✓ SETTORE — 2 REPORT

RISK ASSESSMENT LIGHT

Finanza & Banca

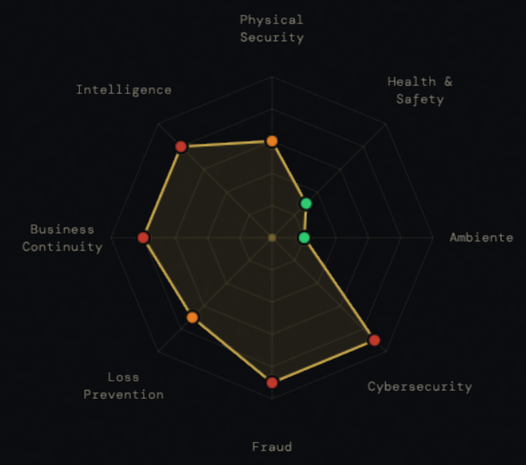
DATA ANALISI
26 maggio 2026

METODOLOGIA
ISO 31000 / Light

AREE ANALIZZATE
8 domini di rischio

LIVELLO GLOBALE
Critico

● LIVELLO DI RISCHIO GLOBALE: CRITICO



78 /100

Il settore finanziario è caratterizzato da rischi critici in cybersecurity e frodi. La continuità operativa è fondamentale date le stringenti normative (DORA, PSD2). L'intelligence è prioritaria.

4	2	0	2
CRITICI	ALTI	MEDI	BASSI

ANALISI PER DOMINIO DI RISCHIO

6

Physical Security

ALTO

Elevata esposizione. Richiesta pianificazione strutturata della sicurezza fisica.

AZIONI RACCOMANDATE
- → Security patrol H24
- → Analisi vulnerabilità fisica
- → Perimetro fisico rinforzato

3

Health & Safety

BASSO

Ambiente di lavoro a basso rischio infortunistico. Adempimenti base D.Lgs 81/08 sufficienti.

AZIONI RACCOMANDATE
- → DVR aggiornato
- → Formazione base lavoratori

2

Ambiente

BASSO

Impatto ambientale ridotto. Adempimenti standard ISO 14001 applicabili.

AZIONI RACCOMANDATE
- → Registro rifiuti
- → Formazione ambientale

9

Cybersecurity

CRITICO

Rischio cyber critico. Target ad alto valore per attaccanti. Richiesta difesa in profondità.

AZIONI RACCOMANDATE
- → CISO dedicato
- → Zero trust architecture
- → Red teaming continuo

9

Fraud

CRITICO

Rischio frode critico. Target primario per organizzazioni criminali. Necessario presidio specialistico.

AZIONI RACCOMANDATE
- → Fraud investigation team
- → Analisi comportamentale
- → Presidio antifrode H24

7

Loss Prevention

ALTO

Elevato rischio di perdite patrimoniali. Richiesto programma LP strutturato.

AZIONI RACCOMANDATE
- → Analisi shrinkage
- → CCTV analitico
- → Team LP dedicato

8

Business Continuity

CRITICO

Business continuity critica. Interruzioni hanno impatto sistemico. DRP completo indispensabile.

AZIONI RACCOMANDATE
- → Resilienza multi-sito
- → Esercitazioni crisi
- → Certificazione ISO 22301

8

Intelligence

CRITICO

Target ad alto valore per intelligence. Richiesta controintelligence e threat assessment continuo.

AZIONI RACCOMANDATE
- → Counterintelligence program
- → Monitoraggio dark web
- → Intelligence officer dedicato

NOTA METODOLOGICA
Il presente documento costituisce un'analisi preliminare di risk assessment di tipo "light", basata su profili di rischio tipici per categoria di settore. Non sostituisce un'analisi di rischio approfondita, personalizzata e condotta in loco da professionisti qualificati. Benedetti Group S.r.l. declina ogni responsabilità per decisioni operative adottate sulla base esclusiva di questo report indicativo. Per un'analisi completa e certificata, contattare il nostro team di esperti.

← NUOVA ANALISI

© 2026 Benedetti Group S.r.l. — Tutti i diritti riservati