**VII CONVEGNO NAZIONALE AICQ SALUTE E SICUREZZA**

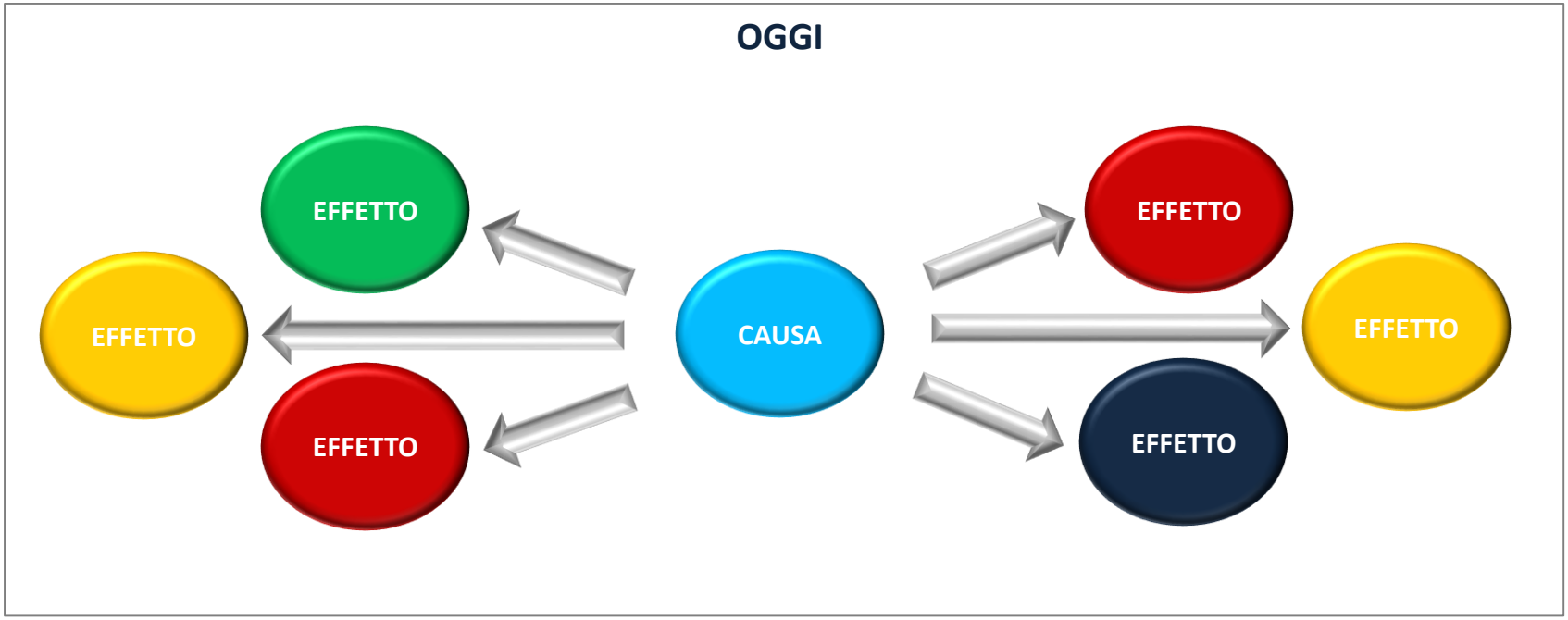
# La Gestione delle Emergenze
# Valutazione dei Rischi e Piani di Recovery
## Ruoli e Responsabilità nei Sistemi di Gestione Salute e Sicurezza

**NAPOLI, Centro Formazione e Convegni INAIL Villa Colonna Bandini**
**Mercoledì, 31 maggio 2017**

IL SISTEMA DI GESTIONE DELLA CONTINUITÀ OPERATIVA

Relazione a cura di Gianna Detoni – FBCI, BCI Italy Forum Leader

# L'EVOLUZIONE NELL'APPROCCIO AL RISCHIO



# CAMBIA IL CONCETTO DI RISCHIO

| Nelle società pre-moderne… | Nelle società avanzate… |
|---|---|
| …era soprattutto legato ad **eventi naturali** esterni all'individuo | …appare **insito nell'uomo** e quindi legato alle sue **decisioni** |

# TERMINOLOGIA: L'APPROCCIO AMERICANO

**Anni '70**

Il concetto di **«disastro»** è soprattutto legato ai primi studi americani sulle **calamità naturali** e tale approccio ha influenzato a lungo la riflessione scientifica

