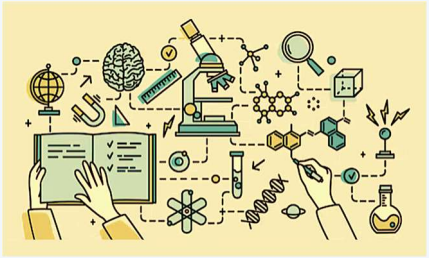
CONFERENZA NAZIONALE

SICUREZZA E INTEGRITÀ DELLA RICERCA

Griglia di valutazione: istruzioni per l'uso

Paolo Valente, INFN-Roma & Segretario CoPER



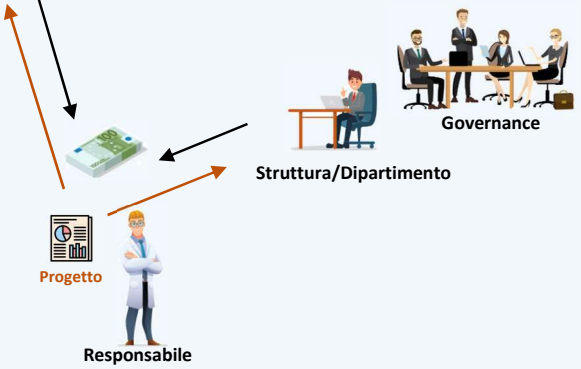
Un tipico progetto di ricerca

La proposta da parte del responsabile dell'**attività di ricerca** generalmente passa attraverso una **valutazione del progetto** da parte dell'istituzione, eventualmente al livello di dipartimento o struttura

Si richiedono risorse materiali, umane e finanziarie

Ministeri, Agenzie, Istituzioni di ricerca nazionali e internazionali, Fondazioni, Aziende, …

Possono essere richiesti **finanziamenti** anche all'**esterno** dell'istituzione, a livello nazionale o internazionale, di tipo pubblico o privato, di tipo competitivo o meno, ecc.



Ci sono **collaboratori**, all'interno o all'esterno dell'istituzione, si formano studenti e spesso viene reclutato nuovo personale

Collaboratori esterni, Studenti

1

Per **individuare** possibili rischi per la sicurezza della ricerca si parte da alcune **domande di base**:

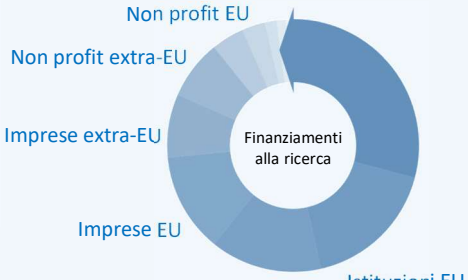
- Sono previste **collaborazioni esterne** ?
- Sono previsti **finanziamenti esterni** ?

Che cosa si intende con ESTERNI?

- **Istituzioni di ricerca non EU** non regolate da **trattati** [escluse agenzie ONU, CERN, ecc.]
- **Soggetti privati** come banche, industrie, imprese, che non sono **prevalentemente** impegnati in ricerca [escluse fondazioni e consorzi di ricerca]

Definizione che può essere **dinamica**, a seconda della situazione geopolitica e delle direttive governative

Schema proposto



1

Per **individuare** possibili rischi per la sicurezza della ricerca si parte da alcune **domande di base**:

- Sono previste **collaborazioni esterne** ?
- Sono previsti **finanziamenti esterni** ?

Se **non ci sono** collaborazioni **né** finanziamenti **ESTERNI** si procede, ricordando le **precauzioni di base** e la normativa di riferimento

OK

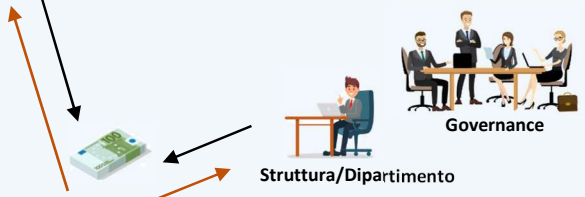
Se ci sono collaboratori **oppure** fondi **ESTERNI** si passa a un'analisi dei rischi specifici tramite una **griglia di valutazione**

2

sicurezzaricerca.mur.gov.it

MUR

Ministeri, Agenzie, Istituzioni di ricerca nazionali e internazionali, Fondazioni, Aziende, …



