

# PSCI Webinar: Business Continuity Management (BCM) in Pharma & Healthcare

*Guy Stone*  
*Global BCM Head Roche Diagnostics*

June 17, 2025

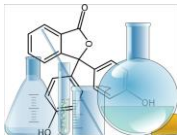
# Speaker



Guy Stone

Global BCM Head  
Roche Diagnostics

.... - 1992



1993-2021	2022-2024	2025-
Sandoz / Novartis	Axpo	Roche
Pharma	Energy	Diagnostics
R&D -> Manufacturing -> Strategy/Risk/ Technical Proj Mgmt.		
Site -> Function -> Division -> Corporate	Division	Division

Science, Strategy, Projects	BCM	BCM & CEM* (Cyber, Pandemic)	BCM
-----------------------------	-----	---------------------------------	-----



\*CEM Crisis & Emergency Management

# AGENDA

## 1.Introduction

## 2.Pharma & Healthcare Perspective

## 3.Resiliency & BCM

## 4.BCM & SCM

## 5.Closing Words and Q&A



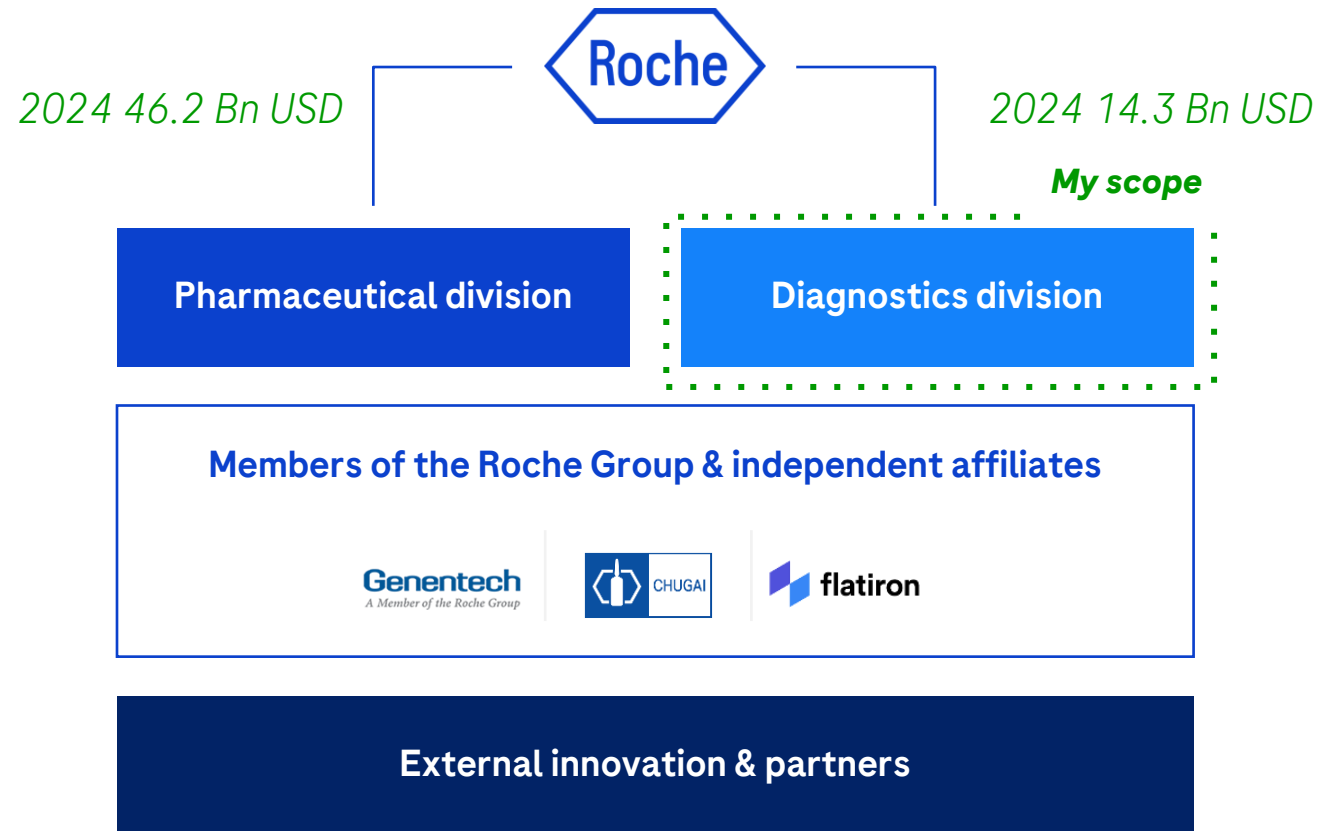
# Introduction to Roche

One of the Top 10 Pharma / Healthcare  
Companies (2024 60.5 Bn USD)

## Our structure and setup

Providing scientific freedom  
to work, think and address  
problems in different ways

Members of the Roche Group & independent affiliates may operate  
under different governance models.



# Introduction to This Webinar

---

## Overview:

In the complex and highly regulated pharmaceutical and healthcare sectors, the ability to anticipate, withstand, respond to, and recover from disruptions is critical. **This webinar will explore the fundamentals and strategic value of Business Continuity Management (BCM), with a particular focus on its alignment with supply chain risk management.**

Attendees will gain insights into **how BCM can be effectively integrated with incident and risk management systems to build resilience across operations. We'll explore best practices for implementing a holistic, coordinated approach** that ensures continuity in the face of global supply chain volatility, regulatory pressures, and emerging threats such as cyberattacks and natural disasters.

## Why PSCI Members and Suppliers Should Attend:

- Learn how to enhance the resilience of your business and supply chain through proactive BCM practices.
- Understand how leading companies in the pharmaceutical sector are aligning business continuity planning with responsible supply chain management.
- Hear practical examples and strategies for minimizing the operational and reputational impacts of disruptions.
- Whether you're a supplier looking to meet client expectations or a PSCI member seeking to build a more secure value chain, this session will offer practical guidance on embedding resilience across your operations.

