PROGETTO BCC ICCREA S3/L5

GESTIONE DEL RISCHIO INFORMATICO IN UN CONTESTO AZIENDALE

Traccia:

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 (in base alla numerosità del vostro gruppo) 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 obiettivi sono un plus), su argomenti come:

• 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.

TASK	RESPONSABILE	POLITICA	UTILIZZO RA
P1 RISK MANAGEMENT ROLES	Direttore della sicurezza dell'informazione (CISO)	Il CISO è incaricato di identificare i ruoli chiave per la gestione del rischio all'interno di FinCompany. Questo include la designazione di responsabilità specifiche per la gestione del rischio a livello operativo, tecnico e strategico, garantendo una chiara suddivisione dei compiti e delle responsabilità. Le linee guida: definizioni dei ruoli e le responsabilità di ogni attore coinvolto nella gestione del rischio, stabilendo le competenze necessarie per svolgere efficacemente ciascun ruolo.	Utilizzo del RA per valutare i potenziali rischi per la privacy associati ai ruoli chiave di gestione del rischio all'interno dell'organizzazione. Questo include l'analisi delle responsabilità di gestione del rischio e la valutazione delle minacce che potrebbero influenzare la privacy dei dati gestiti dai diversi ruoli.
P2 RISK MANAGEMENT STRATEGY	Comitato direttivo per la sicurezza delle informazioni, system owner	Definizione della strategia organizzativa di gestione del rischio per FinCompany, includendo l'identificazione della tolleranza al rischio e le priorità per la gestione dei rischi. Linee guida: fornire criteri chiari per la definizione della strategia organizzativa di gestione del rischio, assicurando che sia allineata agli obiettivi aziendali e agli standard di settore	Utilizzare il Risk Assessment per identificare le aree a rischio e allineare la strategia di gestione del rischio agli obiettivi aziendali e agli standard di settore.
P3 RISK ASSESSMENT ORGANIZATION	Team gestione del rischio	Valutazione del rischio a livello organizzativo per identificare le minacce, le	RA utilizzato per condurre la valutazione del rischio a livello organizzativo,

		vulnerabilità e gli impatti potenziali per FinCompany. Questa valutazione dovrebbe essere basata su metodologie e criteri approvati. Linee guida: definizione dei processi e metodologie da seguire durante la valutazione del rischio a livello organizzativo, garantendo una valutazione accurata e completa dei rischi.	identificando e valutando le minacce, le vulnerabilità e gli impatti per l'organizzazione.
C1 SYSTEM DESCRIPTION	Team sicurezza delle informazioni	Documentare le caratteristiche dei sistemi utilizzati da FinCompany, compresi il sistema bancario core, le applicazioni bancarie online/mobile, la rete aziendale e l'infrastruttura di sicurezza. Linee guida: definizione dei formati standardizzati e procedure per la raccolta accurata delle informazioni sul sistema, coinvolgendo gli stakeholder pertinenti per garantire una comprensione completa dei sistemi e delle loro interconnessioni.	Utilizzare il RA come riferimento per stabilire il livello di dettaglio dei piani di sicurezza e privacy.
C2 SECURITY ORGANIZATION	Team di gestione del rischio e sicurezza delle info	La politica riguarda la categorizzazione di sicurezza dei sistemi e delle informazioni utilizzati da FinCompany, basata sull'impatto negativo potenziale sulle operazioni e sui beni dell'organizzazione, nonché sulla riservatezza, integrità e disponibilità delle informazioni. linee guida dovrebbero definire criteri chiari per determinare l'impatto delle minacce sui	Utilizzare il privacy risk assessment come riferimento per stabilire il livello di dettaglio dei piani di sicurezza e privacy.

		sistemi e sulle informazioni, coinvolgendo gli stakeholder chiave per garantire una valutazione accurata e una classificazione appropriata.	
S1 CONTROL SELECTION	Team sicurezza informatica e compliance	selezionare e adattare i controlli necessari per proteggere i sistemi informativi e l'organizzazione in base al rischio identificato. Ciò include l'assegnazione dei controlli specifici ai componenti del sistema e lo sviluppo di una strategia di monitoraggio continuo. e linee guida dovrebbero definire i criteri per la selezione e l'adattamento dei controlli, tenendo conto delle specifiche esigenze e delle minacce identificate per FinCompany.	Identificazione dei controlli necessari per proteggere la privacy dei dati dei clienti.
I1 CONTROL IMPLEMENTATION	Team di sicurezza informatica e compliance	Attuazione dei controlli specificati nei piani di sicurezza per garantire che i sistemi soddisfino i requisiti di sicurezza identificati durante il processo di valutazione del rischio. inee guida dovrebbero definire i processi e le procedure per l'attuazione dei controlli, assicurando che vengano seguite le migliori pratiche e gli standard di settore.	RA per guidare l'implementazione dei controlli specificati nei piani di sicurezza e privacy di FinCompany. Questo include l'assicurarsi che i controlli implementati siano adeguati a proteggere la privacy dei dati dei clienti in base alla valutazione dei rischi effettuata utilizzando il RA
A1 ASSESSOR SELECTION	Responsabile della sicurezza delle informazioni	Selezione del valutatore o del team di valutazione incaricato di condurre le valutazioni dei controlli di sicurezza. Le linee guida dovrebbero definire i criteri per la selezione del valutatore o del team di valutazione, assicurando che	RA per selezionare valutatori competenti e indipendenti per condurre valutazioni dei rischi relativi alla privacy dei dati dei clienti.

		siano competenti e indipendenti.	
A2 ASSESSMENT PLAN	Comitato di sicurezza dell'informazione	Sviluppo dei piani di valutazione della sicurezza e della privacy per guidare le attività di valutazione dei controlli. Linee guida dovrebbero definire i contenuti e le procedure per lo sviluppo dei piani di valutazione, assicurando la coerenza e l'efficacia delle attività di valutazione.	Utilizzare il Privacy RA per determinare le aree critiche da valutare e per sviluppare piani di valutazione efficaci.
R1 AUTHORIZATION PACKAGE	Responsabile della sicurezza delle informazioni	Reparazione del pacchetto di autorizzazione, che include l'esecutivo sintetico, il piano di sicurezza e privacy del sistema, i rapporti di valutazione e il piano d'azione. Linee guida: definizione dei contenuti e i requisiti per la preparazione del pacchetto di autorizzazione, assicurando che siano conformi alle normative e agli standard aziendali.	RA per compilare il pacchetto di autorizzazione con informazioni dettagliate sui rischi identificati e sui controlli implementati.
M1 SYSTEM AND ENVIROMENT CHANGES	Team di monitoraggio della sicurezza informatica	Monitoraggio continuo del sistema e dell'ambiente operativo per rilevare e rispondere tempestivamente agli eventi di sicurezza. Linee guida: definizione dei processi e le procedure per il monitoraggio continuo, comprese le metriche chiave di performance e gli indicatori di allarme precoce.	Utilizzare il Risk Assessment per monitorare continuamente l'efficacia dei controlli di sicurezza e privacy, rilevare e rispondere agli eventi di sicurezza, e mantenere un livello di rischio accettabile.