PHANTOM s.r.l
IMPOSSIBLE IS OUR TARGET

PHANTOM SRL
SINCE 2024

TRATTAMENTO DEL RISCHIO

Presented To : EPICODE

Team:

- Alessio D'Ottavio
- Davide Di Turo
- Giuseppe Pigniatello
- Luca Iannone
- Manuel Di Gangi
- Marco Fasani

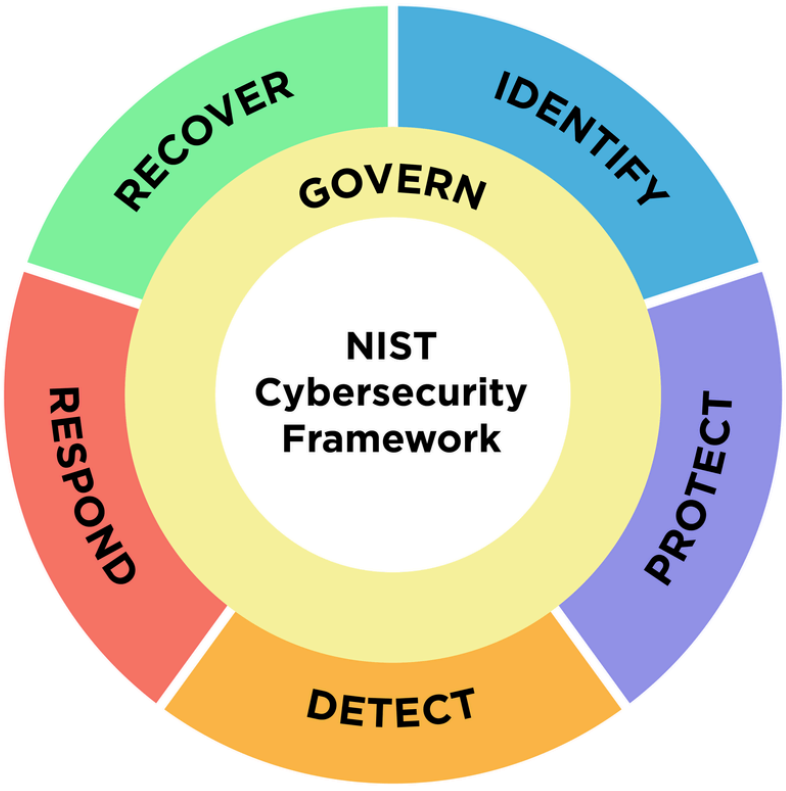
INDICE

Traccia

Un'azienda di servizi finanziari gestisce un'applicazione web che consente ai clienti di accedere ai propri account e effettuare transazioni finanziarie online. L'applicazione web memorizza e gestisce dati sensibili dei clienti, come informazioni personali, dettagli finanziari e credenziali di accesso. Il rischio principale è rappresentato da potenziali attacchi informatici volti a compromettere la sicurezza dell'applicazione web e a ottenere l'accesso non autorizzato ai dati dei clienti. Supponendo di aver già effettuato l'analisi del rischio per lo scenario identificato, l'azienda decide di non accettare il rischio e procedere con la mitigazione del rischio applicando degli ulteriori controlli.

Utilizzando NIST SP 800-53, seleziona 5 controlli, uno per ogni funzione di controllo(Deterrent, Preventive, Detective, Corrective, Compensating) e stabilisci come agisce il controllo sul rischio (può essere anche una combinazione):

- Diminuendo la probabilità che un threat agent avvii una minaccia;
- Diminuendo la probabilità che una minaccia sfrutti una vulnerabilità;
- Diminuendo la vulnerabilità;
- Diminuendo l'impatto se la minaccia riesce a sfruttare la vulnerabilità;



NIST SP 800-53

l National Institute of Standards and Technology (NIST) degli Stati Uniti ha rilasciato una nuova guida per eseguire valutazioni della privacy e dei controlli di sicurezza all'interno dei sistemi e delle organizzazioni: il documento, pubblicato lo scorso 25 gennaio 2022, è un'integrazione della NIST SP 800-53 "Security and Privacy Controls for Information Systems and Organizations", di cui era stata pubblicata la quinta versione a fine 2020: ne abbiamo parlato in questo articolo.

