DIGITALCAMPUS
guidiamo l'innovazione

CSI
your digital partner

Corso NIS2 Advanced

Risk Management

Relatore: **Marcello Cutrone** (Business Continuity Manager - CSI Piemonte)

Alessandria, 19 maggio 2026

ASL AL
REGIONE PIEMONTE

Contenuti del corso

Risk Management e NIS2

Il processo ISO 31000

Una metodologia per l'identificazione, la valutazione e la ponderazione dei rischi

Strategie di trattamento del rischio

RISK Management e NIS2

La Direttiva NIS2 – Misure

Misure di sicurezza di base

41 misure di sicurezza → 10 ambiti di sicurezza NIS

- 36 per soggetti essenziali e importanti.
- 5 addizionali solo per i soggetti essenziali.

Struttura misura: codice + descrizione + requisiti

- Il codice identificativo e la descrizione della misura fanno riferimento al FNSC.
- I requisiti indicano ciò che è richiesto ai fini dell'implementazione.

116 requisiti → Proporzionalità

- 82 per soggetti essenziali e importanti.
- 34 addizionali solo per i soggetti essenziali.

La Direttiva NIS2 – Approccio basato sul rischio

14 requisiti per i soggetti importanti
e **19** per i soggetti essenziali

6 requisiti per i soggetti importanti
e **9** per i soggetti essenziali

Facoltà di limitare l'ambito di applicazione per specifici requisiti ai sistemi informativi di rete la cui compromissione determina un impatto significativo su R, I, D delle attività e servizi per i quali il soggetto rientra nell'ambito di applicazione del decreto NIS.

“ … per almeno i sistemi informativi e di rete rilevanti … ”

“ … in accordo agli esiti della della valutazione del rischio di cui alla misura … ”

Possibilità di adattare le modalità di attuazione di specifici requisiti sulla base degli esiti della valutazione del rischio.

Deroga all’applicazione del requisito se sussistono vincoli normativi (ad esempio, leggi o regolamenti) o tecnici (ad esempio, limiti tecnologici o operativi) che non ne permettano l’implementazione.

“ … fatte salve motivate e documentate ragioni normative o tecniche … ”

“ … forniture con potenziali impatti sulla sicurezza … ”

Sono considerate le forniture la cui eventuale compromissione può determinare effetti sulla sicurezza dei sistemi informativi e di rete.

8 requisiti per i soggetti importanti
e **10** per i soggetti essenziali

3 requisiti per i soggetti importanti
e per i soggetti essenziali

ASL AL
REGIONE PIEMONTE

Rischi e NIS2

Politica e Procedura

GV.PO-01

Sono adottate e documentate politiche di sicurezza informatica per almeno i seguenti ambiti:

a) gestione del rischio;
b) …

Deve essere redatta una policy di sicurezza informatica che preveda che siano gestiti i rischi

GV.RM-03

Nel rispetto delle politiche di cui alla misura GV.PO-01, è definito, attuato, aggiornato e documentato un piano di gestione dei rischi per la sicurezza informatica per identificare, analizzare, valutare, trattare e monitorare i rischi.

Deve essere redatto un piano che descriva le responsabilità e le modalità operative per la gestione del rischio

ASL AL
REGIONE PIEMONTE

Assessment dei rischi

ID.RA-05

In accordo al piano di gestione dei rischi per la sicurezza informatica di cui alla misura GV.RM-03, è eseguita e documentata la valutazione del rischio posto alla sicurezza dei sistemi informativi e di rete, anche con riferimento alle eventuali dipendenze da fornitori e partner terzi, che comprende almeno:

a) l'identificazione del rischio;
b) l'analisi del rischio;
c) la ponderazione del rischio.

Deve essere eseguito un risk assessment, aggiornato almeno ogni 2 anni e approvato dagli organi di amministrazione e direttivi

Il risk assessment, deve prendere in considerazione almeno le minacce interne ed esterne, le vulnerabilità non risolte e gli impatti conseguenti ad eventuali incidenti

Rischi e NIS2

Piano di trattamento dei rischi

È definito, documentato, eseguito e monitorato un **piano di trattamento del rischio** che comprende almeno:

ID.RA-06

a) le opzioni di trattamento e le misure da attuare in merito al trattamento di ciascun rischio individuato e le relative priorità;
b) le articolazioni competenti per l'attuazione delle misure di trattamento dei rischi e le tempistiche per tale attuazione;
c) la descrizione e le ragioni che giustificano l'accettazione di eventuali rischi residui al trattamento.

Deve essere definito un piano di trattamento dei rischi con indicazione delle strategie di trattamento e delle azioni di mitigazione
Il piano deve essere approvato dagli organi di amministrazione e direttivi

ASL AL
REGIONE PIEMONTE

Efficacia delle misure

ID.IM-01

È definito, attuato, aggiornato e documentato un **piano per la valutazione dell'efficacia delle misure di gestione del rischio** per la sicurezza informatica che comprenda l'indicazione delle misure da valutare e i relativi metodi di valutazione.

L'efficacia delle misure e dei presidi deve essere valutata e monitorata

Accordi di riservatezza

GV.RR-04

In accordo agli esiti della valutazione del rischio di cui alla misura ID.RA-05, sono definiti a livello contrattuale gli eventuali obblighi, in materia di sicurezza informatica, che rimangono validi dopo la cessazione o la modifica del rapporto di lavoro dei dipendenti del soggetto NIS (ad esempio prevedendo clausole in materia di riservatezza).

