Cybersecurity: perché la Certificazione di Sicurezza è essenziale per mitigare il rischio

Valentina Mussi | *ICT SECTOR MANAGER - Bureau Veritas Italia*

RELATRICE

Valentina Mussi

ICT SECTOR MANAGER

Bureau Veritas Italia

BUREAU VERITAS
NEL MONDO

PRESENTE IN 140 PAESI

Bureau Veritas è leader mondiale nei servizi di ispezione, verifica di conformità e certificazione

Fondato nel **1828**, il Gruppo aiuta i clienti a migliorare le proprie performance, offrendo servizi e soluzioni ad alto contenuto innovativo, capaci di assicurare che gli asset, i prodotti, le infrastrutture e i processi soddisfino standard e regolamenti in ambito **qualità**, **salute e sicurezza**, **tutela ambientale** e **responsabilità sociale**.

€ 6.2
miliardi
FY 2024

84.250
DIPENDENTI

400.000+
CLIENTI

~1.600
UFFICI E LABORATORI

BUREAU VERITAS ITALIA HOLDING

In Italia il Gruppo Bureau Veritas è presente con le seguenti società, che fanno capo a Bureau Veritas Italia Holding SpA:

BUREAU VERITAS ITALIA
Servizi di ispezione, verifica di conformità e certificazione

CEPAS
Certificazione delle professionalità e della formazione

BUREAU VERITAS CERTEST
Servizi di ispezione, analisi di laboratorio, audit e assistenza per settori moda e lusso

INSPECTORATE
Servizi di ispezione per settori agricolo, petrolchimico e minerario

QCERTIFICAZIONI
Certificazione di prodotto in ambito biologico, agroalimentare e cosmetico

BUREAU VERITAS NEXTA
Servizi di consulenza e di ingegneria, orientati alla pianificazione strategica e alla sostenibilità

CONTEC AQS
Servizi di consulenza tecnica in ambito salute, sicurezza, ambiente e qualità aziendale

EXENET
Servizi di direzione lavori, sicurezza, collaudi e project management per grandi progetti infrastrutturali

PMPI SOLUTIONS
Servizi di project management e ottimizzazione dei processi operativi

BUREAU VERITAS IN ITALIA

PRESENTE DAL 1839

Il Gruppo è presente in Italia con **Bureau Veritas Italia Holding** e le sue società controllate.

€ 211
milioni
VALORE DELLA PRODUZIONE 2024*

~1.400
DIPENDENTI

22
UFFICI LOCALI

28.000
CLIENTI

~2.200
TECNICI E VALUTATORI

Valore della produzione 2024 delle società:

- Bureau Veritas Italia
- Bureau Veritas Nexta
- Cepas
- Qcertificazioni
- Inspectorate
- Certest

NEWS NORMATIVE CYBER

NIS 2	Direttiva Europea recipita a livello italiano con il decreto attuativo 138/2024 con l'obiettivo di **rafforzare il quadro della sicurezza cibernetica** e combattere efficacemente i rischi causati dal **cyber crime**
DORA	Il Digital Operational Resilience Act (DORA) è un regolamento dell'Unione Europea (UE) che mira a **rafforzare la resilienza digitale del settore finanziario.**
CRA	Il Cyber Resilience Act è un regolamento europeo che introduce **requisiti obbligatori di sicurezza informatica per i prodotti hardware e software**, durante il loro intero ciclo di vita. È pensato per **garantire che i prodotti con elementi digitali siano sviluppati in modo più sicuro, proteggendo in ultima analisi i consumatori in tutta Europa. Integra l'attuale quadro giuridico per il marchio CE (dichiarazione di conformità UE) per le proprietà di sicurezza.**
RED	La Direttiva RED (Radio Equipment Directive) è una direttiva europea **che stabilisce le norme per la fabbricazione di apparecchiature radio**. **Si applica a tutti i dispositivi che emettono e ricevono onde radio, come radio, televisori, dispositivi per garage e sistemi di monitoraggio che tramite una connessione internet possano essere esposti a problematiche di cybersicurezza**. Per mitigare questi rischi, la Commissione europea ha adottato un atto delegato -(UE) 2022/30 - della direttiva RED sulle apparecchiature radio al fine di **aumentare il livello di sicurezza informatica, la protezione dei dati personali e della privacy e la protezione delle transazioni finanziarie.**
DATA ACT	Il Data Act è il regolamento che impone agli Stati membri e alle aziende di **armonizzare le proprie normative e procedure sull'accesso ai dati**, e impone una gestione condivisa di queste risorse, ridisegnando il confine tra il controllo nazionale e il potere sovranazionale dell'Unione Europea.
REG MACCHINE	Il Nuovo regolamento Macchine nasce dalla necessità di **uniformare i requisiti di Security e Safety all'interno dell'Unione Europea per far sì che siano aggiornati rispetto al progresso tecnologico.** Il nuovo Regolamento impone di verificare ed affrontare il **rischio connesso ad un attacco cyber con ripercussioni sulla parte di safety**, cioè quella relativa alla sicurezza degli operatori e dell'ambiente.
ACCESSIBILITY ACT	L'Accessibility Act, o European Accessibility Act (EAA), è una direttiva UE (2019/882) che mira a **garantire l'accessibilità di prodotti e servizi specifici per le persone con disabilità.**