Collaboratori esterni, Studenti

Schema proposto

2

Il Responsabile di attività compila una specifica **griglia di valutazione** [online] con il supporto, ove necessario, di un **Referente** per la sicurezza e integrità della ricerca

Il **Referente** SIR **dialoga** con il Responsabile di attività e con la Governance dell'Istituzione e – partendo dai **risultati della griglia di valutazione** e di un'ulteriore analisi del progetto – fornisce **ulteriori linee di mitigazione**

OK

Per **livelli più alti** di rischio o in casi particolari può **richiedere** il supporto del **livello nazionale**

sicurezzaricerca.mur.gov.it

MUR

Referente per la Sicurezza e Integrità della Ricerca

A livello di singola Istituzione [o più Istituzioni consorziate], **esamina i progetti** con indicatori di rischio **sopra soglia** e:

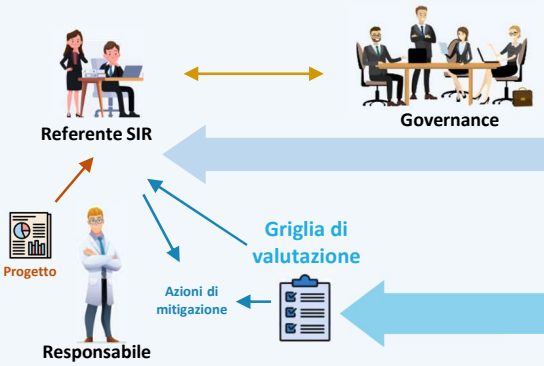
- Fornisce **azioni di mitigazione al responsabile di attività**;
- Fornisce **raccomandazioni alla governance** dell'Istituzione, anche su protocolli per **visite** di ospiti o **viaggi** in paesi con profilo di **rischio alto**
- Si occupa della **formazione** a livello di Istituzione
- Contribuisce all'implementazione delle politiche di **cybersicurezza**
- Contribuisce al rispetto delle politiche su **dual use** ed **exports control**

Responsabile di attività

- Presenta il **progetto di attività** di ricerca all'istituzione ed eventualmente altre agenzie di finanziamento
- Produce una **autovalutazione dei rischi** con l'aiuto di una **griglia** a livello ministeriale

LIVELLO ISTITUZIONE

LIVELLO ATTIVITÀ



Schema proposto

Servizio Nazionale per la Sicurezza e Integrità della Ricerca

- Agisce da **raccordo con ministeri e agenzie rilevanti**
- Predispone e aggiorna: **raccomandazioni** e **linee guida, matrici di rischio**
- Suggerisce azioni di **mitigazione dei rischi**
- Riceve richieste e **fornisce supporto ai referenti SIR**, anche tramite altre istituzioni
- Fornisce **materiale formativo**
- Agisce da **coordinamento nazionale** dei referenti SIR
- Dialoga con il **Centro Europeo SIR**

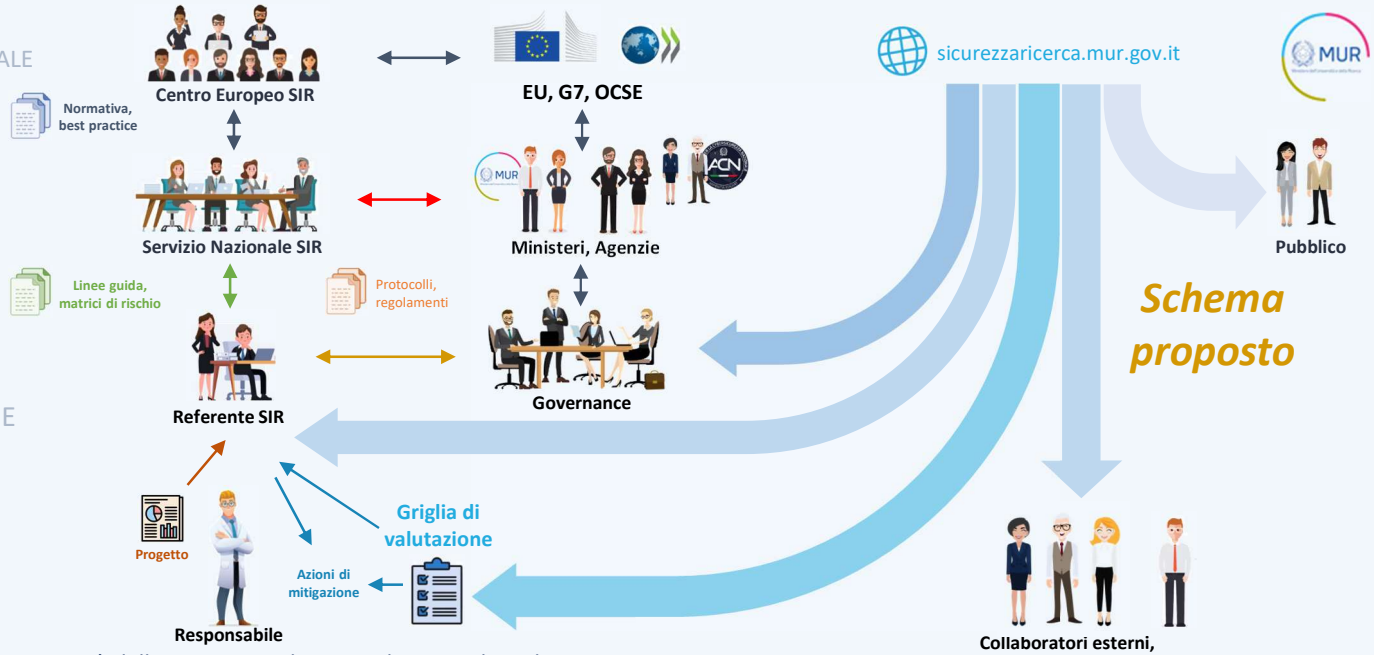
Referente per la Sicurezza e Integrità della Ricerca