L'assessment dei rischi deve prevedere la valutazione del rischio di sicurezza relativo ai dipendenti ed in funzione di questa valutazione devono essere definite eventuali accordi di riservatezza da sottoporre al personale.

Rischio di fornitura

GV.SC-07

Nell’ambito della valutazione del rischio di cui alla misura ID.RA-05, è valutato e
documentato il rischio associato alle forniture. A tal fine, sono valutati almeno:
a) il livello di accesso del fornitore ai sistemi informativi e di rete del soggetto NIS;
b) l'accesso del fornitore alla proprietà intellettuale e ai dati anche sulla base della loro criticità;
c) l'impatto di una grave interruzione della fornitura;
d) i tempi e i costi di ripristino in caso di indisponibilità dei servizi;
e) i ruoli e le responsabilità del fornitore nel governo dei sistemi informativi e di rete.

L’assessment dei rischi deve prevedere la valutazione del rischio associato alle forniture

Affidamento di forniture

GV.SC-01

In merito all'affidamento di forniture con potenziali impatti sulla sicurezza dei sistemi informativi e di rete, anche mediante ricorso agli strumenti delle centrali di committenza … sono previsti:
a) il coinvolgimento dell'organizzazione per la sicurezza informatica di cui alla misura GV.RR-02 nella definizione ed esecuzione dei processi di approvvigionamento a partire dalla fase di identificazione e progettazione della fornitura;
b) in accordo **agli esiti della valutazione del rischio** associato alla fornitura di cui alla misura GV.SC-07, la definizione di requisiti di sicurezza sulla fornitura coerenti con le misure di sicurezza applicate dal soggetto NIS ai sistemi informativi e di rete.

I requisiti delle forniture dovranno comprendere i requisiti di sicurezza che saranno determinati dal risultato della valutazione del rischio

Rischi e NIS2

Sistemi informativi e di rete rilevanti

Per almeno i sistemi informativi e di rete rilevanti e in accordo agli esiti della valutazione del rischio:

PR.AA-03	sono impiegate modalità di autenticazione multifattore
PR.DS-01	fatte salve motivate e documentate ragioni normative o tecniche, i dati memorizzati sui dispositivi portatili, ivi inclusi laptop, smartphone e tablet, e sui supporti removibili, sono cifrati con protocolli e algoritmi allo stato dell'arte e considerati sicuri.
PR.DS-02	fatte salve motivate e documentate ragioni normative o tecniche, sono utilizzati, per la trasmissione dei dati da e verso l'esterno del soggetto NIS, protocolli e algoritmi di cifratura allo stato dell'arte e considerati sicuri.

ASL AL
REGIONE PIEMONTE

Rischi e NIS2

Accesso ai sistemi

PR.AA-01

Tutte le utenze, ivi incluse quelle con privilegi amministrativi e quelle utilizzate per l'accesso remoto, sono censite, approvate da attori interni al soggetto NIS e, fatte salve motivate e documentate ragioni tecniche, in accordo agli esiti della valutazione del rischio di cui alla misura ID.RA-05, sono individuali per gli utenti.
Le credenziali (ad esempio nome utente e password) relative alle utenze sono robuste e aggiornate in accordo agli esiti della valutazione del rischio di cui alla misura ID.RA-05.

PR.AA-03

Le modalità di autenticazione delle utenze per accedere ai sistemi informativi e di rete sono commisurate al rischio.

A tal fine sono valutati almeno i rischi connessi:
a) ai privilegi delle utenze;
b) alla criticità dei sistemi informativi e di rete;
c) alla tipologia di operazioni che le utenze possono effettuare sui sistemi informativi e di rete.

ASL AL
REGIONE PIEMONTE

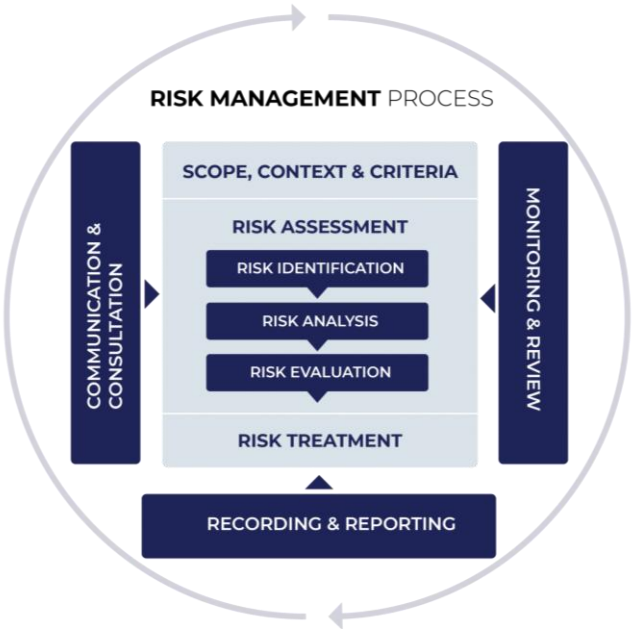
Gestione dei Log

PR.PS-04

In accordo agli esiti della valutazione rischio di cui alla misura ID.RA-05, sono definite e documentate le tempistiche di conservazione dei log.

