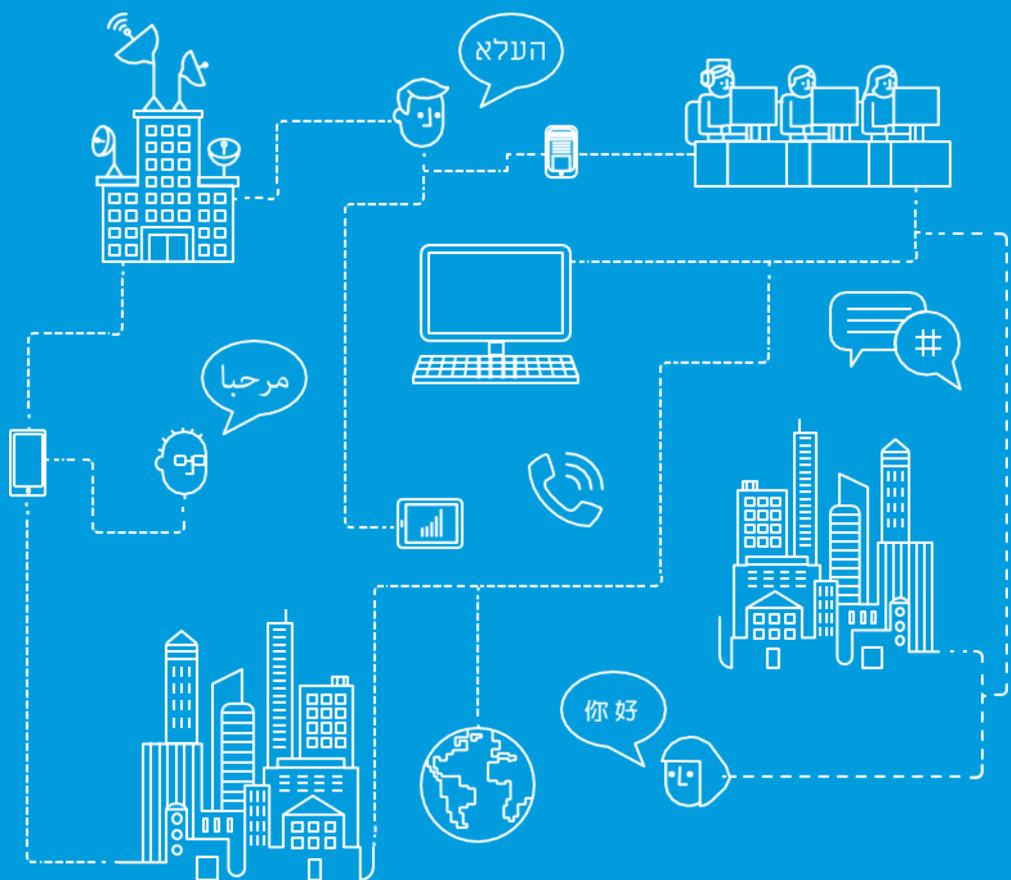


L'importanza di avere un piano B (*Business Continuity*)

Come RSM può aiutarVi ad arrivare preparati e a superare situazioni di crisi



RSM in Italia

Il piano di continuità operativa come strumento per fronteggiare la crisi

Attacco informatico, Pandemia, Fuoco, Alluvione, Terremoto, Sciopero, ...

Questi e altri eventi, più o meno prevedibili, possono costringere le organizzazioni a bloccare la produzione, fermare i sistemi, o persino chiudere gli uffici per giorni, settimane o mesi.

L'emergenza Covid-19 e quella energetica, anche a seguito degli eventi degli ultimi anni, hanno messo in luce limiti e inefficienze di strategie miopi di gestione del rischio, con piani d'emergenza non definiti, obsoleti oppure spesso redatti solo per dovere e mai testati seriamente per verificarne l'efficacia.

Un Piano di Continuità Operativa (PCO) ed un Piano di Disaster Recovery (PDR) efficaci, in tale contesto, possono aiutare le organizzazioni a prevenire o almeno limitare i danni finanziari, tecnologici e fisici derivanti da tali eventi, in modo da ripartire gradualmente, ma in maniera efficiente, con i processi e con il business «*as-usual*» anche dopo eventi disastrosi e imprevisti.