# Interactive Polling

---

What is the level of BCM knowledge in the Audience today

1. None at all
2. 0-3 years
3. Several Years (>3)
4. I am a BCM Expert & Professional



# What is the level of BCM knowledge in the Audience today?

# AGENDA

1.Introduction

**2.Pharma & Healthcare Perspective**

3.Resiliency & BCM

4.BCM & SCM

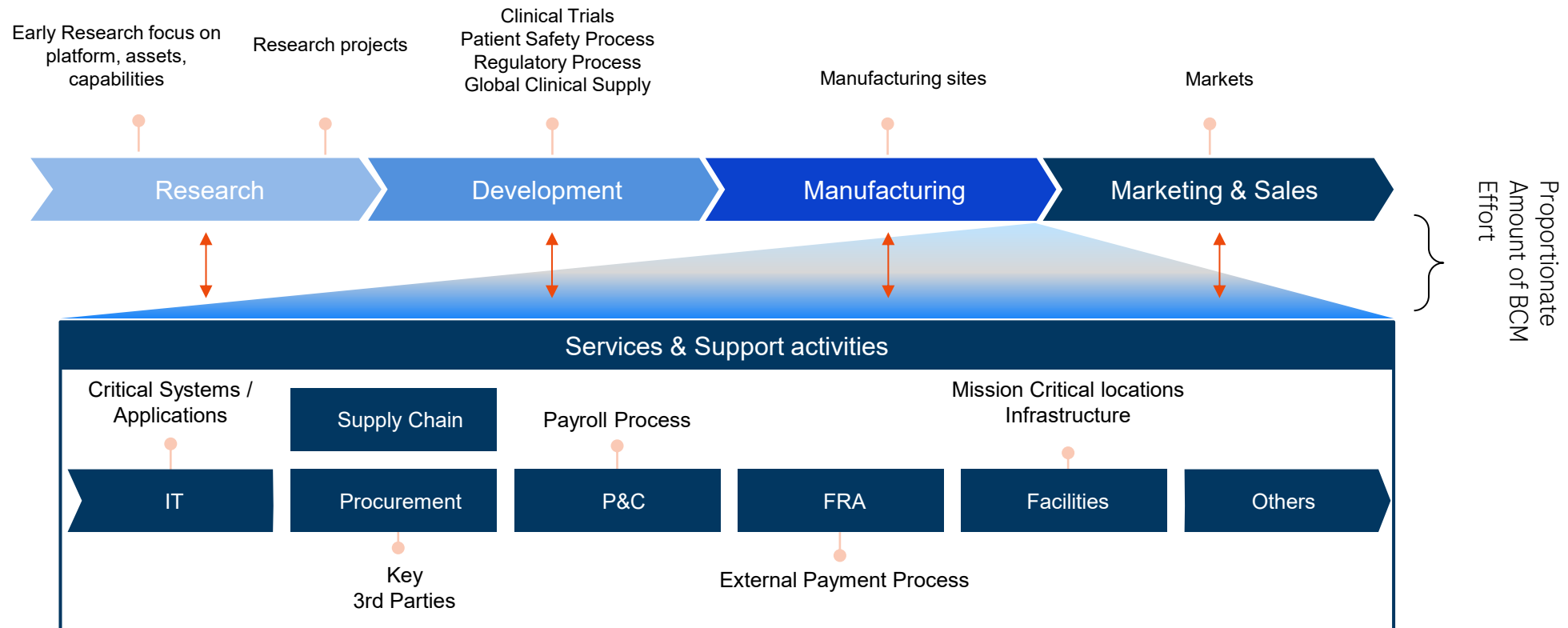
5.Closing Words and Q&A





# Pharma & Healthcare Value Chain

## High Level Business Processes



# Defining the BCM Scope & Priorities

Setting Priorities, to be further refined through the Business Impact Analysis (BIA)

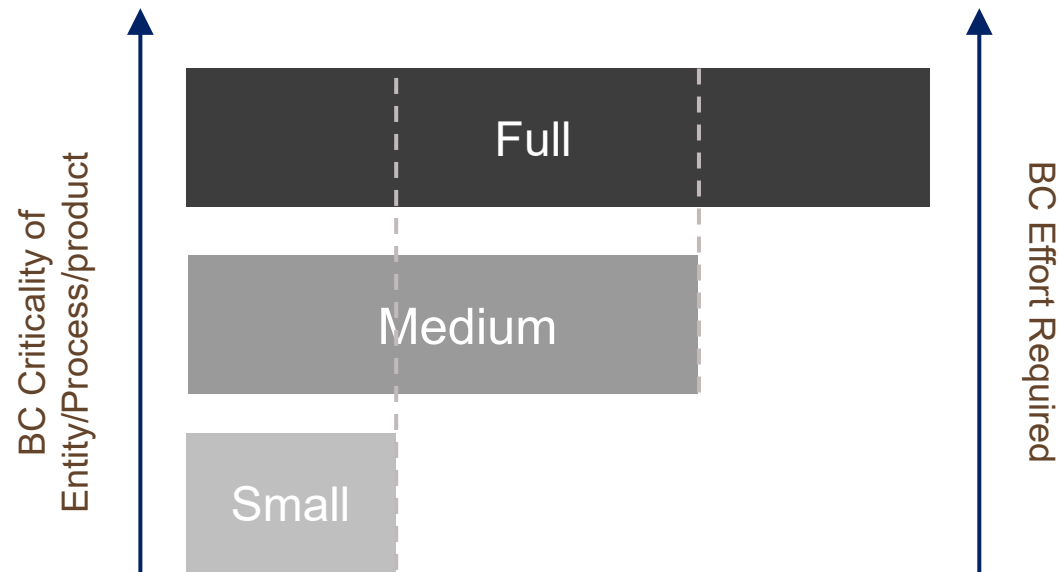
What are the Key Products?				
Medical Importance WHO Essential List	High No alternatives available for any patient	✓	✓	✓
	Med Alternatives available for new patients	✗	✗	✓
	Low Alternatives available for all patients	✗	✗	✓
		Low	Med	High
		Sales & Strategic Importance		
What are the Key Services?				
Finance, Medical Affairs, Compliance/Safety, Communications, Regulatory, Research & Development, Quality, SHE				
Critical Activities		Functions, Systems and Processes that enable the products and services to patients, clinics, regulator		

*Illustrative*



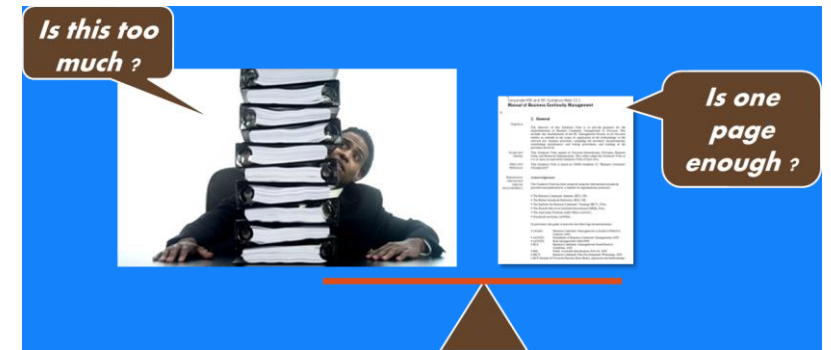
# We Follow a Risk/Impact Based Approach

Also needs to be “Fit For Purpose”



