Università degli Studi di Salerno

Dipartimento di Informatica

Penetration Testing & Ethical Hacking

Tipi e Metodologie di Testing
Parte 1

Arcangelo Castiglione
arcastiglione@unisa.it

Outline

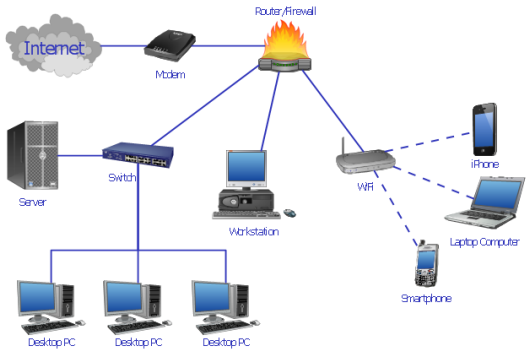
- Terminologia
- Tipologie di Test di Sicurezza
- Tipi di Penetration Testing
- Metodologie di Testing
- Framework Generale per il Penetration Testing (FGPT)
- Penetration Testing Report

Outline

- **Terminologia**
- Tipologie di Test di Sicurezza
- Tipi di Penetration Testing
- Metodologie di Testing
- Framework Generale per il Penetration Testing (FGPT)
- Penetration Testing Report

Terminologia

- **Asset**
  - Dato, dispositivo, insieme di dispositivi (sistema) o insieme di sistemi (*Organizzazione* o *Infrastruttura*) che supporta attività legate alle informazioni
  - Costituisce l'obiettivo da analizzare mediante il processo di valutazione della sicurezza
  - Dovrebbe essere protetto anche rispetto alle persone autorizzate ad accedervi



Terminologia

- **Vulnerabilità: difetto** o **debolezza** dell'asset che **potrebbe essere sfruttata** da un attaccante

- **Minaccia (o Threat): Vulnerabilità sfruttabile con successo**

- Lo sfruttamento di una vulnerabilità potrebbe causare
  - L'accesso non autorizzato all'asset
  - Il furto o la manipolazione dei dati dell'asset
  - L'elevazione dei privilegi (*permessi*) all'interno dell'asset
  - Il malfunzionamento dell'asset
  - Etc.

Terminologia

- **Rischio:**
  - Impatto negativo derivante dalla violazione di un asset
    - Danno, perdita di dati, interruzione del servizio, etc.
  - Il rischio si calcola considerando la probabilità che un attacco avvenga ed il suo potenziale impatto
    - Matrice dei Rischi (Maggiori dettagli in seguito…)

Terminologia

- **Exploit:**
  - *Definizione 1:* Software (codice) che sfrutta una vulnerabilità per causare un comportamento indesiderato o imprevisto in un sistema
    - Ad es., consentire l'accesso non autorizzato a dati o informazioni
  - *Definizione 2:* Strumento (*vettore*) che l'attaccante usa per l'invio di un **payload**
    - **Payload**: codice che se eseguito correttamente sulla **macchina target** permette l'accesso ad essa o **l'elevazione dei privilegi** all'interno di essa
      - **Macchina target**: host appartenente all'asset

Maggiori dettagli nelle prossime lezioni…

Terminologia

- **Un Payload può essere:**
  - Inviato e/o eseguito sulla macchina target tramite un **exploit**
    - **Remote Exploitation**
    - **Local Exploitation**
  - Inviato alla macchina target tramite tecniche di **Social Engineering** ed eseguito su di essa a seguito di azioni compiute dall'utente
    - **Client-Side Exploitation**

Maggiori dettagli nelle prossime lezioni…

Terminologia

- **Auditor** e **Penetration Tester (o Pentester):** professionisti che valutano l'efficacia delle soluzioni (tecniche e non) adottate per garantire la sicurezza di un determinato asset

Terminologia

- **Red Team** vs **Blue Team**
- Sia i **Red Team** che i **Blue Team** lavorano per migliorare la sicurezza di un asset, agendo però in modo diverso
  - Un **Red Team** interpreta il ruolo dell'aggressore, cercando di trovare e sfruttare le vulnerabilità che potrebbero violare la sicurezza di un asset
    - Lo scopo del **Red Team** è quello di testare e mettere alla prova, dal punto di vista di un attaccante, le misure di sicurezza esistenti
  - Un **Blue Team** si difende dagli attacchi e cerca di gestire gli incidenti di sicurezza quando essi si verificano
    - Lo scopo del **Blue Team** non è solo quello di difendersi dagli attacchi provenienti dal **Red Team**, ma anche di fronteggiare qualsiasi attività insolita o sospetta proveniente dal mondo esterno

Outline

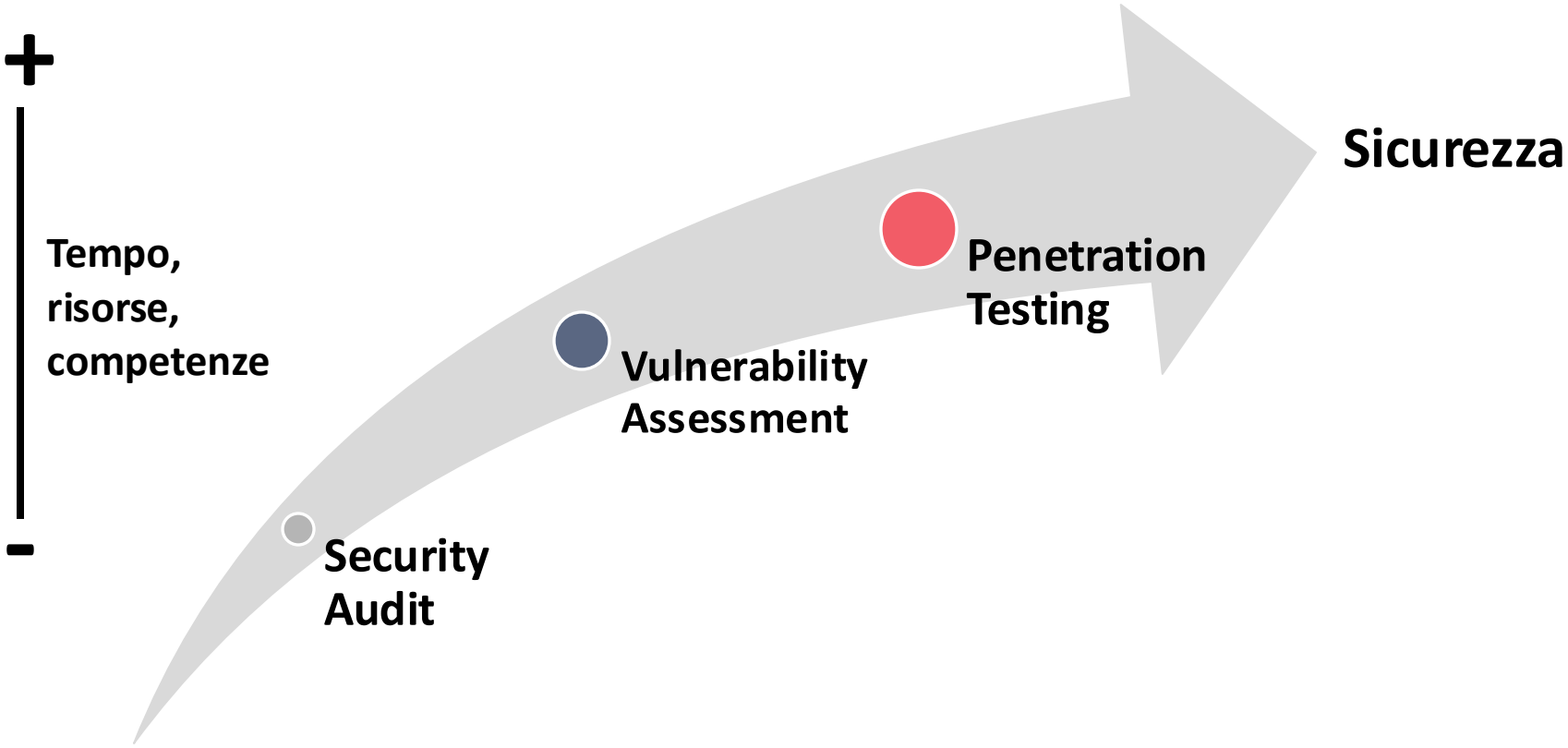
- Terminologia
- **Tipologie di Test di Sicurezza**
- Tipi di Penetration Testing
- Metodologie di Testing
- Framework Generale per il Penetration Testing (FGPT)
- Penetration Testing Report

Tipologie di Test di Sicurezza

- Ciascun test di sicurezza permette di rispondere ad una precisa domanda
  - **Security Audit:** l'asset sta attuando le opportune pratiche di sicurezza?
  - **Vulnerability Assessment:** quali sono le vulnerabilità dell'asset?
  - **Penetration Testing:** quali vulnerabilità dell'asset possono essere sfruttate dagli attaccanti (costituendo quindi una minaccia)?

Tipologie di Test di Sicurezza

Test di Sicurezza tipicamente condotti nell'ambito dell'Ethical Hacking



Tipologie di Test di Sicurezza

Security Audit

- Valuta la sicurezza di un asset rispetto ad un insieme di standard, politiche e procedure di sicurezza note a priori

- Utilizza tipicamente **checklist** di controlli noti a priori per garantire che l'asset sia conforme
  - Alle sue politiche di sicurezza
  - Alle normative ed alle sue responsabilità legali

- Esistono vari tipi di security audit
  - Diversi criteri per valutare la sicurezza di un asset

Tipologie di Test di Sicurezza
Security Audit

- Un tipico Security Audit valuta i seguenti aspetti di un asset
  - Controllo degli Accessi (smartcard, password, token, etc)
  - Configurazione E-mail
  - Configurazioni Hardware e Software
  - Processi di Gestione delle Informazioni
  - Configurazioni di Rete
  - Comportamenti ed Abitudini del Personale
  - Etc

Tipologie di Test di Sicurezza

Security Audit – Enti e Standard Coinvolti

- Vari enti ed organizzazioni hanno definito standard e framework per effettuare Security Audit
  - **ISO** (**I**nternational **O**rganization for **S**tandardization)
  - **IEC** (**I**nternational **E**lectrotechnical **C**ommission)
  - **NIST** (**N**ational **I**nstitute of **S**tandards and **T**echnology)
  - **HITRUST** (**H**ealth **I**nformation **TRUST**) Alliance
  - **CIS** (**C**enter for **I**nternet **S**ecurity)
  - Etc

Tipologie di Test di Sicurezza

Security Audit – ISO/IEC 27000-series

- Serie di standard di sicurezza applicabili nel settore pubblico e privato su base «volontaria»
- Utile quando un asset deve dimostrare le proprie capacità (*conformità*) di sicurezza tramite la certificazione ISO 27000
- I due principali standard della serie (ISO 27001 e 27002) stabiliscono i requisiti e le procedure per creare un **I**nformation **S**ecurity **M**anagement **S**ystem (**ISMS**)
  - **I**nformation **S**ecurity **M**anagement **S**ystem (**ISMS**): consente ad un'organizzazione di individuare le misure organizzative e tecnologiche per proteggere il proprio asset da possibili minacce

Tipologie di Test di Sicurezza

Security Audit – ISO/IEC 27000-series

- La conformità agli standard della serie ISO 27000 viene stabilita attraverso processi di audit e certificazione, generalmente forniti da enti terzi approvati dall'ISO e da altre agenzie accreditate
- La serie ISO 27000 comprende circa 60 standard che coprono vari aspetti relativi alla sicurezza delle informazioni
  - ISO/IEC 27000 — ***I**nformation **S**ecurity **M**anagement **S**ystems — Overview and vocabulary*
  - ISO/IEC 27003 — ***I**nformation **S**ecurity **M**anagement **S**ystem implementation guidance*
  - ISO/IEC 27005 — *Guidance on managing information security risks*
  - ISO/IEC 27006 — *Requirements for bodies providing audit and certification of **I**nformation **S**ecurity **M**anagement **S**ystems*
  - **ISO/IEC 27007** — *Guidelines for **I**nformation **S**ecurity **M**anagement **S**ystems auditing*
  - ISO/IEC TR 27008 — *Guidance for auditors on **ISMS** controls*
  - ……

