Mettersi insieme è un inizio,
Rimanere insieme è un progresso,
LAVORARE INSIEME E' UN SUCCESSO.

La Gestione dei Rischi nelle PMI

Webinar ODCEC - ANRA - 13 Aprile 2023

Risk Management - Rischi Operativi

Agenda

Prima parte (Dott. Gianluigi Lucietto)

- La gestione dei rischi operativi nelle Aziende
- Minacce e Vulnerabilità Aziendali
- Come possiamo proteggere le Organizzazioni dai rischi
- La ISO 31000:2018

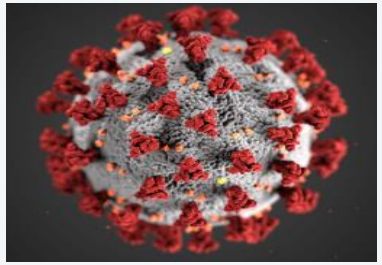
Seconda Parte (Ing. Marco Terzago)

- L'interruzione dell'operatività: come essere preparati
- Business Continuity Management
- Concetti generali ISO22301:2019
- Business Impact Analysis
- Piani di Continuità Operativa

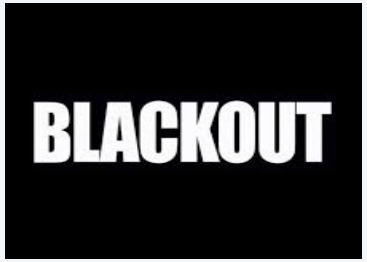
La Gestione dei Rischi - Le Minacce

I rischi assumono molte forme, tante quante le conseguenze che possono colpire ogni organizzazione

Cyber Attack



Emergenze Sanitarie



Blackout/Energia

Extreme Weather

Incertezze politiche & economiche

Scenario Legislativo

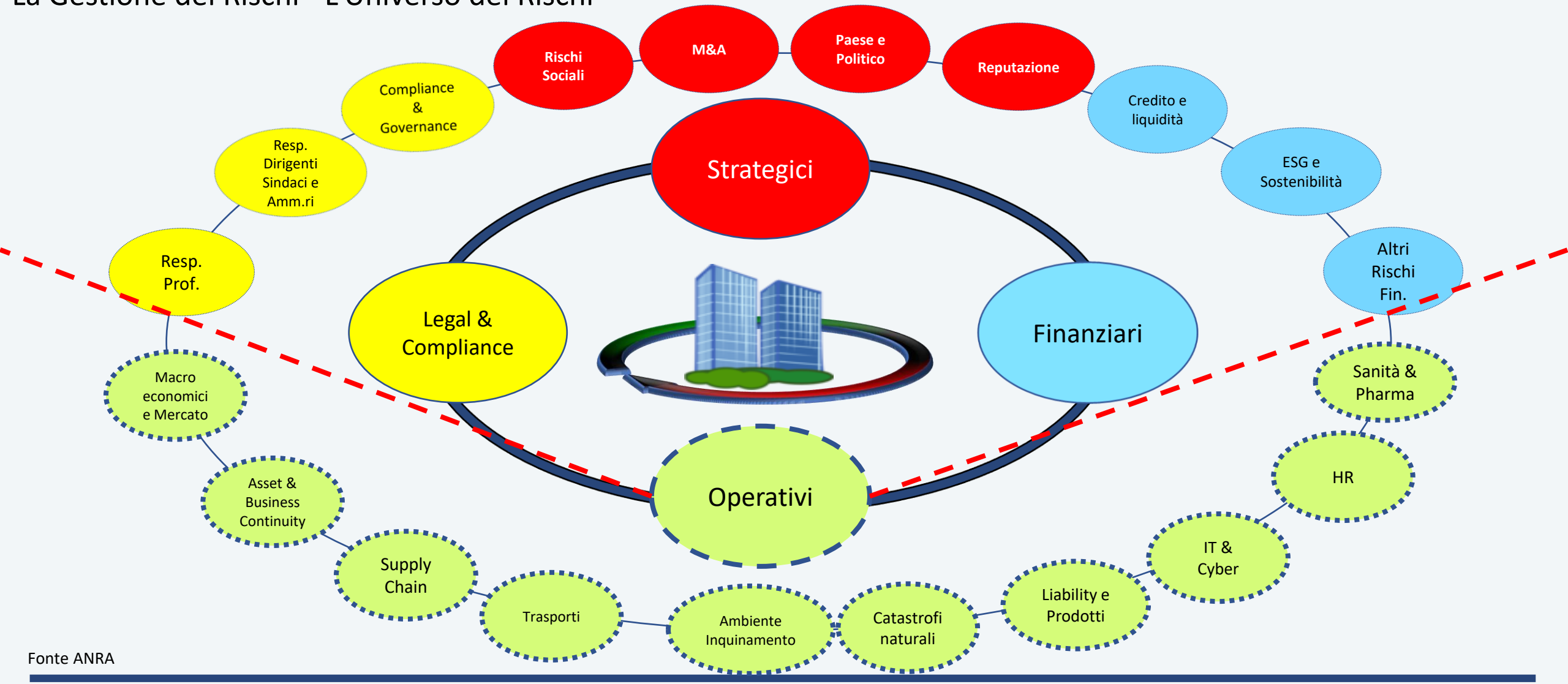
Skill Shortage Re-Skilling

Inquinamento

Supply Chain Disruption

Indisponibilità Servizi Infrastrutturali

La Gestione dei Rischi - L'Universo dei Rischi



Fonte ANRA

La Gestione dei Rischi

Cigno Nero: *evento raro, di grandissimo impatto (Nassim N. Taleb)*

Rinoceronte Grigio: evento estremamente probabile, con un effetto straordinario, il cui potenziale di rischio viene comunque sottovalutato (Michele Wucker)

Un esempio di interruzione

Kentucky Fried Chicken è un colosso da oltre 3,5 miliardi di dollari di fatturato con 21mila ristoranti in 130 Paesi nel mondo. Ma lo scorso febbraio (2018) le alette di pollo dorate e piccanti che il colonnello Harland Sanders, partendo da una stazione di servizio a Corbin (nel Kentucky, appunto) è riuscito a guidare alla conquista il mondo, sono letteralmente scomparse, all'improvviso, dal mercato britannico. Per tagliare i costi è stato commesso quello che sarà probabilmente ricordato come l'errore peggiore della storia di Kfc: ovvero il passaggio di mano della distribuzione nel Regno Unito da Bidvest Group – specializzato in spedizioni alimentari – a Dhl Group, un gigante della logistica che in teoria avrebbe avuto tutte le carte in regola per lavorare bene.

Le perdite registrate: Kfc è stato costretto a chiudere 750 punti vendita, ovvero l'80% di tutti quelli del Regno Unito, perché "non c'era più pollo da friggere". In tutti ristoranti campeggiavano avvisi di scuse, ma ovviamente, non è bastato: è stata necessaria una massiccia campagna mediatica e tre mesi di lavoro per recuperare il terreno perso in termini di reputazione, per Kfc e anche per Dhl. Non solo, secondo le stime, l'impatto dei costi sostenuti per riparare il danno ha inciso per il 2% sulle vendite e del 5% sul profitto operativo nel primo trimestre. Un'interruzione operativa di poche ore complessivamente e in una regione da cui dipende solo il 3% del fatturato consolidato si è tramutata in una perdita annuale dello 0,5% sulle vendite.

La Gestione dei Rischi Operativi

2 Modus Operandi

1 Silos

2 ERM

Rischi Puri

sono rischi il cui accadimento porta ad una perdita certa causata da evento accidentale

(es. incendio, terremoto, alluvione, morte o infortunio dipendenti…)

Rischi Operativi

sono rischi derivanti dalle attività/operazioni

(frode, perdita di fornitore strategico, intervento di autorità, …)

Rischi Finanziari

sono rischi derivanti alla gestione finanziaria

(incremento costi, tassi di interesse, perdite su crediti, …)

Rischi Normativi/Strategici

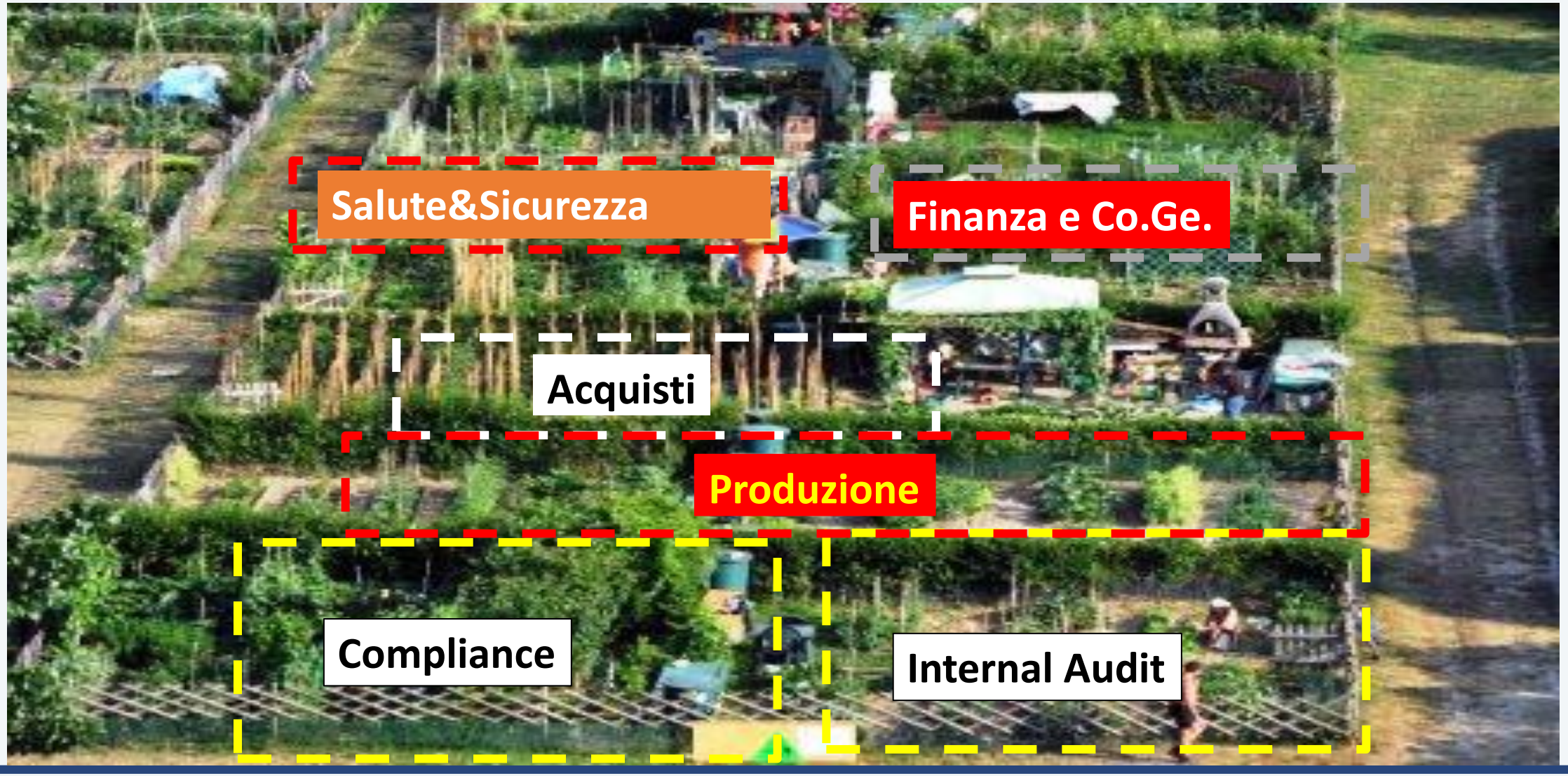
rischi legati a imposizioni normative o decisioni di lungo periodo

(accordi commerciali, modifiche legislative, M&A, …)

Rischi Emergenti

rischio derivante da un pericolo di nuova individuazione al quale può aversi un'esposizione importante o derivante da un'inaspettata, nuova o maggiore esposizione e/o suscettibilità a un rischio noto

Approccio Silos vs ERM



Approccio Silos vs ERM

Come possiamo fare?
La ISO 31000

Introduzione ISO 31000

Lo standard si rivolge a coloro che intendono ***PROTEGGERE il VALORE*** nelle organizzazioni per:

- gestire rischi
- prendere decisioni
- fissare e conseguire obiettivi
- migliorare le prestazioni

Le organizzazioni, nel gestire il rischio, devono:

- considerare fattori interni ed esterni
- stabilire le strategie e prendere decisioni consapevoli
- monitorare come viene gestito nella governance e nella leadership
- considerare tutte le attività insite nell'organizzazione
- considerare l'interazione con le parti interessate
- considerare il comportamento umano e i fattori culturali

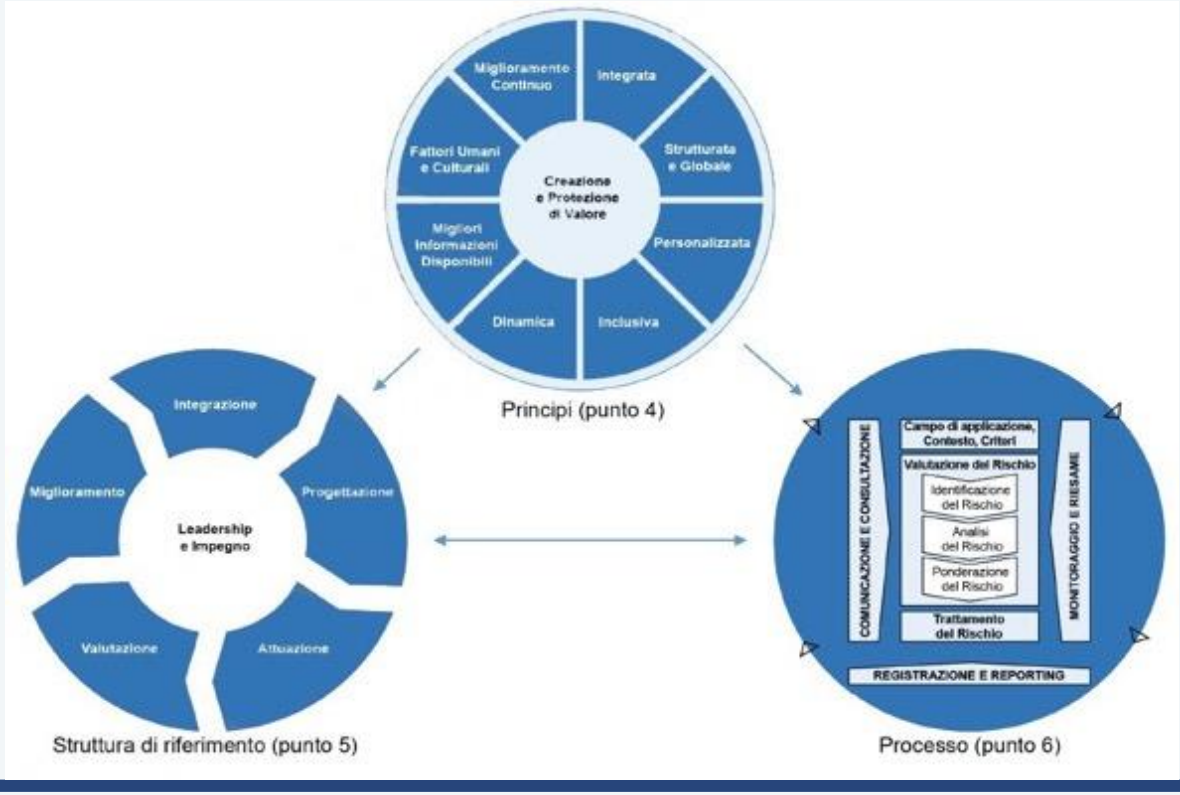
SCOPO E CAMPO DI APPLICAZIONE

La norma può essere applicata a qualsiasi tipo di rischio e fornisce le linee guida per la gestione del rischio che si presentano alle organizzazioni

Può essere applicata, per gestire il rischio, a qualsiasi tipo di azienda o industria

