



Business Continuity & Resilience

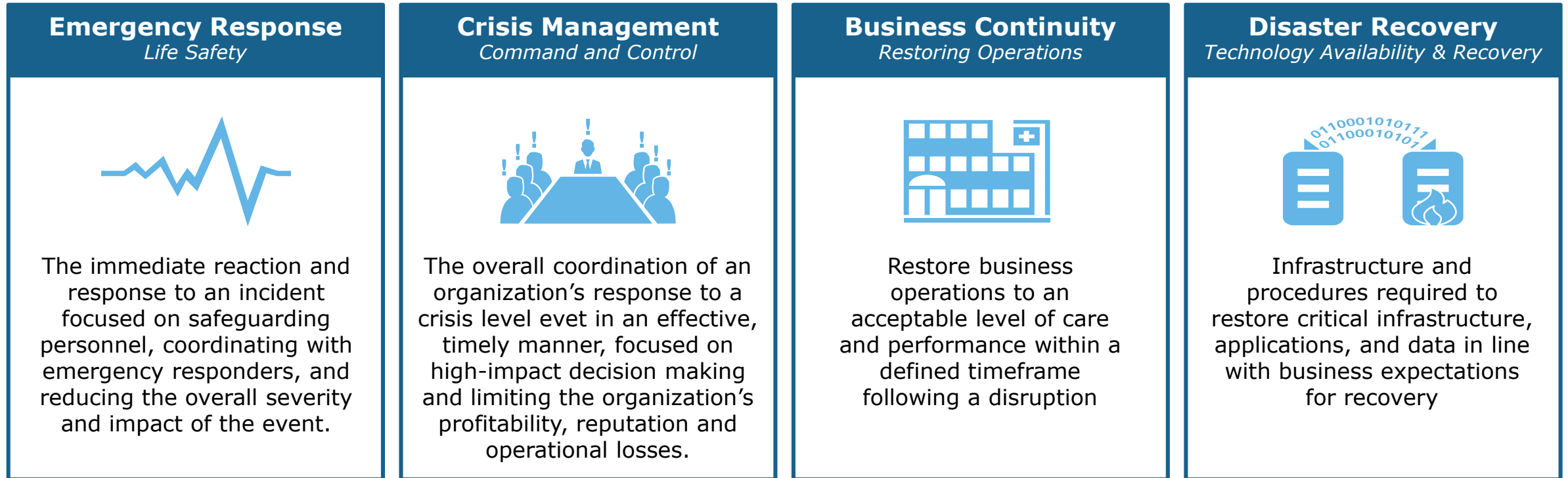
UC Ethics, Compliance and Audit Symposium

Contents

3	What is business resilience?
4	Timeline of events and the resilience lifecycle
5	Recovery requirements and strategy considerations
6	The importance of training and exercising
7	Cyber resilience vs traditional recovery
8	Resilience challenges and success factors
9	Lessons learned from the field

What is business resilience?

Resilience is a state of preparedness and capability that is achieved, in part, through strong orchestration of the emergency response, crisis management, IT disaster recovery and business continuity disciplines.