BC Effort and Detail should match BC Criticality

And Balanced



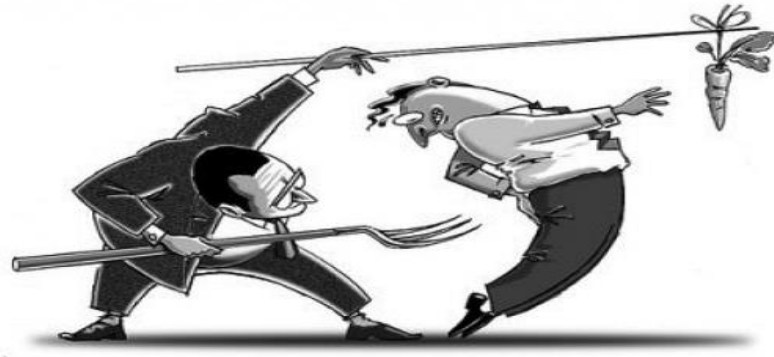
# The Importance of Buy-In

People are motivated by different things

Roche's Mission Statement  
**Doing now what patients need next**

Its the «Right Thing to Do»

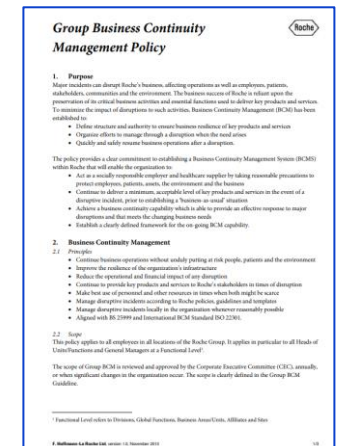
Push  
Audit,  
Compliance



Pull  
Benefits,  
what's in it for me?

Investing in BCM is like **insurance**, risk based, depends on risk appetite

## Roche BCM Policy



# AGENDA

1.Introduction

2.Pharma & Healthcare Perspective

**3.Resiliency & BCM**

4.BCM & SCM

5.Closing Words and Q&A



# Resilience: The 21st Century's Tower of Babel

Poorly and inconsistently defined words ... and when combined, results is even worse



© 2024 Gartner, Inc. and/or its affiliates. All rights reserved. Gartner is a registered trademark of Gartner, Inc. and its affiliates.

# Organizational Resilience Defined

## **Gartner's definition of organizational resilience:**

The ability of an organization to resist, absorb, recover and adapt to business disruption in an ever-changing and increasingly complex environment to enable it to deliver its objectives and rebound and prosper.



**Gartner®**

© 2024 Gartner, Inc. and/or its affiliates. All rights reserved. Gartner is a registered trademark of Gartner, Inc. and its affiliates.

# Interactive Polling

Go to [Slido.com](https://slido.com) and use this room number to interact! #1079531

Is your company / organization also talking about, establishing, “Resilience?”

1. Not Yet
2. In progress, under construction
3. Established







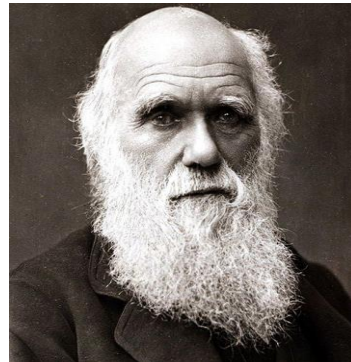
**In your company / organization, BCM and Supply Chain (including procurement) work closely and are aligned?**

# Evolution and Resilience

## Continuous Improvement

*"It is not the strongest of the species that survives, nor the most intelligent, but the one most responsive to change"*

*-Charles Darwin*



*"Evolution favors the survival of the wisest"*

*-Jonas Salk*



# Resilience

What does it mean to you

*Noun*

*1. the capacity to withstand or to recover quickly from difficulties; toughness.*

*"the remarkable resilience of so many institutions"*

*2. the ability of a substance or object to spring back into shape; elasticity.*



# Resiliency

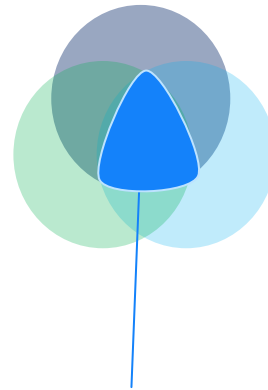
These 3 key elements, when applied correctly can ensure that an organization effectively and efficiently manages risks and incidents while at the same time, evolves and increases its resiliency, and that there is continuous improvement. They are independent processes but interconnected and complimentary

## Enterprise Risk Management (ERM)

*Systematic and consistent framework and process for identifying, assessing and managing key risks (operational, strategic, horizon). Holistic framework integrating other risks Frameworks (i.e. TPRM, SRM, HSE, Quality, etc.)*

*Structured process for determining what is in scope, the «crown jewels», what has to be protected and how, at what point is an interruption unacceptable and how to ensure resumption and recovery beforehand..provides a tested plan and trained team*

## Business Continuity Management (BCM)



## Crisis & Emergency Management (CEM)

*CEM is the process to prepare for and manage emergencies and crises. It is a system that sets out decision-making procedures, internal reporting and defines accountability for situations which cannot be managed by normal business processes.*