La NIST SP 800-53 è una delle pubblicazioni più importanti tra quelle emesse dal NIST, assieme al NIST Cybersecurity Framework (CSF) ed è completata da altri due documenti:

SP 800-53A Assessing Security and Privacy Controls in Information Systems and Organizations
SP 800-53B Control Baselines for Information Systems and Organizations
L'aggiornamento revisione 5 pubblicato a gennaio 2022 riguarda appunto la SP 800-53A Assessing Security and Privacy Controls in Information Systems and Organizations e sostituisce la precedente NIST.SP.800-53Ar4 che risaliva a dicembre 2014, quindi in un tempo in cui non erano ancora nati né il GDPR né il California Consumer Privacy Act (CCPA).

Quest'ultima – lo ricordiamo – è una legge statale sulla protezione dei dati che disciplina il modo in cui le aziende di tutto il mondo sono autorizzate a trattare le informazioni personali dei cittadini residenti in California. CCPA è entrato in vigore il primo gennaio 2020 (pienamente applicabile dal primo luglio 2020) e rappresenta la più recente ed importante legge sulla privacy negli Stati Uniti.

Questa pubblicazione NIST fornisce una metodologia e una serie di procedure per condurre le valutazioni dei controlli di sicurezza e privacy impiegati all'interno dei sistemi e delle organizzazioni in un efficace quadro di gestione del rischio.

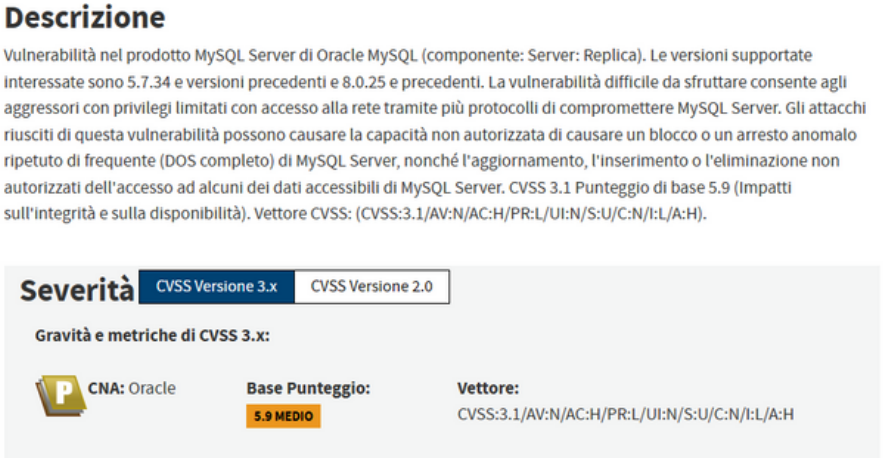
Rischio Intrinseco Web App

Il rischio intrinseco di un'applicazione web si riferisce alla probabilità che l'applicazione possa essere vulnerabile a minacce e attacchi informatici, considerando la sua natura e le sue caratteristiche specifiche. Questi rischi possono variare in base a diversi fattori, tra cui la complessità dell'applicazione, la sensibilità dei dati trattati, la presenza di vulnerabilità nel codice e la conformità normativa.

