



PHANTOM SRL



EXAM S3/L5 2024

Prepared By :
PIGNATELLO GIUSEPPE
IANNONE LUCA
D'OTTAVIO ALESSIO

Presented To :
BCC ICCREA



www.phantomatici.com

INDICE

- Scenario.
- Politiche di gestione del rischio seguendo le normativa NIST.
- Ruoli, responsabilità, processi decisionali e requisiti di segnalazione per la gestione dei rischi.
- Metodologie e criteri per identificare, analizzare e valutare i rischi informatici, tenendo conto di minacce, vulnerabilità, probabilità e impatti.
- Procedure per selezionare, implementare e mantenere i controlli tecnici, operativi e gestionali per mitigare i rischi identificati.
- Procedure per monitorare continuamente i controlli di sicurezza, rilevare e rispondere agli eventi di sicurezza e mantenere un livello di rischio accettabile.
- Controlli e requisiti per proteggere la riservatezza, l'integrità e la disponibilità dei dati dei clienti. Formazione e consapevolezza.
- Piani per formare e sensibilizzare il personale e gli utenti finali sui rischi informatici e le pratiche di sicurezza.
- Consigli su nuove possibili implementazioni per rendere sicuri i dati sensibili dei clienti e il business.
- Ringraziamenti

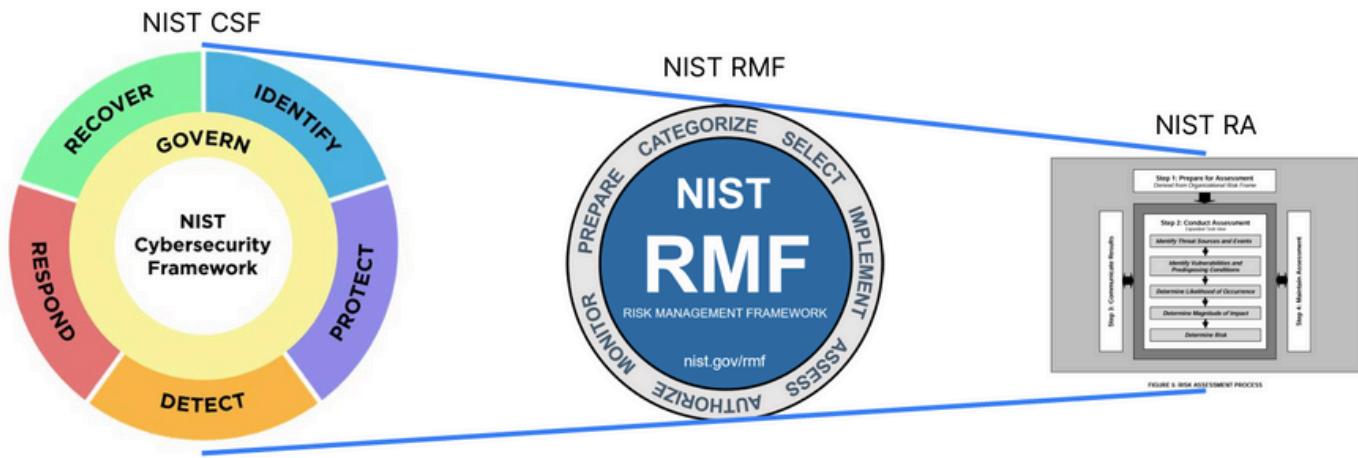


SCENARIO

FinCompany è un'importante istituzione finanziaria che offre servizi bancari tradizionali e digitali. Opera in diversi paesi con una vasta rete di filiali fisiche e sistemi informatici interconnessi. Questi sistemi includono:

- Sistema bancario core per l'elaborazione di transazioni, gestione dei conti e servizi ai clienti
- Applicazioni bancarie online/mobile per l'online banking dei clienti
- Rete aziendale per operazioni interne, comunicazioni e gestione dei dati
- Infrastruttura di sicurezza come firewall, IDS/IPS, autenticazione, crittografia

Essendo un'istituzione finanziaria, gestisce dati altamente sensibili come informazioni finanziarie, identificative e di transazione dei clienti. È fondamentale proteggere questi sistemi e dati da minacce informatiche come attacchi di malware, accesso non autorizzato, furto di dati e interruzioni del servizio.



