ENGAGEMENT DEFINITION

CRA Technical Assessment Scope

Perimetro, metodologia, input richiesti e deliverable dell’assessment tecnico

FAC-SIMILE DIMOSTRATIVO

Titolo	CRA Technical Assessment Scope
Codice	SLX-CRA-SCOPE-001
Versione	1.0
Data	16 agosto 2026
Cliente / Progetto	Caso applicativo - IG-200 Industrial Edge Gateway

Documento pubblico a finalità dimostrativa. I dati del cliente, del prodotto e i finding sono inventati; il contenuto non può essere presentato come assessment reale o evidenza di conformità.

Via Uccellino 9, 44028 Poggio Renatico | www.siliconlogix.it | mpezzullo@siliconlogix.it
Partita IVA: 02189310382

Controllo documento

Titolo	CRA Technical Assessment Scope
Codice documento	SLX-CRA-SCOPE-001
Cliente	Silicon LogiX · caso applicativo
Prodotto	IG-200 Industrial Edge Gateway · HW Rev. B · IGOS 2.4.1
Revisione	1.0
Stato	FAC-SIMILE / Esempio
Classificazione	Pubblico - Fac-simile dimostrativo
Data	16 agosto 2026

Registro revisioni

Rev.	Data	Descrizione	Autore
1.0	16 agosto 2026	Prima emissione del fac-simile	Silicon LogiX

Uso del documento
Questo fac-simile illustra struttura, terminologia e livello di dettaglio di un possibile deliverable. Prima di un incarico reale il contenuto va adattato al prodotto, al perimetro concordato, alle evidenze disponibili e alla procedura di conformità applicabile.

Posizionamento del deliverable
“CRA Technical Evidence Pack” è una denominazione commerciale del servizio Silicon LogiX, non il nome di un documento previsto dal Regolamento (UE) 2024/2847. Il Pack organizza evidenze tecniche, gap e azioni utili a supportare la documentazione tecnica e il percorso di conformità del fabbricante; non sostituisce la responsabilità del fabbricante, una valutazione legale, la dichiarazione UE di conformità, la marcatura CE o l’eventuale valutazione di un organismo notificato.

1. Scopo dell’incarico

Definire in modo verificabile cosa verrà analizzato, con quali evidenze e quale risultato riceverà il cliente.

Obiettivo. Valutare la readiness tecnica del prodotto rispetto agli aspetti di cybersecurity rilevanti per il percorso Cyber Resilience Act, ricostruendo baseline di prodotto, componenti software, superficie esposta, meccanismi di aggiornamento, gestione delle vulnerabilità e disponibilità delle evidenze tecniche.

Output atteso
Una fotografia tecnica del prodotto, una lista di gap/priorità e una roadmap di remediation. Il risultato è pensato per essere utilizzato da R&D, product management, qualità/compliance e specialisti incaricati del percorso di conformità.

- Stabilire una baseline ripetibile di hardware, firmware/software e servizi collegati al prodotto.
- Individuare evidenze già disponibili, evidenze mancanti e aree che richiedono verifica ulteriore.
- Produrre o normalizzare l'inventario software/SBOM per la release concordata, quando il materiale lo consente.
- Collegare i finding tecnici alle aree pertinenti dell'Allegato I e agli elementi documentali dell'Allegato VII.
- Prioritizzare interventi tecnici attuabili dal team interno o affidabili a Silicon LogiX.

2. Prodotto e perimetro dell'assessment

Prodotto	IG-200 Industrial Edge Gateway
Uso previsto	Raccolta e normalizzazione di dati macchina; collegamento Modbus RTU/TCP verso il campo e MQTT/TLS verso servizi remoti.
Hardware baseline	HW Rev. B; ARM Cortex-A53; 1 GB RAM; 8 GB eMMC; 2× GbE; RS-485 isolata; USB service; UART/JTAG.
Software baseline	IGOS 2.4.1; U-Boot 2024.01; Linux 6.1 LTS; Gateway Core 3.2.0; Web UI 1.8.2; MQTT 5/TLS 1.3; Modbus RTU/TCP.
Asset inclusi	Gateway campione, IGOS, U-Boot, immagine Linux, configurazioni di build, Gateway Core, Web UI, update A/B e dipendenze software.
Asset esclusi	Servizi backend non necessari al funzionamento valutato, infrastruttura IT del cliente, sicurezza fisica dell'impianto, assessment legale e certificazione.
Ambiente di riferimento	Rete industriale aziendale con segmentazione prevista ma non assunta come controllo sostitutivo della sicurezza del prodotto.