Tipologie di Test di Sicurezza

Security Audit – ISO/IEC 27007

- Standard riguardante la sicurezza delle informazioni e la protezione della privacy, che fornisce linee guida su
  - Gestione dei programmi di audit (Pianificazione audit)
  - Conduzione delle attività di audit (Esecuzione audit)
  - Valutazione delle competenze degli auditor e/o dei gruppi di audit coinvolti nel processo di verifica

- Applicabile a qualsiasi asset che abbia l'esigenza di
  - Pianificare e condurre audit interni e/o esterni
  - Gestire un programma di audit

Tipologie di Test di Sicurezza

Security Audit – ISO/IEC 27007

- Definisce il modo in cui può essere eseguito un security audit sulla base di vari criteri, tra i quali
  - Politiche e requisiti specificati dalle principali parti interessate
  - Requisiti legali e regolamentari
  - Processi e controlli definiti dall'organizzazione che dovrà essere sottoposta a security audit o da altre parti interessate
  - Piani per la gestione dei rischi ed il raggiungimento degli obiettivi di sicurezza
  - Piani di progetto
  - Etc

Tipologie di Test di Sicurezza
Security Audit – ISO/IEC 27007

- Standard applicabile
  - A tutti i tipi di asset, indipendentemente dalle sue dimensioni
  - Agli audit di varia portata e scala, condotti
    - Da grandi team di audit, tipicamente in asset più grandi
    - Da singoli auditor, sia in asset grandi che piccoli

Tipologie di Test di Sicurezza

Security Audit – NIST Security Audit

- I controlli (*standard* e *best practice*) di sicurezza definiti dal **N**ational **I**nstitute of **S**tandards and **T**echnologies (**NIST**)
  - Svolgono un ruolo importante nella protezione dei sistemi informativi critici degli Stati Uniti (e non solo)
  - Possono essere utilizzati da agenzie governative, aziende private ed altri enti per proteggere i propri asset

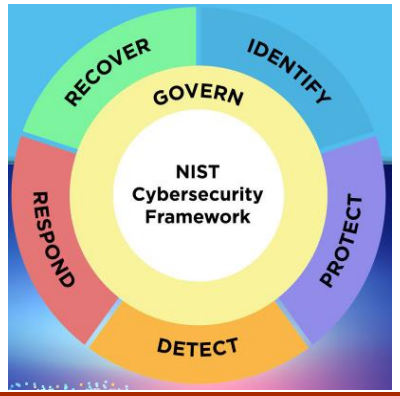
- Tra i principali controlli di sicurezza forniti dal NIST troviamo
  - NIST CyberSecurity Framework (NIST CSF)
  - NIST Special Publication (SP) 800-37 – Risk Management Framework
  - NIST Special Publication (SP) 800-53 – Security and Control Framework
  - NIST Special Publication (SP) 800-171 – Protecting Controlled Unclassified Information

NIST National Institute of Standards and Technology

Tipologie di Test di Sicurezza

Security Audit – NIST Cyber Security Framework (CSF)

- Il **NIST C**yber**S**ecurity **F**ramework (**NIST CSF**)
  - È un insieme di linee guida e *best practice* per migliorare la sicurezza delle informazioni e la gestione dei rischi per un determinato asset
  - Fornisce alle organizzazioni un modo pratico per valutare le proprie capacità di sicurezza
  - Aiuta a identificare
    - I rischi che potrebbero causare danni alle infrastrutture ed ai dati
    - I meccanismi di controllo da implementare per mitigare tali rischi



NIST National Institute of Standards and Technology

Tipologie di Test di Sicurezza

Security Audit – NIST Cyber Security Framework (CSF)

- Progettato per identificare e ridurre i rischi informatici nei settori delle cosiddette «infrastrutture critiche»
  - Compresi i settori non «coperti» da normative quali l'**H**ealth **I**nsurance **P**ortability and **A**ccountability **A**ct (**HIPAA**) ed il **P**ayment **C**ard **I**ndustry **D**ata **S**ecurity **S**tandard (**PCI DSS**)

- Può essere
  - Utilizzato come strumento volontario e collaborativo
  - Applicato a tutte le organizzazioni e settori

- Ultima versione del framework rilasciata il 26 febbraio 2024
  - https://www.nist.gov/cyberframework

NIST National Institute of Standards and Technology

Tipologie di Test di Sicurezza

Security Audit – NIST SP 800-37

- ***NIST SP 800-37 («Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy»)***
  - Definisce un processo *step-by-step* per la valutazione dei rischi e l'implementazione di contromisure per ridurre tali rischi ad un livello accettabile
  - Applicabile da qualsiasi organizzazione che voglia gestire i rischi di sicurezza del proprio asset
    - Indipendentemente dalle dimensioni, dal tipo o dalla complessità di tale asset
  - Utilizzato dal governo federale degli Stati Uniti per garantire la conformità rispetto alla gestione dei rischi
- https://csrc.nist.gov/pubs/sp/800/37/r2/final

NIST National Institute of Standards and Technology

Tipologie di Test di Sicurezza

Security Audit – NIST SP 800-53

- ***NIST SP 800-53 («Security and Privacy Controls for Information Systems and Organizations»)***
  - Insieme di controlli di sicurezza utilizzati per valutare l'efficacia dei meccanismi di protezione in termini di *Confidenzialità*, *Integrità* e *Disponibilità* (**Triade *CIA*** – ***C****onfidentiality*, ***I****ntegrity*, ***A****vailability*)
  - Può essere utilizzato come modello per implementare controlli di sicurezza ad hoc
  - Basato su una checklist rispetto alla quale «misurare» il livello di sicurezza di un determinato asset
  - Consente di effettuare, in maniera flessibile e adattiva, sia attività di monitoraggio periodico che controlli di sicurezza su richiesta
- https://csrc.nist.gov/pubs/sp/800/53/r5/upd1/final

NIST National Institute of Standards and Technology

Tipologie di Test di Sicurezza

Security Audit – NIST SP 800-171

- **NIST SP 800-171 («*Protecting Controlled Unclassified Information (CUI) in Nonfederal Information Systems and Organizations*")**
  - Le **CUI** possono essere sia digitali che fisiche, vengono create da un ente pubblico (o da un'entità per suo conto) e, pur non essendo classificate, richiedono comunque protezione
- Il NIST SP 800-171 fornisce linee guida e controlli su come si devono gestire (accedere, trasmettere ed archiviare) in modo sicuro le **CUI**
- I controlli inclusi nello standard NIST SP 800-171 sono direttamente correlati al NIST SP 800-53, ma sono meno dettagliati e più generalizzati
- È possibile mettere in relazione i due standard se un asset deve dimostrare la conformità con NIST SP 800-53, utilizzando NIST SP 800-171 come base
  - Ciò crea flessibilità per le organizzazioni più piccole: possono dimostrare la conformità man mano che crescono, utilizzando i controlli aggiuntivi inclusi nel NIST SP 800-53
- https://csrc.nist.gov/pubs/sp/800/171/r2/upd1/final

NIST National Institute of Standards and Technology

Tipologie di Test di Sicurezza

Security Audit – NIST SP 800-171 – Google Cloud Plat.

Servizi Google Cloud coperti dalla valutazione di terze parti per NIST 800-171

Comprimi tutto

Google Cloud Platform

- Gestore contesto accesso
- Access Transparency
- Console di amministrazione (incluso SDK Admin, Directory Sync)
- AI Platform Notebooks
- Cloud Run (completamente gestito)
- Cloud SDK
- Cloud Shell
- Cloud Source Repositories
- Cloud Spanner

https://cloud.google.com/security/compliance/nist800-171?hl=it

NIST National Institute of Standards and Technology

Tipologie di Test di Sicurezza

Security Audit – NIST SP 800-171 – Microsoft

Microsoft e NIST SP 800-171 (Azure, Dynamics 365, Intune, Office 365)

Organizzazioni di valutazione di terze parti accreditate, Kratos Secureinfo e Coalfire, hanno collaborato con Microsoft pe attestare che i servizi cloud nell'ambito soddisfano i criteri in NIST SP 800-171, *Protezione delle informazioni non classificate controllate (CUI) in Sistemi informativi non federati e organizzazioni*, quando elaborano CUI. L'implementazione Microsoft dei requisiti FedRAMP garantisce che i servizi cloud microsoft nell'ambito soddisfino o superino i requisiti di NIST SP 800-171 usando i sistemi e le procedure già in uso.

I requisiti NIST SP 800-171 sono un subset di NIST SP 800-53, lo standard usato da FedRAMP. L'appendice D di NIST SP 800-171 fornisce un mapping diretto dei propri requisiti di sicurezza CUI ai controlli di sicurezza pertinenti in NIST SP 800-53, per i quali i servizi cloud nell'ambito sono già stati valutati e autorizzati nell'ambito del programma FedRAMP.

Qualsiasi entità che elabora o archivia il governo degli Stati Uniti CUI — istituti di ricerca, società di consulenza, appaltatori di produzione, deve rispettare i rigorosi requisiti di NIST SP 800-171. Questa attestazione significa che i servizi cloud microsoft nell'ambito possono soddisfare i clienti che desiderano distribuire carichi di lavoro CUI con la certezza che Microsoft sia pienamente conforme. Ad esempio, tutti gli appaltatori DoD che elaborano, archiviano o trasmettono "informazioni di difesa coperte" usando servizi cloud Microsoft nell'ambito nei propri sistemi informativi soddisfano le clausole DFARS del Dipartimento della difesa degli Stati Uniti che richiedono la conformità ai requisiti di sicurezza di NIST SP 800-171.

https://learn.microsoft.com/it-it/compliance/regulatory/offering-nist-sp-800-171

NIST National Institute of Standards and Technology

Tipologie di Test di Sicurezza

Security Audit – NIST SP 800-171 – DoD Assessment

- Gli appaltatori governativi sono un bersaglio frequente di attacchi informatici a causa della loro «vicinanza» ai sistemi informativi del governo

- Lo standard NIST SP 800-171 è utilizzato dal *Dipartimento della Difes*a (*DoD*) degli Stati Uniti per valutare la conformità, in termini di sicurezza, dei suoi appaltatori
  - ***NIST SP 800-171 DoD Assessment Methodology***

- Chiunque deve attenersi allo standard NIST SP 800-171 per poter partecipare, a livello governativo, a gare di appalto, contratti, etc

NIST National Institute of Standards and Technology

Tipologie di Test di Sicurezza

Security Audit – NIST SP 800-171 – Esempio

- ***NIST SP 800-171 DoD Assessment Methodology***: Checklist, basata su linee guida fornite dal NIST al ***D****epartment* ***o****f* ***D****efense* (***DoD***) degli Stati Uniti, per controllare le politiche di sicurezza di determinati «asset» (i.e., appaltatori)

- Permette di valutare la sicurezza dell'asset analizzando 14 *macroaree di rischio* (***Security Family***), ciascuna tramite un insieme di domande

1. *Access Control*
2. *Awareness and Training*
3. *Audit and Accountability*
4. *Configuration Management*
5. *Identification and Authentication*
6. *Incident Response*
7. *Maintenance*
8. *Media Protection*
9. *Personnel Security*
10. *Physical Protection*
11. *Risk Assessment*
12. *Security Assessment*
13. *Systems and Communications Protection*
14. *Systems and Information Integrity*

NIST National Institute of Standards and Technology

Tipologie di Test di Sicurezza

Security Audit – NIST SP 800-171 – Esempio

- Permette di valutare la sicurezza dell'asset analizzando 14 *macroaree di rischio* (***Security Family***), ciascuna tramite un insieme di domande

