



RISK ASSESSMENT PROJECT

Presented by: Lisa Bonato

TRACCIA

Simulare un processo di Risk Assessment, solo Step 1 e Step 2 (tralasciando Step 3 e Step 4), seguendo NIST SP 800-30, per Tier 3 (considerate solo le sorgenti del Tier 3).

Riutilizzate la mappa delle relazioni tra tabelle, che avete prodotto ieri, come guida.

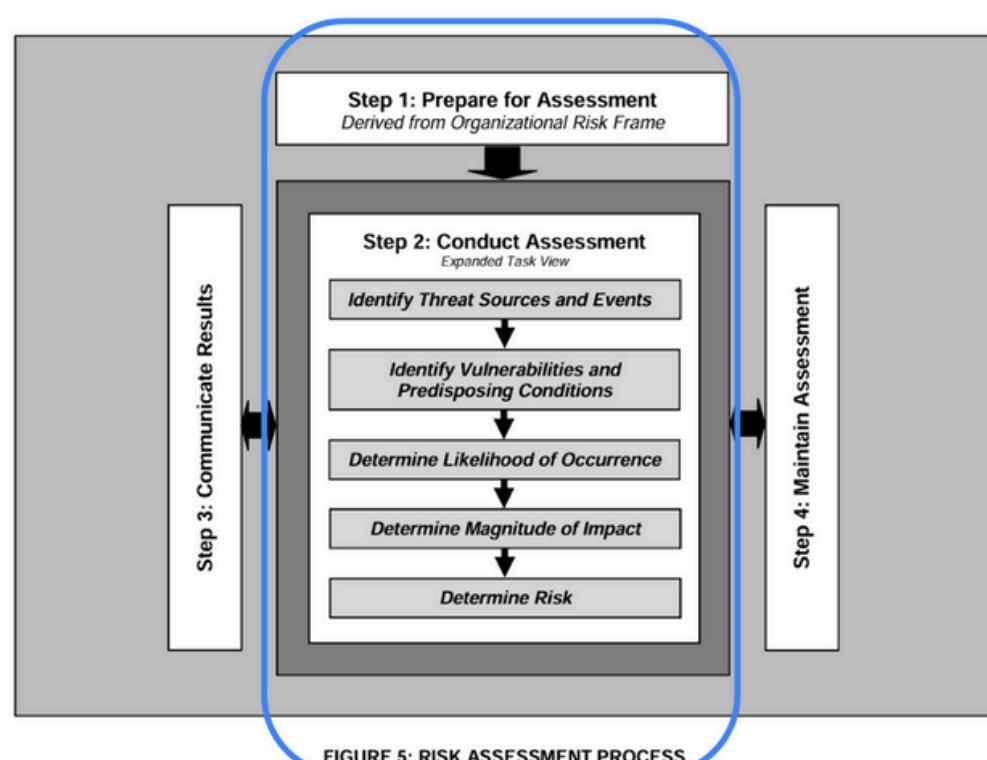


TABLE D-1: INPUTS – THREAT SOURCE IDENTIFICATION

Description	Provided To		
	Tier 1	Tier 2	Tier 3
From Tier 1: (Organization level) - Sources of threat information deemed to be credible (e.g., open source and/or classified threat reports, previous risk/threat assessments). (Section 3.1, Task 1-4) - Threat source information and guidance specific to Tier 1 (e.g., threats related to organizational governance, core missions/business functions, management/operational policies, procedures, and structures, external mission/business relationships). - Taxonomy of threat sources, annotated by the organization, if necessary. (Table D-2) - Characterization of adversarial and non-adversarial threat sources. - Assessment scales for assessing adversary capability, intent, and targeting, annotated by the organization, if necessary. (Table D-3, Table D-4, Table D-5) - Assessment scale for assessing the range of effects, annotated by the organization, if necessary. (Table D-6) - Threat sources identified in previous risk assessments, if appropriate.	No	Yes	Yes if not provided by Tier 2
From Tier 2: (Mission/business process level) - Threat source information and guidance specific to Tier 2 (e.g., threats related to mission/business processes, EA segments, common infrastructure, support services, common controls, and external dependencies). - Mission/business process-specific characterization of adversarial and non-adversarial threat sources.	Yes via RAR	Yes via peer sharing	Yes
From Tier 3: (Information system level) - Threat source information and guidance specific to Tier 3 (e.g., threats related to information systems, information technologies, information system components, applications, networks, environments of operation). - Information system-specific characterization of adversarial and non-adversarial threat sources.	Yes via RAR	Yes via RAR	Yes via peer sharing

