Conosci la tua azienda per gestire il caos: un modello di valutazione dell'Operational Resilience

SUPERVISION, RISKS & PROFITABILITY 2021

Roma, 23 giugno 2021

A. Giacchero, J. Moretti (Risk Management - Operational & ICT Risk)

Disclaimer

Le opinioni e le metodologie espresse nel presente documento sono esclusivamente degli autori e non rappresentano necessariamente prassi o regole in uso presso il Gruppo Cassa Depositi e Prestiti

Teoria del Caos

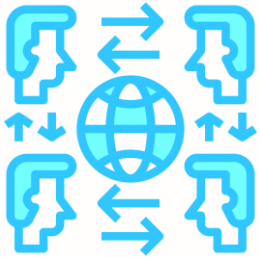
Overview

«Nel mezzo del cammin di nostra vita, mi ritrovai per una selva oscura, ché la diritta via era smarrita..»
Inferno, Canto I

La teoria del caos, in matematica, è lo studio di comportamenti apparentemente casuali o imprevedibili in sistemi governati da leggi deterministiche

Può, il batter d'ali di una farfalla in Brasile, provocare un tornado in Texas? [(1)]

Una minuscola falla nei sistemi di una singola azienda potrebbe mettere a repentaglio la stabilità di un intero sistema



Bisogna avere un caos dentro di sé per generare una stella danzante

(Friedrich Wilhelm Nietzsche)

(1) Titolo di una conferenza tenuta da Edward Lorenz nel 1972

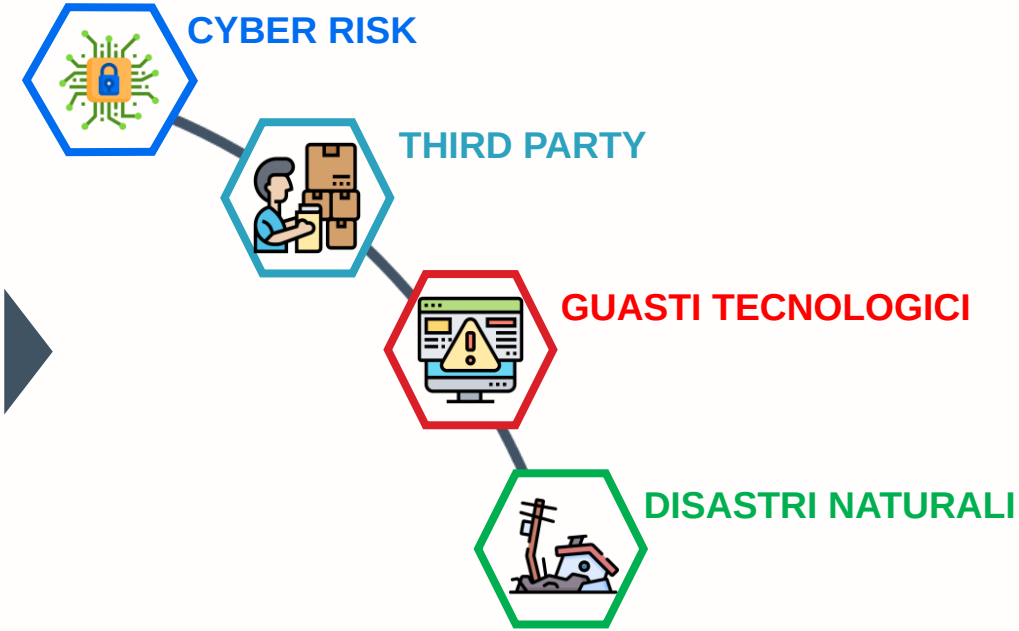
cdp

Operational Resilience

Introduzione

«Per correr miglior acque alza le vele
omai la navicella del mio ingegno,
che lascia dietro a sé mar sì crudele»
Purgatorio, Canto I