Security Family	Subject	No. of questions to answer
3,1	Access Control	22
3,2	Awareness and Training	3
3,3	Audit and Accountability	9
3,4	Configuration Management	9
3,5	Identification and Authentication	11
3,6	Incident Response	3
3,7	Maintenance	6
3,8	Media Protection	9
3,9	Personnel Security	2
3,10	Physical Protection	6
3,11	Risk Assessment	3
3,12	Security Assessment	4
3,13	Systems and Communications Protection	16
3,14	Systems and Information Integrity	7

NIST National Institute of Standards and Technology

Tipologie di Test di Sicurezza

Security Audit – NIST SP 800-171 – Esempio

- Permette di valutare la sicurezza dell'asset analizzando 14 *macroaree di rischio* (***Security Family***), ciascuna tramite un insieme di domande

Security Family	Subject	No. of questions to answer
3,1	Access Control	22
3,2	Awareness and Training	3
3,3	Audit and Accountability	9
3,4	Configuration Management	9
3,5	Identification and Authentication	11
3,6	Incident Response	3
3,7	Maintenance	6
3,8	Media Protection	9
3,9	Personnel Security	2
3,10	Physical Protection	6
3,11	Risk Assessment	3
3,12	Security Assessment	4
3,13	Systems and Communications Protection	16
3,14	Systems and Information Integrity	7

Security Family: Access Control

NIST National Institute of Standards and Technology

Tipologie di Test di Sicurezza

Security Audit – NIST SP 800-171 – Esempio

- Ad es., **Security Family «Access Control»** è valutata mediante **22 domande**

3,1	Access Control	Answer
3.1.1	Limit system access to authorized users, processes acting on behalf of authorized users, and devices (including other systems).	
3.1.2	Limit system access to the types of transactions and functions that authorized users are permitted to execute.	
3.1.3	Control the flow of CUI in accordance with approved authorizations.	
3.1.4	Separate the duties of individuals to reduce the risk of malevolent activity without collusion.	
3.1.5	Employ the principle of least privilege, including for specific security functions and privileged accounts.	
3.1.6	Use non-privileged accounts or roles when accessing nonsecurity functions.	
3.1.7	Prevent non-privileged users from executing privileged functions and capture the execution of such functions in audit logs.	
3.1.8	Limit unsuccessful logon attempts.	
3.1.9	Provide privacy and security notices consistent with applicable CUI rules.	
3.1.10	Use session lock with pattern-hiding displays to prevent access and viewing of data after a period of inactivity.	
3.1.11	Terminate (automatically) a user session after a defined condition.	
3.1.12	Monitor and control remote access sessions.	
3.1.13	Employ cryptographic mechanisms to protect the confidentiality of remote access sessions.	
3.1.14	Route remote access via managed access control points.	
3.1.15	Authorize remote execution of privileged commands and remote access to security-relevant information.	
3.1.16	Authorize wireless access prior to allowing such connections.	
3.1.17	Protect wireless access using authentication and encryption.	
3.1.18	Control connection of mobile devices.	
3.1.19	Encrypt CUI on mobile devices and mobile computing platforms.	
3.1.20	Verify and control/limit connections to and use of external systems.	
3.1.21	Limit use of portable storage devices on external systems.	
3.1.22	Control CUI posted or processed on publicly accessible systems.	

NIST National Institute of Standards and Technology

Tipologie di Test di Sicurezza

Security Audit – NIST SP 800-171 – Esempio

Security Family	Subject	Question Not Answered
3,1	Access Control	22
3,2	Awareness and Training	3
3,3	Audit and Accountability	9
3,4	Configuration Management	9
3,5	Identification and Authentication	11
3,6	Incident Response	3
3,7	Maintenance	6
3,8	Media Protection	9
3,9	Personnel Security	2
3,10	Physical Protection	6
3,11	Risk Assessment	3
3,12	Security Assessment	4
3,13	Systems and Communications Protection	16
3,14	Systems and Information Integrity	7

All'inizio della valutazione, nessuna domanda presente nel NIST SP 800-171 DoD risulta risposta

NIST National Institute of Standards and Technology

Tipologie di Test di Sicurezza

Security Audit – NIST SP 800-171 – Esempio

- La NIST SP 800-171 DoD checklist consente di effettuare una ***Gap Analysis***: **confrontare lo stato attuale di sicurezza di un determinato asset rispetto a specifici requisiti di conformità**

- La checklist assegna un punteggio alla risposta di ciascuna domanda e fornisce un punteggio finale complessivo di sicurezza (relativo a tutte le domande): ***Supplier Performance Risk System (SPRS) Score***
  - Il punteggio più alto che si potrà ottenere (**sicurezza massima**) è **110**
    - Detto «**punteggio base**»
  - Per ciascun controllo di sicurezza non implementato o non applicabile verranno sottratti dei punti da questo punteggio base
  - È possibile avere un ***SPRS Score*** negativo, il cui valore più basso è **-178** (**sicurezza minima**)

NIST National Institute of Standards and Technology

Tipologie di Test di Sicurezza

Security Audit – NIST SP 800-171 – Esempio

- La checklist assegna un punteggio alla risposta di ciascuna domanda e fornisce un punteggio finale complessivo di sicurezza (relativo a tutte le domande): ***Supplier Performance Risk System (SPRS) Score***

Security Family	Subject	Score
3,1	Access Control	-29
3,2	Awareness and Training	-11
3,3	Audit and Accountability	-19
3,4	Configuration Management	-33
3,5	Identification and Authentication	-27
3,6	Incident Response	-11
3,7	Maintenance	-18
3,8	Media Protection	-23
3,9	Personnel Security	-8
3,10	Physical Protection	-14
3,11	Risk Assessment	-9
3,12	Security Assessment	-13
3,13	Systems and Communications Protection	-42
3,14	Systems and Information Integrity	-31
	*SPRS Score	-178

In questo esempio è stato ottenuto un *SPRS Score* di -178 poiché nessun controllo di sicurezza è stato implementato

NIST National Institute of Standards and Technology

Tipologie di Test di Sicurezza

Security Audit – NIST SP 800-171 – Esempio

- Il calcolo del ***SPRS Score*** si basa sui controlli di sicurezza verificati da ciascuna domanda
  - Se il controllo di sicurezza è «**Implementato**», il punteggio assegnato alla domanda (sottratto dal punteggio base) è 0
  - Se il controllo di sicurezza è «**Pianificato per essere implementato**», il valore sottratto dal punteggio base dipenderà dal valore associato alla domanda
    - Ad esempio, se la domanda ha valore 5, il punteggio sarà -5 se il controllo verificato da tale domanda è «**Pianificato per essere implementato**»
  - Se il controllo di sicurezza è «**Non applicabile**», il valore sottratto dal punteggio base dipenderà dal *NIST SP 800-171 DoD Assessment Methodology*, salvo diversa indicazione

Tipologie di Test di Sicurezza

Security Audit – NIST SP 800-171 – Esempio

3,1	Access Control	Answer
3.1.1	Limit system access to authorized users, processes acting on behalf of authorized users, and devices (including other systems).	
3.1.2	Limit system access to the types of transactions and functions that authorized users are permitted to execute.	Implemented Planned to be implemented Not Applicable
3.1.3	Control the flow of CUI in accordance with approved authorizations.	
3.1.4	Separate the duties of individuals to reduce the risk of malevolent activity without collusion.	
3.1.5	Employ the principle of least privilege, including for specific security functions and privileged accounts.	
3.1.6	Use non-privileged accounts or roles when accessing nonsecurity functions.	

Ciascuna domanda può avere una tra queste risposte («Implemented», «Planned to be implemented», «Not Applicable») ed a ciascuna risposta è associato un punteggio, da sottrarre a quello di base

NIST National Institute of Standards and Technology

Tipologie di Test di Sicurezza

Security Audit – NIST Security Audit

- Vantaggi derivanti dall'esecuzione di un NIST security audit
  - Protezione dell'asset
  - Risparmiare sugli eventuali costi derivanti dalla violazione dell'asset
  - Vantaggi sul mercato, grazie ad una migliore ed ampiamente riconosciuta reputazione e fiducia da parte dei clienti
  - Possibilità di partecipare a progetti o contratti governativi
  - Etc.

NIST National Institute of Standards and Technology

Tipologie di Test di Sicurezza

HITRUST Common Security Framework (CSF)

- Framework certificabile, che definisce
  - Approccio completo, flessibile ed efficiente per il controllo della conformità rispetto a normative e standard per la gestione dei rischi
  - Struttura, linee guida, best practice e riferimenti a fonti autorevoli, per il controllo della conformità dal punto di vista della protezione dei dati

- Basato anche su normative, standard e framework definite da altri enti, tra cui, ISO, NIST, HIPAA, GDPR, etc

- Incorpora continuamente nuovi contenuti, man mano che essi diventano disponibili e sono «accettati» tramite processi di revisione

https://hitrustalliance.net/product-tool/hitrust-csf/

HITRUST

Tipologie di Test di Sicurezza
HITRUST Common Security Framework (CSF)

- L'**HITRUST C**ommon **S**ecurity **F**ramework (**CSF**)
  - Include, armonizza e mette in relazione standard, normative e requisiti riconosciuti globalmente, tra cui ISO, GDPR, NIST, etc
  - Adatta i controlli in base al tipo, alle dimensioni ed alla complessità dell'asset
  - Segue un approccio basato sul rischio, che offre più livelli di implementazione, determinati da specifiche soglie di rischio
  - Si evolve in base alle esigenze dell'asset ed alle mutevoli condizioni degli standard e dell'ambiente di conformità normativa
  - Fornisce un approccio unificato per la gestione della conformità rispetto alla protezione dei dati e sfrutta strumenti basati sull'intelligenza artificiale per mantenersi aggiornato

HITRUST

Tipologie di Test di Sicurezza
HITRUST Common Security Framework (CSF)

- L'**HITRUST CSF** utilizza **13 Categorie di Controllo**
  1. *Access Control*
  2. *Human Resources Security*
  3. *Risk Management*
  4. *Security Policy*
  5. *Organization of Information Security*
  6. *Compliance*
  7. *Asset Management*
  8. *Physical and Environmental Security*
  9. *Communications and Operations Management*
  10. *Information Systems Acquisition, Development, and Maintenance*
  11. *Information Security Incident Management*
  12. *Business Continuity Management*
  13. *Privacy Practices*

HITRUST

Tipologie di Test di Sicurezza

CIS (Center for Internet Security) Controls

- I **CIS Critical Security Controls** (**CIS Controls**) sono un insieme di controlli che possono essere utilizzati per migliorare la gestione della sicurezza di un asset

- I **CIS Critical Security Controls**
  - Sono stati definiti a partire dall'identificazione dei cyber-attacchi più comuni e critici che avvengono nel mondo reale a danno degli asset

https://www.cisecurity.org/controls

CIS Center for Internet Security® Creating Confidence in the Connected World.

Tipologie di Test di Sicurezza
CIS (Center for Internet Security) Controls

- I **CIS Critical Security Controls** (**CIS Controls**) sono 18
  1. *Inventario e Controllo delle Risorse Aziendali*
  2. *Inventario e Controllo delle Risorse Software*
  3. *Protezione Dati*
  4. *Configurazione Sicura di Risorse e Software Aziendali*
  5. *Gestione Account*
  6. *Gestione del Controllo degli Accessi*
  7. *Gestione Continua delle Vulnerabilità*
  8. *Gestione dei Log di Controllo*
  9. *Protezione E-mail e Web Browser*

CIS Center for Internet Security® Creating Confidence in the Connected World.