GOVERNANCE E GESTIONE DEL RISCHIO

POLICY DI CYBERSICUREZZA	GESTIONE INTEGRATA DEL RISCHIO	IDENTIFICAZIONE VULNERABLITA'	ANALISI DEL RISCHIO
Una chiara policy di Cybersecurity deve essere documentata e comunicata all'intera organizzazione	I processi di governance devono includere la gestione dei rischi di cybersecurity	Tutte le vulnerabilità dei sistemi e dispositivi devono essere identificate e documentate	La valutazione deve considerare minacce e vulnerabilità probabilità e impatti potenziali

BRUCE SCHNEIER, CRITTOGRAFO AMERICANO:

«LA SICUREZZA INFORMATICA 'E UN PROCESSO NON UN PRODOTTO»

Composto da:

TECNOLOGIE

PERSONE

POLICIES E PROCEDURE

PROTEGGERE LA NOSTRA AZIENDA SIGNIFICA PROTEGGERE TUTTI

QUALI SONO I DANNI DETERMINATI DA UN ATTACCO CYBER?

Richiste di risarcimento da parte di terzi

Danni economici

Danno reputazionale e perdita di clienti e fornitori

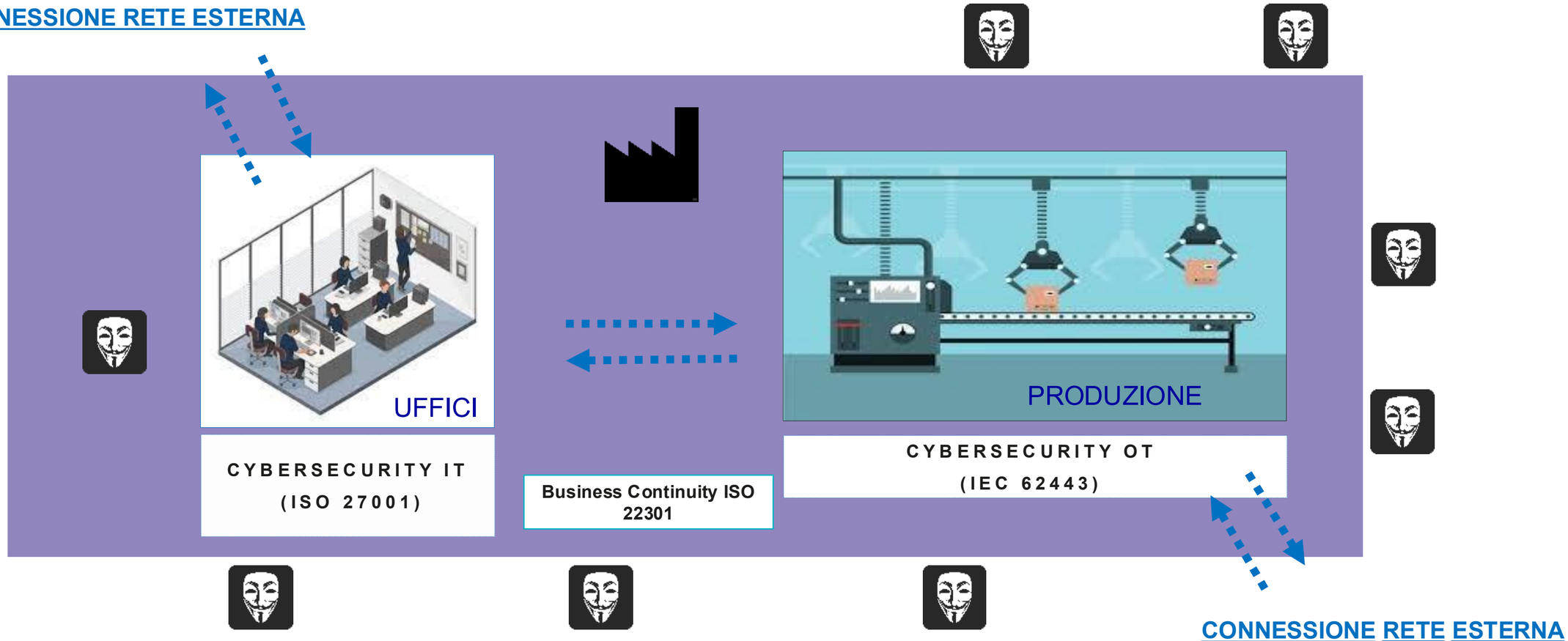
Danni materiali sistemi informatici e hardware