Il Comitato di Basilea ritiene necessario che le aziende **rafforzino** la propria **capacità** di **assorbire eventi correlati al rischio operativo:**



Operational Resilience

Focus pandemia

«Or incomincian le dolenti note
a farmisi sentire; or son venuto
là dove molto pianto mi percuote»
Inferno, Canto V

Con il progredire della pandemia di Covid-19, il Comitato ha osservato come le aziende abbiano **adattato rapidamente l'operatività** in risposta ai **nuovi pericoli** a cui potrebbero essere esposte

Elementi

Pragmaticità

Flessibilità

Benefici

Migliorare la capacità di:

> **resistere**
> **adattarsi**
> **riprendersi**

cdp

Operational Resilience

Definizione

«E 'l duca lui: «Caron, non ti crucciare: vuolsi così colà dove si puote ciò che si vuole, e più non dimandare»
Inferno, Canto I

<<The ability of a bank to deliver critical operations through disruption. This ability enables a bank to identify and protect itself from threats and potential failures, respond and adapt to, as well as recover and learn from disruptive events in order to minimise their impact on the delivery of critical operations through disruption>>

Bank for International Settlements - 'Principles for Operational Resilience', March 2021

Alcune considerazioni

Definizione di ***risk appetite*** e ***risk tolerance*** a fronte di eventi disruptive

Discontinuità operativa in caso di eventi disruptive su '***critical operations***'

Correlazione '***risk tolerance*** - ***critical operations'***

cdp

Regulatory story

«Quali colombe dal disio chiamate
con l'ali alzate e ferme al dolce nido
vegnon per l'aere dal voler portate»
Inferno, Canto V

START

Dic 2018 — *'Cyber Resilience: range of practices'* — BIS

Feb 2019 — *'Guidelines on outsourcing arrangements'* — EBA

Nov 2019 — *'EBA guidelines on ICT and security risk management'* — EBA

Dic 2019 — *'Building the UK financial sector's operational resilience'* — FCA, Bank of England

Apr 2020 — *'Ensuring safe management and operational resilience of the financial sector'* — MAS Monetary Authority of Singapore

Mag 2020 — *'Principles on outsourcing'* — IOSCO

Set 2020 — *'Legislative proposal for an EU regulatory framework on digital operational resilience for the financial sector (DORA)'* — European Commission

Ott 2020 — *'Sound Practices to Strengthen Operational Resilience'* — FDIC, Office of the Comptroller of the Currency

Mar 2021 — *'Operational resilience: Impact tolerances for important business services'* — Bank of England, FCA, Bank of England Prudential Regulation Authority

'Principles for Operational Resilience' — BIS

cdp

Elementi essenziali dell’Operational Resilience

Considerazioni

«Tu scaldi il mondo, tu sovr’esso luci;
s’altra ragione in contrario non ponta,
esser dien sempre li tuoi raggi duci»
Purgatorio, Canto XIII

- Le **linee guida** emesse in **precedenza** non tenevano opportunamente in considerazione tutti gli elementi essenziali
- Non tutte le **situazioni di crisi sono evitabili**

Azioni

Nuove linee guida che **riassumono, migliorano** e **integrano** tutte le normative emesse dal Comitato e dalle autorità di Vigilanza

Definizione di **7 princìpi**

Processo rischi operativi

Continuità operativa

Gestione delle terze parti

ICT

Efficace gestione della **resilienza**

Riduzione **impatto incidenti** su servizi, funzioni e sistemi

Operational Resilience

Superare gli orizzonti del Piano di Continuità

«A guisa d'uom che 'n dubbio si raccerta
e che muta in conforto sua paura,
poi che la verità li è discoperta»
Purgatorio, Canto IX

Mitigazione rischi di business e supporto crescita

Minimizzazione impatti eventi disruptive

Identificazione vulnerabilità nuove e in evoluzione

Obiettivo Operational Resilience

OPERATIONAL RESILIENCE

04 05 06 07 03 02 01

Piano ripristino

Gestione crisi

03

Disaster recovery

BUSINESS CONTINUITY MANAGEMENT

Spostamento focus dal consumer banking all'intero insieme dei servizi finanziari

Riduzione di costi strategici e operativi (vantaggi competitivi a lungo termine)

