

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
dott. Gianluigi Lucietto



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)

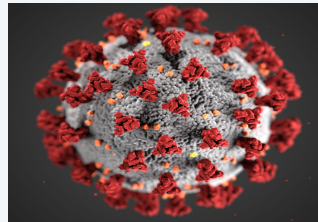
- L'interruzione dell'operatività: come essere preparati
- Business Continuity Management
- Concetti generali ISO 22301:2019
- Business Impact Analysis
- Piani di Continuità Operativa

La Gestione dei Rischi - Le Minacce

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



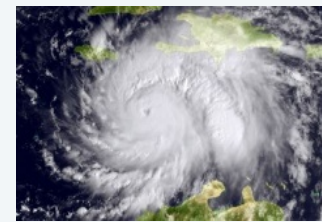
Cyber Attack



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, ...)

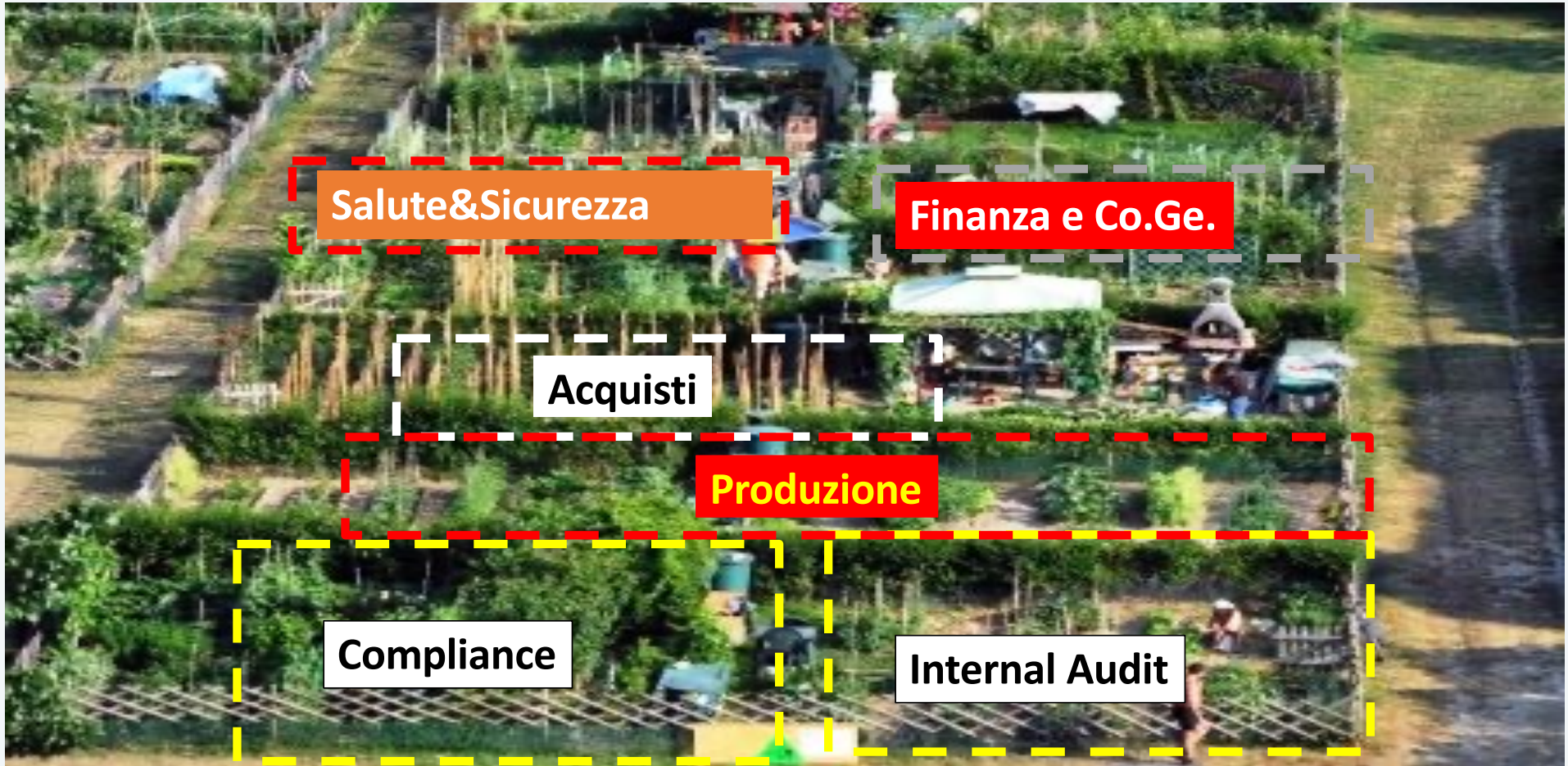
Rischi Emergenti

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

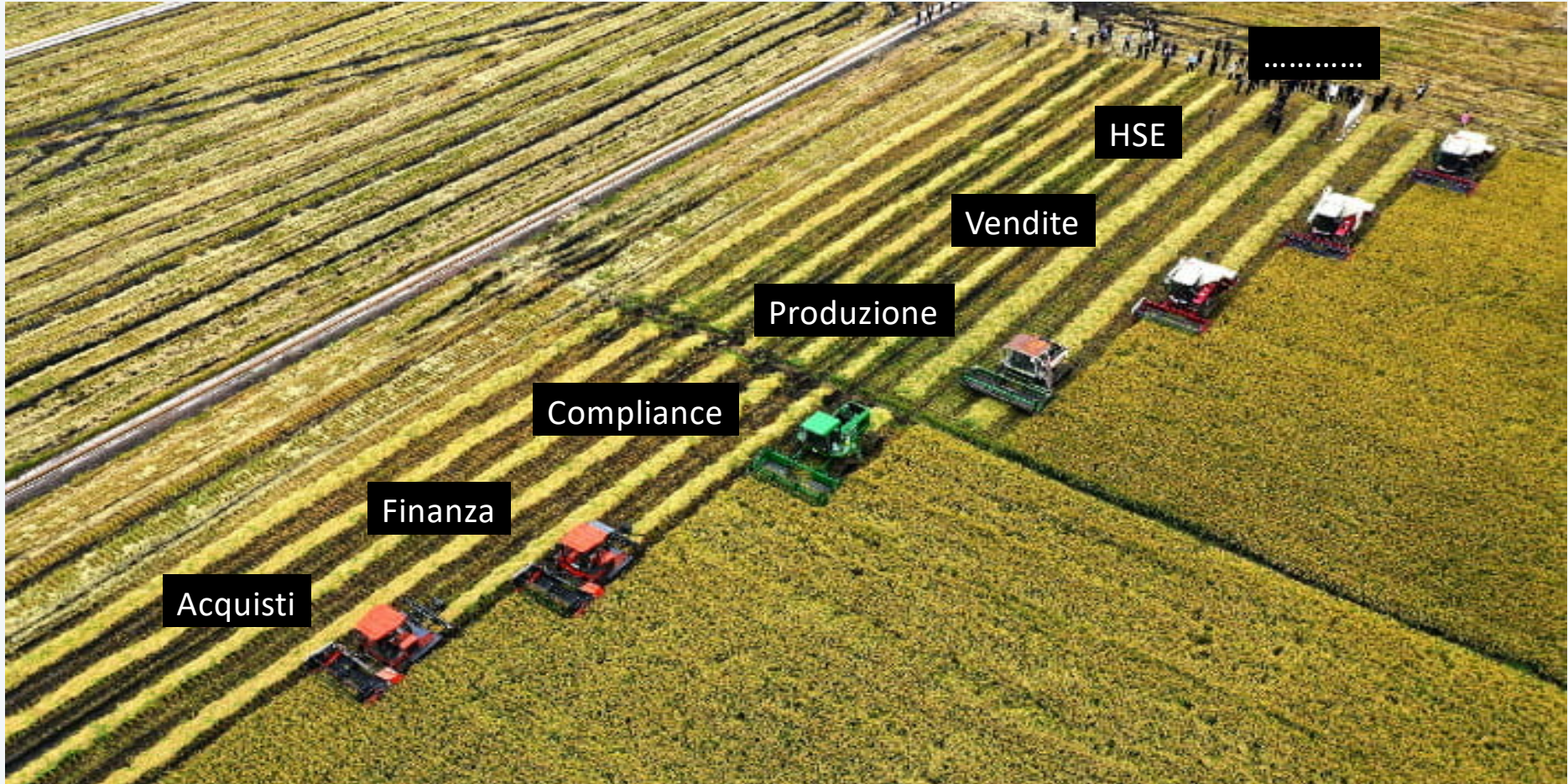




Approccio Silos vs ERM



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

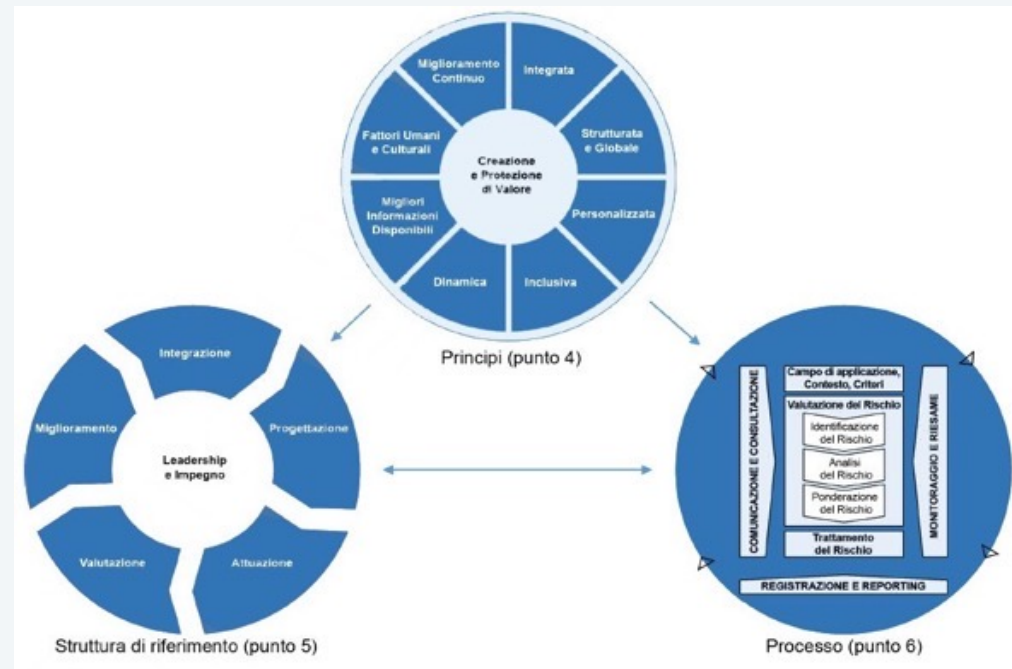
SCOPO E CAMPO DI APPLICAZIONE

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

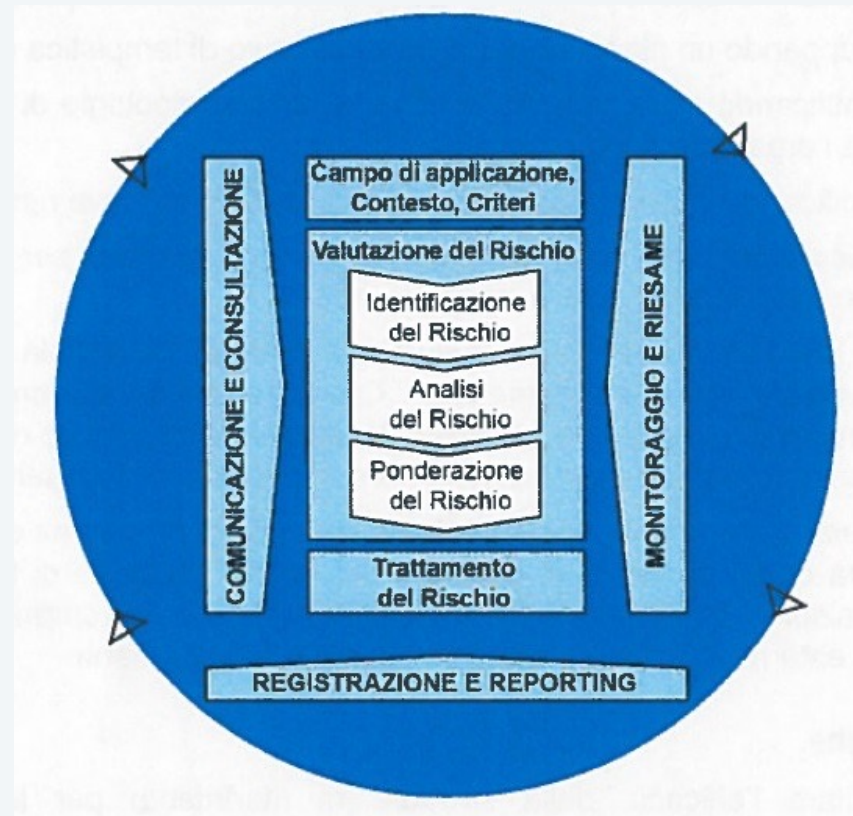
Tale modello decisionale può essere mantenuto durante tutta la vita dell'organizzazione e può essere applicato a tutti i livelli decisionali

Principi - Struttura - Processo