**Anni '80 - '90**

Rimane la differenza fondamentale tra scuola americana ed europea sul concetto di disastro, in USA sempre inteso come evento naturale **improvviso** e **imprevisto**

# TERMINOLOGIA: L'APPROCCIO EUROPEO

In Europa si intende un processo con le stesse caratteristiche dell'Emergenza, ma che può essere un evento di qualsiasi natura

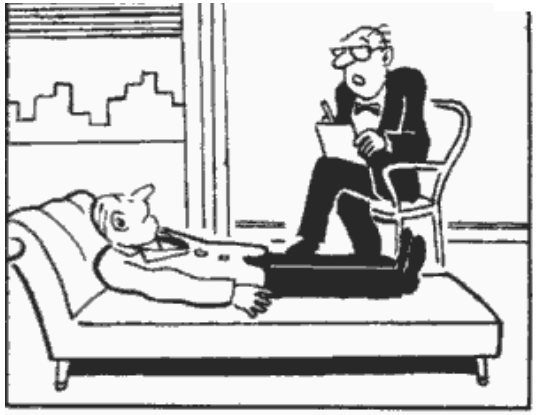
**CALAMITÀ NATURALI**

**SITUAZIONE POLITICA**

**ATTACCHI TERRORISTICI**

# RESILIENZA AL RISCHIO - DEFINIZIONE

**Resilienza:** capacità di un materiale di resistere a forze impulsive



— Intende dire che in un momento di pazzia ha pensato di essere sano?

Un'organizzazione è resiliente quando ha la capacità di cambiare e adattarsi prima che il rischio di riferimento la costringa a farlo

# L'IMPORTANZA DI CONTINUARE A INNOVARE

## Siete troppo **impegnati** per innovare?

$$R© = F(n^m)$$

La resistenza al cambiamento in una Organizzazione è pari al numero dei dipendenti elevato alla potenza con il numero dei Manager

Fonte: Magnus Lindkvist, «The attack of the unexpected»

# SAPER GESTIRE IL CAMBIAMENTO

aicq
Associazione Italiana Cultura Qualità
Comitato Salute e Sicurezza

BLOCKBUSTER®

Kodak

NOKIA
Connecting People

BlackBerry®

Olivetti

PAN AM

MOTOROLA

Polaroid

xerox

HUMMER®
LIKE NOTHING ELSE.™

Fonte: www.businesspundit.com/10-businesses-that-failed-to-adapt/11/

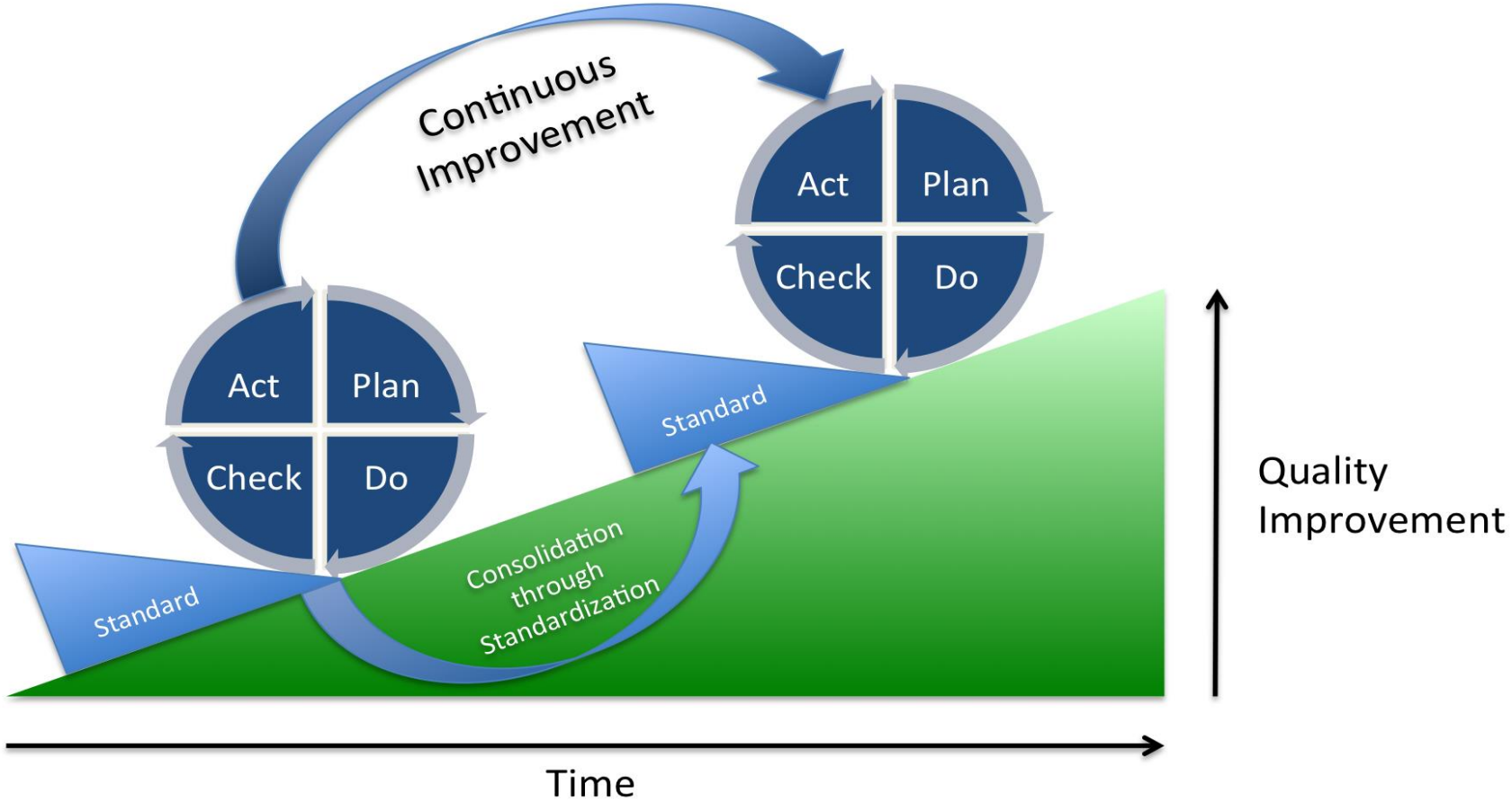
aicq
Associazione Italiana Cultura Qualità
Comitato Salute e Sicurezza

