UNIVERSITA DEGLI STUDI DI ROMA «TOR VERGATA»
CORSI SECURITY MANAGEMENT

CORSO DI PERFEZIONAMENTO IN «SECURITY MANAGER»

CORSO DI FORMAZIONE IN «PROFESSIONISTA DELLA SECURITY»

3 - 4 DICEMBRE 2021

GIANNA DETONI

Introduzione alle strategie di gestione e di controllo dei rischi

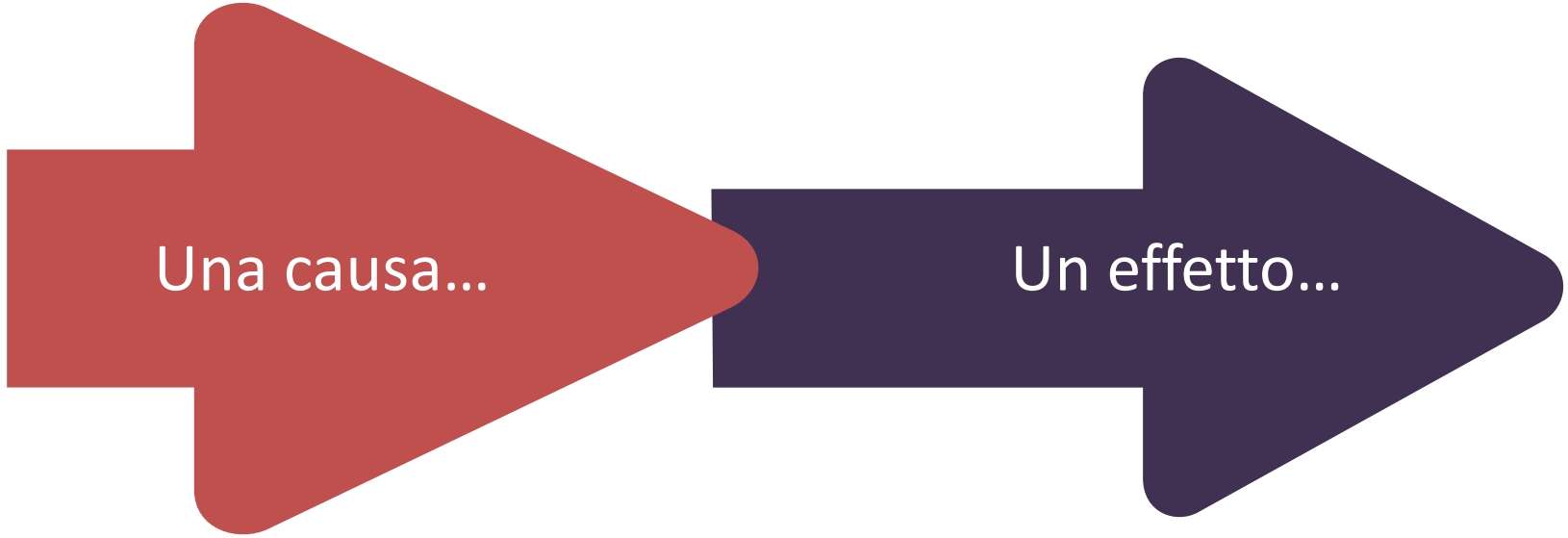
Enterprise Risk Management

Crisis Management e Business Continuity

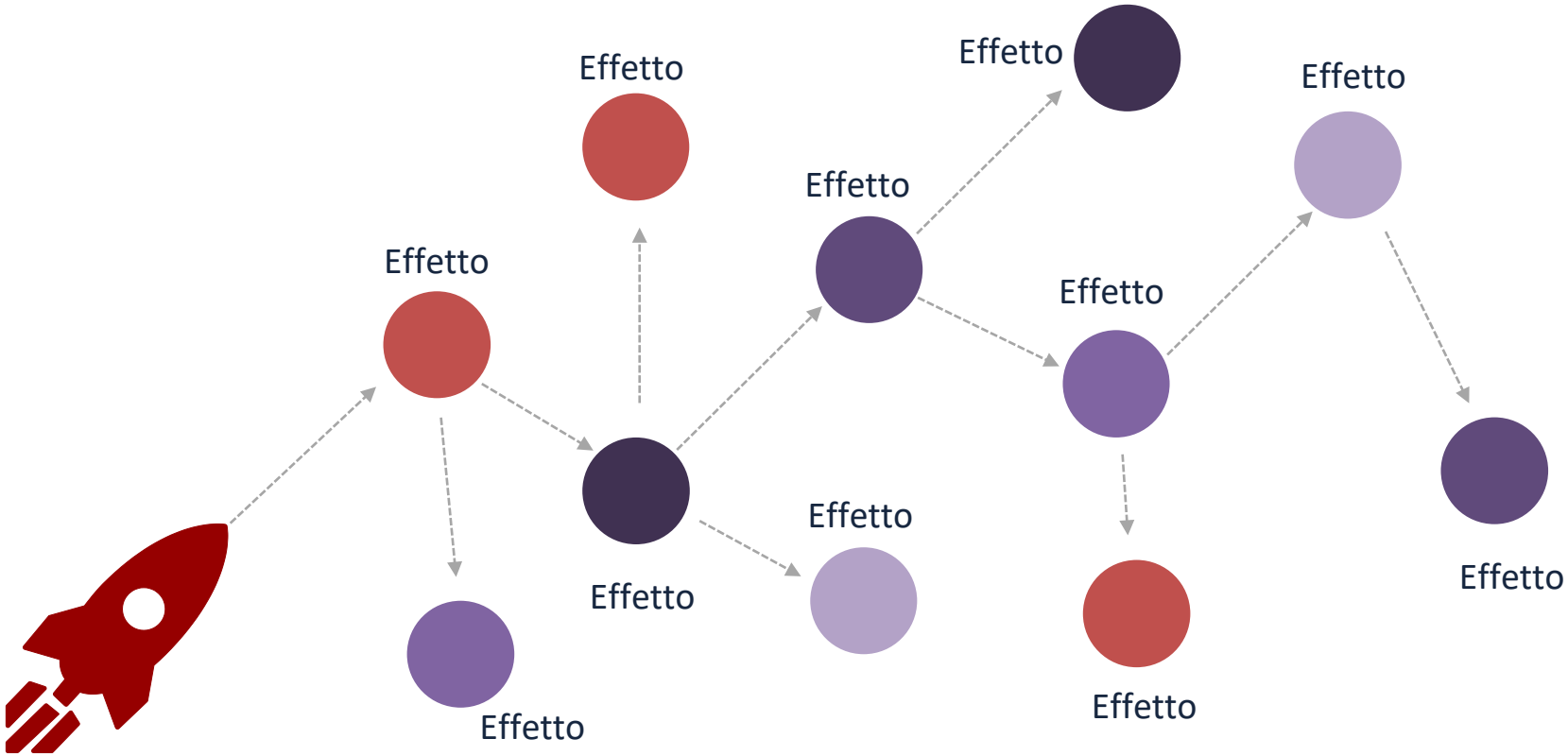
I CONCETTI DI RISCHIO E RESILIENZA
ENTERPRISE RISK MANAGEMENT
CRISIS MANAGEMENT
BUSINESS CONTINUITY

I CONCETTI DI RISCHIO E RESILIENZA

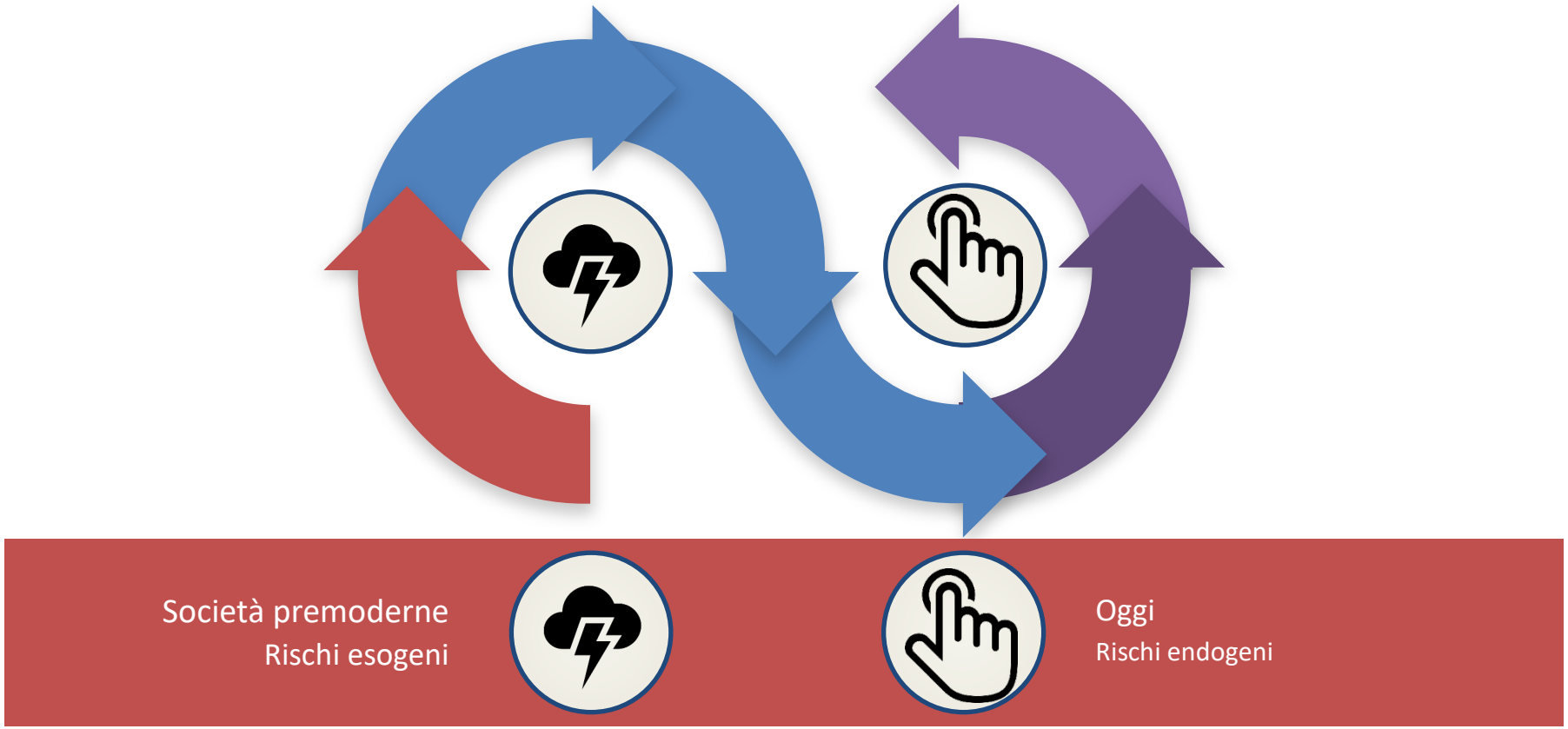
Approccio al rischio: ieri



Approccio al rischio: oggi



Approccio al rischio: evoluzione



Approccio al rischio: evoluzione

Oggi

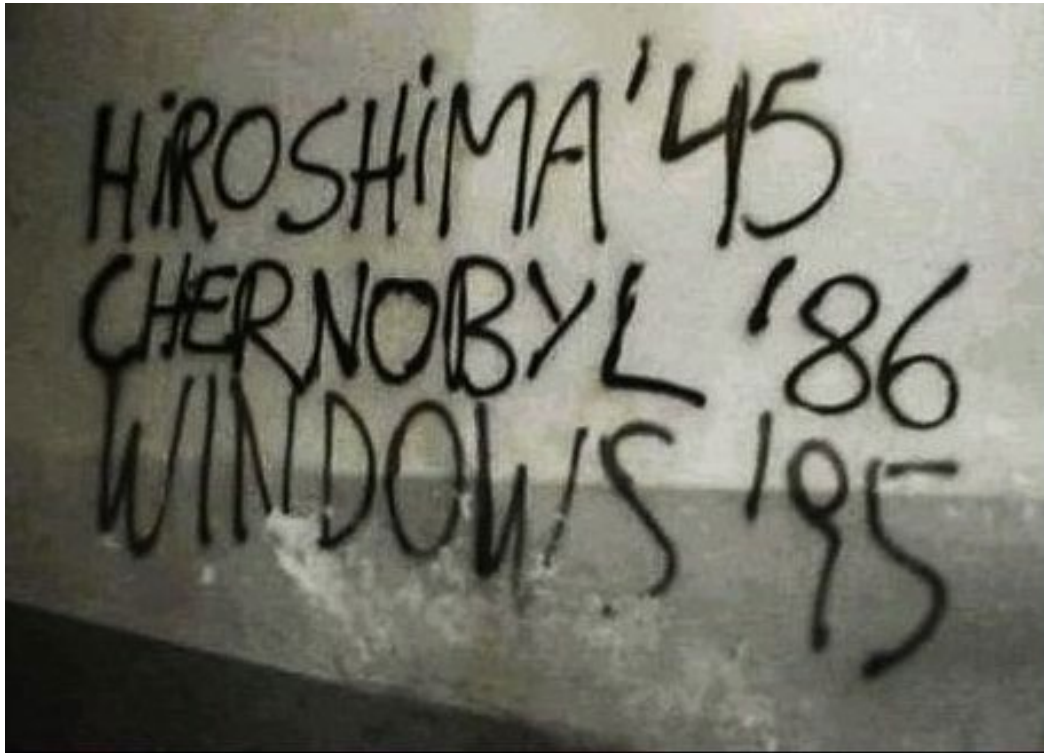
Azione Umana

7

Errore umano

Pandemie

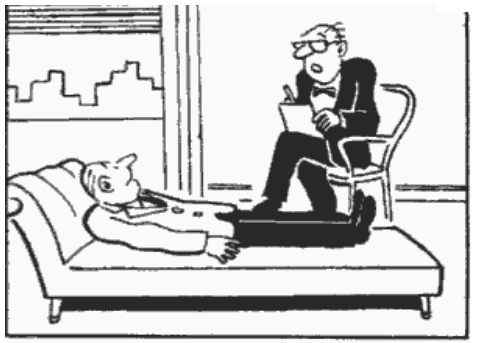
Approccio al rischio: paura del rischio



Piramide di Maslow

Definizione di 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!

La joint venture della resilienza

Resilienza organizzativa: perché?

Cambiamento culturale

R© = F(n^m)

La resistenza al cambiamento di un'organizzazione è pari al numero dei dipendenti (n) elevato alla potenza con il numero di manager(m)

Siete troppo impegnati per innovare?

Fonte: Lindkvist, Magnus. *The Attack of the Unexpected: a Guide to Surprises and Uncertainty*. Marshall Cavendish Business, 2011.

Gestire il cambiamento

16

ENTERPRISE RISK MANAGEMENT

Definizione di rischio – ISO 31000

Scopo dell'Enterprise Risk Management

01 Garantire che l'esposizione al rischio sia coerente con la propensione ad esso

02 Controllare che l'esposizione assunta non superi la capacità di rischio predefinita

03 Confermare che le prestazioni annunciate siano sostenibili anche a lungo termine

Obiettivi dell'Enterprise Risk Management

Fornire al Management la dimensione del rischio con metodi e strumenti tempestivi.