Fonte ISO 31000:2018

Il Processo di Risk Management



Non è sufficiente essere conformi alle leggi?

Tsunami 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

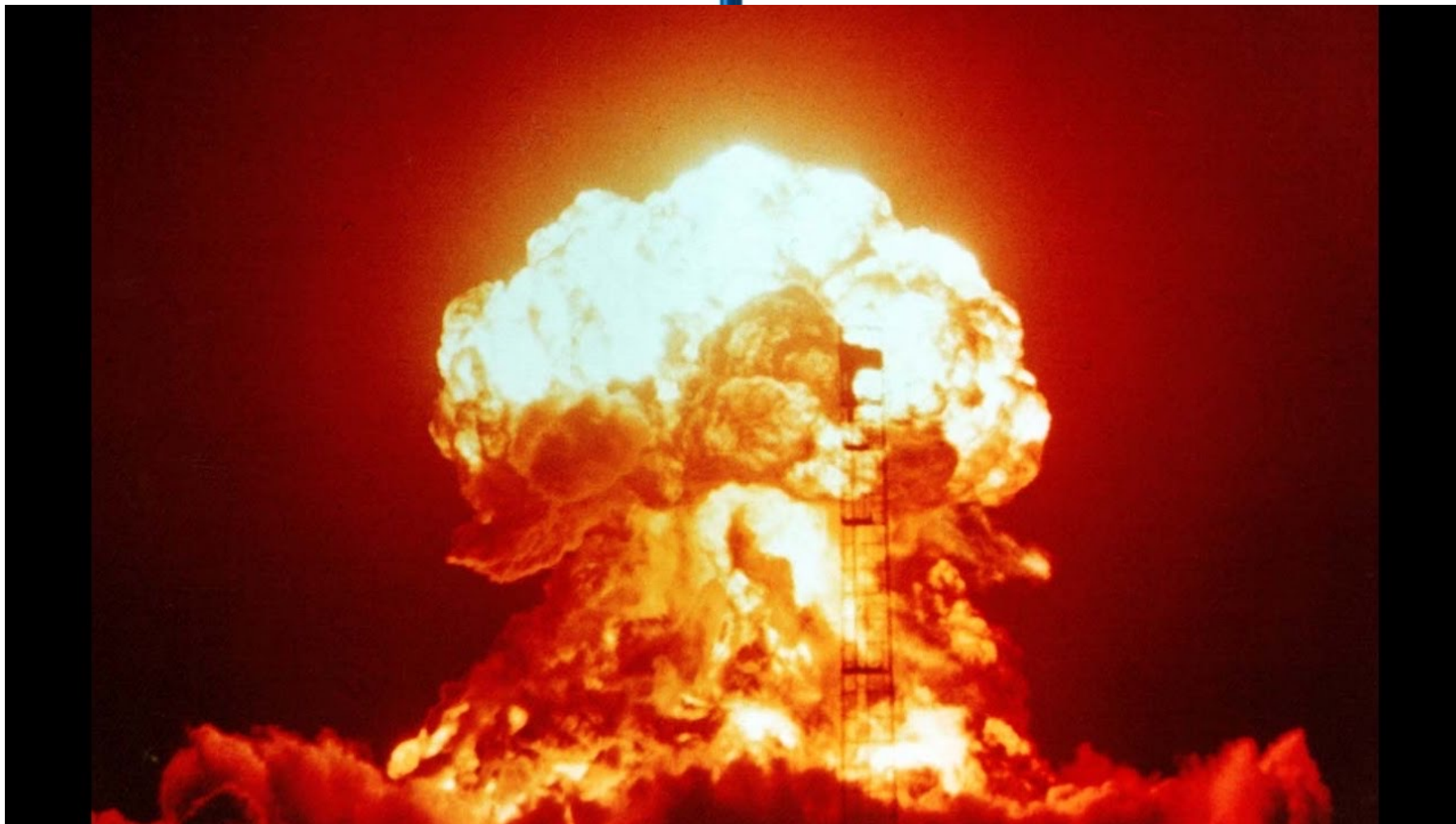
- Analizzare gli stati in cui si trova il/i sistema/i economico/i con il/i quale/i operiamo o da cui potremmo dipendere, «trailblazer analysis»
- Analisi dei rischi e valutazione delle esposizioni ai rischi della nostra organizzazione costante «pass through analysis» sui drivers esterni/interni
- Valutazione 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

