

# RISK MANAGEMENT

## RISK

## ASSESSMENT

MARIA HUAPAYA





# INDICE

## 1. Traccia

## 2. Preparazione per il Risk Assessment (Step 1)

- Identificazione dello scopo
- Identificazione dell'ambito
- Identificazione delle ipotesi e dei vincoli
- Identificazione delle fonti di informazione
- Identificazione del modello di rischio e dell'approccio analitico

## 3. Conduzione dell'Assessment (Step 2)

- Identificazione delle fonti di minaccia: Tabella D-7
- Identificazione degli eventi di minaccia: Tabella E-5
- Identificazione delle vulnerabilità e delle condizioni predisponenti: Tabelle F-3 e F-6
- Determinazione della probabilità di occorrenza: Tabella G-5
- Determinazione dell'impatto: Tabella H-4
- Calcolo del rischio: Tabella I-5

## 4. Piani di Mitigazione e Azione

- Elaborare strategie di mitigazione basate sui rischi identificati.
- Passaggi specifici per l'implementazione delle misure di sicurezza, come MFA e regolari Vulnerability Assessments.

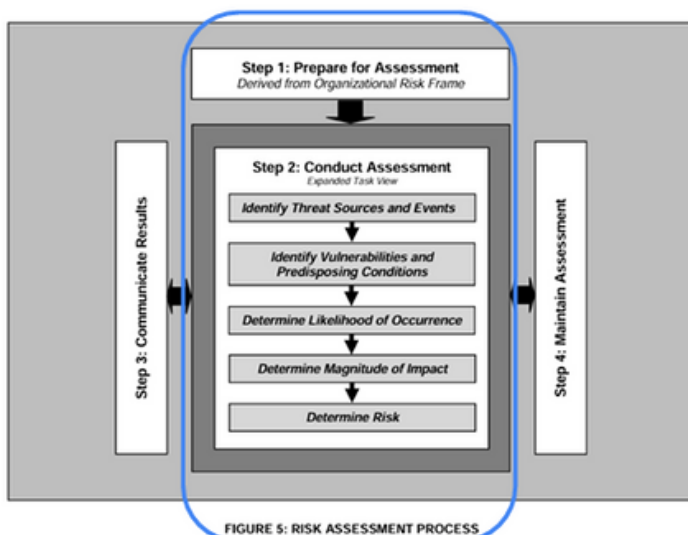
## 5. Riepilogo

# 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
<b>From Tier 1: (Organization level)</b> <ul style="list-style-type: none"> <li>Sources of threat information deemed to be credible (e.g., open source and/or classified threat reports, previous risk/threat assessments) (<b>Section 3.1, Task 1-4</b>)</li> <li>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)</li> <li>Taxonomy of threat sources, annotated by the organization, if necessary (<b>Table D-2</b>)</li> <li>Characterization of adversarial and non-adversarial threat sources</li> <li>Assessment scales for assessing adversary capability, intent, and targeting, annotated by the organization, if necessary (<b>Table D-3, Table D-4, Table D-5</b>)</li> <li>Assessment scale for assessing the range of effects, annotated by the organization, if necessary (<b>Table D-6</b>)</li> <li>Threat sources identified in previous risk assessments, if appropriate</li> </ul>	No	Yes	Yes if not provided by Tier 2
<b>From Tier 2: (Mission/business process level)</b> <ul style="list-style-type: none"> <li>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)</li> <li>Mission/business process-specific characterization of adversarial and non-adversarial threat sources</li> </ul>	Yes via RAR	Yes via peer sharing	Yes
<b>From Tier 3: (Information system level)</b> <ul style="list-style-type: none"> <li>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)</li> <li>Information system-specific characterization of adversarial and non-adversarial threat sources</li> </ul>	Yes via RAR	Yes via RAR	Yes via peer sharing



Scenario: Risk Management Progetto

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.