A livello di singola Istituzione [o più Istituzioni consorziate], **esamina i progetti** con indicatori di rischio **sopra soglia** e:

- Fornisce **azioni di mitigazione al responsabile di attività**;
- Fornisce **raccomandazioni alla governance** dell'Istituzione, anche su protocolli per **visite** di ospiti o **viaggi** in paesi con profilo di **rischio alto**
- Si occupa della **formazione** a livello di Istituzione
- Contribuisce all'implementazione delle politiche di **cybersicurezza**
- Contribuisce al rispetto delle politiche su **dual use** ed **exports control**
- Riceve **linee guida e matrici di rischio** dal **Servizio Nazionale**
- Può richiedere **supporto** al **Servizio Nazionale**

Responsabile di attività

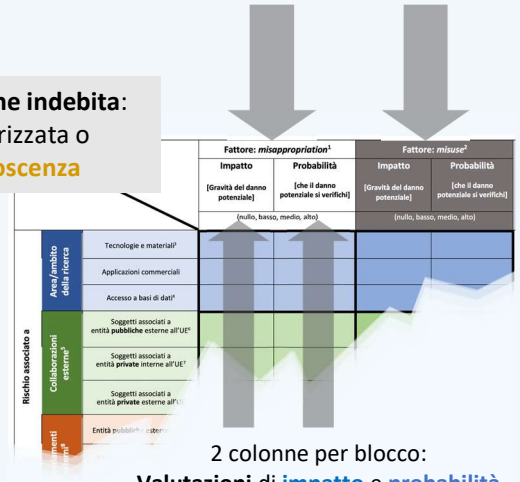
- Presenta il **progetto di attività** di ricerca all'istituzione ed eventualmente altre agenzie di finanziamento
- Produce una **autovalutazione dei rischi** con l'aiuto di una **griglia** a livello ministeriale



Griglia di valutazione: struttura

2 blocchi verticali:
tipologie di azione malevola

Appropriazione indebita:
cioè non autorizzata o illecita di **conoscenza**



2 colonne per blocco:
Valutazioni di **impatto** e **probabilità**

- Quale sarebbe l'entità del **danno** se l'azione malevola si verificasse?

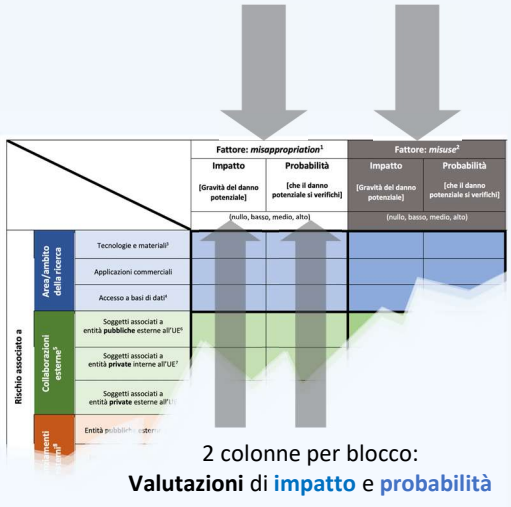
- Con quale **probabilità** l'azione malevola e il danno conseguente si possono verificare?