Tipologie di Test di Sicurezza
CIS (Center for Internet Security) Controls

- I **CIS Critical Security Controls** (**CIS Controls**) sono 18
  10. *Difese Anti Malware*
  11. *Recupero Dati*
  12. *Gestione dell'Infrastruttura di Rete*
  13. *Monitoraggio e Difesa della Rete*
  14. *Formazione su Competenze e Consapevolezza della Sicurezza*
  15. *Gestione dei Service Provider*
  16. *Sicurezza del Software Applicativo*
  17. *Gestione dell'Incident Response*
  18. *Penetration Testing*

CIS Center for Internet Security®
Creating Confidence in the Connected World.

Tipologie di Test di Sicurezza
CIS (Center for Internet Security) Controls

1. *Inventario e Controllo delle Risorse Aziendali*
   - Gestire attivamente (inventariare, monitorare e correggere) tutte le risorse aziendali (ad es., dispositivi degli utenti, inclusi portatili e mobili; dispositivi di rete; dispositivi IoT e Server) collegate all'asset fisicamente, virtualmente, in remoto e tramite Cloud, così da conoscere con precisione tutte le risorse che devono essere monitorate e protette dall'azienda
   - Ciò supporterà anche l'identificazione delle risorse non autorizzate e non (o mal) gestite, che devono essere rimosse o corrette

CIS Center for Internet Security® Creating Confidence in the Connected World.

Tipologie di Test di Sicurezza

CIS (Center for Internet Security) Controls

1. *Inventario e Controllo delle Risorse Aziendali*

NUMBER	TITLE/DESCRIPTION	ASSET TYPE	SECURITY FUNCTION	IG1	IG2	IG3
1.1	**Establish and Maintain Detailed Enterprise Asset Inventory** Establish and maintain an accurate, detailed, and up-to-date inventory of all enterprise assets with the potential to store or process data, to include: end-user devices (including portable and mobile), network devices, non-computing/IoT devices, and servers. Ensure the inventory records the network address (if static), hardware address, machine name, enterprise asset owner, department for each asset, and whether the asset has been approved to connect to the network. For mobile end-user devices, MDM type tools can support this process, where appropriate. This inventory includes assets connected to the infrastructure physically, virtually, remotely, and those within cloud environments. Additionally, it includes assets that are regularly connected to the enterprise's network infrastructure, even if they are not under control of the enterprise. Review and update the inventory of all enterprise assets bi-annually, or more frequently.	Devices	Identify	●	●	●
1.2	**Address Unauthorized Assets** Ensure that a process exists to address unauthorized assets on a weekly basis. The enterprise may choose to remove the asset from the network, deny the asset from connecting remotely to the network, or quarantine the asset.	Devices	Respond	●	●	●
1.3	**Utilize an Active Discovery Tool** Utilize an active discovery tool to identify assets connected to the enterprise's network. Configure the active discovery tool to execute daily, or more frequently.	Devices	Detect		●	●
1.4	**Use Dynamic Host Configuration Protocol (DHCP) Logging to Update Enterprise Asset Inventory** Use DHCP logging on all DHCP servers or Internet Protocol (IP) address management tools to update the enterprise's asset inventory. Review and use logs to update the enterprise's asset inventory weekly, or more frequently.	Devices	Identify		●	●
1.5	**Use a Passive Asset Discovery Tool** Use a passive discovery tool to identify assets connected to the enterprise's network. Review and use scans to update the enterprise's asset inventory at least weekly, or more frequently.	Devices	Detect			●

CIS Center for Internet Security®
Creating Confidence in the Connected World.

Tipologie di Test di Sicurezza
CIS (Center for Internet Security) Controls

2. *Inventario e Controllo delle Risorse Software*
   - Gestire attivamente (inventariare e correggere) tutto il software (sistemi operativi ed applicazioni) utilizzato dall'azienda, così che solo quello autorizzato venga installato ed eseguito, mentre quello non autorizzato venga individuato e ne venga impedita l'installazione o l'esecuzione

Tipologie di Test di Sicurezza

CIS (Center for Internet Security) Controls

2. *Inventario e Controllo delle Risorse Software*

NUMBER	TITLE/DESCRIPTION	ASSET TYPE	SECURITY FUNCTION	IG1	IG2	IG3
2.1	**Establish and Maintain a Software Inventory** Establish and maintain a detailed inventory of all licensed software installed on enterprise assets. The software inventory must document the title, publisher, initial install/use date, and business purpose for each entry; where appropriate, include the Uniform Resource Locator (URL), app store(s), version(s), deployment mechanism, and decommission date. Review and update the software inventory bi-annually, or more frequently.	Applications	Identify	●	●	●
2.2	**Ensure Authorized Software is Currently Supported** Ensure that only currently supported software is designated as authorized in the software inventory for enterprise assets. If software is unsupported, yet necessary for the fulfillment of the enterprise's mission, document an exception detailing mitigating controls and residual risk acceptance. For any unsupported software without an exception documentation, designate as unauthorized. Review the software list to verify software support at least monthly, or more frequently.	Applications	Identify	●	●	●
2.3	**Address Unauthorized Software** Ensure that unauthorized software is either removed from use on enterprise assets or receives a documented exception. Review monthly, or more frequently.	Applications	Respond	●	●	●
2.4	**Utilize Automated Software Inventory Tools** Utilize software inventory tools, when possible, throughout the enterprise to automate the discovery and documentation of installed software.	Applications	Detect		●	●
2.5	**Allowlist Authorized Software** Use technical controls, such as application allowlisting, to ensure that only authorized software can execute or be accessed. Reassess bi-annually, or more frequently.	Applications	Protect		●	●
2.6	**Allowlist Authorized Libraries** Use technical controls to ensure that only authorized software libraries, such as specific .dll, .ocx, .so, etc., files are allowed to load into a system process. Block unauthorized libraries from loading into a system process. Reassess bi-annually, or more frequently.	Applications	Protect		●	●
2.7	**Allowlist Authorized Scripts** Use technical controls, such as digital signatures and version control, to ensure that only authorized scripts, such as specific .ps1, .py, etc., files are allowed to execute. Block unauthorized scripts from executing. Reassess bi-annually, or more frequently.	Applications	Protect			●

CIS Center for Internet Security®
Creating Confidence in the Connected World.

Tipologie di Test di Sicurezza
CIS (Center for Internet Security) Controls

3. *Protezione Dati*
   - Sviluppare processi e controlli tecnici per identificare, classificare, gestire, conservare ed eliminare in modo sicuro i dati

Tipologie di Test di Sicurezza

CIS (Center for Internet Security) Controls

3. *Protezione Dati*

NUMBER	TITLE/DESCRIPTION	ASSET TYPE	SECURITY FUNCTION	IG1	IG2	IG3
3.1	**Establish and Maintain a Data Management Process** Establish and maintain a data management process. In the process, address data sensitivity, data owner, handling of data, data retention limits, and disposal requirements, based on sensitivity and retention standards for the enterprise. Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	Data	Identify	●	●	●
3.2	**Establish and Maintain a Data Inventory** Establish and maintain a data inventory, based on the enterprise's data management process. Inventory sensitive data, at a minimum. Review and update inventory annually, at a minimum, with a priority on sensitive data.	Data	Identify	●	●	●
3.3	**Configure Data Access Control Lists** Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.	Data	Protect	●	●	●
3.4	**Enforce Data Retention** Retain data according to the enterprise's data management process. Data retention must include both minimum and maximum timelines.	Data	Protect	●	●	●

CIS Center for Internet Security®
Creating Confidence in the Connected World.

Tipologie di Test di Sicurezza

CIS (Center for Internet Security) Controls

3. *Protezione Dati*

NUMBER	TITLE/DESCRIPTION	ASSET TYPE	SECURITY FUNCTION	IG1	IG2	IG3
3.5	**Securely Dispose of Data** Securely dispose of data as outlined in the enterprise's data management process. Ensure the disposal process and method are commensurate with the data sensitivity.	Data	Protect	●	●	●
3.6	**Encrypt Data on End-User Devices** Encrypt data on end-user devices containing sensitive data. Example implementations can include: Windows BitLocker®, Apple FileVault®, Linux® dm-crypt.	Devices	Protect	●	●	●
3.7	**Establish and Maintain a Data Classification Scheme** Establish and maintain an overall data classification scheme for the enterprise. Enterprises may use labels, such as "Sensitive," "Confidential," and "Public," and classify their data according to those labels. Review and update the classification scheme annually, or when significant enterprise changes occur that could impact this Safeguard.	Data	Identify		●	●
3.8	**Document Data Flows** Document data flows. Data flow documentation includes service provider data flows and should be based on the enterprise's data management process. Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	Data	Identify		●	●
3.9	**Encrypt Data on Removable Media** Encrypt data on removable media.	Data	Protect		●	●
3.10	**Encrypt Sensitive Data in Transit** Encrypt sensitive data in transit. Example implementations can include: Transport Layer Security (TLS) and Open Secure Shell (OpenSSH).	Data	Protect		●	●
3.11	**Encrypt Sensitive Data at Rest** Encrypt sensitive data at rest on servers, applications, and databases containing sensitive data. Storage-layer encryption, also known as server-side encryption, meets the minimum requirement of this Safeguard. Additional encryption methods may include application-layer encryption, also known as client-side encryption, where access to the data storage device(s) does not permit access to the plain-text data.	Data	Protect		●	●
3.12	**Segment Data Processing and Storage Based on Sensitivity** Segment data processing and storage based on the sensitivity of the data. Do not process sensitive data on enterprise assets intended for lower sensitivity data.	Network	Protect		●	●
3.13	**Deploy a Data Loss Prevention Solution** Implement an automated tool, such as a host-based Data Loss Prevention (DLP) tool to identify all sensitive data stored, processed, or transmitted through enterprise assets, including those located onsite or at a remote service provider, and update the enterprise's sensitive data inventory.	Data	Protect			●
3.14	**Log Sensitive Data Access** Log sensitive data access, including modification and disposal.	Data	Detect			●

CIS Center for Internet Security®
Creating Confidence in the Connected World.

Tipologie di Test di Sicurezza
CIS (Center for Internet Security) Controls

4. *Configurazione Sicura di Risorse e Software Aziendali*
   - Stabilire e mantenere la configurazione sicura delle risorse (dispositivi degli utenti, inclusi portatili e mobili; dispositivi di rete; dispositivi IoT e Server) e dei software (sistemi operativi ed applicazioni) aziendali

Tipologie di Test di Sicurezza

CIS (Center for Internet Security) Controls

4. *Configurazione Sicura di Risorse e Software Aziendali*

NUMBER	TITLE/DESCRIPTION	ASSET TYPE	SECURITY FUNCTION	IG1	IG2	IG3
4.1	**Establish and Maintain a Secure Configuration Process** Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile; non-computing/IoT devices; and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	Applications	Protect	●	●	●
4.2	**Establish and Maintain a Secure Configuration Process for Network Infrastructure** Establish and maintain a secure configuration process for network devices. Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	Network	Protect	●	●	●
4.3	**Configure Automatic Session Locking on Enterprise Assets** Configure automatic session locking on enterprise assets after a defined period of inactivity. For general purpose operating systems, the period must not exceed 15 minutes. For mobile end-user devices, the period must not exceed 2 minutes.	Users	Protect	●	●	●
4.4	**Implement and Manage a Firewall on Servers** Implement and manage a firewall on servers, where supported. Example implementations include a virtual firewall, operating system firewall, or a third-party firewall agent.	Devices	Protect	●	●	●
4.5	**Implement and Manage a Firewall on End-User Devices** Implement and manage a host-based firewall or port-filtering tool on end-user devices, with a default-deny rule that drops all traffic except those services and ports that are explicitly allowed.	Devices	Protect	●	●	●
4.6	**Securely Manage Enterprise Assets and Software** Securely manage enterprise assets and software. Example implementations include managing configuration through version-controlled-infrastructure-as-code and accessing administrative interfaces over secure network protocols, such as Secure Shell (SSH) and Hypertext Transfer Protocol Secure (HTTPS). Do not use insecure management protocols, such as Telnet (Teletype Network) and HTTP, unless operationally essential.	Network	Protect	●	●	●

CIS Center for Internet Security®
Creating Confidence in the Connected World.