*Resiliency*

**Often, there is some confusion, mix up about what is what and where are the boundaries**

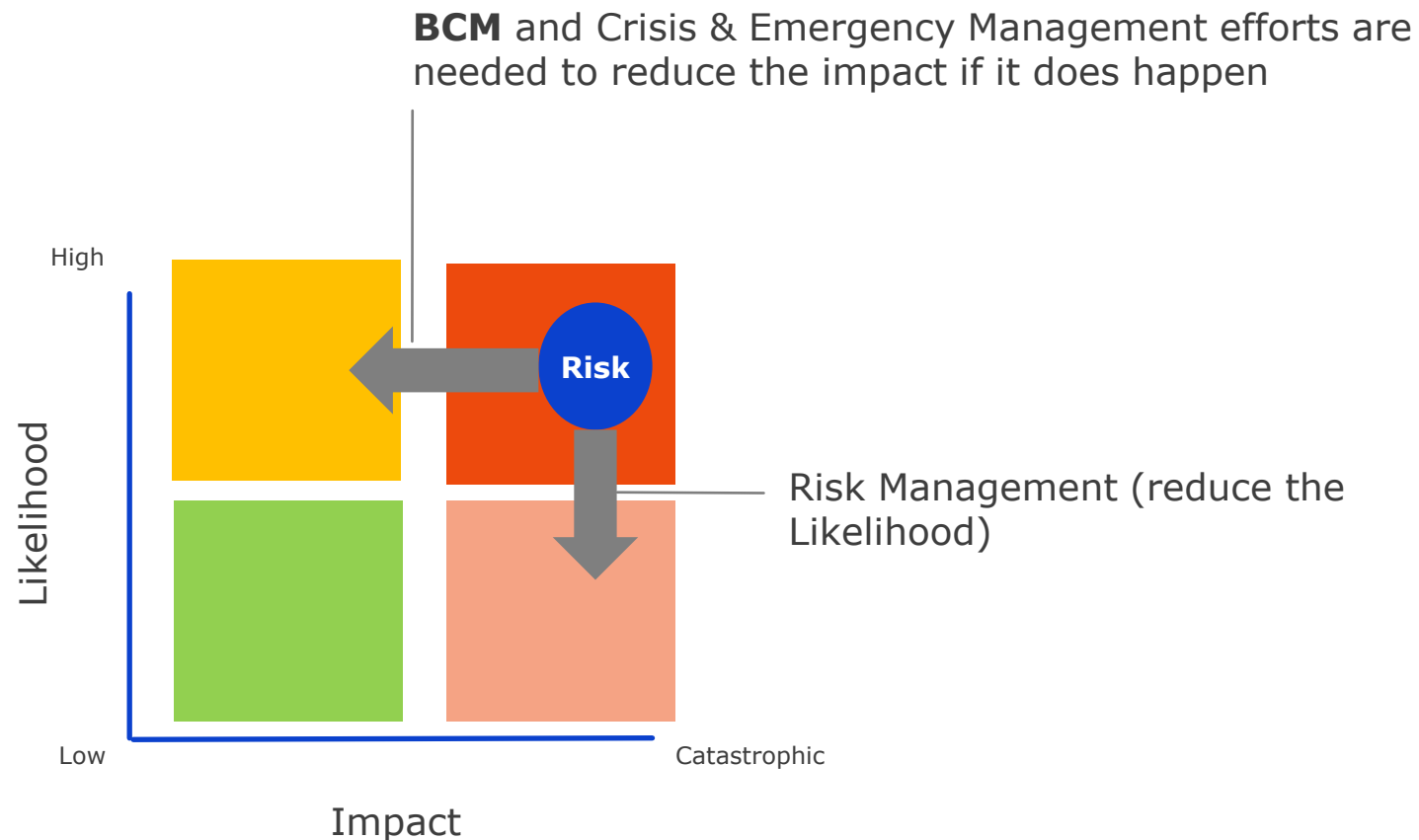
# Primary Goals of ERM, BCM & CEM

## Relationships during Peacetime



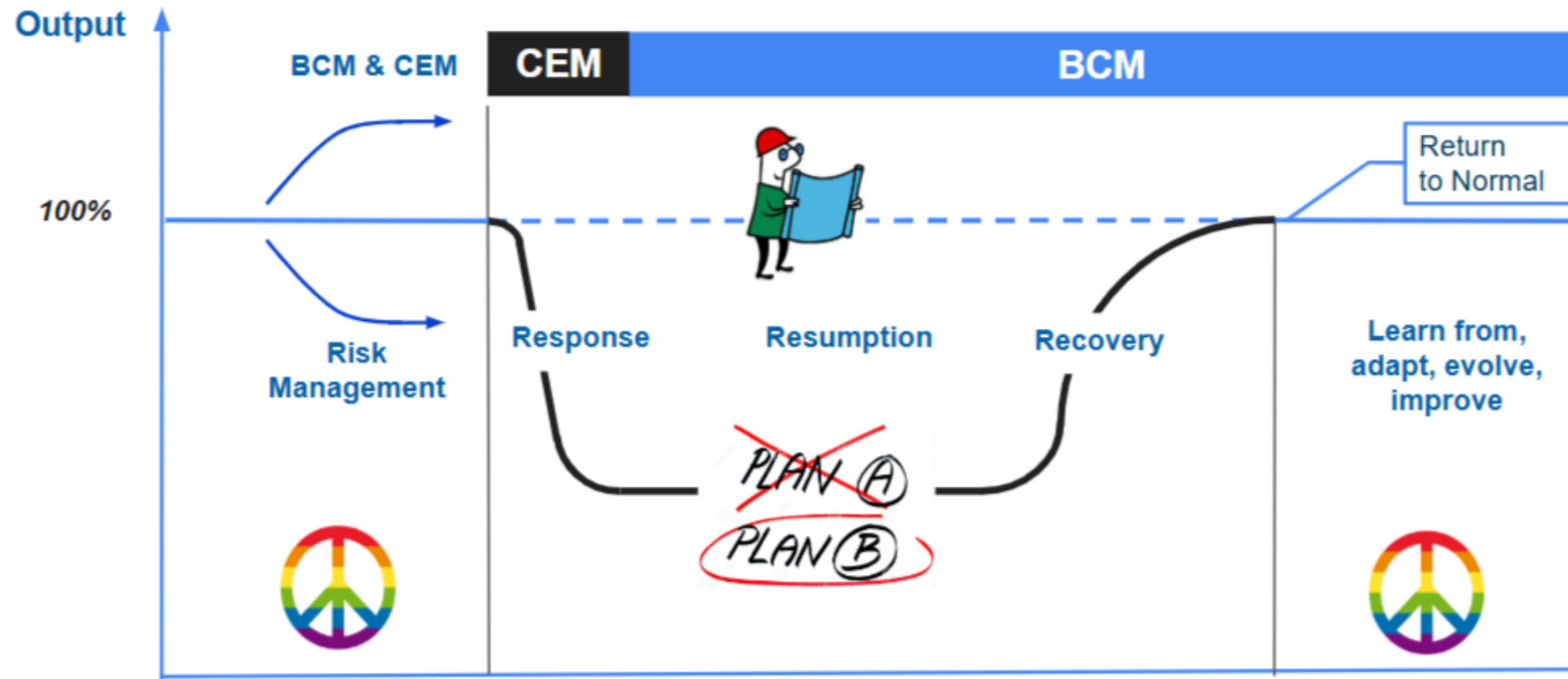
# Risk Management and BCM

Another way of looking at it  
BCM can be considered as a Risk Management Strategy