Uso distorto della **conoscenza** ovvero:
- Diverso da quello originariamente dichiarato
- Illecito o non autorizzato
- Tale da arrecare **danno** a cose o persone, di tipo materiale o immateriale (per es. lesione di diritti, discriminazione…)

Conoscenza:
quanto **disponibile** o **prodotto** nell'ambito dell'attività di ricerca in senso generale, ovvero:
- Dati
- Risultati e documenti
- Metodologie
- Tecnologie

Griglia di valutazione: struttura

2 blocchi verticali:
tipologie di azione malevola



2 colonne per blocco:
Valutazioni di **impatto** e **probabilità**

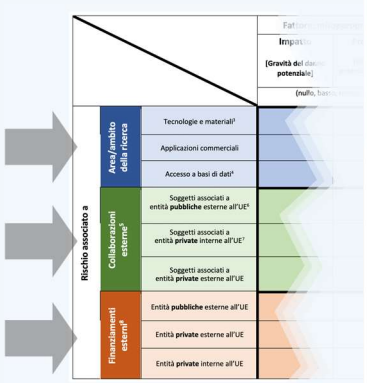
L'area disciplinare e in senso più lato la tematica e la tipologia dell'attività di ricerca (fondamentale, applicata, conto terzi, ecc.); il coinvolgimento o la disponibilità di asset (materiali e immateriali)

La collaborazione con partner non appartenenti a istituzioni EU

Fonti di finanziamento non provenienti da istituzioni EU

Area scientifica o tecnologie critiche o sensibili*

blocchi orizzontali:
3 **aree di rischio**

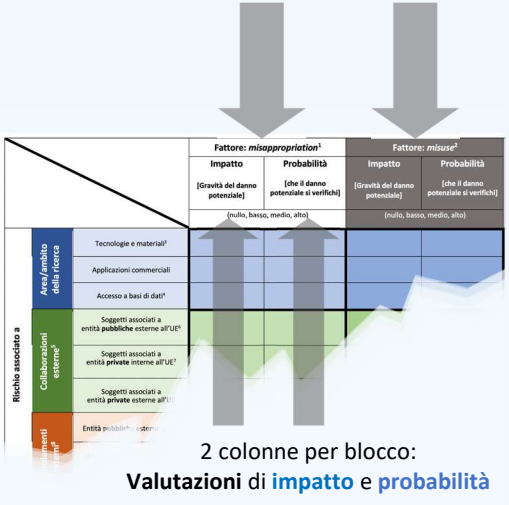


** "ANNEX to the Commission Recommendation on critical technology areas for the EU's economic security for further risk assessment with Member States", 3 ottobre 2023:*

