# Assessment

## Approccio baseline

Per gli asset individuati, i seguenti controlli, scanditi dalla pubblicazione NIST 800-53, devono essere assicurati per mitigare il livello di rischio LOW associato agli asset:

### Access control

* AC-1: **ACCESS CONTROL POLICY AND PROCEDURES**
  1. Distribuzione al personale dell’organizzazione di documentazione relativa a (1) access control policy (concentrandosi sull’ambito di applicazione, sui ruoli, sulle responsabilità, …) e (2) procedure per effettuare l’enforcement di queste policy; **✓**
     + **Dobbiamo scrivere ad alto livello la policy di controllo degli accessi, qualcosa di simile alla specifica formale**
* AC-2: **ACCOUNT MANAGEMENT**
  1. Identificare i tipi di account significativi per l’organizzazione a supporto delle funzioni di business; **✓**
     + **Account significativi = utenti, amministratore.**
  2. Assegnazione degli account manager per la gestione degli account dei sistemi informativi;**✓**
     + **L’amministratore può gestire gli account del sistema informativo attraverso la dashboard di Auth0.**
  3. Specifica le condizioni di appartenenza a gruppi e ruoli (no use)
  4. Specifica gli utenti autorizzati del sistema informativo, i gruppi e l’appartenenza ai ruoli, l’autorizzazione agli accessi ed altri attributi per ciascun account; **✓**
     + **Abbiamo identificato e documentato le autorizzazioni per l’accesso alle risorse sulla base degli attributi associati agli utenti e alle risorse**
  5. Richiedere l’approvazione per la creazione di nuovi utenti; **✓**
     + **Non previsto**
  6. Creazione, abilitazione, modifica, disabilitazione e rimozione degli account dei sistemi informativi in accordo con determinate procedure e condizioni; **✓**
     + **L’amministratore del sistema ha la possibilità di gestire gli account del sistema informativo nella dashboard di Auth0**
  7. Monitoraggio dell’uso degli account del sistema informativo; **✓**
     + **Nella dashboard di Auth0 è possibile visualizzare log degli accessi degli utenti al sistema informativo. [FORSE LOGGING]**
  8. Notifica gli account manager quando ci sono: account non più richiesti; utenti sono terminati o trasferiti; le informazioni vengono modificate; **X**
     + **Al momento non è prevista la notifica ad un account Amministratore, qualora un utente volesse eliminare il suo account.**
     + **Possiamo implementare questa funzionalità attraverso la management API di Auth0 ed un accesso al Database.**
  9. Autorizzare l’accesso al sistema informativo basato su valide autorizzazioni d’accesso, uso inteso del sistema e altri attributi così come richiesti dall’organizzazione; **✓**
     + **Il sistema garantisce valide autorizzazioni d’accesso, così come descritto dalle policy presenti nella documentazione**
* AC-3: **ACCESS ENFORCEMENT**
  1. Il sistema informativo effettua l’enforcement delle autorizzazioni approvate per l’accesso logico alle informazioni e alle risorse di sistema in accordo con le policy applicabili di access control; **✓**
     + **Mediante le policy sviluppate in XACML è garantito l’enforcement delle policy applicabili di access control**
* AC-7: **UNSUCCESSFUL LOGON ATTEMPTS**
  1. Il sistema informativo effettua l’enforcement di un limite di consecutivi tentativi di login da un utente; **✓**
     + **Auth0 stabilisce un limite di 10 tentativi di login consecutivi (fallimentari) che provengano dallo stesso IP.**
  2. Applicazione di una politica di blocco per l’utente in caso di eccessivo numero di tentavi **✓**
     + **Al raggiungimento del limite di tentativi, l’utente interessato viene avvisato mediante email e viene bloccato l’indirizzo ip “sospetto”.**
* AC-8: **SYSTEM USE NOTIFICATION (no use)**
  1. Informazioni sulla privacy prima di garantire l’accesso di un utente al sistema **O**
* AC-14: **PERMITTED ACTIONS WITHOUT IDENTIFICATION OR AUTHENTICATION**
  1. Documentare l’insieme di azioni che possono essere performate da un utente non identificato oppure autenticato nei rispetti delle funzioni di business dell’organizzazione **✓**
     + **La documentazione descrive in maniera esaustiva le azioni che un utente può effettuare, per quanto implementato 🡪 un utente non identificato o autenticato può accedere solo alla pagina di presentazione del sistema informativo.**
* AC-17: **REMOTE ACCESS**
  1. Stabilire e documentare restrizioni nell’uso, requisiti di configurazione e connessione e linee guida per l’implementazione per ogni tipo di accesso remoto; **✓**
     + **Questa funzionalità non è stata implementata qualora un Amministratore volesse accedere da remoto al “Web Server” o al “Database Server” per gestirne la configurazione. [DA RIVEDERE]**
  2. Autorizzare accessi remoti al sistema informativo solo a valle dell’abilitazione di tali connessioni **✓**
     + **Il sistema informativo viene acceduto unicamente tramite connessione sicura HTTPS (lato webserver) e tramite openVPN, che garantisce comunicazione sicura e requisiti CIA con mutua autenticazione**
* AC-18: **WIRELESS ACCESS (no use) - O**
* AC-19: **ACCESS CONTROL FOR MOBILE DEVICES (no use) - O**
* AC-20: **USE OF EXTERNAL INFORMATION SYSTEMS (no use) - O**
* AC-22: **PUBLICLY ACCESSIBLE CONTENT**
  1. Gestione dei contenuti resi pubblici dal sistema: revisionare il contenuto proposto prima che possa essere reso accedibile **✓**
     + **Poiché gli amministratori del sistema sono gli unici a poter pubblicare contenuto, essendo questi entità fidate (noi), ci assicuriamo che il materiale pubblicato venga preventivamente revisionato. Tuttavia, in tutta onestà, sarebbe possibile per l’utente inserire username non appropriati, e in tal caso bisognerebbe aggiungere controlli a dizionario.**