RISK Management: il processo ISO 31000

Il processo secondo la norma ISO 31000



Risk appetite (propensione al rischio)

Risk tolerance (devianza tollerabile rispetto alla propensione)

Risk capacity (massimo livello di rischio sopportabile)

Identificare le minacce e le opportunità

Analizzare il rischio (Probabilità e Impatti)

Ponderare il rischio rispetto alle soglie

- Aver chiari gli **obiettivi del business**
- Definire le **soglie di tolleranza**
- Fare un **Risk assessment**
- Scegliere le azioni di trattamento dei rischi valutati
- **Identificare gli indicatori di rischio** e i parametri di controllo (KRI)
- Reporting e approvazione da parte del management
- Monitoraggio, miglioramento e revisione periodica

Il rischio è….

Il rischio è….

L’**effetto** dell’**incertezza** sugli **obiettivi**



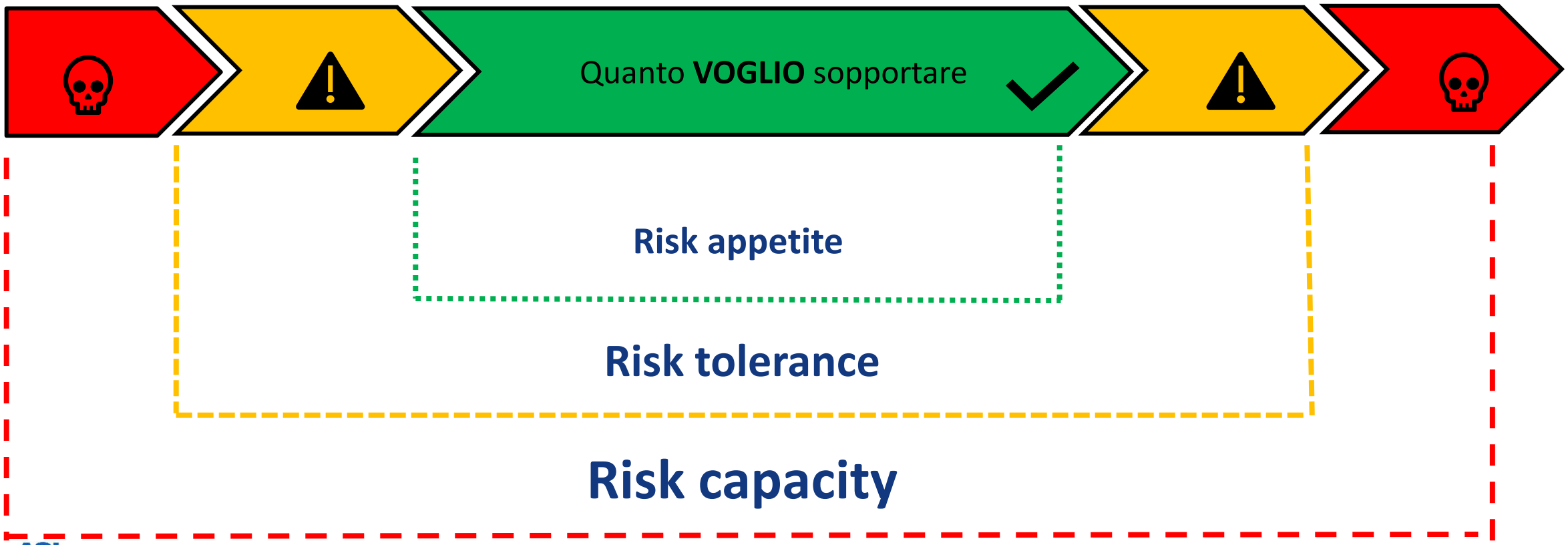
Obiettivi del business

- **S** SPECIFIC
- **M** MEASURABLE
- **A** ACHIEVABLE
- **R** RELEVANT
- **T** TIME-BASED

Stabilire le soglie di tolleranza al rischio

Piano strategico

Quanto **POSSO DISCOSTARMI** dai miei **obiettivi**

