Assessment Low

AC-1 🡺 [dobbiamo descrivere nella documentazione una policy che descriva i requisiti di sicurezza richiesti ed i meccanismi per fare l’enforcement di tali policy]

AC-2 🡺

1. Identificare gli account significativi per l’organizzazione [aggiungi amministratore]
2. Assegnare gli account manager per la gestione degli account dei sistemi informativi [amministratore]
3. Stabilire delle condizioni per l’appartenenza a gruppi specifici e ruoli
4. Specificare privilegi e autorizzazioni per ogni utente
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 dubbio]
7. Monitoraggio dell’uso degli account del sistema informativo; [in dubbio, ma forse si]
8. Notifica degli account manager (account non più richiesti, utenti sono terminati o trasferiti, quando le informazioni vengono modificate) [non implementato]
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 [OK]

AC-3 🡺 Il sistema informativo effettua l’enforcement di autorizzazione approvate per l’accesso logico alle informazioni e alle risorse di sistema in accordo con le policy applicabili di access control; [OK]

AC-4, AC-5, AC-6 🡺 LOW = NOT SELECTED (stefano non lo mette proprio)

AC-7 🡺 Il sistema informativo effettua l’enforcement di un limite di consecutivi tentativi di login da un utente [non implementato] Applicazione di una politica di blocco per l’utente in caso di eccessivo numero di tentavi [non implementato]

AC-8 🡺 no use

AC-9, AC-10, AC-11, AC-12 🡺 NOT SELECTED

AC-14 🡺 L’organizzazione identifica le azioni degli utenti che possono essere effettuate sul sistema informativo senza identificazione o autenticazione nel rispetto delle funzioni di business dell’organizzazione [in dubbio, ma credo di si]

AC-17 🡺