Scegliete uno o più step del NIST RMF, per ogni task degli step selezionati, definite la politica di gestione del rischio (basta una piccola descrizione) in linea con lo scenario organizzativo proposto, individuando nello specifico se il **RA** è utilizzato in quella attività e come. Non va implementato il RA ma vanno definiti solo delle linee guida o dei principi.

Gli step che abbiamo deciso di definire sono:

- Ruoli, responsabilità, processi decisionali e requisiti di segnalazione per la gestione dei rischi.
- Metodologie e criteri per identificare, analizzare e valutare i rischi informatici, tenendo conto di minacce, vulnerabilità, probabilità e impatti.
- Procedure per selezionare, implementare e mantenere i controlli tecnici, operativi e gestionali per mitigare i rischi identificati.
- Processi di test, valutazione e autorizzazione per garantire che i sistemi soddisfino i requisiti di sicurezza e abbiano un livello di rischio accettabile.
- Procedure per monitorare continuamente i controlli di sicurezza, rilevare e rispondere agli eventi di sicurezza e mantenere un livello di rischio accettabile.
- Controlli e requisiti per proteggere la riservatezza, l'integrità e la disponibilità dei dati dei clienti. Formazione e consapevolezza
- Piani per formare e sensibilizzare il personale e gli utenti finali sui rischi informatici e le pratiche di sicurezza.
- Processi di risposta agli incidenti, contenimento, indagine, ripristino e comunicazione per fronteggiare efficacemente le violazioni di sicurezza.
- Cadenze e modalità per la revisione e il reporting della posizione di rischio dell'organizzazione ai dirigenti e alle parti interessate.
- Requisiti di sicurezza per le relazioni con i fornitori e l'approvvigionamento di servizi e tecnologie.

POLITICA DI GESTIONE DEL RISCHIO

(SEGUENDO I PRINCIPI DEL NIST)

La politica di gestione del rischio, secondo le linee guida del **National Institute of Standards and Technology** (NIST), è un insieme di principi, procedure e direttive che un'organizzazione adotta per identificare, valutare, mitigare e monitorare i rischi legati alla sicurezza delle informazioni e dei sistemi. Questa politica è essenziale per garantire che un'organizzazione gestisca in modo efficace e proattivo i rischi che possono minacciare la sicurezza delle sue risorse e dei suoi dati sensibili. Le normative del NIST forniscono un quadro dettagliato per la gestione del rischio, che include diversi documenti di riferimento come il **NIST Special Publication (SP) 800-37 Revision 2**, intitolato "Guida per l'implementazione del framework di gestione del rischio". Questo documento offre un approccio basato sul ciclo di vita per la gestione del rischio, noto come Risk Management Framework (RMF), che comprende i seguenti passaggi:

- 1. Preparazione:** Questo passaggio coinvolge la preparazione di un'organizzazione per la gestione del rischio, identificando i suoi obiettivi e i requisiti di sicurezza, assegnando responsabilità e autorità per la gestione del rischio e stabilendo una base per il processo di gestione del rischio.
- 2. Categorizzazione:** In questo passaggio vengono identificate e categorizzate le risorse di informazione e i sistemi in base al loro impatto sulla sicurezza, determinando il livello di protezione necessario.
- 3. Selezione dei controlli:** Questo passaggio coinvolge la selezione dei controlli di sicurezza appropriati per affrontare i rischi identificati, basandosi sulle categorie di sicurezza stabilite nel passaggio precedente.
- 4. Implementazione dei controlli:** Una volta selezionati i controlli di sicurezza, vengono implementati e integrati nei processi e nei sistemi dell'organizzazione.
- 5. Valutazione:** In questa fase, vengono valutati i controlli di sicurezza per determinare se sono stati implementati correttamente e se sono efficaci nel mitigare i rischi identificati.
- 6. Autorizzazione:** Dopo aver valutato i controlli di sicurezza, viene presa una decisione sull'autorizzazione del sistema per l'operazione e l'uso in base al livello di rischio accettabile.
- 7. Monitoraggio continuo:** Infine, i controlli di sicurezza e il livello di rischio vengono monitorati continuamente nel tempo per garantire che rimangano efficaci e per identificare e rispondere prontamente a nuove minacce o vulnerabilità.