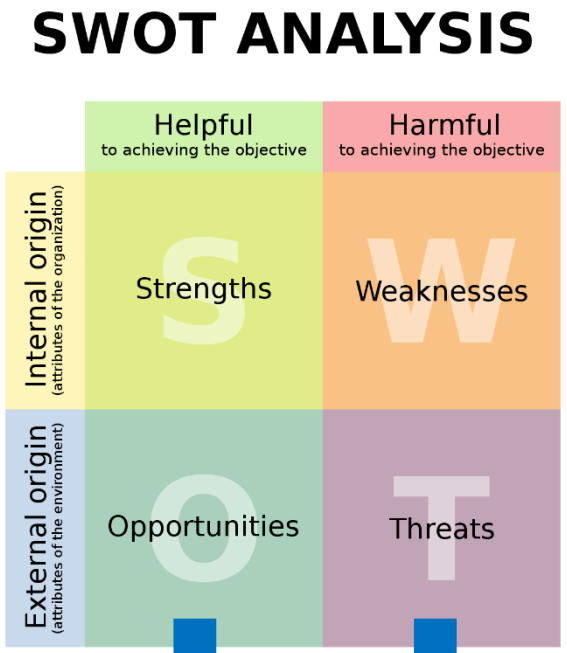


ASL AL
REGIONE PIEMONTE

Identificare le minacce e le opportunità | Swot analysis

Piano strategico

- Obiettivo a
- Obiettivo b
- Obiettivo c
- Obiettivo d
- Obiettivo …

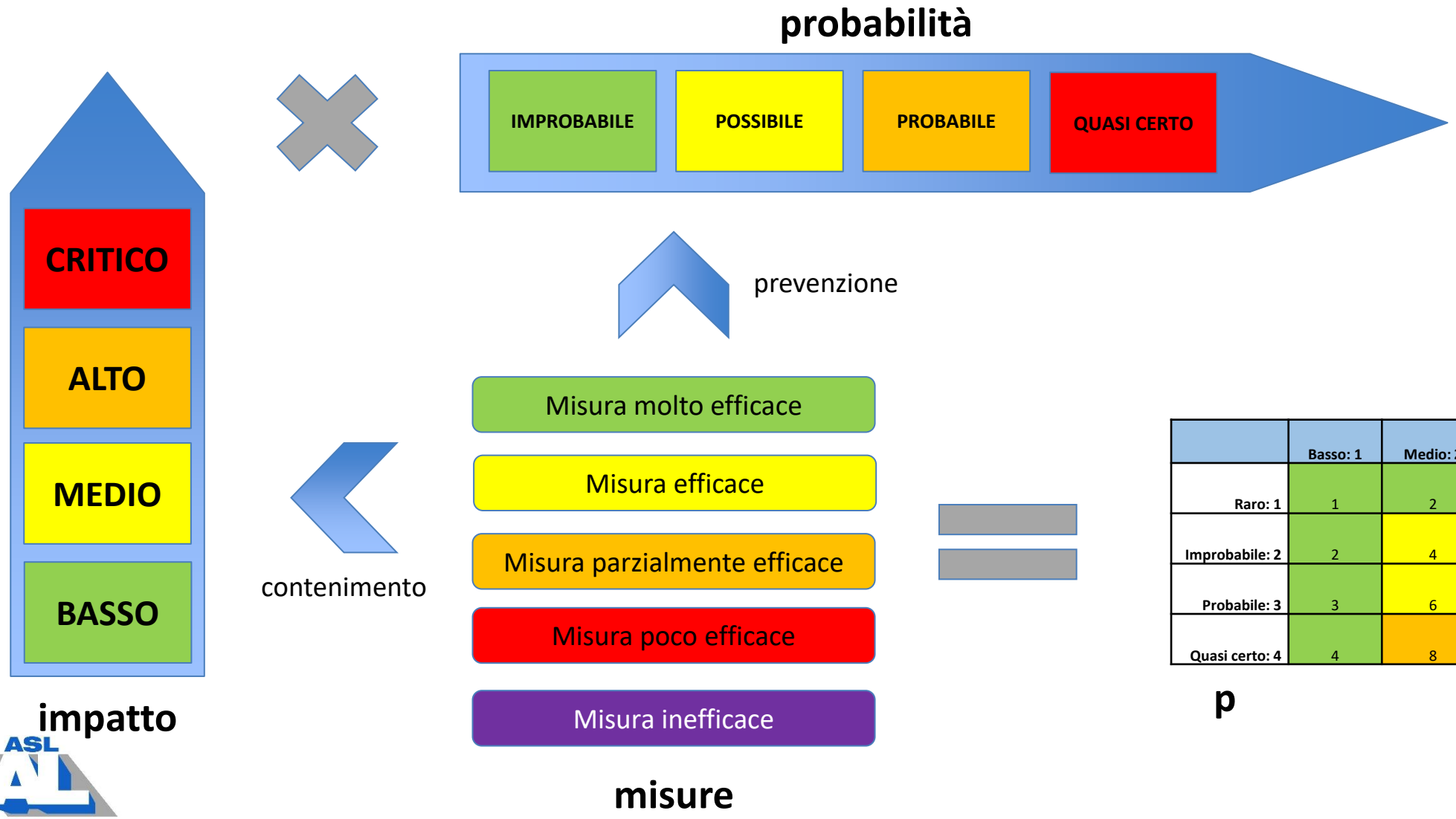


prendo coscienza dei punti forza e debolezza dell'organizzazione

li confronto con le minacce e le opportunità del contesto

agisco di conseguenza per garantire il raggiungimento degli obiettivi di business

Analizzare il rischio | Dal rischio inerente al rischio attuale



	Basso: 1	Medio: 2	Alto: 3	Critico: 4
Raro: 1	1	2	3	4
Improbabile: 2	2	4	6	8
Probabile: 3	3	6	9	12
Quasi certo: 4	4	8	12	16

i

p

Analizzare il rischio | probabilità e impatto

Matrice 4 x 4

Per limitare la soggettività e per facilitare la focalizzazione sugli elementi rilevanti

Probabilità/verosimiglianza	Livello
4	Quasi certo
3	Probabile
2	Possibile
1	Improbabile

Impatto	Livello
4	Critico
3	Alto
2	Medio
1	Basso

Impatto per asset										
Dati			Hardware	Software	Rete e comunicazioni	Fisici	Persone	Finanziari	Processi	Immateriali
R	I	D								