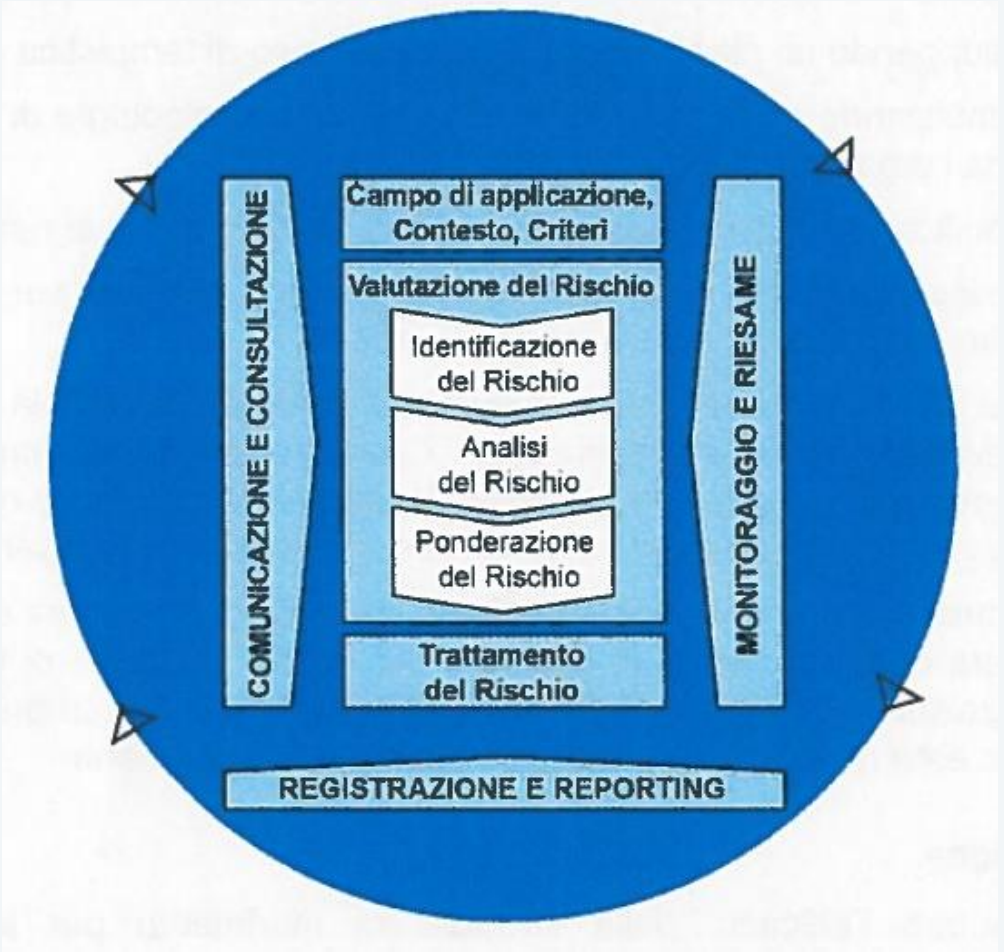
Tale modello decisionale può essere mantenuto durante tutta la vita dell'organizzazione e può essere applicato a tutti i livelli decisionali

Principi - Struttura - Processo



Fonte ISO 31000:2018

Il Processo di Risk Management



Non è sufficiente essere conformi alle leggi?

Tsunomic effect

È l'effetto di una devastante forza d'urto economica di cui difficilmente si riesce a calcolare la durata nel tempo, l'ampiezza dell'impatto e la profondità con cui uno o più settori, una o più economie sono colpite.

(G. Lucietto/G. Mastromattei)

Due approcci differenti CM vs RM

Approccio Tattico vs. Strategico

Il **rispetto delle regole e dei regolamenti prescritti**, nonché di leggi e norme, impone all'organizzazione di valutare e monitorare attentamente gli aspetti di *Compliance*, in quanto, **se non rispettati**, possono comportare **multe, sanzioni** di elevato importo, condanne penali, fermi operativi e danni alla reputazione.

Il *Risk Management* comporta, invece, le **attività di analisi** (i.e.: identificazione, misurazione e ponderazione), di trattamento, di monitoraggio, di rendicontazione, di registrazione e di revisione dei rischi **in base agli obiettivi strategici dell'organizzazione**.

Approccio Prescrittivo vs. Predittivo

La natura **prescrittiva** della *Compliance* e la natura **predittiva** del *Risk Management* spiega, in parte, perché la prima è più tattica e il secondo è più strategico.

La *Compliance* impone alle organizzazioni il **rispetto delle regole**, dei regolamenti, delle leggi, delle normative e degli standard vigenti.

Il *Risk Management*, invece, deve essere in grado di **identificare e valutare l'impatto** che i rischi avranno sull'organizzazione stimolando, altresì, processi di gestione alternativi e innovativi in grado di ridurre al minimo i rischi o sfruttarne gli aspetti positivi (opportunità).

Due approcci differenti CM vs RM

Avversione al rischio vs. creazione di valore

La *Compliance* si avvale del *Risk Management* per generare valore; ovvero, la *Compliance* data la sua natura prescrittiva e di controllo, raramente si traduce in proposte aziendali generatrici di valore a lungo termine, limitandosi alla **verifica dell'osservanza delle regole per evitare i rischi**.

Il *Risk Management*, invece, è propedeutico a **convertire le restrizioni** associate alla conformità **in un valore aggiunto** per l'organizzazione.

Approccio Silos vs Integrato

La ***Compliance*** si basa spesso su un approccio **"a *silos*"** (mono-direzionale) che, di fatto, non impatta sul processo di *Compliance*; al contrario**, i programmi integrati** di *Risk Management* (ERM) risultano più efficaci se non operano "per *silos*" e se **si basano sulla trasparenza**. Ovvero, **l'integrazione di aree**, funzioni, sistemi tecnologici e processi è necessaria per individuare i rischi all'interno e all'esterno di un'organizzazione e il modo in cui devono essere gestiti sia che si tratti di evitare le loro implicazioni sia di promuoverne il valore.

La gestione dei rischi è come il sistema frenante di una macchina, non solo offre al pilota un mezzo per frenare la macchina, ma anche offre al pilota la consapevolezza di poter andare più forte (m.s.)

… sempreché non si decida di mettere il sistema frenante di una Panda ad una Ferrari…

Occorre essere «Adaptive»

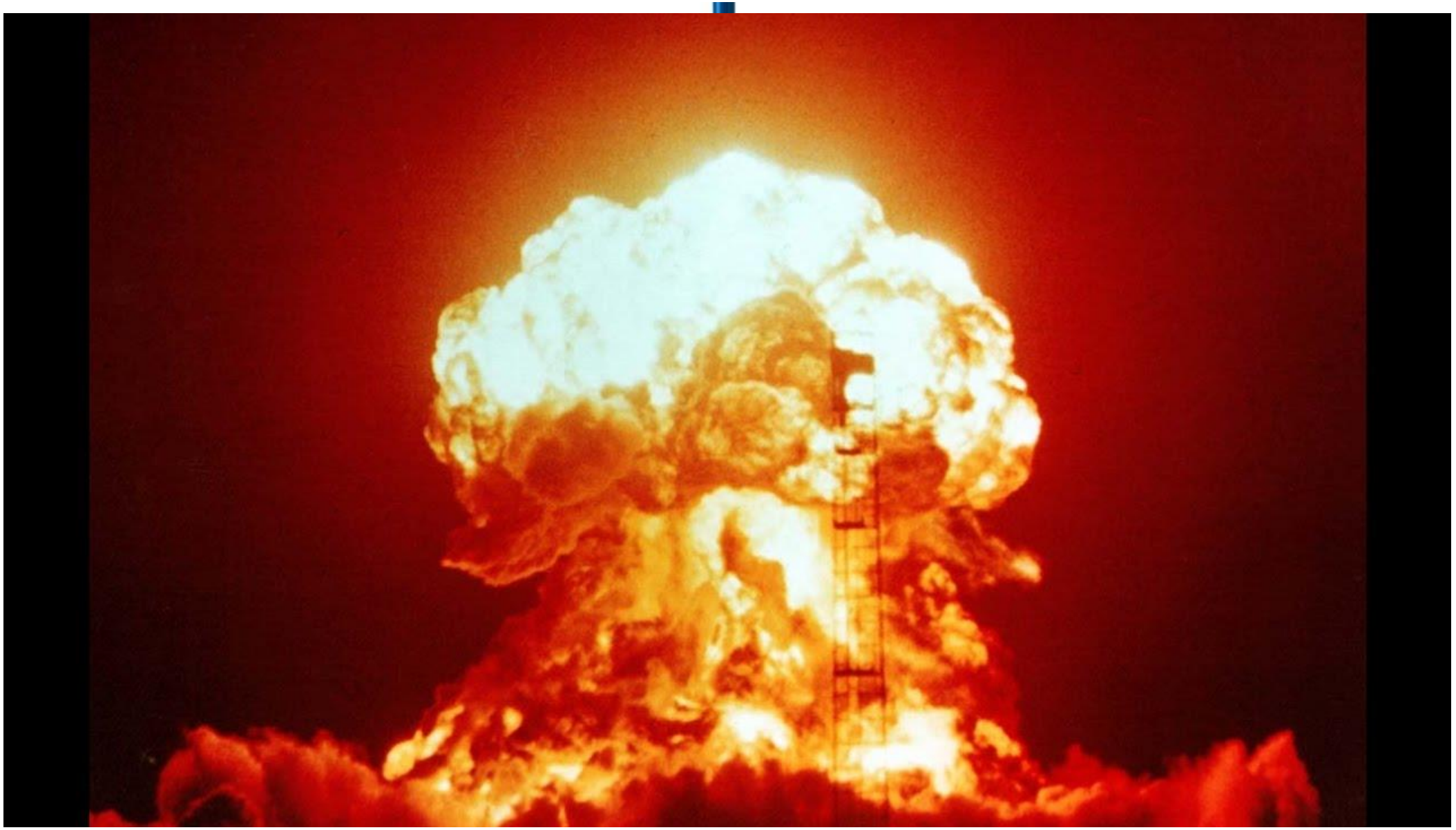
… e per essere adaptive RM&CM devono collaborare per

- Analizzare gli stati in cui si trova il/i sistema/i economico/i con il/i quale/i operiamo o da cui potremmo dipendere, «trailblazer analysis»
- Analisi dei rischi e valutazione delle esposizioni ai rischi della nostra organizzazione costante «pass through analysis» sui drivers esterni/interni
- Valutazione dei potenziali impatti sull'azienda
- Identificazione di soluzioni adattive
- Valutazione sull'applicabilità delle tecniche di gestione identificate
- Selezione delle tecniche di gestione più appropriate
- Implementazione delle tecniche selezionate
- Monitoraggio continuo dell'evoluzione dei rischi e adattamento continuo

Perché dobbiamo fare tutto questo se abbiamo un sistema organizzato?

?

TUTTO DA UNA SEMPLICE GOCCIA



COME POSSIAMO EVITARE IL DISORDINE/IL CHAOS

Analizziamo il termine CHAOS

Bob Schoultz during his 30-year career as a Navy SEAL

Disorganized

C. Constant
H. Headaches
A. And
O. Ongoing
S. Surprises

Organized

C. Constantly
H. Havings
A. An
O. Organizing
S. System

Moto Browniano
È il moto incessante e disordinato di piccolissime particelle sospese in acqua o gas

Quanto il CHAOS irrompe…

…attivazione piano

Verificare l'accaduto/attacco

Mettere in sicurezza Sistema, Struttura/Infrastruttura

Neutralizzare l'evento

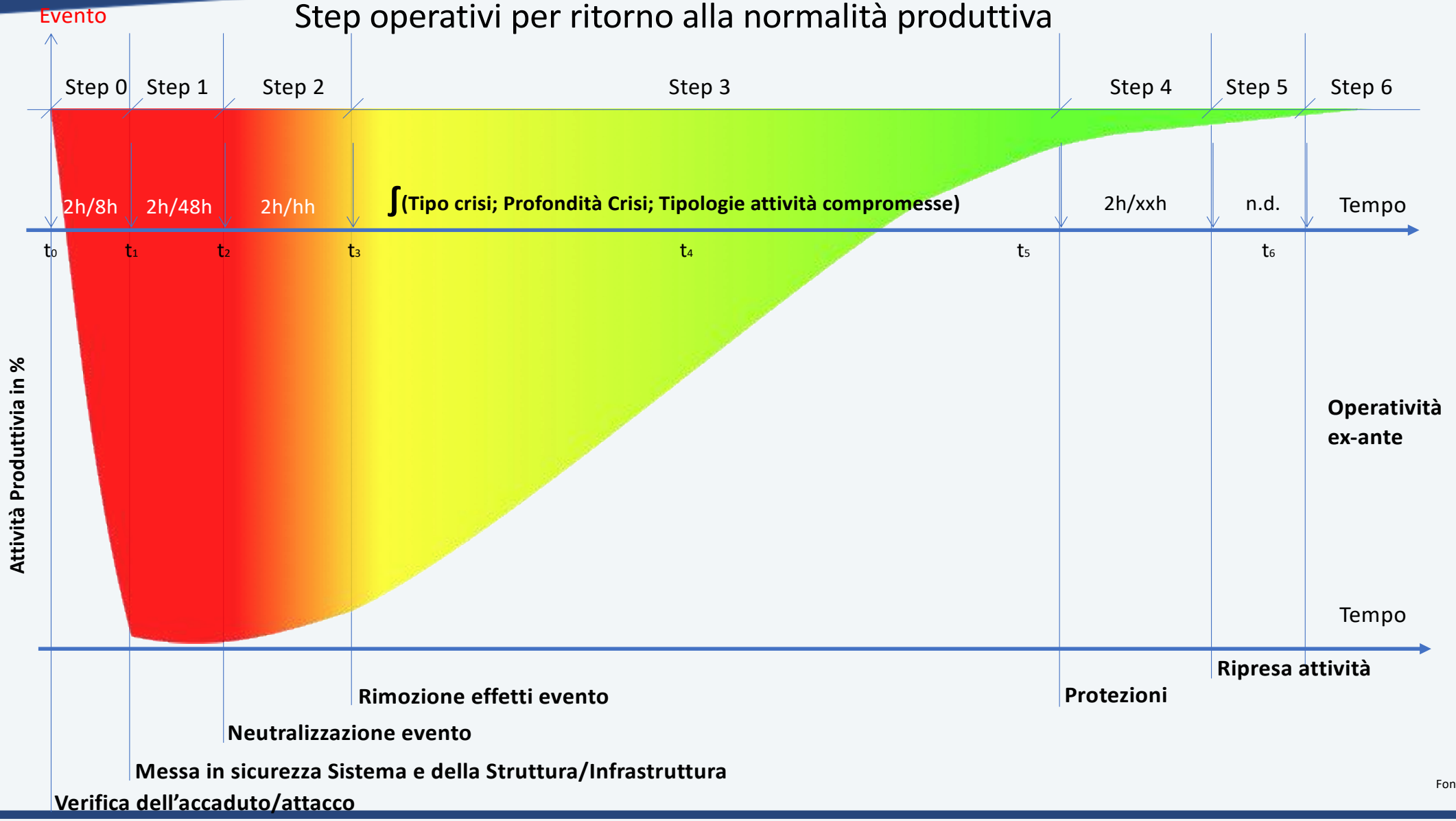
Rimuovere effetti evento

Proteggere

Ripartire

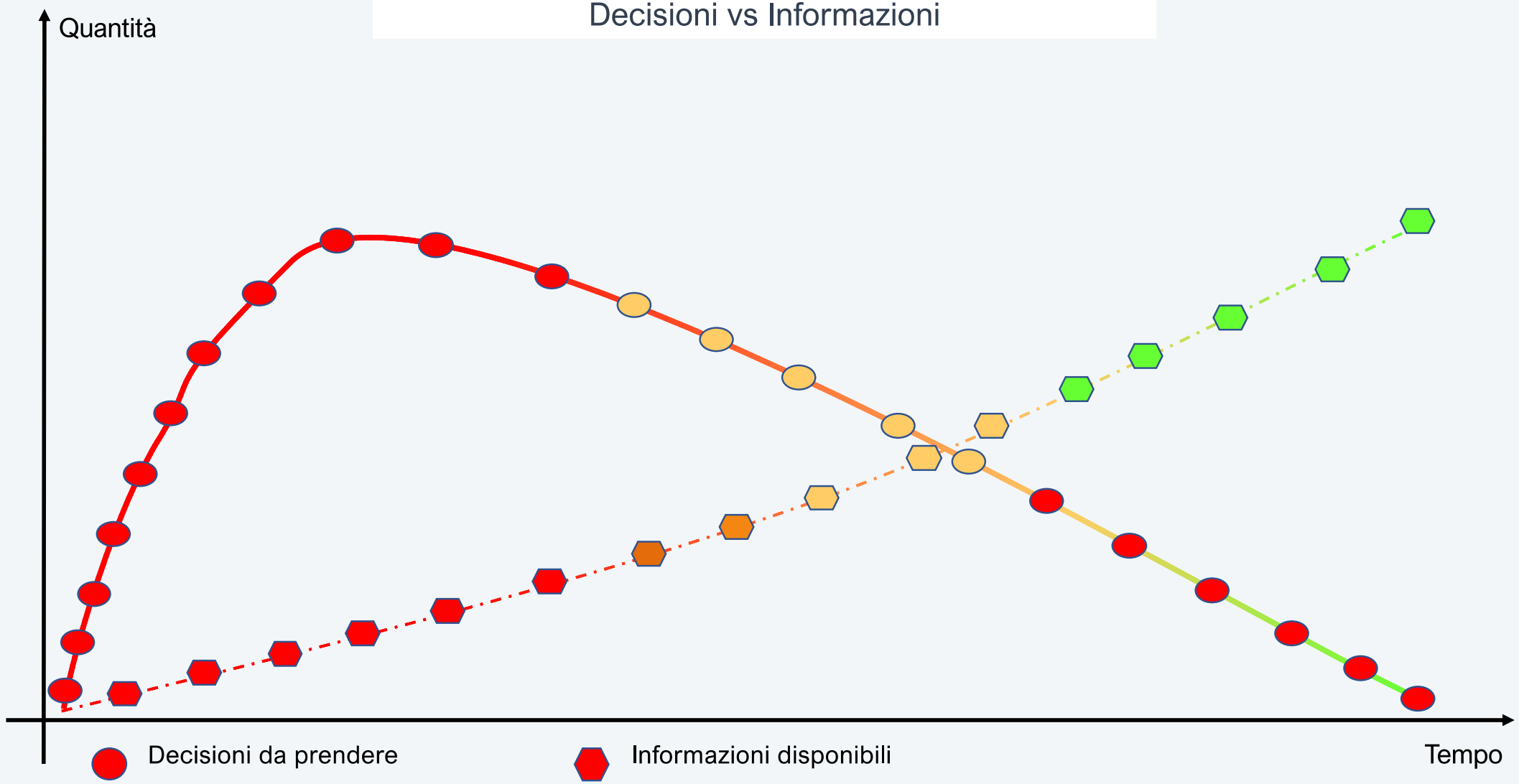
dobbiamo avere in mente che durante una crisi