TRACCIA

Scenario:

L'azienda Alpha è un fornitore leader di servizi sanitari online che gestisce un'ampia infrastruttura IT che include sistemi basati su cloud, applicazioni web e dispositivi mobili. L'azienda gestisce anche dati sanitari sensibili per i propri pazienti.

- L'organizzazione si è resa conto di essere target di un gruppo criminale organizzato con un buon livello di preparazione e delle significative risorse per condurre attacchi coordinati. Dai sistemi di monitoraggio, è emerso che solo questa azienda è continuamente sorvegliata dal gruppo criminale. Da ulteriori analisi, si arriva alla conclusione che il gruppo criminale vuole esfiltrare delle informazioni all'azienda sui dati sanitari degli utenti per rivenderli, creando una persistenza all'interno dell'organizzazione e non facendosi rilevare.
- In questo momento la sorgente delle minaccia è alla fase di ricognizione esterna con diversi metodi (scanning, sniffing, OSINT, sorveglianza), non si rilevano ricognizioni interne.
- L'organizzazione non ha abilitato MFA e non effettua regolarmente Vulnerability Assessment
- L'organizzazione tratta informazioni personali e il loro software deve consentire la condivisione delle informazioni tra gli utenti, ciò si applica alla maggior parte dei loro sistemi.
- Tutte le attività di ricognizioni sono attive, però lo scanning e sniffing portano a degli impatti bassi perché presente un firewall e WAF su cloud, invece gli effetti potrebbero essere moderati nella ricerca open source o nella sorveglianza di alcuni target particolari.
- Consideriamo solamente il danneggiamento degli asset dovuto a perdita o danneggiamento degli asset informativi, con un impatto alto.

TRACCIA

Siete liberi di impostare scopo, ambito, ipotesi e vincoli per limitare l'estensione del RA.

Utilizzate gli step visti a lezione e definite solamente le tabelle essenziali che vi serviranno per il calcolo finale del rischio:

- D-7
- E-5
- F-3
- F-6
- H-4
- I-5

Ipotizzate che l'organizzazione può accettare solamente un rischio basso per tutti gli eventi di rischio identificati, dovuto al valore del loro asset principale «dati sanitari». Fate delle valutazioni e delle ipotesi sui prossimi passaggi da eseguire per riportare il livello di rischio ottenuto entro quello desiderato.



Step 1: Prepare for Assessment Derived from Organizational Risk Frame

SCOPO

Procedere alla modellizzazione di un Risk Assessment relativo al solo asset dei dati personali gestiti dall'organizzazione. Inoltre, l'assessment si limiterà alle macro fasi Prepare for assessment e Conduct Assessment del NIST 800-30 per il solo Tier3.

IPOTESI

- Il gruppo criminale ha accesso a risorse significative e un buon livello di preparazione per condurre attacchi coordinati
- La mancanza di abilitazione del Multi-Factor Authentication (MFA) e la mancata esecuzione regolare di Vulnerability Assessment potrebbero lasciare l'azienda vulnerabile
- L'azienda Alpha tratta informazioni personali e richiede la condivisione di informazioni tra gli utenti, aumentando il rischio di esfiltrazione di dati sensibili (Target del gruppo criminale)

AMBITO

Il RA sarà limitato ai dati che sono archiviati e gestiti su cloud. Questi dati sono condivisi fra gli utenti: sia gli operatori/dipendenti che i pazienti.