Per il calcolo del rischio si utilizza il valore di impatto relativo all'asset sul quale la minaccia potrebbe produrre il **massimo impatto**

Valutazione impatto | criteri

		Economico	Compliance	Reputazionale	Livello di Servizio	Sicurezza del dato e delle informazioni		
Impatto	Livello					Integrità	Disponibilità	Riservatezza
4	Critico	Impatto economico pari o superiore al 10% del valore della produzione.	Condanna penale nei confronti del management, ovvero sospensione temporanea dell'attività d'impresa.	Danno d'immagine con esposizione mediatica sovraregionale e teporalmente rilevante (> 5 giorni)	La violazione degli SLA contrattualizzati comporta la perdita del cliente.	I dati gestiti sono oggetto di transazioni economiche, finanziarie o sanitarie o segreti aziendali. La mancanza di integrità dei dati ha impatti molto elevati sulle attività operative (superiore a 1 FTE).	L'indisponibilità dei dati oltre agli SLA e ai tempi di RTO e RPO definiti contrattualmente può comportare interruzioni a servizi pubblici essenziali con effetto domino su altri servizi.	I dati sono di tipo particolare ad elevato interesse pubblico o nazionale e l'eventuale diffusione può compromettere in maniera permanente il business e i diritti degli interessati.
3	Alto	Impatto economico superiore al 5% e inferiore al 10% del valore della produzione.	Sanzione amministrativa di natura pecuniaria.	Danno d'immagine con esposizione mediatica regionale e temporalmente rilevante (4-5 giorni)	La violazione degli SLA contrattualizzati comporta la perdita del servizio.	I dati gestiti sono oggetto di transazioni economiche, finanziarie o sanitarie. La mancanza di integrità dei dati ha elevati impatti sulle attività operative (fino a 1 FTE).	L'indisponibilità dei dati oltre agli SLA e ai tempi di RTO e RPO definiti contrattualmente può comportare interruzioni a servizi pubblici essenziali.	I dati sono di tipo particolare e l'eventuale diffusione a terzi può compromettere significativamente il business e i diritti degli interessati.
2	Medio	Impatto economico superiore al 1% e inferiore al 5% del valore della produzione.	Contezioso in sede civile per violazione di termini contrattuali o dovuto ad altre forme di risarcimento del danno.	Danno d'immagine con esposizione mediatica locale (provincia) e temporalmente limitata (2-3 giorni).	La violazione degli SLA contrattualizzati comporta l'applicazione di penali.	I dati gestiti non fanno parte di transazioni economiche, finanziarie o sanitarie. La mancanza di integrità dei dati ha elevati impatti sulle attività operative (tra 0,1 e 0,5 FTE).	L'indisponibilità dei dati oltre agli SLA e ai tempi di RTO e RPO definiti contrattualmente può comportare interruzioni a servizi pubblici non essenziali.	I dati sono di tipo personale e l'eventuale diffusione a terzi può compromettere il business e i diritti degli interessati.
1	Basso	Impatto economico inferiore al 1% del valore della produzione.	Violazione di norma volontaria, policy e procedure interne.	Danno d'immagine moderato o a diffusione interna.	Nessuno SLA definito, ovvero non vi sono penali in caso di violazione degli SLA contrattualizzati.	I dati gestiti non fanno parte di transazioni economiche, finanziarie o sanitarie. La mancanza di integrità dei dati non ha elevati impatti sulle attività operative (< 0,1 FTE).	L'indisponibilità dei dati oltre agli SLA e ai tempi di RTO e RPO definiti contrattualmente può comportare contestazioni da parte dei soggetti interessati.	I dati sono di natura interna e l'eventuale diffusione a terzi non ha significativi impatti sul business e sui diritti degli interessati.

Valutazione probabilità o verosimiglianza | criteri

Probabilità/verosimiglianza	Livello	Criterio connesso alla possibilità	Criterio probabilistico	Serie storiche
4	Quasi certo	E' quasi certo che l'evento possa verificarsi nei prossimi 5 anni e la probabilità è così alta che potrebbe verificarsi già entro il prossimo anno (es. furto nei supermercati; attacco cyber ad aziende con dati ritenuti di valore).	Probabilità > 60% nei prossimi 5 anni	L'evento si è verificato oltre le 5 volte negli ultimi 5 anni o più di 2 volte nell'ultimo anno.
3	Probabile	E' probabile il verificarsi dell'evento nei prossimi 5 anni e l'occorrere di tale evento è prevedibile secondo le fonti di informazione disponibili (es. aumento dei costi dell'energia a fronte di conflitti in determinate aree del mondo)	30% < Prob < 60% nei prossimi 5 anni	L'evento si è verifiato da 4 a 5 volte negli ultimi 5 anni.
2	Possibile	E' possibile il verificarsi dell'evento nei prossimi 5 anni e l'occorrere di tale evento non susciterebbe sorpresa (es. terremoto in aree considerate significativamente sismiche)	10% < Prob < 30% nei prossimi 5 anni	L'evento si è verificato da 2 a 3 volte negli ultimi 5 anni
1	Improbabile	E' improbabile che possa verificarsi, se non in condizioni straordinarie ad oggi imprevedibili (es. alluvione in sito lontano da corsi d'acqua)	0% < Prob <10% nei prossimi 5 anni	L'evento si è verificato non più di 1 volta negli ultimi 5 anni.