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



# **PREPARAZIONE PER IL RISK ASSESSMENT DI ALPHA HEALTHCARE (STEP 1)**

## **IDENTIFICAZIONE DELLO SCOPO**

Il processo di Risk Assessment per Alpha Healthcare mira a identificare, valutare e gestire i rischi associati alla protezione dei dati sanitari sensibili gestiti dall'organizzazione. Lo scopo principale è prevenire l'esfiltrazione di dati e altre violazioni di sicurezza da parte di attori esterni, in particolare gruppi criminali organizzati che hanno dimostrato un interesse specifico nei sistemi di Alpha Healthcare. Questa valutazione aiuterà a definire le misure di sicurezza necessarie per proteggere i dati, considerando l'attuale assenza di MFA e la mancanza di assessment periodici delle vulnerabilità.


## **IDENTIFICAZIONE DELL'AMBITO**

L'ambito di questa valutazione è rigorosamente definito per includere tutti i sistemi informativi che processano, trasmettono o memorizzano dati sanitari. Questo include:

- Sistemi Cloud: dove i dati sono archiviati e gestiti tramite soluzioni basate su cloud.
- Applicazioni Web: che i pazienti e il personale utilizzano per accedere e gestire i dati sanitari.
- Dispositivi Mobili: utilizzati dal personale medico per l'accesso remoto ai dati dei pazienti. Questa delimitazione garantisce che ogni componente che potrebbe essere esposto a rischi viene considerato nella valutazione.

## **IDENTIFICAZIONE DELLE IPOTESI E DEI VINCOLI**

- Ipotesi: presumiamo che le minacce principali provengano da attori esterni con intenti malevoli, capaci di attacchi sofisticati per ottenere accesso ai dati sanitari. Si presume inoltre che l'organizzazione non abbia adottato misure di sicurezza fondamentali come MFA, aumentando il rischio di compromissione.

- 
- **Vincoli:** le risorse limitate per la sicurezza potrebbero impedire l'adozione immediata di misure di mitigazione avanzate. La valutazione deve quindi considerare soluzioni che bilancino efficacia e costi, fornendo il miglior miglioramento possibile della sicurezza all'interno del budget disponibile.

## **IDENTIFICAZIONE DELLE FONTI DI INFORMAZIONE**

La valutazione si baserà su una combinazione di fonti di informazione interne ed esterne:

- **Interni:** registri degli eventi di sicurezza, rapporti di incidenti passati, e politiche di sicurezza attuali.
- **Esterni:** aggiornamenti e raccomandazioni da enti di standardizzazione e sicurezza come il NIST e l'ISACs, nonché intelligence di settore su minacce emergenti. Queste fonti permetteranno di avere una visione completa delle minacce attuali e potenziali.

## **IDENTIFICAZIONE DEL MODELLO DI RISCHIO E DELL'APPROCCIO ANALITICO**

Il modello di rischio adottato considererà i seguenti aspetti:

- **Probabilità di Occorrenza:** quanto frequentemente ci si può aspettare che determinate minacce si manifestino, basato su dati storici e tendenze attuali.
- **Impatto:** quali danni potrebbero risultare da ciascun evento di minaccia, sia in termini di perdite finanziarie che di danni alla reputazione. Un approccio qualitativo, supportato da valutazioni semi-quantitative per alcune aree, sarà utilizzato per fornire una stima del rischio complessivo.



# CONDUZIONE DELL'ASSESSMENT (STEP 2)

## IDENTIFICAZIONE DELLE FONTI DI MINACCIA

Per identificare le fonti di minaccia specifiche per il Tier 3, facciamo riferimento alla Tabella D-7 come richiesto.

Considerando l'ambiente di Alpha Healthcare, concentriamo l'attenzione su minacce che derivano da fonti esterne, principalmente gruppi criminali organizzati che mirano a sfruttare le vulnerabilità dei sistemi informativi per accedere ai dati sanitari.

Minacce Specifiche per il Tier 3:

- Gruppi Criminali Organizzati: questi attori hanno dimostrato capacità e intenzioni chiare nel mirare a organizzazioni sanitarie per ottenere un profitto tramite la vendita di dati rubati o il riscatto attraverso attacchi ransomware.
- Attacchi Cybernetici Avanzati: utilizzano tecniche come phishing avanzato, attacchi a zero-day e altre forme di ingegneria sociale per penetrare le difese di rete.
- Spionaggio Informatico: mirato alla raccolta di dati per scopi di ricatto o danneggiamento della reputazione aziendale.