# CENNI NORMATIVI: GLI STANDARD INTERNAZIONALI

*Una panoramica delle Norme e degli Standard internazionali vigenti*

# NORMA ISO 22301:2012 - SOCIETAL SECURITY

## Requisiti per il Sistema di Gestione della Continuità Operativa



# ISO 22301:2012 DIVENTA «EN»

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**

# STANDARD INTERNAZIONALI

ISO 22301, 22313:2012
Business Continuity Management Systems

ISO 22316:2017
Organizational Resilience

ISO 22317:2015
Guidelines for Business Impact Analysis (BIA)

ISO 22318:2015
Guidelines for Supply Chain Continuity

# BUSINESS CONTINUITY: GIÀ OBBLIGATORIA

Istituzioni finanziarie

Infrastrutture critiche

Pubblica Amministrazione

Basilea II – rischio operativo Solvency II - Assicurazioni

D. Lgs. 61/2011

D. Lgs. 235/2010

# BUSINESS CONTINUITY: GIÀ OBBLIGATORIA

Istituzioni finanziarie

Basilea II
Circ. 285 di Banca d'Italia
Solvency II - Assicurazioni

Servizi assicurativi

D. Lgs. 61/2011

Pubblica amministrazione

D. Lgs. 235/2010

# IL VALORE AGGIUNTO DELLA CONTINUITÀ OPERATIVA

*Più resilienti, più efficienti, più profittevoli…*

# BUSINESS CONTINUITY: È PRATICATA DA SEMPRE

- Si applica la scienza al **buon senso**
- Facilita la lettura di **governance** complesse
- Si ottimizza il costo della **prevenzione**
- Si guardano i **processi** in modo critico
- Si guardano i **clienti** in modo critico
- Si guardano i **profitti** in modo critico
- Si comparano **prodotti e servizi** in modo critico

# LE FASI DI IMPLEMENTAZIONE DEL BCMS

aicq
Associazione Italiana Cultura Qualità
Comitato Salute e Sicurezza

Business Continuity Institute
Licensed Training Partner

GESTIONE DELLA POLICY E DEL PROGRAMMA — **FASE 1**

INCORPORARE LA BC NELLA CULTURA AZIENDALE — **FASE 2**

ANALISI — **FASE 3**

PROGETTAZIONE — **FASE 4**

IMPLEMENTAZIONE — **FASE 5**

CONVALIDA — **FASE 6**

# PROGRAMMA O PIANO?

La gestione della continuità operativa è definita come un **processo manageriale olistico**