Rischio identificato

A seguito delle analisi svolte, è stato identificato il rischio di un potenziale attacco informatico mirato all'applicazione web dell'azienda di servizi finanziari, con l'obiettivo di compromettere la sicurezza dei dati sensibili dei clienti e ottenere l'accesso non autorizzato agli account. Ecco qualche esempio di vulnerabilità note:

1. **SQL Injection (SQLi):** Questa vulnerabilità si verifica quando un'applicazione web incorpora input utente non filtrati all'interno di comandi SQL. Gli attaccanti possono sfruttare questa vulnerabilità per eseguire comandi SQL dannosi che consentono loro di accedere, modificare o eliminare dati dal database.
2. **Cross-Site Scripting (XSS):** In un attacco XSS, gli hacker inseriscono script dannosi all'interno del contenuto dinamico di una pagina web. Quando gli utenti visualizzano la pagina, gli script vengono eseguiti nel loro browser, consentendo agli attaccanti di rubare cookie di sessione, modificare il contenuto della pagina o reindirizzare gli utenti verso siti web dannosi.
3. **Mancata autenticazione e autorizzazione:** Se un'applicazione web non implementa correttamente controlli di autenticazione e autorizzazione, gli attaccanti possono sfruttare questa vulnerabilità per ottenere accesso non autorizzato ai dati o alle funzionalità dell'applicazione.



1. Controllo dissuasione (Deterrent)

- Controllo: Implementazione di avvisi di sicurezza e dichiarazioni di responsabilità all'accesso dell'applicazione.
- Come agisce sul rischio: Questo controllo dissuade i threat agent fornendo una chiara comunicazione sul monitoraggio attivo della sicurezza e sulle azioni legali che verranno intraprese contro gli attacchi informatici. Ciò può ridurre la probabilità che un threat agent avvii una minaccia, in quanto renderà l'attacco meno attraente o rischioso.

Identificativo NIST SP 800-53 Rev. 5 "**AC-8 SYSTEM USE NOTIFICATION**".
Questo controllo prevede l'implementazione di avvisi legali e dichiarazioni di responsabilità all'interno delle reti e delle applicazioni al fine di informare gli utenti riguardo alle politiche di utilizzo accettate, alle responsabilità legali e alle possibili conseguenze delle azioni non autorizzate. Questo controllo assicura che gli utenti siano pienamente consapevoli delle regole e delle restrizioni associate all'accesso e all'utilizzo delle risorse informatiche, facilitando così una maggiore trasparenza e conformità alle politiche di sicurezza dell'organizzazione.

NIST SP 800-53A Rev. 5
Assessment dei controlli da effettuare dopo l'implementazione

AC-08	SYSTEM USE NOTIFICATION	
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	AC-08-Examine	[SELECT FROM: Access control policy; privacy and security policies, procedures addressing system use notification; documented approval of system use notification messages or banners; system audit records; user acknowledgements of notification message or banner; system design documentation; system configuration settings and associated documentation; system use notification messages; system security plan; privacy plan; privacy impact assessment; privacy assessment report; other relevant documents or records].
	AC-08-Interview	[SELECT FROM: System/network administrators; organizational personnel with information security and privacy responsibilities; legal counsel; system developers].
	AC-08-Test	[SELECT FROM: Mechanisms implementing system use notification].

2. Controllo prevenzione (Preventive)

- Controllo: Implementazione di un firewall perimetrale e regole di accesso basate su ruoli e implementazione di autenticazione 2FA o MFA (codice OTP generato su dispositivi aziendali per l'accesso).
- Come agisce sul rischio: Questo controllo riduce la probabilità che una minaccia sfrutti una vulnerabilità bloccando l'accesso non autorizzato all'applicazione web tramite regole di filtraggio del traffico e limitando l'accesso solo a utenti autorizzati. Inoltre, il firewall può bloccare attacchi noti e tentativi di exploit.

Identificativo NIST SP 800-53 Rev. 5 "**SC-7 BOUNDARY PROTECTION**".
Questo controllo richiede l'implementazione di controlli tecnici per gestire l'accesso alla rete e proteggere i sistemi informativi da minacce esterne e interne.

Identificativo NIST SP 800-53 Rev. 5 "**AC-3 ACCESS ENFORCEMENT**".
Questo controllo stabilisce i criteri per garantire che l'accesso ai sistemi informativi e alle risorse sia limitato solo a utenti autorizzati. Una delle sottocategorie del controllo AC-3 **sottocategoria 7,** riguarda l'implementazione di controlli di accesso basati su ruoli (RBAC), che consentono di assegnare privilegi e autorizzazioni agli utenti in base ai ruoli specifici che ricoprono all'interno dell'organizzazione.

