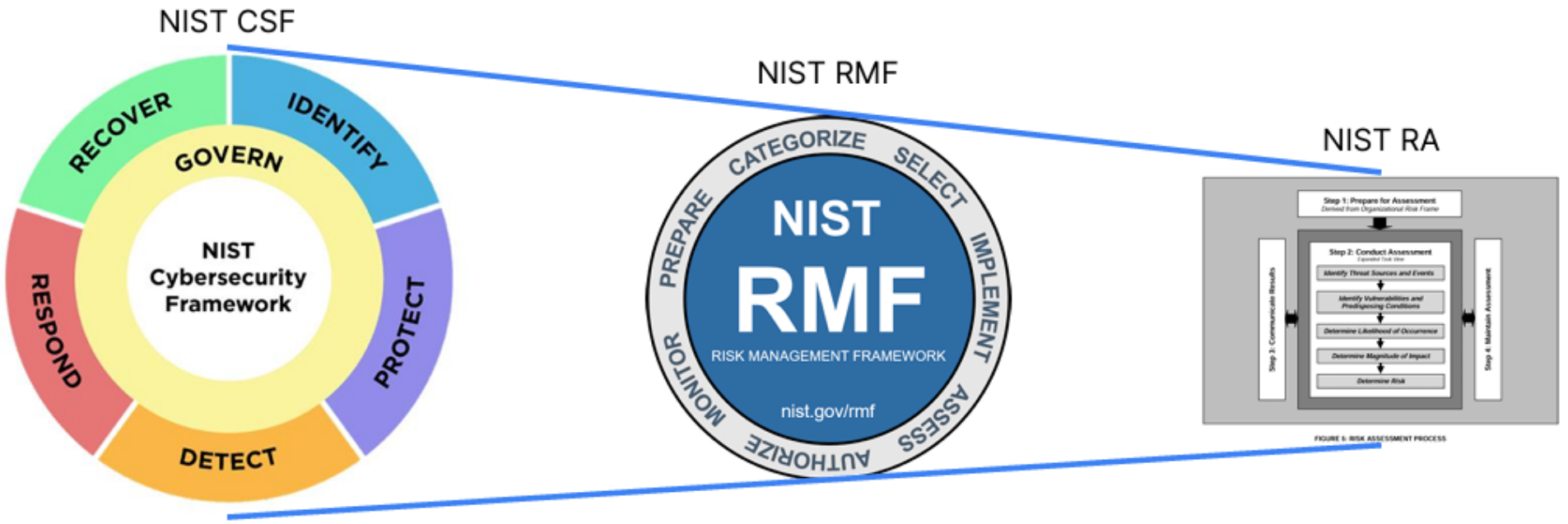
BCC S3L5 GESTIONE DEL RISCHIO INFORMATICO IN UN CONTESTO AZIENDALE

La settimana scorsa abbiamo visto come strutturare il Risk Assessment NIST SP 800-30, che è utilizzato in diversi punti del NIST RMF SP 800-37 che a sua volta è una componente del NIST CSF 2.0 CSWP 29. In questo progetto andremo a sviluppare uno dei documenti fondamentali per la gestione del rischio:

- **Politica di gestione del rischio**: questo documento definisce gli obiettivi, i principi e le linee guida generali per la gestione dei rischi all'interno dell'organizzazione.



Scenario

- Risk Management Progetto 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
- • Cadenze e modalità per la revisione e il reporting della posizione di rischio dell'organizzazione ai dirigenti e alle parti interessati
- •Requisiti di di sicurezza per le relazione con i fornitori e l'approvigionamento di servizi e tecnologie

Esempio

SYSTEM DESCRIPTION

TASK C-1 Document the characteristics of the system.