APPROCCIO OLISTICO

cdp

I princìpi dell'Operational Resilience

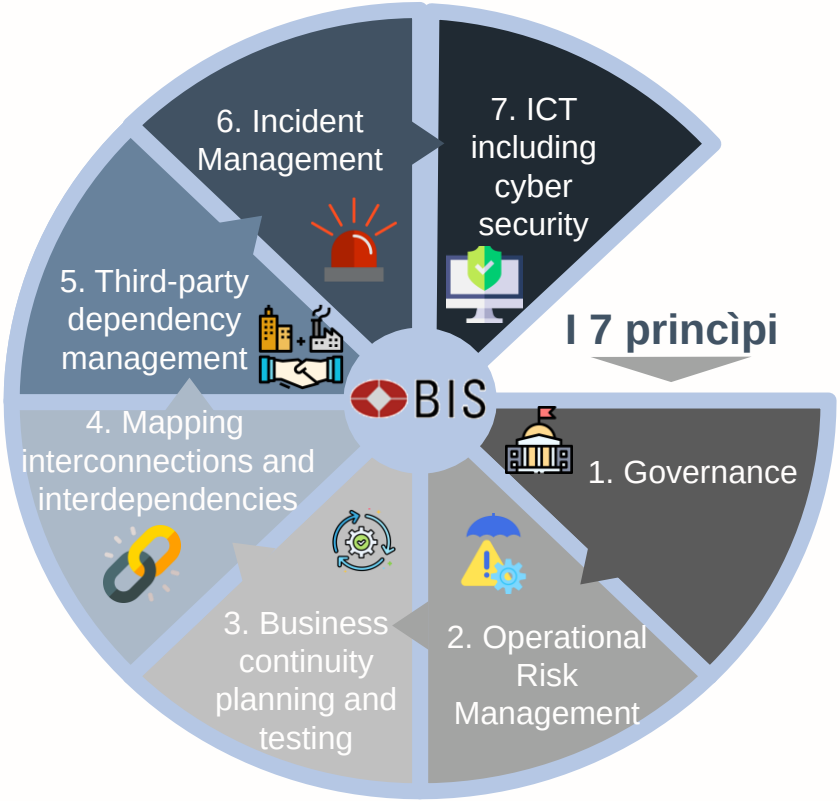
Genesi e riferimenti

«Temer si dee di sole quelle cose c'hanno potenza di fare altrui male; de l'altre no, ché non son paurose»
Inferno, Canto II

Principles for Operational Resilience
(March 2021)

Principles for the Sound Management of Operational Risk
(March 2021)

- I princìpi del Comitato di Basilea per la resilienza operativa sono organizzati in **7 categorie**
- Le 7 categorie si basano sul recente documento '**Principles for the Sound Management of Operational Risk**' nonché su ulteriori linee guida inerenti alla gestione della **corporate governance**, della **business continuity**, dell'**outsourcing** e di risk management



I princìpi dell'Operational Resilience

«Maggior difetto men vergogna lava»
Inferno, Canto XXX

Statement

OBIETTIVO	DESCRIZIONE
▪ Impostazione governance azienda	(i) Rispondere, (ii) adattarsi, (iii) ripristinare e (iv) apprendere
▪ Strutturazione funzione Operational Risk Management	▪ Identificazione minacce ▪ Valutazione rischi potenziali
▪ Test Piano Business Continuity	Garantire la continuità operativa a fronte di scenari di disastro
▪ Identificazione relazioni tra asset aziendali	Inventario di persone, processi, tecnologie, informazioni e facilities
▪ Gestione rischio terze parti	Risk assessment e due diligence pre-stipula su fornitori
▪ Processo di gestione degli incidenti	Lesson learned per il miglioramento del processo
▪ Gestione rischio informatico e cybersecurity	Aggiornamento continuo del catalogo minacce e contromisure

cdp

Il modello di valutazione

Questionario *(1/2)*

«La gloria di colui che tutto move per l'universo penetra, e risplende in una parte più e meno altrove»
Paradiso, Canto I