Identificativo NIST SP 800-53 Rev. 5 "**IA-2 IDENTIFICATION AND AUTHENTICATION**".
Questo controllo stabilisce le linee guida per l'implementazione di metodi di autenticazione che richiedono l'utilizzo di più fattori per verificare l'identità dell'utente.

NIST SP 800-53A Rev. 5
Assessment dei controlli da effettuare dopo l'implementazione

SC-07	BOUNDARY PROTECTION	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	SC-07_ODP	*one of the following PARAMETER VALUES is selected: {physically; logically};*
	SC-07a.[01]	communications at external managed interfaces to the system are monitored;
	SC-07a.[02]	communications at external managed interfaces to the system are controlled;
	SC-07a.[03]	communications at key internal managed interfaces within the system are monitored;
	SC-07a.[04]	communications at key internal managed interfaces within the system are controlled;
	SC-07b.	subnetworks for publicly accessible system components are ***<SC-07_ODP SELECTED PARAMETER VALUE>*** separated from internal organizational networks;
	SC-07c.	external networks or systems are only connected to through managed interfaces consisting of boundary protection devices arranged in accordance with an organizational security and privacy architecture.

	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	SC-07-Examine	[SELECT FROM: System and communications protection policy; procedures addressing boundary protection; list of key internal boundaries of the system; system design documentation; boundary protection hardware and software; system configuration settings and associated documentation; enterprise security architecture documentation; system audit records; system security plan; other relevant documents or records].
	SC-07-Interview	[SELECT FROM: System/network administrators; organizational personnel with information security responsibilities; system developer; organizational personnel with boundary protection responsibilities].
	SC-07-Test	[SELECT FROM: Mechanisms implementing boundary protection capabilities].

AC-03(07)	**ACCESS ENFORCEMENT | ROLE-BASED ACCESS CONTROL**	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	AC-03(07)_ODP[01]	***roles upon which to base control of access are defined;***
	AC-03(07)_ODP[02]	***users authorized to assume roles (defined in AC-03(07)_ODP[01]) are defined;***
	AC-03(07)[01]	a role-based access control policy is enforced over defined subjects;
	AC-03(07)[02]	a role-based access control policy is enforced over defined objects;
	AC-03(07)[03]	access is controlled based on ***<AC-03(07)_ODP[01] roles>*** and ***<AC-03(07)_ODP[02] users authorized to assume such roles>***.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	AC-03(07)-Examine	[SELECT FROM: Access control policy; role-based access control policies; procedures addressing access enforcement; system design documentation; system configuration settings and associated documentation; list of roles, users, and associated privileges required to control system access; system audit records; system security plan; privacy plan; other relevant documents or records].
	AC-03(07)-Interview	[SELECT FROM: Organizational personnel with access enforcement responsibilities; system/network administrators; organizational personnel with information security and privacy responsibilities; system developers].
	AC-03(07)-Test	[SELECT FROM: Mechanisms implementing role-based access control policy].

IA-02	**IDENTIFICATION AND AUTHENTICATION (ORGANIZATIONAL USERS)**	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	IA-02[01]	organizational users are uniquely identified and authenticated;
	IA-02[02]	the unique identification of authenticated organizational users is associated with processes acting on behalf of those users.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	IA-02-Examine	[SELECT FROM: Identification and authentication policy; procedures addressing user identification and authentication; system security plan, system design documentation; system configuration settings and associated documentation; system audit records; list of system accounts; other relevant documents or records].
	IA-02-Interview	[SELECT FROM: Organizational personnel with system operations responsibilities; organizational personnel with information security responsibilities; system/ network administrators; organizational personnel with account management responsibilities; system developers].
	IA-02-Test	[SELECT FROM: Organizational processes for uniquely identifying and authenticating users; mechanisms supporting and/or implementing identification and authentication capabilities].