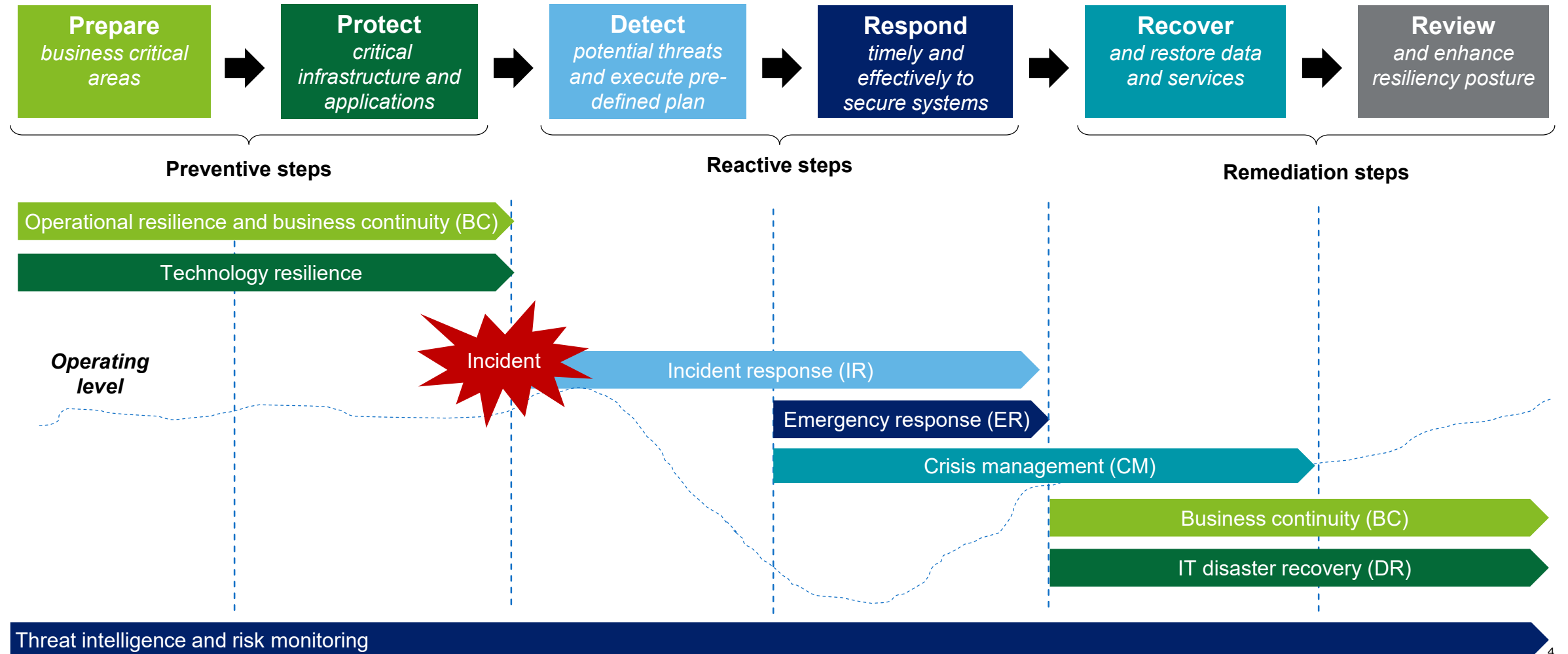


Not all catastrophes are natural disasters or technology outages—resilience program should:

- address almost any type of disruption
- encourage seamless coordination between technology, business and incident command teams
- aid in the recovery of any type of business function or process

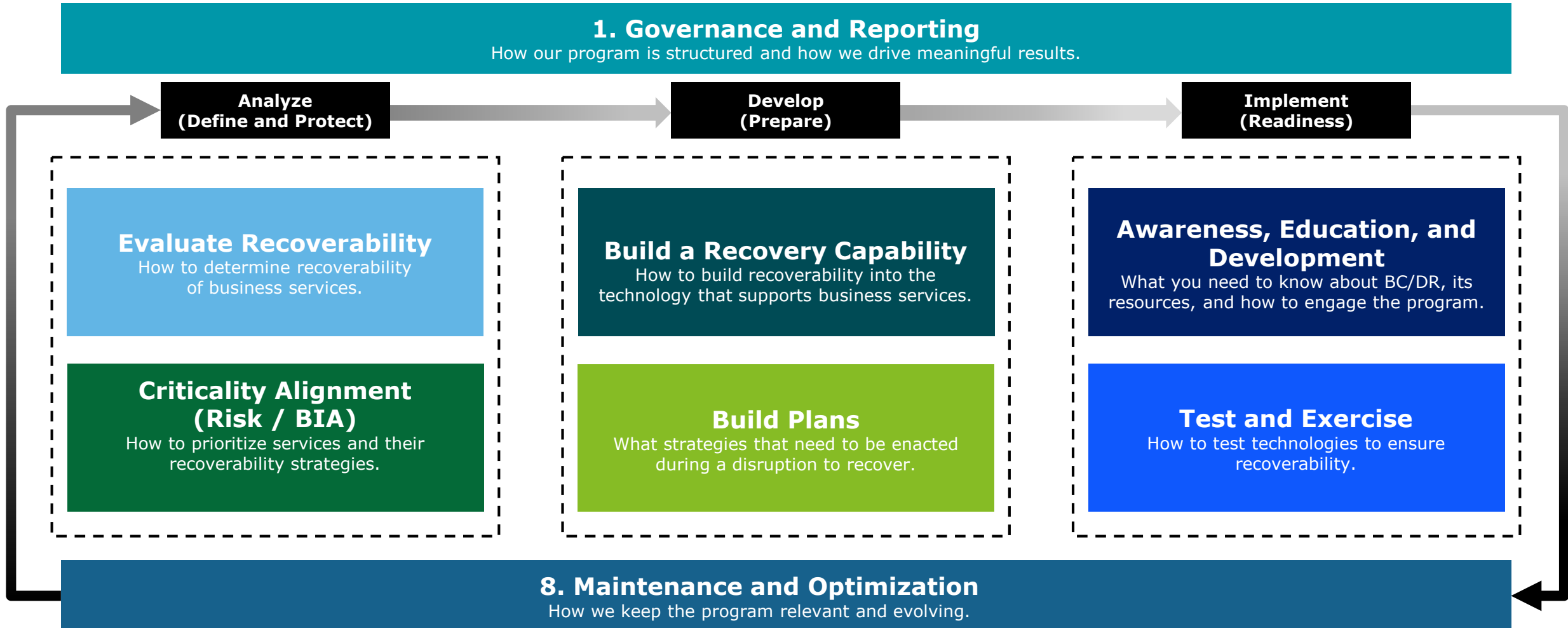
Recovery timeline and resilience disciplines