### Identification and authentication control

* IA-1: **IDENTIFICATION AND AUTHENTICATION POLICY AND PROCEDURES**
  + Sviluppo, documentazione e disseminazione di policy di autenticazione e identificazione che indirizzino obiettivi, ruoli, responsabilità e coordinazione tra le entità dell’organizzazione, insieme a procedure che facilitino l’implementazione di suddette policy e di suddetti controlli. **✓**
    - **La documentazione descrive e dissemina in maniera estensiva concetti e regole relative all’autenticazione, nonché le tecnologie con le quali l’enforcement di queste viene realizzato.**
* IA-2: **IDENTIFICATION AND AUTHENTICATION (ORGANIZATIONAL USERS)**
  + Controllo per il quale il Sistema informativo possa identificare e autenticare in maniera unica utenti dell’organizzazione **✓**
    - **Il protocollo LDAP, e nella fattispecie, la Active Directory, garantisce di sua natura l’impossibilità di avere ambiguità nell’identificazione e autenticazione degli utenti**
* IA-2(1) : **IDENTIFICATION AND AUTHENTICATION | NETWORK ACCESS TO PRIVILEGED ACCOUNTS**
  + Il Sistema informativo implementa più fattori di autenticazione alla rete per utenti privilegiati **✓**
    - **Utenti Amministratori accederanno al sistema mediante le loro credenziali (username e password), che però verranno fornite dal vivo in quanto tali amministratori saranno dipendenti dell’organizzazione**
* IA-2(12) : **IDENTIFICATION AND AUTHENTICATION | ACCEPTANCE OF PIV CREDENTIALS (no use) -**
  + Il Sistema informativo accetta e verifica elettronicamente credenziali VIP (Personal Identity Verification) **O**
* IA-4 : **IDENTIFIER MANAGEMENT**
  + Controllo relativo alla gestione degli identificativi dell’organizzazione tramite ricezione di autenticazione da parte di una entità del Sistema. È necessario selezionare un identificativo che identifichi un individuo, un Gruppo, un ruolo o un dispositivo, nonchè poter assegnare un identificativo a individui, gruppi, ruoli o dispositivo. È inoltre fondamentale prevenire il riuso di identificativi e disabilitare eventualmente identificativi dopo un certo periodo di inattività. **✓**
    - **Mentre l’unicità degli utenti viene garantita dalla gestione dell’Active Directory, la disabilitazione è delegata all’amministratore del sistema LDAP server**
* IA-5 : **AUTHENTICATOR MANAGEMENT**
  + Controllo per l’organizzazione finalizzato alla gestione di sistemi autenticatori attraverso la verifica dell’identità dell’individuo, Gruppo, ruolo o dispositivo che riceve l’autenticatore. È necessario che gli autenticatori abbiamo meccanismi adatti, ed è necessario poterne valutare la compromissione o eventuali danni, ed in tal caso revocare il ruolo di autenticatore a tali sottosistemi. È necessario proteggere gli autenticatori dalla divulgazione di informazioni non autorizzate, da modifiche, da cambiamenti e così via. **✓**
