CERTIFICATO DI VALIDAZIONE E VERIFICA

Controllo e Riduzione della Superficie d'Attacco (NIST 800-53)

Informazioni Generali

Organizzazione:	_____
Ambiente Target (es. Azure Tenant ID):	_____
Responsabile della Valutazione (Assessor):	_____
Data di Verifica:	19 novembre 2025

Obiettivo e Standard di Riferimento

Questo documento attesta la verifica della superficie d'attacco dell'infrastruttura cloud/on-premise indicata. La validazione è condotta in conformità con:

- **NIST SP 800-53 Rev. 5:** Security and Privacy Controls for Information Systems.
- **NIST SP 800-171:** Protecting Controlled Unclassified Information.
- **NIST CSF 2.0:** Cybersecurity Framework (Identify, Protect, Detect, Respond, Recover).

Istruzioni: Contrassegnare con una X le caselle [SI] o [NO]. Se un controllo non è applicabile, segnare [N/A].

1 Identity and Access Management (IAM)

Riferimento NIST: Famiglia AC (Access Control) e IA (Identification and Authentication).

Requisiti Necessari (Must-Have)

1. **[SI] ☐ [NO] ☐ MFA Universale [IA-2]:** L'autenticazione a più fattori (MFA) è abilitata obbligatoriamente per tutti gli utenti, in particolare per gli amministratori globali (Root/Global Admin).
2. **[SI] ☐ [NO] ☐ Principio del Privilegio Minimo [AC-6]:** Gli account utente e di servizio possiedono solo i permessi strettamente necessari per le loro funzioni (RBAC configurato).
3. **[SI] ☐ [NO] ☐ Disabilitazione Legacy Auth [AC-17]:** I protocolli di autenticazione legacy (es. POP3, IMAP, SMTP auth) sono bloccati a livello di tenant.

Requisiti Sufficienti (Advanced Defense)

4. **[SI] ☐ [NO] ☐ Privileged Identity Management (PIM/JIT) [AC-1, AC-2]:** L'accesso amministrativo è fornito "Just-In-Time" e "Just-Enough-Access", con approvazione workflow e limiti temporali.
5. **[SI] ☐ [NO] ☐ Conditional Access Risk-Based [AC-3]:** Le policy di accesso negano automaticamente il login in base a segnali di rischio in tempo reale (es. impossible travel, IP anonimi).

2 Protezione della Rete e Perimetro

Riferimento NIST: Famiglia SC (System and Communications Protection) e CA (Security Assessment).

Requisiti Necessari (Must-Have)

1. **[SI] ☐ [NO] ☐ Network Segmentation [SC-7]:** Le risorse sono segmentate tramite Virtual Network (VNET) e sottoreti. Non esiste un "flat network".
2. **[SI] ☐ [NO] ☐ Chiusura Porte di Gestione [SC-7(12)]:** Le porte di gestione (RDP 3389, SSH 22) NON sono esposte direttamente su internet (0.0.0.0/0).
3. **[SI] ☐ [NO] ☐ Filtraggio Traffico [SC-7(5)]:** Sono attivi Firewall (L4) o Application Gateway (L7) per ispezionare tutto il traffico in ingresso e in uscita.

Requisiti Sufficienti (Advanced Defense)

4. **[SI] ☐ [NO] ☐ DDoS Protection Standard [SC-5]:** È abilitata una protezione avanzata contro attacchi Distributed Denial of Service specifica per l'applicazione, non solo volumetrica base.
5. **[SI] ☐ [NO] ☐ Private Link / Service Endpoints [SC-7(21)]:** I servizi PaaS (es. Database, Storage) non sono accessibili via endpoint pubblico ma solo tramite link privati all'interno della VNET.

3 Gestione Asset e Vulnerabilità

Riferimento NIST: Famiglia RA (Risk Assessment) e SI (System and Information Integrity).

Requisiti Necessari (Must-Have)

1. **[SI] ☐ [NO] ☐ Inventario degli Asset [CM-8]:** Esiste un inventario aggiornato e automatizzato di tutte le risorse cloud esposte.
2. **[SI] ☐ [NO] ☐ Scansione Vulnerabilità Continua [RA-5]:** È attivo uno scanner di vulnerabilità (es. Defender for Cloud, Nessus) sugli endpoint e sulle immagini container.

Requisiti Sufficienti (Advanced Defense)

3. **[SI] ☐ [NO] ☐ Automated Patch Management [SI-2]:** Le patch di sicurezza critiche vengono applicate automaticamente entro 72 ore dal rilascio.
4. **[SI] ☐ [NO] ☐ Attack Path Analysis [RA-3]:** Vengono utilizzate analisi basate su grafi per identificare percorsi di attacco laterali combinando identità e configurazioni errate.

4 Protezione dei Dati

Riferimento NIST: Famiglia SC (System and Communications Protection).

Requisiti Necessari (Must-Have)

1. **[SI] ☐ [NO] ☐ Encryption at Rest & Transit [SC-28]:** Tutti i dati sensibili sono cifrati a riposo e in transito (TLS 1.2+).
2. **[SI] ☐ [NO] ☐ Backup Immutabili [CP-9]:** I backup sono configurati con protezione contro la cancellazione (Soft Delete) e, ove possibile, immutabilità (WORM).

Requisiti Sufficienti (Advanced Defense)

3. **[SI] ☐ [NO] ☐ Customer-Managed Keys (BYOK) [SC-12]:** Per i dati altamente confidenziali, le chiavi di cifratura sono gestite dal cliente e non dal Cloud Provider.

Esito della Validazione

In base alle risposte fornite sopra, l'analisi della superficie d'attacco produce il seguente esito:

☐ **CONFORME (Validated):** Tutti i *Requisiti Necessari* sono soddisfatti. Almeno il 50% dei *Requisiti Sufficienti* è soddisfatto. Il rischio residuo è accettabile.

☐ **CONFORME CON RISERVA (Conditional):** Tutti i *Requisiti Necessari* sono soddisfatti, ma mancano significativi controlli sufficienti. Richiede piano di rientro entro 90 giorni.

☐ **NON CONFORME (Failed):** Uno o più *Requisiti Necessari* non sono soddisfatti. La superficie d'attacco è esposta a rischi critici.

Firme di Autorizzazione

Il Valutatore (Assessor)	**Il Responsabile Sicurezza (CISO/CIO)**
Firma: _____	Firma: _____
Data: 19 novembre 2025	Data: 19 novembre 2025

Nota Legale: Questo certificato rappresenta lo stato dell'arte al momento della verifica. Le configurazioni cloud sono dinamiche; si raccomanda una verifica continua secondo NIST CA-7 (Continuous Monitoring).