3. Controllo individuazione (Detective)

- Controllo: Implementazione di sistemi di rilevamento delle intrusioni (IDS/IPS) e dei registri di accesso.
- Come agisce sul rischio: Questo controllo riduce la probabilità che una minaccia sfrutti una vulnerabilità rilevando e segnalando immediatamente anomalie o attività sospette nell'applicazione web. Gli IDS monitorano costantemente il traffico di rete e i registri di accesso registrano le attività degli utenti per consentire una rapida risposta agli incidenti di sicurezza.

Identificativo NIST SP 800-53 Rev. 5 "**SI-4 SYSTEM MONITORING**".
Questo controllo stabilisce le linee guida per il monitoraggio delle attività dei sistemi informativi al fine di rilevare, registrare e rispondere a eventi di sicurezza.

- **Sottocategoria 1**: “Connetti e configura i singoli strumenti di rilevamento delle intrusioni in un sistema di rilevamento delle intrusioni a livello di sistema.”
- **Sottocategoria 3**: “Impiegare strumenti e meccanismi automatizzati per integrare strumenti e meccanismi di rilevamento delle intrusioni nei meccanismi di controllo degli accessi e di controllo del flusso.”

NIST SP 800-53A Rev. 5
Assessment dei controlli da effettuare dopo l’implementazione

SI-04(01)	SYSTEM MONITORING | SYSTEM-WIDE INTRUSION DETECTION SYSTEM	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	SI-04(01)[01]	individual intrusion detection tools are connected to a system-wide intrusion detection system;
	SI-04(01)[02]	individual intrusion detection tools are configured into a system-wide intrusion detection system.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	SI-04(01)-Examine	[SELECT FROM: System and information integrity policy; system and information integrity procedures; procedures addressing system monitoring tools and techniques; system design documentation; system monitoring tools and techniques documentation; system configuration settings and associated documentation; system audit records; system security plan; other relevant documents or records].
	SI-04(01)-Interview	[SELECT FROM: System/network administrators; organizational personnel with information security responsibilities; organizational personnel installing, configuring, and/or maintaining the system; organizational personnel responsible for monitoring the system; organizational personnel responsible for the intrusion detection system].
	SI-04(01)-Test	[SELECT FROM: Organizational processes for intrusion detection and system monitoring; mechanisms supporting and/or implementing intrusion detection capabilities].

SI-04(03)	SYSTEM MONITORING | AUTOMATED TOOL AND MECHANISM INTEGRATION	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	SI-04(03)[01]	automated tools and mechanisms are employed to integrate intrusion detection tools and mechanisms into access control mechanisms;
	SI-04(03)[02]	automated tools and mechanisms are employed to integrate intrusion detection tools and mechanisms into flow control mechanisms.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	SI-04(03)-Examine	[SELECT FROM: System and information integrity policy; system and information integrity procedures; access control policy and procedures; procedures addressing system monitoring tools and techniques; system design documentation; system monitoring tools and techniques documentation; system configuration settings and associated documentation; system audit records; system security plan; other relevant documents or records].
	SI-04(03)-Interview	[SELECT FROM: System/network administrators; organizational personnel with information security responsibilities; organizational personnel installing, configuring, and/or maintaining the system; organizational personnel responsible for monitoring the system; organizational personnel responsible for the intrusion detection system].
	SI-04(03)-Test	[SELECT FROM: Organizational processes for intrusion detection and system monitoring; mechanisms supporting and/or implementing the intrusion detection and system monitoring capability; mechanisms and tools supporting and/or implementing the access and flow control capabilities; mechanisms and tools supporting and/or implementing the integration of intrusion detection tools into the access and flow control mechanisms].

4. Controllo correttivo (Corrective)

- Controllo: Implementazione di un sistema di backup dei dati regolare e di procedure di ripristino.
- Come agisce sul rischio: Questo controllo riduce l'impatto se la minaccia riesce a sfruttare una vulnerabilità ripristinando rapidamente i dati e i servizi dell'applicazione web da un backup recente. In caso di violazione o perdita di dati, il ripristino rapido può limitare le conseguenze negative per l'azienda e i suoi clienti.

