GUIDA AI CASI D'USO

# Anticipa, previeni e riduci al minimo l'impatto delle interruzioni dell'attività

Nove best practice per costruire la resilienza operativa

servicenow

Viviamo in tempi incerti. Oggi le organizzazioni devono affrontare numerose minacce operative che possono ostacolare la loro attività, portando a ingenti danni finanziari e reputazionali. Queste minacce spaziano da inondazioni, incendi e terremoti ad attacchi informatici, tensioni politiche e recessioni economiche. Oltre a questi rischi ambientali e sociali esterni, le aziende devono anche fare i conti con le minacce interne, come controversie lavorative, guasti tecnici e violazioni della privacy dei dati, ognuna delle quali può metterle in ginocchio.

Attendere l'arrivo del disastro non è una strategia. È il cocktail perfetto per una catastrofe. Piuttosto, le imprese dovrebbero concentrarsi sulla resilienza operativa: la capacità di anticipare e prevenire le interruzioni operative e la capacità di rispondere, riprendersi e adattarsi rapidamente a questi eventi quando si verificano.

La resilienza deve essere una competenza fondamentale di qualsiasi attività, non un ripiego. E i vantaggi sono evidenti. Una recente ricerca del Boston Consulting Group ha rilevato che le organizzazioni resilienti sono in grado di attenuare lo shock delle crisi, di riprendersi più rapidamente e di recuperare maggiormente rispetto alle organizzazioni meno preparate.  In effetti, secondo la ricerca, circa il 30% del rendimento totale degli azionisti (TSR) di un'azienda è legato alla resilienza.

Ma la resilienza operativa non si ottiene da sola. Richiede un forte impegno organizzativo, una strategia chiara e un'esecuzione efficace. Inoltre, la resilienza operativa è un processo sempre in divenire. Con l'evoluzione delle aziende e delle minacce che esse devono affrontare, le organizzazioni devono continuamente adattarsi e ampliare le proprie funzionalità di resilienza operativa.

In questo white paper esaminiamo nove best practice, basate su esperienze reali e risultati aziendali comprovati, per costruire e mantenere la resilienza operativa.

# 1. Stabilire una governance efficace in tutta l'organizzazione

La resilienza operativa non è limitata a un singolo reparto. Si estende all'intera azienda, coinvolgendo tutte le funzioni aziendali e i vari processi critici. Ad esempio, se la tua è un'azienda manifatturiera, l'anticipazione, la prevenzione e una risposta efficace alle interruzioni sono azioni che non coinvolgono solo i team di produzione, ma anche strutture, risorse umane, IT, il reparto dedicato all'approvvigionamento e molti altri. Anche il comparto Finanza svolge un ruolo fondamentale, sia per sostenere gli investimenti nella resilienza operativa, ad esempio rafforzando le strutture o la sicurezza informatica, sia per garantire che i processi finanziari essenziali su cui si basano i ricavi e i flussi di cassa siano anch'essi resilienti.

Ecco perché la resilienza operativa deve partire dai vertici. I consigli di amministrazione devono definire la resilienza come una priorità aziendale e identificare le aree chiave su cui concentrarsi. Inoltre, essi devono determinare e comunicare chiaramente la propensione al rischio dell'organizzazione. Sapere quali livelli di rischio sono accettabili e in quali aree è fondamentale per costruire la resilienza operativa. Successivamente, la dirigenza deve affrontare queste priorità a livello di consiglio di amministrazione e trasformarle in iniziative specifiche di resilienza, rimuovendo i silo organizzativi, potenziando i responsabili aziendali e funzionali, stabilendo criteri di successo misurabili e implementando un framework per l'esecuzione, la visibilità e la responsabilità. Tale governance non deve sovrapporsi all'attività ordinaria, ma deve permeare i processi aziendali, anziché limitarsi a circondarli.

## 2. Identificare e dare la priorità ai servizi aziendali

Di fatto, la resilienza operativa consiste nel garantire che i servizi aziendali critici siano solidi e al tempo stesso flessibili. Ma che cos'è un servizio aziendale? È una capacità aziendale specifica, come la gestione di transazioni di e-commerce, la gestione dei pagamenti a terzi o il supporto clienti. È probabile che la tua azienda disponga di decine, o addirittura centinaia, di questi servizi. Tuttavia, la loro criticità varia e dipende dal tuo modello aziendale. Ad esempio, è probabile che la gestione delle transazioni di e-commerce sia estremamente critica se sei un rivenditore online, mentre potrebbe esserlo l'approvazione di nuovi clienti se ti occupi di carte di credito.