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

Identifier	Threat Source Source of Information	In Scope	Capability	Intent	Targeting
Organization -defined	Table D-2 and Task 1-4 or Organization-defined	Yes / No	Table D-3 or Organization -defined	Table D-4 or Organization -defined	Table D-5 or Organization -defined
D-7/1	ADVERSARIAL	YES	HIGH	HIGH	HIGH

## IDENTIFICAZIONE DEGLI EVENTI DI MINACCIA

Per una comprensione approfondita degli eventi di minaccia che possono influenzare i sistemi informativi di Alpha Healthcare, utilizziamo la Tabella E-5. Questa analisi si concentra sugli eventi specifici che possono verificarsi a seguito delle minacce identificate nella fase precedente.

TABLE E-5: TEMPLATE – IDENTIFICATION OF THREAT EVENTS

Identifier	Threat Event Source of Information	Threat Source	Relevance
Organization-defined	Table E-2, Table E-3, Task 1-4 or Organization-defined	Table D-7, Table D-8 or Organization-defined	Table E-4 or Organization-defined
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 information 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

## IDENTIFICAZIONE DELLE VULNERABILITÀ E DELLE CONDIZIONI PREDISPONENTI

### IDENTIFICAZIONE DELLE VULNERABILITÀ (TABELLA F-3)

- Assenza di Multi-Factor Authentication (MFA): questa mancanza espone l'organizzazione a un rischio significativo di accessi non autorizzati. Senza MFA, il furto di credenziali può permettere agli attaccanti di accedere facilmente ai sistemi critici senza ostacoli aggiuntivi.
- Mancanza di Vulnerability Assessment Regolari: la non esecuzione regolare di controlli per identificare e mitigare le vulnerabilità lascia l'organizzazione esposta a rischi che potrebbero essere altrimenti identificati e risolti. Questo include la mancata patch di software con vulnerabilità note che possono essere sfruttate dagli attaccanti.

### IDENTIFICAZIONE DELLE CONDIZIONI PREDISPONENTI (TABELLA F-6)

Information-Related: Personally Identifiable Information

Condizione Predisponente: la gestione di informazioni personalmente identificabili (PII) su larga scala aumenta il rischio di esposizione in caso di violazioni della sicurezza. La presenza di queste informazioni nei sistemi informativi



dell'organizzazione le rende un bersaglio attraente per attacchi mirati a sottrarre o compromettere dati sensibili.

Pervasività della Condizione: Alta. I dati PII sono ampiamente distribuiti e accessibili attraverso vari sistemi informativi all'interno dell'organizzazione, aumentando la superficie di attacco e la complessità nella gestione della loro sicurezza.

Technical-Architectural: Solutions for and/or approaches to user-based collaboration and information sharing (F-6/2)

Condizione Predisponente: le soluzioni tecniche e architettoniche adottate per facilitare la collaborazione e la condivisione di informazioni tra gli utenti possono introdurre vulnerabilità se non adeguatamente protette. Questo include sistemi di condivisione di file, piattaforme collaborative e altri strumenti di comunicazione che, se compromessi, possono permettere agli attaccanti di accedere a reti interne e dati sensibili.

Pervasività della Condizione: Alta. L'uso estensivo di strumenti collaborativi è vitale per le operazioni quotidiane ma rende critica l'implementazione di robuste misure di sicurezza per proteggere le comunicazioni e i dati condivisi.