Fonte: ISO 22301:2012

- Il Piano è «solo» un output
- Il Piano in sé è sopravvalutato
- Il Piano in sé non ci dice nulla

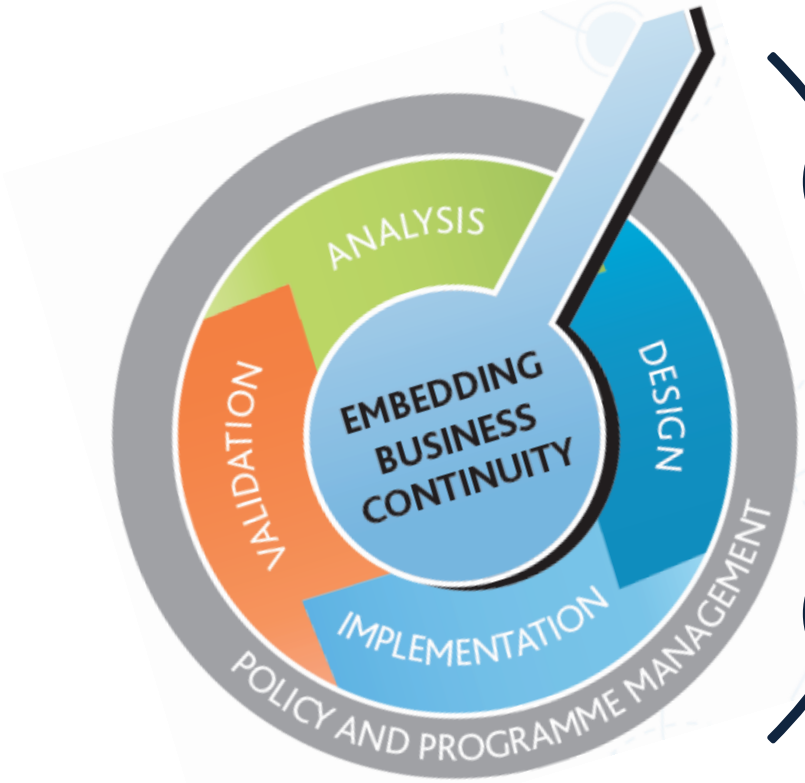
# POLICY & GESTIONE DEL PROGRAMMA

È la prima fase del ciclo di vita della business continuity e serve a definire in maniera formale la politica organizzativa, il campo di applicazione del Programma di continuità, i ruoli e le responsabilità

- Leadership del Top Management
- Chiarezza degli obiettivi
- Nomina di persone competenti

# INCORPORAZIONE DELLA BUSINESS CONTINUITY

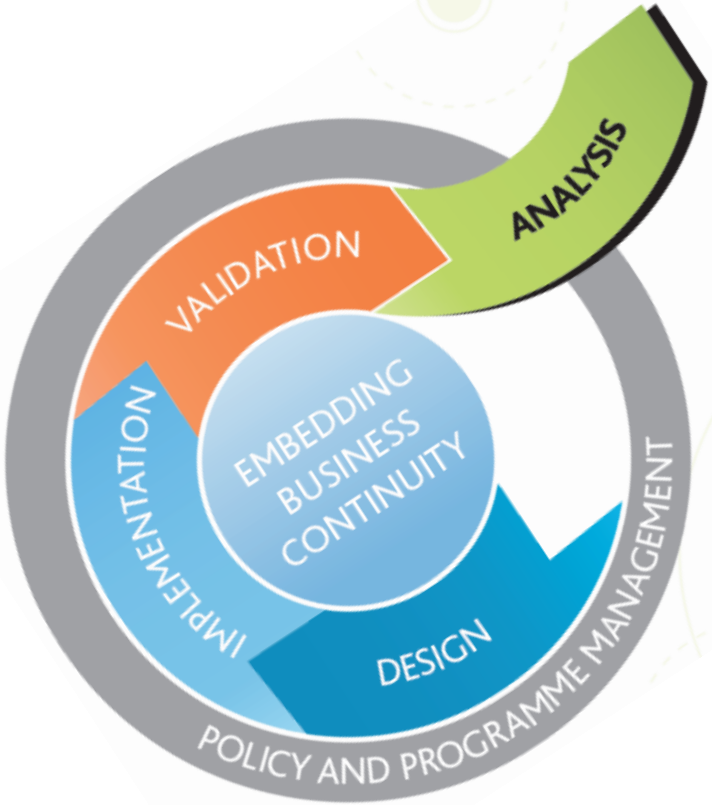
È una fase molto importante della business continuity per incorporare il tema della resilienza nel DNA dell'organizzazione