Identificare e dare priorità ai servizi aziendali richiede un approccio coerente e consolidato. Non può essere fatto in silo organizzativi. Per stabilire le priorità, è necessario avere una visibilità centralizzata e condizioni di parità. Inoltre, nella valutazione dei servizi aziendali bisogna adottare un approccio "esterno". Se si chiede solo al responsabile di un servizio aziendale quanto sia critico il suo servizio, è probabile che ne sopravvaluti l'importanza. Cerca di chiedere anche agli stakeholder aziendali che utilizzano tale servizio o che sono interessati da esso.

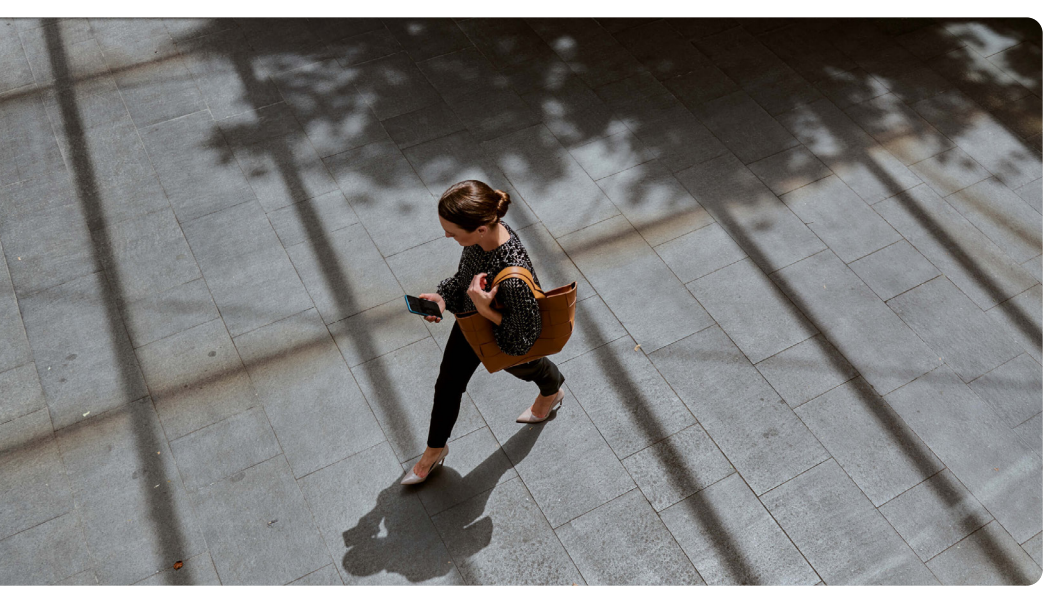
Tornando all'esempio dell'e-commerce, chiedi al reparto Finanza quale sarebbe l'impatto sui ricavi dell'azienda se le tue funzionalità di e-commerce andassero fuori uso. Informati sulla durata: quanto tempo è accettabile per un'interruzione? Un'interruzione di 12 ore per un servizio aziendale di approvvigionamento può essere accettabile, ma un'interruzione di settimane potrebbe portare al blocco dell'intera attività.

# 3. Mappare le dipendenze e le interconnessioni dei servizi aziendali critici

Una volta identificati e classificati i servizi aziendali critici, è necessario sapere come vengono erogati. In genere, ogni servizio aziendale dipende da un insieme ben definito di processi aziendali, strutture, persone e tecnologie, e un problema che riguarda uno qualsiasi di questi componenti di base rappresenta una minaccia per il servizio aziendale nel suo complesso. La comprensione di questi componenti e delle loro correlazioni consente di valutare con rapidità e precisione l'impatto potenziale dei rischi operativi e di intraprendere le azioni più opportune per garantire la resilienza operativa (approfondiremo più avanti).

Anche in questo caso, è necessario un approccio coerente e consolidato. È inoltre importante adottare un approccio iterativo, iniziando con alcuni servizi aziendali critici per accelerare il time to value. Raccogli tutte le dipendenze e le interconnessioni per i servizi aziendali scelti in un unico posto. Creando una visione unificata e affidabile, potenzierai l'intera azienda, consentendo a più funzioni aziendali di collaborare, prendere decisioni informate e orientarsi nella stessa direzione per migliorare la resilienza operativa.