Condividere e comunicare il profilo di rischio e le relative prassi di gestione del rischio attraverso tutta l'organizzazione

Creare la cultura affinché il rischio diventi un elemento misurabile integrato nel controllo dei processi

Preparare il Board e l'Executive ad un'assunzione e gestione consapevoli del rischio globale e dinamico (rischio ricorrente – rischi emergenti)

Incentivare i manager a seconda della loro capacità di controllare i rischi assunti creando valore per l'organizzazione

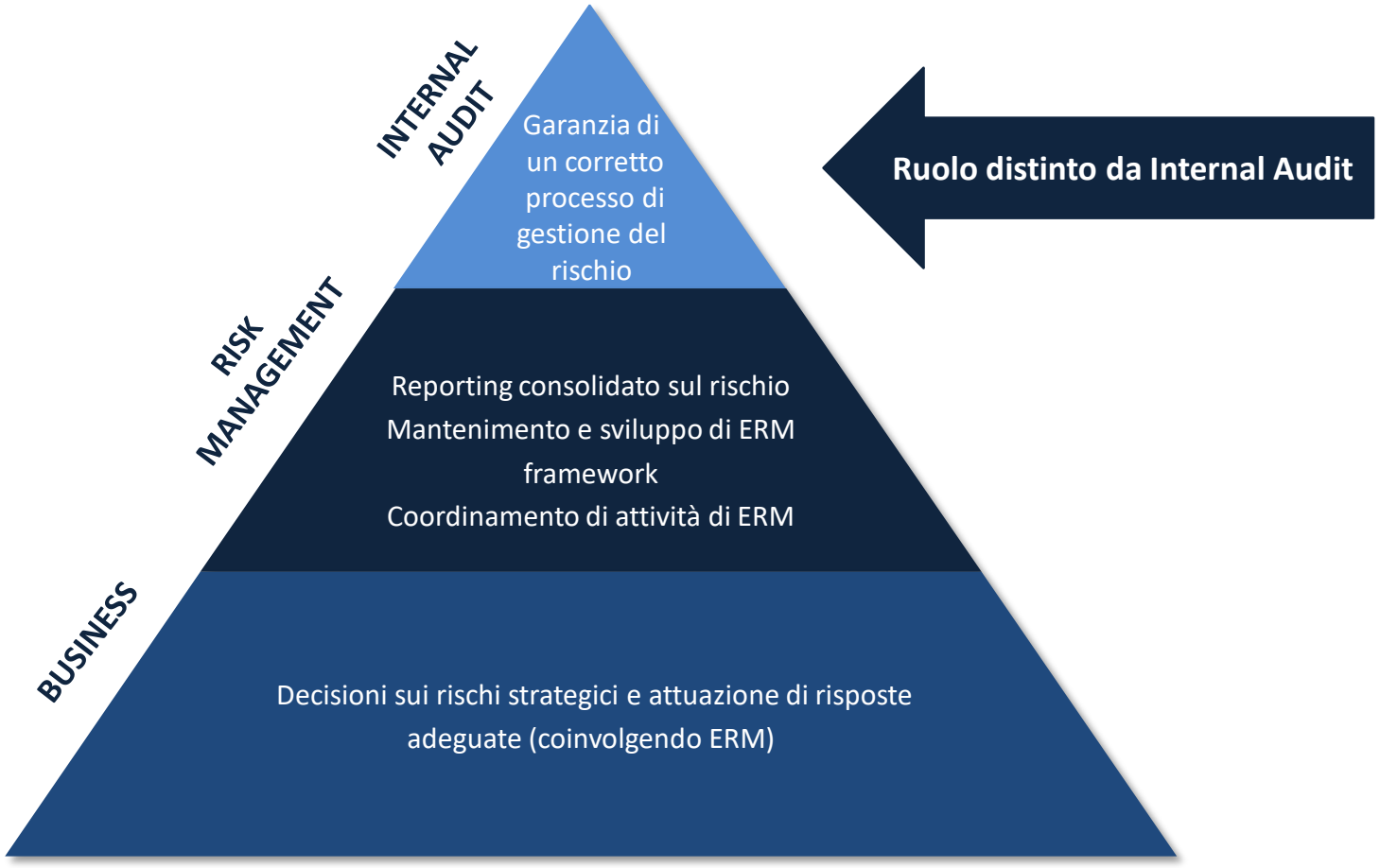
Strategie Costi/Benefici

Misure di Protezione

Creazione di valore

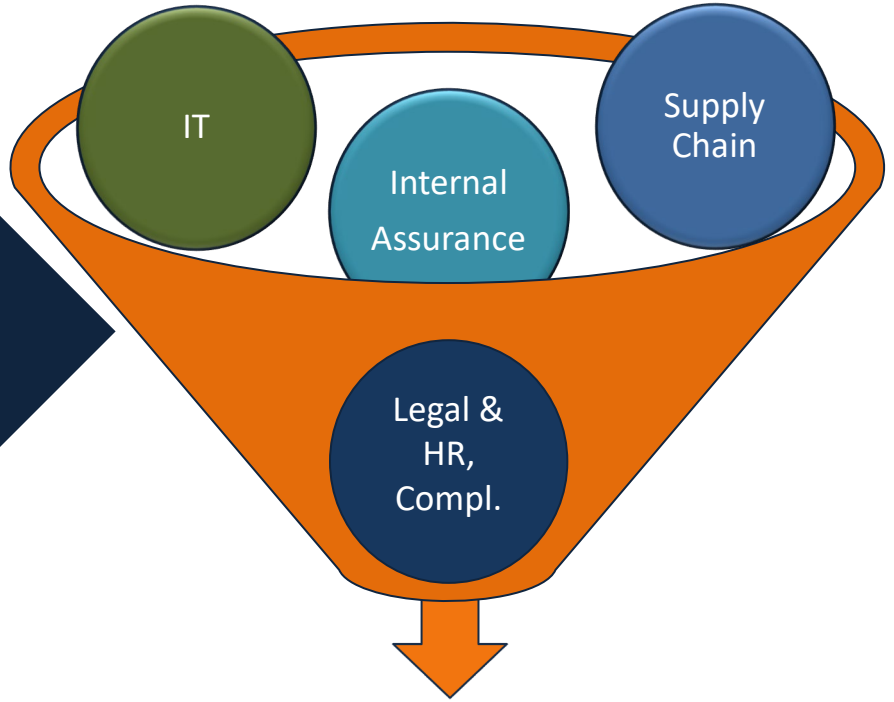
Bilanciamento

Collocazione del Risk Management



No Silos

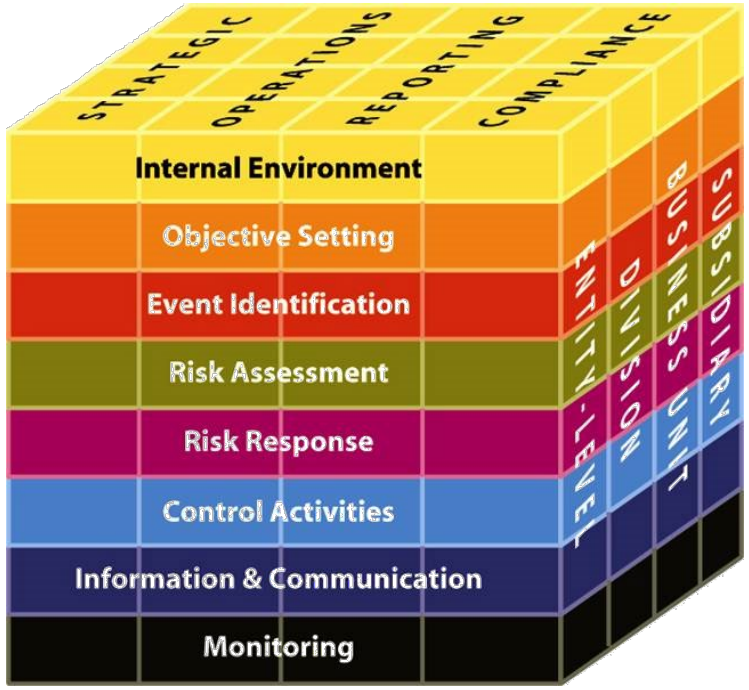
Strumenti di Risk Management già incorporati nel business, ma non inseriti in un quadro comune



Necessario allineare l'ERM con tutte le altri funzioni organizzative che già hanno un approccio basato sul rischio

La metodologia CO.S.O.

Il Committee of Sponsoring Organizations of the Treadway Commission sviluppa un Modello di Risk Management a partire dal 1992



Tale modello continua ad evolversi fino a diventare *Co.S.O. ERM Integrated Framework*

I componenti del CO.S.O.

Internal Environment: definizione della cultura organizzativa

Objective Setting: determinazione degli obiettivi (strategici, operativi, reporting e compliance)

Event Identification: identificazione degli eventi che possono influenzare il raggiungimento degli obiettivi dell'organizzazione (rischi – opportunità – minacce)

Risk Assessment: valutazione degli eventi già identificati in base a probabilità di accadimento (indice di frequenza) e all'impatto (magnitudo)

I componenti del CO.S.O.

Risk Response: applicazione delle tecniche di riduzione del rischio ritenute più idonee

Control Activities: verifica dell'effettiva applicazione delle direttive attraverso il rispetto di regole e procedure

Information e Communication: gestione corretta delle informazioni affinché il Management possa intervenire tempestivamente (diffondere obiettivi e recepire nuovi rischi)

Monitoring: verifica dell'adeguatezza del sistema di controllo interno e del livello delle performance

Fattori che influenzano l'ambiente interno

Risk Assessment

La valutazione dei rischi individua e analizza i fattori che possono pregiudicare il raggiungimento degli obiettivi

Indicazioni sul controllo interno

Il controllo interno è un **processo**: è lo strumento che conduce alla fine, non la fine del processo in se stesso

Il controllo interno è anche responsabilità degli **individui** coinvolti ad ogni livello dell'organizzazione

Il controllo interno fornisce solo una **garanzia ragionevole**, non assoluta, al Management e al Board

Informazione e Comunicazione

- Rilevare, identificare, raccogliere, diffondere le informazioni rilevanti
- Da fonti esterne e da fonti interne
- Aprire tutti i canali di comunicazione Bottom up – Top down
- I sistemi informativi producono rapporti, dati operativi, gestionali,…

Qualità delle informazioni

Puntuali e affidabili

Permettono interventi tempestivi

Devono supportare il decision making

- Fonte Dei Dati
- Periodo Di Riferimento
- Competenza Dei Dati
- Destinatario Dei Dati
- Livello Di Dettaglio
- Obiettivo Del Reporting
- Processi Di Follow-up

Monitoring: supervisione continua

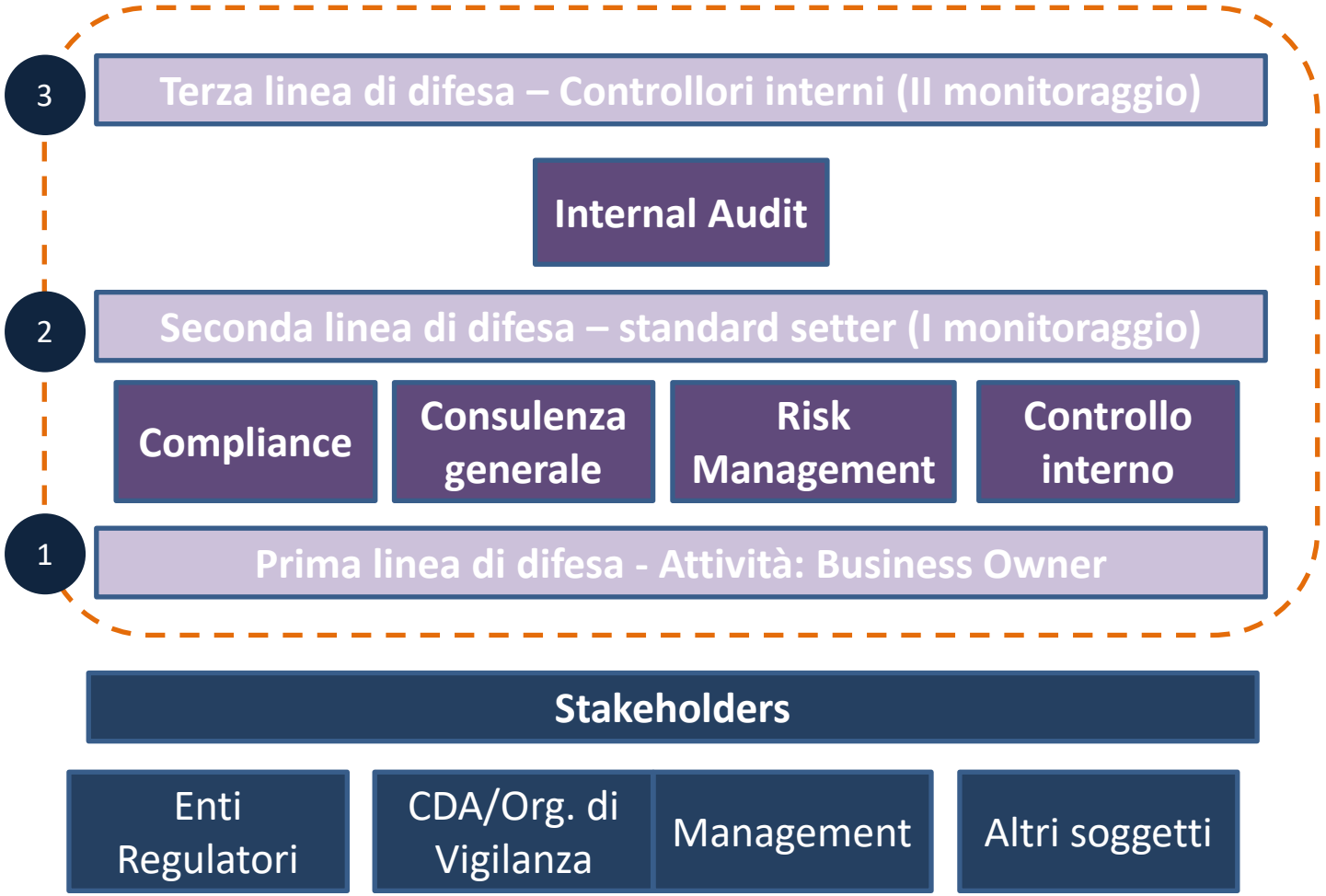
Valutazione nel tempo dell'affidabilità del sistema di controllo interno

Valutazioni periodiche o specifiche (combinazione dei due metodi)

Normali attività di controllo del management o dei quadri

Iniziative del personale nello svolgimento delle proprie mansioni

La metodologia “tre linee di difesa” 1/2



Fonte: IRM – Institute of Risk Management

La metodologia “tre linee di difesa” 2/2

3	Internal audit	• Altri controlli (mandato, autorità, regolamentazione, comunicazione, adeguatezza del personale chiave e strumenti) • Efficacia dei controlli in essere
2	Standard setter	• Raggiungimento degli obiettivi aziendali • Attenuazione/gestione dei rischi • Funzionamento efficace dei controlli
1	Business owner	• Raggiungimento degli obiettivi aziendali • Attenuazione/gestione dei rischi

Fonte: KPMG, “L’Enterprise Risk Management in Italia”

Il Reporting: componenti e ambito

Componenti

- Ambiente di controllo
- Definizione degli obiettivi
- Identificazione dei rischi
- Valutazione dei rischi
- Attività di gestione dei rischi
- Attività di controllo
- Monitoraggio

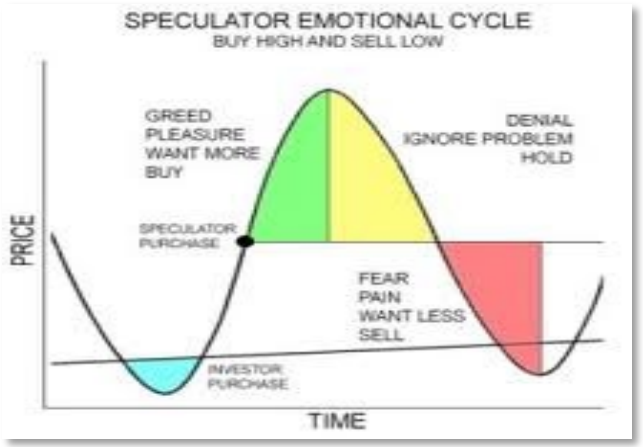
Ambito

Gruppo, Legal Entity, Business Unit

I rischi nel mondo finanziario

I rischi "puri" sono quelli causati da un accadimento negativo. Se tutto va bene, la nostra situazione non cambia.

Attraverso la speculazione, il rischio può dare conseguenze positive. Nell'impatto ci si può arricchire.



Sarbanes - Oxley Act

Legge Federale del 2002, nata dopo diversi **scandali contabili** (tra cui Arthur Andersen ed Enron)

Maggiore **responsabilità del Management** sulla correttezza delle informazioni contabili e finanziarie

Viene creata una nuova **Autorità di controllo** dei revisori esterni

Si inasprisce la **pena per crimini contabili** e illeciti fiscali

Rischi puri

Per molti anni i Risk Manager hanno solo acquistato polizze assicurative per trasferire i rischi "puri". La gestione del rischio è più semplice e non implica sforzi per mitigarlo o eliminarlo.

Fino agli anni '70 i rischi "finanziari" non erano considerati. I tassi di interesse erano stabili e la fluttuazione delle valute era mantenuta in un range stretto (accordo di Bretton Woods).

Le assicurazioni ipotizzavano la massima perdita tollerata e la probabilità di perdita possibile e quantificavano il rischio tramite analisi matematico/statistiche

Rischi speculativi

Anni '70: il prezzo del petrolio cresce grazie all'accordo OPEC – produzione inferiore a prezzi più alti: l'inflazione cresce e anche i rischi finanziari

1972: termina l'accordo Bretton Woods e la fluttuazione dei cambi delle valute impatta sull'import/export. I tassi di interesse aumentano.