TABLE F-3: TEMPLATE – IDENTIFICATION OF VULNERABILITIES

Identifier	Vulnerability Source of Information	Vulnerability Severity
Organization- defined	Task 2-3, Task 1-4 or Organization-defined	Table F-2 or Organization-defined
<b>F-3/1</b>	<b>Multi-Factor Authentication (MFA) non abilitato</b>	<b>HIGH</b>
<b>F-3/2</b>	<b>Mancanza di Vulnerability Assessment Regolari</b>	<b>HIGH</b>

TABLE F-6: TEMPLATE – IDENTIFICATION OF PREDISPOSING CONDITIONS

Identifier	Predisposing Condition Source of Information	Pervasiveness of Condition
Organization- defined	Table F-4, Task 1-4 or Organization-defined	Table F-5 or Organization-defined
<b>F-6/1</b>	<b>Information-Related: Personally Identifiable Information</b>	<b>HIGH</b>
<b>F-6/2</b>	<b>Technical-Architectural: Solutions for and/or approaches to user-based collaboration and information sharing</b>	<b>HIGH</b>

# DETERMINAZIONE DELLA PROBABILITÀ DI OCCORRENZA (TABELLA G-5)

## Valutazione della Probabilità

Classifichiamo la probabilità degli eventi di minaccia come "Molto Alto", considerando:

- Elevata Frequenza e Tentativi di Attacco: gli attacchi contro Alpha Healthcare sono frequenti e persistenti, con evidenze di tentativi di intrusione continui. La natura dei dati gestiti dall'organizzazione (dati sanitari sensibili) attira attenzione e tentativi da parte di cybercriminali.
- Vulnerabilità Non Mitigate: la mancanza di misure di sicurezza fondamentali come il Multi-Factor Authentication (MFA) e la mancata realizzazione di valutazioni regolari delle vulnerabilità aumentano significativamente la probabilità che gli attacchi non solo siano tentati, ma che abbiano successo.

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

# DETERMINAZIONE DELL'IMPATTO

## Analisi dell'Impatto

Tipo di Impatto: Harm to Assets

Asset Colpiti: Damage to or Loss of Information Systems or Networks

Massimo Impatto: Alto

## Valutazione Dettagliata dell'Impatto:

- Danno agli Asset IT: l'impatto degli eventi di minaccia identificati, come intrusioni nei database, attacchi di phishing, e ransomware, può risultare in una significativa perdita o compromissione dei sistemi informativi e delle reti. Questo include la perdita di integrità e disponibilità dei dati sanitari sensibili, essenziali per le operazioni quotidiane di Alpha Healthcare.

- **Conseguenze Operative e Finanziarie:** un attacco riuscito che danneggia i sistemi informativi o le reti può avere gravi conseguenze operative, incluse interruzioni dei servizi, perdita di fiducia dei pazienti, e obblighi legali e sanzioni derivanti dalla violazione dei dati.
- **Ripristino e Mitigazione:** il costo e l'impegno necessario per ripristinare i sistemi informativi e le reti dopo un attacco possono essere significativi. Questo include il ripristino dei dati, la sostituzione di hardware/software compromesso, e l'implementazione di misure di sicurezza rafforzate post-incidente.

TABLE H-4: TEMPLATE – IDENTIFICATION OF ADVERSE IMPACTS

Type of Impact	Impact Affected Asset	Maximum Impact
Table H-2 or Organization-defined	Table H-2 or Organization-defined	Table H-3 or Organization-defined
<b>Harm to Assets</b>	<b>Damage to or loss of information systems or networks</b>	<b>HIGH</b>

## CALCOLO DEL RISCHIO COMPLESSIVO

### Determinazione del Rischio Complessivo

- Eventi con capacità, intento e targeting elevati, combinati con una moderata probabilità di successo, risultano in un rischio complessivo classificato come "moderato" per alcuni eventi. Tuttavia, per gli eventi con una combinazione di alta probabilità di attacco e successo, il rischio complessivo è valutato come "alto".
- Questo sottolinea la necessità di misure di mitigazione mirate a ridurre sia la probabilità che l'impatto di questi attacchi, specialmente dove il rischio è classificato come alto.