Tipologie di Test di Sicurezza

CIS (Center for Internet Security) Controls

4. *Configurazione Sicura di Risorse e Software Aziendali*

4.7	**Manage Default Accounts on Enterprise Assets and Software** Manage default accounts on enterprise assets and software, such as root, administrator, and other pre-configured vendor accounts. Example implementations can include: disabling default accounts or making them unusable.	Users	Protect	●	●	●
4.8	**Uninstall or Disable Unnecessary Services on Enterprise Assets and Software** Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.	Devices	Protect		●	●
4.9	**Configure Trusted DNS Servers on Enterprise Assets** Configure trusted DNS servers on enterprise assets. Example implementations include: configuring assets to use enterprise-controlled DNS servers and/or reputable externally accessible DNS servers.	Devices	Protect		●	●
4.10	**Enforce Automatic Device Lockout on Portable End-User Devices** Enforce automatic device lockout following a predetermined threshold of local failed authentication attempts on portable end-user devices, where supported. For laptops, do not allow more than 20 failed authentication attempts; for tablets and smartphones, no more than 10 failed authentication attempts. Example implementations include Microsoft® InTune Device Lock and Apple® Configuration Profile maxFailedAttempts.	Devices	Respond		●	●
4.11	**Enforce Remote Wipe Capability on Portable End-User Devices** Remotely wipe enterprise data from enterprise-owned portable end-user devices when deemed appropriate such as lost or stolen devices, or when an individual no longer supports the enterprise.	Devices	Protect		●	●
4.12	**Separate Enterprise Workspaces on Mobile End-User Devices** Ensure separate enterprise workspaces are used on mobile end-user devices, where supported. Example implementations include using an Apple® Configuration Profile or Android™ Work Profile to separate enterprise applications and data from personal applications and data.	Devices	Protect			●

CIS Center for Internet Security®
Creating Confidence in the Connected World.

Tipologie di Test di Sicurezza
CIS (Center for Internet Security) Controls

5. *Gestione Account*
   - Utilizzare processi e strumenti per la gestione dell'accounting degli utenti, sia dal punto di vista dell'autenticazione che dell'autorizzazione
     - Inclusi gli account amministratore, e gli account di servizio per risorse aziendali e software

Tipologie di Test di Sicurezza

CIS (Center for Internet Security) Controls

5. *Gestione Account*

NUMBER	TITLE/DESCRIPTION	ASSET TYPE	SECURITY FUNCTION	IG1	IG2	IG3
5.1	**Establish and Maintain an Inventory of Accounts** Establish and maintain an inventory of all accounts managed in the enterprise. The inventory must include both user and administrator accounts. The inventory, at a minimum, should contain the person's name, username, start/stop dates, and department. Validate that all active accounts are authorized, on a recurring schedule at a minimum quarterly, or more frequently.	Users	Identify	●	●	●
5.2	**Use Unique Passwords** Use unique passwords for all enterprise assets. Best practice implementation includes, at a minimum, an 8-character password for accounts using MFA and a 14-character password for accounts not using MFA.	Users	Protect	●	●	●
5.3	**Disable Dormant Accounts** Delete or disable any dormant accounts after a period of 45 days of inactivity, where supported.	Users	Respond	●	●	●
5.4	**Restrict Administrator Privileges to Dedicated Administrator Accounts** Restrict administrator privileges to dedicated administrator accounts on enterprise assets. Conduct general computing activities, such as internet browsing, email, and productivity suite use, from the user's primary, non-privileged account.	Users	Protect	●	●	●
5.5	**Establish and Maintain an Inventory of Service Accounts** Establish and maintain an inventory of service accounts. The inventory, at a minimum, must contain department owner, review date, and purpose. Perform service account reviews to validate that all active accounts are authorized, on a recurring schedule at a minimum quarterly, or more frequently.	Users	Identify		●	●
5.6	**Centralize Account Management** Centralize account management through a directory or identity service.	Users	Protect		●	●

CIS Center for Internet Security®
Creating Confidence in the Connected World.

Tipologie di Test di Sicurezza
CIS (Center for Internet Security) Controls

6. *Gestione del Controllo degli Accessi*
   - Utilizzare processi e strumenti per creare, assegnare, gestire e revocare credenziali di accesso e privilegi per gli account utente, amministratore e di servizio per risorse e software aziendali

Tipologie di Test di Sicurezza

CIS (Center for Internet Security) Controls

6. *Gestione del Controllo degli Accessi*

NUMBER	TITLE/DESCRIPTION	ASSET TYPE	SECURITY FUNCTION	IG1	IG2	IG3
6.1	**Establish an Access Granting Process** Establish and follow a process, preferably automated, for granting access to enterprise assets upon new hire, rights grant, or role change of a user.	Users	Protect	●	●	●
6.2	**Establish an Access Revoking Process** Establish and follow a process, preferably automated, for revoking access to enterprise assets, through disabling accounts immediately upon termination, rights revocation, or role change of a user. Disabling accounts, instead of deleting accounts, may be necessary to preserve audit trails.	Users	Protect	●	●	●
6.3	**Require MFA for Externally-Exposed Applications** Require all externally-exposed enterprise or third-party applications to enforce MFA, where supported. Enforcing MFA through a directory service or SSO provider is a satisfactory implementation of this Safeguard.	Users	Protect	●	●	●
6.4	**Require MFA for Remote Network Access** Require MFA for remote network access.	Users	Protect	●	●	●
6.5	**Require MFA for Administrative Access** Require MFA for all administrative access accounts, where supported, on all enterprise assets, whether managed on-site or through a third-party provider.	Users	Protect	●	●	●
6.6	**Establish and Maintain an Inventory of Authentication and Authorization Systems** Establish and maintain an inventory of the enterprise's authentication and authorization systems, including those hosted on-site or at a remote service provider. Review and update the inventory, at a minimum, annually, or more frequently.	Users	Identify		●	●
6.7	**Centralize Access Control** Centralize access control for all enterprise assets through a directory service or SSO provider, where supported.	Users	Protect		●	●
6.8	**Define and Maintain Role-Based Access Control** Define and maintain role-based access control, through determining and documenting the access rights necessary for each role within the enterprise to successfully carry out its assigned duties. Perform access control reviews of enterprise assets to validate that all privileges are authorized, on a recurring schedule at a minimum annually, or more frequently.	Data	Protect			●

CIS Center for Internet Security®
Creating Confidence in the Connected World.

Tipologie di Test di Sicurezza
CIS (Center for Internet Security) Controls

7. *Gestione Continua delle Vulnerabilità*
   - Sviluppare un piano per valutare e tenere traccia continuamente delle vulnerabilità su tutte le risorse aziendali appartenenti all'asset, così da ridurre al minimo i rischi
   - Monitorare costantemente le fonti di informazione, così da poter scoprire nuove vulnerabilità e minacce

Tipologie di Test di Sicurezza

CIS (Center for Internet Security) Controls

7. *Gestione Continua delle Vulnerabilità*

NUMBER	TITLE/DESCRIPTION	ASSET TYPE	SECURITY FUNCTION	IG1	IG2	IG3
7.1	**Establish and Maintain a Vulnerability Management Process** Establish and maintain a documented vulnerability management process for enterprise assets. Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	Applications	Protect	●	●	●
7.2	**Establish and Maintain a Remediation Process** Establish and maintain a risk-based remediation strategy documented in a remediation process, with monthly, or more frequent, reviews.	Applications	Respond	●	●	●
7.3	**Perform Automated Operating System Patch Management** Perform operating system updates on enterprise assets through automated patch management on a monthly, or more frequent, basis.	Applications	Protect	●	●	●
7.4	**Perform Automated Application Patch Management** Perform application updates on enterprise assets through automated patch management on a monthly, or more frequent, basis.	Applications	Protect	●	●	●
7.5	**Perform Automated Vulnerability Scans of Internal Enterprise Assets** Perform automated vulnerability scans of internal enterprise assets on a quarterly, or more frequent, basis. Conduct both authenticated and unauthenticated scans, using a SCAP-compliant vulnerability scanning tool.	Applications	Identify		●	●
7.6	**Perform Automated Vulnerability Scans of Externally-Exposed Enterprise Assets** Perform automated vulnerability scans of externally-exposed enterprise assets using a SCAP-compliant vulnerability scanning tool. Perform scans on a monthly, or more frequent, basis.	Applications	Identify		●	●
7.7	**Remediate Detected Vulnerabilities** Remediate detected vulnerabilities in software through processes and tooling on a monthly, or more frequent, basis, based on the remediation process.	Applications	Respond		●	●

CIS Center for Internet Security®
Creating Confidence in the Connected World.

Tipologie di Test di Sicurezza
CIS (Center for Internet Security) Controls

8. *Gestione dei Log di Controllo*
   - Raccogliere, esaminare e conservare i log di controllo degli eventi che potrebbero aiutare a rilevare, comprendere o recuperare da un attacco

Tipologie di Test di Sicurezza

CIS (Center for Internet Security) Controls

8. *Gestione dei Log di Controllo*

NUMBER	TITLE/ DESCRIPTION	ASSET TYPE	SECURITY FUNCTION	IG1	IG2	IG3
8.1	**Establish and Maintain an Audit Log Management Process** Establish and maintain an audit log management process that defines the enterprise's logging requirements. At a minimum, address the collection, review, and retention of audit logs for enterprise assets. Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	Network	Protect	●	●	●
8.2	**Collect Audit Logs** Collect audit logs. Ensure that logging, per the enterprise's audit log management process, has been enabled across enterprise assets.	Network	Detect	●	●	●
8.3	**Ensure Adequate Audit Log Storage** Ensure that logging destinations maintain adequate storage to comply with the enterprise's audit log management process.	Network	Protect	●	●	●
8.4	**Standardize Time Synchronization** Standardize time synchronization. Configure at least two synchronized time sources across enterprise assets, where supported.	Network	Protect		●	●
8.5	**Collect Detailed Audit Logs** Configure detailed audit logging for enterprise assets containing sensitive data. Include event source, date, username, timestamp, source addresses, destination addresses, and other useful elements that could assist in a forensic investigation.	Network	Detect		●	●
8.6	**Collect DNS Query Audit Logs** Collect DNS query audit logs on enterprise assets, where appropriate and supported.	Network	Detect		●	●

CIS Center for Internet Security®
Creating Confidence in the Connected World.

Tipologie di Test di Sicurezza

CIS (Center for Internet Security) Controls

8. *Gestione dei Log di Controllo*

8.7	**Collect URL Request Audit Logs**	**Network**	**Detect**		●	●
	Collect URL request audit logs on enterprise assets, where appropriate and supported.					
8.8	**Collect Command-Line Audit Logs**	**Devices**	**Detect**		●	●
	Collect command-line audit logs. Example implementations include collecting audit logs from PowerShell®, BASH™, and remote administrative terminals.					
8.9	**Centralize Audit Logs**	**Network**	**Detect**		●	●
	Centralize, to the extent possible, audit log collection and retention across enterprise assets.					
8.10	**Retain Audit Logs**	**Network**	**Protect**		●	●
	Retain audit logs across enterprise assets for a minimum of 90 days.					
8.11	**Conduct Audit Log Reviews**	**Network**	**Detect**		●	●
	Conduct reviews of audit logs to detect anomalies or abnormal events that could indicate a potential threat. Conduct reviews on a weekly, or more frequent, basis.					
8.12	**Collect Service Provider Logs**	**Data**	**Detect**			●
	Collect service provider logs, where supported. Example implementations include collecting authentication and authorization events, data creation and disposal events, and user management events.					

CIS Center for Internet Security®
Creating Confidence in the Connected World.