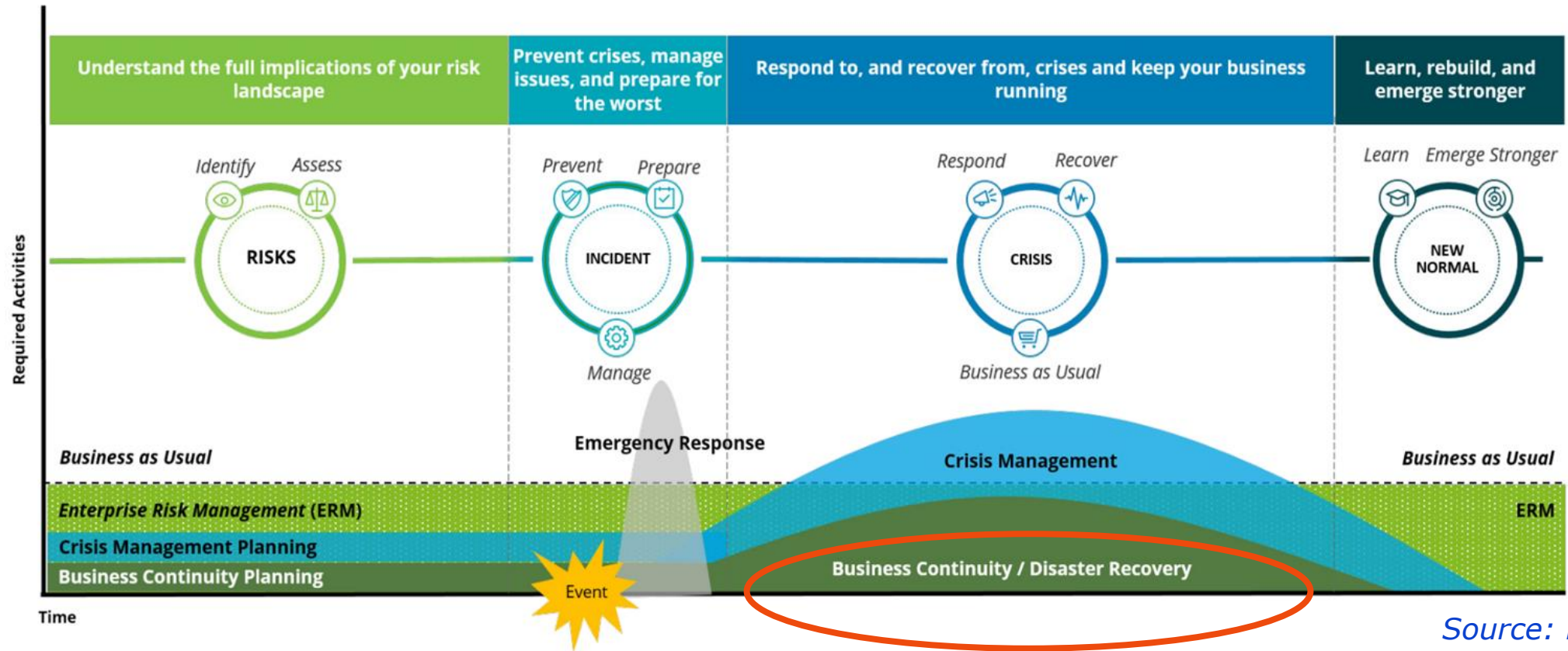
# Crisis & Emergency Management and BCM

## Relationships during Activation



# Big Picture how it all fits together

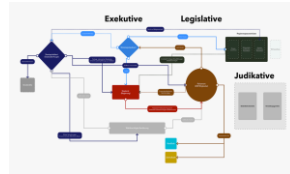
Chronologically: Classical Example of how it goes





# What is Business Continuity Management?

## BIA Business Impact Analysis



### 1. What is Key and Critical

Systematic process and criteria to define, quantify how critical, rank. Map interdependencies (internal, external, IT, etc.), identify single points of failures

*Based on Business Strategy, Objectives, priorities as well as Stakeholder perspectives*