Potential Inputs: System design and requirements documentation; authorization boundary information; list of security and privacy requirements allocated to the system, system elements, and the environment

[24] The RMF *Categorize* step is a precondition for the selection of security controls. However, for privacy, there are other factors considered by organizations that guide and inform the selection of privacy controls. These factors are described in the RMF *Prepare-System Level* step, Task P-15.

of operation; physical or other processes controlled by system elements; system element information; system component inventory; system element supply chain information, including inventory and supplier information; security categorization; data map of the information life cycle for information types processed, stored, and transmitted by the system; information on system use, users, and roles.

Expected Outputs: Documented system description.

Primary Responsibility: System Owner.

Supporting Roles: Authorizing Official or Authorizing Official Designated Representative; Information Owner or Steward; System Security Officer; System Privacy Officer.

System Development Life Cycle Phase: New – Initiation (concept/requirements definition).
Existing – Operations/Maintenance.

Discussion: A description of the system characteristics is documented in the security and privacy plans, included in attachments to the plans, or referenced in other standard sources for the information generated as part of the SDLC. Duplication of information is avoided, whenever possible. The level of detail in the security and privacy plans is determined by the organization and is commensurate with the

Task	Responsabile	Politica	Utilizzo RA
C-1 System Description	System Owner	Documentare in dettaglio le caratteristiche dei sistemi IT, inclusi lo scopo, i componenti hardware/software, le interconnessioni di rete, i flussi di dati, gli utenti e i fornitori nella supply chain.Considerare di includere una valutazione dei rischi della supply chain per identificare eventuali fornitori o componenti a rischio.	In questo task è utilizzato il privacy risk assessment come riferimento per stabilire il livello di dettaglio dei piani di sicurezza e privacy.

POLITICA DI GESTIONE DEL RISCHIO PER FINCOMPANY

- La politica di gestione del rischio per FinCompany mira a stabilire una struttura chiara per identificare, valutare e mitigare i rischi legati ai sistemi informatici e alle operazioni finanziarie. La politica è allineata con le linee guida del NIST RMF (SP 800-37) e del NIST CSF, utilizzando il framework di valutazione dei rischi descritto nel NIST SP 800-30.

Obiettivi della Politica

- Proteggere la riservatezza, l'integrità e la disponibilità dei dati dei clienti.
- Garantire la conformità alle normative e agli standard di sicurezza informatica.
- Ridurre al minimo l'impatto delle minacce informatiche sulle operazioni aziendali.
- Promuovere una cultura aziendale orientata alla sicurezza informatica e alla gestione del rischio.

STEP DEL NIST RMF E POLITICHE CORRELATE

1 Categorizzazione dei Sistemi Informativi

- Task: Categorizzazione dei sistemi informativi basata sull'analisi di impatto.
- Responsabile: Chief Information Security Officer (CISO)
- Politica: Tutti i sistemi informativi devono essere categorizzati secondo il loro impatto potenziale sulla missione aziendale, sui dati dei clienti e sulle operazioni. L'analisi deve includere una valutazione dei rischi per determinare la probabilità e l'impatto delle minacce identificate. Utilizzare il RA per determinare le categorie di rischio e stabilire i livelli di protezione necessari

2 Selezione dei Controlli di Sicurezza

- Task: Selezionare i controlli di sicurezza appropriati per proteggere i sistemi informativi.
- Responsabile: IT Security Manager
- Politica: Selezionare i controlli di sicurezza tecnici, operativi e gestionali basandosi sui rischi identificati durante la fase di categorizzazione. L'uso del RA è essenziale per valutare l'efficacia dei controlli proposti e per garantire che siano adeguati a mitigare i rischi specifici rilevati.

3 Implementazione dei Controlli di Sicurezza

- Task: Implementare i controlli di sicurezza selezionati e documentare la loro implementazione.
- Responsabile: IT Operations Team
- Politica: Implementare i controlli di sicurezza selezionati e documentare dettagliatamente la loro applicazione e funzionamento. Utilizzare il RA per monitorare e verificare che i controlli implementati riducano i rischi a livelli accettabili.