Tipologie di Test di Sicurezza
CIS (Center for Internet Security) Controls

9. *Protezione E-mail e Web Browser*
   - Migliorare le protezioni ed i rilevamenti delle minacce provenienti da E-mail e Web
     - Tali minacce rappresentano un'opportunità per gli aggressori di manipolare il comportamento umano attraverso il coinvolgimento diretto (i.e., *social engineering*)

Tipologie di Test di Sicurezza

CIS (Center for Internet Security) Controls

9. *Protezione E-mail e Web Browser*

NUMBER	TITLE/DESCRIPTION	ASSET TYPE	SECURITY FUNCTION	IG1	IG2	IG3
9.1	**Ensure Use of Only Fully Supported Browsers and Email Clients** Ensure only fully supported browsers and email clients are allowed to execute in the enterprise, only using the latest version of browsers and email clients provided through the vendor.	Applications	Protect	●	●	●
9.2	**Use DNS Filtering Services** Use DNS filtering services on all enterprise assets to block access to known malicious domains.	Network	Protect	●	●	●
9.3	**Maintain and Enforce Network-Based URL Filters** Enforce and update network-based URL filters to limit an enterprise asset from connecting to potentially malicious or unapproved websites. Example implementations include category-based filtering, reputation-based filtering, or through the use of block lists. Enforce filters for all enterprise assets.	Network	Protect		●	●
9.4	**Restrict Unnecessary or Unauthorized Browser and Email Client Extensions** Restrict, either through uninstalling or disabling, any unauthorized or unnecessary browser or email client plugins, extensions, and add-on applications.	Applications	Protect		●	●
9.5	**Implement DMARC** To lower the chance of spoofed or modified emails from valid domains, implement DMARC policy and verification, starting with implementing the Sender Policy Framework (SPF) and the DomainKeys Identified Mail (DKIM) standards.	Network	Protect		●	●
9.6	**Block Unnecessary File Types** Block unnecessary file types attempting to enter the enterprise's email gateway.	Network	Protect		●	●
9.7	**Deploy and Maintain Email Server Anti-Malware Protections** Deploy and maintain email server anti-malware protections, such as attachment scanning and/or sandboxing.	Network	Protect			●

CIS Center for Internet Security®
Creating Confidence in the Connected World.

Tipologie di Test di Sicurezza
CIS (Center for Internet Security) Controls

10. *Difese Anti Malware*
    - Prevenire o controllare l'installazione, la diffusione e l'esecuzione di programmi o script dannosi sulle risorse aziendali

Tipologie di Test di Sicurezza

CIS (Center for Internet Security) Controls

10. *Difese Anti Malware*

NUMBER	TITLE/ DESCRIPTION	ASSET TYPE	SECURITY FUNCTION	IG1	IG2	IG3
10.1	**Deploy and Maintain Anti-Malware Software** Deploy and maintain anti-malware software on all enterprise assets.	Devices	Protect	●	●	●
10.2	**Configure Automatic Anti-Malware Signature Updates** Configure automatic updates for anti-malware signature files on all enterprise assets.	Devices	Protect	●	●	●
10.3	**Disable Autorun and Autoplay for Removable Media** Disable autorun and autoplay auto-execute functionality for removable media.	Devices	Protect	●	●	●
10.4	**Configure Automatic Anti-Malware Scanning of Removable Media** Configure anti-malware software to automatically scan removable media.	Devices	Detect		●	●
10.5	**Enable Anti-Exploitation Features** Enable anti-exploitation features on enterprise assets and software, where possible, such as Microsoft® Data Execution Prevention (DEP), Windows® Defender Exploit Guard (WDEG), or Apple® System Integrity Protection (SIP) and Gatekeeper™.	Devices	Protect		●	●
10.6	**Centrally Manage Anti-Malware Software** Centrally manage anti-malware software.	Devices	Protect		●	●
10.7	**Use Behavior-Based Anti-Malware Software** Use behavior-based anti-malware software.	Devices	Detect		●	●

CIS Center for Internet Security®
Creating Confidence in the Connected World.

Tipologie di Test di Sicurezza
CIS (Center for Internet Security) Controls

11. *Recupero Dati*
    - Stabilire e mantenere pratiche di ripristino dei dati che permettano di ripristinare le risorse aziendali ad uno stato sicuro pre-incidente

Tipologie di Test di Sicurezza

CIS (Center for Internet Security) Controls

11. *Recupero Dati*

NUMBER	TITLE/DESCRIPTION	ASSET TYPE	SECURITY FUNCTION	IG1	IG2	IG3
11.1	**Establish and Maintain a Data Recovery Process** Establish and maintain a data recovery process. In the process, address the scope of data recovery activities, recovery prioritization, and the security of backup data. Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	Data	Recover	●	●	●
11.2	**Perform Automated Backups** Perform automated backups of in-scope enterprise assets. Run backups weekly, or more frequently, based on the sensitivity of the data.	Data	Recover	●	●	●
11.3	**Protect Recovery Data** Protect recovery data with equivalent controls to the original data. Reference encryption or data separation, based on requirements.	Data	Protect	●	●	●
11.4	**Establish and Maintain an Isolated Instance of Recovery Data** Establish and maintain an isolated instance of recovery data. Example implementations include version controlling backup destinations through offline, cloud, or off-site systems or services.	Data	Recover	●	●	●
11.5	**Test Data Recovery** Test backup recovery quarterly, or more frequently, for a sampling of in-scope enterprise assets.	Data	Recover		●	●

CIS Center for Internet Security®
Creating Confidence in the Connected World.

Tipologie di Test di Sicurezza
CIS (Center for Internet Security) Controls

12. *Gestione dell'Infrastruttura di Rete*
    - Installare, configurare e gestire attivamente i dispositivi di rete, al fine di impedire agli aggressori di sfruttare servizi di rete e punti di accesso vulnerabili

Tipologie di Test di Sicurezza

CIS (Center for Internet Security) Controls

12. *Gestione dell'Infrastruttura di Rete*

NUMBER	TITLE/DESCRIPTION	ASSET TYPE	SECURITY FUNCTION	IG1	IG2	IG3
12.1	**Ensure Network Infrastructure is Up-to-Date** Ensure network infrastructure is kept up-to-date. Example implementations include running the latest stable release of software and/or using currently supported network-as-a-service (NaaS) offerings. Review software versions monthly, or more frequently, to verify software support.	Network	Protect	●	●	●
12.2	**Establish and Maintain a Secure Network Architecture** Establish and maintain a secure network architecture. A secure network architecture must address segmentation, least privilege, and availability, at a minimum.	Network	Protect		●	●
12.3	**Securely Manage Network Infrastructure** Securely manage network infrastructure. Example implementations include version-controlled-infrastructure-as-code, and the use of secure network protocols, such as SSH and HTTPS.	Network	Protect		●	●
12.4	**Establish and Maintain Architecture Diagram(s)** Establish and maintain architecture diagram(s) and/or other network system documentation. Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	Network	Identify		●	●
12.5	**Centralize Network Authentication, Authorization, and Auditing (AAA)** Centralize network AAA.	Network	Protect		●	●
12.6	**Use of Secure Network Management and Communication Protocols** Use secure network management and communication protocols (e.g., 802.1X, Wi-Fi Protected Access 2 (WPA2) Enterprise or greater).	Network	Protect		●	●
12.7	**Ensure Remote Devices Utilize a VPN and are Connecting to an Enterprise's AAA Infrastructure** Require users to authenticate to enterprise-managed VPN and authentication services prior to accessing enterprise resources on end-user devices.	Devices	Protect		●	●
12.8	**Establish and Maintain Dedicated Computing Resources for All Administrative Work** Establish and maintain dedicated computing resources, either physically or logically separated, for all administrative tasks or tasks requiring administrative access. The computing resources should be segmented from the enterprise's primary network and not be allowed internet access.	Devices	Protect			●

CIS Center for Internet Security®
Creating Confidence in the Connected World.

Tipologie di Test di Sicurezza
CIS (Center for Internet Security) Controls

13. *Monitoraggio e Difesa della Rete*
    - Utilizzare processi e strumenti per creare e mantenere nel tempo
      - Un monitoraggio completo della rete
      - Difese verso le minacce alla sicurezza dell'infrastruttura di rete e degli utenti dell'asset

Tipologie di Test di Sicurezza

CIS (Center for Internet Security) Controls

13. *Monitoraggio e Difesa della Rete*

NUMBER	TITLE/DESCRIPTION	ASSET TYPE	SECURITY FUNCTION	IG1	IG2	IG3
13.1	**Centralize Security Event Alerting** Centralize security event alerting across enterprise assets for log correlation and analysis. Best practice implementation requires the use of a SIEM, which includes vendor-defined event correlation alerts. A log analytics platform configured with security-relevant correlation alerts also satisfies this Safeguard.	Network	Detect		●	●
13.2	**Deploy a Host-Based Intrusion Detection Solution** Deploy a host-based intrusion detection solution on enterprise assets, where appropriate and/or supported.	Devices	Detect		●	●
13.3	**Deploy a Network Intrusion Detection Solution** Deploy a network intrusion detection solution on enterprise assets, where appropriate. Example implementations include the use of a Network Intrusion Detection System (NIDS) or equivalent cloud service provider (CSP) service.	Network	Detect		●	●
13.4	**Perform Traffic Filtering Between Network Segments** Perform traffic filtering between network segments, where appropriate.	Network	Protect		●	●

CIS Center for Internet Security®
Creating Confidence in the Connected World.

Tipologie di Test di Sicurezza

CIS (Center for Internet Security) Controls

13. *Monitoraggio e Difesa della Rete*

NUMBER	TITLE/DESCRIPTION	ASSET TYPE	SECURITY FUNCTION	IG1	IG2	IG3
13.5	**Manage Access Control for Remote Assets** Manage access control for assets remotely connecting to enterprise resources. Determine amount of access to enterprise resources based on: up-to-date anti-malware software installed, configuration compliance with the enterprise's secure configuration process, and ensuring the operating system and applications are up-to-date.	Devices	Protect		●	●
13.6	**Collect Network Traffic Flow Logs** Collect network traffic flow logs and/or network traffic to review and alert upon from network devices.	Network	Detect		●	●
13.7	**Deploy a Host-Based Intrusion Prevention Solution** Deploy a host-based intrusion prevention solution on enterprise assets, where appropriate and/or supported. Example implementations include use of an Endpoint Detection and Response (EDR) client or host-based IPS agent.	Devices	Protect			●
13.8	**Deploy a Network Intrusion Prevention Solution** Deploy a network intrusion prevention solution, where appropriate. Example implementations include the use of a Network Intrusion Prevention System (NIPS) or equivalent CSP service.	Network	Protect			●
13.9	**Deploy Port-Level Access Control** Deploy port-level access control. Port-level access control utilizes 802.1x, or similar network access control protocols, such as certificates, and may incorporate user and/or device authentication.	Devices	Protect			●
13.10	**Perform Application Layer Filtering** Perform application layer filtering. Example implementations include a filtering proxy, application layer firewall, or gateway.	Network	Protect			●
13.11	**Tune Security Event Alerting Thresholds** Tune security event alerting thresholds monthly, or more frequently.	Network	Detect			●

CIS Center for Internet Security®
Creating Confidence in the Connected World.