Nascono sofisticati prodotti di copertura del rischio (forward, future, option, swap) detti "derivati", il cui valore deriva da altri strumenti finanziari

I Risk Manager per anni hanno continuato a trincerarsi nel comodo calcolo "assicurativo"

Anni ’90: Enterprise Disaster Management

Occorre conoscere il rischio, oppure decidere di non prenderlo, a prescindere da quali profitti siano sottintesi, promessi o confermati

I Risk Manager non hanno avuto il coraggio o l’autorevolezza di bloccare gli acrobati della Finanza

La gestione del rischio per Basilea II

Ogni operazione bancaria comporta un rischio specifico

↓

Il rischio deve essere misurato e coperto da capitale proprio

↓

A rischi maggiori deve corrispondere una dotazione patrimoniale superiore

L'approccio alla gestione del rischio

Metodi sistematici

Applicazione di coefficienti su controvalore a rischio (requisito patrimoniale)

Metodi organizzativi

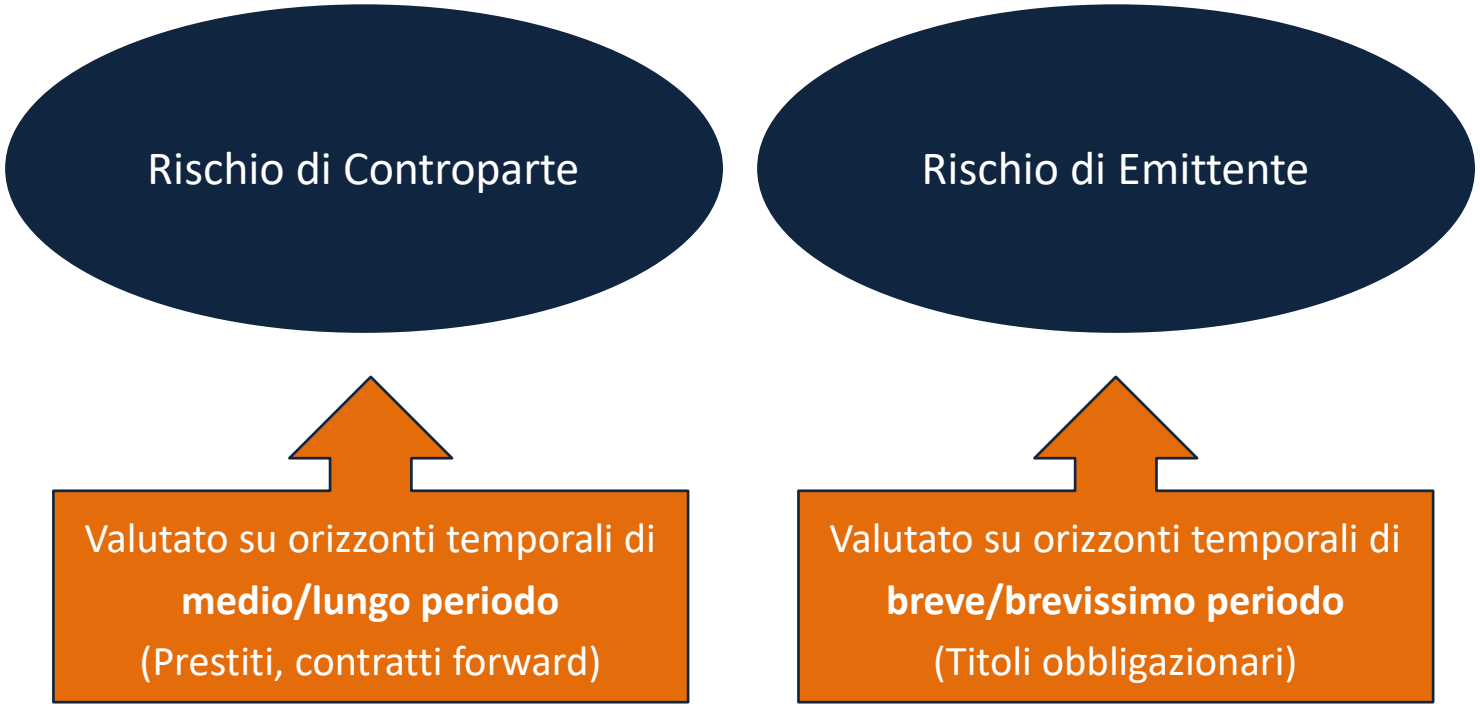
Requisiti strutturali quali il sistema di controllo interno, procedure, segnalazione anomalie ecc.

Autonomia delle banche nel processo di determinazione del rischio organizzativo complessivo

I tre pilastri di Basilea

Regole per quantificare i rischi	Nuovi principi per la supervisione	Ricorso alla disciplina di mercato
Determinare l'adeguatezza patrimoniale	Focus sulle autorità di Vigilanza	Aumentare la trasparenza del mercato

Il rischio di credito



Il rischio di mercato 1/2

Il crollo del mercato azionario del 1987 rivela la necessità di misurazione del rischio per la sopravvivenza di organizzazioni seriamente esposte

↓

Nasce nel mondo finanziario e preoccupa sia le organizzazioni che le istituzioni

↓

Tutti i modelli statistici usati fino ad allora non avevano previsto la crisi e tutta la matematica quantistica viene riconsiderata

Il rischio di mercato 2/2

Le crisi imprevedibili – chiamate da Nassim Taleb (scrittore, matematico, epistemologo) ***black swans*** – sono **ricorrenti** (1-2 ogni 10 anni) e hanno un impatto immediato su mercati diversi

Se tali eventi ricorrenti fossero **inclusi nell'analisi quantitativa**, le organizzazioni non si limiterebbero a guardare risultati e modificare strategie nel quotidiano

Escludendo tali eventi, i profitti fatti nel periodo tra i *black swan* potrebbero essere molto inferiori alle perdite sofferte durante tali crisi e le organizzazioni potrebbero *fallire*

Misurazione del rischio di mercato (VAR)

Il VAR (Value At Risk), creato dalla matematica finanziaria è un metodo di misurazione del rischio di perdita di valore finanziario del portafoglio organizzativo

Si basa su valutazioni *worst case* e considera:

- Confidenza dell'investimento (max % di perdita attesa annua). Valore ottimista: 95%-99%
- Tempo – in genere un giorno, un mese o un anno
- Stima della perdita dell'investimento in valuta o in %

Formula matematica del VAR

$$\mathrm{VaR}_{\alpha}(L) = -\inf\{l \in \Re : P(L > l) \leq 1 - \alpha\} = -\inf\{l \in \Re : F_L(l) \geq \alpha\}$$

Esistono tre diversi metodi per calcolare il VAR:

Metodo storico	Si basa su dati oggettivi di **perdite storiche** e assume che le perdite ricorrano nella storia finanziaria
Varianza – covarianza	Assume l'**andamento armonico** del ritorno sugli investimenti azionari e quindi solo ritorno atteso e deviazione standard da stimare
Monte Carlo	Modello di **simulazione matematica** che elabora dati multipli ed ipotetici di valore del portafoglio

I rischi organizzativi

Mappa dei rischi organizzativi: probabilità dell'evento

Molto probabile	Accade con continuità, quindi prevedibile e misurabile
Probabile	Accade molte volte in un ciclo/tempo considerato
Occasionale	Può accadere qualche volta
Improbabile	Può succedere o è già successo in questa organizzazione o in una simile
Inverosimile	Evento che non è mai accaduto in organizzazioni simili, ma potrebbe accadere
Impossibile	Collegato a fattori che sono praticamente impossibili

Risk assessment e impatto

Probabilità x Impatto = Risk Rating

Attribuire una valutazione ad ogni «asset vulnerabile» identificato

Ad esempio: catastrofico, critico, minore e trascurabile

Occorre anche valutare l'esistenza di eventuali altri rischi non presenti

Risk rating: codificazione del rischio

Un elemento grafico di lettura immediata

Rischio elevato	Da monitorare	Rischio basso	Non Applicabile

Risk rating: esempio

P / I	Impossibile	Improbabile	Possibile	Occasionale	Moderato	Frequente
Trascurabile	Basso	Basso	Basso	Basso	Basso	Medio
Minore	Basso	Basso	Basso	Basso	Medio	Alto
Moderato	Basso	Basso	Basso	Medio	Alto	Critico
Critico	Basso	Basso	Medio	Alto	Critico	Critico
Catastrofico	Medio	Alto	Critico	Critico	Critico	Critico

Categoria di rating: critico, alto, medio, basso

Il documento di valutazione dei rischi (DVR)

DVR, Codice Etico e Codice di Comportamento

Walk the talk

Condotte improprie e sicurezza dell'ambiente di lavoro:

- Discriminazioni
- Stipendi
- Riconoscimenti
- Salute
- Sicurezza

Una definizione di rischio operativo

È il rischio procurato dal cedimento di procedure interne, risorse e sistemi

L'accordo di Basilea definisce, tra i rischi operativi, la continuità operativa, il crisis management e la gestione delle frodi:

Frodi **interne**:
furto di beni, evasione fiscale, errori intenzionali, corruzione

Frodi **esterne**:
furto di informazioni, danni di hacker, furti di beni e contraffazioni

Rischio operativo e frodi interne

Condotte improprie, discriminazioni, stipendi e riconoscimenti disarmonici, sicurezza

Manipolazione del mercato, commercio improprio, prodotti ingannevoli, falsa contabilità

Danni su beni immobili: vandalismo e terrorismo

Danni al business, interruzioni di servizi, problemi di software o di hardware, cybercrime

Problemi nell'esecuzione, errori, mancato rispetto di scadenze, negligenza

Fraud Management

Organizzazioni concentrate soprattutto sulle frodi esterne

Vulnerabilità enorme per le frodi interne

Estorsioni

V	Violence
I	Ideology
C	Compromise
E	Economical reasons
E	Ego

Che cos'è una frode?

Atto illegale commesso per usufruire o appropriarsi di beni dell'organizzazione, deviandone la destinazione con l'intenzione di evitare il dovuto pagamento

Atto di sabotaggio, anche senza ritorno economico, generalmente effettuato dall'interno con l'obiettivo di danneggiare l'organizzazione per rivalsa e/o vendetta

L'uso dell'inganno per ottenere un ingiusto vantaggio

LA CAPACITÀ DI ALLERTA

Il rischio “frodi interne” aumenta in caso di crisi, recessioni e instabilità

- Paura di perdite finanziarie
- Pressione economica e finanziaria, timore per i propri risparmi
- Timori di instabilità lavorativa
- Paura di perdere il lavoro, precarietà dell’impiego, difficoltà di remunerazione
- Diminuzione di controlli
- Riduzioni drastiche di personale non-front
- Tanti, maledetti e subito
- Perdite, target finanziari irraggiungibili

Rischi economici

Paura di perdite finanziarie

- Capacità di spesa inferiore
- Perdita di benefit
- Difficoltà a ottenere prestiti/mutui
- **Frode**
- Inferiore razionalità sugli atti illeciti
- Minori aumenti di stipendio o bonus

Il posto di lavoro a rischio

Timori di instabilità lavorativa

- SIamo tutti precari
- L'organizzazione è in difficoltà
- Mantenimento figli a tempo infinito
- **Frode**
- Illecito percepito come esproprio
- L'età pensionabile si allontana

Il rischio di perdita di controllo

Diminuzione dei controlli

- Taglio dei costi (controlli inclusi?)
- Procedure non aggiornate
- Aumentano i conflitti d'interesse
- **Frode**
- Maglie del controllo larghissime
- Separazione dei ruoli disattesa

Rischi di sostenibilità

Tanti, maledetti e subito

- Target finanziari irraggiungibili
- Ricerca del profitto a tutti i costi
- Stipendio o bonus a breve termine
- **Frode**
- Sostenibilità futura problema di altri
- Staff aggressivo e creatività negativa

CRISIS MANAGEMENT

Evoluzione della resilienza

Disaster Recovery	Business Continuity	Crisis Management	Resilienza
			
Anni ‘70 Focalizzato sulla continuità di infrastrutture e sistemi tecnologici.	Anni ‘90 Focalizzato sulla necessità di un piano alternativo anche per le persone e i processi.	Anni ‘00 Salvaguardare la reputazione attraverso il coinvolgimento del top management.	Anni ’10 Capacità di un’organizzazione di assorbire il cambiamento e di adattarsi.

Il più grande ostacolo...

NON SUCCEDERÀ MAI

Il fattore umano

73% degli incidenti di sicurezza interna sono statI causati da vulnerabilità nel software e azioni dell'utente scorrette

42% degli incidenti che hanno causato la perdita di dati di informazioni sensibili sono stati causati dagli utenti

Fonte: Kaspersky Lab

TV5 Monde

'…la sfida più grande è il modo in cui la società lavora. Ogni dipendente ha dovuto cambiare il proprio comportamento.'

Yves Bigot - director-general

Fonte: Corera, Gordon. "How France's TV5 Was Almost Destroyed by 'Russian Hackers'." BBC News, BBC, 10 Oct. 2016

Conseguenze più frequenti di un'interruzione

Perdita di produttività

69,3%

Impatto su morale o benessere interni

42,8%

Lamentele della clientela

41,4%

Danno reputazionale

39,5%

Perdita di fatturato

36,3%

Fonte: Elliott, R., Thomas C. & Muhammad K. "BCI Horizon Scan Report 2020". *Business Continuity Institute*, 2020

Cos'è una crisi?

Il significato di crisi

L'origine della parola
(dal greco *Krisis*) significa scelta, decisione

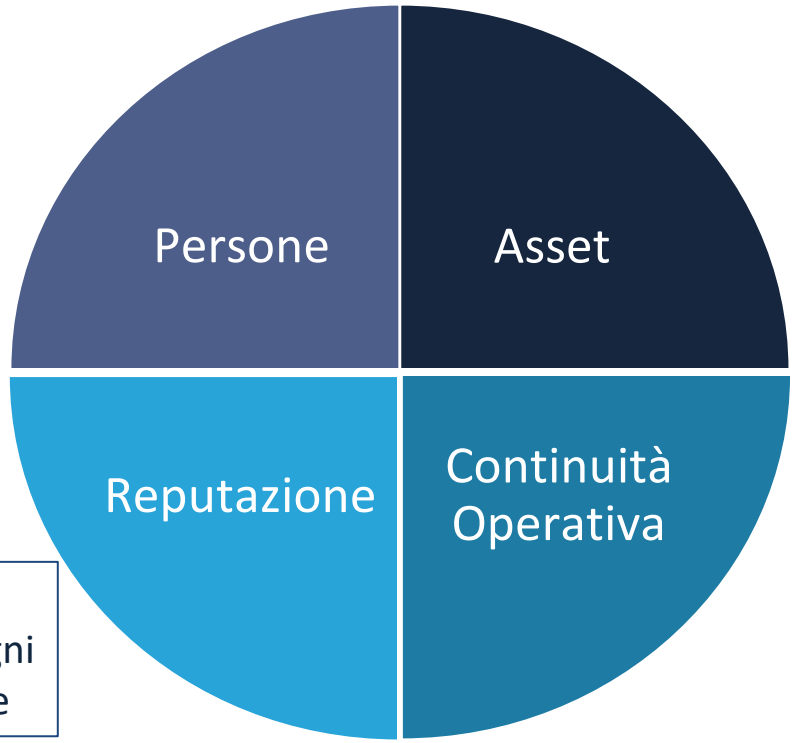
In Cinese la parola è formata da due ideogrammi che significano:
危 pericolo
机 opportunità

La gestione della crisi

L'unica cosa più difficile della pianificazione di un'emergenza è spiegare perché non l'hai fatto

Le regole d'oro

Il Top Management è responsabile delle decisioni atte a salvaguardare:



Un'organizzazione resiliente riesce ad attivare ruoli e responsabilità diversi per ogni parte dell'organizzazione da salvaguardare

I riferimenti del team di crisi

COMPOSIZIONE DEL TEAM DI CRISI (Aggiornato al 31 dicembre 2019)	NUMERO VERDE PER RIUNIONI VIRTUALI DI CRISI: 800 555 555			
	Cellulare	Casa	E-mail lavoro	E-mail personale
Direttivo Crisi (Top Management)				
Presidente – Sergio Mattarella	333 1234567	02 12345678	mattarella@pantaray.eu	mattarella@gmail.com
Back-up – Mario Draghi	333 1234568	02 12345679	draghi@pantaray.eu	draghi@yahoo.it
Funzione di Business (ad es. Funzione Trading)				
Responsabile – Gordon Gekko	333 1234510	02 12345680	gekko@pantaray.eu	gekko@yahoo.com
Back-up – Jordan Belfort	333 1234511	02 12345681	belfort@pantaray.eu	belfort@gmail.com
Funzione di Supporto (ad es. Funzione IT)				
Responsabile – Mark Zuckerberg	333 1234512	02 12345682	zuckerberg@pantaray.eu	zuckerberg@gmail.com
Back-up – Bill Gates	333 1234513	02 12345683	gates@pantaray.eu	gates@gmail.com
Funzione Strategica (ad es. Funzione Comunicazione)				
Responsabile – Enrico Mentana	333 1234514	02 12345684	mentana@pantaray.eu	mentana@gmail.com
Back-up – Sergio Rizzo	333 1234515	02 12345685	rizzo@pantaray.eu	rizzo@gmail.com