Valutazione presidi | criteri

Efficacia delle misure		Range medio di mitigazione	Coefficiente di mitigazione	Criterio
Molto efficace (strutturato)	**4**	3,5 - 4	0,9	La misura si dimostra di assoluta e comprovata efficacia, tale da ridurre in maniera consistente e definitiva la minaccia. Tale risultato può essere desunto in virtù di incident occorsi, nell'adozione di tale misura, all'ente o a realtà terze in virtù di dati storici, oppure in ragione di valutazioni empiriche.
Efficace (Definito)	**3**	2,5 - 3,49	0,75	La misura si dimostra efficace e capace di ridurre in maniera significativa la minaccia, seppur in maniera non del tutto risolutiva. Tale risultato può essere desunto in virtù di incident occorsi, nell'adozione di tale misura, all'ente o a realtà terze in virtù di dati storici, oppure in ragione di valutazioni empiriche.
Parzialmente efficace (Basato su prassi)	**2**	2,0 - 2,49	0,5	La misura dimostra un certo grado di efficacia ma non tale da garantire un presidio puntuale della minaccia, la quale continua a presentare punti di significativa vulnerabilità. Tale risultato può essere desunto in virtù di incident occorsi, nell'adozione di tale misura, all'ente o a realtà terze in virtù di dati storici, oppure in ragione di valutazioni empiriche.
Poco efficace (Iniziale)	**1**	1,0 - 1,99	0,25	La misura si è dimostrata poco efficace a contenere la minaccia, o la sua efficacia non è dimostrata / dimostrabile sulla base dei dati storici e/o per via empirica o dovuta all'applicazione in contesti simili, anche presso realtà terze. La misura è stata adottata ma

Ponderazione QUALITATIVA del rischio

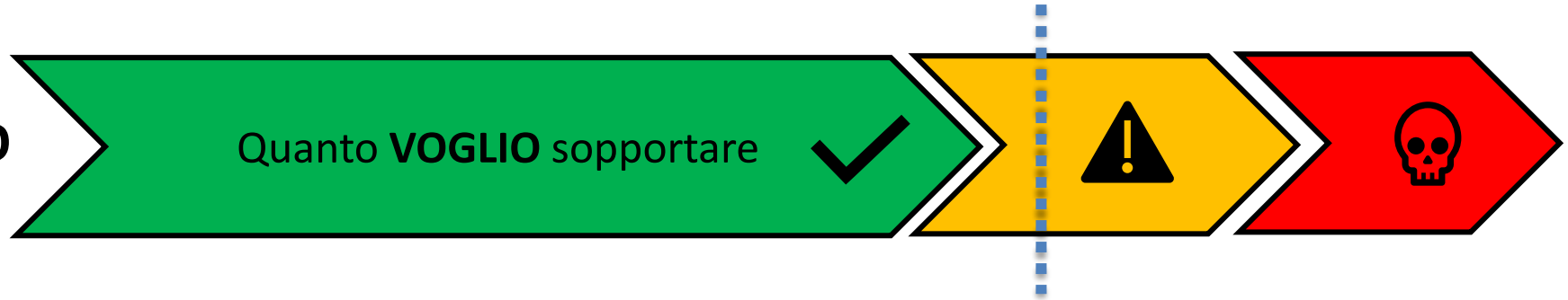
Confrontare il risultato…

	Basso: 1	Medio: 2	Alto: 3	Critico: 4
Raro: 1	1	2	3	4
Improbabile: 2	2	4	**6**	8
Probabile: 3	3	6	9	12
Quasi certo: 4	4	8	12	16

6 = oltre la soglia di accettazione (risk appetite) ma entro la soglia di tolleranza (risk tolerance)

… con le soglie di accettabilità definite

PROFILO DI RISCHIO



Risk Appetite Framework

Definisce le priorità di trattamento del rischio

Probabilità/Impatto	Basso: 1	Medio: 2	Alto: 3	Critico: 4
Raro: 1	Risk Acceptance	Risk Acceptance	Risk Tolerance	Risk Capacity
Improbabile: 2	Risk Acceptance	Risk Tolerance	Risk Tolerance	Risk Capacity
Probabile: 3	Risk Acceptance	Risk Tolerance	Risk Capacity	Out of risk
Quasi certo: 4	Risk Acceptance	Risk Capacity	Out of risk	Very critical

Priorità	livello di rischio	Azioni di controllo
1	Very critical	da implementare entro 1 mese
2	Out of risk	da implementare entro 6 mese
3	Risk Capacity	da implementare entro 1 anno
4	Risk Tolerance	da implementare entro 3 anni
5	Risk Acceptance	non richieste

ASL AL
REGIONE PIEMONTE

Ponderazione QUANTITATIVA del rischio

Costo Totale del rischio (€)

Costi diretti delle perdite

+

Costi indiretti delle perdite

+

Costi per la protezione

+

Costi per la prevenzione

+

Costi per il trasferimento

ATTENZIONE

Il trasferimento non deve essere la prima opzione di trattamento del rischio. Le assicurazioni non coprono tutti i costi… e costano.

Trasferisco solo ciò che non posso / voglio / mi conviene mitigare.

