility for the plan and planning process.
6. Management team participate in testing and simulation exercises.

KPMG

Audit Program for a BCM

Key BCP Criteria - Quality Assurance and Change Controls

A change management process for the resumption plan has been implemented.

A framework for management oversight and monitoring for resumption planning activities is in place.

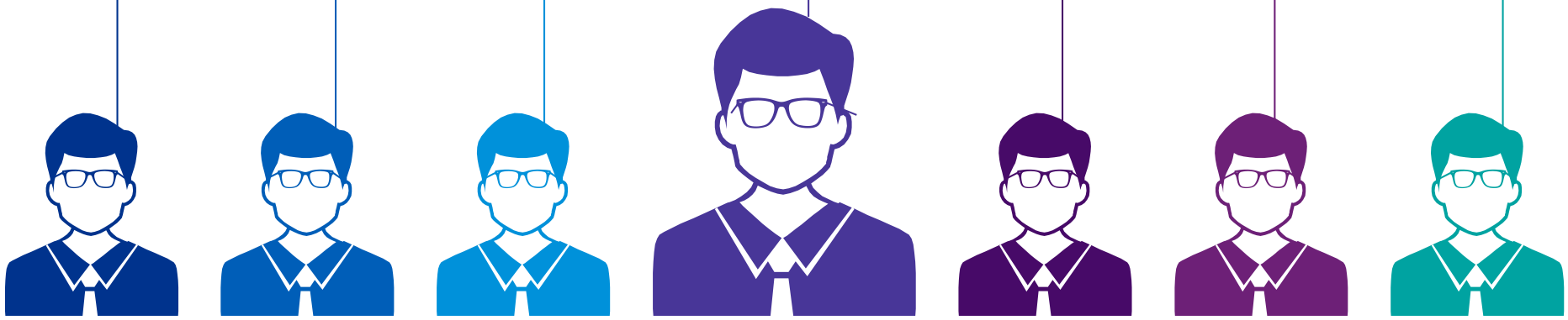
A testing methodology that includes objectives, criteria, and an approach has been defined and is in place.

Periodic training is performed for all aspects of the plan.

Testing of the resumption plan has been performed.

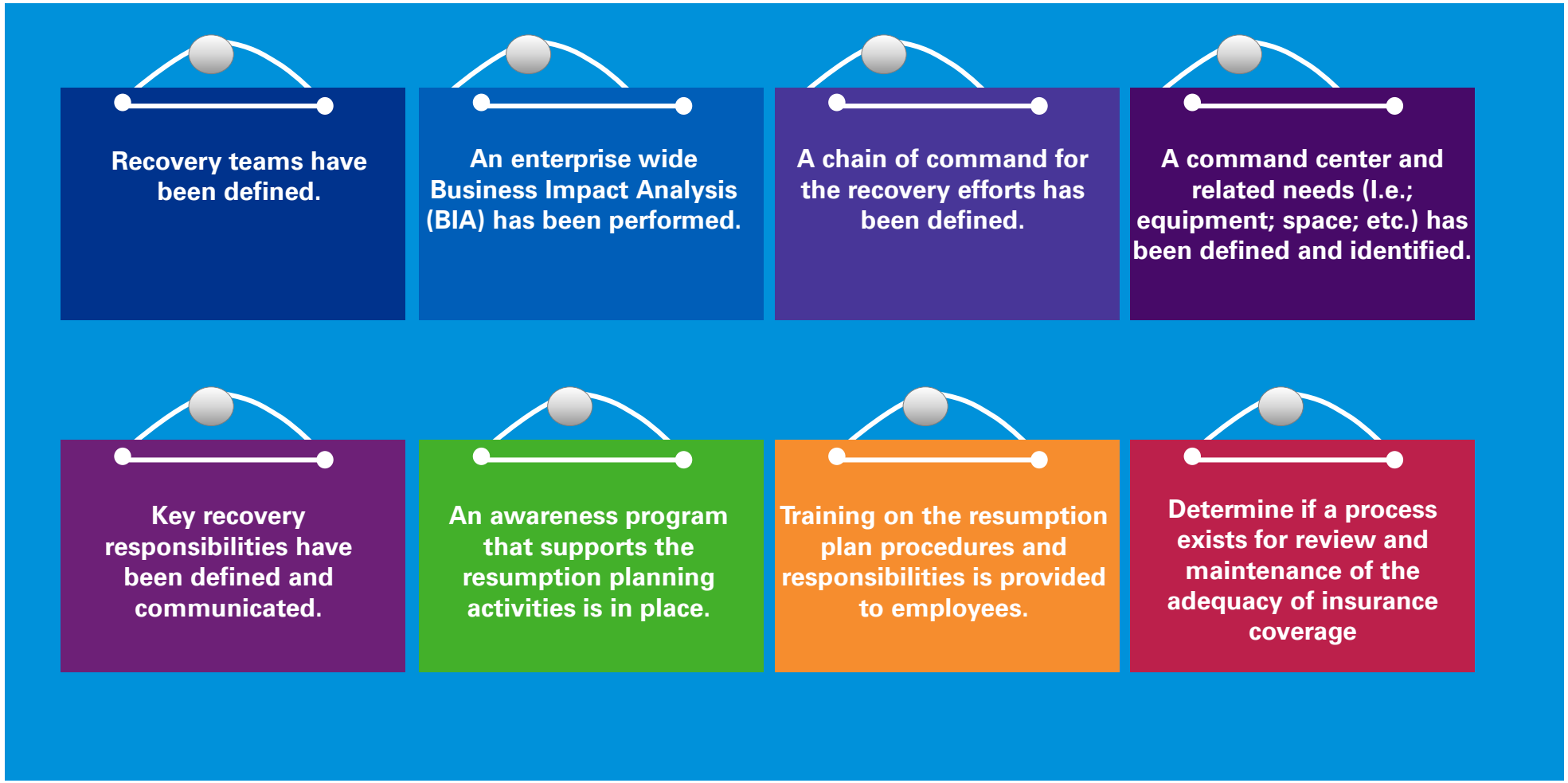
Results of tests are reviewed by management and incorporated into the planning process.