    - **La gestione del sistema di autenticazione, LDAP server, è responsabilità dell’amministratore di sistema di tale server. Questa figura si ipotizza essere fidata; nonostante sia possibile limitarne le funzioni operative sulla directory, non è possibile in linea di principio evitare che egli divulghi informazioni sensibili. Tuttavia la tracciabilità garantita dal tool di Apache Active Directory, ci consente di risalire quantomeno al malfattore unico possibile. Inoltre le password sono salvate con SSHA, e quindi non è possibile recuperare almeno questa informazione**
* IA-5(1) : **AUTHENTICATOR MANAGEMENT | PASSWORD-BASED AUTHENTICATION**
  + Il Sistema informativo deve far uso di un Sistema di autenticazione basato sulla password che abbia una minima complessità prevista in termini di lunghezza, di mix di caratteri, caratteri maiuscoli e minuscoli. Bisogna inoltre trasmettere e proteggere password tramite cifratura e stabilire un Massimo time to live per tali password. **✓**
    - **Il webserver si assicura che le password immesse all’atto della registrazione rispettino uno standard di sicurezza che preveda una lunghezza minima ed una certa alternanza di caratteri**
* IA-5(11) : **AUTHENTICATOR MANAGEMENT | HARDWARE TOKEN BASED AUTHENTICATION (no use)**
  + Il Sistema informative deve poter impiegare un meccanismo per la generazione di token basati su hardware. Non utilizzabile. **O**
* IA-6 : **AUTHENTICATOR FEEDBACK**
  + Il Sistema informativo non deve tornare messaggi di feedback relativi al processo di autenticazion, al fine proteggere il Sistema da eventuali exploit. **✓**
    - **Il codice del sistema è stato schermato in maniera tale da non ritornare a livello interfaccia utente eventuali eccezioni, se non solo avvisaglie di connessioni non avvenute correttamente o di credenziali errate.**
* IA-7 : **CRYPTOGRAPHIC MODULE AUTHENTICATION**
  + Il Sistema informativo deve implementare meccanismi per l’autenticazione tramite un modulo crittografico adeguato **✓**
    - **L’infrastruttura webserver implementa opportuni moduli per la cifratura e decifratura di file sensibili, e inoltre tutti i canali sono coperti da tecnologie basate su SSL**
* IA-8 : **IDENTIFICATION AND AUTHENTICATION (NON ORGANIZATIONAL USERS)**
  + Il Sistema informativo deve identificare e autenticare in maniera univoca gli utenti non organizzativi **✓**
    - **L’active directory garantisce l’unicità di utenti non organizzativi**
* IA-8(1) : **IDENTIFICATION AND AUTHENTICATION | ACCEPTANCE OF PIV CREDENTIALS FROM OTHER AGENCIES (no use) O**
* IA-8(2) : **IDENTIFICATION AND AUTHENTICATION | ACCEPTANCE OF THIRD PARTY CREDENTIALS (no use) O**
* IA-8(3) : **IDENTIFICATION AND AUTHENTICATION | USE OF FICAM APPROVED PRODUCTS (no use) O**
* IA-8(4) : **IDENTIFICATION AND AUTHENTICATION | USE OF FICAM ISSUED PROFILES (no use) O**