Continuità operativa (definizione ISO 22301:2019):

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

Resilienza (Definizione ISO 22300:2018):

"Capacità di assorbire e di adattarsi in un ambiente in evoluzione"

Elaborare, formalizzare e testare periodicamente un approccio efficace alla gestione dei rischi operativi in azienda vuol dire dare vita a un piano di *Business Continuity Management* tale da gestire proattivamente le situazioni emergenziali e limitare gli effetti degli eventi avversi, accelerando i tempi di ripresa del business.



L'obiettivo di un *Piano di Business Continuity* è di salvaguardare il business dell'organizzazione, il funzionamento dei processi e della supply chain, anche in caso di **eventi** che lo mettono a **rischio**.

- **Eventi imprevedibili o poco probabili:** conflitti, pandemia, eventi naturali, incidenti, blocchi della supply chain), ...
- **Eventi prevedibili:** neve, sciopero, interruzioni programmate della produzione, ...

- Rischio operativo
- Rischio finanziario
- Rischio reputazionale
- Rischio di compliance
- Rischio di sicurezza/safety

I fattori chiave da considerare:

Coerenza: Il Piano deve essere allineato ai requisiti dall'organizzazione e correttamente dimensionato per prioritizzare i processi «critici».

Terze parti: Il Piano deve considerare i rischi derivanti dalla presenza di *outsourcer* e/o terze parti rilevanti, che possano inficiare la corretta operatività dell'organizzazione.

Aggiornamento: Il Piano deve essere costantemente valutato ed, se necessario, aggiornato per riflettere i cambiamenti tecnologici e organizzativi.



La nostra metodologia

Conosciamo le principali pratiche e linee guida, avendo aiutato molte organizzazioni a sviluppare o migliorare i loro PCO e PDR, e supportiamo i nostri Clienti nell'arrivare preparati alla gestione di eventi imprevisti attraverso un'attenta pianificazione, test e formazione del personale.

IL NOSTRO APPROCCIO COMPRENDE CINQUE PASSAGGI:

Avvio del programma.

Esaminiamo i protocolli ed i programmi esistenti, i ruoli e le responsabilità, i documenti, la gestione del piano ed il suo supporto esecutivo oltre che il piano di definizione delle priorità. Molte aziende, possono basarsi su un punto di partenza per poi sviluppare un piano più completo.

Definizione dei requisiti.

Valutiamo le minacce e gli sforzi di mitigazione; analizziamo i driver di impatto aziendale, gli obiettivi di ripristino (*Recovery Point Objective - RPO*) ed i tempi di ripristino (*Recovery Time Objective - RTO*); inoltre conduciamo un'analisi di impatto tecnico, comprensiva delle caratteristiche del sistema Informatico.

Determinazione della strategia.

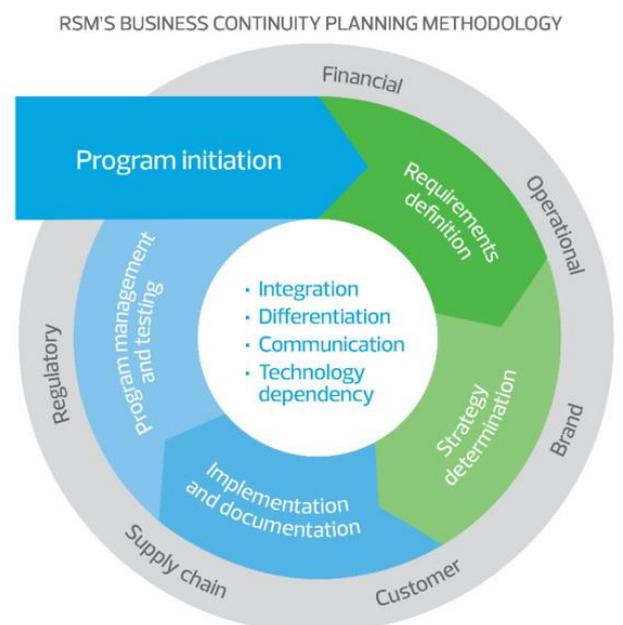
A questo riguardo conduciamo un'analisi delle aree di miglioramento per allineare i requisiti di ripristino aziendale con le capacità attuali dell'azienda, in modo da trovare le migliori opzioni e soluzioni per rimediare a qualunque lacuna riscontrabile.

Pianificare lo sviluppo, l'implementazione e la documentazione

In questa fase, sviluppiamo i piani di ripristino delle risorse tecnologiche (ad es. applicazioni, infrastruttura, documentazione, sequenza di ripristino e documentazione prioritaria), oltre che i piani di continuità operativa, piani di gestione degli incidenti e della crisi e le considerazioni di sicurezza (*fallback plan*).