La politica di gestione del rischio del NIST si basa su un approccio **sistemico e iterativo**, che consente alle organizzazioni di adattarsi ai cambiamenti nel panorama della minaccia e nel contesto operativo, assicurando la sicurezza delle informazioni e dei sistemi nel lungo termine.



RUOLI E RESPONSABILITÀ NELLE POLITICHE DI GESTIONE DEL RISCHIO.

TASK P-1:

Identificare e assegnare individui a ruoli specifici associati alla gestione del rischio per la sicurezza e la privacy.

Input Potenziali: Politiche e procedure di sicurezza e privacy dell'organizzazione; organigrammi dell'organizzazione.

Output Attesi: Assegnazioni di ruoli nel Framework di Gestione del Rischio documentate.

Responsabilità Primarie: Responsabile dell'Agenzia; Responsabile delle Informazioni; Funzionario Senior dell'Agenzia per la Privacy.

Politica: Viene sottolineata l'importanza di definire chiaramente i ruoli e le responsabilità all'interno della gestione del rischio per la sicurezza e la privacy. Descrive come questi ruoli possono variare in base alla struttura e alla missione dell'organizzazione. Si evidenzia inoltre che la combinazione di ruoli per la sicurezza e la privacy richiede attenzione poiché le due discipline possono richiedere competenze diverse e avere priorità che possono essere in conflitto.

Alcuni ruoli possono essere assegnati a gruppi o uffici anziché a singoli individui.

RA: Viene effettuato un risk assessment (valutazione del rischio) durante la fase iniziale di definizione dei ruoli e delle responsabilità nelle politiche di gestione del rischio.

La valutazione del rischio è un passaggio critico nel processo di gestione del rischio e fornisce una base per la definizione dei ruoli e delle responsabilità.

Durante il risk assessment, vengono identificate le potenziali minacce, le vulnerabilità e gli impatti associati ai sistemi e alle risorse dell'organizzazione.

Questa analisi fornisce informazioni cruciali per comprendere i rischi che l'organizzazione deve affrontare e stabilire la necessità di ruoli specifici per mitigare questi rischi.

Ad esempio, se durante il risk assessment emergono rischi legati alla gestione degli accessi ai dati sensibili, potrebbe essere necessario definire un ruolo specifico di "Responsabile della Sicurezza dell'Accesso" per garantire che vengano implementati i controlli adeguati per proteggere tali dati e monitorare gli accessi.

IDENTIFICARE, VALUTARE E ANALIZZARE I RISCHI.

TASK P-3:

Valutare il rischio per la sicurezza e la privacy a livello organizzativo e aggiornare i risultati della valutazione del rischio su base continua.

Input Potenziali: Strategia di gestione del rischio; obiettivi aziendali o di missione; informazioni correnti sulle minacce; risultati della valutazione del rischio per la sicurezza e la privacy a livello di sistema; risultati della valutazione del rischio della catena di fornitura; risultati precedenti della valutazione del rischio per la sicurezza e la privacy a livello organizzativo; accordi di condivisione delle informazioni o memorandum di intesa; informazioni sulla sicurezza e la privacy provenienti dal monitoraggio continuo.

Output Attesi: Risultati della valutazione del rischio a livello organizzativo.

Responsabilità Primarie: Funzionario Senior Responsabile della Gestione del Rischio o Responsabile Esecutivo del Rischio; Funzionario Senior per la Sicurezza delle Informazioni dell'Agenzia; Funzionario Senior dell'Agenzia per la Privacy.

Politica: Viene evidenziato che la valutazione del rischio a livello organizzativo si basa su informazioni aggregate provenienti da varie fonti, inclusi risultati di valutazioni a livello di sistema, monitoraggio continuo e considerazioni strategiche sul rischio. Si sottolinea l'importanza di considerare il rischio derivante dall'operazione e dall'uso dei sistemi informativi, nonché dagli scambi di informazioni con sistemi interni ed esterni e dall'impiego di fornitori esterni. Si menziona anche la possibilità di condurre valutazioni del rischio per la catena di fornitura dell'organizzazione.