Ma non finisce qui. Nel creare questa visione unificata delle dipendenze e delle interconnessioni, la tempestività e l'accuratezza sono importanti. La scarsa qualità dei dati potrebbe portare a decisioni sbagliate e minare rapidamente la fiducia degli stakeholder aziendali. È importante non cercare di costruire e mantenere un vasto archivio di dati da zero. Piuttosto, integra i dati esistenti dai sistemi in cui già risiedono queste informazioni o, meglio ancora, crea una vista unificata su una piattaforma che già ospita molti di questi dati.



Ad esempio, se la tua organizzazione IT dispone già di un repository (spesso un database di gestione delle configurazioni o CMDB) che raccoglie le applicazioni, l'infrastruttura IT e il modo in cui sono collegate, allora integra questi dati piuttosto che cercare di replicarli manualmente. Non solo creerai fiducia e otterrai risultati migliori, ma risparmierai anche tempo e fatica.

# 4. Prevenire le interruzioni identificando e affrontando in modo proattivo i rischi operativi

Gestire efficacemente i rischi e la conformità costituisce il primo passo nella strategia di resilienza operativa. Identificando proattivamente i rischi e affrontandoli, ridurrai al minimo la probabilità di interruzioni dell'attività. Ricorda che la gestione del rischio deve riguardare l'intera organizzazione e non limitarsi a una funzione aziendale isolata. Facilita la segnalazione dei rischi per ogni membro del personale, ad esempio mettendo a disposizione interfacce self-service che permettono al personale di comunicarli già nel momento in cui si manifestano. Crea processi collaborativi che aiutino i team di rischio e i responsabili aziendali a lavorare insieme per rimediare ai rischi. Ancora una volta, è fondamentale comprendere le dipendenze e le interconnessioni dei processi aziendali per dare priorità ai rischi. Ad esempio, è possibile identificare un rischio per un processo, una struttura o persino un'apparecchiatura IT specifica. Ma per comprenderne la criticità, è necessario sapere su quali servizi aziendali influisce il componente a rischio.

La conformità va di pari passo con la gestione del rischio. Tramite l'implementazione dei controlli, puoi supervisionare i potenziali rischi, in modo da prevenire in modo proattivo gli incidenti operativi. E come abbiamo detto in precedenza, la resilienza operativa deve essere integrata nei processi aziendali, non solo circondarli. Digitalizzando i processi aziendali, puoi incorporare i controlli direttamente nei workflow di processo, assicurandoti che vengano applicati in modo coerente. In questo modo potrai monitorare costantemente i controlli, anziché affidarti solo a verifiche periodiche. Ciò riduce il margine di rischio, così potrai identificare rapidamente le non conformità sistemiche, riconoscerle come rischi emergenti e affrontarle attraverso i processi di gestione del rischio.

# 5. Aumentare la resilienza identificando e analizzando diversi scenari di interruzione

La resilienza operativa non può limitarsi alla teoria. Per raggiungere effettivamente una resilienza operativa, è necessario identificare e analizzare diversi scenari di interruzione al fine di determinare l'impatto che ognuno di essi avrebbe sulla tua azienda.

Immagina di giocare una partita a Jenga. Se estrai un blocco, la tua azienda crolla o la torre rimane in piedi? Ad esempio, cosa succederebbe se un'alluvione colpisse una delle tue strutture? Un'interruzione della filiera ti impedirebbe di rispettare gli impegni contrattuali o la tua azienda sarebbe così resiliente da passare subito a fornitori alternativi? Prendendo in considerazione un'ampia gamma di scenari, potrai identificare le lacune nella tua resilienza operativa e considerarle come rischi a cui porre rimedio.

E ancora una volta (è bene ribadirlo), per analizzare questi scenari è necessario comprendere le dipendenze e le interrelazioni dei servizi aziendali. Torniamo all'esempio della struttura allagata. Quali team lavorano in quella struttura, a quali processi aziendali partecipano e quale infrastruttura fisica è presente? Infine, quali servizi aziendali supportano le persone, i processi e i sistemi interessati?