Area Tecnologica	Tecnologie
SEMICONDUTTORI	• Microelettronica, compresi i processori • Tecnologie fotoniche (inclusi i laser ad alta energia) • Chip ad alta frequenza • Attrezzature per la produzione di semiconduttori avanzati
INTELLIGENZA ARTIFICIALE	• Calcolo ad alte prestazioni • Cloud computing e edge computing • Tecnologie di analisi dei dati • Visione artificiale, elaborazione del linguaggio, riconoscimento degli oggetti
QUANTISTICA	• Calcolo quantistico • Crittografia quantistica • Comunicazioni quantistiche • Sensori e radar quantistici
BIOTECNOLOGIE	• Tecniche di modifica genetica • Nuove tecniche genomiche • Gene-drive (propulsione genetica) • Biologia sintetica
CONNETTIVITÀ, NAVIGAZIONE E DIGITALI	• Comunicazioni digitali e connettività sicure, come RAN e Open RAN (Radio Access Network) e 6G • Tecnologie di sicurezza informatica, incluse la cyber-sorveglianza, sistemi di sicurezza e intrusioni, informatica forense digitale • Internet delle cose e Realtà Virtuale • Tecnologie di registro distribuito e identità digitale • Tecnologie di guida, navigazione e controllo, incluse l'avionica e il posizionamento marino
SENSORI	• Sensori elettro-ottici, radar, chimici, biologici, di radiazioni e di rilevamento distribuito • Magnetometri, gradiometri magnetici • Sensori di campo elettrico subacquei • Misuratori e gradiometri di gravità
TECNOLOGIE SPAZIALI E DI PROPULSIONE	• Tecnologie specifiche per lo spazio, che vanno dal livello di componente a quello di sistema • Tecnologie per la sorveglianza spaziale e l'osservazione della Terra • Posizionamento spaziale, navigazione e temporizzazione (PNT) • Comunicazioni sicure, compresa la connettività in orbita terrestre bassa (LEO) • Tecnologie di propulsione, incluse l'ipersonica e componenti per uso militare
ENERGIE	• Tecnologie di fusione nucleare, reattori e generazione di energia, tecnologie di conversione/arricchimento/riciclaggio radiologico • Idrogeno e nuovi combustibili • Tecnologie a emissioni zero, incluse le fotovoltaiche • Reti intelligenti e stoccaggio dell'energia, batterie
ROBOTICA E SISTEMI AUTONOMI	• Droni e veicoli (aerei, terrestri, di superficie e subacquei) • Robot e sistemi di precisione controllati da robot • Esoscheletri • Sistemi abilitati dall'intelligenza artificiale
MATERIALI, MANIFATTURA E RICICLAGGIO	• Tecnologie per nanomateriali, materiali intelligenti, materiali ceramici avanzati, materiali stealth, materiali progettati per essere sicuri e sostenibili • Manifattura additiva • Manifattura digitale di micro-precisione, e lavorazione/saldatura laser su piccola scala • Tecnologie per l'estrazione, la lavorazione e il riciclaggio di materiali grezzi critici (inclusa l'estrazione idrometallurgica, la bio-lisciviazione, la filtrazione basata sulla nanotecnologia, la lavorazione elettrochimica e la massa nera)

Griglia di valutazione: struttura

2 blocchi verticali:
tipologie di azione malevola



2 colonne per blocco:
Valutazioni di **impatto** e **probabilità**

L'area disciplinare e in senso più lato la tematica e la tipologia dell'attività di ricerca (fondamentale, applicata, conto terzi, ecc.); il coinvolgimento o la disponibilità di asset (materiali e immateriali)

La collaborazione con partner non appartenenti a istituzioni EU

Fonti di finanziamento non provenienti da istituzioni EU

Area scientifica o tecnologie critiche o sensibili*

Potenziale sfruttamento commerciale non previsto

Potenziale accesso e uso non previsto/illecito di dati

blocchi orizzontali:
3 **aree di rischio**

3 righe ovvero
categorie di rischio
per ciascuna area

Istituzioni di ricerca extra-EU

Imprese

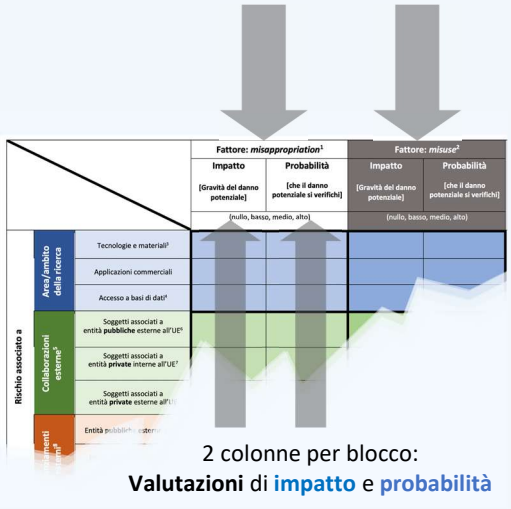
Nella EU

Extra-EU

** "ANNEX to the Commission Recommendation on critical technology areas for the EU's economic security for further risk assessment with Member States", 3 ottobre 2023:*