- Allineamento del linguaggio
- Sensibilizzazione a 360°
- Coinvolgimento nei test

# ANALISI

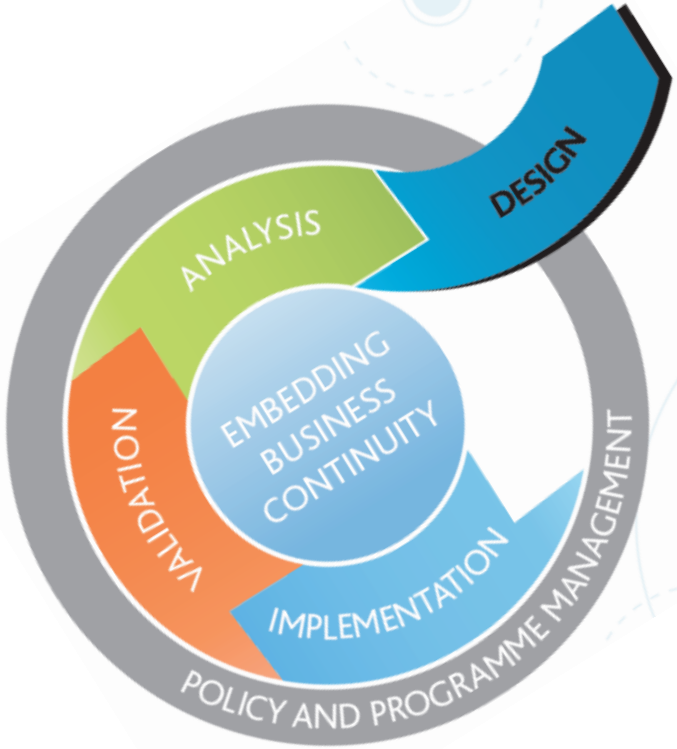
È la prima pratica professionale «tecnica», di fatto rappresenta l'architrave del Sistema di Gestione della Continuità Operativa ed è composta dalla Business Impact Analysis, Analisi delle Risorse e dall'Analisi delle Minacce




- Analisi del processo end-to-end
- Comparabilità dei risultati
- Modello di BIA quali-quantitativo

# PROGETTAZIONE

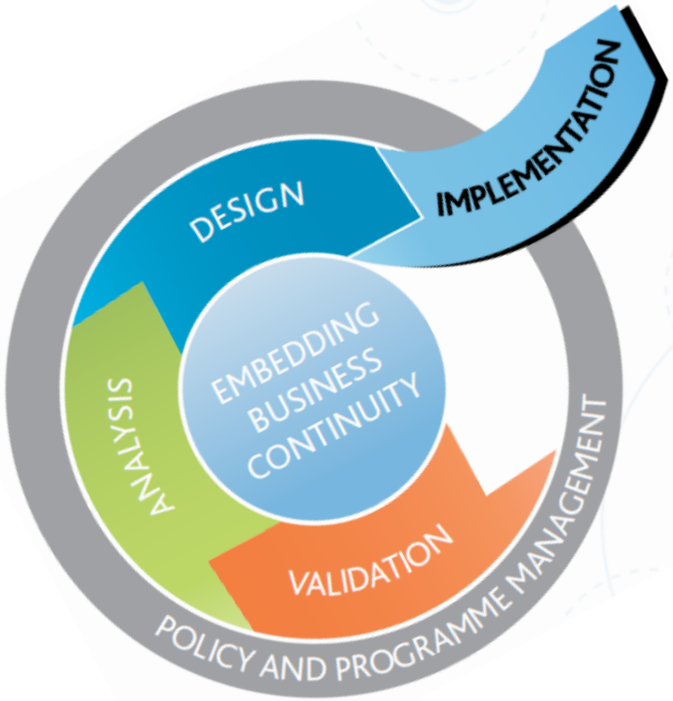
Questa fase costituisce un passaggio intermedio fondamentale tra il consolidamento delle Analisi e l'implementazione dei Piani, garantendo omogeneità alle strategie e alle tattiche di continuità, come alle misure di mitigazione delle minacce