Ruoli e responsabilità

RUOLO	RESPONSABILITÀ
Logistica, Facility, Servizi Generali	≷ Comunicare la natura dell'incidente ai membri del team di crisi ≷ Fornire piani per il ripristino temporaneo o permanente dei servizi ≷ Fornire alternative per la ripresa del business ≷ Prima di ripristinare i servizi, testare infrastrutture e sistemi di sicurezza assicurandosi che non vi siano danni
Risorse Umane	≷ Distribuire al personale del sito colpito un documento con le informazioni necessarie in caso di emergenza ≷ Con il management delle LOB, ritenersi responsabili per il personale, inclusi consulenti e dipendenti temporanei ≷ Valutare la necessità di trattamenti medici o eventuali ricoveri ≷ Entro 24 ore dall'incidente, determinare le condizioni dei dipendenti e offrire assistenza ≷ Supportare lo sviluppo della comunicazione con lo staff relativamente all'incidente ≷ **Comunicare con i familiari**
Relazioni assicurative	≷ Determinare in primo luogo se vi sono specifiche questioni assicurative sollevate dall'incidente ≷ Quando l'incidente si rivela tale, sviluppare un'analisi ai fini della policy assicurativa ≷ Mettersi in contatto con gli assicuratori ≷ Dopo l'incidente, fornire assistenza e coordinare la preparazione della richiesta di risarcimento
Contabilità e Finanza	≷ **Attivare una contabilità straordinaria** ≷ Stimare eventuali perdite su lunghi periodi di tempo dovute alla crisi ≷ Rivedere lo sviluppo del mercato e avvertire le linee di business dell'impatto su di esse ≷ Fare controlli che consentano di gestire le finanze dell'organizzazione in modo appropriato nella crisi ≷ Produrre rendiconti finanziari, report e altri documenti richiesti dalla regolamentazione

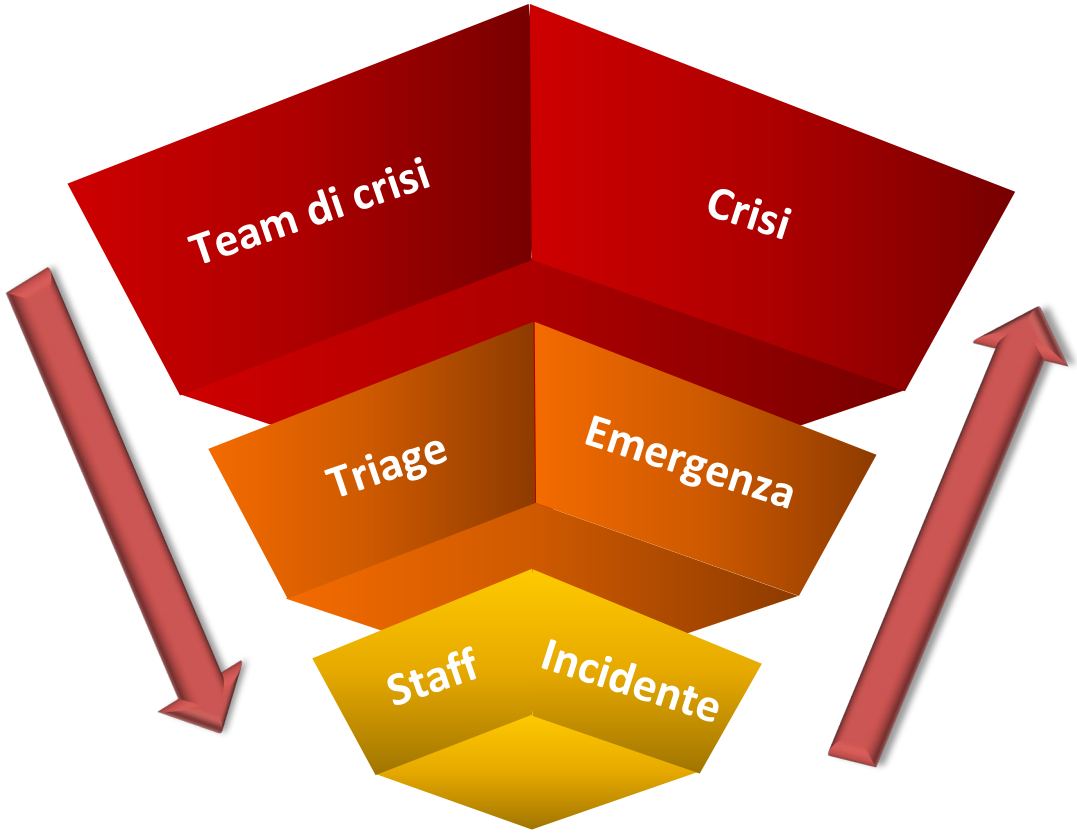
Ruoli e responsabilità

RUOLO	RESPONSABILITÀ
Internal Audit	≷ Assicurarsi che i processi, le procedure e i controlli utilizzati durante il processo di ripristino siano adeguati ≷ Identificare e risolvere i problemi relativi alla sicurezza e al controllo dei processi alternativi ≷ Assicurare l'accuratezza dei report prodotti dopo l'evento critico ≷ **Monitorare che i controlli siano mantenuti normalmente**
Tecnologia	≷ Fornire al CMT dettagli sulle tecnologie utilizzabili (telecomunicazioni, Data processing) nel sito colpito ≷ Comunicare la situazione della tecnologia del sito colpito ≷ Attivare processi alternativi di back-up ≷ Coordinare il ripristino della tecnologia di back-up nel sito colpito, ingaggiare esperti *ad hoc* ≷ Fornire al team le informazioni chiave (ad es. piani, siti di recovery) per le diverse linee di business
Marketing e Comunicazione	≷ Accertarsi dei fatti accaduti, valutare danni e rischi ≷ Partecipare al comando di crisi con i coordinatori chiave (ad es. CMT, HR, Security) ≷ Dare istruzioni al Senior Executive Management, in coordinamento con il CMT ≷ Sviluppare il messaggio iniziale e riesaminarlo con il CMT e le altre figure chiave ≷ Se appropriato, inviare messaggi periodici e interfacciarsi con media e dipendenti ≷ Sostenere il livello Corporate nello sviluppo di strategie di comunicazione con i dipendenti ≷ **Assicurarsi che la comunicazione con lo Staff sia tempestiva e coerente**
Linee di Business	≷ Mettersi in contatto con le aree colpite e con i team di risposta ≷ Definire le condizioni dei business e delle attività critiche per mantenere la continuità operativa ≷ Con l'HR, accertarsi delle condizioni dei dipendenti colpiti ≷ Delineare le condizioni dei clienti colpiti dalla crisi e del settore ≷ Coordinare le richieste di risorse addizionali da parte dei diversi business

Programma di preparazione alle crisi

- Procedure e strumenti adeguati, ruoli e responsabilità chiari
- Strategia di formazione ed esercitazione
- Analisi dei rischi e identificazione di potenziali crisi
- Redazione/aggiornamento di un piano di crisi

Procedura di escalation

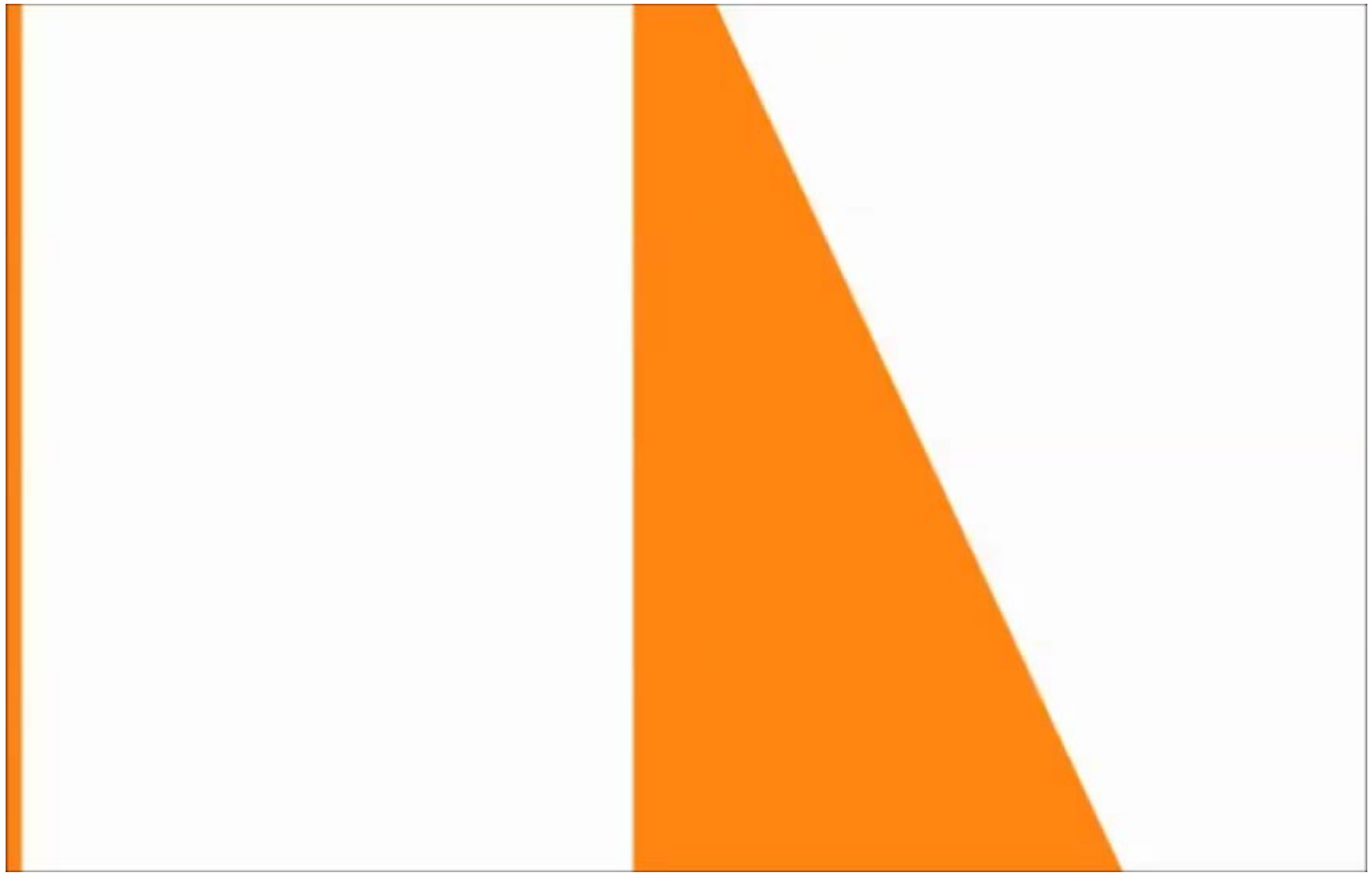


Una crisi può essere dichiarata dal CMT

1. Quando il Top Management percepisce un evento come potenziale crisi
2. Quando un evento non è gestibile a livello operativo

La classificazione degli incidenti

Il ruolo del chairman



Il ruolo del CdA in una crisi: durante

"The Crisis Management Seminar broke up early when someone spilled a pot of hot coffee and nobody knew what to do about it."

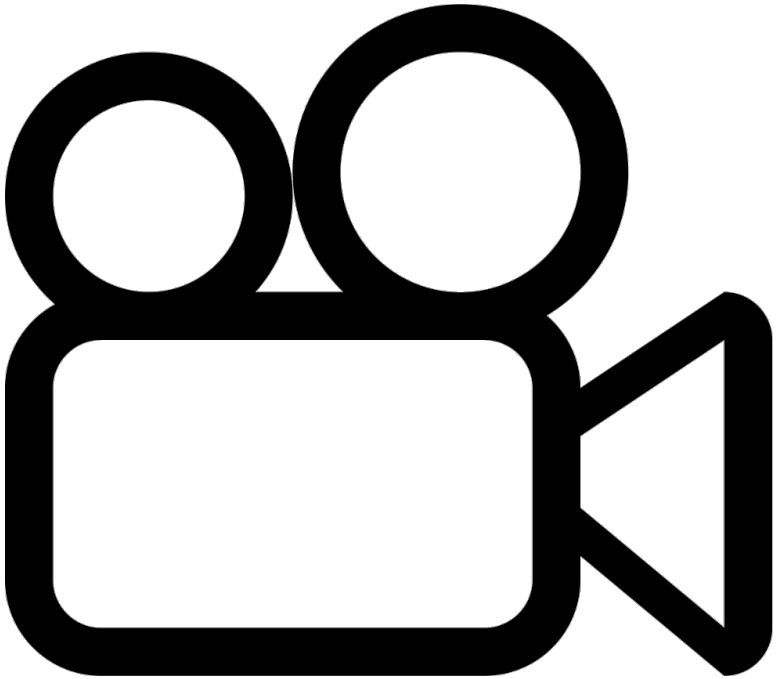
Rispetto dei ruoli
Lasciare la gestione operativa al Comitato di Crisi

Vigilanza
Ricevere e analizzare le informazioni dal Comitato di Crisi

Intervento
Entrare in azione in caso di gravi errori del management

C’è uno script da seguire

1. Il coordinatore apre la teleconferenza: ricorda l’incidente di riferimento e il protocollo
2. Il coordinatore fa un’introduzione, l’appello partecipanti e dirige la riunione
3. Il coordinatore ricorda i ‘next step’ e predispone un verbale di riunione da mandare a tutti



Il protocollo di comportamento durante una crisi

Una metodologia di gestione della crisi **di successo** prevede non solo l'adozione di procedure, ma anche il mantenimento di un approccio collaborativo ed efficiente

- **Parlare solo quando il coordinatore vi cede la parola**
- Rispondere solo a telefonate urgenti (*phone etiquette*)
- Non cercare un colpevole
- Non sottovalutare pericoli, ma non creare inutili allarmismi
- **Non fingere di avere risposte che non si hanno**
- **Lasciare l'ego fuori dalla sala crisi**

Comunicare nella crisi

La comunicazione nella crisi

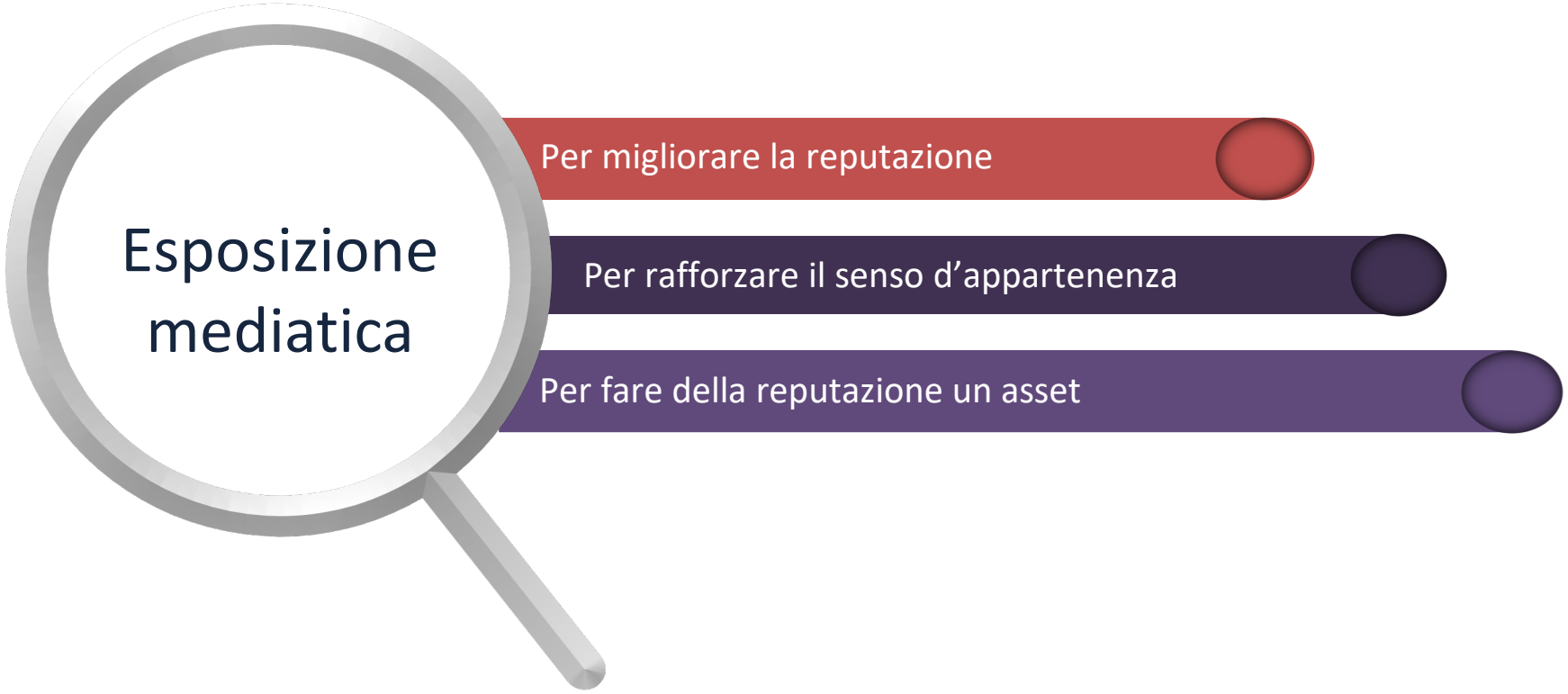
Nelle crisi la percezione è realtà!