Ricorda che un'interruzione di queste risorse può avere un impatto su più servizi aziendali e che è necessario comprenderne l'impatto per stabilire la criticità della potenziale interruzione. Anche definire il grado di impatto è fondamentale. Ad esempio, se l'allagamento di una struttura incide solo sul 10% della capacità di produzione, rientrando nei livelli di tolleranza e propensione al rischio, allora potrebbe essere meno critico rispetto a un disastro che interrompe completamente un processo aziendale cruciale. In questo modo è possibile definire le priorità e affrontare il rischio di alluvione, così come altri, in modo appropriato. Considera la durata potenziale dell'impatto e verifica che rientri nei limiti di tolleranza che hai già identificato per i servizi aziendali interessati (ne parleremo più avanti, quando tratteremo la gestione della continuità operativa).

# 6. Concentrarsi sul rafforzamento dell'infrastruttura IT per mantenere in funzione i servizi aziendali

Con la trasformazione digitale delle aziende, la tecnologia è ormai alla base di ogni aspetto delle loro attività. Di conseguenza, il rafforzamento dell'infrastruttura e dei processi IT merita un'attenzione particolare nell'ambito della strategia di resilienza operativa. Ciò comporta due attività correlate. Innanzitutto, assicurati che l'infrastruttura IT sia resistente e possa affrontare tempestivamente le interruzioni e, in secondo luogo, riduci al minimo le probabilità di riuscita e l'impatto degli attacchi informatici.

Per resistere e riprendersi rapidamente dalle interruzioni, è necessario progettare e sfruttare l'IT ai fini della resilienza. Ad esempio, progetta la resilienza con meccanismi di ridondanza e di ripristino automatico, sia che si tratti dell'abilità di tollerare un guasto a un server all'interno di un cluster di server, sia del passaggio automatico a un data center di backup in caso di guasto catastrofico, oppure di assicurarti che i fornitori cloud siano sufficientemente resilienti. Dal punto di vista operativo, investi in strumenti efficaci che ti aiutino a diagnosticare e a risolvere rapidamente problemi quali errate configurazioni dell'infrastruttura, applicazioni e infrastrutture sovraccariche, guasti puntuali e bug software di recente introduzione. In questo caso, la visibilità del servizio aziendale è fondamentale, sia per dare priorità agli investimenti orientati alla resilienza sia per dare priorità e diagnosticare guasti e degrado operativi.

La sicurezza informatica è altrettanto importante. Implementa processi ben strutturati che offrano la visibilità e il controllo necessari per applicare rapidamente le patch alle vulnerabilità del software, per rispondere efficacemente agli incidenti di sicurezza e per identificare e risolvere le configurazioni errate della sicurezza (ad esempio, lo storage cloud non protetto). Ancora una volta, la visibilità dei servizi aziendali è fondamentale. Infatti, una vulnerabilità o un incidente di sicurezza che colpisce un servizio aziendale chiave o i dati personali presenta di solito maggiori criticità rispetto a un incidente che espone il programma di manutenzione delle strutture. E proprio come per gli altri rischi, non è possibile gestire quelli IT in silo. È necessaria una collaborazione interfunzionale. Infatti, sono il team di sicurezza e quello IT a dover rispondere congiuntamente agli attacchi informatici. Se la violazione riguarda dati personali o dei clienti, potrebbe essere necessario coinvolgere anche altri team, come quello legale e delle pubbliche relazioni.

Infine, i rischi IT e di sicurezza informatica devono essere strettamente collegati alla più ampia gestione del rischio operativo. Abbiamo già sottolineato l'importanza di collegare i problemi IT e di sicurezza ai servizi aziendali. Occorre inoltre identificare e gestire i rischi informatici in modo olistico insieme ad altri rischi operativi, ad esempio per stabilire le priorità e allocare gli investimenti per la mitigazione del rischio o per valutare e gestire il rischio di vulnerabilità che rimangono senza patch a causa di problemi di compatibilità del software. Allo stesso modo, sono necessari controlli per evitare che i singoli membri del personale compromettano la sicurezza informatica e che questi siano in grado di segnalare i rischi informatici, come i tentativi di phishing, insieme ad altri tipi di rischi.