Step operativi per ritorno alla normalità produttiva

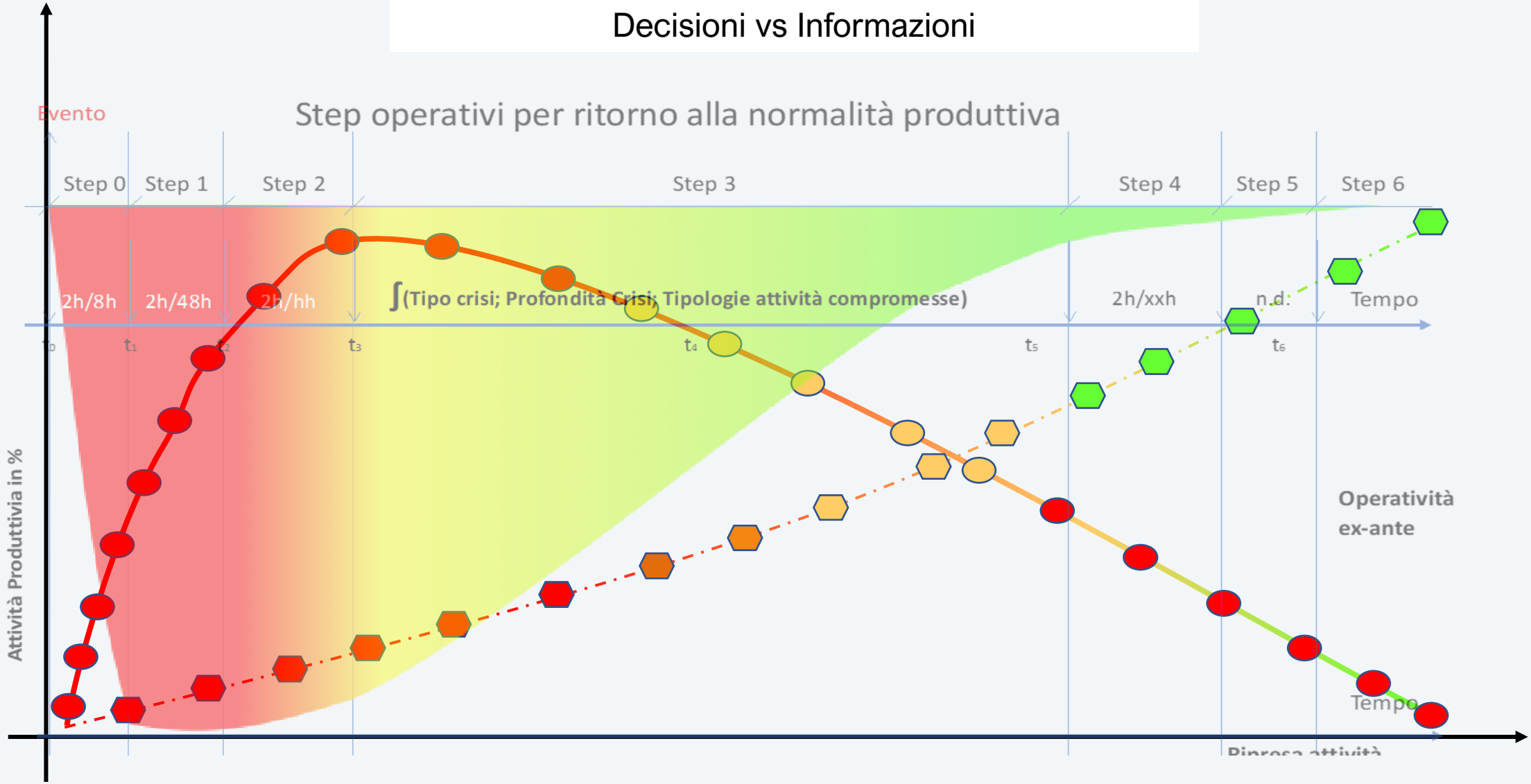


Fonte: G.Lucietto

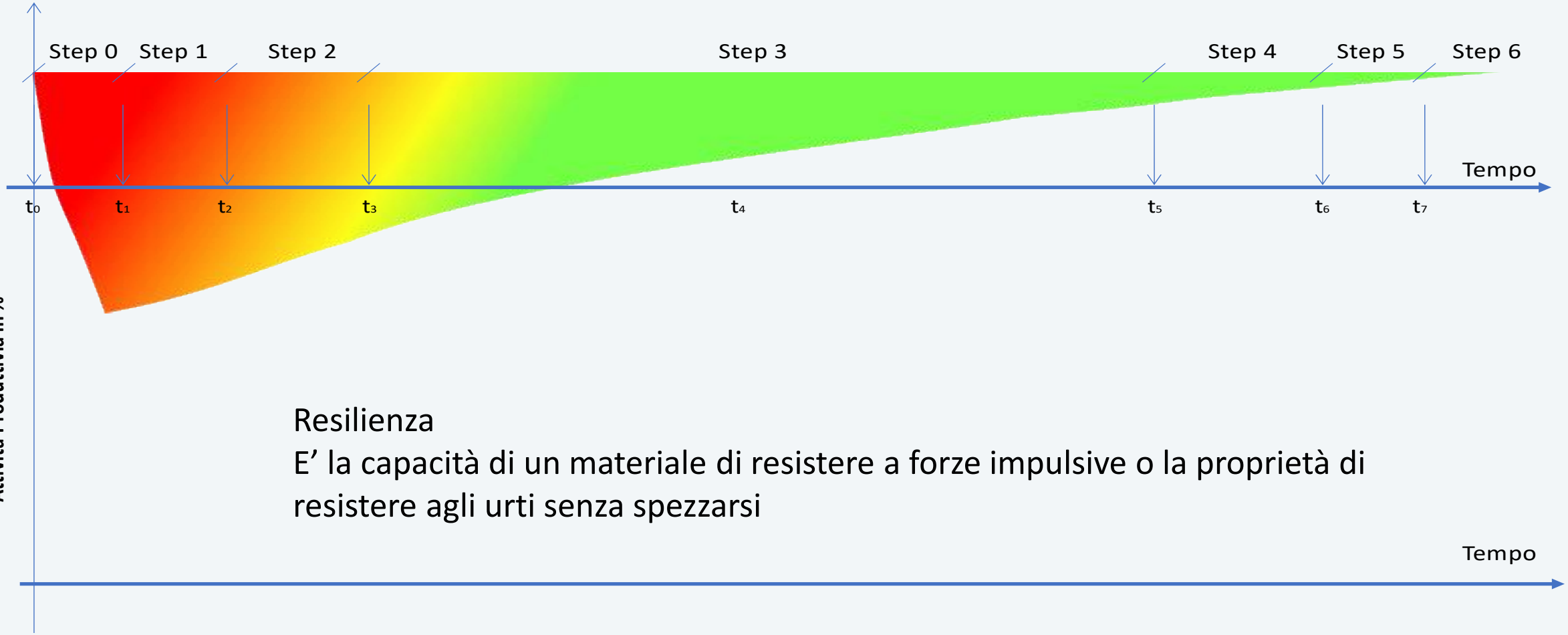
Decisioni vs Informazioni



Decisioni vs Informazioni



Step operativi per ritorno alla normalità



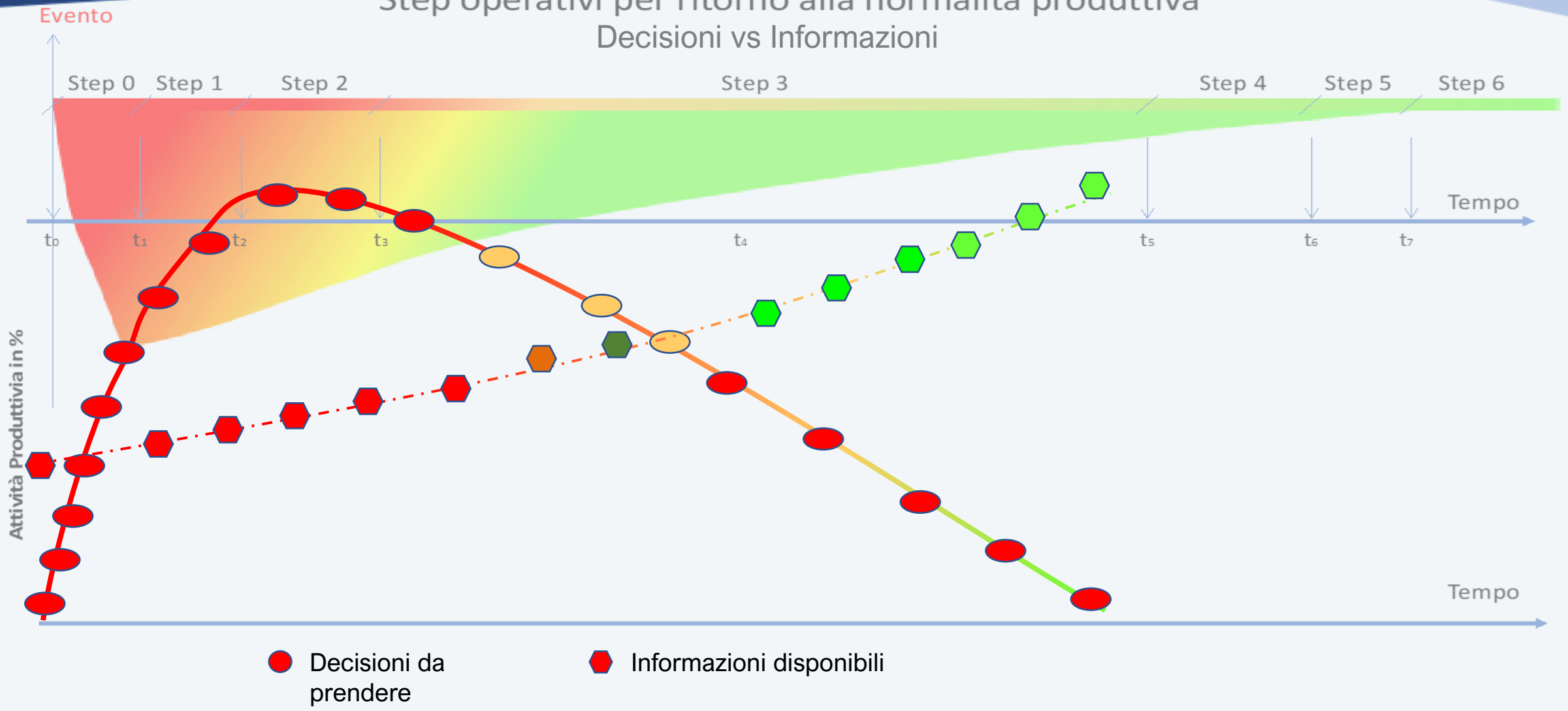
Resilienza

E’ la capacità di un materiale di resistere a forze impulsive o la proprietà di resistere agli urti senza spezzarsi

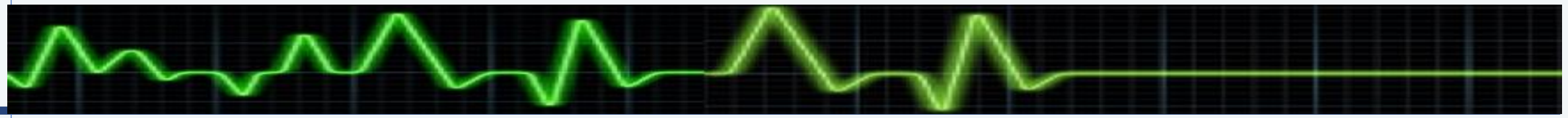
Fonte: G.Lucietto

Step operativi per ritorno alla normalità produttiva

Decisioni vs Informazioni



Fonte: G.Lucietto



Sistema Organizzato

processi
attività

relazioni

prodotti

servizi

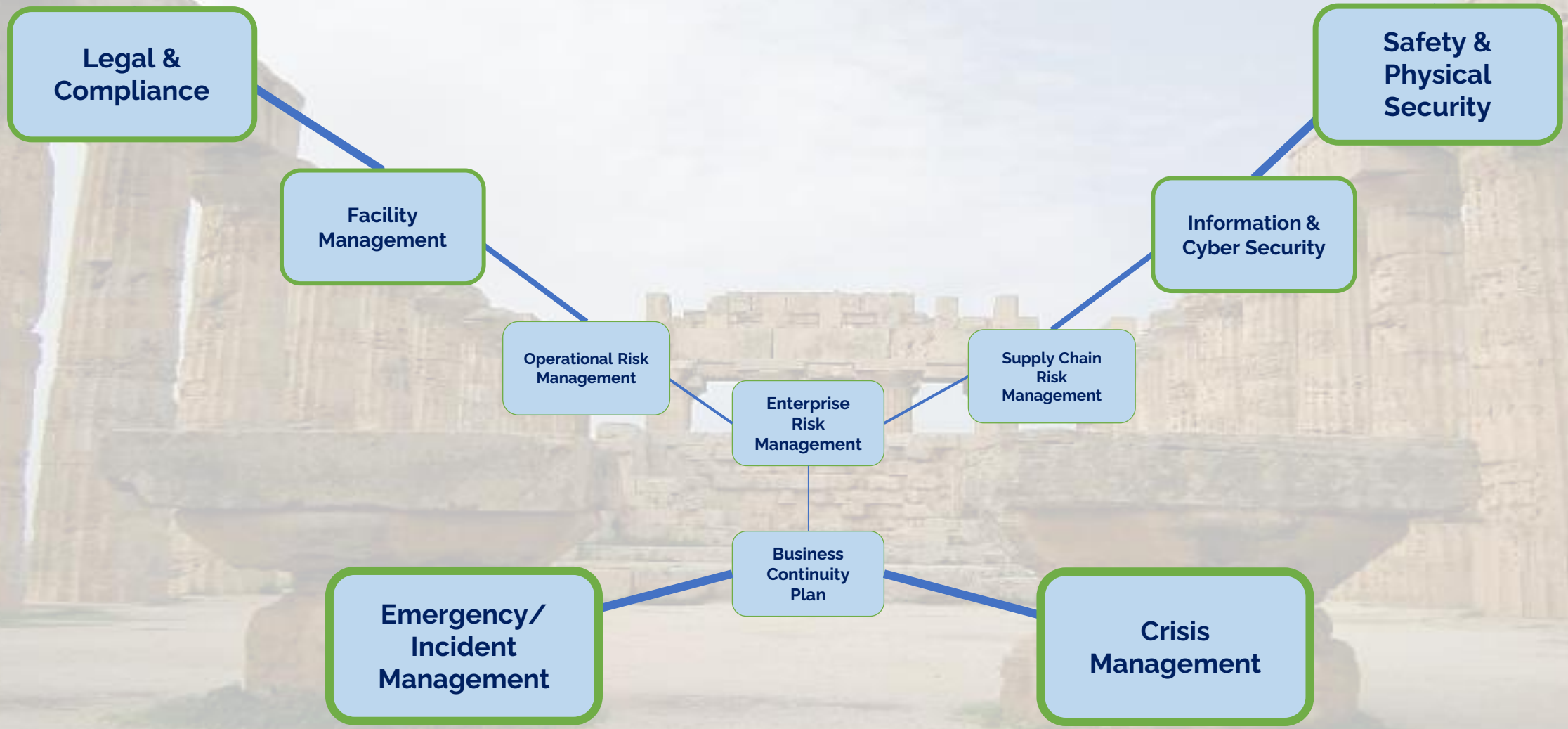
asset

conoscenze
competenze

come proteggiamo il nostro sistema?