- RTO e RPO realistici
- Coerenza tra strategie/tattiche
- Economie di scopo

# IMPLEMENTAZIONE

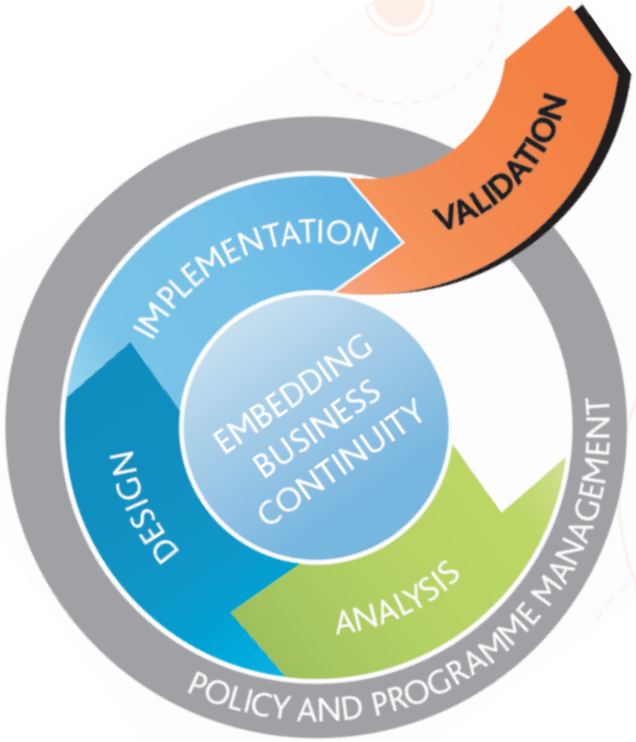
Solo in questa quinta fase si predispongono i Piani di continuità a livello strategico (ad es.: Piano di Crisi), tattico (ad es.: Piani funzionali o Disaster Recovery Plan) e operativo (Piani di emergenza) per delineare la risposta a un evento critico




- Piani diretti, concisi e rilevanti
- Piani adattabili
- Piani costantemente aggiornati

# CONVALIDA

Nulla di quanto fatto in precedenza può essere considerato valido se non si effettuano le opportune esercitazioni, le verifiche di audit e la revisione delle performance del Programma di business continuity




- Test realistici e inclusivi
- Auditor certificati e competenti
- BC nel sistema incentivante

Associazione Italiana Cultura Qualità
Comitato Salute e Sicurezza

# LA BUSINESS CONTINUITY MALE INTERPRETATA

*Imparare dagli errori più comuni….*

# COSA **NON** È LA BIA?

~~Valutazione del processo~~

~~Valutazione dei profitti~~

~~Valutazione di efficienza~~

~~Valutazione delle risorse~~

~~Valutazione del manager~~

~~Valutazione del fornitore~~

La Business Impact Analysis è il **processo di analisi delle attività e degli effetti che un'interruzione del business può avere su di esse**

Fonte: ISO 22301:2012

# SOGGETTIVITÀ VS. OGGETTIVITÀ

## A = ANALISI

Nel corso della BIA occorre eliminare le opinioni soggettive al fine di rendere i risultati il più possibile **oggettivi** e **comparabili**

# CRITICITÀ VS. IMPORTANZA

**CRITICO ≠ IMPORTANTE**

**CRITICO = URGENTE**

Bozza di RTO

Bozza di RPO

# TIENI A MENTE GLI OBIETTIVI DELLA BIA

- Stabilire le **priorità** per la protezione e il recupero dei processi critici in caso di interruzione
- Fornire un **fondamento logico** per la definizione di strategie e tattiche omogenee nell'organizzazione
- Produrre dati oggettivi in grado di **indirizzare gli investimenti** in continuità e resilienza
- Determinare una bozza di **Recovery Time Objective (RTO)** e **Recovery Point Objective (RPO)**

# SVILUPPA UN MODELLO CHE…

…non sia esclusivamente qualitativo o quantitativo

…tenga conto dei requisiti di continuità

…provochi riflessioni sulle minacce

…consenta l'aggregazione dei risultati

# SVILUPPA UN MODELLO CHE…

…non sia esclusivamente

…tenga
dei req
conti

vochi
ni sulle
acce

**La costruzione di un modello di BIA efficace è il passaggio più complesso del BCMS**

l'aggregazione dei risultati

# RESISTI ALL'IMPULSO

Non considerare le probabilità di un evento avverso

Non considerare le strategie di continuità

Non considerare le tattiche di continuità

Non considerare le misure di mitigazione delle minacce

Non pensare al Piano di continuità

**Guida il process-owner nelle giuste riflessioni**

# …E I REQUISITI DI CONTINUITÀ?

QUANTE PERSONE E QUALI?

▼

QUANTE RISORSE TECNOLOGICHE E QUALI?

▼

QUALI FORNITORI?