Gestione e test del programma

Il passaggio finale si concentra sullo sviluppo di processi ricorrenti e sostenibili per garantire che piani e processi documentati rimangano aggiornati e si allineino con gli obiettivi aziendali. I servizi includono esercizi di ripristino (sviluppo della formazione in loco e online) per la Direzione, il personale e la governance.



Come possiamo aiutarVi

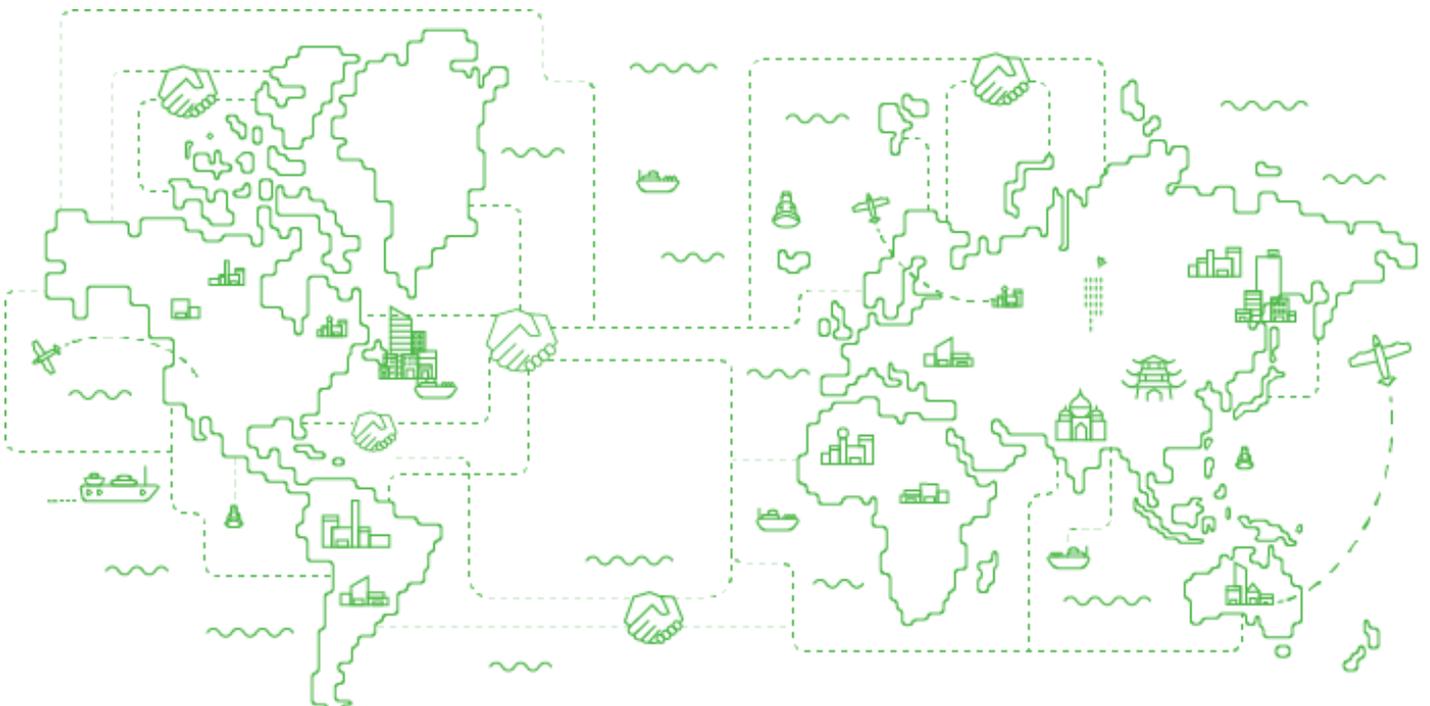
Supportiamo i nostri Clienti con un **team multidisciplinare** che nell'identificazione e nella mitigazione di eventuali lacune dei Piani esistenti, nel definire un Piano da zero, testare protocolli e procedure, formare i dipendenti e mantenere aggiornato il piano man mano che la tua organizzazione cambia nel tempo.

Supporto nello svolgimento di *Business Impact Assessment* degli scenari di crisi sui processi aziendali ritenuti critici

Disegno, audit e valutazione di piani di *Business Continuity* e di piani di *Disaster Recovery*

Disegno, audit e valutazione dell'impianto normativo di riferimento per la gestione delle crisi

Supporto nella predisposizione del sistema di gestione ISO 22301 ed accompagnamento prima, dopo e durante il processo di certificazione



Perché RSM?