Errori da evitare

- Essere timidi
- Attenersi a una versione dei fatti, se essa è cambiata
- Rimanere intrappolati nelle previsioni
- Tirare a indovinare o fare congetture
- Indossare occhiali da sole, masticare gomme o fumare
- Mentire

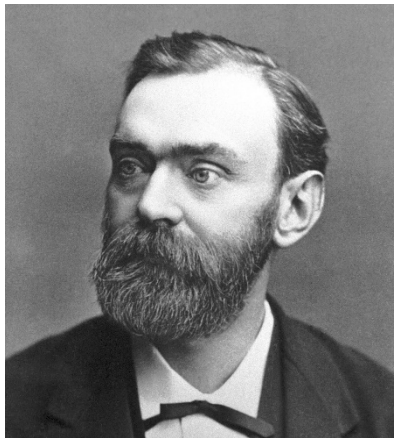
La forma è sostanza

Una crisi può essere un'opportunità



Reputazione – la mitigazione dei danni

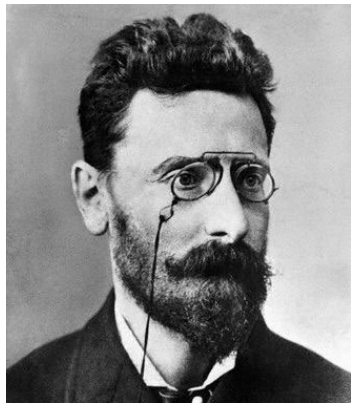
Alfred Nobel



ARTHUR ANDERSEN

FINMECCANICA

Joseph Pulitzer



CHEMICAL

90

Il caso BP

20/04/2010: esplosione Deepwater Horizon

3 Mln 

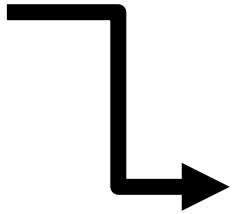
L'esplosione ha rilasciato in definitiva più di 3 milioni di barili di greggio.

11 

Il numero delle persone morte nell'aprile del 2010.

60 Mld $

Il costo per coprire le spese legali e di bonifica.

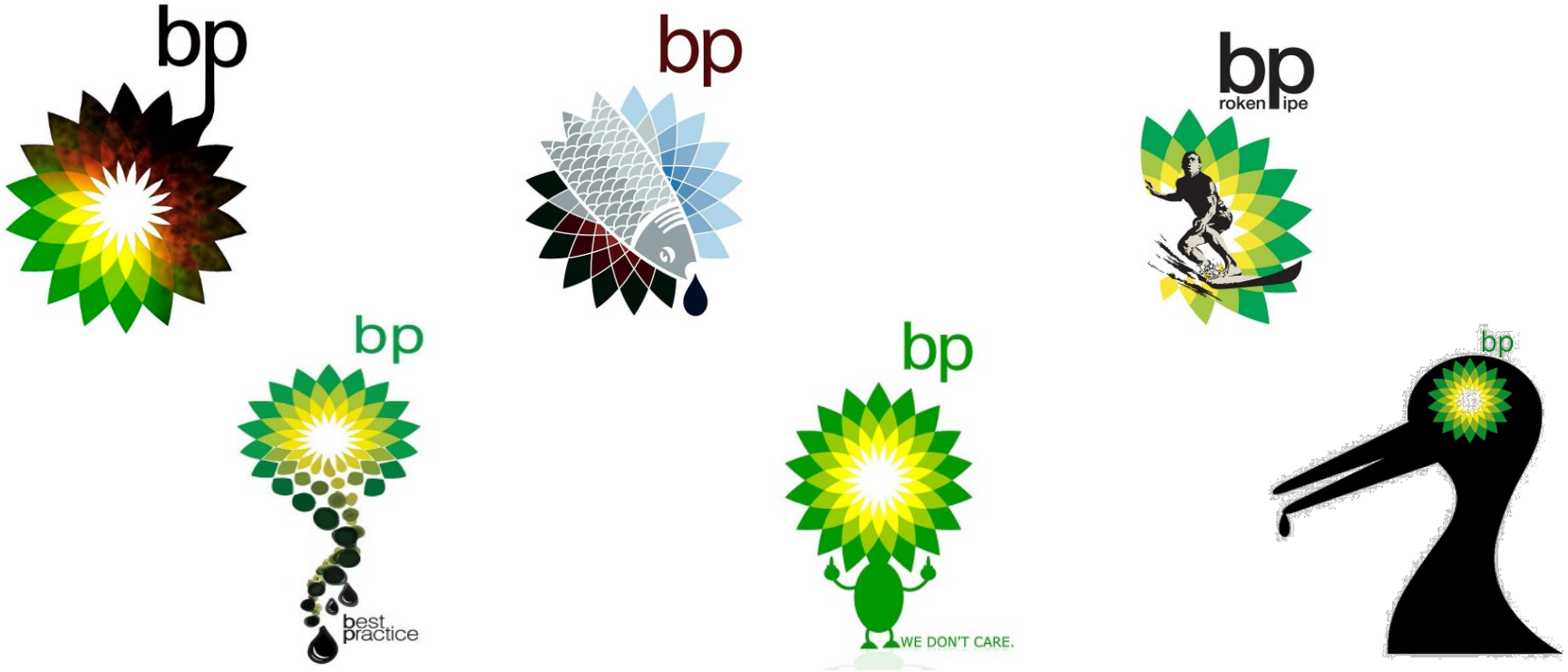
50% 

Le azioni di BP crollano in borsa.

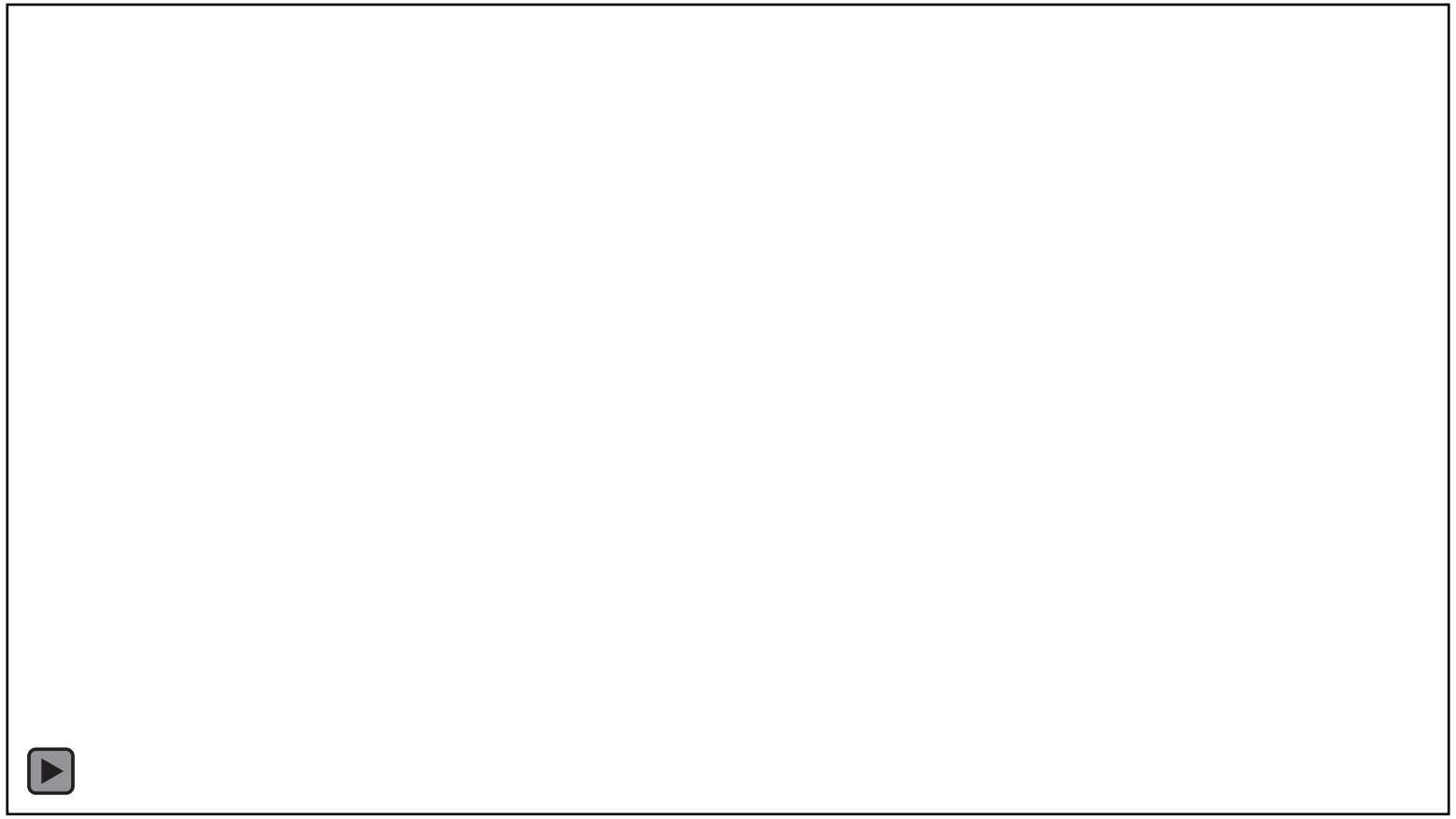
Fonte: Bomey, Nathan. "BP's Deepwater Horizon Costs Total $62B." *USA Today*, Gannett Satellite Information Network, 14 July 2016,

92

Il rebranding di British Petroleum



L’asset più importante



BP Prank

Il danno reputazionale

theguardian

UK world sport football opinion culture business lifestyle fashion environment tech travel browse all sections

home › world › US americas asia australia africa middle east cities development europe

September 11 2001

Starbucks charged rescuers for water

Staff and agencies

Wednesday 26 September 2001
16.31 BST

Shares
87

Save for later

A branch of the coffee chain Starbucks charged New York rescue workers for water to treat victims of the suicide attack on the World Trade Centre, it emerged today.
Ambulance workers were forced to scramble in their pockets for money to pay a $130 (£88) bill for three cases of water used to treat victims for shock after the twin towers collapsed.

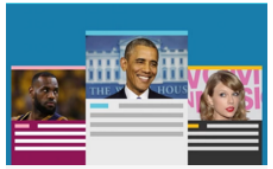
Orin Smith, president of the Seattle-based coffee chain, sent a refund and free coffee to the ambulance crew after the incident was revealed.

"It's totally inconsistent with the kind of behaviour we would have expected from our people, so it has been very upsetting to learn of this," Mr Smith said.

He added that he did not know why the coffee shop in Battery Park Plaza, near the scene of the attack, had charged for the water.

Al Rapisarda, president of Midwood Ambulance Service, whose workers had to come up with the cash, said he had been personally called by Mr Smith to apologise for the outlet's actions.

"It was a misunderstanding with Starbucks," said Mr Rapisarda.



The stories you need to read, in one handy

Abercrombie & Fitch: il silenzio è oro

> [...] we want to market to cool, good-looking people. We don't market to anyone other than that.
> In every school there are the cool and popular kids, and then there are the not-so-cool kids. Candidly, we go after the cool kids. We go after the attractive all-American kid with a great attitude and a lot of friends. A lot of people don't belong [in our clothes], and they can't belong. Are we exclusionary? Absolutely. (2006)

Mike Jeffries, *Chief Executive Officer*

Fonte: "Abercrombie & Fitch Fat-Shaming's Crisis and the Result." *TheFierceEntrepreneur*, 3 Mar. 2016..

96

Abercrombie & Fitch: il silenzio è oro

> [...] vogliamo vendere a persone interessanti e di bell'aspetto. Non vendiamo a nessuno diverso da questo.
> In ogni scuola ci sono ragazzi brillanti e popolari e poi ci sono quelli non così brillanti. Sinceramente, noi inseguiamo i ragazzi brillanti. Inseguiamo il ragazzo tutto americano attraente e con l'atteggiamento giusto e molti amici. Molte persone non ne fanno parte [nei nostri vestiti], e non possono farne parte. Siamo esclusivisti? Assolutamente. (2006)

Mike Jeffries, *Chief Executive Officer*

Fonte: "Abercrombie & Fitch Fat-Shaming's Crisis and the Result." *TheFierceEntrepreneur*, 3 Mar. 2016..

A&F in forte perdita replica dopo qualche anno

Nel 2013, A&F annuncia che avrebbe aggiunto una linea di abbigliamento taglie forti per le donne l'anno successivo.

L'azienda dichiara anche che le taglie forti sarebbero state disponibili
solo online e solo per le donne.

Il CEO nel 2013: "[..] I sincerely regret that my choice of words was interpreted in a manner that has caused offense."
"[..] mi dispiace sinceramente che la scelta delle mie parole sia stata interpretata in un modo che ha causato offesa."

Nel dicembre del 2014 il CEO
Michael Jeffries "va in pensione".

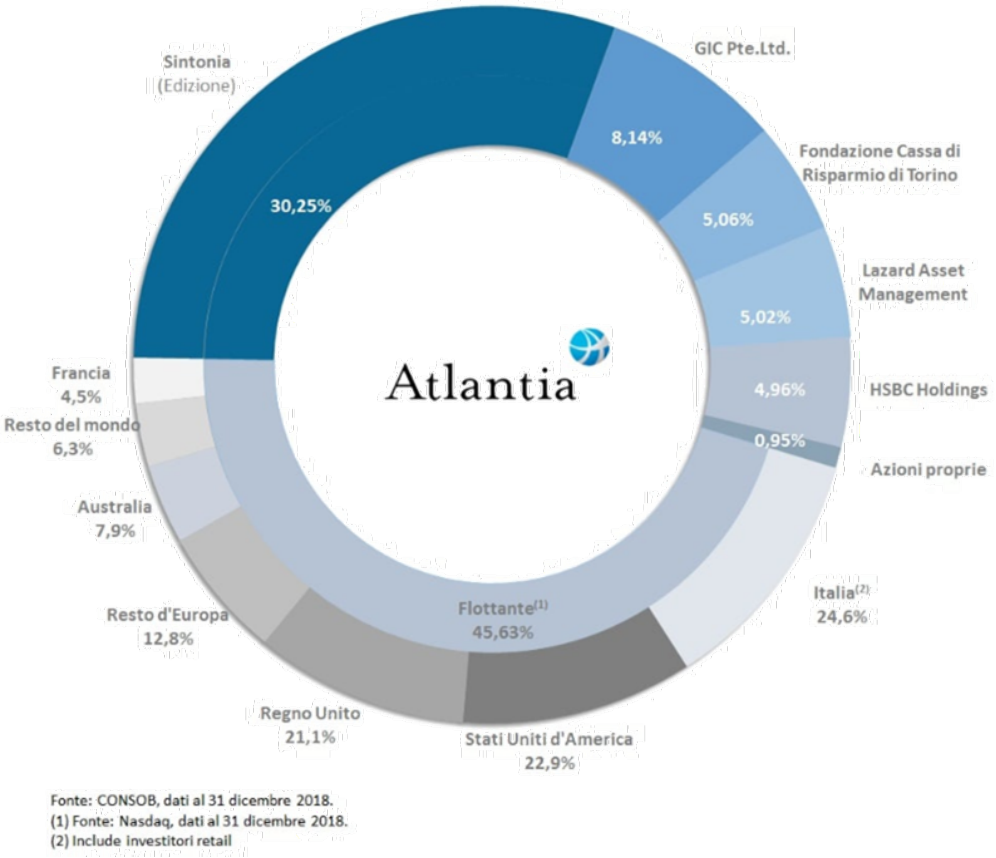
Fonte: "Abercrombie & Fitch Fat-Shaming's Crisis and the Result." *TheFierceEntrepreneur*, 3 Mar. 2016..

Genova – Ponte Morandi

- 14 agosto 2018 – Ponte Morandi crolla alle 11:36
- Costo umano: 43 morti, 9 feriti
- Il crollo ha coinvolto 36 vetture e 3 camion
- Abitazioni/società evacuate o schiacciate
- Danni economici: € 422 milioni

Fonte: Gli Effetti Del Crollo Del Ponte Morandi Su Economia, Occupazione E Integrazione Sociale. Osservatorio Statistico Dei Consulenti Del Lavoro, 2019, pp. 1–10.