Identificativo NIST SP 800-53 Rev. 5 "**CP-9 SYSTEM BACHUP**".
Questo controllo stabilisce le linee guida per la protezione dei dati attraverso l'implementazione di procedure di backup regolari.

Identificativo NIST SP 800-53 Rev. 5 "**CP-10 SYSTEM RECOVERY AND RECONSTITUTION**".
Questo controllo stabilisce le linee guida per la pianificazione e l'implementazione di procedure di ripristino dei dati e dei servizi in caso di interruzione.

NIST SP 800-53A Rev. 5

Assessment dei controlli da effettuare dopo l'implementazione

CP-09	SYSTEM BACKUP	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	CP-09_ODP[01]	***system components for which to conduct backups of user-level information is defined;***
	CP-09_ODP[02]	***frequency at which to conduct backups of user-level information consistent with recovery time and recovery point objectives is defined;***
	CP-09_ODP[03]	***frequency at which to conduct backups of system-level information consistent with recovery time and recovery point objectives is defined;***
	CP-09_ODP[04]	***frequency at which to conduct backups of system documentation consistent with recovery time and recovery point objectives is defined;***
	CP-09a.	backups of user-level information contained in ***<CP-09_ODP[01] system components>*** are conducted ***<CP-09_ODP[02] frequency>***;
	CP-09b.	backups of system-level information contained in the system are conducted ***<CP-09_ODP[03] frequency>***;
	CP-09c.	backups of system documentation, including security- and privacy-related documentation are conducted ***<CP-09_ODP[04] frequency>***;
	CP-09d.[01]	the confidentiality of backup information is protected;
	CP-09d.[02]	the integrity of backup information is protected;
	CP-09d.[03]	the availability of backup information is protected.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	CP-09-Examine	[SELECT FROM: Contingency planning policy; procedures addressing system backup; contingency plan; backup storage location(s); system backup logs or records; system security plan; privacy plan; other relevant documents or records].
	CP-09-Interview	[SELECT FROM: Organizational personnel with system backup responsibilities; organizational personnel with information security and privacy responsibilities].
	CP-09-Test	[SELECT FROM: Organizational processes for conducting system backups; mechanisms supporting and/or implementing system backups].

CP-10	SYSTEM RECOVERY AND RECONSTITUTION	
	CP-10-Interview	[SELECT FROM: Organizational personnel with contingency planning, recovery, and/or reconstitution responsibilities; organizational personnel with information security responsibilities].
	CP-10-Test	[SELECT FROM: Organizational processes implementing system recovery and reconstitution operations; mechanisms supporting and/or implementing system recovery and reconstitution operations].

5. Controllo compensativo (Compensating)

- Controllo: Implementare un SIEM per l'analisi dei log.
- Come agisce sul rischio: Questo controllo riduce la probabilità che un threat agent avvii una minaccia aumentando la sicurezza, permettendo di rilevare delle minacce e rispondere prontamente agli incidenti di sicurezza. Inoltre questa implementazione permette di compensare (in parte) l'errore umano o la malafede di un dipendente.

Identificativo NIST SP 800-53 Rev. 5 "**SI-4 SYSTEM MONITORING**".
Questo controllo stabilisce le linee guida per il monitoraggio delle attività dei sistemi informativi al fine di rilevare, registrare e rispondere a eventi di sicurezza.

Identificativo NIST SP 800-53 Rev. 5 "**AU-3 CONTENT OF AUDIT RECORDS**".
Questo controllo si concentra sulla registrazione delle attività di sistema per garantire la tracciabilità e la responsabilità delle azioni degli utenti e dei processi all'interno dell'ambiente IT.
Anche se AU-3 non menziona direttamente l'implementazione di un SIEM, un tale sistema può essere un componente chiave per l'implementazione efficace del controllo.