VINCOLI

- L'azienda deve garantire la condivisione delle informazioni tra gli utenti senza compromettere la sicurezza dei dati personali sottoposti al GDPR
- Le attività di monitoraggio come lo scanning e lo sniffing sono ostacolate dalla presenza di un firewall e WAF su cloud, tuttavia, la ricerca open source e la sorveglianza di target specifici possono ancora rappresentare un rischio moderato
- Il livello di rischio residuo accettabile dall'organizzazione è “LOW”



Step 1: Prepare for Assessment

Derived from Organizational Risk Frame

Identificare sorgenti di informazioni per Threat, vulnerabilità e impatti da utilizzare nella valutazione del rischio (tabelle D-1, E-1, F-1, H-1, I-1)



Lo scenario di riferimento viene utilizzato come sorgente di informazione.

Definire o perfezionare il modello di rischio, l'approccio di assessment e l'approccio di analisi da utilizzare nella valutazione del rischio.



Il processo seguito è quello definito in NIST RMF e NIST 800-30.

STEP 2: CONDUCT ASSESSMENT

IDENTIFY THREAT SOURCES



Tabella D-1

- Identificare gli input delle fonti di minaccia
- Determinare se le fonti di minaccia sono rilevanti per l'organizzazione e di portata adeguata



Tabella D-2

- Identificare le fonti di minaccia
D-2.1 = La fonte della minaccia è di tipo avversaria e proviene dall'esterno dell'organizzazione.
Si tratta di un gruppo organizzato che cerca di sfruttare la dipendenza dell'organizzazione dalle risorse informatiche. Come possiamo vedere le caratteristiche sono Capacità, Intento e Targeting (inteso come obiettivo)



Tabella D-7

- Valutare la capacità dell'avversario (Tabella D-3).
- Valutare l'intento dell'avversario (Tabella D-4).
- Valutare l'obiettivo dell'avversario (Tabella D-5).



Tabella D-8

- Valutare la gamma di effetti delle fonti di minaccia (Tabella D-6).



TABLE D-7: TEMPLATE – IDENTIFICATION OF ADVERSARIAL THREAT SOURCES

Identifier	Threat Source Source of Information	In Scope	Capability	Intent	Targeting
D-7-1	ADVERSARIAL - Group-Established	Yes	High	Moderate	High



IDENTIFY THREAT EVENTS

TABLE E-2: ADVERSARIAL THREAT EVENTS

- **E-5-1** = ricognizione/scansione della rete perimetrale
- **E-5-2** = network sniffing delle reti esposte
- **E-5-3** = raccolta informazioni organizzative utilizzando fonti open source
- **E-5-4** = ricognizione e sorveglianza dell'organizzazione in modo mirato