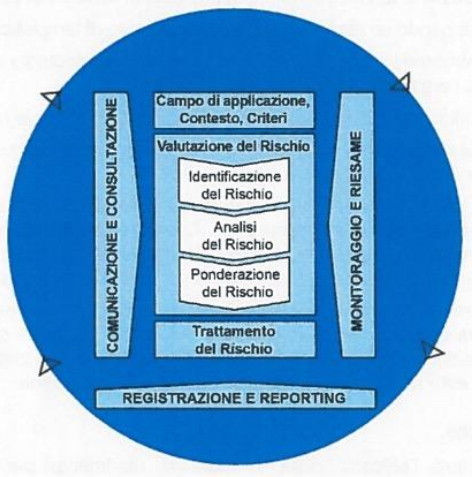
Ogni sistema organizzato è un sistema produttivo

Strategie Operative di Difesa

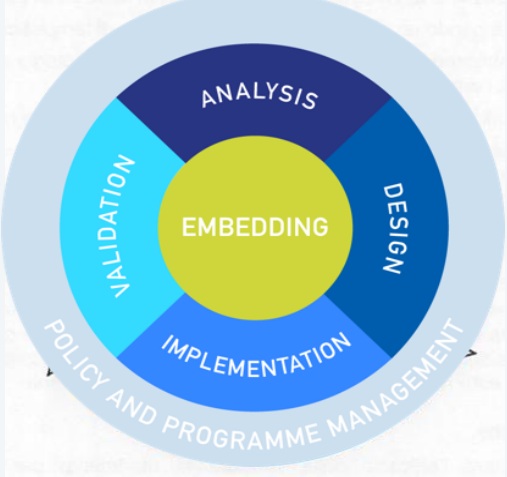


lavorano insieme con un unico obiettivo: garantire la resilienza

1- Risk Management



2- Business Continuity



adattamento continuo

ISO 31000:2018 - Process

Rimando a GPG2018 BCI

Business Continuity

Capacità di un'organizzazione **di continuare l'erogazione** di prodotti e servizi entro tempi accettabili con una capacità produttiva predefinita **durante una interruzione**

La Norma ISO 22301:2019

Fornisce i requisiti per un efficiente Sistema di Gestione della Continuità Operativa (Business Continuity Management System - BCMS).

Si applica a tutte le organizzazioni, siano esse piccole, medie, grandi, locali, nazionali o globali, pubbliche o private

Fonte: ISO 22301:2012

Quali rischi

Fonte Allianza Risk Barometer

Cosa fare per diventare virtuosi e non farsi sopraffare?

0 Implementare un efficace sistema di gestione dei rischi

1 Definire policy e programma di continuità operativa

2 Incorporare la continuità operativa nell'organizzazione

3 Eseguire le analisi di impatto (BIA - Business Impact Analysis)

4 Progettare il sistema di continuità operativa

5 Implementare il piano di continuità operativa

6 Validare il sistema

è caduto molto tempo fa, e non si è mai arreso…

Cosa hanno fatto i virtuosi per proteggersi?

Drivers di Rischio della Supply Chain

Supplier risks

Monitoraggio costante:

- dei fornitori chiave
- qualità delle forniture
- Maggior **flessibilità**

Network Risk

Pianificazione continua

- collaborativa
- previsionale

Process risks

- Riduzione della variabilità/varietà delle produzioni
- **Monitoraggio** dei Colli di Bottiglia noti
- **Ri-pianificazione** e dimensionamento dei magazzini

Demand risks

Monitoraggio e gestione:

- dei clienti chiave
- della domanda e sue distorsioni
- cicli di vita dei prodotti

Financial Risk

Monitoraggio:

- Volatilità dei prezzi materie prime
- Credito & Tasso di Interesse
- Cambio
- Rischio Liquidità
- Rischio di Controparte

Environment/Social Risk

- Catastrofi naturali
- Terrorismo e guerre
- Cambiamenti normativi
- Tassazione, dazi e quote
- Scioperi
- Pandemie

Cosa hanno fatto i virtuosi per proteggere la propria organizzazione?
si sono adattati velocemente

Analisi:

- dello stato di emergenza dovuto a diffusione Virus SARS-COV2
- dei rischi e valutazione delle esposizioni ai rischi
- dell'influenza dei drivers sulle esposizioni

Valutazione dei potenziali impatti sull'azienda

Identificazione di soluzioni adattive e valutazione applicabilità delle tecniche identificate

Selezione e implementazione delle tecniche di gestione più appropriate

Monitoraggio costante dell'evoluzione dell'emergenza

Adattamento continuo

Rischio Biologico
Rischio a Criticità Differita

re-attività vs pro-attività adattiva

Dove il sistema ha fallito nel proteggere la propria filiera?

Dove il **sistema** era **rigido** ovvero dove il vincolo normativo non ha permesso l'adattamento al periodo di emergenza perché fondato sul privilegio - Sistemi non modificabili/adattabili nel breve periodo hanno creato disfunzioni operative.

(es. la Scuola)

La **rigidità** del sistema ha reso impossibile la gestione dell'emergenza creando **disfunzioni e incapacità di agire nell'emergenza di breve periodo**. es. orario nella scuola, smart working inefficiente causa lentezza degli approvvigionamenti dell'apparato pubblico (HD e SW).
Più il **sistema** normativo è **flessibile** più velocemente si **gestisce** l'emergenza e si **compensa**, se è rigido non si compensa nulla.

Il funzionamento del sistema di difesa

Presidi Tecnici
I° livello

Strutture - Servizi
Personale Operativo

Presidi Organizzativi
II° livello

Organizzazione - Processi - Controlli
Monitoraggio Rischi

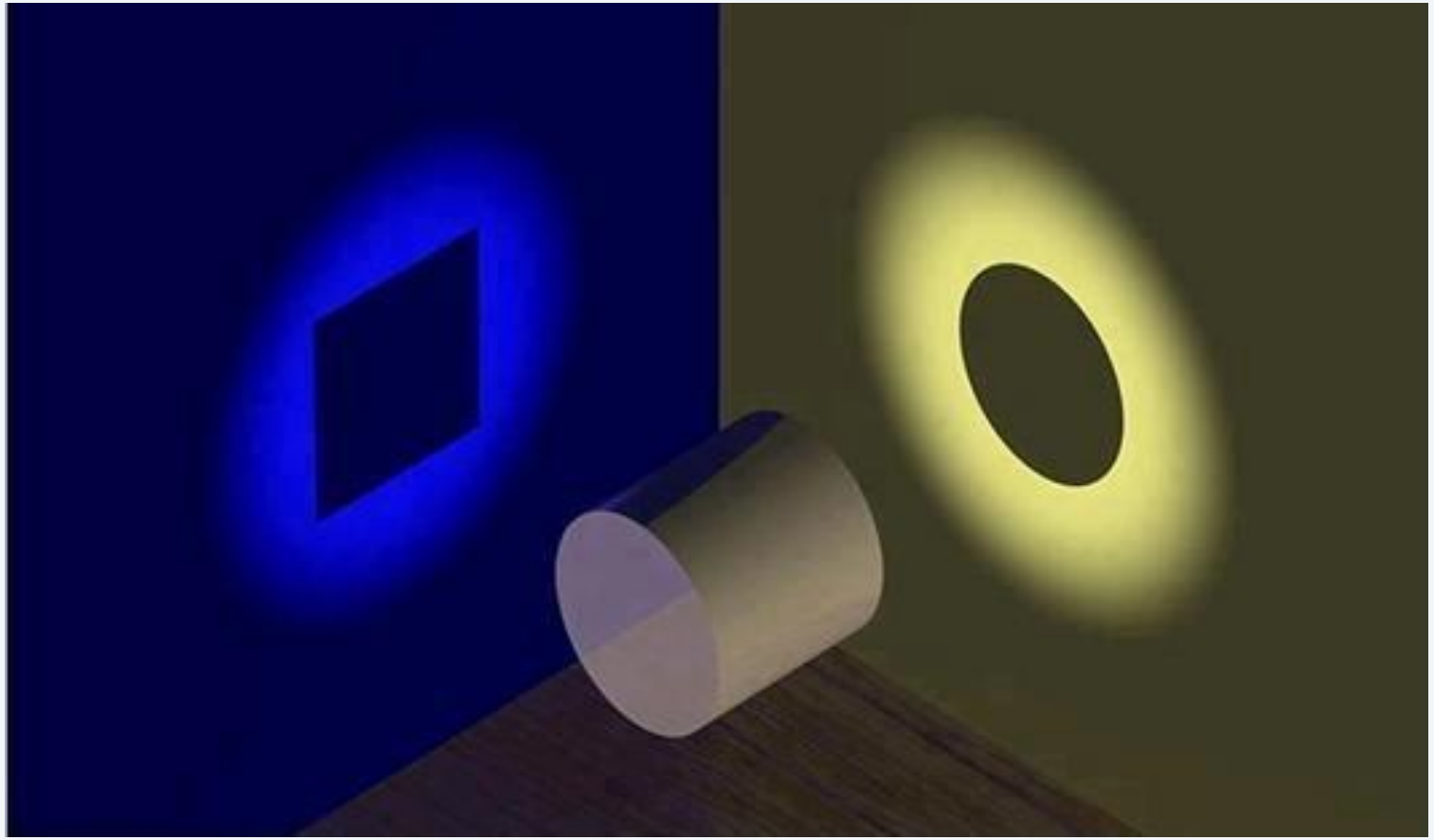
Presidi Giuridici
III° Livello

Vigilanza e Controllo
O.d.V- Internal Audit

Le Mura di Teodosio II
Costantinopoli

è caduto molto tempo fa, e non si è mai arreso…

Ricordatevi che la gestione dei rischi è un viaggio e non una destinazione finale



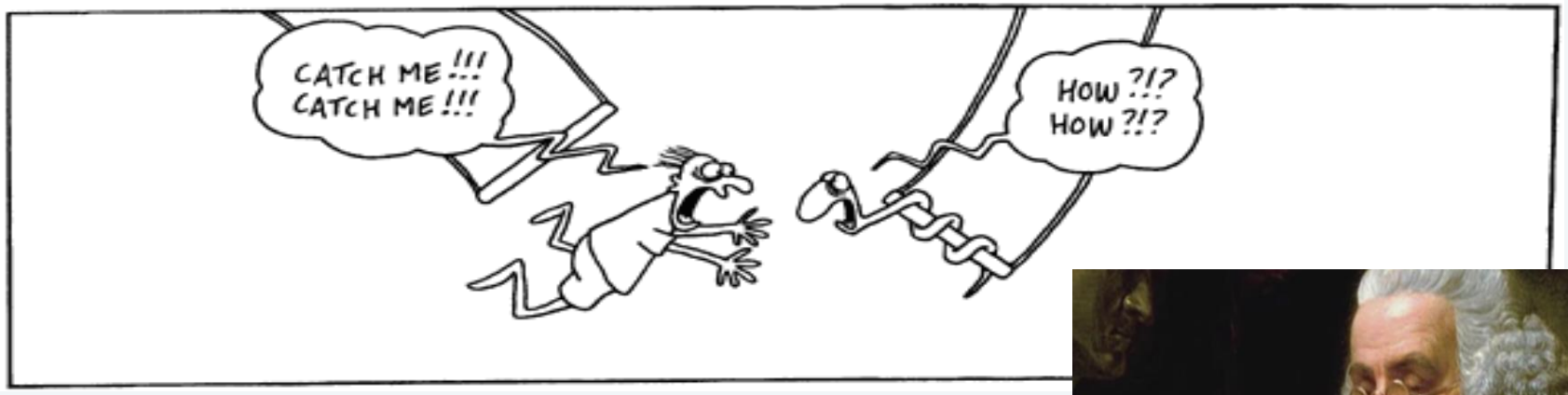
Quando cambi il modo di osservare le cose, le cose che osservi cambiano (fisica quantistica)

Seconda Parte (Ing. Marco Terzago)

- L'interruzione dell'operatività: come essere preparati
- Business Continuity Management
  - Che cos'è?
  - Perché?
  - Prepararsi a cosa?
  - Obiettivi
  - Case Study
- Concetti generali ISO22301:2019
- Business Impact Analysis
- Piani di Continuità Operativa
- Conclusioni

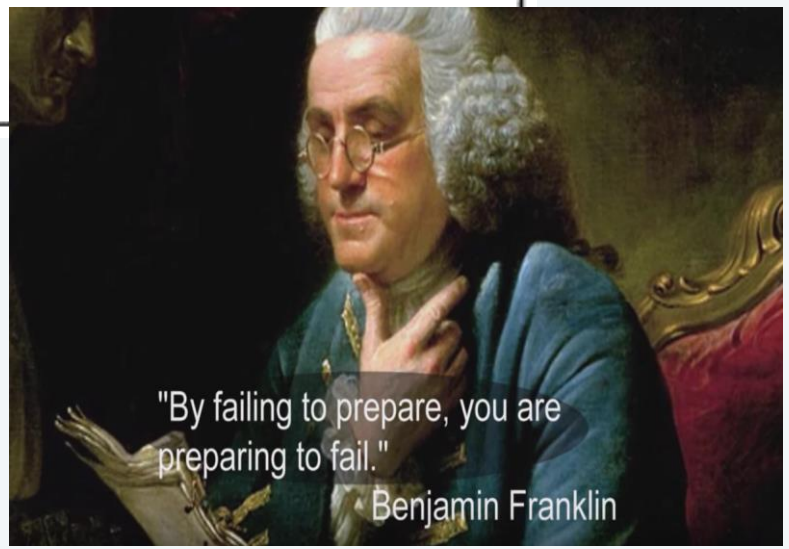
Business Continuity Management: un punto di vista …

Essere correttamente preparati è una scienza complessa…



I nostri padri latini dicevano:
«***Previdet ac providet***»

Gli anglosassoni dicono:
«***Sbagliare a prepararsi significa prepararsi a sbagliare***»



Business Continuity Management: che cos'è?

Il **Business Continuity Management (BCM)** o **Gestione della Continuità Operativa** dei processi di un'azienda comprende l'insieme di attività, strutture organizzative, strumenti ed infrastrutture volte a preservare la continuità dei processi a fronte di eventi che concorrono in maniera potenziale e/o reale alla loro interruzione.

Il perseguimento della continuità operativa aziendale si realizza attraverso la progettazione, l'implementazione, il monitoraggio ed il miglioramento continuo di un adeguato programma, definito in accordo ai principali standard internazionali e nel rispetto delle direttive nazionali.

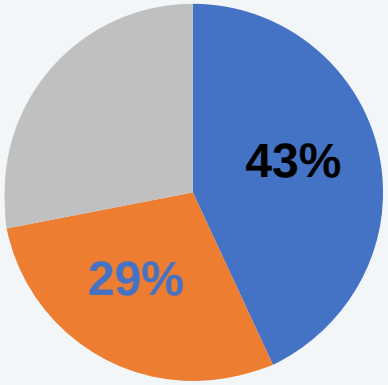
Business Continuity Management: perché?

Per ciò che nel mondo anglosassone è definita “preparedness”, ovvero l’avere pianificato il sistema organizzativo e le azioni manageriali ed operative da attivare in seguito ad un evento incidentale significativo per ripristinare le attività entro tempi definiti

“Experience is a hard teacher because it gives the test first, the lesson afterwards” (Vernon Sanders Law)

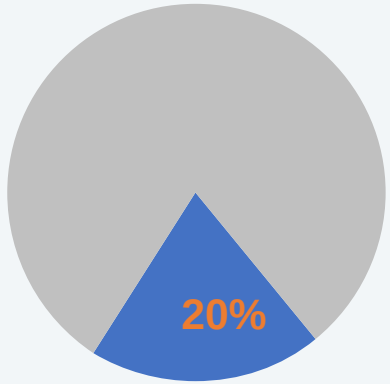
- Ristabilire l’operatività delle funzioni critiche nel più breve tempo possibile
- Stabilire mezzi alternativi per il prosieguo delle attività produttive e/o di supporto aziendali
- Minimizzare i danni a persone ed asset aziendali
- Mantenere la fiducia dei Clienti, del personale e, in generale, di tutti i portatori di interesse rilevanti per l’Azienda
- Assicurare che le informazioni fornite al personale, ai media ed al pubblico siano rilasciate in maniera strutturata
- Operare in sinergia con le azioni di Corporate Governance, Responsabilità Sociale e Risk Management dell’Azienda

Perché è necessario essere preparati?