Indagati principali…



Fonte: CONSOB, dati al 31 dicembre 2018.
(1) Fonte: Nasdaq, dati al 31 dicembre 2018.
(2) Include investitori retail

- **SPEA Engineering S.p.A.** il 60% del capitale sociale è detenuto da Atlantia S.p.A. La restante quota è egualmente ripartita tra Autostrade per l'Italia S.p.A. e Aeroporti di Roma S.p.A., ambedue controllate dalla holding **Atlantia**.
  - 30,25% delle azioni di Atlantia: nucleo stabile di azionisti costituito da una cordata guidata da **Edizione** (controllata dalla famiglia Benetton).
- **Dirigenti di Anas S.p.A.**
- **Dirigenti del Ministero delle Infrastrutture e dei trasporti**

Fonte: Filetto, Giuseppe, and Marco Lignana. "Ponte Morandi, Nella Lista Dei Nuovi Indagati Spuntano Altri 53 Nomi." Repubblica.it, La Repubblica, 8 Mar. 2019
Fonte: "Il Gruppo." Atlantia, www.atlantia.it/it/il-gruppo.

Assolutamente da evitare

1. Benetton-party a Cortina d'Ampezzo a 24h dal disastro: la festa non è stata rovinata.
2. Il 18 agosto arrivano le scuse di Giovanni Castellucci, amministratore delegato di Autostrade per l'Italia, in conferenza stampa a Genova, la prima dopo la tragedia.
3. Il Governo si esprime a più voci e rilascia dichiarazioni spesso avventate e dissonanti invece di centralizzare la comunicazione in un unico portavoce.

Fonte: Giarelli, Lorenzo, and Camilla Tagliabue. "Il Benetton-Party a Ferragosto 'La Festa Non è Stata Rovinata.'" Il Fatto Quotidiano, Il Fatto Quotidiano, 19 Aug. 2018
Fonte: "Castellucci (Autostrade): Percepita Una Distanza, Mi Scuso. Nuovo Ponte in 8 Mesi." Rainewsca

Il caso Domino's Pizza

- Due dipendenti postano un video su You Tube che li ritrae in atteggiamenti disgustosi nel cucinare una pizza.
- Il video diventa virale e in poche ore. Domino's riceve un'allerta e riesce a identificare il negozio in cui lavorano i due dipendenti. Gli stessi vengono subito licenziati.
- Domino's avverte il dipartimento della salute e la polizia locale. I due ragazzi vengono arrestati.
- I punti vendita di Domino's si svuotano in tutto il Paese. Domino's reagisce subito con una buona comunicazione.
- Il caso diventa famoso come 'Pizza turnaround'. Le vendite di Domino's aumentano del 14% dopo la buona risposta alla crisi.

102

...sui social deve reagire!

Pizza Tracker – Altri Inconvenienti

Sul sito web Domino's crea Tracker, uno strumento che consente al cliente di tenere traccia, in tempo reale, della sua pizza personalizzata permettendo anche di valutarla

Un cliente insoddisfatto pubblica in internet un video della pizza con il formaggio completamente attaccato al cartone

Doyle risponde al video scusandosi e dicendo che tali inconvenienti non dovrebbero verificarsi

104

Pizza Tracker, Altro Caso di Successo

Domino's pubblica feedback sia negativi sia positivi sul sito web, sul New York Times e riprendendo le recensioni negative anche in alcuni spot tv!

Perché ?

Per riconquistare la fiducia della clientela, mostrando di non aver niente da nascondere. In fin dei conti è solo una pizza!

Per Domino's è un'apertura verso onestà e responsabilità e funziona!

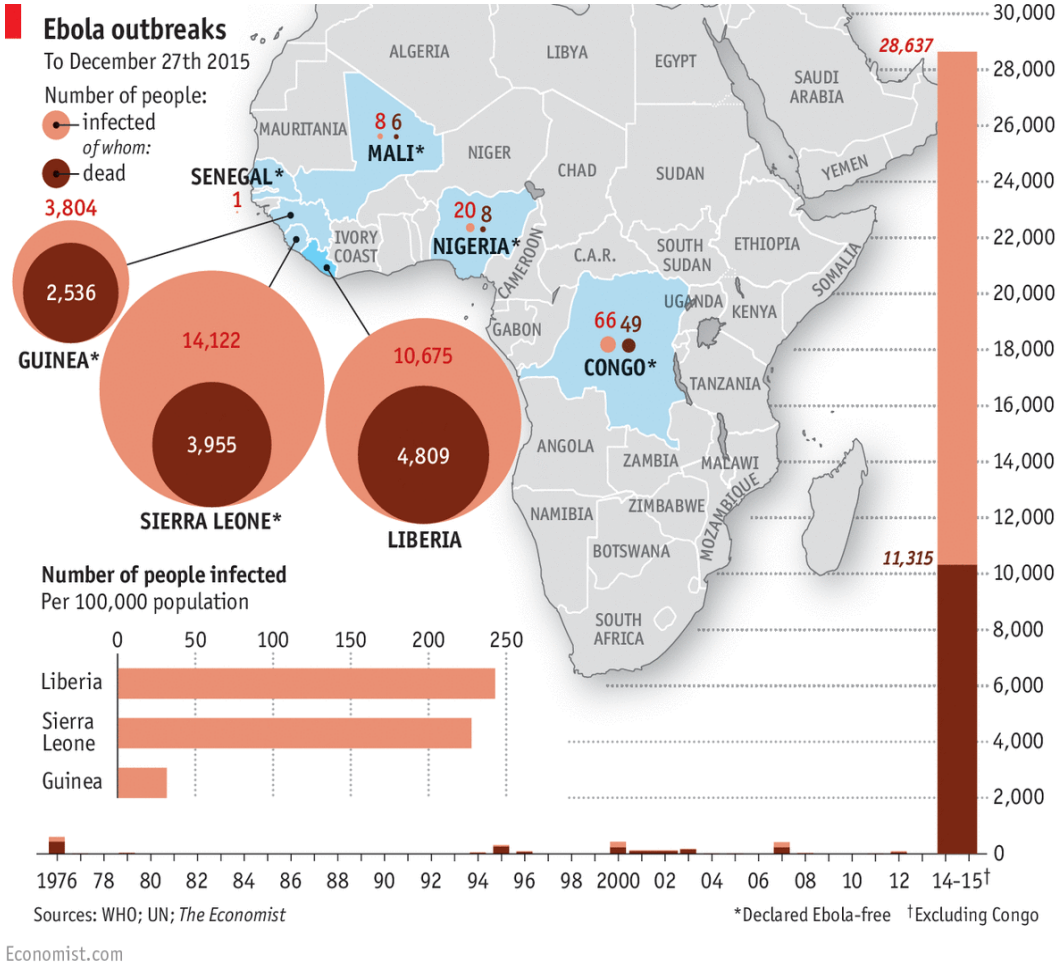
105

Il piano di crisi – elementi chiave

- Linee guida e procedure di escalation
- Componenti del CMT e back-up
- Criteri di ingaggio, attivazione, disattivazione
- Checklist dettagliata per il team di crisi
- Risorse e informazioni indispensabili
- Strategia predefinita di comunicazione

Pandemie – la sfida del nuovo millennio

Oggi, se un'organizzazione è ben preparata a fronteggiare il rischio pandemia, può dichiararsi ad un **eccellente livello di resilienza** per superare ogni tipo di rischio



Da lezioni PANTA RAY 2010-2019

BUSINESS CONTINUITY

Continuità e Resilienza

Fonte: ISO 22300 – Societal Security – Terminology
Fonte: ISO 22316 – Security and resilience – Organizational resilience – Principles and attributes

Trend del Business

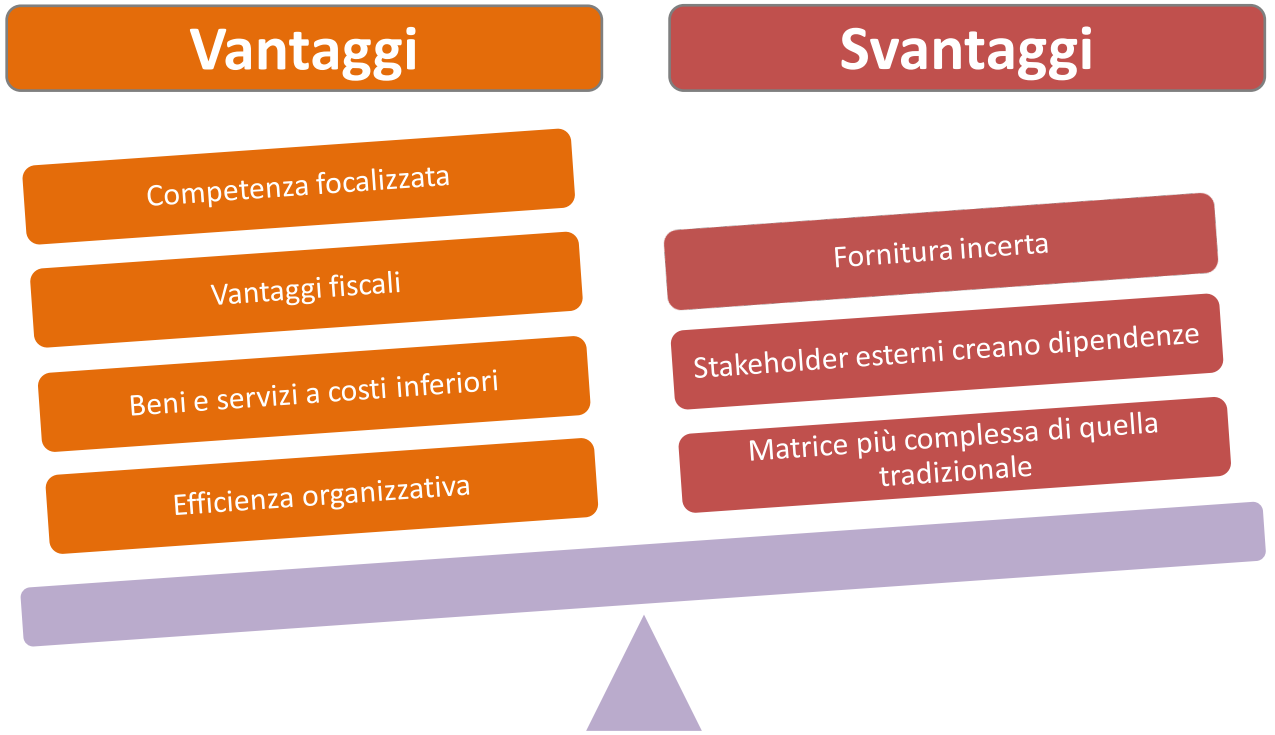
I mercati diventano sempre più competitivi

Il business va indirizzato su attività di maggior valore aggiunto (più profittevoli)

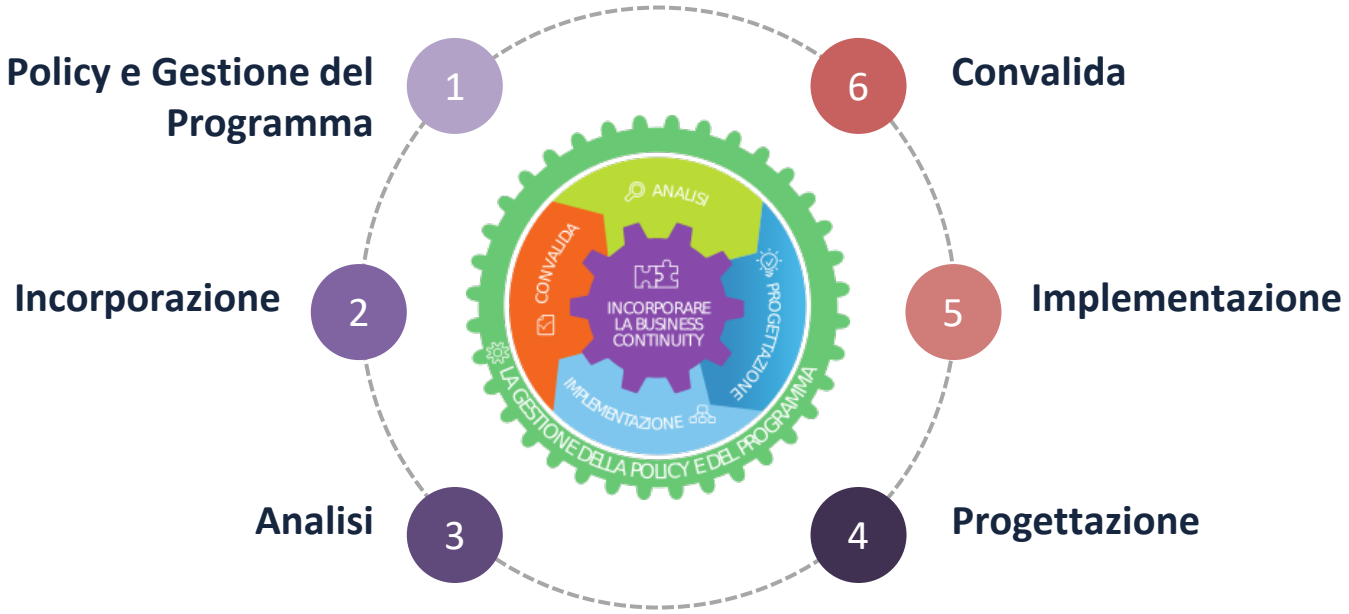
Energia e investimenti solo su aree e prodotti standard

Le organizzazioni disinvestono tutte le altre attività e comprano da organizzazioni specializzate la competenza diretta

L'Organizzazione non è verticale



Business Continuity Management System



Definire una Policy e un Programma

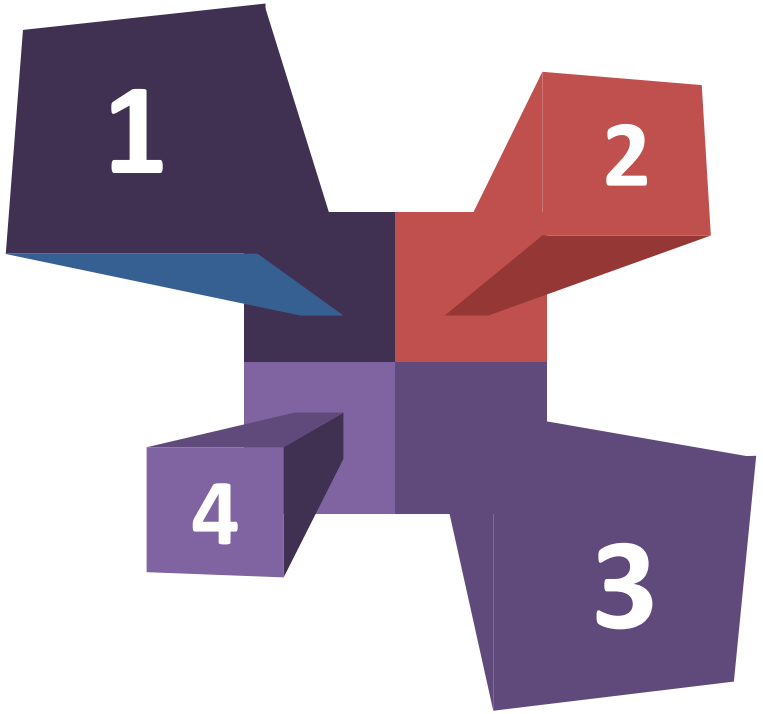
Documento inspirational

Massimo due pagine

Il Top Management è il responsabile della policy di continuità operativa e deve occuparsi dell'implementazione di un programma che risponda con chiarezza alle seguenti domande:

- Qual è il perimetro del sistema di gestione
- Chi coordina il programma e costituzione del team
- Quali sono gli obiettivi strategici e operativi
- Robusta convalida: test, revisione e mantenimento
- Il programma fa parte della cultura aziendale

Il Top Management risponde a queste domande:



1. Qual è il **perimetro** del sistema di gestione?
2. Chi coordina il programma e chi è che fa parte del **team?**
3. Quali sono gli **obiettivi** strategici e operativi?
4. Il programma **fa parte** della cultura aziendale?

Stabilire una governance

- Ruoli e responsabilità
- Programma ≠ progetto
- Impegno dei top manager

Il BC Manager – ruolo

Disponibilità 7/24

Capacità di interagire con i membri del team di crisi

Capacità di leadership

Buone capacità di analisi

Capacità di challenging, personalità ed esperienza

Buona conoscenza dell'organizzazione

Incorporare la Business Continuity

- Terminologia allineata
- Consapevolezza a 360-gradi
- BC è responsabilità di tutti

Incorporare la Business Continuity

Integrare la business continuity nelle attività di business quotidiane è un passo fondamentale per limitare l'impatto di eventi critici che potrebbero colpire l'organizzazione.