▼

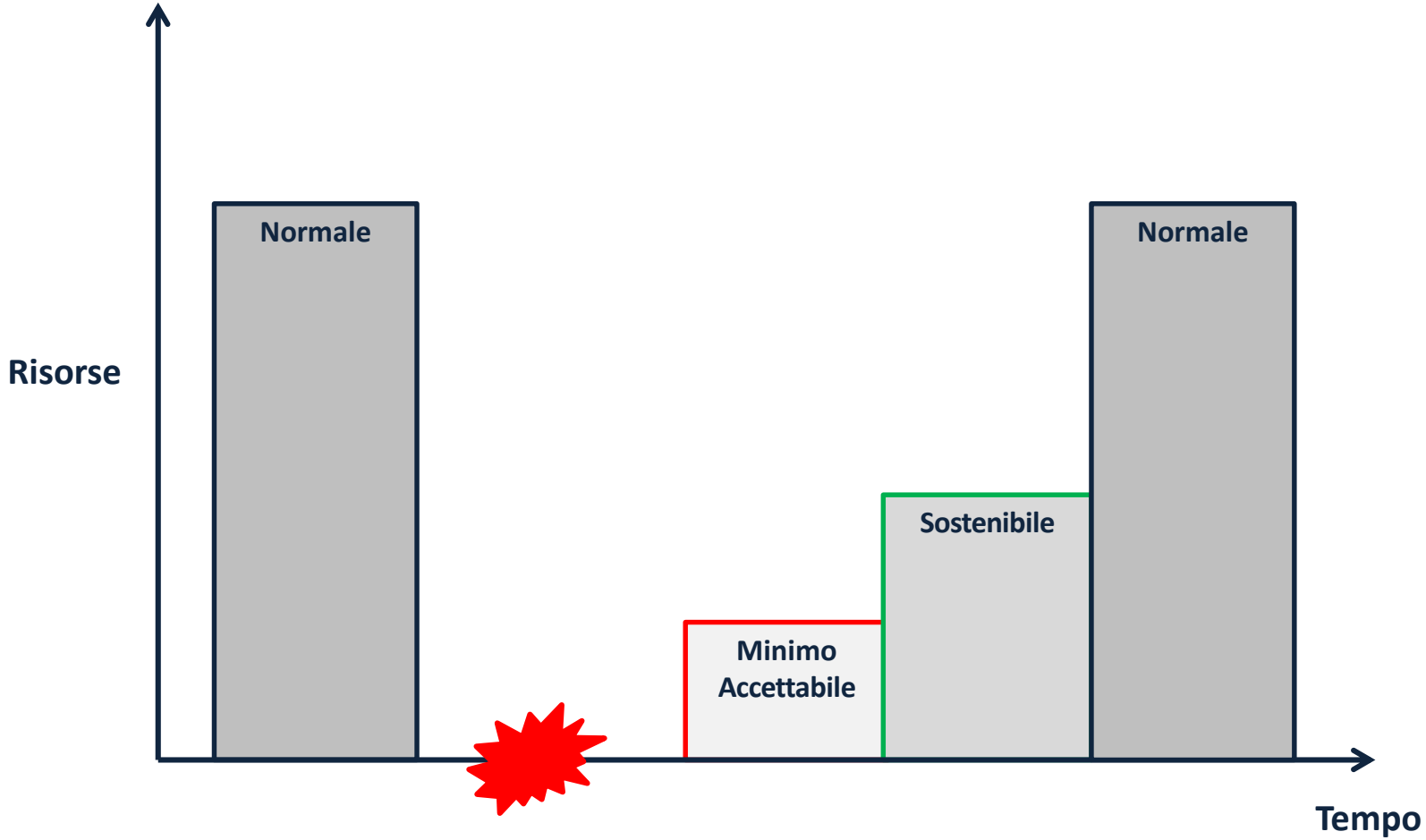
ANALISI DELLE MINACCE

▼ ▼

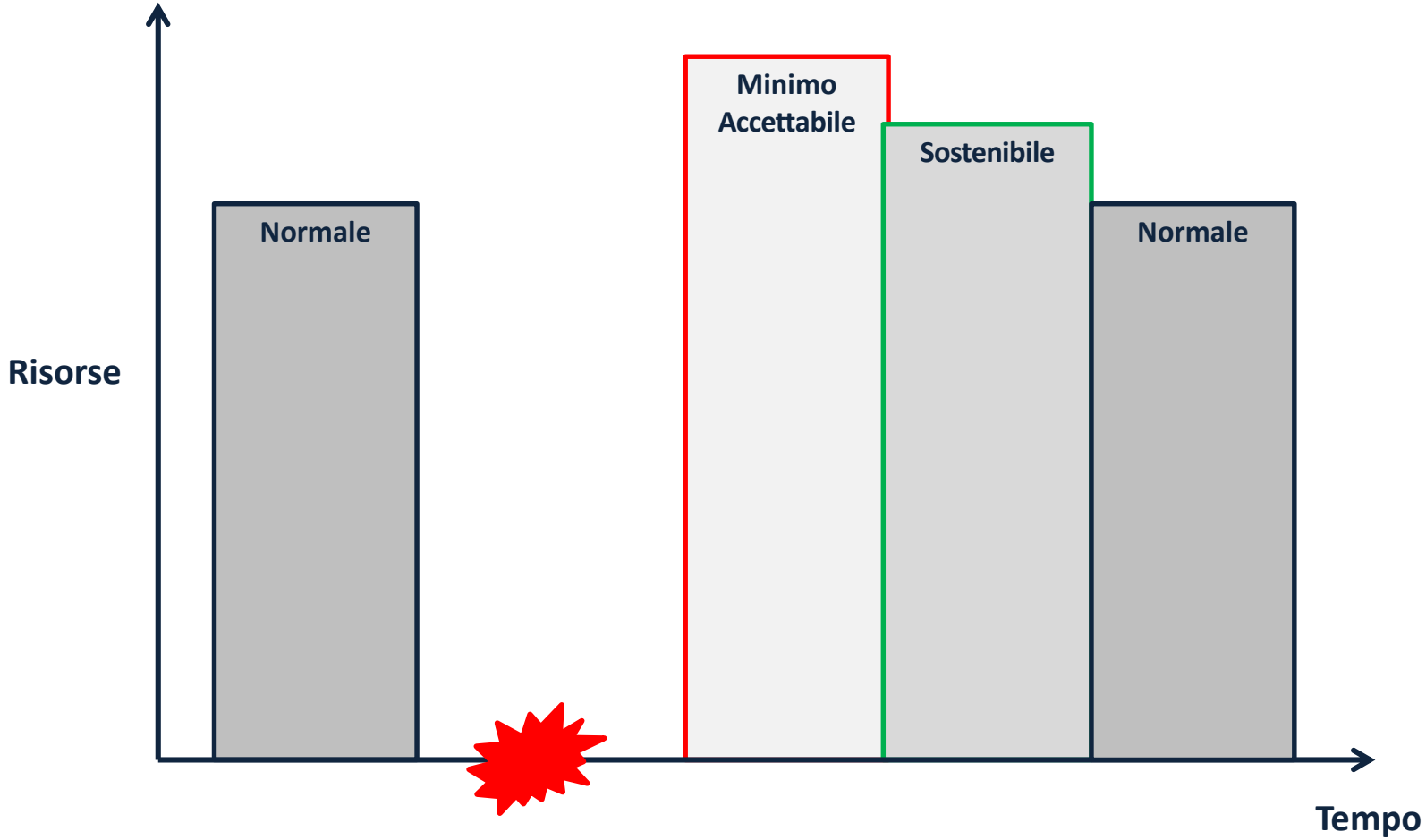
SINGOLI PUNTI DI CEDIMENTO

CONCENTRAZIONI INACCETTABILI DI RISCHIO

# REQUISITI PER LE RISORSE



# REQUISITI PER LE RISORSE – OSSERVAZIONI



# IL PIANO DI CONTINUITÀ OPERATIVA

Il piano di Business Continuity

- È disponibile **fuori** dal sito dell'organizzazione
- È **facile** da leggere e da scorrere
- **Non** è un documento di **formazione**
- Bisogna **eliminare** la **letteratura morta**

# IL BESTIARIO NEL MONDO DELLA BC

Ho il Disaster Recovery – sono a posto

Ho grande capacità di reazione all'emergenza

Ho un gruppo elettrogeno che ricarico se necessario

Nella mia zona non ho rischi di catastrofi naturali

È troppo costosa... Solo i big se la possono permettere

**Ho dato in outsourcing i miei processi critici…**

Associazione Italiana Cultura Qualità
Comitato Salute e Sicurezza

# IL SISTEMA DI GESTIONE DELLA CONTINUITÀ OPERATIVA

*I fattori critici di successo e gli errori da evitare nell'implementazione del programma*

*GIANNA DETONI – FBCI – BCI ITALY FORUM LEADER*