Crescita di fatturato globale

15%*

=

\$8bn

RSM è fra le maggiori organizzazioni al mondo specializzate in revisione e consulenza fiscale, societaria e finanziaria.



At RSM, our purpose is to instill confidence in a world of change. Our rapid growth is the result of our professionals supporting clients in over 120 countries to unlock value despite operating in an environment of unprecedented change and unpredictability.



Jean M. Stephens

CEO
RSM International

Crescita percentuale per *Business line*



Consulting



Accounting



Tax



Audit

I nostri numeri



830

Uffici



57,000

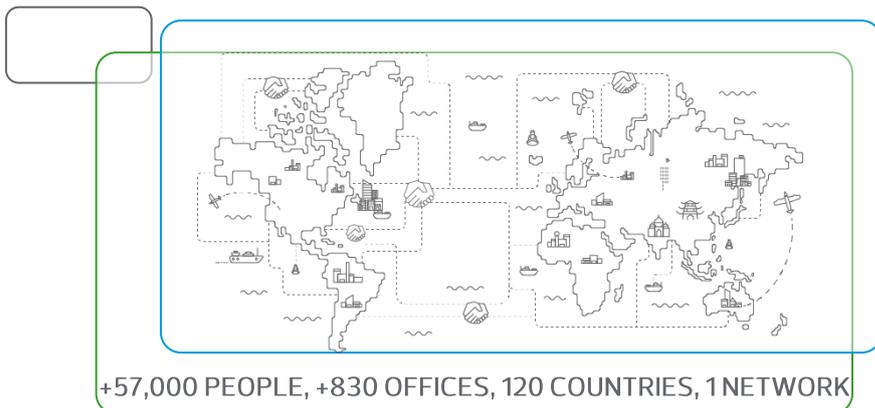
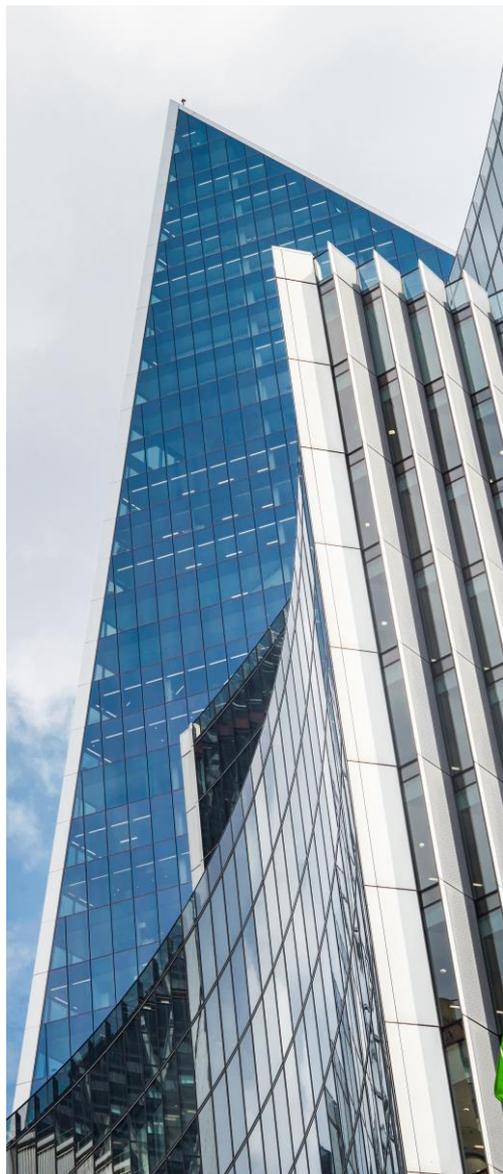
Persone



120

Paesi





Contatti

Simone Segnalini

Partner | Digital, Risk & Transformation Leader

+39 06 87695257

Simone.Segnalini@rsmitaly.com

Mario Bertoli

Director | Digital, Risk & Transformation – Digital & Security

+39 06 87695257

Mario.Bertoli@rsmitaly.com

Luca Quagliata

Senior Manager | Digital, Risk & Transformation – Risk & Internal Controls

+39 06 87695257

Luca.Quagliata@rsmitaly.com



www.rsm.global/italy