NIST SP 800-53A Rev. 5
Assessment dei controlli da effettuare dopo l'implementazione

SI-04	SYSTEM MONITORING	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	SI-04_ODP[01]	***monitoring objectives to detect attacks and indicators of potential attacks on the system are defined;***
	SI-04_ODP[02]	***techniques and methods used to identify unauthorized use of the system are defined;***
	SI-04_ODP[03]	***system monitoring information to be provided to personnel or roles is defined;***
	SI-04_ODP[04]	***personnel or roles to whom system monitoring information is to be provided is/ are defined;***
	SI-04_ODP[05]	***one or more of the following PARAMETER VALUES is/are selected: {as needed; <SI-04_ODP[06] frequency>};***
	SI-04_ODP[06]	***a frequency for providing system monitoring to personnel or roles is defined (if selected);***
	SI-04a.01	the system is monitored to detect attacks and indicators of potential attacks in accordance with ***<SI-04_ODP[01] monitoring objectives>***;
	SI-04a.02[01]	the system is monitored to detect unauthorized local connections;
	SI-04a.02[02]	the system is monitored to detect unauthorized network connections;
	SI-04a.02[03]	the system is monitored to detect unauthorized remote connections;
	SI-04b.	unauthorized use of the system is identified through ***<SI-04_ODP[02] techniques and methods>***;
	SI-04c.01	internal monitoring capabilities are invoked or monitoring devices are deployed strategically within the system to collect organization-determined essential information;

	SI-04c.02	internal monitoring capabilities are invoked or monitoring devices are deployed at ad hoc locations within the system to track specific types of transactions of interest to the organization;
	SI-04d.[01]	detected events are analyzed;
	SI-04d.[02]	detected anomalies are analyzed;
	SI-04e.	the level of system monitoring activity is adjusted when there is a change in risk to organizational operations and assets, individuals, other organizations, or the Nation;
	SI-04f.	a legal opinion regarding system monitoring activities is obtained;
	SI-04g.	***<SI-04_ODP[03] system monitoring information>*** is provided to ***<SI-04_ODP[04] personnel or roles>*** ***<SI-04_ODP[05] SELECTED PARAMETER VALUE(S)>***.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	SI-04-Examine	[SELECT FROM: System and information integrity policy; system and information integrity procedures; procedures addressing system monitoring tools and techniques; continuous monitoring strategy; facility diagram/layout; system design documentation; system monitoring tools and techniques documentation; locations within the system where monitoring devices are deployed; system configuration settings and associated documentation; system security plan; other relevant documents or records].
	SI-04-Interview	[SELECT FROM: System/network administrators; organizational personnel with information security responsibilities; organizational personnel installing, configuring, and/or maintaining the system; organizational personnel responsible for monitoring the system].
	SI-04-Test	[SELECT FROM: Organizational processes for system monitoring; mechanisms supporting and/or implementing system monitoring capabilities].

AU-03	**CONTENT OF AUDIT RECORDS**	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	AU-03a.	audit records contain information that establishes what type of event occurred;
	AU-03b.	audit records contain information that establishes when the event occurred;
	AU-03c.	audit records contain information that establishes where the event occurred;
	AU-03d.	audit records contain information that establishes the source of the event;
	AU-03e.	audit records contain information that establishes the outcome of the event;
	AU-03f.	audit records contain information that establishes the identity of any individuals, subjects, or objects/entities associated with the event.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	AU-03-Examine	[SELECT FROM: Audit and accountability policy; system security plan; privacy plan; procedures addressing content of audit records; system design documentation; system configuration settings and associated documentation; list of organization-defined auditable events; system audit records; system incident reports; other relevant documents or records].
	AU-03-Interview	[SELECT FROM: Organizational personnel with audit and accountability responsibilities; organizational personnel with information security and privacy responsibilities; system/network administrators].
	AU-03-Test	[SELECT FROM: Mechanisms implementing system auditing of auditable events].