Danni interruzione attività

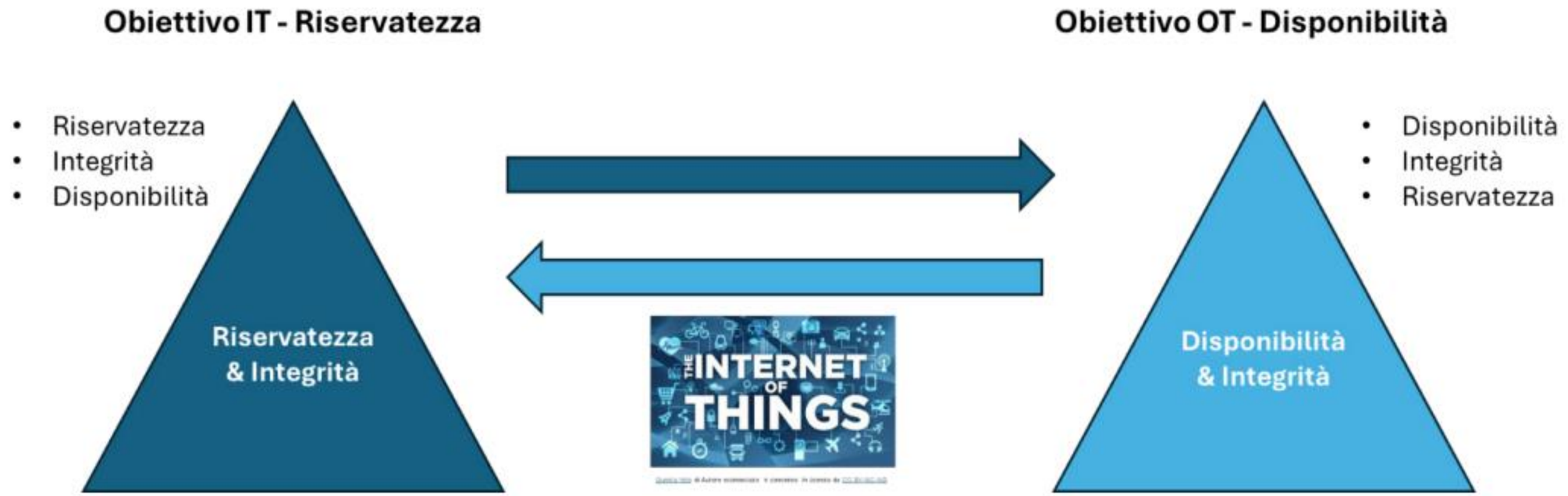
Furto dati/ proprietà intellettuale etc

Danni – Sicurezza – Persone

CYBERSECURITY IT- OT



INTEGRAZIONE CYBERSICUREZZA TRA AMBIENTI IT E OT



REPORT CLUSIT 25 – rapp. grafica di Federica M. R. Livelli

COME CALCOLARE L'IMPATTO DI UN ATTACCO CYBER?

BUSINESS IMPACT ANALYSIS (B.I.A.)