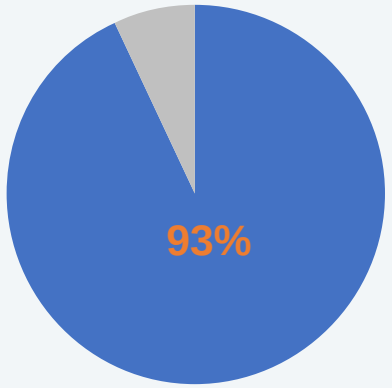
- 43% delle aziende non ha ripreso le attività dopo un disastro
- Più del 29% ha chiuso nei successivi 3 anni

(Fonte: U.S. National Fire Protection Agency)



- 20% delle PMI è soggetta ha disastri gravi ogni 5 anni

(Fonte: Richmond House Group)



- 93% delle aziende che hanno una perdita significativa di dati escono dal business nei successivi 5 anni

(Fonte: U.S. Bureau of Labor)

Dipendenti demotivati sono la fonte di rischio più grande e più dannosa per l'azienda
(Fonte: US National Computer Security Association)

Business Continuity Management: Prepararsi a cosa ?

BBC

Venezuela to seize cement plants

Venezuelan President Hugo Chavez

Cement production is the latest target of Mr Chavez's nationalisation drive. Venezuela has said it will seize local plants and offices belonging to Mexican cement giant Cemex, as it proceeds with nationalising its cement industry.

NECESSITA' DI

SISTEMI INTEGRATI

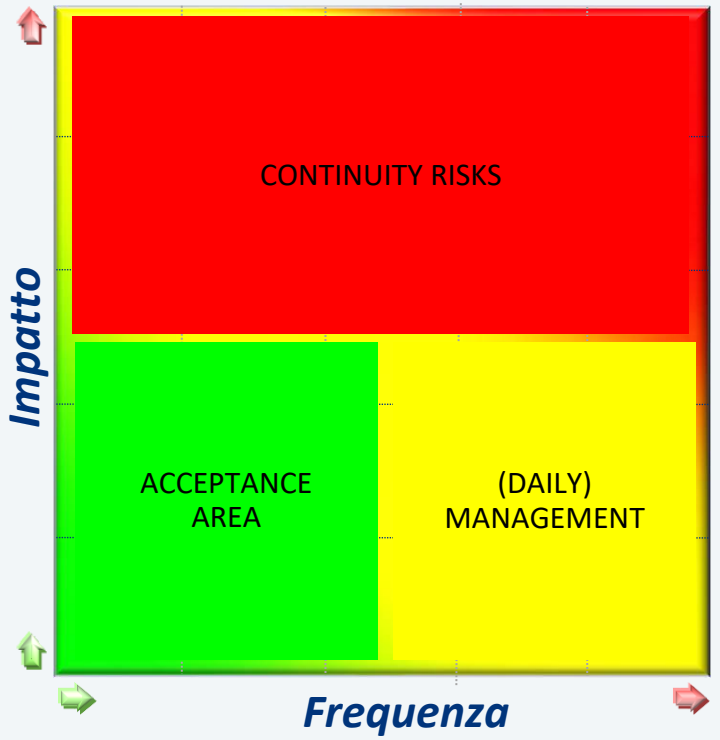
PER BUSINESS CONTINUITY,

RISK MANAGEMENT E

CRISIS MANAGEMENT

Business Continuity Management
Prepararsi a cosa? Alcuni spunti…

- Perdita di sito produttivo principale
- Recall prodotto per problematiche di sicurezza/qualità
- Perdita di un magazzino strategico prodotti finiti
- Protratta indisponibilità sistema informativo principale
- Incendio invasivo presso uffici headquarter
- Indisponibilità (anche parziale) di macchinari di processo
- Indisponibilità di un partner/fornitore strategico
- Indisponibilità (anche parziale) di fornitori servizi di logistica
- …



Alcuni eventi sono difficilmente pianificabili…

9/11

Tsunami Oceano indiano, 2004

Uragano Katrina, 2005

Crisi Finanziaria Globale, 2008-2010

Pandemia H1N1, 2009

Terremoto Haiti, 2010

BP Deepwater Horizon, 2010

Vulcano Eyjafjallajkull Islanda 2010

Alluvioni Australia, 2011

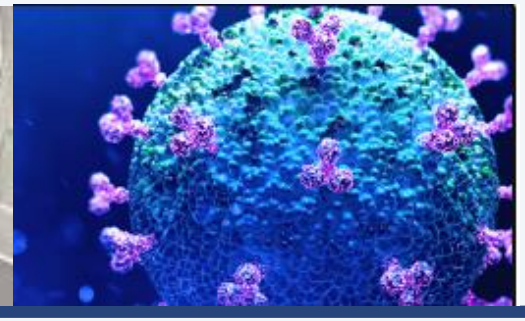
Tsunami Giappone, 2011

Crisi Nucleare Fukushima 2011

Crisi Nord-Africa, 2011

Incendio nella webfarm di Aruba, 2011

Pandemia COVID-19 2020-202x …



… ma si può essere preparati per affrontarli

Principali Standard Internazionali

- BCI & DRI Professional Practices
- ISO 22301 – Business Continuity Management
- Quality Standards ISO 27000 Series
  - ISO 27001 - Information security management systems — Requirements
  - ISO 27002 - Code of practice for information security management
- British Standards – PAS 77:2006 IT Service Continuity Management
- ISO/PAS 22399:2007 – Crisis Management Standards
- ISO 31000, Risk management standard
- Basel II & Basel III Agreement
- Bank for International Settlements - High-level Principles for Business Continuity Planning
- European Central Bank
- European Commission – Markets in Financial Instruments Directive (MiFID)

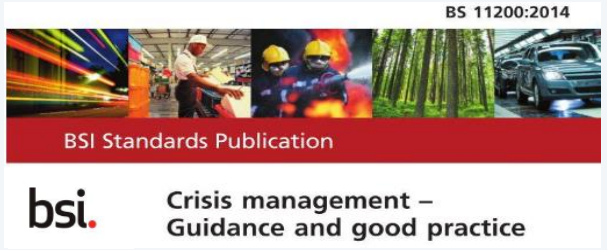
BCM = BCP+ DRP

- **Piano di Business Continuity** (rif. ~~BS 25999~~ >>>> ISO 22301)
  - ➢ È il documento che definisce le modalità per la gestione dell'azienda in situazioni di emergenza
  - ➢ Caratteristiche: documento organico, approvato dalla Direzione, focalizzato sul 'dopo' evento; tratta dei processi critici per il business
  - ➢ Obiettivo del documento è quello di stabilire le strategie e le modalità con cui si deve assicurare la sopravvivenza dei processi aziendali dopo che si è verificato un evento traumatico che ha impedito il normale svolgersi dei processi stessi.

- **Piano di Disaster Recovery** (rif. ~~BS 25777~~ >>>> ISO 27031)
  - ➢ Piano finalizzato ad assicurare il funzionamento dei processi ICT con mezzi alternativi a quelli impiegati in condizioni normali
  - ➢ Costituisce parte integrante del piano di Business Continuity
  - ➢ Caratteristiche: si concentra sul problema della indisponibilità (distruzione, inaccessibilità) dei processi ICT e sul funzionamento delle procedure informatiche critiche.

Che cos'è una CRISI?

Crisis: ***abnormal and unstable situation that threatens the organization's strategic objectives, reputation or viability***
(**BS 11200:2014** "*Crisis Management*")



BS 11200: "A standard for non-standard events"
Prof Edward Borodzicz

Gestione del rischio
Vocabolario

Crisi: **(UNI 11230:2007 "*Gestione del rischio – Vocabolario*").**

UNI 11230

MARZO 2007

crisi (en) crisis	Situazione generata da un **evento** (3.1.4) in grado di danneggiare in modo rilevante un'**organizzazione** (3.1.17). Nota 1 La rilevanza va rapportata alle caratteristiche dell'**organizzazione** (3.1.17). Nota 2 La crisi può coinvolgere, per esempio, la sicurezza delle persone, l'ambiente, le attività operative e la reputazione dell'**organizzazione** (3.1.17).
gestione della crisi (en) crisis management	Processo avente l'obiettivo di fronteggiare e superare una **crisi** (3.5.1). Nota 1 La gestione della crisi, tra l'altro, pianifica i comportamenti dell'**organizzazione** (3.1.17), compreso il **piano di emergenza** (3.5.3). Nota 2 Nella gestione della crisi, la comunicazione riveste un ruolo fondamentale.

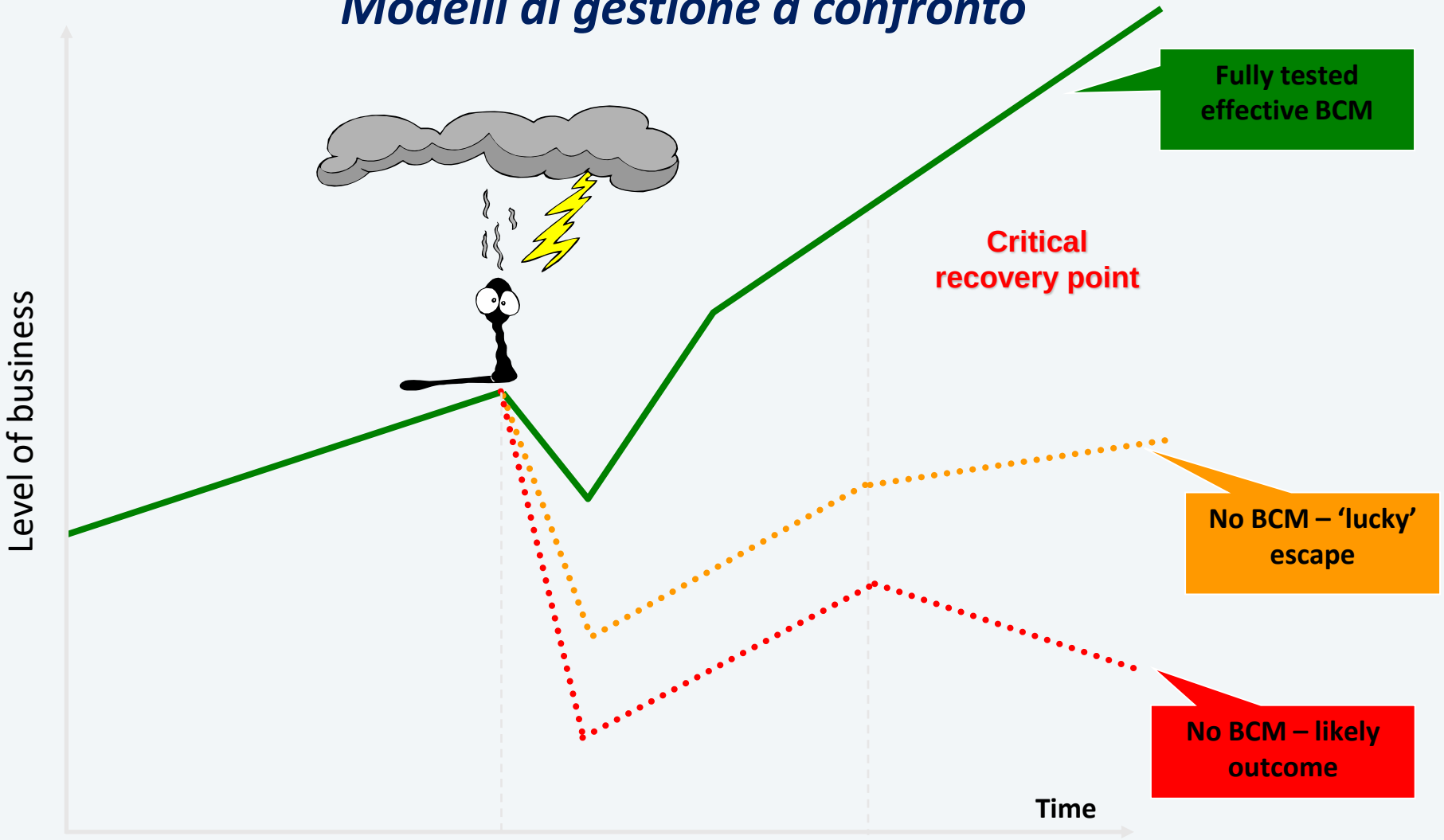
- sui risultati finanziari di un'organizzazione
- sulle relazioni con dipendenti, clienti o fornitori
- sul brand
- sulla **reputazione**.

Che cos'è un DISASTRO ?

Si tratta di un'interruzione nei processi o nelle funzioni aziendali critiche che provoca gravi ripercussioni finanziarie e / o operative, o che necessita l'attivazione del sito alternativo ed il trasferimento dei team incaricati al ripristino.

Pertanto, ogni azienda deve definire quello che è una crisi e quello che è un disastro

What if?
Modelli di gestione a confronto



BCM Case Study
Nokia/Ericsson (1/3)

- Nuovo Messico, Marzo 2000, un fulmine colpisce una linea elettrica
- L'interruzione temporanea di fornitura elettrica danneggia i ventilatori di un forno in uno stabilimento di semiconduttori Philips ad Albuquerque
- Un principio d'incendio viene controllato nel giro di pochi minuti dai dipendenti. I VVF, arrivati presso lo stabilimento, possono solo ispezionare e valutare lo stato dello stabilimento
- I danni appaiono di modesta entità:
  - Otto vassoi contenenti la nanocircuiteria per la produzione di qualche migliaia di chip per cellulari sono distrutti
  - La società prevede di riprendere la produzione entro una settimana
- Successivamente viene rilevato che fumo e fuliggine hanno contaminato un'area molto più vasta dello stabilimento, il che causa un fermo della produzione per settimane
- Due clienti principali: Ericsson e Nokia, che assorbono il 40% della produzione dello stabilimento

Source: The Economist, "When the Chain Breaks" (15-Jun-2006)

BCM Case Study
Nokia/Ericsson (2/3)

La risposta di Nokia

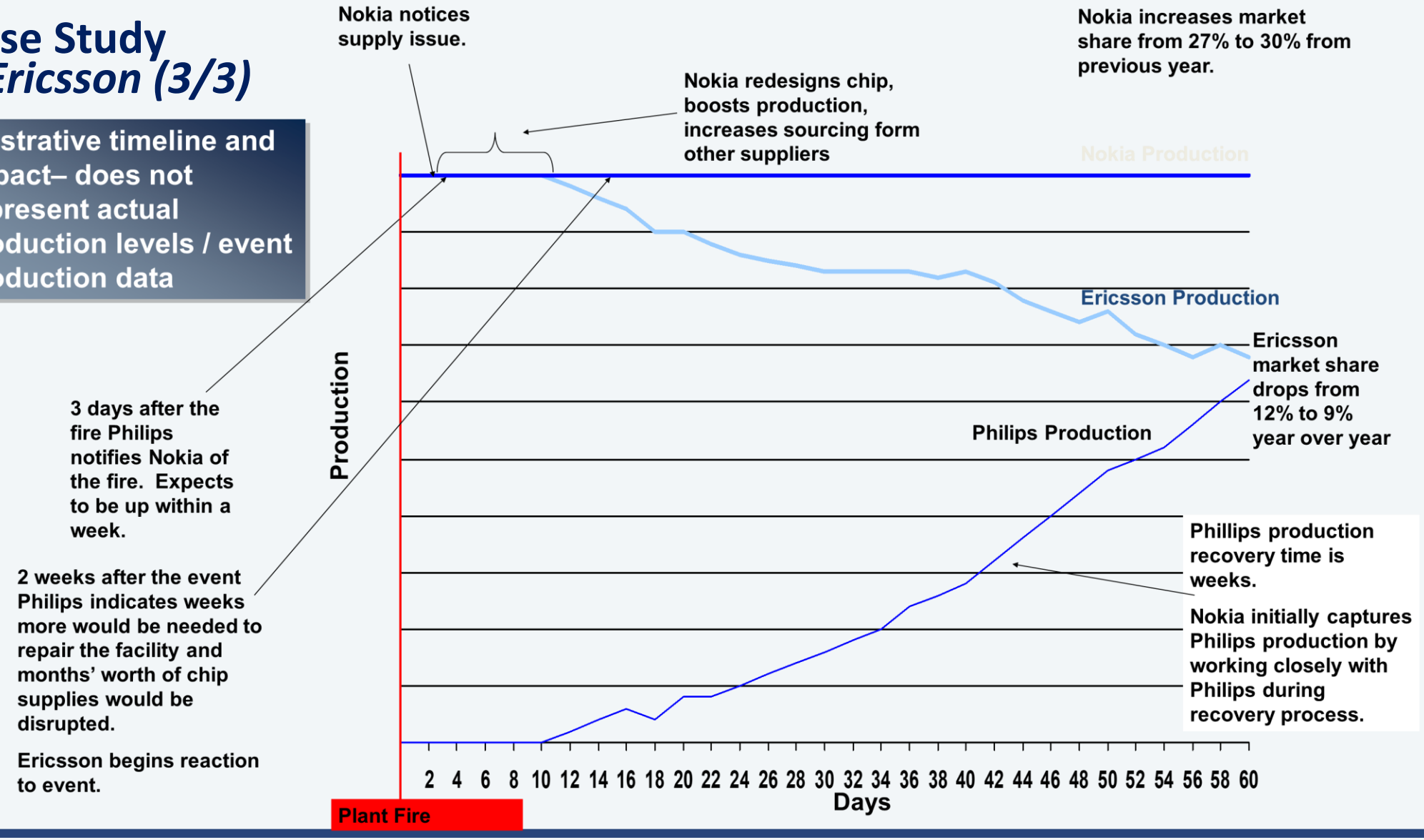
- Il supply-chain manager di Nokia prende consapevolezza del problema, a soli due giorni dall'incendio, quando il loro sistema rileva che alcune spedizioni erano state trattenute
- Nokia decide immediatamente di tenere sotto monitoraggio lo stabilimento
- Prima del 10° giorno dall'evento, Nokia ha già iniziato ad acquisire pezzi da fonti alternative