	Governance	Operational Risk Management	Business continuity planning and testing	Mapping interconnections and interdependencies
I 7 princìpi	1	2	3	4
ESEMPI – Domande	**1.1** E' stata istituita una funzione di Security Risk Management? **1.2** E' stata definita una reportistica periodica e tempestiva agli Organi Societari sulle tematiche di rischio e sulla strategia di gestione dei rischi?	**2.1** Esiste un framework di gestione dei rischi operativi che prevede la valutazione del disegno/adeguatezza dei presìdi di controllo? **2.2** La società organizza iniziative di formazione (corsi, seminari) sui rischi operativi?	**3.1** Sono regolarmente identificati i processi critici dell'azienda, nonché le dipendenze chiave interne ed esterne? **3.2** Il succession plan è stato definito per mitigare lo scenario di indisponibilità di 'personale chiave'?	**4.1** E' stato definito ed è regolarmente manutenuto un inventario degli asset aziendali (people, technology, processes, information, facilities), in cui sono identificate le interconnessioni e le interdipendenze tra gli asset a supporto dei processi critici?
Riferimenti normativi / standard	 Guidelines - Corporate governance principles for banks (July 2015)	 Principles for the Sound Management of Operational Risk (March 2021)	 Circolare 285/2013 Banca d'Italia, 34° aggiornamento 22 settembre 2020	 Framework COBIT 2019 (2019)

Il modello di valutazione

Questionario *(2/2)*

«Le leggi son, ma chi pon mano ad esse?
Nullo, però che 'l pastor che procede,
rugumar può, ma non ha l'unghie fesse»
Purgatorio, Canto XVI

	Third-party dependency management	Incident Management	ICT including cyber security
I 7 princìpi	5 	6 	7 
ESEMPI **Domande**	**5.1** E' previsto un risk assessment ex-ante per valutare i presìdi di sicurezza messi in atto dai fornitori? **5.2** E' stata definita una exit strategy per mitigare il vendor lock-in?	**6.1** E' stato formalizzato un processo di gestione degli incidenti? **6.2** E' previsto un processo di lesson learned che prevede segnalazioni da fonti esterne e da fonti interne (a seguito dell'accadimento di incidenti)?	**7.1** La libreria delle minacce cyber viene aggiornata nel continuo? **7.2** E' previsto un programma di security awareness (*e.g.* campagne di phishing)?
Riferimenti normativi / standard	 EBA Guidelines on outsourcing arrangements (February 2015)	 ITIL Foundation 4 (Febbraio 2019)	 Framework Nazionale per la Cybersecurity e la Data Protection (Febbraio 2019)

Le risposte alle domande sono espresse su una scala di 4 valori
(*cfr.* slide successiva)

cdp

Il modello di valutazione

Scala di valutazione

«Vien dietro a me, e lascia dir le genti: sta come torre ferma, che non crolla già mai la cima per soffiar di venti»
Purgatorio, Canto V

- I Referenti rispondono a ciascuna domanda esprimendo un giudizio sul livello di implementazione della misura indicata, sulla base della seguente scala di Likert [1]