Integrare la BC nella cultura organizzativa

Certificazione CBCI per il team BC	Sensibilizzazione al Top Management	Sensibilizzazione per i process-owner
Sensibilizzazione e-learning a tutto il personale	Includere la BC nell'agenda di riunioni rilevanti	Organizzare workshop/seminari periodici

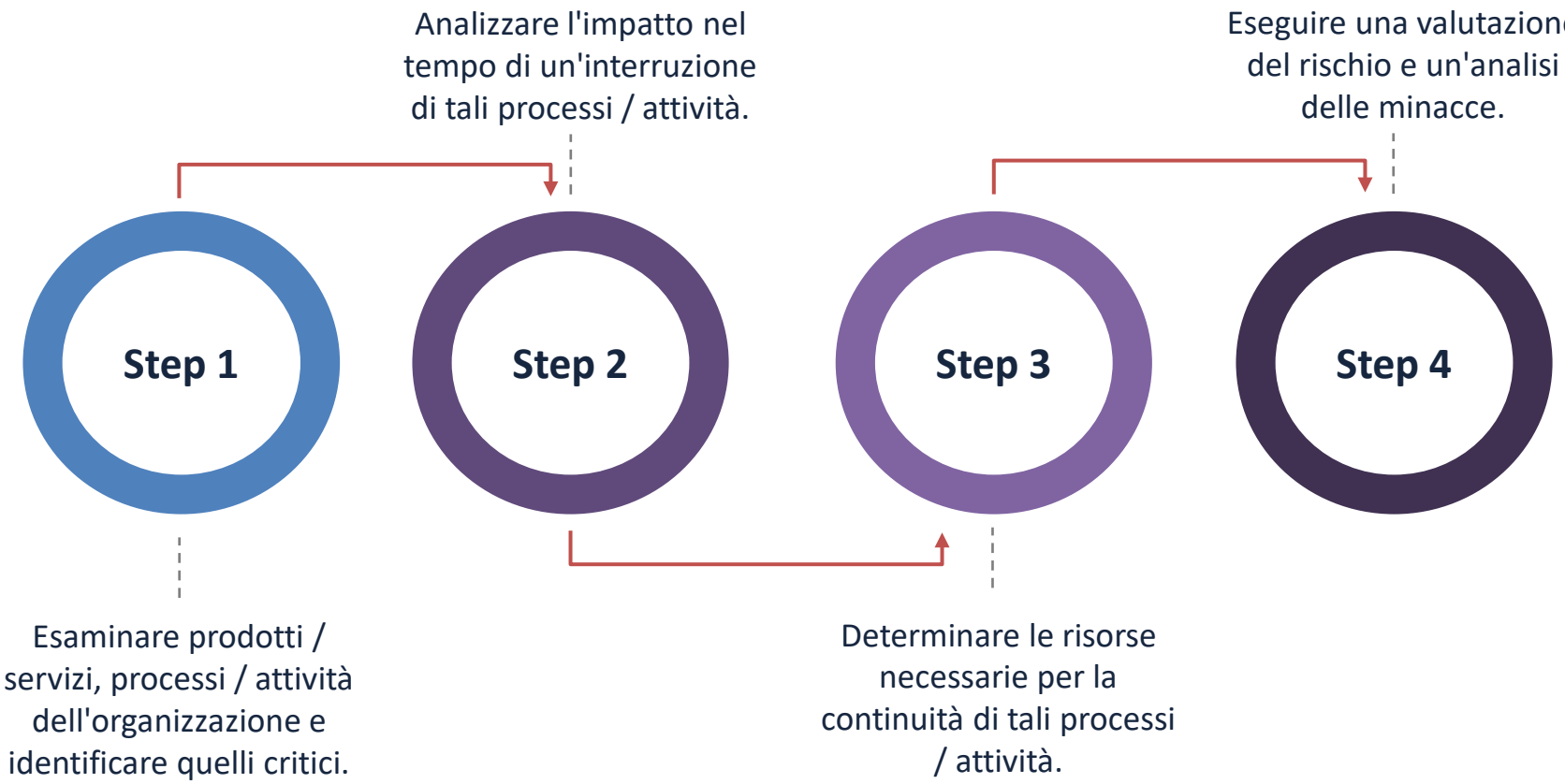
Vantaggi a lungo termine dell'incorporazione BC

Fonte: Riglietti, G., e Aguada L. "BCI Continuity and Resilience Report 2018". Business Continuity Instituteca

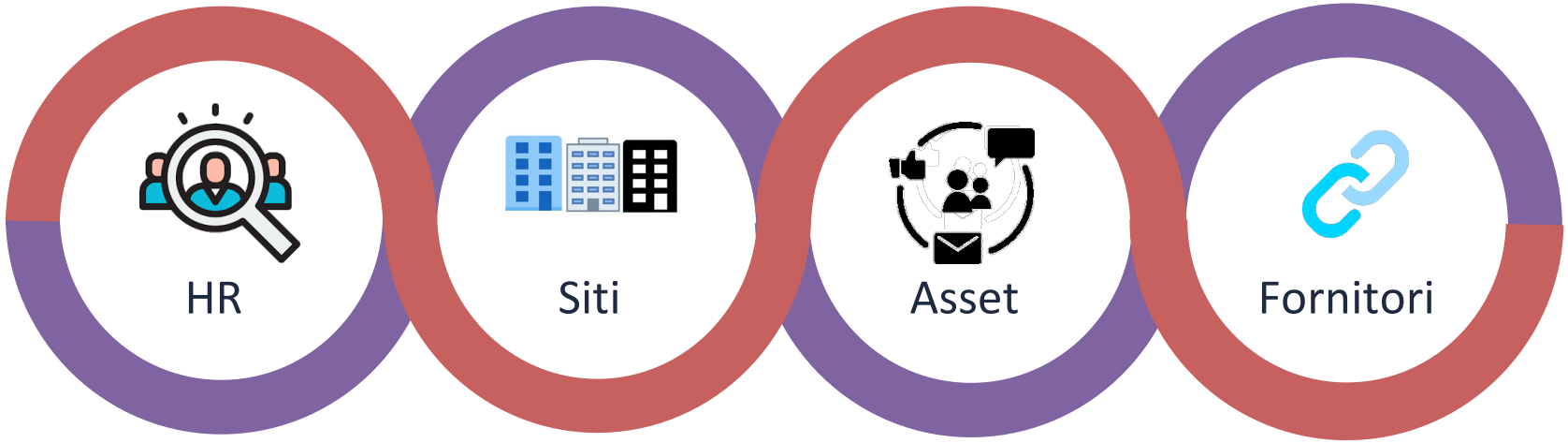
Analizzare i processi critici

- Critico ≠ importante
- Valuta l'impatto nel tempo
- Risorse di continuità

La fase di analisi in breve



Risorse di continuità



Ruoli e responsabilità

BC Manager	Top Management	Process-owner
Progetta un modello di BIA adatto agli scopi dell' organizzazione	Sponsorizza il progetto di BIA e promuove il compimento dell'Analisi	Effettua l'analisi del processo, tenendo conto degli input/output
Propone al TM le soglie di tollerabilità per ogni tipologia di impatto	Approva le soglie di tollerabilità proposte dal BC Manager	Definisce proattivamente gli impatti di un'interruzione sul proprio processo
Consolida i risultati e li presenta al TM per definire strategie e tattiche	Esamina i risultati consolidati e li analizza in maniera critica	È responsabile dei dati inseriti nella BIA e della loro approvazione

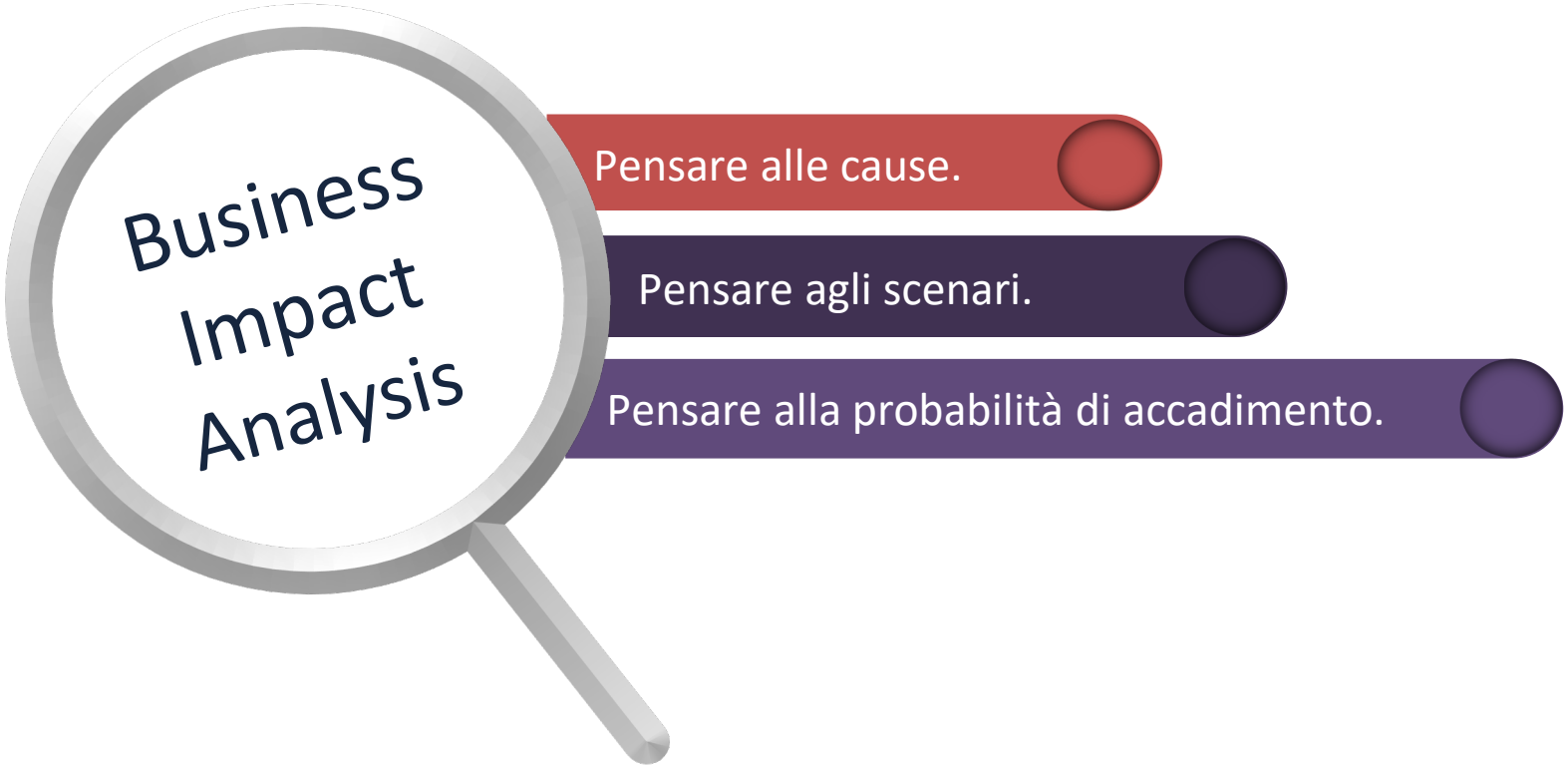
La BIA – non è…


Valutazione dei profitti
Valutazione del processo
Valutazione del manager
Valutazione di efficenza
Valutazione dei rischi
Valutazione delle risorse
Valutazione del fornitore

Vulnerabilità vs. Obiettività

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

Errori comuni

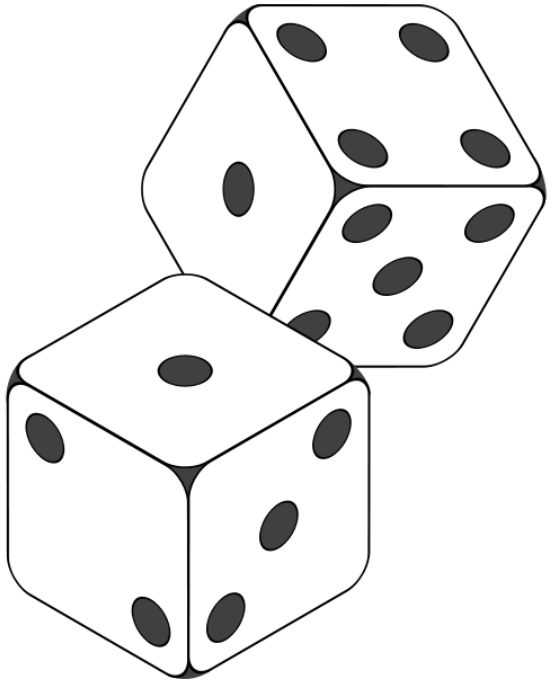


Worst Case Scenario

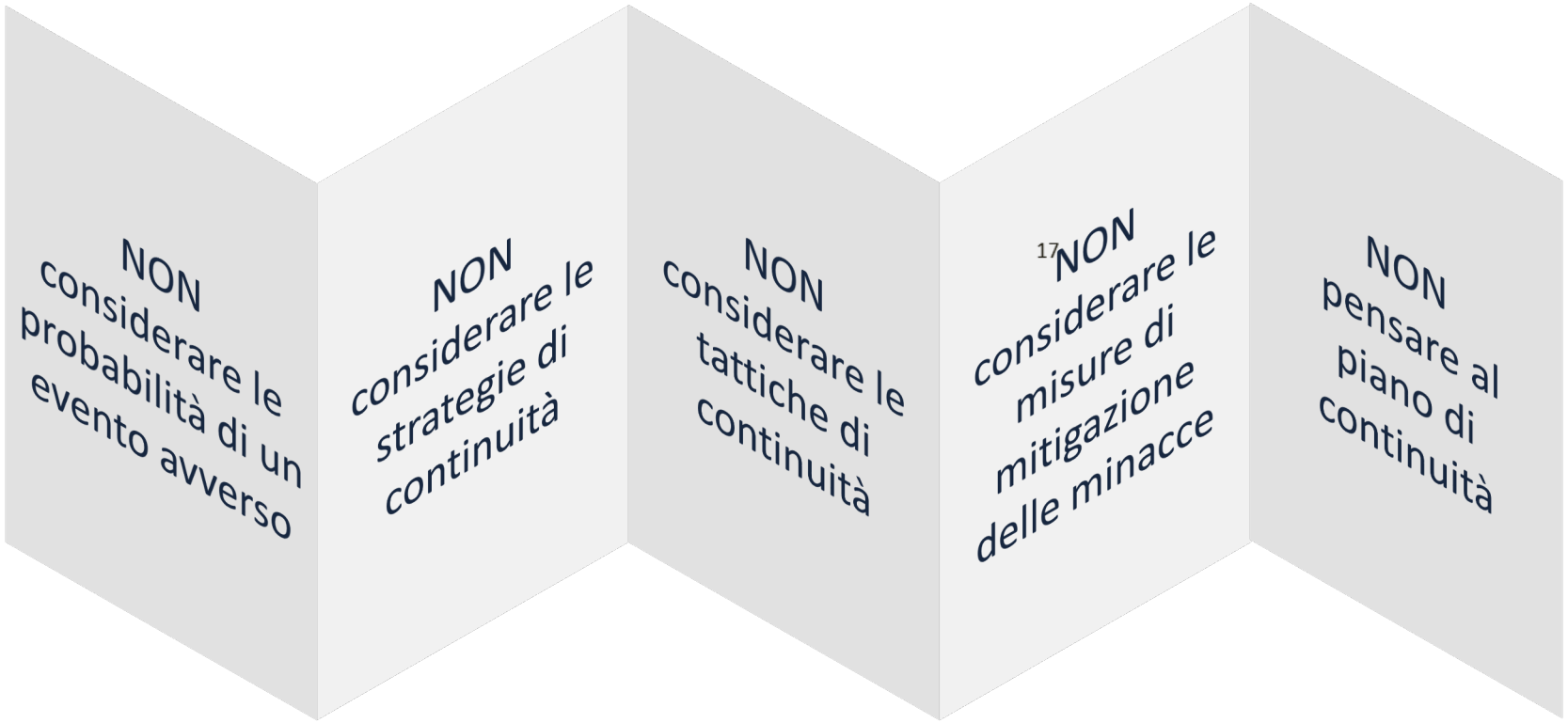
Per documentare gli impatti che nel tempo deriverebbero da una perdita/interruzione, si parte da un'ipotesi di 'worst case scenario'.

Risk Management ≠ BC

Quando si conduce la BIA, l'ipotesi di partenza è che la probabilità del verificarsi dell'interruzione sia pari al 100%.