# 7. Estendere la resilienza operativa alla catena del valore di terze parti

La tua azienda non è isolata. Per fornire beni e servizi, dipende da un ecosistema di terze parti, tra cui fornitori, canali di distribuzione, partner e altre entità. Ogni relazione è fondamentale per il suo successo, ma può anche minacciare la resilienza operativa. Ad esempio, cosa succederebbe se un fornitore chiave non fosse in grado di effettuare le consegne per un periodo prolungato a causa di interruzioni del lavoro o disordini politici? O se esponesse i dati aziendali critici a causa di pratiche di sicurezza informatica poco rigorose? Quale sarebbe l'impatto sui ricavi se un distributore fallisse? Considera anche i rischi etici: ad esempio, quale sarebbe l'impatto sulla reputazione della tua azienda se un fornitore ricorresse allo sfruttamento o al lavoro minorile?

Ecco il nocciolo della questione. Per aumentare la tua resilienza operativa, dovrai assicurarti che anche i collaboratori di terze parti siano resilienti. Ciò significa valutare costantemente la resilienza e il rischio di terze parti in base all'importanza (o a determinati livelli) prima di avviare una collaborazione. I criteri di valutazione devono essere analoghi a quelli utilizzati per la tua azienda, tra cui la stabilità finanziaria, la sicurezza informatica, la resilienza delle infrastrutture, la vulnerabilità ai rischi esterni e altri fattori. Una volta stabilita la collaborazione, dovrai anche monitorare costantemente la resilienza, ad esempio effettuando valutazioni periodiche. Prendi in considerazione la possibilità di sfruttare i dati di fornitori indipendenti che si occupano di risk intelligence. Questo può aiutarti a rilevare i problemi emergenti molto più rapidamente di quanto non faresti se ti affidassi solo alle verifiche, consentendoti di rispondere in modo proattivo e di ridurre al minimo i potenziali impatti dei rischi.

La valutazione della resilienza di terzi deve essere parte integrante del framework complessivo di resilienza operativa. I rischi di terze parti devono essere collegati ai tuoi servizi aziendali proprio come lo sono i tuoi processi aziendali, le tue strutture, il tuo personale e la tua infrastruttura. La resilienza vale quanto l'anello più debole della catena, quindi è necessaria una visibilità unificata delle dipendenze interne ed esterne per quantificare e migliorare la resilienza.

Il contesto poi è tutto. Ad esempio, se gli stessi beni o servizi vengono offerti da varie terze parti, eventuali problemi con un singolo fornitore potrebbero non comportare un rischio significativo per il servizio aziendale complessivo. Tuttavia, se un fornitore a rischio rappresenta il singolo punto di errore di un servizio aziendale, si tratta di un rischio critico che deve essere affrontato immediatamente. Portando tutte le informazioni sui rischi in un unico luogo, potrai vedere l'intero quadro e prendere decisioni aziendali informate, sia che si tratti della necessità di diversificare la filiera, sia che si tratti dell'insourcing di funzioni aziendali critiche in mancanza di fornitori sufficientemente resilienti.

# 8. Ridurre al minimo l'impatto delle interruzioni creando e collaudando i piani di continuità aziendale

Nonostante i tentativi di prevenire le interruzioni, i disastri si verificheranno comunque. Quando si verificano, è necessario avere tra le mani un piano di risposta efficace. È questo il ruolo della pianificazione della continuità aziendale.

Anticipando e prevenendo le interruzioni, avrai già creato una solida base per la pianificazione della continuità aziendale. Hai identificato i tuoi servizi aziendali critici, mappato le strutture, i processi, le persone e le infrastrutture che li supportano ed esaminato i diversi scenari che potrebbero interrompere i servizi. Conosci anche i tempi di inattività accettabili. Ora è il momento di identificare le fasi di ripristino del servizio aziendale entro il tuo Recovery Time Objective per i principali scenari di interruzione.

Creare questi piani richiede uno sforzo coordinato. Ogni struttura, processo, team o componente dell'infrastruttura ha un proprietario. Questi proprietari hanno il compito di identificare le azioni necessarie per ripristinare un componente interessato, ma anche il tempo necessario per farlo. Combina questi input per creare il tuo piano di ripristino aziendale. Stabilisci se il piano soddisfa il tuo Recovery Time Objective e collabora con i relativi proprietari per risolvere i problemi. Tieni presente che non è necessario che un servizio aziendale si ripristini completamente entro il Recovery Time Objective: l'obiettivo è farlo funzionare abbastanza bene da supportare le operazioni aziendali.

