# 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; **✓**
     + **È stata sviluppata una documentazione riguardante l’access control policy e i meccanismi per applicarla.**
* AC-2: **ACCOUNT MANAGEMENT**
  1. Identificare i tipi di account significativi per l’organizzazione a supporto delle funzioni di business; **✓**
     + **Abbiamo identificato due tipologie di account significativi, gli utenti e gli amministratori.**
  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.**
  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 (no use) - O**
* AC-18: **WIRELESS ACCESS (no use) - O**
* AC-19: **ACCESS CONTROL FOR MOBILE DEVICES (no use) - O**
* AC-20: **USE OF EXTERNAL INFORMATION SYSTEMS**
  1. L’organizzazione stabilisce i termini e le condizioni in maniera consistente con le relazioni di fiducia stabilite con altre organizzazioni che possiedono, operano e/o gestiscono sistemi informative esterni, permettendo agli individui autorizzati di accedere al Sistema informativo da sistemi informativi esterni e di **✓**
  2. Processare, memorizzare o trasmettere informazioni controllate dall’organizzazione utilizzando sistemi informative esterni **✓**
     + **Il sistema prevede l’uso del servizio esterno Auth0, il cui uso è stato regolamentato nella documentazione.**
* AC-22: **PUBLICLY ACCESSIBLE CONTENT**
  1. Gestione dei contenuti resi pubblici dal sistema: revisionare il contenuto proposto prima che possa essere reso accessibile **X**
     + **Al momento non è stato implementato alcun controllo dei contenuti pubblicati sul sistema.**
     + **Tuttavia l’amministratore dovrebbe controllare i contenuti pubblicati e moderare di conseguenza, anche sospendendo un account utente o rimuovendolo.**

### Identification and authentication control

* IA-1: **IDENTIFICATION AND AUTHENTICATION POLICY AND PROCEDURES**
  1. 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)**
  1. Controllo per il quale il Sistema informativo possa identificare e autenticare in maniera unica utenti dell’organizzazione **✓**
     + **Il servizio esterno Auth0 garantisce l’impossibilità di avere ambiguità nell’identificazione e autenticazione degli utenti**
* IA-2(1) : **IDENTIFICATION AND AUTHENTICATION | NETWORK ACCESS TO PRIVILEGED ACCOUNTS**
  1. Il Sistema informativo implementa autenticazione con più fattori per l’accesso tramite rete per utenti privilegiati **X**
     + **Al momento non è stato implementata una simile funzionalità per gli amministratori, che semplicemente accedono tramite una email ed una password comunicate dal vivo.**
     + **Tuttavia la funzionalità potrebbe essere implementabile mediante il servizio Auth0.**
* IA-2(12) : **IDENTIFICATION AND AUTHENTICATION | ACCEPTANCE OF PIV CREDENTIALS (no use) -**
  1. Il Sistema informativo accetta e verifica elettronicamente credenziali VIP (Personal Identity Verification) **O**
* IA-4 : **IDENTIFIER MANAGEMENT**
  1. L’organizzazione gestisce gli identificativi del sistema informativo attraverso l’autorizzazione del personale ad assegnare un identificativo ad un individuo, un gruppo, un ruolo, o un dispositivo
  2. Attraverso la selezione di un identificativo che identifichi un individuo, un gruppo, un ruolo o un dispositivo,
  3. nonchè l’assegnazione di un identificativo a individui, gruppi, ruoli o dispositivo.
  4. È inoltre fondamentale prevenire il riuso di identificativi e
  5. disabilitare eventualmente identificativi dopo un certo periodo di inattività.
     + **Non previsto**
* IA-5 : **AUTHENTICATOR MANAGEMENT**
  1. L’organizzazione gestisce gli autenticatori del sistema informativo 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, Auth0, è responsabilità dell’amministratore. Ipotizziamo questa figura sia fidata; è possibile in ogni momento revocare, tramite il pannello di amministrazione di Auth0, la nomina di amministratore. Non è possibile evitare questa figura divulghi informazioni sensibili.**
* IA-5(1) : **AUTHENTICATOR MANAGEMENT | PASSWORD-BASED AUTHENTICATION**
  1. 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 sistema di autenticazione Auth0, ci permette di stabilire nel suo pannello di amministrazione la robustezza delle password richiesta all’atto della registrazione. Le password non sono mai conservate o “comunicate” in chiaro, ma sono protette con bcrypt, funzione crittografica di hash.**
* IA-5(11) : **AUTHENTICATOR MANAGEMENT | HARDWARE TOKEN BASED AUTHENTICATION (no use)**
  1. Il Sistema informative deve poter impiegare un meccanismo per la generazione di token basati su hardware. Non utilizzabile. **O**
* IA-6 : **AUTHENTICATOR FEEDBACK**
  1. 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 (no use) O**
  1. Il Sistema informativo deve implementare meccanismi per l’autenticazione tramite un “modulo crittografico” adeguato **O**
* IA-8 : **IDENTIFICATION AND AUTHENTICATION (NON ORGANIZATIONAL USERS)**
  1. Il Sistema informativo deve identificare e autenticare in maniera univoca gli utenti non organizzativi **✓**
     + **Auth0 garantisce unicità degli 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**
  1. 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, SSL)**
* SC-5 : **DENIAL OF SERVICE PROTECTION - O**
  1. 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.**
* SC-7 : **BOUNDARY PROTECTIONS**
  1. Il Sistema informativo deve monitorare e controllare le comunicazioni al confine esterno del Sistema ed ai confini chiave interni nel sistema e deve
  2. implementare sottoreti per componenti accessibili dal Sistema, fisicamente o logicamente, che siano separate dall’organizzazione interna della rete.
  3. 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 due server principali, client escluso.**
     + **Internamente le comunicazioni:**
       - **Avvengono in maniera cifrata tramite SSL.**
     + **Esternamente le comunicazioni:**
       - **Avvengono in maniera cifrata sul porto 8443. (webserver)**
* SC-12 : **CRYPTOGRAPHIC KEY ESTABLISHMENT AND MANAGEMENT**
  1. 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 ✓**
  1. il Sistema informativo deve implementare usi e tipi di cifratura in accordo con le leggi federali, regolamentazioni e standard.
     + **Il sistema adotta cifratura RS256 (RSA Signature with SHA-256) per i certificati JWT di Auth0**
     + **Per i certificati utilizzati da tomcat (webserver) prevedono l’utilizzo di RSA a 2048 bit per la chiave pubblica, e firma del certificato con SHA-256 (SHA256withRSA)**
     + **Per i certificati utilizzati dal Database Server viene utilizzato RSA a 2048 bit per la chiave pubblica, e firma del certificato con SHA-1 (sha1WithRSAEncryption)**
* SC-15 : **COLLABORATIVE COMPUTING DEVICES (no use)**
  1. 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**
* SC-20 : **SECURE NAME/ ADDRESS RESOLUTION SERVICE**
  1. Il Sistema informativo deve fornire artefatti di 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. **X**
     + **Non implementato.**
* SC-21 : **SECURE NAME / ADDRESS RESOLUTION SERVICE (no use) O**
  1. 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**
  1. 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**
  1. Il Sistema informativo deve mantenere domini di esecuzione separata per ogni processo esecutivo **✓**
     + **Ogni componente del sistema è distribuito su macchine differenti.**