Each of the resilience discipline play a critical role in an organizations ability to prepare, respond, and recover from a range of scenarios including cyber attacks, natural disasters, terrorism, supply chain disruptions, extreme adverse events and other brand and reputational concerns.



The resilience lifecycle: a programmatic approach

The resilience lifecycle includes a structured approach to establish and sustain a resilience capability throughout an organization. A resilience method should be aligned with leading standards such as ISO22301, NFPA1600, ITIL, NIST, as well as specific regulations by industry.



Recovery requirements and strategy considerations

Accurately gathering the building, technology, human resource, and third party requirements needed for the timely recovery of critical processes during a disruption to operations is a critical component of understanding recovery requirements to drive strategy decisions.

Below are key considerations when developing recovery strategies for each type of enabling asset:



Buildings

- Where do most employees sit on a day-to-day basis?
- What backup facilities are available to employees?
- Do employees have the ability to work remotely?



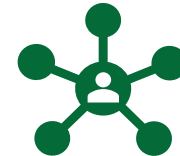
Technology assets and applications

- What applications are unique to each process?
- What other IT assets are used to perform each process?
- Do manual workarounds exist if there is a IT outage?



Human resources

- What is the minimum number of employees needed to perform each process?
- What employees are crucial / key to the process?
- To what level have employees been cross trained?