La risposta di Ericsson

- Avendo deciso di semplificare la supply chain usando singoli fornitori per alcuni componenti, incluso i chips di Philips, Ericscon non dispone di un "piano B"
- Ericsson affronta una carenza importante di semiconduttori
- La posizione di Ericsson peggiora rapidamente in quanto la produzione di modelli attuali e il lancio di nuovi prodotti sono bloccati
- Nel 2001, Ericsson decide di lasciare il mercato dei cellulari come produttore, spostando il business in una joint venture con Sony

BCM Case Study
Nokia/Ericsson (3/3)

Illustrative timeline and impact– does not represent actual production levels / event production data



ANRA
Associazione Nazionale dei Risk Manager e Responsabili Assicurazioni Aziendali

ISO 22301:2019

INTERNATIONAL STANDARD **ISO 22301**

First edition
2012-05-15

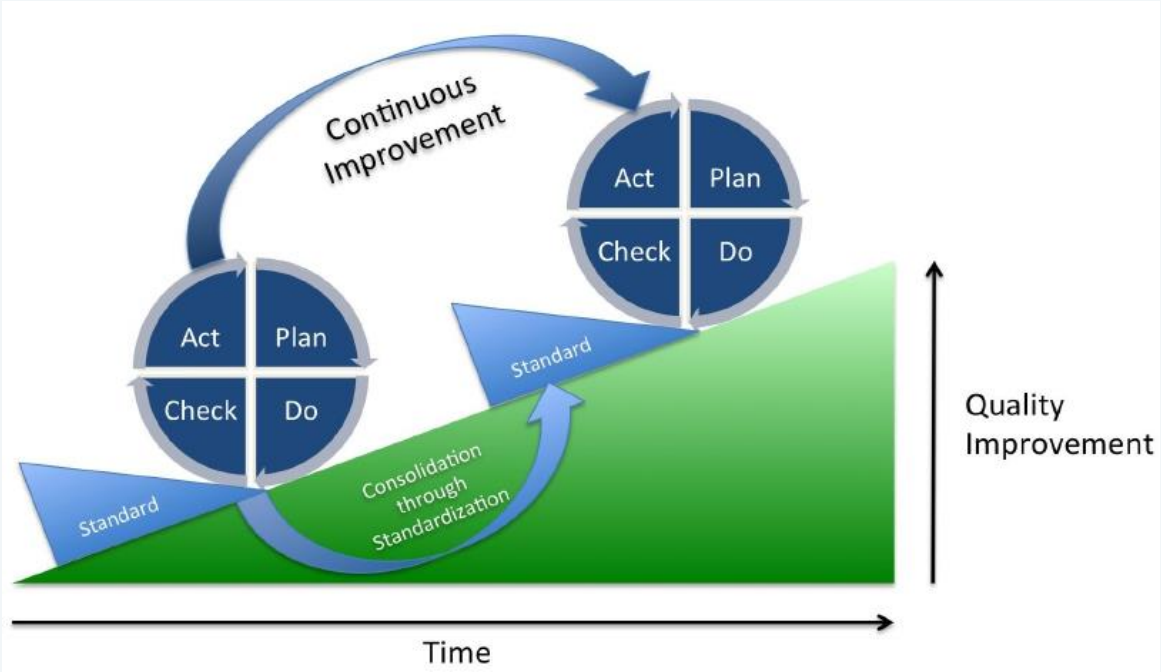
Corrected version
2012-06-15

Societal security — Business continuity management systems — Requirements

Sécurité sociétale — Gestion de la continuité des affaires — Exigences

Reference number
ISO 22301:2012(E)

Security and resilience — Business continuity management systems — Requirements



ORIGINE

La Norma ISO 22301 è il risultato del seguente processo:

1. Il primo standard emanato in materia è la BS 25999
2. Pubblicata a novembre 2006 dal British Standards Institution
3. Fornisce una metodologia per processi, principi e terminologia
4. Viene aggiornata nel novembre 2007
5. Entra in vigore nel 2012 e viene rivista nel 2019

ISO 22301: «EN» dal 2015

ISO TC 223 | *Join us and contribute to a more secure society*

Home | About iso/tc 223 | Organization | Published standards | Under development | Events | Library | News archive | Contact

CEN decides to adopt ISO 22300 and ISO 22301 as European standards

ISO 22300 on terminology and ISO 22301 on BCM requirements that was published in 2012 have now been adopted by CEN (the European standardization organization) as European standards. The decision was taken through CEN/TC 391, the European committee on Societal and citizen security.

European Standards (ENs) are documents that have been ratified by one of the three European Standardization Organizations (ESOs), CEN, CENELEC or ETSI; recognized as competent in the area of voluntary technical standardization and listed in Annex I of EU Directive 98/34/EC.

An EN (European Standard) "carries with it the obligation to be implemented at national level by being given the status of a national standard and by withdrawal of any conflicting national standard". Therefore, a European Standard (EN) automatically becomes a national standard in each of the 33 CEN-CENELEC member countries.

Several other standards from ISO/TC 223 are also under ballot to become European standards, including ISO 22311 on video surveillance formats as well as ISO 22313 which provide guidance on BCM.

Search this site ›

Success stories ›

Interviews ›

Upcoming events

ISO 22301 E NORME EUROPEE

Vantaggi della Certificazione ISO 22301

- Resilienza organizzativa
- Efficienza operativa
- Perdite derivanti da interruzioni
- Rischi reputazionali

1 PREMESSA

La Norma ISO 22301 è stata inclusa sin dal 2015 nell'elenco delle European Norms (ENs), documenti ratificati da una delle tre European Standardization Organization competenti in materia di produzione di standard tecnici come da Norma UE n. 1025/2012.

2 SENTIMENT DEGLI ESPERTI

Cultori della materia ed esperti a livello internazionale concordano nel pensare che qualora il Parlamento Europeo dovesse decidere di regolamentare la Continuità operativa delle Infrastrutture Critiche, la ISO 22301 si trasformerebbe da un «semplice» standard a una **norma cogente**.

3 REAZIONI DEL MERCATO

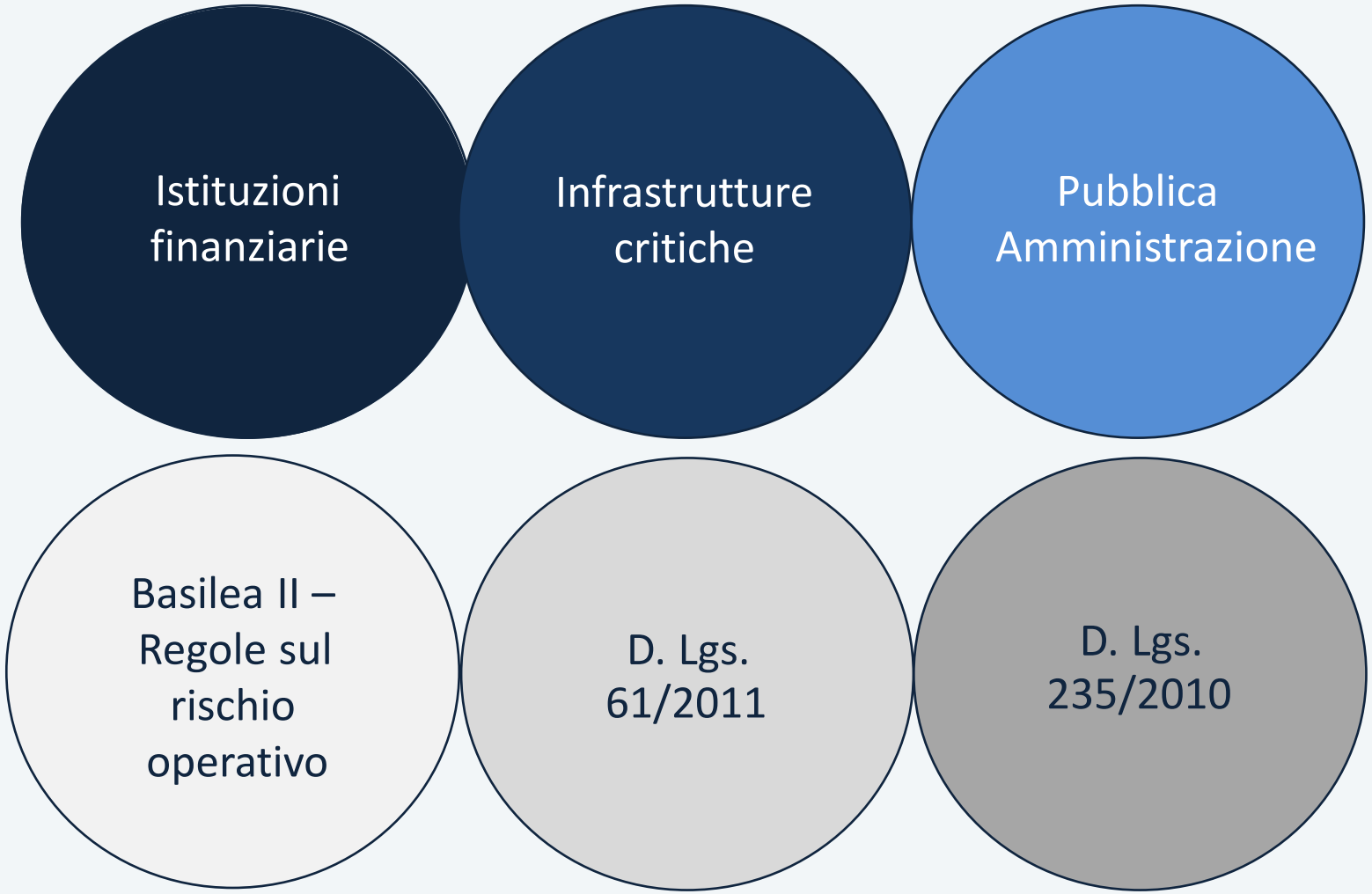
Sono già diverse le organizzazioni europee che hanno intrapreso un percorso verso la certificazione secondo i principi dettati dalla Norma ISO 22301. Tra di esse, molte aziende pubbliche o private che costituiscono Infrastrutture Critiche o appartengono a settori ad esse funzionali (fornitori).

4 PROSPETTIVE PER LE ORGANIZZAZIONI

Le Infrastrutture Critiche o i fornitori di Infrastrutture Critiche sono quindi fortemente incentivati all' adozione dello standard. Un Sistema di Gestione della Continuità Operativa conforme alla Norma ISO 22301:, infatti, conferisce resilienza ed efficienza a tutta l'organizzazione.

1 Una EN diventa automaticamentelo standard di riferimentoin vigore negli Stati membri del sistema CEN-CENELEC

BCM: GIÀ OBBLIGATORIO



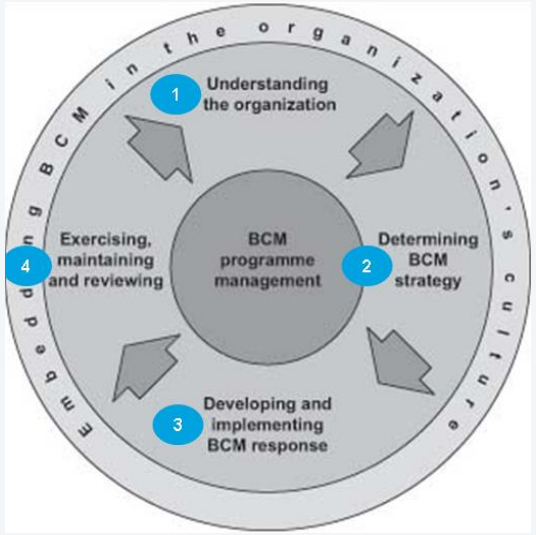
BCM Lifecycle Layout della ISO 22301

COMPRENDERE L'ORGANIZZAZIONE
1

DEFINIRE LE STRATEGIE DI CONTINUITA' OPERATIVA
2

SVILUPPARE ED IMPLEMENTARE PIANI DI CONTINUITA' OPERATIVA
3

ESERCITAZIONE, MANUTENZIONE E REVISONE DEI PIANI
4



Comprendere l'Organizzazione

- Condurre una **Business Impact Analysis (BIA)**;
- Identificare ed elencare le **attività critiche**;
- Definire i **requisiti** della Business Continuity;
- Condurre un Corporate **Risk Assessment**;
- Mitigazione delle Perdite e **Gestione del Rischio**:
  - ✓ Per ciascuna attività critica indicare l'opzione scelta per mitigare le perdite includendo le Strategie di Recovery e il Recovery Time Objective (RTO);
- Sottoscrizione delle **azioni** e delle **contromisure** da intraprendere per ogni minaccia: 4T (Trattare, Tollerare, Trasferire o Terminare).

Definire le Strategie di BCM

Le Strategie di Recovery devono includere:

- Opzioni considerate per le attività e le risorse critiche;
- Persone chiave – Conoscenza della Continuità;
- Edifici, siti alternativi, lavoro da casa, …;
- Tecnologia minima richiesta per il recovery dei sistemi, applicazioni ed informazioni vitali all'interno degli RTO definiti;
- Persone assegnate per salvaguardare e trattare con gli stakeholder chiave;
- Preparazione all'Emergenza;
- Sottoscrizione di tutte le strategie sopra elencate.

Sviluppare e Implementare Risposte di BCM

- Struttura di Risposta conforme ai piani di Risposta all'Incidente, Business Continuity e Recovery/Ripresa.
- Contenuto dei piani:
  - ✓ Scopo, obiettivo e relazioni con gli altri piani; ruoli e responsabilità; attivazione del piano; responsabile del piano e responsabile della sua manutenzione;
  - ✓ Elenco della attività e delle azioni; contatti per l'emergenza includendo anche i parenti prossimi; attività del personale; risposta ai media e controllo delle news date dai media; gestione degli stakeholder; appendici (mappe, piantine, contratti, moduli standard, etc.);
  - ✓ Qualsiasi altra informazione vitale ed importante.

Esercitazione, Manutenzione, Revisione

Ogni organizzazione deve disporre:

- ✓ Esercitazioni regolari su tutti i componenti del programma;
- ✓ Esercitazioni sulle disposizioni di BCM inclusi scopi ed obiettivi per ciascun test e debriefing dopo il test;
- ✓ Mantenere e revisionare le disposizioni di BCM, secondo le evidenze rilevate e nel rispetto degli ultimi regolamenti, di nuovi accordi e revisioni.