Moto Browniano

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

Organized

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

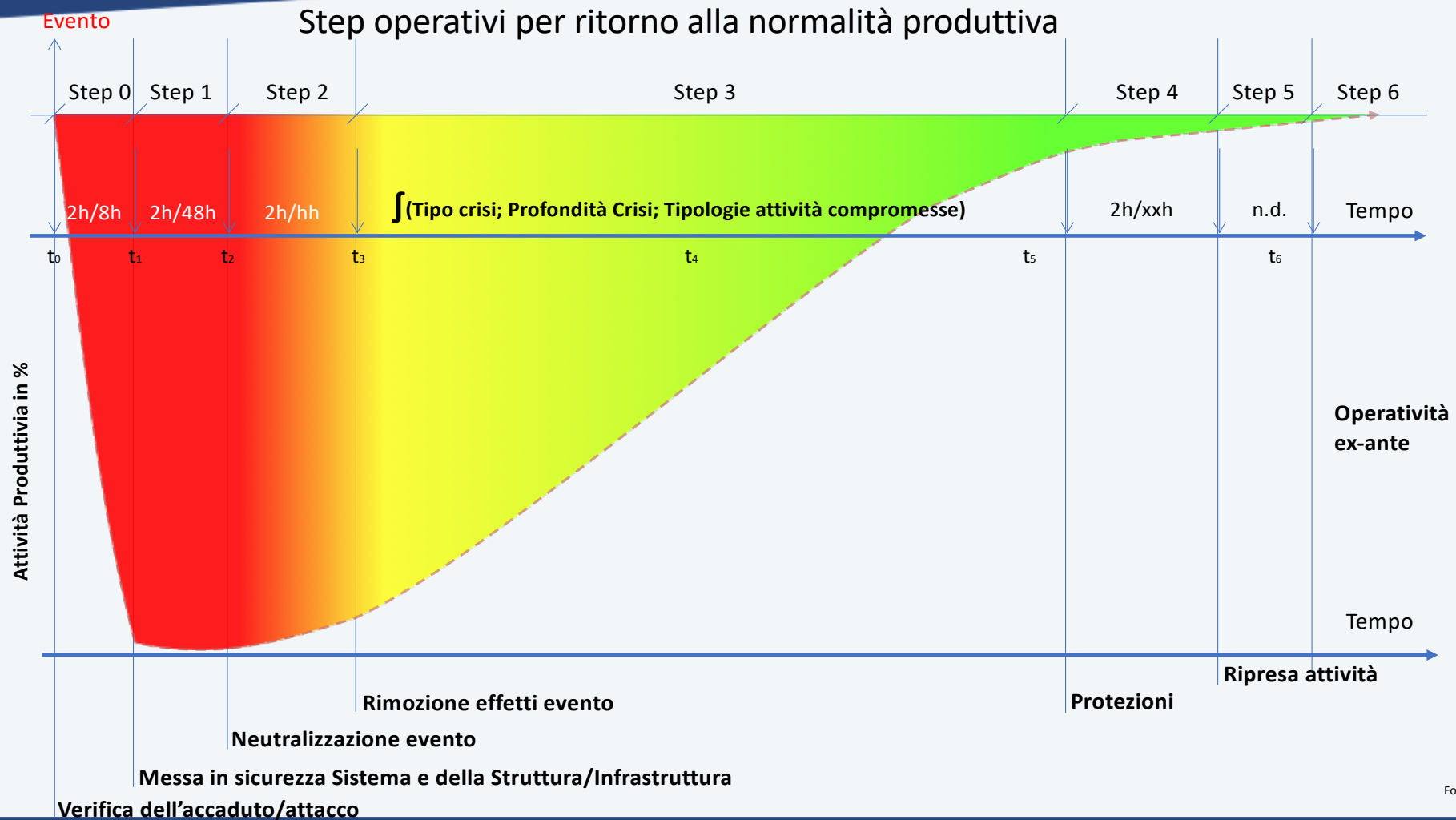
Quanto il CHAOS irrompe...

...attivazione piano

- Verificare l'accaduto/attacco
- Mettere in sicurezza Sistema, Struttura/Infrastruttura
- Neutralizzare l'evento
- Rimuovere effetti evento
- Proteggere
- Ripartire