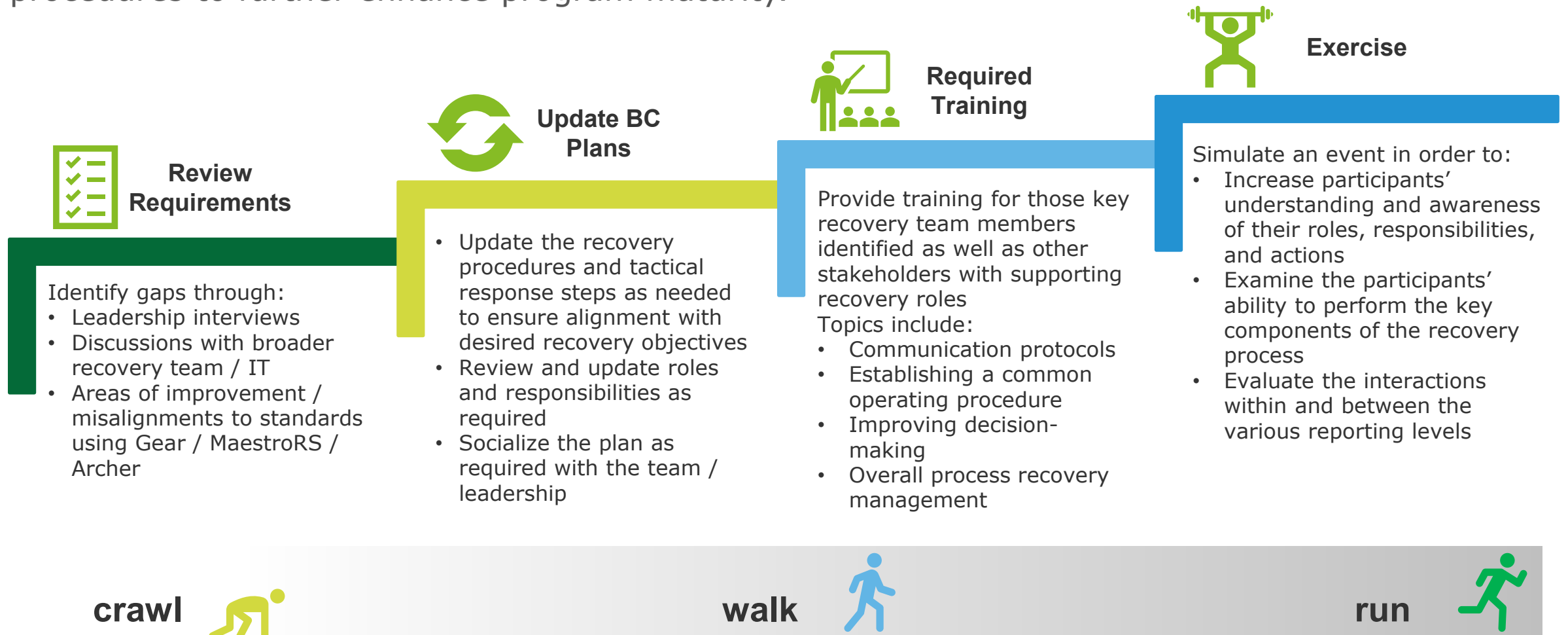


Third parties

- What aspects of the process, if any, are outsourced to a third party service provider?
- Are there any backup service providers available through a retainer? Can the process be insourced for a period of time?

The importance of training and exercising

Training and exercising activities becomes increasingly important as teams begin to decrease reliance on physical plans, and improve understanding and 'muscle memory' of recovery procedures to further enhance program maturity.

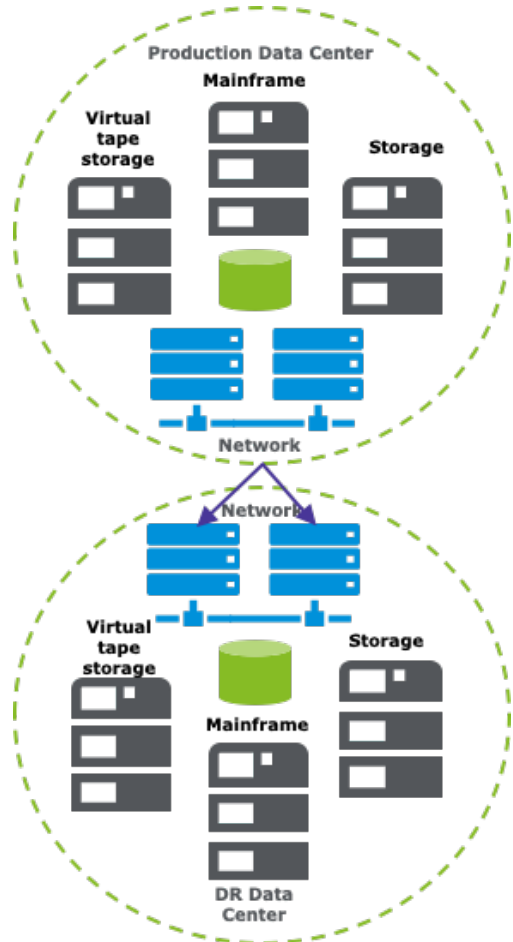


Cyber resilience vs traditional recovery

With increased resilience and replication within the environment, the risk of propagating malware or malicious code across primary processing and recovery data centers also increases. In order to protect against this, cyber resilience incorporates advanced replication technologies and air-gapped cyber data vaults to protect critical data.