Tipologie di Test di Sicurezza
CIS (Center for Internet Security) Controls

14. *Formazione sulle Competenze e la Consapevolezza della Sicurezza*
    - Stabilire e mantenere un programma di sensibilizzazione sulla sicurezza per influenzare il comportamento del personale
    - Ciò farà sì che il personale sia attento alla sicurezza e adeguatamente qualificato, riducendo così i rischi per l'azienda

Tipologie di Test di Sicurezza

CIS (Center for Internet Security) Controls

14. *Formazione sulle Competenze e la Consapevolezza della Sicurezza*

NUMBER	TITLE/DESCRIPTION	ASSET TYPE	SECURITY FUNCTION	IG1	IG2	IG3
14.1	**Establish and Maintain a Security Awareness Program** Establish and maintain a security awareness program. The purpose of a security awareness program is to educate the enterprise's workforce on how to interact with enterprise assets and data in a secure manner. Conduct training at hire and, at a minimum, annually. Review and update content annually, or when significant enterprise changes occur that could impact this Safeguard.	N/A	Protect	●	●	●
14.2	**Train Workforce Members to Recognize Social Engineering Attacks** Train workforce members to recognize social engineering attacks, such as phishing, pre-texting, and tailgating.	N/A	Protect	●	●	●
14.3	**Train Workforce Members on Authentication Best Practices** Train workforce members on authentication best practices. Example topics include MFA, password composition, and credential management.	N/A	Protect	●	●	●
14.4	**Train Workforce on Data Handling Best Practices** Train workforce members on how to identify and properly store, transfer, archive, and destroy sensitive data. This also includes training workforce members on clear screen and desk best practices, such as locking their screen when they step away from their enterprise asset, erasing physical and virtual whiteboards at the end of meetings, and storing data and assets securely.	N/A	Protect	●	●	●
14.5	**Train Workforce Members on Causes of Unintentional Data Exposure** Train workforce members to be aware of causes for unintentional data exposure. Example topics include mis-delivery of sensitive data, losing a portable end-user device, or publishing data to unintended audiences.	N/A	Protect	●	●	●
14.6	**Train Workforce Members on Recognizing and Reporting Security Incidents** Train workforce members to be able to recognize a potential incident and be able to report such an incident.	N/A	Protect	●	●	●

CIS Center for Internet Security®
Creating Confidence in the Connected World.

Tipologie di Test di Sicurezza

CIS (Center for Internet Security) Controls

14. *Formazione sulle Competenze e la Consapevolezza della Sicurezza*

NUMBER	TITLE/DESCRIPTION	ASSET TYPE	SECURITY FUNCTION	IG1	IG2	IG3
14.7	**Train Workforce on How to Identify and Report if Their Enterprise Assets are Missing Security Updates** Train workforce to understand how to verify and report out-of-date software patches or any failures in automated processes and tools. Part of this training should include notifying IT personnel of any failures in automated processes and tools.	N/A	Protect	●	●	●
14.8	**Train Workforce on the Dangers of Connecting to and Transmitting Enterprise Data Over Insecure Networks** Train workforce members on the dangers of connecting to, and transmitting data over, insecure networks for enterprise activities. If the enterprise has remote workers, training must include guidance to ensure that all users securely configure their home network infrastructure.	N/A	Protect	●	●	●
14.9	**Conduct Role-Specific Security Awareness and Skills Training** Conduct role-specific security awareness and skills training. Example implementations include secure system administration courses for IT professionals, OWASP® Top 10 vulnerability awareness and prevention training for web application developers, and advanced social engineering awareness training for high-profile roles.	N/A	Protect		●	●

CIS Center for Internet Security®
Creating Confidence in the Connected World.

Tipologie di Test di Sicurezza
CIS (Center for Internet Security) Controls

15. *Gestione dei Service Provider*
    - Sviluppare un processo per valutare i fornitori di servizi che detengono dati sensibili o sono responsabili delle piattaforme o dei processi IT critici di un'azienda
    - Garantire che tali fornitori proteggano tali piattaforme e dati in modo appropriato

Tipologie di Test di Sicurezza

CIS (Center for Internet Security) Controls

15. *Gestione dei Service Provider*

NUMBER	TITLE/DESCRIPTION	ASSET TYPE	SECURITY FUNCTION	IG1	IG2	IG3
15.1	**Establish and Maintain an Inventory of Service Providers** Establish and maintain an inventory of service providers. The inventory is to list all known service providers, include classification(s), and designate an enterprise contact for each service provider. Review and update the inventory annually, or when significant enterprise changes occur that could impact this Safeguard.	N/A	Identify	●	●	●
15.2	**Establish and Maintain a Service Provider Management Policy** Establish and maintain a service provider management policy. Ensure the policy addresses the classification, inventory, assessment, monitoring, and decommissioning of service providers. Review and update the policy annually, or when significant enterprise changes occur that could impact this Safeguard.	N/A	Identify		●	●
15.3	**Classify Service Providers** Classify service providers. Classification consideration may include one or more characteristics, such as data sensitivity, data volume, availability requirements, applicable regulations, inherent risk, and mitigated risk. Update and review classifications annually, or when significant enterprise changes occur that could impact this Safeguard.	N/A	Identify		●	●

CIS Center for Internet Security®
Creating Confidence in the Connected World.

Tipologie di Test di Sicurezza

CIS (Center for Internet Security) Controls

15. *Gestione dei Service Provider*

NUMBER	TITLE/DESCRIPTION	ASSET TYPE	SECURITY FUNCTION	IG1	IG2	IG3
15.4	**Ensure Service Provider Contracts Include Security Requirements** Ensure service provider contracts include security requirements. Example requirements may include minimum security program requirements, security incident and/or data breach notification and response, data encryption requirements, and data disposal commitments. These security requirements must be consistent with the enterprise's service provider management policy. Review service provider contracts annually to ensure contracts are not missing security requirements.	N/A	Protect		●	●
15.5	**Assess Service Providers** Assess service providers consistent with the enterprise's service provider management policy. Assessment scope may vary based on classification(s), and may include review of standardized assessment reports, such as Service Organization Control 2 (SOC 2) and Payment Card Industry (PCI) Attestation of Compliance (AoC), customized questionnaires, or other appropriately rigorous processes. Reassess service providers annually, at a minimum, or with new and renewed contracts.	N/A	Identify			●
15.6	**Monitor Service Providers** Monitor service providers consistent with the enterprise's service provider management policy. Monitoring may include periodic reassessment of service provider compliance, monitoring service provider release notes, and dark web monitoring.	Data	Detect			●
15.7	**Securely Decommission Service Providers** Securely decommission service providers. Example considerations include user and service account deactivation, termination of data flows, and secure disposal of enterprise data within service provider systems.	Data	Protect			●

CIS Center for Internet Security®
Creating Confidence in the Connected World.

Tipologie di Test di Sicurezza
CIS (Center for Internet Security) Controls

16. *Sicurezza del Software Applicativo*
    - Gestire il ciclo di vita della sicurezza del software (sviluppato internamente o acquisito) per prevenire, rilevare e correggere le problematiche di sicurezza prima che esse possano avere un impatto sull'azienda

CIS Center for Internet Security® Creating Confidence in the Connected World.

Tipologie di Test di Sicurezza

CIS (Center for Internet Security) Controls

16. *Sicurezza del Software Applicativo*

NUMBER	TITLE/DESCRIPTION	ASSET TYPE	SECURITY FUNCTION	IG1	IG2	IG3
16.1	**Establish and Maintain a Secure Application Development Process** Establish and maintain a secure application development process. In the process, address such items as: secure application design standards, secure coding practices, developer training, vulnerability management, security of third-party code, and application security testing procedures. Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	Applications	Protect		●	●
16.2	**Establish and Maintain a Process to Accept and Address Software Vulnerabilities** Establish and maintain a process to accept and address reports of software vulnerabilities, including providing a means for external entities to report. The process is to include such items as: a vulnerability handling policy that identifies reporting process, responsible party for handling vulnerability reports, and a process for intake, assignment, remediation, and remediation testing. As part of the process, use a vulnerability tracking system that includes severity ratings, and metrics for measuring timing for identification, analysis, and remediation of vulnerabilities. Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard. Third-party application developers need to consider this an externally-facing policy that helps to set expectations for outside stakeholders.	Applications	Protect		●	●
16.3	**Perform Root Cause Analysis on Security Vulnerabilities** Perform root cause analysis on security vulnerabilities. When reviewing vulnerabilities, root cause analysis is the task of evaluating underlying issues that create vulnerabilities in code, and allows development teams to move beyond just fixing individual vulnerabilities as they arise.	Applications	Protect		●	●
16.4	**Establish and Manage an Inventory of Third-Party Software Components** Establish and manage an updated inventory of third-party components used in development, often referred to as a "bill of materials," as well as components slated for future use. This inventory is to include any risks that each third-party component could pose. Evaluate the list at least monthly to identify any changes or updates to these components, and validate that the component is still supported.	Applications	Protect		●	●
16.5	**Use Up-to-Date and Trusted Third-Party Software Components** Use up-to-date and trusted third-party software components. When possible, choose established and proven frameworks and libraries that provide adequate security. Acquire these components from trusted sources or evaluate the software for vulnerabilities before use.	Applications	Protect		●	●
16.6	**Establish and Maintain a Severity Rating System and Process for Application Vulnerabilities** Establish and maintain a severity rating system and process for application vulnerabilities that facilitates prioritizing the order in which discovered vulnerabilities are fixed. This process includes setting a minimum level of security acceptability for releasing code or applications. Severity ratings bring a systematic way of triaging vulnerabilities that improves risk management and helps ensure the most severe bugs are fixed first. Review and update the system and process annually.	Applications	Protect		●	●
16.7	**Use Standard Hardening Configuration Templates for Application Infrastructure** Use standard, industry-recommended hardening configuration templates for application infrastructure components. This includes underlying servers, databases, and web servers, and applies to cloud containers, Platform as a Service (PaaS) components, and SaaS components. Do not allow in-house developed software to weaken configuration hardening.	Applications	Protect		●	●

CIS Center for Internet Security®
Creating Confidence in the Connected World.

Tipologie di Test di Sicurezza

CIS (Center for Internet Security) Controls

16. *Sicurezza del Software Applicativo*

NUMBER	TITLE/DESCRIPTION	ASSET TYPE	SECURITY FUNCTION	IG1	IG2	IG3
16.8	**Separate Production and Non-Production Systems** Maintain separate environments for production and non-production systems.	Applications	Protect		●	●
16.9	**Train Developers in Application Security Concepts and Secure Coding** Ensure that all software development personnel receive training in writing secure code for their specific development environment and responsibilities. Training can include general security principles and application security standard practices. Conduct training at least annually and design in a way to promote security within the development team, and build a culture of security among the developers.	Applications	Protect		●	●
16.10	**Apply Secure Design Principles in Application Architectures** Apply secure design principles in application architectures. Secure design principles include the concept of least privilege and enforcing mediation to validate every operation that the user makes, promoting the concept of "never trust user input." Examples include ensuring that explicit error checking is performed and documented for all input, including for size, data type, and acceptable ranges or formats. Secure design also means minimizing the application infrastructure attack surface, such as turning off unprotected ports and services, removing unnecessary programs and files, and renaming or removing default accounts.	Applications	Protect		●	●
16.11	**Leverage Vetted Modules or Services for Application Security Components** Leverage vetted modules or services for application security components, such as identity management, encryption, and auditing and logging. Using platform features in critical security functions will reduce developers' workload and minimize the likelihood of design or implementation errors. Modern operating systems provide effective mechanisms for identification, authentication, and authorization and make those mechanisms available to applications. Use only standardized, currently accepted, and extensively reviewed encryption algorithms. Operating systems also provide mechanisms to create and maintain secure audit logs.	Applications	Protect		●	●
16.12	**Implement Code-Level Security Checks** Apply static and dynamic analysis tools within the application life cycle to verify that secure coding practices are being followed.	Applications	Protect			●
16.13	**Conduct Application Penetration Testing** Conduct application penetration testing. For critical applications, authenticated penetration testing is better suited to finding business logic vulnerabilities than code scanning and automated security testing. Penetration testing relies on the skill of the tester to manually manipulate an application as an authenticated and unauthenticated user.	Applications	Protect			●
16.14	**Conduct Threat Modeling** Conduct threat modeling. Threat modeling is the process of identifying and addressing application security design flaws within a design, before code is created. It is conducted through specially trained individuals who evaluate the application design and gauge security risks for each entry point and access level. The goal is to map out the application, architecture, and infrastructure in a structured way to understand its weaknesses.	Applications	Protect			●

CIS Center for Internet Security®
Creating Confidence in the Connected World.