BIA: DEFINIZIONE

E’ uno strumento volto a:

- Identificare funzioni e flussi di lavoro **critici**
- Determinare l’**impatto** qualitativo e quantitativo di una crisi (misurazione del rischio)
- Stabilire un **Recovery Time Objective** per ogni processo critico

ANRA
Associazione Nazionale dei Risk Manager e Responsabili Assicurazioni Aziendali

1° Elemento: il PROCESSO di BUSINESS

Esecuzione di una serie di attività all'interno di una funzione che porta ad un'azione effettuata per un cliente/utente

Molto difficile che operi in isolamento

Input e output ben definiti

INTERDIPENDENZE

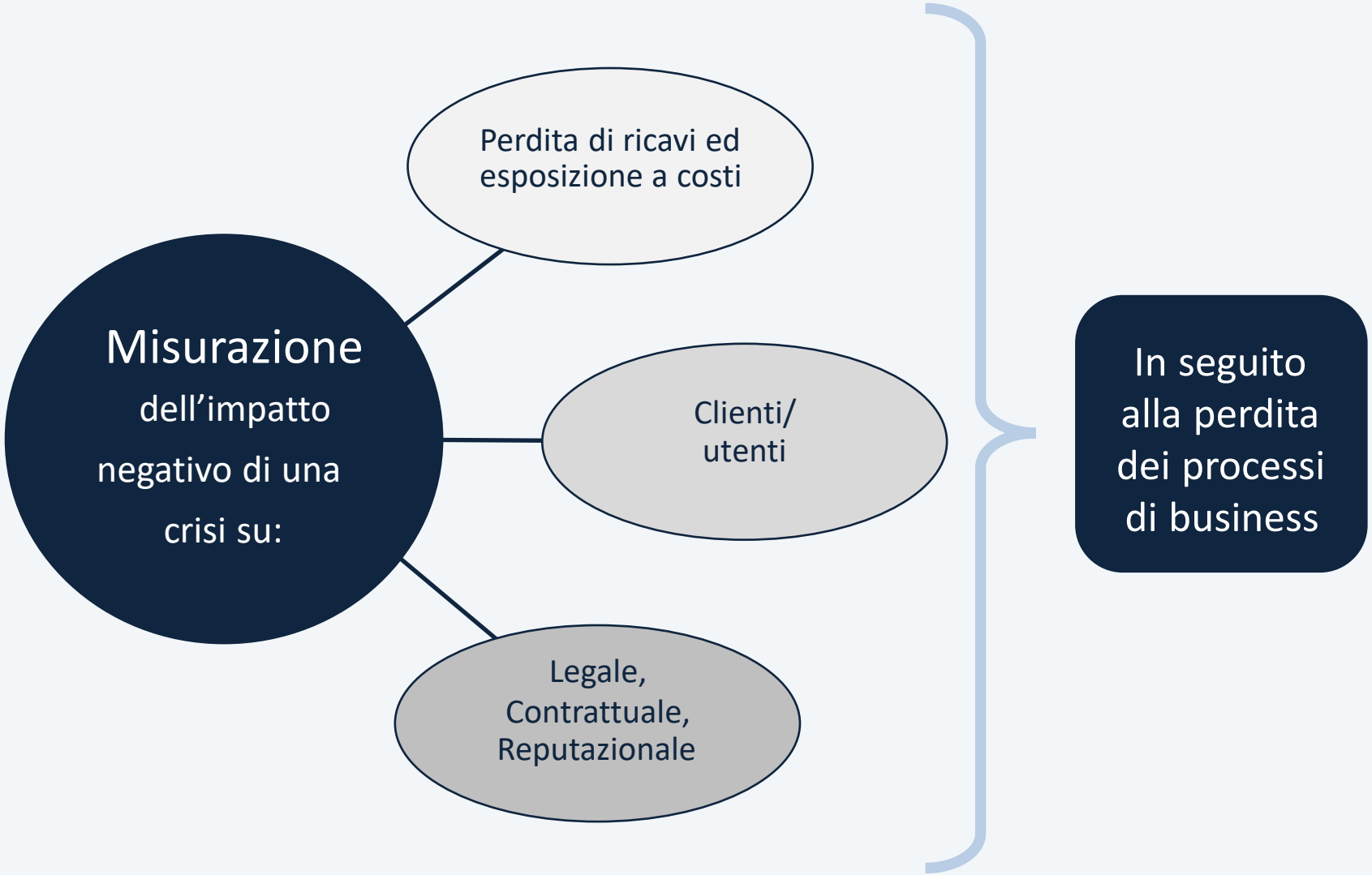
ATTENZIONE alle **INTERDIPENDENZE**!!!

All'interno dell'organizzazione spesso esistono delle **forti relazioni** tra processi/strutture, fornitori, risorse

- Le **INTERDIPENDENZE** possono essere:

1. **Interne** all'organizzazione
2. **Esterne** all'organizzazione
3. **Coinvolgere terze parti**

2° Elemento: LA MISURARAZIONE DELL'IMPATTO



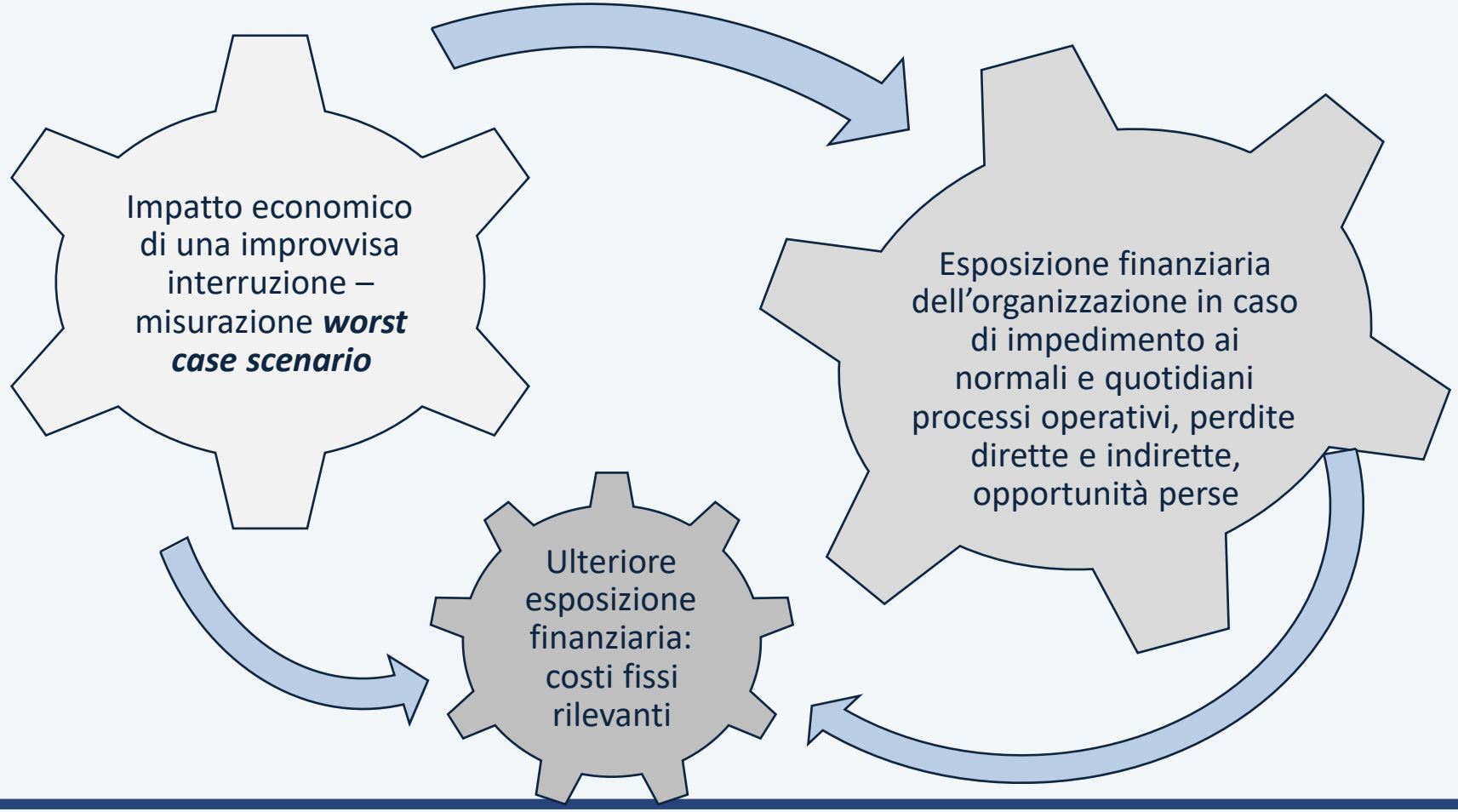
PIANIFICAZIONE E GESTIONE DEL PROCESSO DI BIA - I

I. Determinare e stabilire i **criteri qualitativi e quantitativi** da utilizzare per valutare l'impatto sull'organizzazione dell'evento avverso.

- Esempi di CATEGORIE D'IMPATTO:
  - **Economico**
  - **Reputazionale**
  - **Legale e normativo**

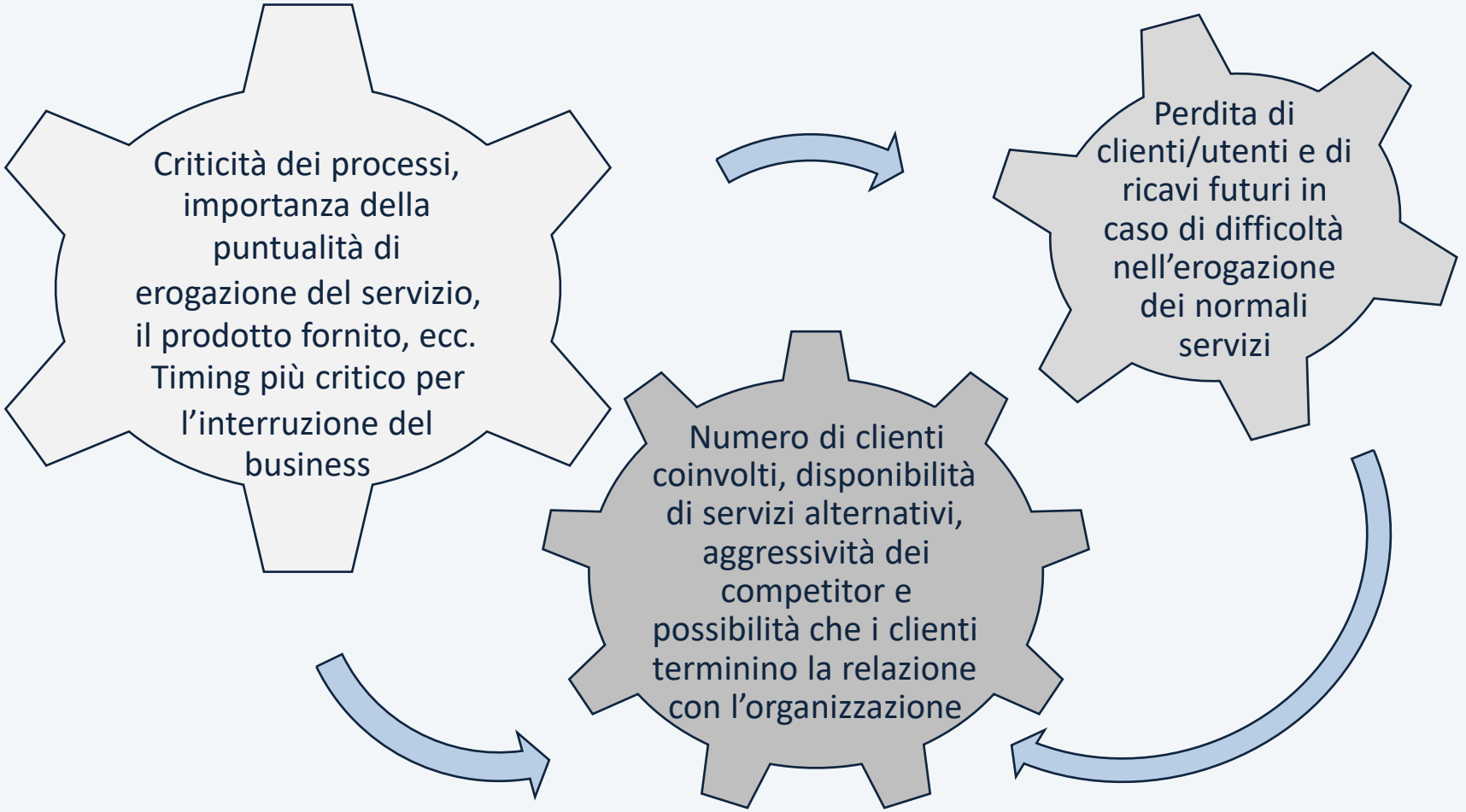
IMPATTO ECONOMICO

Perdite di ricavi ed esposizione a maggiori costi



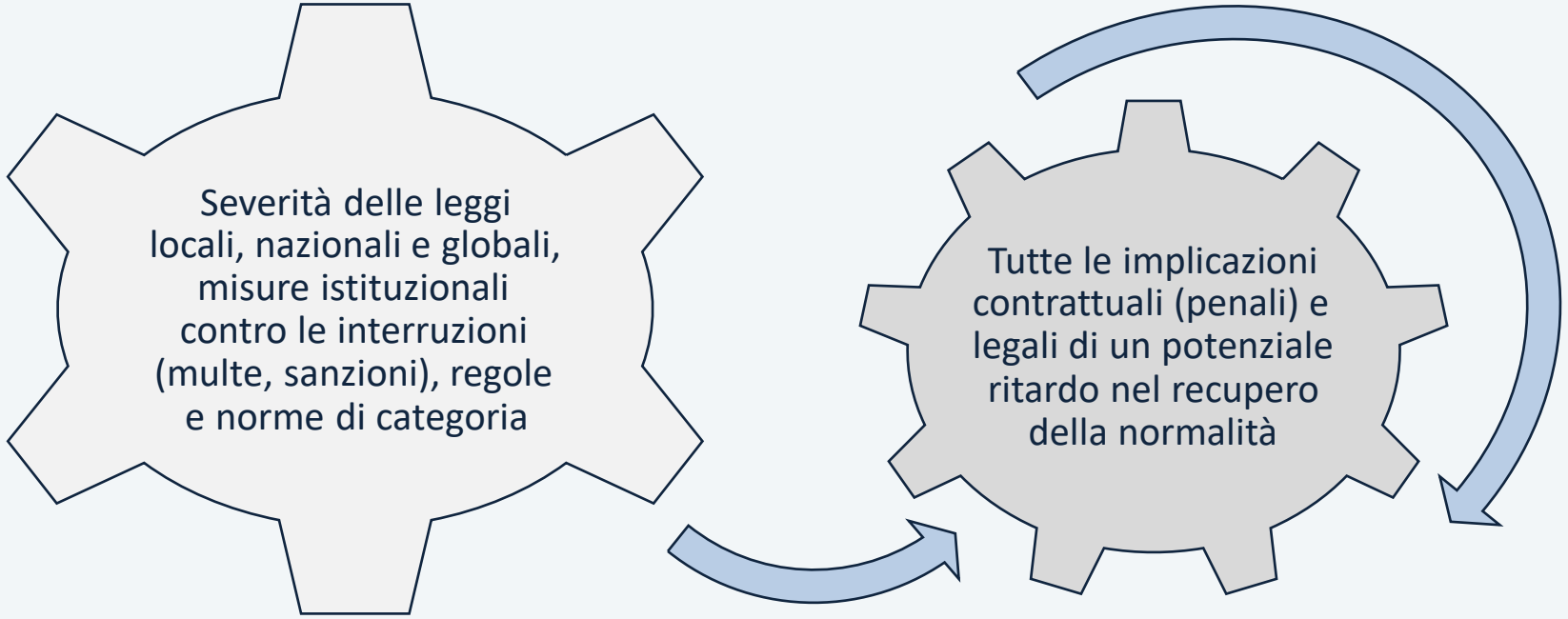
IMPATTO COMMERCIALE/REPUTAZIONALE

Impatto su clienti/utenti



IMPATTO LEGALE E NORMATIVO

Impatto sulle istituzioni, authority, privacy (legale/contrattuale/reputazionale)



La misurazione di questa sezione spesso provoca la riduzione del RTO che non ha un grande impatto nelle altre due categorie

PIANIFICAZIONE E GESTIONE DEL PROCESSO DI BIA - II

II. Ottenere **l'approvazione del Top Management** relativamente ai criteri ed alle metodologie utilizzate nel processo di BIA e stabilire gli obiettivi (VEDI SOTTO) e l'ambito di applicazione

1

IDENTIFICARE E PRIORITIZZARE

i processi e le attività aziendali che impatterebbero maggiormente sull'organizzazione se non fossero più disponibili a seguito del verificarsi di un evento avverso.

2

ANALIZZARE

i risultati ottenuti per accertare eventuali differenze tra gli obiettivi di BC e quanto l'organizzazione sia stata effettivamente in grado di raggiungere, formulando suggerimenti e correzioni.

3

IMPLEMENTAZIONE, REVISIONE E MIGLIORAMENTO

continuo nel tempo del processo di BIA.

ISO 22317

Specifica Tecnica : linee guida per la Business Impact Analysis (BIA)

ISO22317 è una guida dettagliata utile per:

Costruire
Implementare
Mantenere

} una BIA

nel rispetto dei requisiti contenuti all'interno della ISO 22301

CONCETTO DI CRITICITÀ

In un'organizzazione ci sono molte funzioni che sono molto importanti, ma non critiche. Esse non saranno oggetto di analisi, non saranno esposte a strategie costose, ma saranno comunque parte del Sistema BCM e dovranno sviluppare un piano.