RA: La valutazione dei rischi è a tutti gli effetti un punto fondamentale del risk assessment.

PROCEDURE PER SELEZIONARE E IMPLEMENTARE I CONTROLLI.

TASK P-7:

Sviluppare ed implementare una strategia a livello organizzativo per il monitoraggio continuo dell'efficacia dei controlli.

Input Potenziali: Strategia di gestione del rischio; risultati della valutazione del rischio a livello organizzativo e di sistema; politiche organizzative per la sicurezza e la privacy.

Output Attesi: Una strategia di monitoraggio continuo organizzativo implementata.

Responsabilità Primaria: Funzionario Senior Responsabile della Gestione del Rischio o Responsabile Esecutivo del Rischio (Funzione).

Politica: Viene sottolineata l'importanza di monitorare costantemente la sicurezza e la privacy in tutta l'organizzazione e l'efficacia dei controlli implementati. Si evidenzia che una strategia di monitoraggio continuo a livello organizzativo è essenziale per condurre in modo efficiente e conveniente tale monitoraggio. Si menziona anche l'inclusione di considerazioni sul rischio della catena di fornitura nelle strategie di monitoraggio continuo, come la revisione della proprietà estera dei fornitori.

RA: In questo Task il Risk Assessment è implicitamente coinvolto visto il compito di sviluppare e implementare una strategia di monitoraggio continuo per valutare l'efficacia dei controlli.

La valutazione dei rischi è un componente cruciale della gestione della sicurezza delle informazioni e della privacy, e stabilire una strategia di monitoraggio continuo implica la considerazione dei rischi che possono influenzare l'efficacia dei controlli di sicurezza implementati.

STRATEGIA DI MONITORAGGIO CONTINUO DEI CONTROLLI DI SICUREZZA.

TASK S-5:

Sviluppare ed implementare una strategia a livello di sistema per monitorare l'efficacia dei controlli che sia coerente con e integri la strategia di monitoraggio continuo dell'organizzazione.

Input Potenziali: Strategia di gestione del rischio dell'organizzazione; strategia di monitoraggio continuo dell'organizzazione; risultati della valutazione del rischio a livello organizzativo e di sistema; piani di sicurezza e privacy; politiche di sicurezza e privacy dell'organizzazione.

Output Attesi: Strategia di monitoraggio continuo per il sistema, inclusi i trigger basati sul tempo per l'autorizzazione continua.

Responsabilità Primaria: Proprietario del Sistema; Fornitore di Controlli Comuni.

Politica: Viene sottolineata l'importanza del monitoraggio continuo dei controlli implementati o ereditati dai sistemi informativi come parte della gestione del rischio. Si evidenzia che una strategia efficace di monitoraggio continuo a livello di sistema dovrebbe essere sviluppata e implementata in coordinamento con la strategia di monitoraggio continuo dell'organizzazione fin dalle fasi iniziali dello sviluppo del sistema. Questa strategia dovrebbe essere coerente con la strategia di monitoraggio continuo dell'organizzazione, affrontando specificamente quei controlli per i quali non è previsto il monitoraggio come parte della strategia organizzativa.

RA: Il compito di sviluppare e implementare una strategia di monitoraggio continuo per valutare l'efficacia dei controlli suggerisce l'importanza di comprendere e valutare i rischi associati alla sicurezza e alla privacy a livello di sistema tramite un precedente Risk Assessment.

CONTROLLI E REQUISITI PER PRESERVARE LA CIA TRIADE.

TASK C-2

Classificare il sistema e documentare i risultati della categorizzazione della sicurezza.