Rating resilienza	Rating resilienza (qualitativo)	Descrizione
4	Ottimo	Le attività e gli strumenti del framework di Operational Resilience sono in linea con le migliori prassi esistenti e sono formalizzati. Sono aggiornati nel continuo, tenendo in considerazione le lesson learned
3	Buono	Le attività e gli strumenti del framework di Operational Resilience sono in linea con le migliori prassi esistenti e sono formalizzati. Non sempre sono aggiornati in considerazione degli incidenti occorsi
2	Sufficiente	Le attività e gli strumenti del framework di Operational Resilience non sempre trovano formalizzazione nel corpo normativo interno (le attività si svolgono in base a prassi operative informali). Non sempre sono aggiornati in considerazione degli incidenti occorsi
1	Carente	Le attività e gli strumenti del framework di Operational Resilience sono implementati solo parzialmente, oppure non aggiornati in base al profilo di rischio dell'azienda
n.a.	Non sa rispondere	Il Referente intervistato non è in grado di stimare il livello di implementazione delle attività e degli strumenti del framework di Operational Resilience. Prudenzialmente, si considera un livello di resilienza 'Carente'

(1) La scala è stata liberamente ispirata dal lavoro di Pescaroli et al., 'A Likert Scale-Based Model for Benchmarking Operational Capacity, Organizational Resilience, and Disaster Risk Reduction', *International Journal of Disaster Risk Science* 11 (2020): 404-409.

Il modello di valutazione

Score finale

«A l'alta fantasia qui mancò possa; ma già volgeva il mio disio e 'l velle, sì come rota ch'igualmente è mossa, l'amor che move il sole e l'altre stelle»

Paradiso, Canto XXXIII

Punteggio di ciascun principio…

Weakest link

Il livello di resilienza di un principio è pari al peggior livello di resilienza rilevato per le domande che vi afferiscono

Esempio Principio 'x'

Domanda 1: Rating 'Ottimo'
Domanda 2: Rating 'Carente'
Domanda 3: Rating 'Ottimo'
Rating di resilienza Principio 'x': 'Carente'

! È sufficiente una minima vulnerabilità per generare un grave incidente

…e score finale della resilienza aziendale

Valore medio

Media aritmetica dei rating di resilienza dei 7 princìpi e arrotondamento a numero intero (vedi tabella)

Media rating (M)	Rating resilienza	Rating resilienza (qualitativo)
M ≥ 3,5	4	Ottimo
2,5 ≤ M < 3,5	3	Buono
1,5 ≤ M < 2,5	2	Sufficiente
M < 1,5	1	Carente

cdp

Conclusioni

«E quindi uscimmo a riveder le stelle»
Inferno, Canto XXXIV

La **resilienza operativa** costituisce, nel contesto attuale, una **prerogativa fondamentale** per gli istituti finanziari

Autovalutare il proprio livello di resilienza operativa consente di identificare gli elementi che - in casi estremi - potrebbero **minare la sopravvivenza** stessa dell'istituto e, di conseguenza, può orientare le **strategie di mitigazione**

Grazie

Fonti immagini

- https://tieniinmanolaluce.me/2013/01/02/dante-alighieri-divina-commedia-inferno-canto-ii-sintesi/
- www.flaticon.com
- https://divinacommedia.weebly.com/inferno-canto-xxx.html
- http://infernodivino.blogspot.com
- http://www.galerie-katerina.org/it/inferno-canto-34-3/
- https://www.bis.org/bcbs/
- https://www.eba.europa.eu/
- https://www.bankofengland.co.uk/
- https://www.mas.gov.sg/
- https://ec.europa.eu/info/index_en
- https://www.fca.org.uk/
- https://www.iosco.org/
- https://www.federalreserve.gov/
- https://www.fdic.gov/
- https://www.occ.treas.gov/
- https://www.axelos.com/store/book/itil-foundation-itil-4-edition
- https://www.isacajournal-digital.org/isacajournal/2019_volume_3/MobilePagedArticle.action?articleId=1485396#articleId1485396ù
- https://www.istockphoto.com/it/illustrazioni/strada
- https://www.limestreetguide.com/event/operational-resilience-lma-webinar
- https://dlpng.com/png/6725387
- https://it.depositphotos.com/80845024/stock-illustration-businessman-pushing-hard-against-falling.html
- https://www.powerusersoftwares.com/