4 Valutazione dei Controlli di Sicurezza

- Task: Valutare l'efficacia dei controlli di sicurezza.
- Responsabile: Independent Security Assessor
- Politica: Condurre valutazioni regolari per verificare l'efficacia dei controlli di sicurezza implementati. Utilizzare il RA per identificare eventuali vulnerabilità residue e per fornire raccomandazioni su ulteriori misure di mitigazione.

5 Autorizzazione dei Sistemi Informativi

- Task: Autorizzare l'operazione dei sistemi informativi.
- Responsabile: Authorizing Official (AO)
- Politica: L'autorizzazione all'operatività dei sistemi informativi deve basarsi su una valutazione approfondita dei rischi residui e sulla conferma che i controlli di sicurezza siano sufficienti. Il RA fornisce il quadro di riferimento per la decisione, garantendo che i rischi siano gestiti adeguatamente.

6 Monitoraggio dei Controlli di Sicurezza

- Task: Monitorare continuamente i controlli di sicurezza e lo stato di sicurezza dei sistemi informativi.
- Responsabile: Security Operations Center (SOC) Team
- Politica: Monitorare continuamente i controlli di sicurezza per rilevare e rispondere prontamente agli eventi di sicurezza. Il RA è utilizzato per aggiornare e rivedere periodicamente il profilo di rischio, assicurando che i controlli rimangano efficaci nel tempo.

LINEE GUIDA SPECIFICHE

Ruoli e Responsabilità

- CISO: Supervisiona l'intero programma di gestione del rischio e garantisce la conformità con le politiche di sicurezza.
- IT Security Manager: Responsabile della selezione e implementazione dei controlli di sicurezza.
- IT Operations Team: Implementa e documenta i controlli di sicurezza.
- Independent Security Assessor: Valuta l'efficacia dei controlli di sicurezza.
- Authorizing Official (AO): Autorizza i sistemi informativi.
- SOC Team: Monitora continuamente la sicurezza dei sistemi informativi.

Metodologie e Criteri di Valutazione

- Utilizzare metodologie standardizzate come quelle del NIST SP 800-30 per identificare, analizzare e valutare i rischi informatici. Considerare minacce, vulnerabilità, probabilità e impatti per determinare il livello di rischio.

Procedure di Controllo e Mitigazione

- Selezionare controlli tecnici, operativi e gestionali basandosi su una valutazione dei rischi. Implementare controlli di sicurezza come firewall, IDS/IPS, autenticazione e crittografia per proteggere i dati sensibili.

Monitoraggio Continuo

- Implementare processi di monitoraggio continuo per rilevare e rispondere agli eventi di sicurezza. Utilizzare strumenti di monitoraggio e gestione dei log per mantenere un livello di rischio accettabile.

Formazione e Consapevolezza

- Sviluppare programmi di formazione per sensibilizzare il personale e gli utenti finali sui rischi informatici e sulle pratiche di sicurezza. Effettuare sessioni di formazione periodiche e test di consapevolezza.

Risposta agli Incidenti

- Definire processi chiari per la risposta agli incidenti, includendo contenimento, indagine, ripristino e comunicazione. Assicurarsi che il personale sia addestrato e pronto a rispondere efficacemente alle violazioni.

Revisione e Reporting

- Stabilire cadenze regolari per la revisione e il reporting della posizione di rischio dell'organizzazione. Fornire report dettagliati ai dirigenti e alle parti interessate.

Relazioni con i Fornitori

- Definire requisiti di sicurezza per la gestione delle relazioni con i fornitori. Assicurarsi che i fornitori rispettino le politiche di sicurezza e i controlli di rischio dell'organizzazione.

- La politica di gestione del rischio per FinCompany è progettata per garantire che i rischi siano identificati, valutati e mitigati in modo efficace. L'adozione delle linee guida del NIST RMF e l'uso del RA assicurano che l'organizzazione mantenga un elevato livello di sicurezza e conformità, proteggendo al contempo i dati sensibili dei clienti.