Input potenziali: strategia di gestione del rischio; tolleranza al rischio organizzativo; confine di autorizzazione (vale a dire, sistema) informazioni; risultati della valutazione del rischio a livello di organizzazione e di sistema; tipologie di informazioni trattate, memorizzati o trasmessi dal sistema; elenco dei requisiti di sicurezza e privacy assegnati al sistema, elementi del sistema e ambiente operativo; autorità organizzativa o scopo per il funzionamento del sistema; analisi dell'impatto aziendale o analisi della criticità; informazioni su missioni, funzioni aziendali, e missione/processi aziendali supportati dal sistema.

Risultati attesi: livelli di impatto determinati per ciascun tipo di informazione e per ciascun obiettivo di sicurezza (riservatezza, integrità, disponibilità); categorizzazione della sicurezza basata sul livello massimo di informazioni tipi di livelli di impatto.

Responsabilità Primaria: Proprietario del Sistema; Proprietario delle informazioni.

Politica: La categorizzazione della sicurezza considera gli impatti negativi potenziali derivanti dalla perdita di confidenzialità, integrità o disponibilità delle informazioni sulle operazioni organizzative, gli asset, gli individui, altre organizzazioni e la nazione. Le organizzazioni hanno la flessibilità di utilizzare FIPS 200 per definire un livello di impatto singolo per un sistema o CNSSI 1253 per stabilire tre valori di impatto per ogni obiettivo di sicurezza. Il processo coinvolge il proprietario del sistema, il custode delle informazioni e i leader senior per assicurare che i sistemi siano categorizzati in linea con la missione e gli obiettivi aziendali.

RA: Viene implementato per garantire che il sistema sia progettato e sviluppato tenendo conto dei rischi di sicurezza e privacy.

PIANI PER FORMARE E SENSIBILIZZARE IL PERSONALE E GLI UTENTI FINALI SUI RISCHI INFORMATICI E LE PRATICHE DI SICUREZZA

TASK I-1

Implementare i controlli nei piani di sicurezza e privacy.

Input potenziali: Piani di sicurezza e privacy approvati; documenti di progettazione del sistema; sicurezza organizzative e politiche e procedure sulla privacy; analisi di impatto o criticità aziendale; architettura d'impresa informazione; informazioni sull'architettura di sicurezza; informazioni sull'architettura della privacy; elenco di sicurezza e requisiti di privacy assegnati al sistema, elementi del sistema; e ambiente di funzionamento; sistema informazioni sugli elementi; inventario dei componenti del sistema; valutazione del rischio a livello di organizzazione e di sistema.

Risultati attesi: controlli attuati o implementazione di nuovi controlli per ridurre eventuali rischi non accettabili.

Responsabilità Primaria: Proprietario del Sistema; Fornitore di controllo comune.

Politica: Il testo parla di come le organizzazioni mettono in pratica le misure di sicurezza e privacy nei loro sistemi, assicurandosi che siano conformi all'architettura aziendale e ai requisiti di sicurezza e privacy. Si adottano le migliori pratiche, utilizzando metodologie di ingegneria dei sistemi di sicurezza e privacy e valutando i rischi per guidare le decisioni sull'implementazione dei controlli. Quando non è possibile controllare direttamente quali controlli vengano implementati, si considera l'uso di elementi di sistema testati o validati da terze parti. Si presta particolare attenzione ai requisiti di assicurazione per garantire che i controlli siano implementati correttamente.

Per quanto riguarda i controlli comuni ereditati dai sistemi, si collabora con i fornitori per determinare il modo migliore per implementarli. Se i controlli comuni non sono sufficienti per soddisfare i requisiti del sistema, i proprietari del sistema trovano controlli supplementari da implementare. Si valuta come mitigare le differenze tra i requisiti di sicurezza o privacy e i controlli comuni. Le organizzazioni conducono valutazioni iniziali durante lo sviluppo e l'implementazione dei sistemi per identificare e correggere tempestivamente eventuali problemi, riducendo così i costi e i ritardi.

RA: è necessario un Risk Assessment perché l'implementazione dei controlli di sicurezza e privacy nei sistemi dell'organizzazione comporta una serie di rischi potenziali che devono essere valutati e gestiti in modo appropriato.

CONSIGLI RIGUARDO NUOVE IMPLEMENTAZIONI.