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	H	H	Confirmed	VH	F-3/2	M	L	M	H	M
E-5/1	D-7/1	H	H	H	Confirmed	VH	F-3/2	M	L	M	H	M
E-5/1	D-7/1	H	H	H	Confirmed	VH	F-3/1	H	M	H	H	H
E-5/1	D-7/1	H	H	H	Confirmed	VH	F-3/1	H	M	H	H	H

**L** = Low

**M** = Moderate

**H** = High

**VH** = Very High

# PIANI DI MITIGAZIONE E AZIONE

## ELABORARE STRATEGIE DI MITIGAZIONE BASATE SUI RISCHI IDENTIFICATI

Le strategie di mitigazione saranno focalizzate sul ridurre sia la probabilità che l'impatto degli eventi di minaccia, considerando i risultati del calcolo del rischio. Le azioni principali includono:

- Implementazione del Multi-Factor Authentication (MFA): introdurre MFA per tutte le piattaforme di accesso ai dati sensibili per aumentare la sicurezza degli accessi.
- Regolare Vulnerability Assessment: implementare un programma di valutazione delle vulnerabilità e gestione delle patch per identificare e mitigare le vulnerabilità in modo tempestivo.
- Rafforzamento delle infrastrutture di sicurezza: aggiornare e migliorare le infrastrutture di sicurezza IT, inclusi firewall avanzati, sistemi di rilevamento delle intrusioni, e soluzioni di sicurezza per endpoint.

## PASSAGGI SPECIFICI PER L'IMPLEMENTAZIONE DELLE MISURE DI SICUREZZA

Ogni strategia di mitigazione sarà accompagnata da una serie di azioni dettagliate, come:

- Sviluppo e Implementazione di Policy di Sicurezza: creare o aggiornare le politiche di sicurezza per includere l'uso obbligatorio di MFA e le procedure per regolari vulnerability assessments.
- Formazione Continua del Personale: organizzare sessioni regolari di formazione sulla sicurezza per educare i dipendenti su come riconoscere e gestire i tentativi di phishing e altre minacce di sicurezza.
- Piani di Risposta agli Incidenti: sviluppare o rivedere i piani di risposta agli incidenti per garantire che l'organizzazione possa rispondere efficacemente agli incidenti di sicurezza e minimizzare l'impatto operativo.



# RIEPILOGO

Durante il processo di Risk Assessment, abbiamo identificato una serie di minacce significative, valutato la probabilità e l'impatto degli eventi di minaccia, e sviluppato un piano di mitigazione dettagliato per affrontare questi rischi.

## **Le principali conclusioni includono:**

- **Alta Suscettibilità a Minacce Cyber:** Alpha Healthcare è particolarmente esposta a minacce cyber, data la natura sensibile dei dati gestiti e le lacune esistenti nelle misure di sicurezza.
- **Necessità di MFA e Vulnerability Assessments Regolari:** l'introduzione del MFA e la realizzazione regolare di vulnerability assessments sono essenziali per aumentare la resistenza dell'organizzazione contro gli attacchi informatici.
- **Importanza della Formazione del Personale:** la formazione continua del personale risulta cruciale per ridurre il rischio di attacchi riusciti, specialmente quelli che sfruttano l'ingegneria sociale.

Per garantire che le misure di mitigazione rimangano efficaci e che l'organizzazione sia preparata ad affrontare minacce future, è importante stabilire una serie di azioni continue:

- **Monitoraggio Continuo:** implementare soluzioni di monitoraggio continuo per rilevare rapidamente eventuali attacchi e rispondere in modo proattivo.
- **Revisioni Periodiche del Risk Assessment:** condurre revisioni periodiche del risk assessment per assicurare che le strategie di mitigazione siano aggiornate rispetto all'evolversi delle minacce e delle vulnerabilità.
- **Aggiornamento delle Politiche di Sicurezza:** aggiornare regolarmente le politiche di sicurezza per riflettere le migliori pratiche del settore e le raccomandazioni degli esperti di sicurezza.
- **Simulazioni di Attacchi e Test di Penetrazione:** eseguire regolarmente test di penetrazione e simulazioni di attacchi per valutare la resilienza delle infrastrutture IT e delle politiche di sicurezza.

# GRAZIE

MARIA HUAPAYA