New Hires receive training or orientation related to their departments recovery plan.



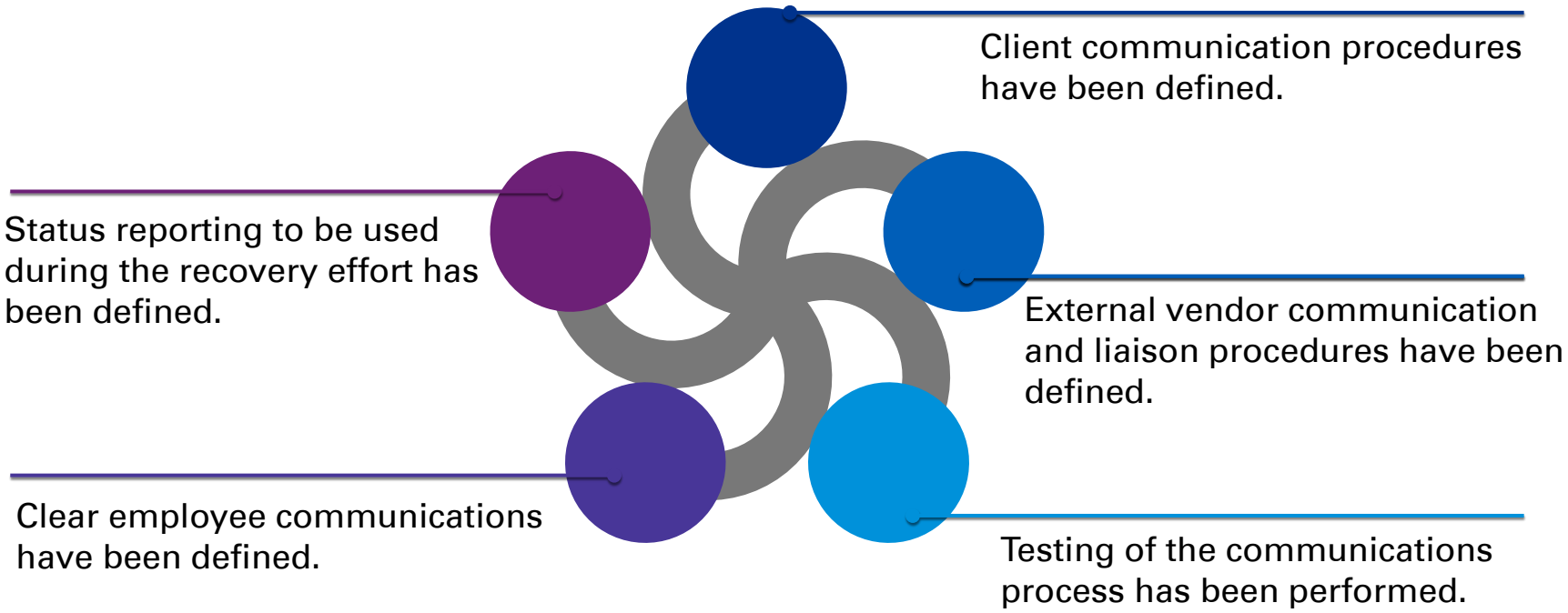
Audit Program for a BCM

Key BCP Criteria - Structure, Organization, and Planning



Audit Program for a BCM

Key BCP Criteria - Communication



Audit Program for a BCM

Key BCP Criteria - Other (Restoration, Vendor Plans)