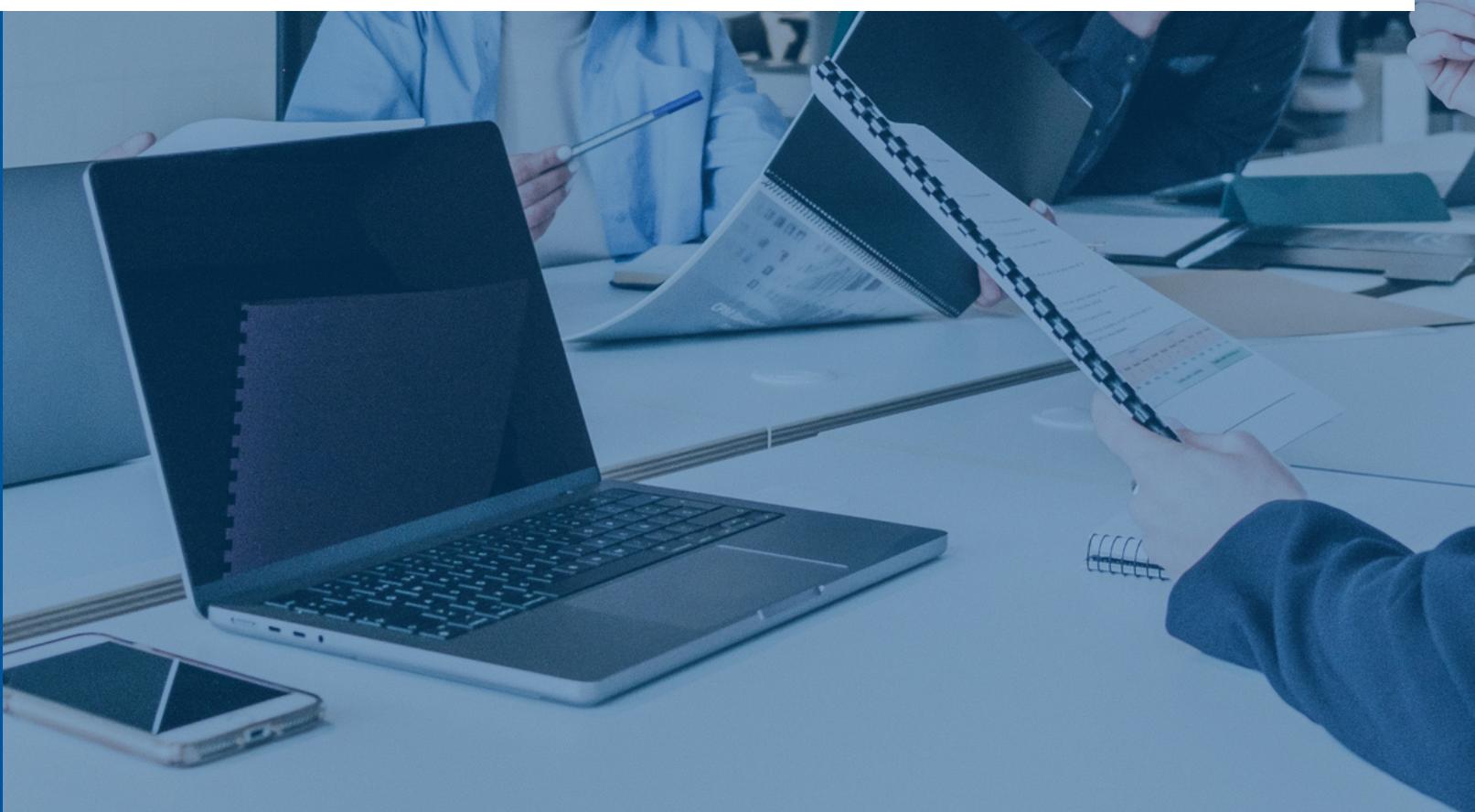
TABLE E-4: RELEVANCE OF THREAT EVENTS

CONFIRMED

Tutti e quattro gli eventi di minaccia sono stati individuati dall'organizzazione

TABLE E-5: TEMPLATE – IDENTIFICATION OF THREAT EVENTS

Identifier	Threat Event Source of Information	Threat Source	Relevance
E-5-1	Perform perimeter network reconnaissance/scanning.	D-7-1	Confirmed
E-5-2	Perform network sniffing of exposed networks.	D-7-1	Confirmed
E-5-3	Gather informations using open source discovery of organizational information.	D-7-1	Confirmed
E-5-4	Perform reconnaissance and surveillance of targeted organizations.	D-7-1	Confirmed



IDENTIFY VULNERABILITIES AND PREDISPOSING CONDITIONS

TABLE F-2: VULNERABILITY SEVERITY

- **HIGH:** l'assenza di MFA -> di grande preoccupazione con controlli compensativi minimi
- **MODERATE:** Vulnerability Assessment non regolari -> di moderata preoccupazione

TABLE F-4: TAXONOMY OF PREDISPOSING CONDITIONS

- **INFORMATION:** informazioni personalmente identificabili
- **TECHNICAL- Architectural:** Soluzioni e/o approcci alla collaborazione basata sull'utente e alla condivisione delle informazioni

TABLE F-5: PERVASIVENESS OF PREDISPOSING CONDITIONS

- **HIGH:** le condizioni predisponenti si applicano alla maggior parte dei sistemi dell'organizzazione

TABLE F-3: TEMPLATE – IDENTIFICATION OF VULNERABILITIES		
Identifier	Vulnerability Source of Information	Vulnerability Severity
F-3-1	MFA non abilitato.	High
F-3-2	Vulnerability Assessment non regolare	Moderate

TABLE F-6: TEMPLATE – IDENTIFICATION OF PREDISPOSING CONDITIONS

Identifier	Predisposing Condition Source of Information	Pervasiveness of Condition
F-6-1	INFORMATION – Personally Identifiable Information	High
F-6-2	TECHNICAL – Architectural – Solutions for and/or approaches to user-based collaboration and information sharing	High

TABLE G-2: LIKELIHOOD OF THREAT EVENT INITIATION (ADVERSARIAL)

- **VERY HIGH:** L'avversario è quasi certo di avviare l'evento di minaccia.