VALUTAZIONE DELL'IMPATTO: ALTO / MEDIO / BASSO

IMPATTO ECONOMICO

1. Alto: ha conseguenze in grado di incidere significativamente sul risultato economico dell'azienda, assorbibili in più esercizi;

2. Medio: ha conseguenze rilevanti sul risultato economico dell'azienda, comunque assorbibili nell'esercizio di riferimento**;**

3. Basso: ha conseguenze non rilevanti sul risultato economico dell'azienda.

IMPATTO NORMATIVO

1. Alto: esiste il rischio di sospensione dell'attività specifica o di una non conformità particolarmente significativa;

2. Medio: esistono sanzioni amministrative/penali contrattuali;

3. Basso: nessun tipo di sanzione/non conformità.

IMPATTO REPUTAZIONALE

1. Alto: se il mercato percepisce l'indisponibilità dei prodotti/servizi erogati dal sotto processo con conseguenze sulla fidelizzazione della clientela e sull'avviamento che si manifestano per un periodo maggiore dell'esercizio di riferimento;

2. Medio: se il mercato percepisce l'indisponibilità dei prodotti/servizi erogati dal sotto processo ma, attraverso opportuni presidi (comunicazione, presidi organizzativi, altro) viene mantenuta la fidelizzazione della clientela senza conseguenze sull'avviamento, o comunque contenute nell'esercizio di riferimento;

3. Basso: se l'indisponibilità dei prodotti/servizi erogati dal sotto processo non viene percepita dal mercato (portatori di interessi, terzi, non percepiscono l'indisponibilità dei prodotti/servizi erogati dal processo).

BUSINESS IMPACT ANALYSIS (B.I.A.)

FASI DELLA BIA

- **Identificazione delle attività critiche per l'organizzazione "Critical Business Functions- attività, processi e sistemi essenziali " (CBF):** l'analisi di tutte le attività svolte dall'organizzazione e l'individuazione di quelle che sono fondamentali per la continuità del business.

- **L'identificazione dei rischi associati a ciascuna attività critica:** analisi dei i rischi che possono influenzare la disponibilità delle attività critiche, ad esempio guasti hardware o software, problemi di sicurezza, eventi naturali, errori umani, etc.

- **La valutazione degli impatti derivanti dalla mancata disponibilità delle attività critiche**. Analisi degli gli effetti negativi che la mancata disponibilità delle attività critiche potrebbe avere sull'organizzazione, ad esempio perdite finanziarie, danni all'immagine dell'azienda, perdita di clienti, etc.

PERSONALE
PROCESSI ORGANIZZATIVI
SISTEMI E APPLICAZIONI

BUSINESS IMPACT ANALYSIS (B.I.A.)

ESECUZIONE BIA – ALCUNE METRICHE PER LA DETERMINAZIONE

- **Tempo di inattività massimo tollerabile (Maximum Tolerable Downtime) o Interruzione massima accettabile (Maximum Acceptable Outage)** – esprime il lasso totale di tempo per il quale una CBF può non essere disponibile senza causare danni significativi per l'organizzazione. Questo indicatore viene generalmente definito dall'owner del sistema, che è responsabile anche verso l'organizzazione per il corretto funzionamento delle CBF.

- **Recovery Time Objective (RTO)** – esprime il periodo di tempo massimo entro il quale una CBF deve essere ripristinata in seguito ad una interruzione di servizio per evitare gravi conseguenze per l'organizzazione. Poiché il superamento del MTD porterebbe a danni significativi, l'RTO per definizione, deve essere inferiore o uguale ad esso.

- **Recovery Point Objective (RPO)** – rappresenta la quantità di dati la cui perdita è considerata tollerabile, e può essere rappresentata anche come periodo di tempo, ad esempio in caso di RPO uguale ad un giorno si intende che non è tollerabile la perdita di più di un giorno di dati. Questo indicatore, così come l'indicatore MTD, deve essere definito dall'organizzazione

BUSINESS IMPACT ANALYSIS (B.I.A.)

RISULTATI DELLA BIA

I principali risultati derivanti dalla BIA includono **l'identificazione delle attività critiche per il business,** i **rischi associati** e gli **impatti derivanti** dalla mancata disponibilità delle stesse.

La BIA definisce le **priorità di ripristino delle attività critiche e le strategie di continuità** del business per minimizzare gli impatti negativi derivanti da eventuali interruzioni delle attività.

BUSINESS IMPACT ANALYSIS (B.I.A.)