Tipologie di Test di Sicurezza
CIS (Center for Internet Security) Controls

17. *Gestione dell'Incident Response*
    - Stabilire un programma per sviluppare e mantenere una capacità di risposta agli incidenti (ad es., politiche, piani, procedure, ruoli definiti, formazione e comunicazioni) per rilevare e fronteggiare rapidamente un attacco

CIS Center for Internet Security®
Creating Confidence in the Connected World.

Tipologie di Test di Sicurezza

CIS (Center for Internet Security) Controls

17. *Gestione dell'Incident Response*

NUMBER	TITLE/DESCRIPTION	ASSET TYPE	SECURITY FUNCTION	IG1	IG2	IG3
17.1	**Designate Personnel to Manage Incident Handling** Designate one key person, and at least one backup, who will manage the enterprise's incident handling process. Management personnel are responsible for the coordination and documentation of incident response and recovery efforts and can consist of employees internal to the enterprise, third-party vendors, or a hybrid approach. If using a third-party vendor, designate at least one person internal to the enterprise to oversee any third-party work. Review annually, or when significant enterprise changes occur that could impact this Safeguard.	N/A	Respond	●	●	●
17.2	**Establish and Maintain Contact Information for Reporting Security Incidents** Establish and maintain contact information for parties that need to be informed of security incidents. Contacts may include internal staff, third-party vendors, law enforcement, cyber insurance providers, relevant government agencies, Information Sharing and Analysis Center (ISAC) partners, or other stakeholders. Verify contacts annually to ensure that information is up-to-date.	N/A	Respond	●	●	●
17.3	**Establish and Maintain an Enterprise Process for Reporting Incidents** Establish and maintain an enterprise process for the workforce to report security incidents. The process includes reporting timeframe, personnel to report to, mechanism for reporting, and the minimum information to be reported. Ensure the process is publicly available to all of the workforce. Review annually, or when significant enterprise changes occur that could impact this Safeguard.	N/A	Respond	●	●	●

CIS Center for Internet Security®
Creating Confidence in the Connected World.

Tipologie di Test di Sicurezza

CIS (Center for Internet Security) Controls

17. *Gestione dell'Incident Response*

NUMBER	TITLE/DESCRIPTION	ASSET TYPE	SECURITY FUNCTION	IG1	IG2	IG3
17.4	**Establish and Maintain an Incident Response Process** Establish and maintain an incident response process that addresses roles and responsibilities, compliance requirements, and a communication plan. Review annually, or when significant enterprise changes occur that could impact this Safeguard.	N/A	Respond		●	●
17.5	**Assign Key Roles and Responsibilities** Assign key roles and responsibilities for incident response, including staff from legal, IT, information security, facilities, public relations, human resources, incident responders, and analysts, as applicable. Review annually, or when significant enterprise changes occur that could impact this Safeguard.	N/A	Respond		●	●
17.6	**Define Mechanisms for Communicating During Incident Response** Determine which primary and secondary mechanisms will be used to communicate and report during a security incident. Mechanisms can include phone calls, emails, or letters. Keep in mind that certain mechanisms, such as emails, can be affected during a security incident. Review annually, or when significant enterprise changes occur that could impact this Safeguard.	N/A	Respond		●	●
17.7	**Conduct Routine Incident Response Exercises** Plan and conduct routine incident response exercises and scenarios for key personnel involved in the incident response process to prepare for responding to real-world incidents. Exercises need to test communication channels, decision-making, and workflows. Conduct testing on an annual basis, at a minimum.	N/A	Recover		●	●
17.8	**Conduct Post-Incident Reviews** Conduct post-incident reviews. Post-incident reviews help prevent incident recurrence through identifying lessons learned and follow-up action.	N/A	Recover		●	●
17.9	**Establish and Maintain Security Incident Thresholds** Establish and maintain security incident thresholds, including, at a minimum, differentiating between an incident and an event. Examples can include: abnormal activity, security vulnerability, security weakness, data breach, privacy incident, etc. Review annually, or when significant enterprise changes occur that could impact this Safeguard.	N/A	Recover			●

CIS Center for Internet Security®
Creating Confidence in the Connected World.

Tipologie di Test di Sicurezza
CIS (Center for Internet Security) Controls

18. *Penetration Testing*
    - Valutare l'efficacia delle misure di sicurezza e la resilienza delle risorse aziendali
        - Identificando e sfruttando i punti deboli nei controlli di sicurezza
            - Riguardanti processi e fattori tecnologici
        - Simulando gli obiettivi e le azioni che potrebbe compiere un utente malintenzionato

Tipologie di Test di Sicurezza

CIS (Center for Internet Security) Controls

18. *Penetration Testing*

NUMBER	TITLE/DESCRIPTION	ASSET TYPE	SECURITY FUNCTION	IG1	IG2	IG3
18.1	**Establish and Maintain a Penetration Testing Program** Establish and maintain a penetration testing program appropriate to the size, complexity, and maturity of the enterprise. Penetration testing program characteristics include scope, such as network, web application, Application Programming Interface (API), hosted services, and physical premise controls; frequency; limitations, such as acceptable hours, and excluded attack types; point of contact information; remediation, such as how findings will be routed internally; and retrospective requirements.	N/A	Identify		●	●
18.2	**Perform Periodic External Penetration Tests** Perform periodic external penetration tests based on program requirements, no less than annually. External penetration testing must include enterprise and environmental reconnaissance to detect exploitable information. Penetration testing requires specialized skills and experience and must be conducted through a qualified party. The testing may be clear box or opaque box.	Network	Identify		●	●
18.3	**Remediate Penetration Test Findings** Remediate penetration test findings based on the enterprise's policy for remediation scope and prioritization.	Network	Protect		●	●
18.4	**Validate Security Measures** Validate security measures after each penetration test. If deemed necessary, modify rulesets and capabilities to detect the techniques used during testing.	Network	Protect			●
18.5	**Perform Periodic Internal Penetration Tests** Perform periodic internal penetration tests based on program requirements, no less than annually. The testing may be clear box or opaque box.	N/A	Identify			●

CIS Center for Internet Security®
Creating Confidence in the Connected World.

Tipologie di Test di Sicurezza

Vulnerability Assessment

- Identifica, tipicamente tramite strumenti automatici (ma anche manuali), tutte le potenziali vulnerabilità che potrebbero essere sfruttate da un attaccante

- Utilizzato per valutare
  - La Sicurezza Fisica
  - Il Personale (attraverso tecniche di *Social Engineering* e similari)
  - La Sicurezza dei Sistemi
  - La Sicurezza delle Reti
  - Etc

Tipologie di Test di Sicurezza
Vulnerability Assessment

- Valuta i controlli di sicurezza interni ed esterni
- Indica i «potenziali» rischi nelle difese esistenti
- Raccomanda e dà priorità alle strategie per porre rimedio ai rischi

Tipologie di Test di Sicurezza
Vulnerability Assessment

- Due tipologie di Vulnerability Assessment
  - **Vulnerability Assessment Interno** si occupa della sicurezza dei sistemi interni
  - **Vulnerability Assessment Esterno** si occupa della sicurezza delle difese perimetrali

- In entrambe le tipologie, ogni componente dell'asset (informatica, umana e fisica) è valutata usando più modalità e strumenti di attacco
  - Così da poter rilevare eventuali minacce e quantificare le misure da intraprendere per far fronte a tali minacce

Tipologie di Test di Sicurezza
Vulnerability Assessment

- **Osservazione**
  - La scoperta di una vulnerabilità non implica che si tratti di un problema di cui preoccuparsi
  - Tale vulnerabilità potrebbe non essere sfruttabile o, qualora essa venisse sfruttata, potrebbe non causare danni all'asset in cui essa risiede

Tipologie di Test di Sicurezza
Penetration Testing

- Processo che emula fedelmente le azioni (malevole) che potrebbe effettuare un attaccante
  - Violare un sistema sfruttando le sue vulnerabilità
  - Ottenere i massimi privilegi possibili nel sistema violato (ad es., *root*, *Administrator*, etc), assumendone il totale controllo
    - Furto di dati, spionaggio, etc
  - Causare malfunzionamenti al sistema
  - Etc

- Processo anche noto come *Ethical Hacking*

Tipologie di Test di Sicurezza
Penetration Testing

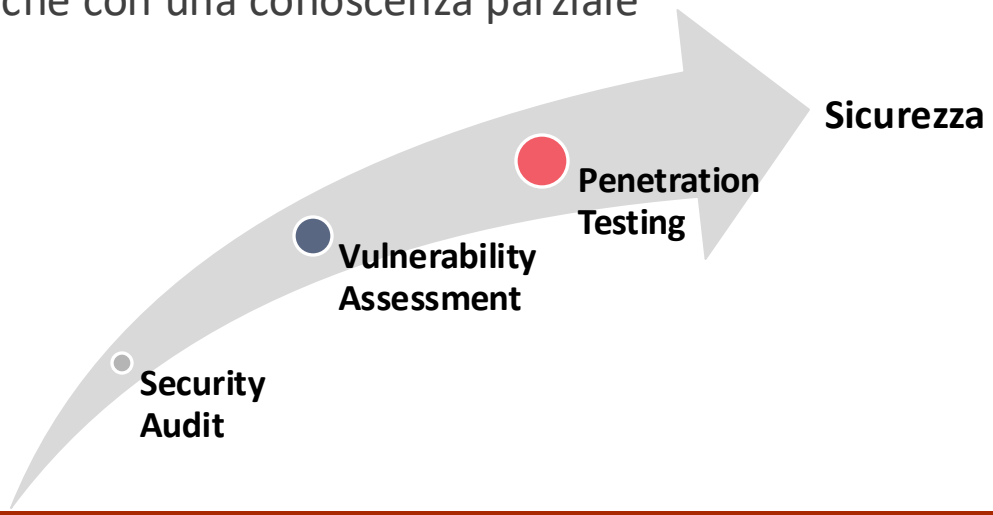
- Il Penetration Testing potrebbe essere eseguito
  - **Indipendentemente**, come processo stand-alone, oppure
  - **Durante un processo di gestione dei rischi**, incorporato nel normale ciclo di vita dello sviluppo software
    - Ad es., *Microsoft Security Development Lifecycle (SDL)*

Tipologie di Test di Sicurezza
Penetration Testing

- **Osservazione:** La sicurezza di un asset non dipende solo da fattori tecnologici ma anche da altri
  - Controllo degli accessi fisici
  - Sorveglianza degli ambienti
  - Definizione ed implementazione di adeguate politiche di sicurezza
  - Analisi dei comportamenti del personale
  - Formazione del personale
  - Etc

Tipologie di Test di Sicurezza
Penetration Testing

- Il **penetration testing** è considerato come la **più «aggressiva» forma di valutazione della sicurezza**
  - Deve essere condotto da professionisti qualificati
- Può essere condotto con o senza la conoscenza preliminare dell'asset da analizzare
  - Talvolta anche con una conoscenza parziale



Tipologie di Test di Sicurezza
Penetration Testing

- Il penetration testing è tipicamente usato per valutare tutte le componenti di un asset
  - Applicazioni
  - Dispositivi di Rete
  - Sistemi Operativi
  - Mezzi di Comunicazione
  - Sicurezza Fisica
  - Psicologia Umana
  - Etc

Vulnerability Assessment vs. Penetration Testing

- **Vulnerability Assessment**
  - Fornisce una visione esaustiva dei difetti dell'asset in esame
    - Non misura l'impatto dei difetti sull'asset
  - Identifica e quantifica in modo non invasivo tutte le vulnerabilità (tipicamente, note) dell'asset
- **Penetration Testing**
  - Va oltre l'identificazione delle vulnerabilità
    - Include le fasi di **Exploitation** e **Post-Exploitation**
  - Notevolmente più intrusivo del Vulnerability Assessment
    - Utilizza tutte le metodologie e gli strumenti usati da un attaccante reale (i.e., *Black Hat Hacker*)