Resistere agli impulsi



Valutazione dei rischi e delle minacce

Singoli Punti di Cedimento

Una **fonte unica** di un servizio, attività e/o processo

Senza alcun back-up o alternativa

La cui **perdita potrebbe portare al totale cedimento** di un'attività critica per la mission

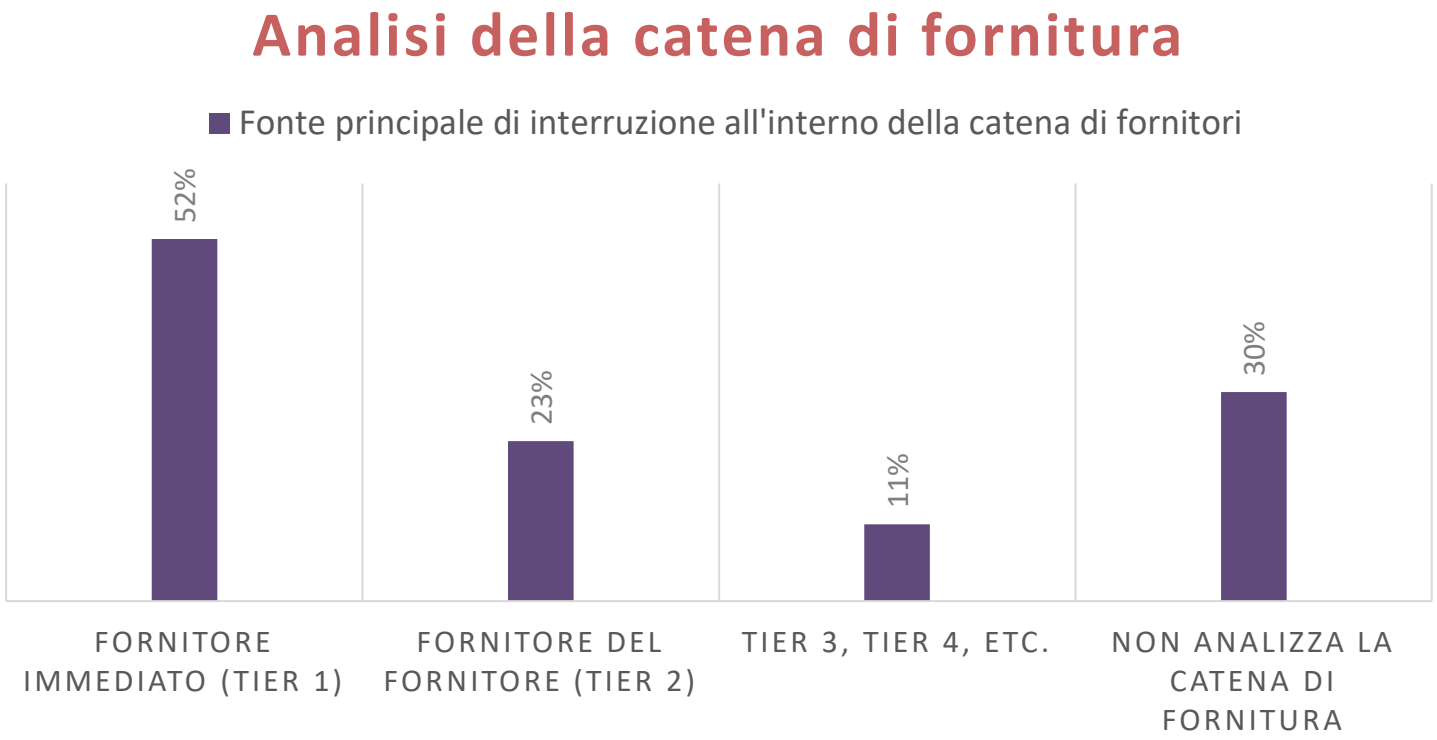
Livelli inaccettabili di rischio

Attività critiche per la mission, loro dipendenze, processi sistemici e personale

Situati nello stesso edificio o **nelle immediate vicinanze**

Che **non sono riprodotti altrove**

Focus sui fornitori



Fonte: Riglietti, G., e Aguada L. "BCI Continuity and Resilience Report 2018". Business Continuity Institute

Supply Chain e Resilienza

Anche quando raggiungiamo un livello accettabile di resilienza all'interno della nostra organizzazione, come possiamo assicurarci che i nostri fornitocari stiano facendo lo stesso?

Progettare soluzioni di continuità

- Obiettivi di recupero realistici
- Soluzioni di continuità coerenti
- Costi accessibili/ragionevoli

Opzioni strategiche

Diversificazione	Duplicazione	Stand-by
RTO = 0	RTO < 24	RTO < 72

Acquisizione post-incidente	Subappalto	Assicurazione
Fornitori pre-qualificati	Service Level Agreements	BC non è garantita

Limitazione di responsabilità – food delivery

Glovo non sarà responsabile per qualsiasi interruzione di servizio, errore di connessione, indisponibilità o malfunzionamento del servizio di accesso a Internet, interruzioni di Internet o qualsiasi altra questione al di fuori del suo controllo.

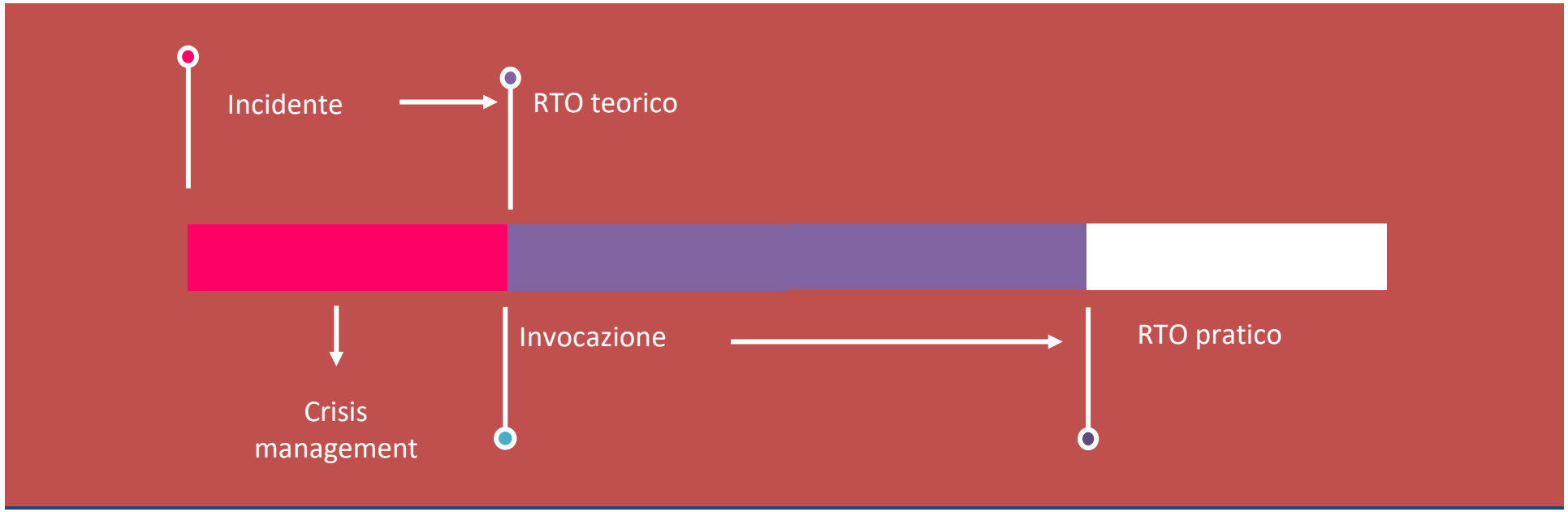
Inoltre, Uber non rilascia alcuna dichiarazione, garanzia o assicurazione circa l'affidabilità, tempestività, qualità, idoneità o disponibilità dei servizi, o dei servizi o beni richiesti tramite l'uso dei servizi, o che i servizi saranno senza interruzioni o senza errori

Fonte: Glovo. "Condizioni Generali Di Uso e Contrattazione." *Glovo*, 31 Dec. 2019.
Fonte: Uber Technologies, "Termini e Condizioni" *Uber*, 4 Dec. 2017.

Obiettivi di recupero

Recovery Point Objective	Recovery Time Objective
Punto in cui i dati utilizzati da un'attività devono essere recuperati per consentire all'attività di operare sul ripristino.	Periodo di tempo a seguito di un incidente entro cui i prodotti, i servizi, le attività e le risorse devono essere recuperate.

RTO teoria contro realtà



Attuazione dei piani di continuità

- Conciso, adattabile, rilevante
- ‘Checklist’
- Regolarmente aggiornato/testato

Contenuto del piano di Business Continuity

Il piano è efficiente quando…

Convalida del BCMS

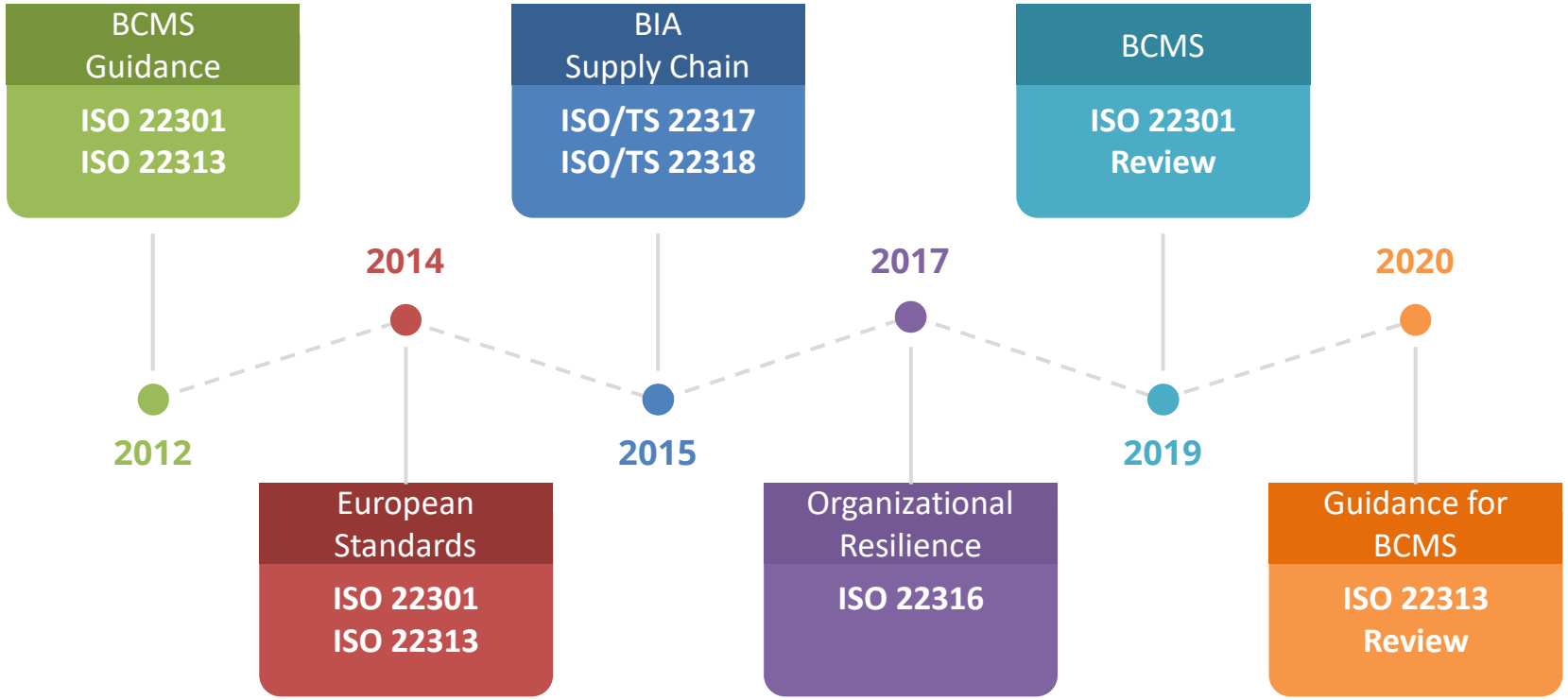
- Test comprensivi e realistici
- Confermare obiettivi della Policy
- Auditor competenti

Software di gestione della BC: principi cardine

Quali principi dovrebbe incorporare una piattaforma per la gestione della Business Continuity?

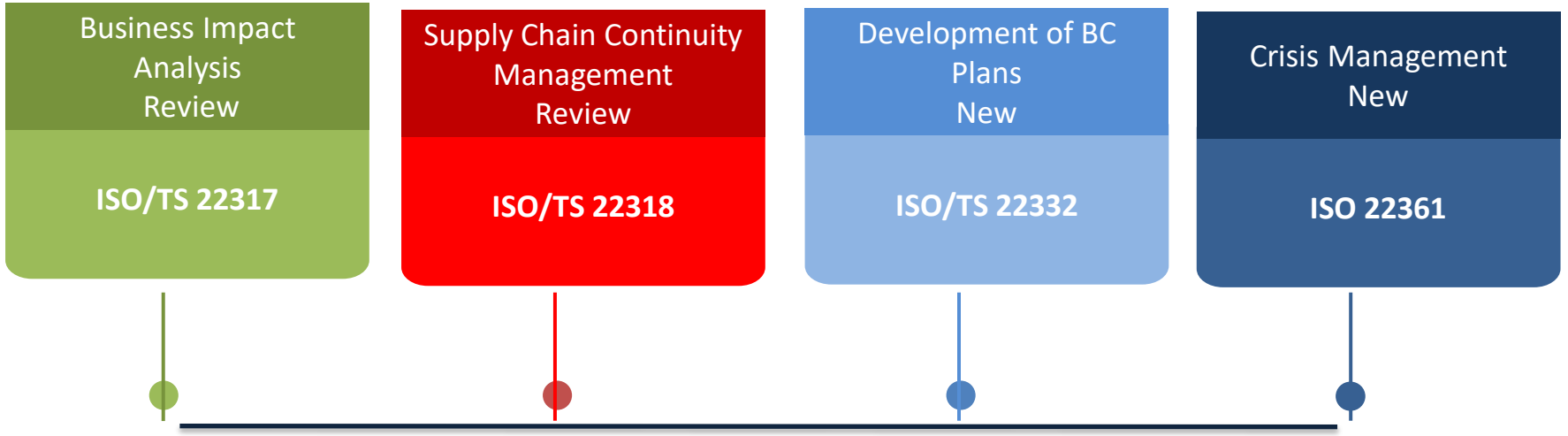
1. Automazione delle attività
2. Facilità d'uso per gli utenti
3. Monitoraggio process owner
4. Responsabilizzazione utenti
5. Piattaforma resiliente (cloud)
6. Produzione automatica di report

Standards related to continuity and resilience



Standards related to continuity and resilience

2021



Standards related to continuity and resilience

2023

Organizational Resilience

ISO 22336

Disclaimer

PANTA RAY

Le informazioni contenute nel presente documento possono essere modificate in qualsiasi momento o risultare imprecise per vari motivi, come ad esempio modifiche dei prodotti o servizi, lancio di nuovi servizi e/o prodotti, differenze tra i prodotti di diversi produttori, modifiche del software o dell'hardware o altro. PANTA RAY non si assume alcun obbligo di aggiornare o altrimenti correggere o rivedere le informazioni. PANTA RAY si riserva tuttavia la facoltà di rivedere le informazioni e di apportare di volta in volta modifiche al contenuto delle stesse senza alcun obbligo di notificare tali revisioni o modifiche ad alcuno.

PANTA RAY NON RILASCIA ALCUNA DICHIARAZIONE O GARANZIA IN MERITO AL CONTENUTO DEL PRESENTE DOCUMENTO E DECLINA OGNI RESPONSABILITÀ PER POSSIBILI INESATTEZZE, ERRORI OD OMISSIONI EVENTUALMENTE CONTENUTI NELLE PRESENTI INFORMAZIONI.

PANTA RAY RESPINGE ESPRESSAMENTE OGNI GARANZIA ESPLICITA O IMPLICITA DI ACCURATEZZA, COMMERCIABILITÀ O IDONEITÀ PER UN DETERMINATO SCOPO. PANTA RAY NON SARÀ IN NESSUN CASO RESPONSABILE NEI CONFRONTI DI ALCUNO PER EVENTUALI DANNI DIRETTI, INDIRETTI, SPCIALI O CONSEQUENZIALI RISULTANTI DALL'USO DELLE INFORMAZIONI CONTENUTE NEL PRESENTE DOCUMENTO OVVERO PER I RISULTATI O LE ATTIVITÀ SVOLTE DA CHIUNQUE, COMPRESI SENZA ALCUN LIMITE, MANCATI GUADAGNI, INTERRUZIONI DEL BUSINESS, DANNI O DISTRUZIONE DI PROPRIETÀ OVVERO PERDITA DI PROGRAMMI O ALTRI DATI, ANCHE SE PANTA RAY È ESPRESSAMENTE INFORMATA DELL'EVENTUALITÀ CHE TALI DANNI SI POSSANO VERIFICARE.

GIANNA DETONI

PANTA RAY

gianna.detoni@pantaray.eu
www.pantaray.eu

UNIVERSITA DEGLI STUDI DI ROMA «TOR VERGATA»
CORSI SECURITY MANAGEMENT

CORSO DI PERFEZIONAMENTO IN «SECURITY MANAGER»

CORSO DI FORMAZIONE IN «PROFESSIONISTA DELLA SECURITY»

3 - 4 DICEMBRE 2021

GIANNA DETONI

Introduzione alle strategie di gestione e di controllo dei rischi

Enterprise Risk Management

Crisis Management e Business Continuity