## Risk Identification & Assessment



### 2. What are the risks / incidents could interrupt these things

*Ensure also risk management is applied*

## 5. Continuous Improvement



## BC Strategies & BC Plans



**3. Define, implement strategies** to address these, covered by **Plans** and **Teams** to deal with interruptions

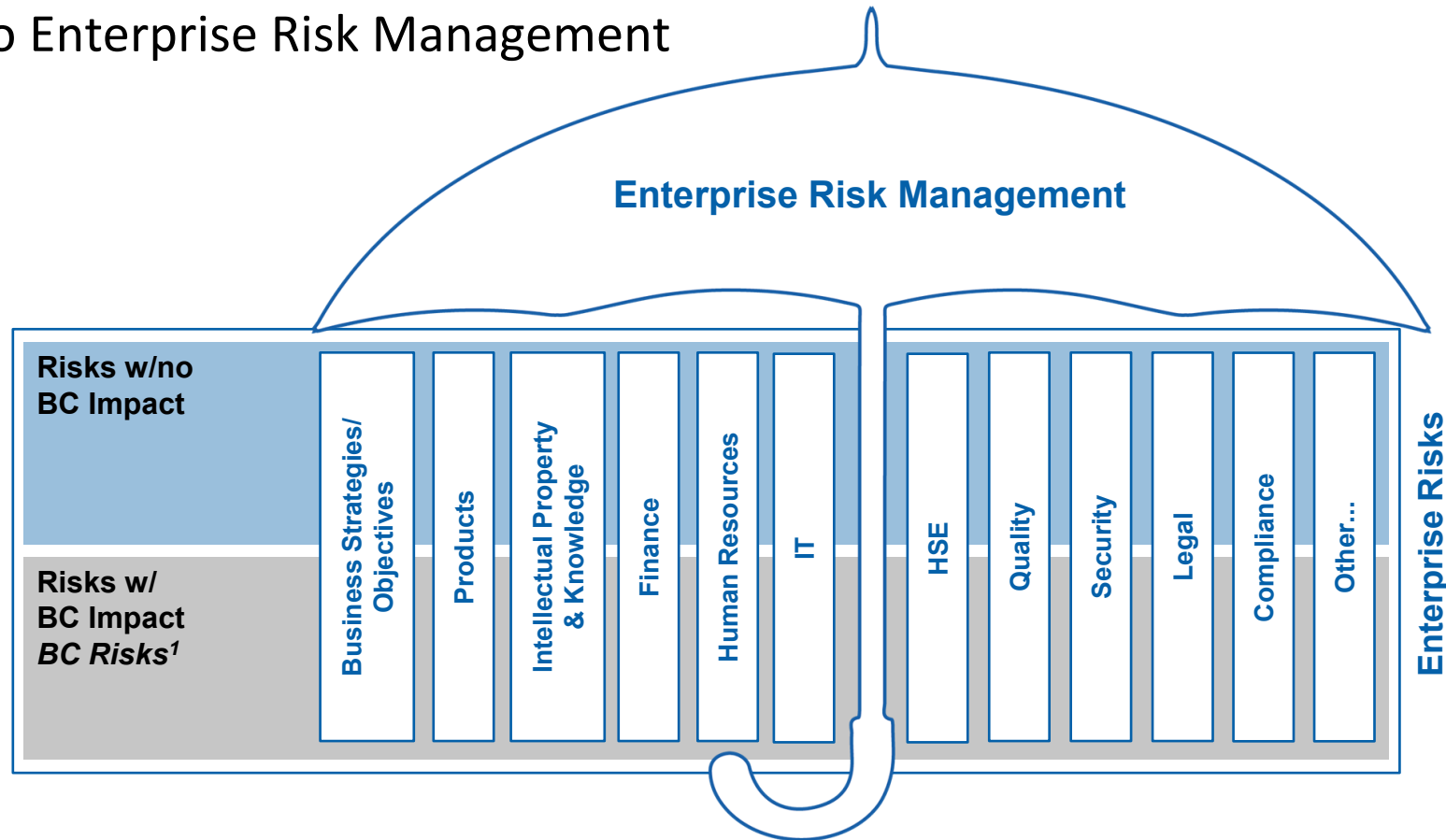
## Test & Exercising



**4. Practice**, stay in shape, ensure up to date and relevant

# What are BC Risks / Incidents?

## Relationship to Enterprise Risk Management



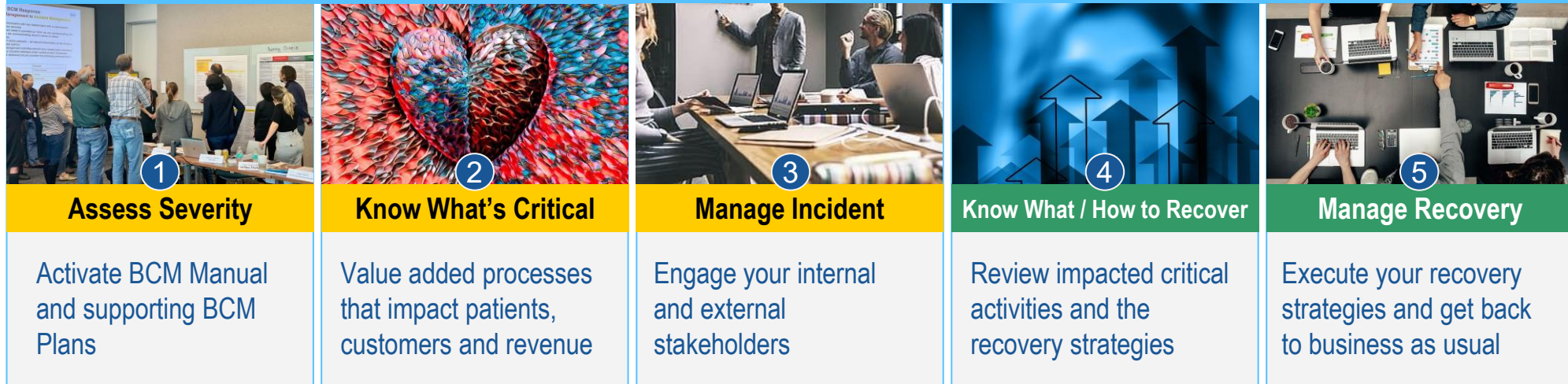
<sup>1</sup>**Internal** and **external** risks which could result in the disruption of the organization's prioritized products and services and supporting key processes, activities and resources. These risks must include those along the entire supply chain as well as those in other areas like: research, development, commercial operations, IT etc.

# Disruptions

Disruptions are becoming more frequent and more severe but less predictable



BCM helps us navigate through disruptions and bounce back quickly



# Interactive Polling

Go to [Slido.com](https://slido.com) and use this room number to interact! #1079531

## What keeps “you” up at Night?

Name your Top 3 Risks that would be BCM relevant (i.e. interruption of a key or critical product or service)

1. ?
2. ?
3. ?





# What keeps 'you' up at Night?



# What do Some Risk Reports Say ?



**Cyber incidents**



**Business interruption**



**Natural catastrophes**



**Changes in legislation and regulation**



**Climate Change**



**Fire, Explosion**



**Macroeconomic developments**



**Market developments**  
market stagnation, market fluctuation)



**Political risks and violence**



**New technologies**

The most important global business risks for 2025

Source: Allianz Risk Barometer 2025

<https://commercial.allianz.com/content/dam/onemarketing/commercial/commercial/reports/Allianz-Risk-Barometer-2025.pdf>

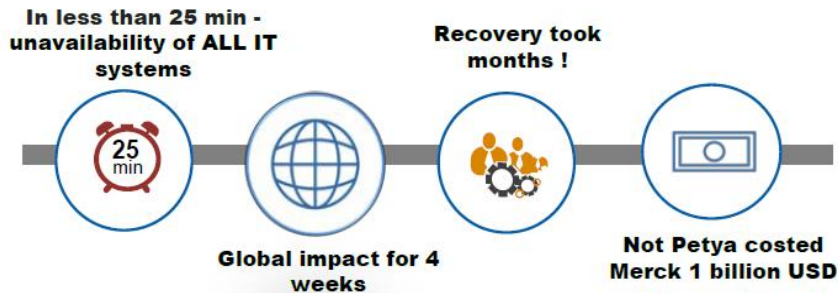
# Cyber Threats (i.e. Ransomware attacks)

Its not a question of “If”, but “When” !

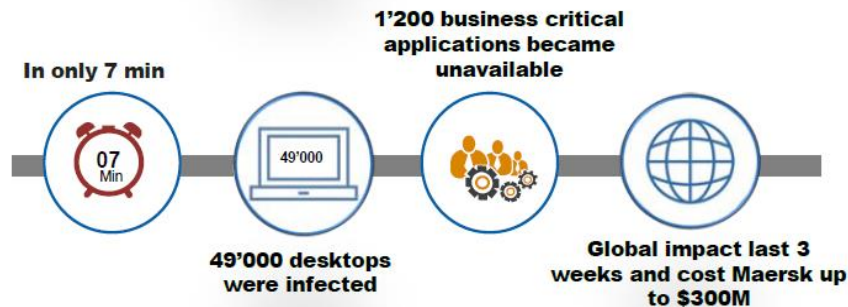
**Cyber threats are real ...  
It is a matter of when not if ...**



Merck & Co. Inc.  
June 2017



MAERSK  
Maersk logistics  
June 2017



JPMORGAN  
CHASE & CO.