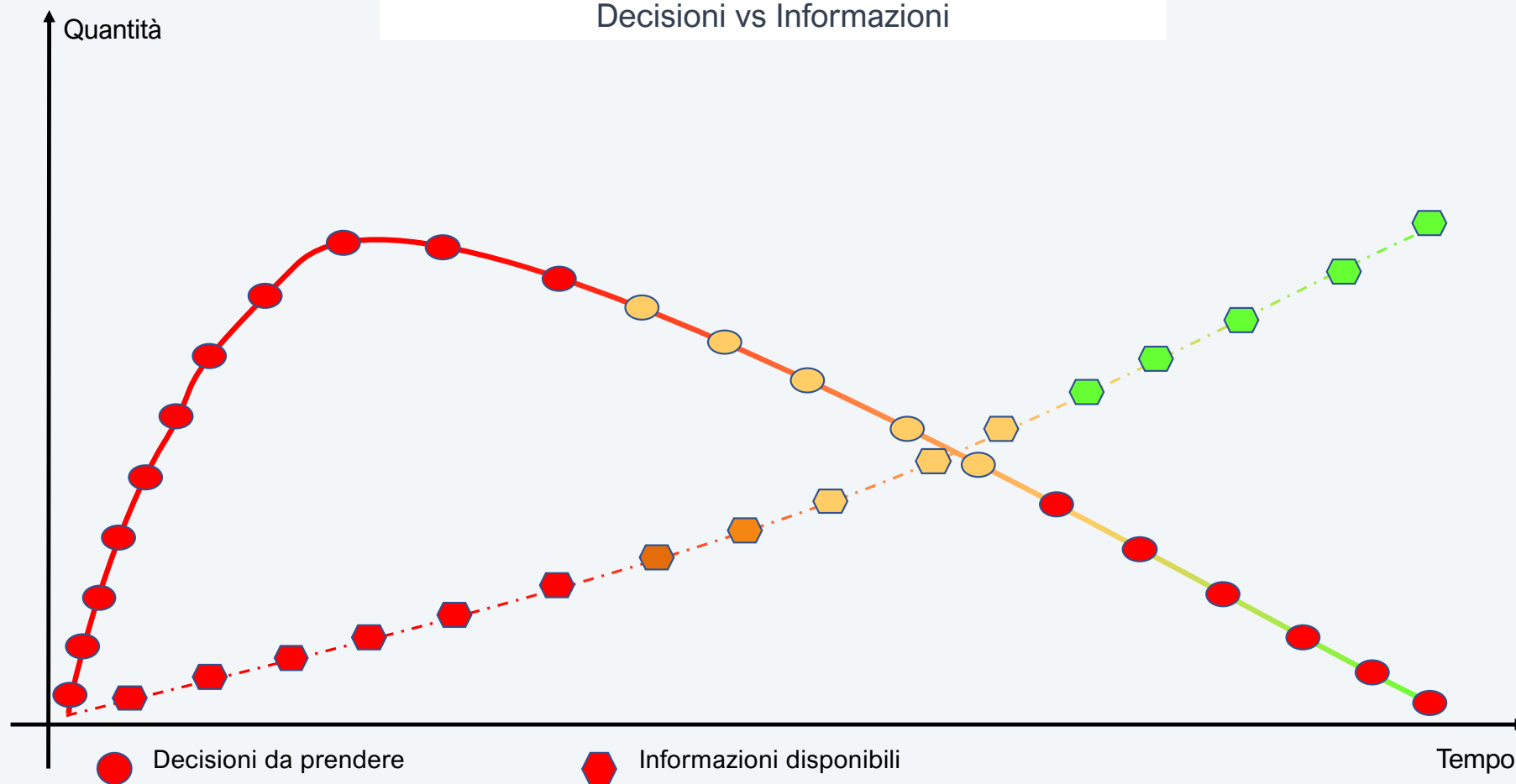
dobbiamo avere in mente che durante una crisi