Mitigare il rischio = Riduzione del premio assicurativo!

… confronto con le soglie di accettabilità definite (€)

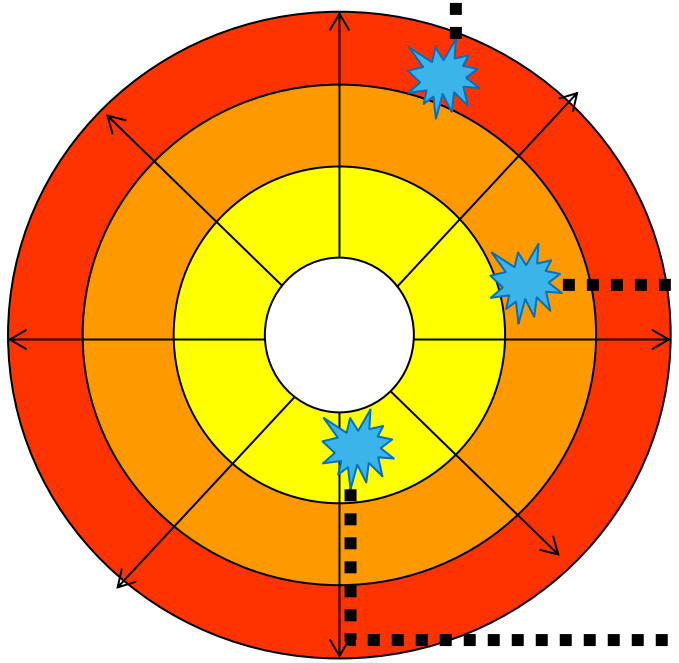
ASL AL

REGIONE PIEMONTE

Decidere le misure di trattamento

- [**ACCEPT**] Ritenuto, ovvero il suo impatto considerato sopportabile (risk capacity)
- [**MITIGATE**] Mitigato, attraverso un'azione di trattamento che vada a ridurre la probabilità, agendo in prevenzione del danno o l'impatto, agendo in contenimento del danno
- [**TRANSFER**] Trasferito a terzi, ad esempio ad un fornitore o ad una compagnia assicurativa
- [**AVOID**] Evitato, eliminando la causa, ad esempio rinunciando all'obiettivo connesso

Decidere le misure di trattamento



RISCHI ESTERNI (nessuna possibilità di influenzarli, dipendenza pura)

- [**AVOID**] Non possibile (… o eliminare l'obiettivo)
- [**MITIGATE**] Solo business continuity, stress test, scenario analysis, monitoraggio
- [**TRANSFER**] Non possibile
- [**ACCEPT**] Accettare il rischio (se < risk capacity)

RISCHI PARZIALMENTE INDIRIZZABILI (posso influenzarli indirettamente)

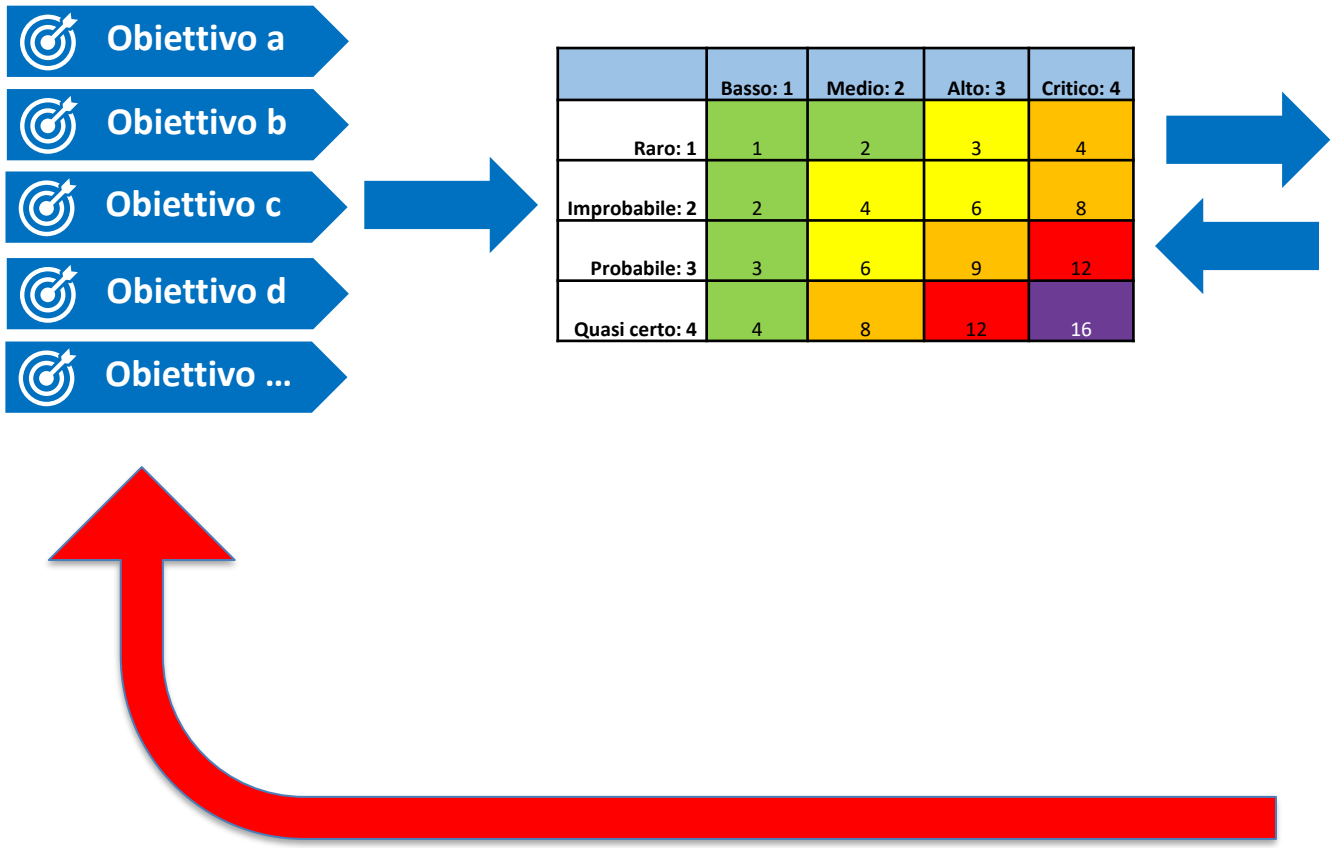
- [**AVOID**] Evitare il rischio (es. internalizzare, abbandonare il processo, cambiare fornitore)
- [**MITIGATE**] Diminuire gli impatti del rischio (es. business continuity, partnership, monitoraggio)
- [**TRANSFER**] Trasferire il rischio (es. assicurazione, outsourcing, condivisione)
- [**ACCEPT**] Accettare il rischio (perché tollerabile)