Una volta creato un piano, dovrai testarlo. Crea dei workflow, in particolare workflow digitali automatizzati, che chiedano a ciascun team di ripristino di simulare le azioni da intraprendere. Esamina i risultati dei test e risolvi eventuali problemi. Ripeti questi test regolarmente per assicurarti che il piano continui a funzionare e vada di pari passo con l'evolversi della tua attività. Mantieni il piano aggiornato tenendo traccia delle modifiche ai vari componenti che supportano il servizio aziendale. L'automazione può essere utile in questo senso, ad esempio utilizzando meccanismi di individuazione automatica per tenere traccia dei cambiamenti dell'infrastruttura IT.

Se si verificasse un'interruzione, avresti dei workflow testati per favorire il ripristino. Tuttavia, accertati di avere la flessibilità necessaria per adattarti a circostanze impreviste, anziché limitarti a eseguire il piano alla cieca. Anche avere consapevolezza della situazione è fondamentale, ad esempio utilizzando visualizzazioni basate su mappe per mostrare quali strutture sono a rischio nel momento in cui si verifica un evento climatico. Verifica inoltre di disporre di processi di comunicazione efficaci per collegare i team di recupero, informare il personale e creare visibilità per gli altri stakeholder.

## 9. Lavorare su visibilità e controllo unificati per guidare i progressi e misurare il successo

A questo punto, ti sembrerà evidente il collegamento tra le best practice per la resilienza operativa. Condividono una base comune: la comprensione dei servizi aziendali e delle loro dipendenze e interconnessioni. Le best practice operano insieme per aumentare la resilienza operativa, invece di rimanere in silo. Inoltre, coinvolgono più parti interessate all'interno dell'azienda: non esiste un singolo reparto che si occupa del rischio operativo mentre un altro è l'unico responsabile della pianificazione della continuità operativa.

Per questo motivo, è fondamentale adottare un approccio unificato alla resilienza operativa piuttosto che affidarsi a sistemi sconnessi. Idealmente, è necessaria un'unica piattaforma che offra visibilità e controllo generale, riunendo persone, processi, sistemi e dati per favorire risultati aziendali.

Un approccio unificato è utile a comprendere la totalità della resilienza operativa e in questo modo si possono identificare e guidare iniziative specifiche per migliorarla. Gli stakeholder aziendali hanno a disposizione un framework e degli strumenti comuni, invece di essere oberati da una miriade di sistemi. Inoltre, è possibile definire chiari obiettivi di successo e stabilire metriche per tenere traccia dei progressi.

Ad esempio, puoi misurare il numero complessivo di rischi per un servizio aziendale e verificare se il numero diminuisce nel tempo, sia che tali rischi derivino da terze parti, da vulnerabilità del software, da lacune nella pianificazione della continuità operativa o da altri fattori.

# In sintesi

La tua azienda deve affrontare un numero sempre crescente di minacce interne ed esterne che possono portare a interruzioni operative. Queste possono avere un forte impatto negativo a livello finanziario e reputazionale. Ecco perché è fondamentale concentrarsi sul rafforzamento della resilienza operativa, ovvero la capacità di anticipare e prevenire le interruzioni e di rispondere e recuperare efficacemente quando si verificano.

Seguendo le best practice descritte in questo white paper, potrai incrementare la resilienza operativa, proteggerti dalle interruzioni e accrescere il valore per gli azionisti. Abbiamo trattato nove best practice:

1. Stabilire una governance efficace in tutta l'organizzazione
2. Identificare e dare la priorità ai servizi aziendali
3. Mappare le dipendenze e le interconnessioni dei servizi aziendali critici
4. Prevenire le interruzioni identificando e affrontando in modo proattivo i rischi operativi
5. Aumentare la resilienza identificando e analizzando diversi scenari di interruzione
6. Concentrarsi sul rafforzamento dell'infrastruttura IT per mantenere in funzione i servizi aziendali
7. Estendere la resilienza operativa alla catena del valore di terze parti
8. Ridurre al minimo l'impatto delle interruzioni creando e collaudando i piani di continuità aziendale
9. Lavorare su visibilità e controllo unificati per guidare i progressi e misurare il successo

Scarica il solution brief sulla resilienza operativa

Consulta il Value Calculator per stimare il valore di business che potresti ottenere con ServiceNow

**Note**

[1] Boston Consulting Group, "How Resilient business created Advantage in Adversity during COVID-19" (Come le imprese resilienti hanno saputo sfruttare le avversità durante il COVID-19), 4 novembre 2021

servicenow



servicenow.com/it