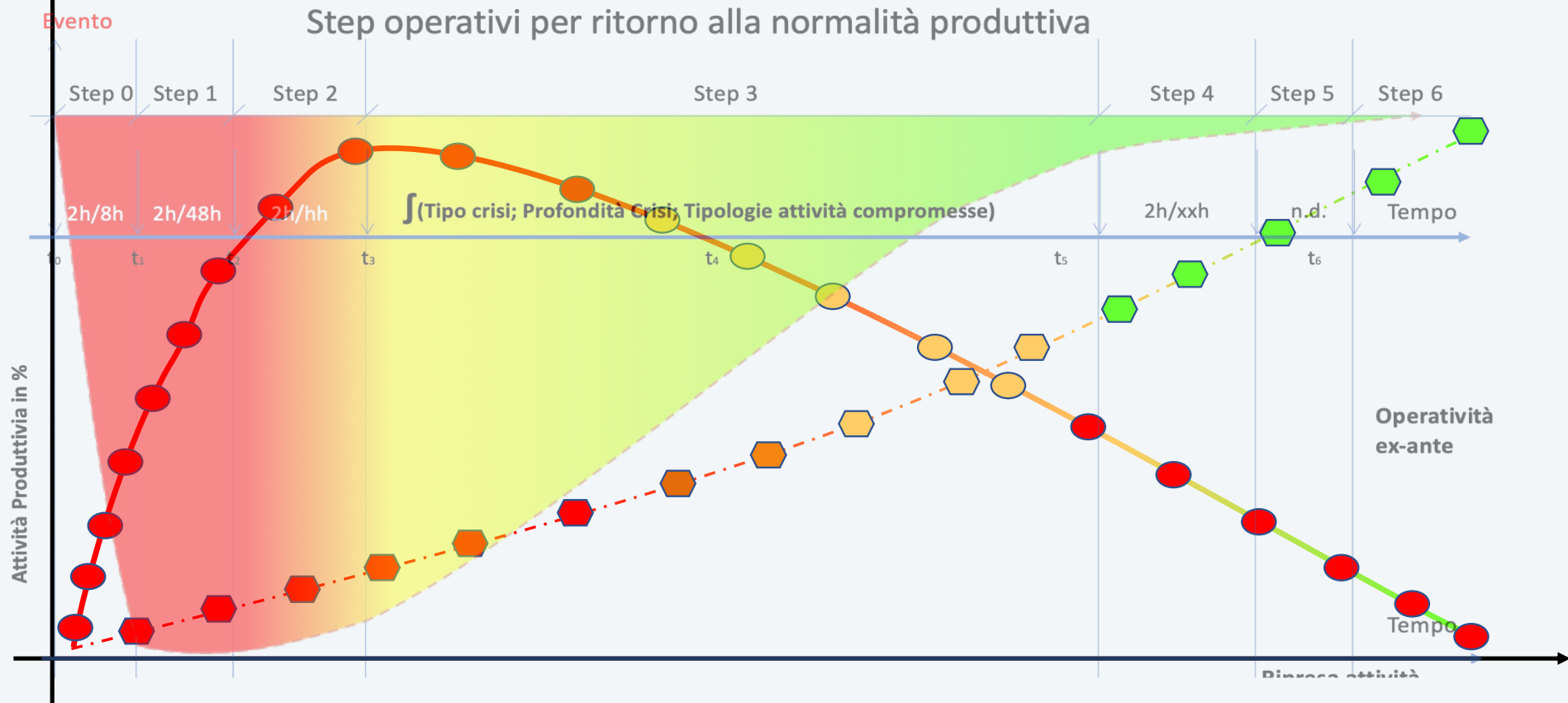


Fonte: G.Lucietto

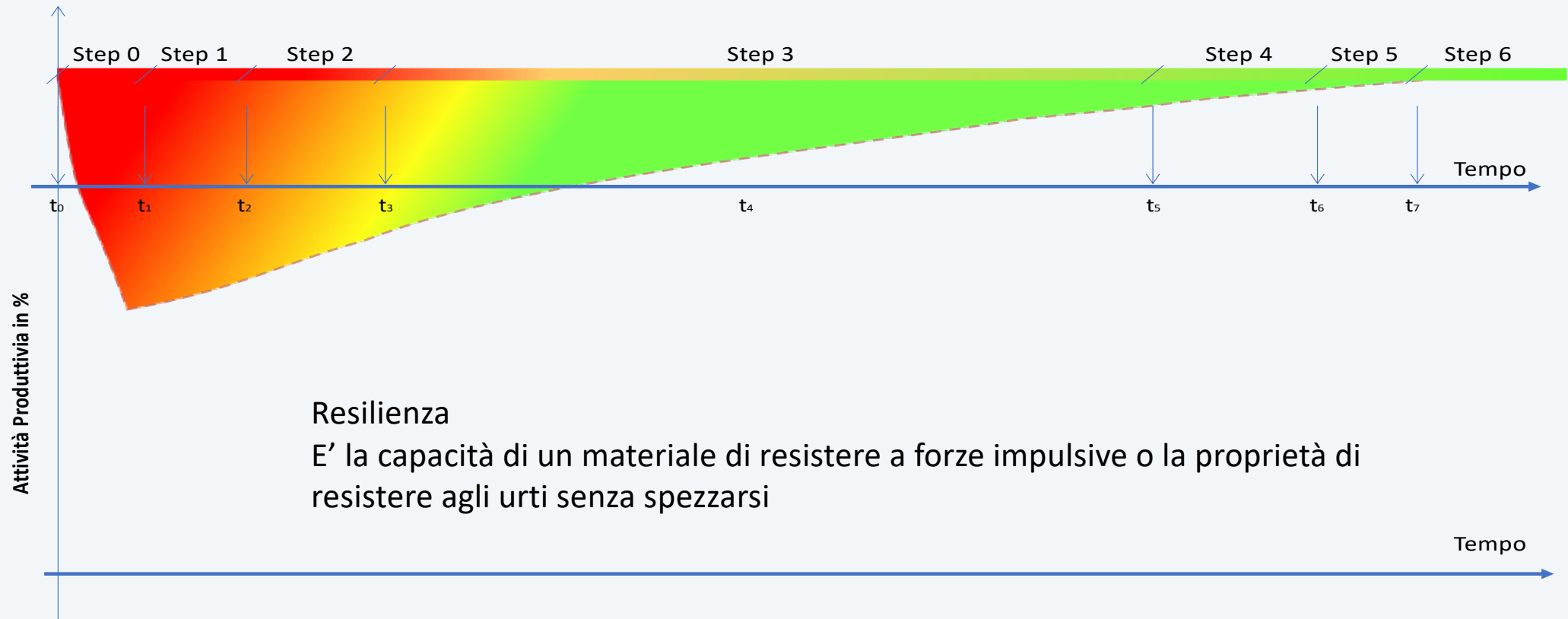
Decisioni vs Informazioni



Decisioni vs Informazioni



Step operativi per ritorno alla normalità

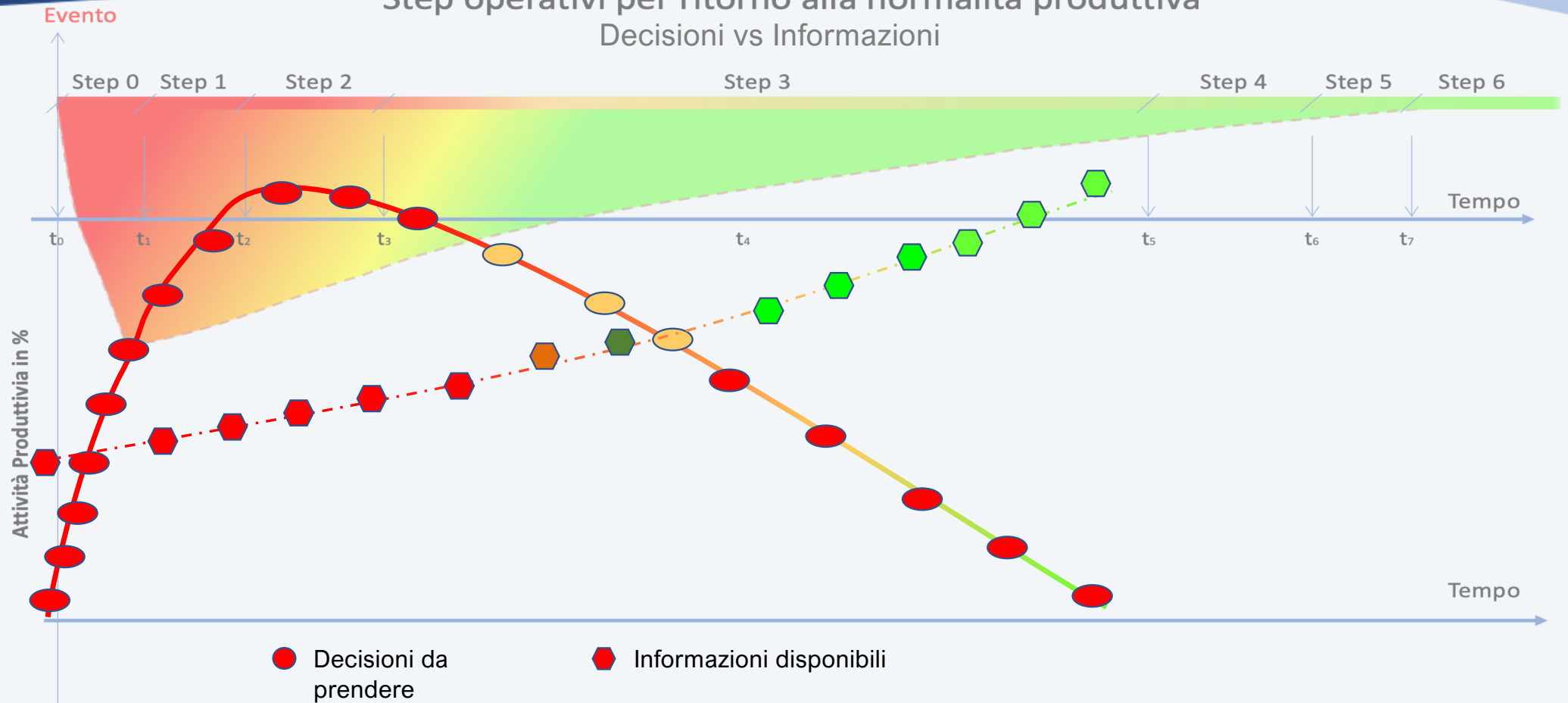


Resilienza

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

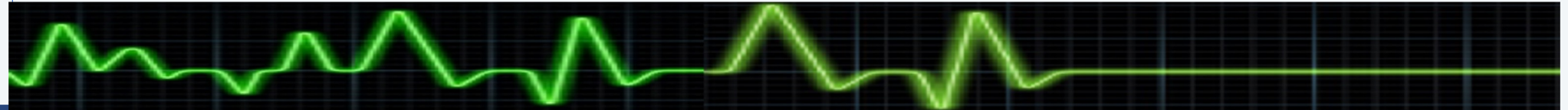
Fonte: G. Lucietto

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

**Facility
Management**

**Legal &
Compliance
Management**

**Infrastructure
Management**

**Finance
Management**

**Business
Strategy**

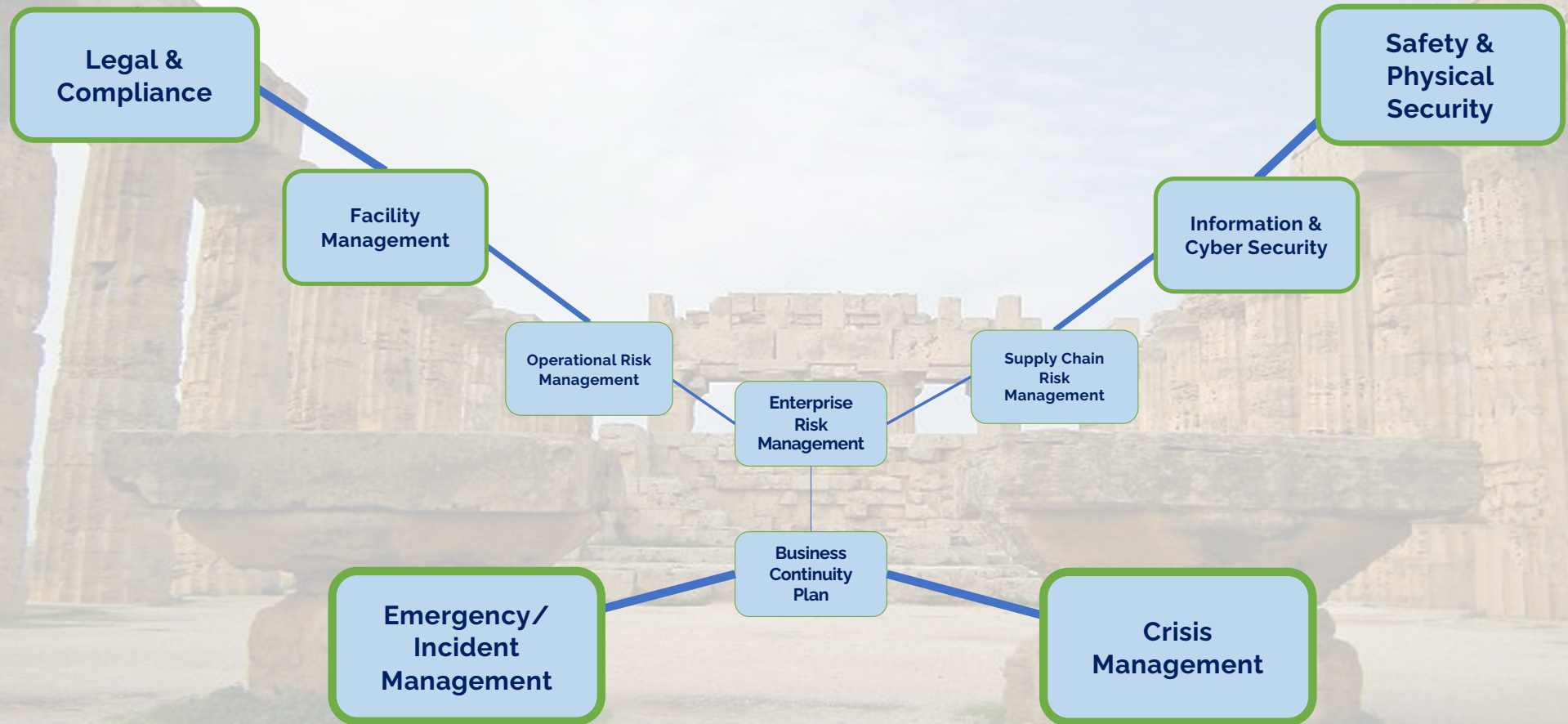
**Supply Chain
Management**

**Physical
Security**

**ICT
Management**

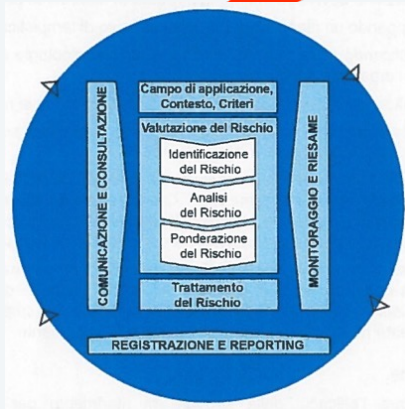
Safety

Strategie Operative di Difesa



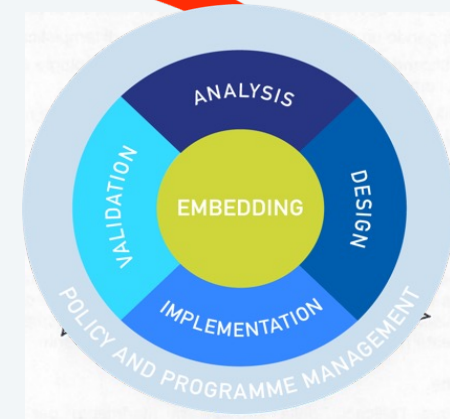