altran



acino

ebay

SONY

Marriott

Die Bundesregierung

UBER



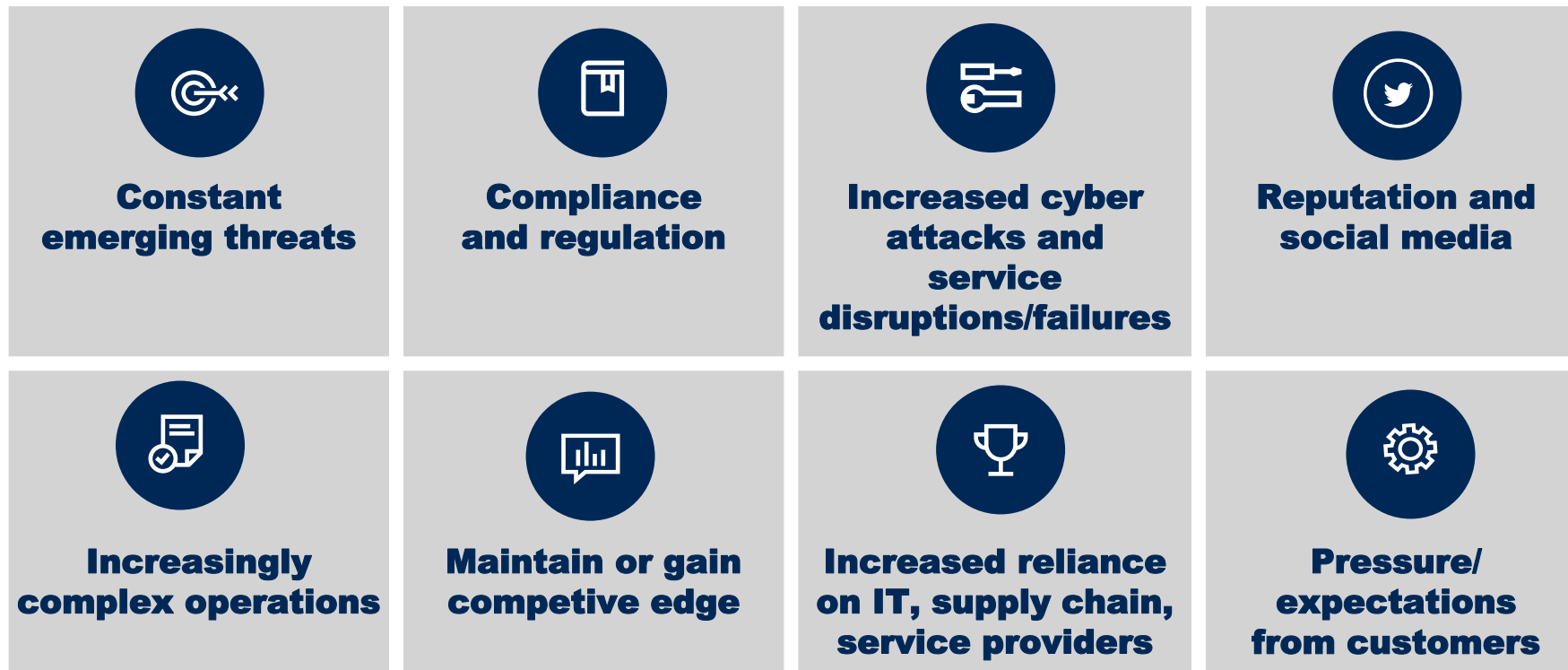
Ministry of Defense  
Government CH

KraussMaffei  
Group

**Are we Safe or  
just Lucky?**

# Back to Resilience

## Why Is Everyone Talking About Resilience?


























































**Gartner**<sup>®</sup>



# Back to Resiliency

## Many Resilience Frameworks

Organizational/operational resilience	Business continuity/disaster recovery	Cybersecurity	Supply chain/third-party risk management	Crisis/emergency management
<p> ISO 22316:2017 - Security and resilience — Organizational resilience — Principles and attributes (2017)</p> <p> Financial Conduct Authority (FCA), Prudential Regulation Authority (PRA), Bank of England (BOE) Operational Resilience</p> <p> Federal Reserve, Office of Comptroller, FDIC Interagency Paper – Strengthening Operational Resilience</p> <p> FFIEC Operational Resilience</p> <p> Digital Operational Resilience Act (DORA)</p> <p> APRA Prudential Standard CPS 230 Operational Risk Management (2023)</p> <p> Office of the Superintendent of Financial Institutions (OSFI): Operational Risk and Resilience (2023)</p> <p> Basel Committee on Banking Supervision (BCBS): Principles of Operational Resilience</p> <p> Central Bank of Ireland (CBI) Cross Industry Guidance on Operational Resilience (2021)</p> <p> Hong Kong Monetary Authority (HKMA) SPM Module OR-2 Operational Resilience (2022)</p> <p> South African Reserve Bank D10-2021 - Directive on Operational Resilience (2021)</p> <p> Vendor frameworks (e.g., Gartner, PwC, Fusion Risk Management, Protiviti, i3 Australia, ServiceNow, ICOR Organizational Resilience Framework, Carnegie Mellon CERT Resilience Management Model (CERT-RMM))</p>	<p> ISO 22301:2019 – Business continuity management systems – Reqs</p> <p> ISO 22317 - Societal security — Business continuity management systems — Guidelines for business impact analysis (BIA)</p> <p> ISO 22313 - Security and resilience — business continuity management systems — Guidance on the use of ISO 22301</p> <p> ISO 22330 - Security and resilience — Business continuity management systems — Guidelines for people aspects of business continuity</p> <p> ISO 27031:2011 Information technology – Guidelines for info &amp; communication technology (ITC) readiness for business continuity</p> <p> FFIEC Business Continuity Management Handbook</p> <p> NIST SP 800-34 – Contingency Planning Guide for Federal Information Systems</p> <p> Appendix D: Mandatory Procedures for Business Continuity Management Control (Directive on Security Management)</p> <p> NFPA 1600 Standard on Continuity, Emergency, and Crisis Management</p> <p> UAE NCEMA7000 Business Continuity Management Standard</p> <p> (FS) Saudi Arabian Monetary Authority (SAMA) Business Continuity Management Framework</p> <p> Hong Kong Monetary Authority (HKMA) TM-G-2 Business Continuity Planning (2022)</p> <p> BCI: Good Practices Guidelines – Business Continuity</p> <p> DRII: Business Continuity Management Professional Practices</p>	<p> NIST SP 800-160 – Developing Cyber Resilient Systems</p> <p> NIST Cybersecurity Framework (CSF)</p> <p> U.S. Cybersecurity Maturity Model CMMC</p> <p> SEC Rules on Cybersecurity Risk Mgmt, Strategy, Gov &amp; Incident Disclosure by Public Companies</p> <p> FFIEC: Cybersecurity Resource Guide for Financial Institutions (cyber resilience)</p> <p> Office of the Superintendent of Financial Institutions: OFSI B-13 Guideline on Technology and Cyber Risk Management</p> <p> (FS) Monetary Authority of Singapore (MAS) Notice 655 Cyber Hygiene</p> <p> Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCA)</p> <p> Cyber Resilience Act (CRA)</p> <p> European Banking Authority (EBA) Guidelines on ICT and SRM</p> <p> European Union NIS2 Directive</p> <p> European Banking Authority (EBA): Cyber Resilience Oversight Expectations for Financial Market Infrastructure (FS)</p> <p> European Banking Authority (EBA): TIBER-EU Testing Framework (FS)</p> <p> Financial Stability Board (FSB): Effective Practices for Cyber Incident Response and Recovery (FS)</p> <p> Federal Financial Supervisory Authority BaFin BAIT Supervisory Reqs for IT Security in Financial Institutions (2021)</p>	<p> ISO 22318 – Societal security — Business continuity management systems — Guidelines for supply chain continuity</p> <p> (FS) PRA: Outsourcing and Third-Party Risk Management</p> <p> Office of the Superintendent of Financial Institutions (OSFI) Guideline B-10 Third Party Risk Management</p> <p> European Banking Authority (EBA): Guidelines on ICT and Security Risk Management (FS)</p> <p> European Banking Authority (EBA): Guidelines on Outsourcing Arrangements (FS)</p> <p> Monetary Authority of Singapore: Guidelines on Outsourcing</p> <p> Hong Kong Insurance Authority (HKIA) Guidelines on Outsourcing</p> <p> U.S. Department of Health &amp; Human Services: Essential Medicines Supply Chain and Manufacturing Resilience</p> <p> Organization for Economic Co-operation and Development (OECD) Framework for Supply Chain Resilience</p> <p> Interagency Report 7622, National Supply Chain Risk Management Practices for Federal Information Systems</p>	<p> U.S. FEMA NIMS/ICS</p> <p> ISO 22320:2018 - Security and resilience - Emergency management - Guidelines for incident management</p> <p> ISO 22396:2018 – Security and resilience – Community resilience – Guidelines for supporting vulnerable persons in an emergency</p> <p> ISO 22361:2022 - Security and resilience — Crisis management — Guidelines to help any organization identify and manage a crisis</p> <p> UAE National Emergency and Crisis Management Framework</p>