RISCHI INTERNI (posso gestirli direttamente)

- [**AVOID**] Evitare il rischio (es. internalizzare, cambiare fornitore)
- [**MITIGATE**] Diminuire gli impatti del rischio (es. ridurre probabilità, impatto, monitoraggio)
- [**TRANSFER**] Trasferire il rischio (es. assicurazione, outsourcing, condivisione)
- [**ACCEPT**] Accettare il rischio (perché tollerabile)

ASL AL
REGIONE PIEMONTE

Monitorare i rischi con i Key Risk Indicatori (KRI)



Es. Key Risk Indicator

- **Rischio reputazionale:** numero di reclami dei cittadini, copertura mediatica negativa.
- **Rischio finanziario:** deviazione dal budget, debito pubblico.
- **Esempi più specifici per uno sportello pubblico.**
- **Rischio di interruzione del servizio:** tempo medio di risoluzione delle richieste, percentuale di richieste non evase entro i tempi stabiliti.
- **Rischio di perdita di dati:** numero di incidenti informatici, percentuale di dati non protetti.
- **Rischio di non conformità:** numero di non conformità riscontrate nelle verifiche interne o esterne.

Monitoraggio, miglioramento e revisione

Essenziali per:

- valutare la corretta applicazione delle misure e dei controlli
- rilevare gli scostamenti rispetto ai piani previsti
- supportare le decisioni
- garantire efficacia e miglioramento continuo
- recepire le variazioni del contesto e delle minacce
- mantenere la coerenza dei controlli nel tempo, al mutare del contesto

Fonti di informazione:

- Analisi degli incident e degli eventi
- Key performance indicator
- Key risk indicator
- Audit e Riesami

Template – Risk Assessment

Tipologia	Codice Rischio	Minaccia/Pericolo	Punti di debolezza	Conseguenza	Risk owner
Operativo		Assenza di connettività			
Operativo		Indisponibilità dei dati			

Impatto per asset											Probabilità accadimento (verosimiglianza) inerente (da 1 MIN a 4 MAX)	Impatto inerente (da 1 MIN a 4 MAX)	Rischio inerente (impatto*probabilità)	Risk Rating (*rif. foglio Algoritmi e scale)
Dati			Hardware	Software	Rete e comunicazioni	Fisici	Persone	Finanziari	Processi	Immateriali				
R	I	D												
		3									2	3	**6**	**RISK TOLERANCE**
			4								3	4	**12**	**OUT OF RISK**

Presidi/Controlli preventivi in essere (P)	Presidi/Controlli contenitivi in essere (I)	Efficacia media dei controlli preventivi (da 1 a 4)	Efficacia media dei controlli contenitivi (da 1 a 4)	Coefficiente di mitigazione P	Coefficiente di mitigazione I	Probabilità residua (da 1 a 4)	Impatto residuo (da 1 a 4)	Rischio attuale	Risk Rating (*rif. foglio Algoritmi e scale)	Strategia di trattamento del rischio
Monitoraggio linea di emergenza	Contratto con il fornitore Monitoraggio	3	3	0,5	0,5	1	1,5	**1,5**	**RISK ACCEPTANCE**	**Accettazione**
Sistemi di sicurezza perimetrale Sistemi di sicurezza presenti nel cloud (es. antiramsonware) Linee guida software sicuro	Monitoraggio NOC Procedure di BC e DR Backup	2	3	0,75	0,5	2,25	2	**4,5**	**RISK TOLERANCE**	**Mitigazione**

ASL AL

REGIONE PIEMONTE

DIGITALCAMPUS
guidiamo l'innovazione

CSI
your digital partner

Grazie

marcello.cutrone@csi.it

ASL AL
REGIONE PIEMONTE