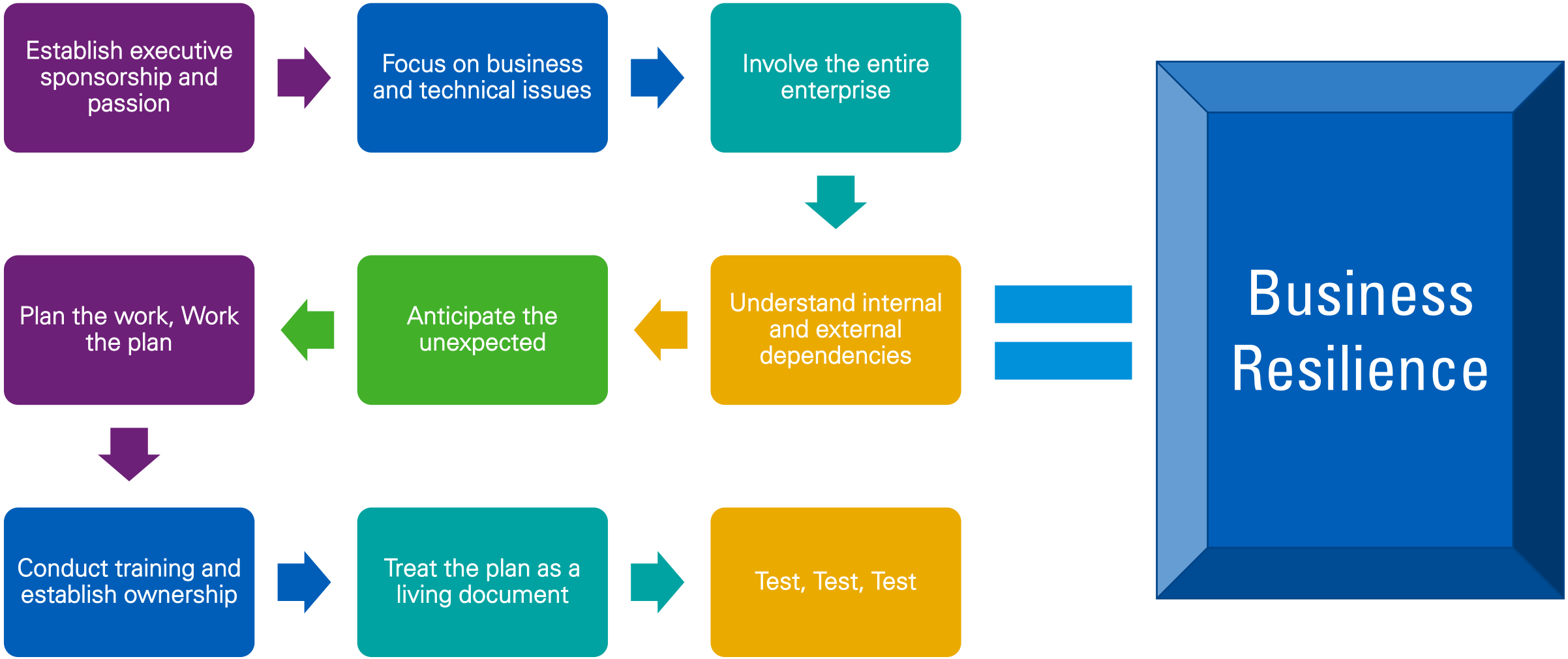
Restoration activities that support return to the "home" site have been defined.

Ascertain if management has obtained and evaluated the adequacy of contingency plans of its critical servicer(s).

Sensitive document handling procedures to be followed at the alternate site have been defined.

Determine if the organization has considered the impact of a disaster on the vendors and service providers side.

Ingredients for a successful plan



Thank you!

#CEOOutlook

Antony Nzamu
Associate Director
KPMG Advisory Services Limited
T: +254 709 576 247
E: anzamu@kpmg.co.ke

kpmg.com/socialmedia