**Gartner®**

# Operational Resilience Ecosystem



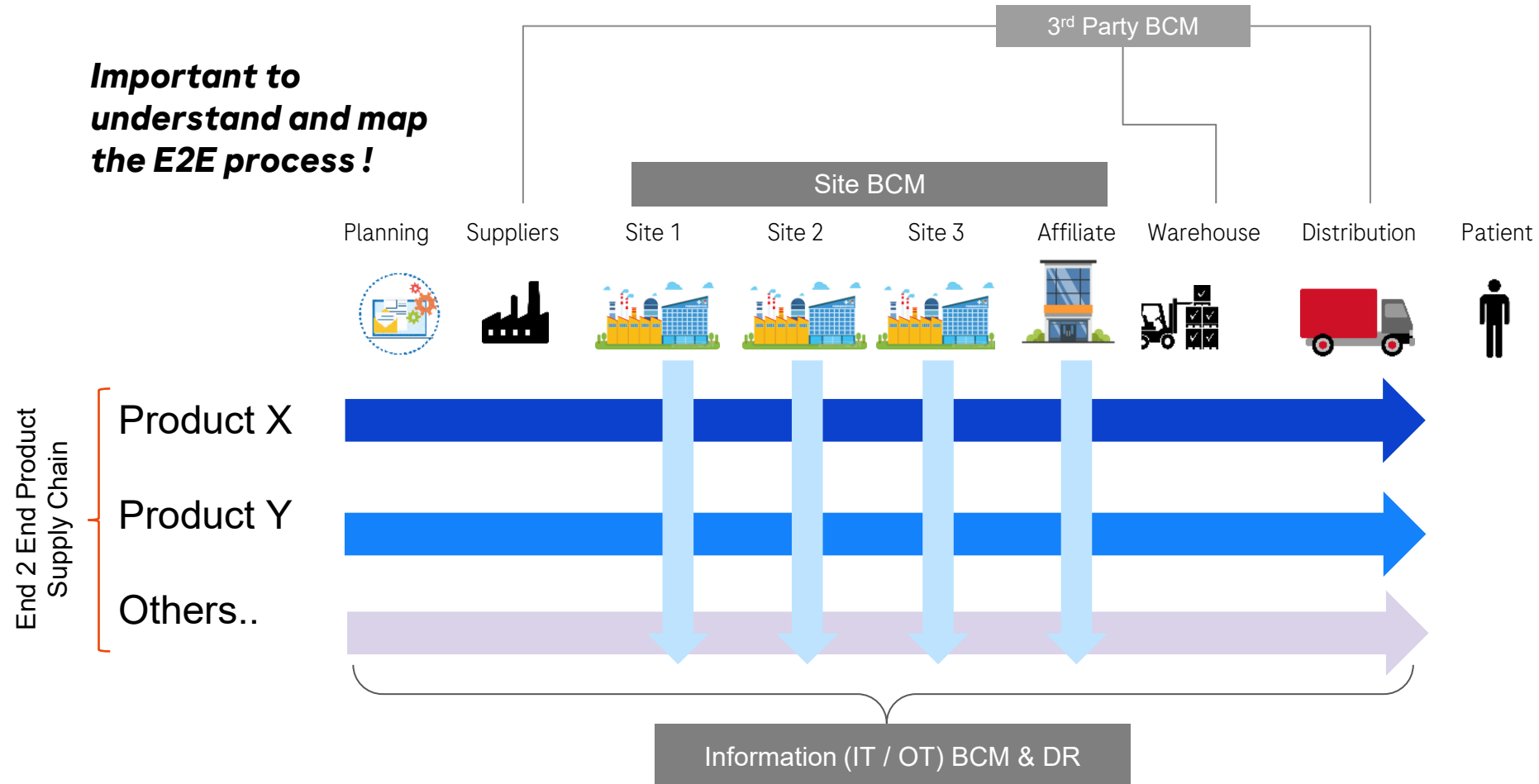
# AGENDA

- 1.Introduction
- 2.Pharma & Healthcare Perspective
- 3.Resiliency & BCM
- 4.BCM & SCM (and SRM\*)**
- 5.Closing Words and Q&A

\*Supply (Chain) Risk Management

# Supply Chain Risk Management vs. BCM

## E2E vs. Silo



# Follow a Holistic Approach

Another way of looking at it



An integrated supply and operations risk management approach, based on 3 core elements

- **Supply Risk Management: Additional E2E view and protection of especially critical products for the patients and future of the company**
- **BCM: Identifies Key Products & Services and risks and defines strategies to respond in case of disruption**
- **Operational Excellence & Risk Management: Stabilize manufacturing processes and ensure required service levels**

Each risk management level builds on the previous, further enhancing the assessment

# Interactive Polling

Go to [Slido.com](https://slido.com) and use this room number to interact! #1079531

In your company / organization, BCM and Supply Chain (including procurement) work closely and are aligned?

1. No, they do not even know each other
2. Some ad-hoc connection
3. Conceptually yes, they should, but reality is different
4. They work very closely together, and the result is an aligned, E2E view and management of the supply chain and risks...



# AGENDA

1.Introduction

2.Pharma & Healthcare Perspective

3.Resiliency & BCM

4.BCM & SCM

**5.Closing Words and Q&A**



# Some Key Take Home Messages

- ★ Follow a **Holistic Approach** (not silos) -> **Resilience** is the bigger picture and goal
- ★ Have the **Right people** doing it (those who get it, want it) with enough resources
- ★ **Don't do it for compliance** or “tick the box” (embed, embrace, integrate) -> find value, do it for the right reasons, North Star !
- ★ It needs to be **Business Owned**, managed and driven (we support)
- ★ **Risk/Impact based** and **Fit for purpose**
- ★ Documents are important but so is **capability of people and teams**
- ★ **Supply Chain**, including 3rd parties, has a special relationship with and in the context of BCM, even if some “grey zones”, align and approach it holistically and synergistically





# Q&A

---



# Contact us

Get in touch to learn more  
about what we do:

[www.pscinitiative.org](http://www.pscinitiative.org)



[info@pscinitiative.org](mailto:info@pscinitiative.org)



+44 (0) 7587 076 059