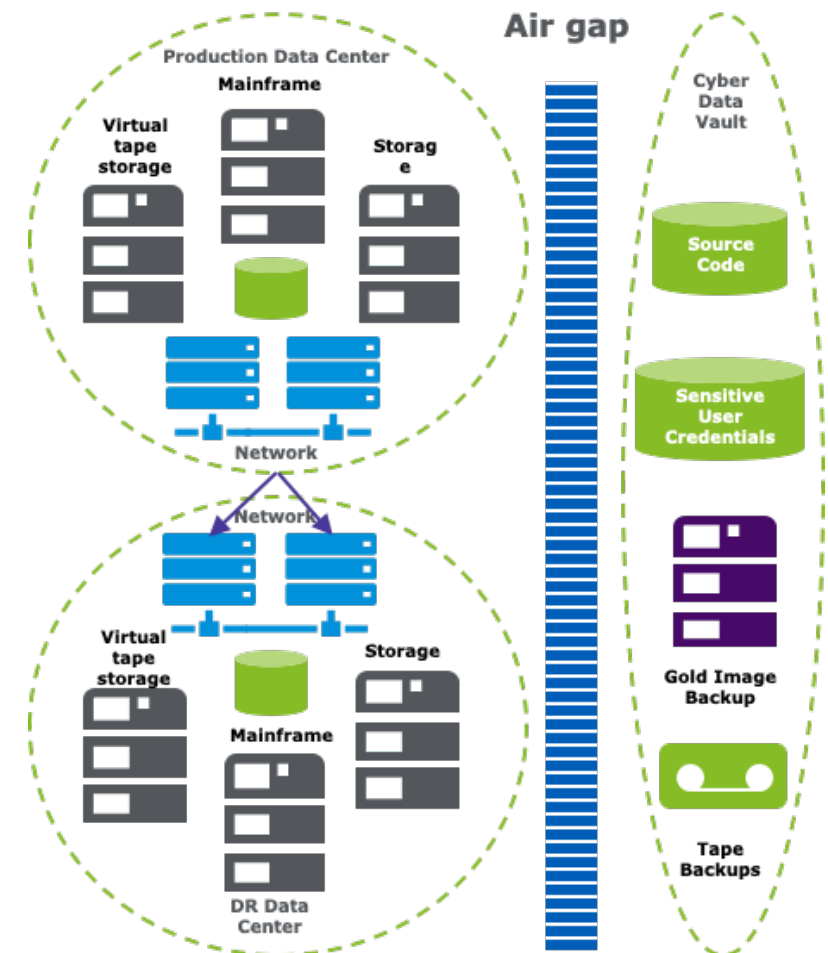
Traditional disaster recovery characteristics

- Replication of data stores across primary and recovery data centers
- Active-Active/Active-Passive failover mechanisms
- High availability configuration
- Virtual tape storage
- Tape backup and offsite storage



Cyber resilience characteristics

- Traditional IT DR plus
 - Air-gapped storage (logical and/or physical) of immutable copies of critical data sets
 - End-point recovery solutions for rapid restoration of workstations
 - Highly integrated with cyber response and crisis management



Resilience challenges and success factors

There are a number of challenges companies typical struggle with to manage risk and sustain results. By focusing on 5 critical success factors, organizations have a higher likelihood of sustained success in mitigating risks and effectively responding to disruptions.

Challenges



Too much focus on "the BCP" – plans are often static and inaccessible during incidents



BC management systems lack data quality to make quick decisions with the best information



Training is a tick-box activity and doesn't encourage commitment and engagement of the business

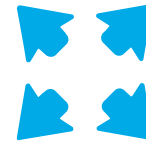


Exercises are routine, overly simplified and do not build organizational "muscle memory"



Measurements that fail to give business leaders visibility and confidence in the organization's ability to recovery

Success Factors



Harmonized response to risks and disruptions – cyber, natural disaster, technology outages, supply chain disruptions



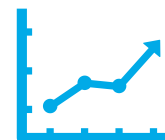
Analytics that can provide insight into risks and impacts, providing information that enables organizations' ability to make decisions



Techniques and media that encourage and streamline engagement of the business, technology and 3rd party resources



Simulations that utilize the analytics to improve organizational "muscle memory" during disruptions

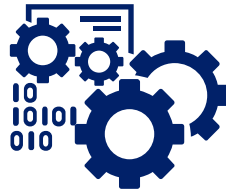


System driven metrics that enable executives to make informed funding decisions about business continuity

Lessons learned from the field

We aim to provide services and work products that protect our client's business operations and enable the continuation of critical business processes after disruptive event. Ultimately, we aim to help create a culture of resilience at our clients.

Keep it Practical and Pragmatic



- Understand the client's perspective and business need
- Avoid unnecessary work products; ask yourself if your work is driving value for the client

Building a Culture of Resilience



- Resilience should not be a "check-the-box" activity
- Resilience needs to be an organizational priority; it can't just be relevant during a disruption or crisis

Measure Confidence in Recoverability



- An effective resilience program provides confidence in an organization's recovery capabilities
- This is achieved not just through effective recovery strategies, but also through testing and exercising

Communication is Critical



- Translate technical concepts in simple business language
- Insights and action items should be clearly defined and communicated



This presentation contains general information only and Deloitte is not, by means of this presentation, rendering accounting, business, financial, investment, legal, tax, or other professional advice or services. This presentation is not a substitute for such professional advice or services, nor should it be used as a basis for any decision or action that may affect your business. Before making any decision or taking any action that may affect your business, you should consult a qualified professional advisor.

Deloitte shall not be responsible for any loss sustained by any person who relies on this presentation.



Professional Services means audit, tax, consulting and financial advisory services.

Copyright © 2019 Deloitte Development LLC. All rights reserved.

36 USC 220506