IMPLEMENTAZIONE RISULTATI BIA

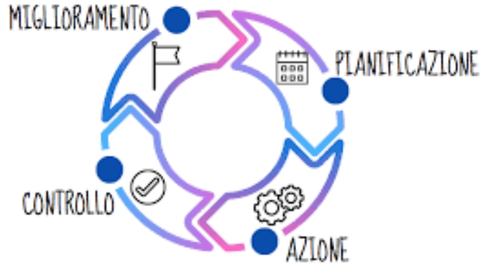
Obiettivo: **implementare le misure di continuità del business per garantire la ripresa delle attività il più rapidamente possibile:**

- Procedure di emergenza e **policy di governance**;
- La creazione di squadre di ripristino delle attività;
- La definizione di un sistema di comunicazione di emergenza;
- Creazione di piani di ripristino delle attività.

VANTAGGI NELL'ADOZIONE DI UN SISTEMA DI GESTIONE IN RELAZIONE ALLA BIA

ISO 27001
IEC 62443
ISO 22301

- ✓ **Valorizzazione e protezione degli Asset**
- ✓ **Aumento della consapevolezza dei rischi e delle contromisure adottate o da adottare**
- ✓ **Responsabilizzazione e formazione delle Risorse Umane, anche tramite di training specifici**
- ✓ **Monitoraggio continuo**



Le fasi del ciclo di Deming sono:

› **Plan –** l'organizzazione identifica i rischi cyber potenziali che potrebbero influire sulle sue operazioni e pianifica strategie di mitigazione appropriate stabilendo obiettivi chiari in termini di livello di rischio.

› **Do –** in questa fase, le strategie di risposta al rischio vengono implementate al fine di ridurre il rischio cyber entro i livelli desiderati sulla base della pianificazione effettuata nella fase "Plan".

› **Check –** monitoraggio continuo dell'efficacia delle misure di risposta al rischio implementate nella fase precedente. Inoltre, si raccolgono dati e si analizzano i risultati per verificare se gli obiettivi di gestione del rischio sono stati raggiunti.

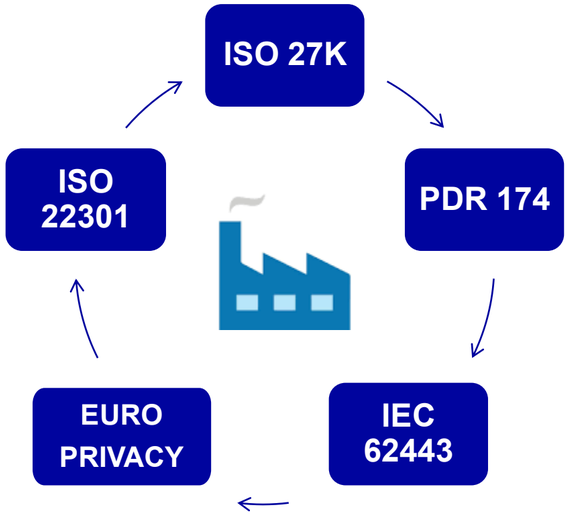
› **Act –** sulla base dei risultati della fase di verifica, si apportano modifiche e miglioramenti alle strategie di gestione del rischio cyber. Vengono intraprese azioni correttive per risolvere le carenze identificate e le strategie di risposta vengono adattate per rispondere ai cambiamenti nel contesto dell'organizzazione o nei rischi stessi.

VANTAGGI NELL'ADOZIONE DI UN SISTEMA DI GESTIONE INTEGRATO

- ✓**Valorizzazione e protezione degli Asset**
- ✓**Aumento della consapevolezza dei rischi e delle contromisure adottate o da adottare**
- ✓**Responsabilizzazione e formazione delle Risorse Umane, anche tramite di training specifici**
- ✓**Monitoraggio continuo**

Vantaggi Operativi

- Standardizzazione
- Flessibilità
- Adattabilità
- Consapevolezza diffusa



Vantaggi Strategici

- Approccio olistico
- Riduzione della frammentazione
- Ottimizzazione degli investimenti
- Maggiore efficacia dei controlli

Q&A

Contatti:

VALENTINA MUSSI

ICT Sector Manager

valentina.mussi@bureauveritas.com

BUREAU VERITAS ITALIA

Venite a trovarci al nostro Stand!