### System and communications protection control

* SC-1 : **SYSTEM AND COMMUNICATIONS PROTECTION POLICY AND PROCEDURE**
  + L’organizzazione deve prevedere policy di protezione sia per il Sistema che per la comunicazione e implementare procedure che facciano l’enforcement di tale policy. **✓**
    - **Il sistema prevede policy atte alla protezione del sistema stesso, le cui comunicazioni vengono protette attraverso determinati protocolli (HTTPS, LDAPS, SSH,openVPN)**
* SC-5 : **DENIAL OF SERVICE PROTECTION - O**
  + Il Sistema informativo deve proteggersi, o limitare gli effetti, di attacchi di tipo Denial of Service, impiegando opportune safeguards.
    - **Si potrebbero implementare meccanismi di rilevazione automatici basati su IP che rilevino se un numero di richieste massime in un intervallo di tempo è stato rilevato. Tale controllo può essere implementato sia a livello Firewall, che applicativo**
* SC-7 : **BOUNDARY PROTECTIONS**
  + Il Sistema informativo deve monitorare e controllare le comunicazioni con confine esterni al Sistema e implementare sottoreti per componenti accedibili dal Sistema, fisicamente o logicamente, che siano separate dall’organizzazione interna della rete. Inoltre è necessario connettersi alla rete esterna solo attraverso interfacce consistenti di dispositive di protezione di confine, in accordo con l’architettura prevista dall’organizzazione **✓**
    - **Il sistema prevede una organizzazione di rete concernente i tre server principali, client escluso.**
    - **Internamente le comunicazioni:**
      * **Avvengono in maniera cifrata tramite LDAPS ed SSH.**
    - **Esternamente le comunicazioni:**
      * **Avvengono in maniera cifrata sul porto 8443, esposto in WAN. (webserver)**
      * **Non avvengono sul porto 22 per il server SSH, poiché il server SSH del webserver accetta solo determinati certificati e credenziali**
      * **Avvengono in maniera sicura con l’host server tramite VPN, poiché solo un utente registrato può disporre delle configurazioni necessarie**
      * **Non avvengono sul port 10636 per LDAPS, poiché anche esso fa uso di appositi certificati e credenziali.**
    - **Si potrebbero aggiungere delle regole al firewall che impediscano l’accesso dall’esterno sia al porto 22 Webserver che a quello 10636 per LDAP.**
* SC-12 : **CRYPTOGRAPHIC KEY ESTABLISHMENT AND MANAGEMENT**
  + L’organizzazione deve stabilire e gestire chiavi crittografiche per le tecniche di cifratura adottate. **✓**
    - **Le chiavi crittografiche sono gestite e protette**
* SC-13 :  **CRYPTOGRAPHIC PROTECTION ✓**
  + il Sistema informativo deve implementare usi e tipi di cifratura in accordo con le leggi federali, regolamentazioni e standard.
    - **Il sistema adotta cifrature AES, RSA**
* SC-15 : **COLLABORATIVE COMPUTING DEVICES**
  + Il Sistema informativo deve proibire l’attivazione remota di dispoitivi di calcolo collaborativi, con le opportune eccezioni, e deve fornire indicazioni esplicite agli utenti che fisicamente utilizzano tali dispositivi **O**
    - **Sarebbe possibile a tal proposito, data SSH come vulnerabilità in tale contesto, implementare il server SSH su di una macchina Virtuale, così da non permettere l’accesso all’intero sistema, qualora uno degli amministratori andasse rogue**
* SC-20 : **SECURE NAME/ ADDRESS RESOLUTION SERVICE**
  + Il Sistema informativo deve fornire autenticazione dei dati d’origine e verifiche di integrità per il processo di risoluzione dei nomi, in risposta a richieste di indirizzo esterne. È inoltre necessario fornire I mezzi per indicare lo stato di sicurezza della comunicazione e abilitare la verifica della catena di fiducia. **✓**
    - **Tale requisito è soddisfatto grazie non solo al protocollo HTTPS, ma anche grazie alla PKI realizzata all’interno del sistema, di cui il Webserver ne fa da self signed CA**
* SC-21 : **SECURE NAME / ADDRESS RESOLUTION SERVICE (no use) O**
  + Il Sistema informativo richiede ed effettua una autenticazione dei dati d’origine e verifica di integrità dei dati sulla risposta di risoluzione di indirizzo che il Sistema riceve da entità autoritarie.
* SC-22 : **ARCHITECTURE AND PROVISIONING FOR NAME/ADDRESS RESOLUTION SERVICE(no use)O**
  + Il Sistema informativo che fornisce il servizio di naming e risoluzione di indirizzi per l’organizzazione deve essere fault tolerant, e deve implementare una separazione dei ruoli interna ed esterna (non avendo tale provider, non possiamo utilizzarlo)
* SC-39 : **PROCESS ISOLATION**
  + Il Sistema informativo deve mantenere domini di esecuzione separata per ogni processo esecutivo **✓**
    - **Ogni componente del sistema è distribuito su macchine differenti.**