lavorano insieme con un unico obiettivo:
garantire la resilienza

1- Risk Management



ISO 31000:2018 - Process

2- Business Continuity



Rimando a GPG2018 BCI

adattamento continuo

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 22301:2019

Quali rischi



Fonte Allianz 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

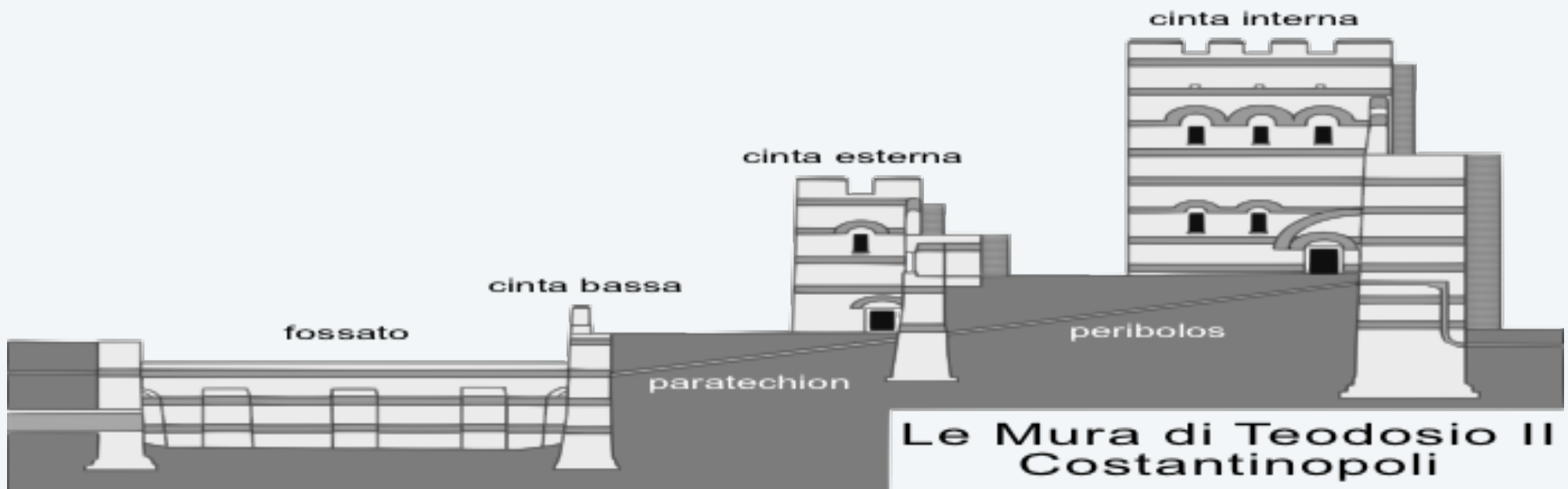
Strutture - Servizi
Personale Operativo

Presidi Organizzativi II° livello

Organizzazione - Processi - Controlli
Monitoraggio Rischi

Presidi Giuridici III° Livello

Vigilanza e Controllo
O.d.V- Internal Audit





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

Bio



Consulente in Risk Management & Business Continuity Management – Risk Consulting Network

Docente Corso di Perfezionamento in Risk Management - Università di Verona – Dip.to di Economia Aziendale

Professore a Contratto - Corso di Supply Chain Risk Management - Università di Verona – Dip.to di Scienze Giuridiche

Certified Business Continuity Professional - Disaster Recovery International Institute - USA The DRI

Certified International Instructor - Disaster Recovery International Institute - USA The DRI

Associate in Risk Management - The Institute - USA Philadelphia

Associate Member Business Continuity Institute - UK The BCI

Membro Consiglio Direttivo - Membro Comitato Formazione ANRA

Membro Commissione UNI - Risk Management

Laurea in Economia e Commercio - Università di Verona

Docente Corso Risk Management - Università di Parma

Docente ANRA - Moduli I, II, V

Docente ANRA corso ANRA/DRI - Business Continuity BCLE2000