CRITICO ≠ IMPORTANTE

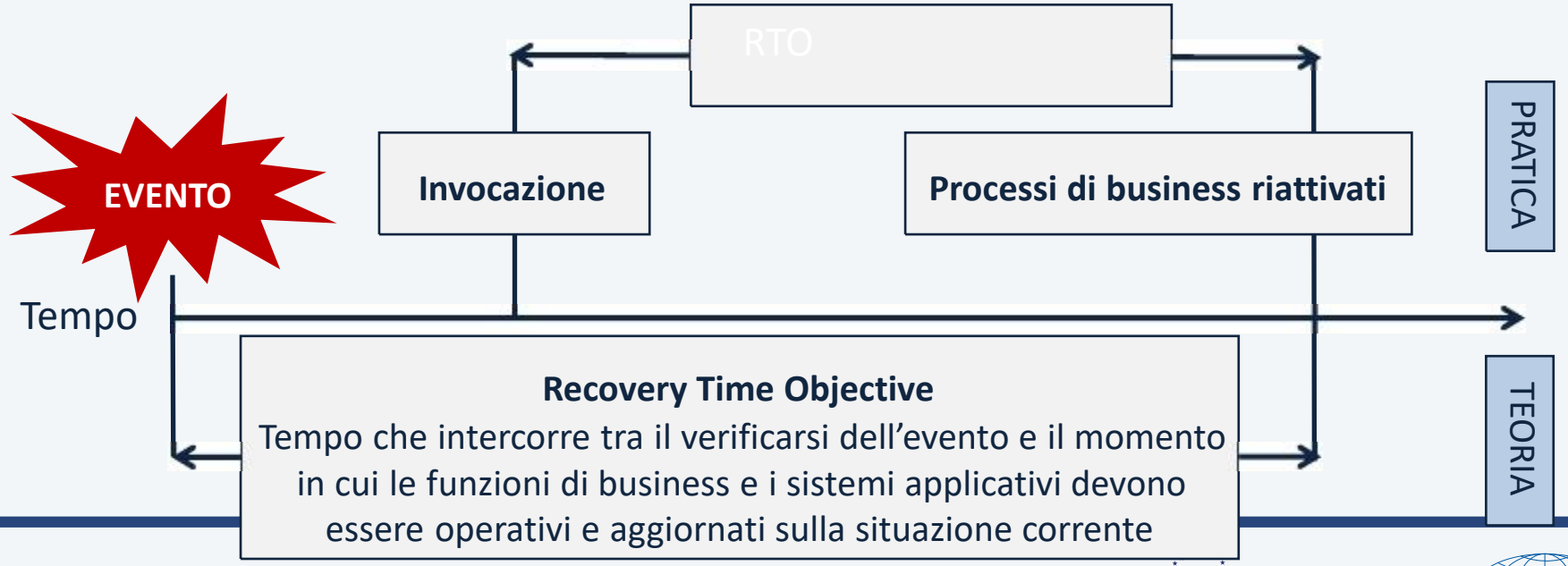
CRITICO = URGENTE

RECOVERY TIME OBJECTIVE (RTO)

"È il tempo massimo concesso all'interruzione del processo come conseguenza di un evento critico"

Gli RTO sono spesso usati come base per:

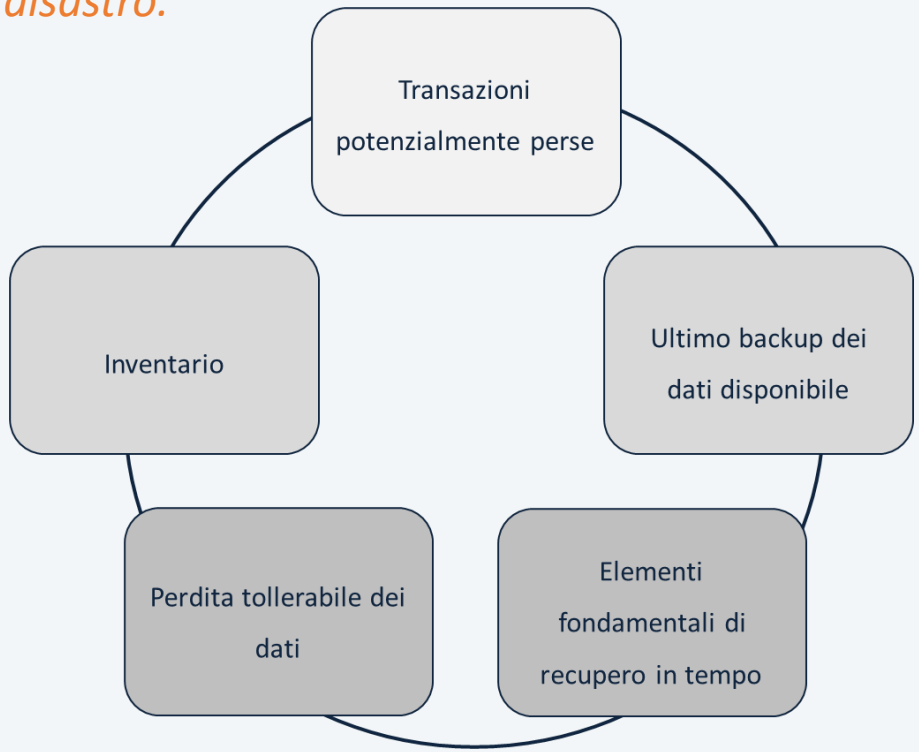
- Stabilire priorità
- Sviluppare strategie
- Determinare se un evento è un'interruzione o un disastro



RECOVERY POINT OBJECTIVE (RPO)

È un valore definito pari alla perdita massima di dati sostenibile in caso di crisi.

Esempio: RPO= 1 g significa che è possibile sopportare la perdita di dati relativi alle 24h di lavoro precedenti al disastro.



CONTENUTI DEL PIANO

Chi	Chi ha la responsabilità delle azioni di recupero
Cosa	Cosa è necessario per recuperare/continuare le funzioni e l'operatività
Dove	Dove andare per recuperare/continuare le funzioni e l'operatività
Quando	Quando devono essere ripristinate le funzioni di business e l'operatività
Come	Come effettuare il recupero (procedure dettagliate di ripristino, continuità e ritorno alla normalità)

CONTATTI CRITICI - ELENCO

- [ ] Fornitori/Vendor – la loro Business Continuity è garantita?
- [ ] Clienti/utenti – abbiamo clausole di continuità operativa?
- [ ] Media – abbiamo preimpostato buoni rapporti?
- [ ] Forze dell'Ordine
- [ ] Ambasciate/Consolati
- [ ] Agenzie di viaggio
- [ ] Organi istituzionali – chi chiamare?
- [ ] Competitors
- [ ] Broker assicurativi

IL PIANO HA SUCCESSO QUANDO…

È flessibile, adattabile, chiaro, conciso	È coordinato con fornitori e gestori esterni	È approvato e supportato dal Top Mgmt	È ben documentato con checklist dei task
Prevede crisi in "worst case scenario"	Include elenco dei vital records	Include risorse chiave e loro alternative	È aggiornato ed è stato testato regolarmente

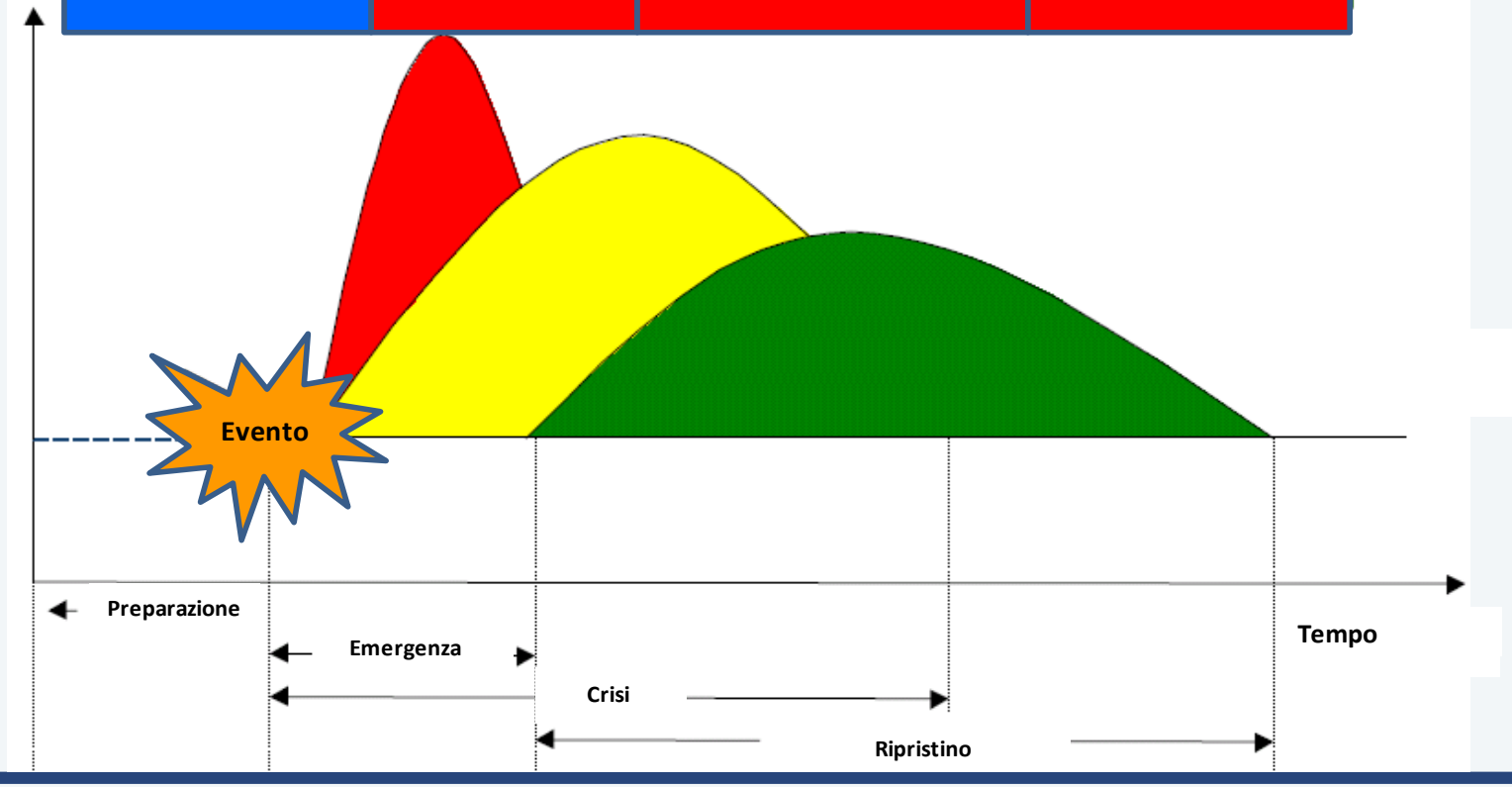
IL DOCUMENTO FINALE

SITO ALTERNATIVO DI RECOVERY

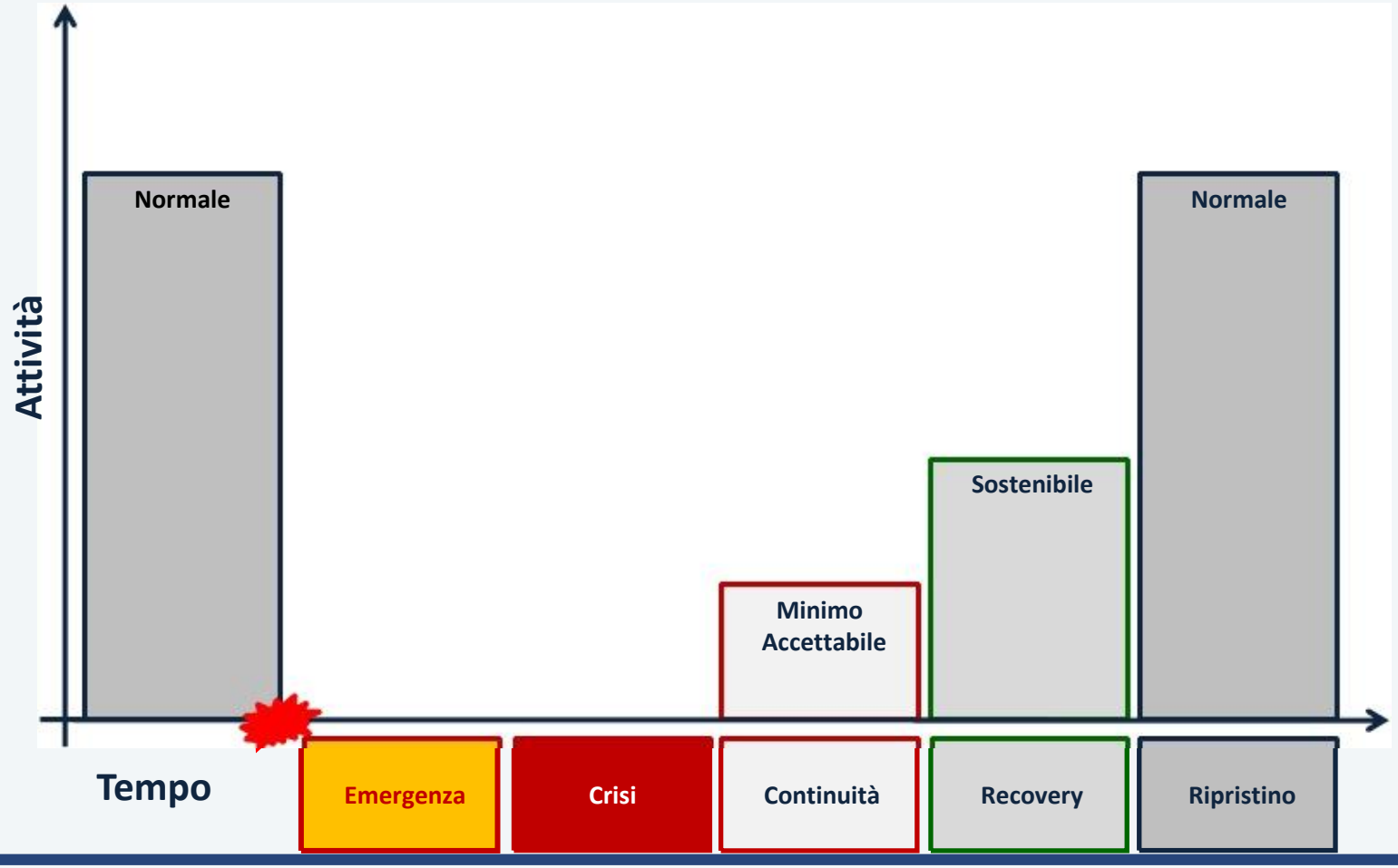
Spazio condiviso o esclusivo? Contratto	Tecnologia e telecomunicazioni adeguate	Stessa cura per la sicurezza	Trasporto pubblico o organizzato dall'organizzazione
Mensa, servizi posta, accessori utili disponibili	In regola e a norma di legge	Siamo benvenuti sul territorio?	Sostenibile per almeno 30 giorni

DIVERSE FASI

FASE DI PREPARAZIONE	GESTIONE EMERGENZA	GESTIONE CRISI	RIPRISTINO
Locale e centrale	Locale	Locale e centrale	Locale e centrale



DIVERSI PIANI PER GESTIRE LE VARIE FASI



Conclusioni: i benefici del BCM

Analisi dei Processi Critici/Vantaggio Competitivo	Aumento di produttività
Business focus/Ri-analisi di risorse e investimenti/Eliminazione di metodologie obsolete	Processi più efficienti
Migliore sfruttamento della tecnologia esistente/ Ottimizzazione spazio dischi e mq	Risparmio costi
Un modello resiliente è facilmente trasferibile, comparabile e fornisce informazioni più sintetiche, utili al più alto livello di business	Portabilità
Motivazione, spirito di corpo, lealtà, pubblicità positiva, felicità dell'organizzazione, orgoglio di appartenenza	Attaccamento al brand

Sitografia e Bibliografia

- www.anra.it
- www.bcmanager.it
- www.bsi-group.org
- www.dri-italy.it
- www.drii.org
- www.thebci.net

GUIDA ANFIA AQ-028
"BUSINESS CONTINUITY MANAGEMENT - GUIDA ALLO SVILUPPO DI UN PROGRAMMA SI GESTIONE AZIENDALE DELLA CONTINUITA' OPERATIVA"
ediz. 1^ - Giugno 2015