FinCompany è un'importante istituzione finanziaria che offre servizi bancari tradizionali e digitali. Opera in diversi paesi con una vasta rete di filiali fisiche e sistemi informatici interconnessi. Questi sistemi includono:

- Sistema bancario core per l'elaborazione di transazioni, gestione dei conti e servizi ai clienti
- Applicazioni bancarie online/mobile per l'online banking dei clienti
- Rete aziendale per operazioni interne, comunicazioni e gestione dei dati
- Infrastruttura di sicurezza come firewall, IDS/IPS, autenticazione, crittografia

Non avendo certezze riguardo ulteriori sistemi di difesa, ci preme consigliare fortemente nuove implementazioni così da ridurre la possibilità e l'eventuale impatto di attacchi informatici:

1. Valutazione e Gestione del Rischio

- **Valutazioni periodiche del rischio:** Condurre valutazioni regolari dei rischi per identificare e mitigare le minacce emergenti.
- **Programma di gestione del rischio:** Implementare un programma completo di gestione del rischio per monitorare e gestire continuamente i rischi di sicurezza.

2. Protezione delle Infrastrutture e dei Dati

- **Segmentazione della rete:** Segmentare la rete aziendale per limitare i movimenti laterali degli attaccanti in caso di compromissione.

3. Autenticazione e Accesso

- **Autenticazione multifattore (MFA):** Implementare MFA per l'accesso ai sistemi e alle applicazioni critiche.
- **Gestione degli accessi privilegiati:** Utilizzare soluzioni di gestione degli accessi privilegiati per monitorare e controllare l'accesso degli utenti con privilegi elevati.

4. Sicurezza delle Applicazioni

- **Sicurezza delle applicazioni mobile/online:** Integrare pratiche di sviluppo sicuro (SDLC) e test di sicurezza nelle applicazioni bancarie online e mobile.
- **Penetration testing:** Condurre test di penetrazione regolari per identificare e risolvere le vulnerabilità nelle applicazioni.

5. Monitoraggio e Risposta agli Incidenti

- **Centro operativo di sicurezza (SOC):** Stabilire un SOC per monitorare continuamente gli eventi di sicurezza e rispondere rapidamente agli incidenti.
- **SIEM (Security Information and Event Management):** Implementare una soluzione SIEM per raccogliere e analizzare i log di sicurezza e rilevare comportamenti anomali.

6. Formazione e Consapevolezza dei Dipendenti

- **Programmi di formazione continua:** Educare i dipendenti sulle migliori pratiche di sicurezza e sulle tecniche di phishing e ingegneria sociale.
- **Simulazioni di phishing:** Eseguire campagne di phishing simulate per aumentare la consapevolezza e la prontezza dei dipendenti.

7. Conformità e Normative

- **Conformità alle normative:** Assicurarsi di essere conformi alle normative locali e internazionali sulla sicurezza e sulla privacy dei dati, come GDPR, PCI DSS, NIST, ISO e altre.
- **Audit regolari:** Condurre audit regolari per verificare la conformità e identificare le aree di miglioramento.

8. Resilienza e Continuità Operativa

- **Piani di continuità operativa:** Sviluppare e testare piani di continuità operativa e di recupero di emergenza per garantire la continuità dei servizi in caso di incidenti.
- **Backup e ripristino:** Implementare soluzioni di backup regolari e testare i processi di ripristino per garantire l'integrità e la disponibilità dei dati.

9. Gestione della Supply Chain

- **Valutazione dei fornitori:** Condurre valutazioni di sicurezza dei fornitori e richiedere loro di aderire a standard di sicurezza adeguati.
- **Contratti di sicurezza:** Includere clausole di sicurezza nei contratti con i fornitori per garantire che mantengano standard di sicurezza appropriati.

Queste misure combinate contribuiranno a rafforzare la postura di sicurezza di FinCompany, proteggendo le informazioni sensibili e assicurando la continuità operativa dei servizi bancari sia tradizionali che digitali.





PHANTOM SRL



**GRAZIE
2024**

Prepared By :
PIGNATELLO GIUSEPPE
IANNONE LUCA
D'OTTAVIO ALESSIO

Presented To :
BCC ICCREA



www.phantomatici.com