TABLE G-4: LIKELIHOOD OF THREAT EVENT RESULTING IN ADVERSE IMPACTS

- **VERY HIGH:** Se l'evento di minaccia viene avviato o si verifica, è quasi certo che avrà un impatto negativo.

DETERMINE LIKELIHOOD

TABLE G-5: ASSESSMENT SCALE – OVERALL LIKELIHOOD

Likelihood of Threat Event Initiation or Occurrence	Likelihood Threat Events Result in Adverse Impacts				
	Very Low	Low	Moderate	High	Very High
Very High	Low	Moderate	High	Very High	Very High
High	Low	Moderate	Moderate	High	Very High
Moderate	Low	Low	Moderate	Moderate	High
Low	Very Low	Low	Low	Moderate	Moderate
Very Low	Very Low	Very Low	Low	Low	Low

TABLE H-2: EXAMPLES OF ADVERSE IMPACTS

- **HARM TO ASSETS:**

Danneggiamento a o perdita di asset informativi

TABLE H-3: IMPACT OF THREAT EVENTS

- **HIGH:** Si prevede che l'evento di minaccia possa avere un effetto negativo grave o catastrofico sulle operazioni dell'organizzazione, sui beni dell'organizzazione, sulle persone, su altre organizzazioni o sulla nazione. Significa che, ad esempio, l'evento di minaccia potrebbe:
 - (i) causare un grave degrado o la perdita della capacità di missione in misura e durata tale da impedire all'organizzazione di svolgere una o più delle sue funzioni primarie;
 - (i) provocare gravi danni ai beni dell'organizzazione,
 - (i) provocare gravi perdite finanziarie, o
 - (iv) provocare danni gravi o catastrofici a persone che comportano la perdita della vita o lesioni gravi che mettono in pericolo la vita.

DETERMINE IMPACT

TABLE H-4: TEMPLATE – IDENTIFICATION OF ADVERSE IMPACTS

Type of Impact	Impact Affected Asset	Maximum Impact
HARM TO ASSETS	Damage to or of loss of information assets	High

L'impatto dell'avverarsi della minaccia identificata “danneggiamento o perdita di asset informativi (dati)” è alto.

DETERMINE RISK

TABLE I-5: TEMPLATE – ADVERSARIAL RISK

1	2	3	4	5	6	7	8	9	10	11	12	13
Threat Event	Threat Sources	Threat Source Characteristics			Relevance	Likelihood of Attack Initiation	Vulnerabilities and Predisposing Conditions	Severity and Pervasiveness	Likelihood Initiated Attack Succeeds	Overall Likelihood	Level of Impact	Risk
		Capability	Intent	Targeting								
E-5-1	D-7-1	H	M	H	C	VERY H	F-3-2	M	L	M	H	M
E-5-2	D-7-1	H	M	H	C	VERY H	F-3-2	M	L	M	H	M
E-5-3	D-7-1	H	M	H	C	VERY H	F-3-1	H	M	H	H	H
E-5-4	D-7-1	H	M	H	C	VERY H	F-3-1	H	M	H	H	H

DETERMINE RISK

Il rischio calcolato durante l'Assessment viene comunicato agli stakeholders organizzativi designati con un rapporto documentato di valutazione del rischio.

Comunicazione del Risk Assessment agli stakeholders.

Le misure di sicurezza implementate diminuiscono il livello del rischio a quello accettabile dalla società.

Effettuare un nuovo Risk Assessment per verificare l'efficacia dei controlli implementati, comunicando i risultati al personale organizzativo specifico.