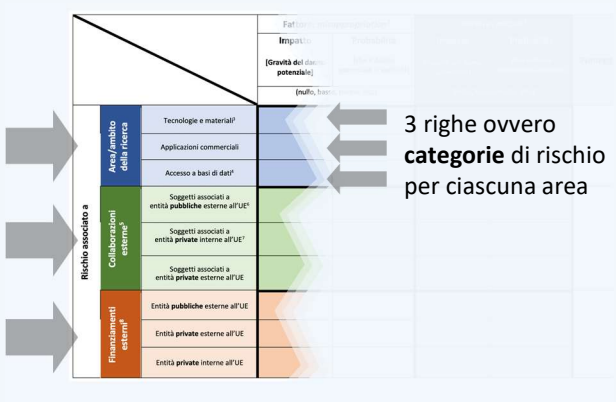
Griglia di valutazione: struttura

2 blocchi verticali:
tipologie di azione malevola



2 colonne per blocco:
Valutazioni di **impatto** e **probabilità**

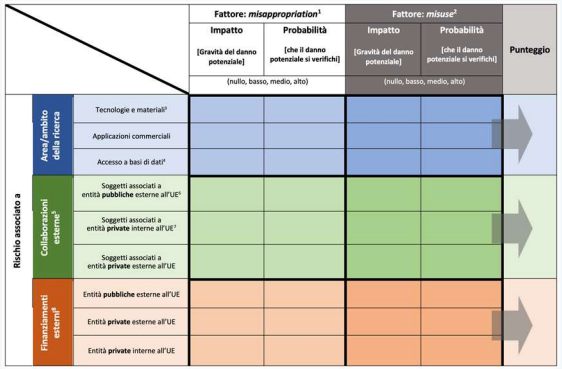
blocchi orizzontali:
3 **aree di rischio**



3 righe ovvero
categorie di rischio
per ciascuna area

Per **ogni campo** una **valutazione**

Le singole valutazioni (2× 2 ×3) si **combinano** a dare **3 score**, uno **ciascuna delle aree**



Griglia di valutazione: livelli

A questa fase di autovalutazione arrivano attività che hanno o collaborazioni o finanziamenti esterni, e quindi possibilmente si possono verificare delle conseguenze non volute; si può graduare il **danno potenziale** semplicemente con dei livelli qualitativi: per esempio nullo, basso, medio o alto

Allo stesso modo per la **probabilità** che si verifichi una circostanza non voluta, e quindi un danno, si possono utilizzare gli stessi livelli

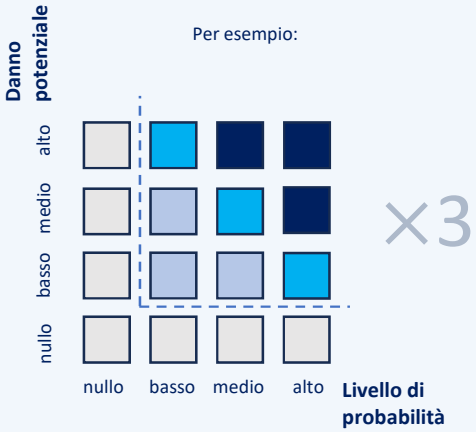
Per esempio:

			Fattore: *misappropriation*[1]		Fattore: *misuse*[2]		Punteggio
			Impatto [Gravità del danno potenziale]	Probabilità [che il danno potenziale si verifichi]	Impatto [Gravità del danno potenziale]	Probabilità [che il danno potenziale si verifichi]	
			(nullo, basso, medio, alto)		(nullo, basso, medio, alto)		
Rischio associato a	Area/ambito della ricerca	Tecnologie e materiali[3]	basso	**medio**	basso	basso	**medio**
		Applicazioni commerciali	**medio**	**medio**	basso	**medio**	
		Accesso a basi di dati[4]	*nullo*	basso	*nullo*	basso	
	Collaborazioni esterne[5]	Soggetti associati a entità **pubbliche** esterne all'UE[6]	**medio**	basso	basso	basso	**medio**
		Soggetti associati a entità **private** interne all'UE[7]	**medio**	basso	basso	basso	
		Soggetti associati a entità **private** esterne all'UE	**medio**	basso	basso	basso	
	Finanziamenti esterni[8]	Entità **pubbliche** esterne all'UE	basso	*nullo*	basso	*nullo*	**basso**
		Entità **private** esterne all'UE	basso	*nullo*	basso	*nullo*	
		Entità **private** interne all'UE	basso	basso	basso	basso	

Griglia di valutazione: risultati

Per **ciascuna** delle tre aree della griglia si può ottenere uno **score** per il **rischio** combinando il **danno potenziale** con la **probabilità** che si verifichi

Per esempio:



Una **valutazione complessiva** del **rischio** può essere ottenuta **combinando gli score** per le tre aree: **tematica**, **collaborazioni** e **finanziamenti esterni**

Per esempio:

Nota bene: il dettaglio degli score e di come si combinano può essere meglio definito e adattato per es. sulla base di un periodo di test

Ringraziamenti

È stato un **piacere** e un **privilegio** far parte
di una squadra straordinaria

Grazie!