Regola di baseline
Ogni conclusione deve essere legata a una versione identificabile del prodotto. Modifiche hardware/software successive possono invalidare parte delle evidenze e richiedere un delta assessment.

3. Materiale richiesto al cliente

Categoria	Evidenza richiesta	Obbligatoria per baseline	Note
Prodotto	1–2 unità campione o accesso remoto controllato	Sì	Serial number e revisione hardware identificabili

Categoria	Evidenza richiesta	Obbligatoria per baseline	Note
Firmware	Binari, release note, configurazione di build e, se incluso, repository sorgente	Sì	Sorgenti necessari per analisi approfondita delle dipendenze
Architettura	Schema a blocchi, interfacce, trust boundary, flussi principali	Sì	Può essere ricostruita durante workshop se incompleta
Dipendenze	Manifest, package list, licenze, componenti third-party/open source	Preferibile	Usati per SBOM e dependency review
Update	Procedura OTA/service, firma, verifica, rollback/recovery	Sì	Inclusi server/tool lato produttore se nel perimetro
Security	Credenziali default, ruoli, configurazioni, secure boot/debug policy	Sì	Condivisione tramite canale concordato/NDA
Vulnerability handling	Policy CVD, mailbox/contatto, workflow CVE/CVE-like, advisory	Preferibile	Se assente viene registrato come gap di processo
Test	Report interni, test di sicurezza, fuzzing/pen-test precedenti	No	Usati come evidence, non assunti validi senza tracciabilità
Lifecycle	Support period, EOL/EOS policy, release cadence	Preferibile	Serve per motivare il support period e la manutenzione

4. Attività previste

1. Kick-off tecnico e definizione della baseline: prodotto, versioni, varianti, ambiente, owner interni e confini dell'assessment.
2. Product inventory e architecture reconstruction: componenti hardware/software, flussi, dipendenze e trust boundary rilevanti.
3. SBOM & dependency review: inventario top-level e, quando tecnicamente disponibile, componenti transitivi/relazioni di build; normalizzazione in formato machine-readable concordato.
4. Attack surface review: interfacce fisiche e logiche, servizi di rete, protocolli, ruoli, credenziali, canali di manutenzione e debug.
5. Security-control review: secure/default configuration, access control, integrità/confidenzialità, logging, hardening e mitigazioni applicabili in base al rischio.
6. Update & recovery review: autenticità/integrità degli update, distribuzione, rollback, recovery, gestione errori e separazione tra security update e feature update quando pertinente.
7. Vulnerability handling review: tracciamento componenti/vulnerabilità, CVD, contatto di segnalazione, triage, remediation, advisory e monitoraggio durante il support period.
8. Evidence mapping: collegamento tra evidenze disponibili, aree tecniche dell'Allegato I e contenuti dell'Allegato VII.

9. Findings & remediation roadmap: gap, priorità, dipendenze, quick win, interventi strutturali e open point da assegnare a owner specifici.

5. Metodo di assessment e classificazione

5.1 Livelli di evidenza

Livello	Significato	Esempio
Verificato	Osservato su dispositivo, configurazione, sorgente o test ripetibile	Verifica firma dell'immagine su update path
Documentato	Supportato da documento/versione tracciabile ma non ripetuto nel test	Procedura di release approvata
Dichiarato	Informazione fornita dal team senza evidenza sufficiente al momento	"Debug disabilitato in produzione"
Non verificato	Materiale non disponibile o attività fuori perimetro	Backend cloud escluso dall'incarico

5.2 Stato di readiness

Stato	Uso nel report
OK	Evidenza tecnica coerente con il criterio verificato nel perimetro concordato. Non equivale a certificazione di conformità.
PARZIALE	Controllo o evidenza esistente ma incompleta, non uniforme o non sufficientemente tracciabile.
GAP	Requisito tecnico/processo rilevante non implementato o evidenza mancante con impatto significativo sulla readiness.
N/A	Non applicabile alla baseline, con motivazione da validare nel percorso di conformità.
NON VERIFICATO	Nessuna conclusione: evidenza assente, componente fuori scope o verifica non prevista.

5.3 Priorità tecnica

Priorità	Criterio operativo
ALTA	Rischio elevato, prerequisito di più controlli, potenziale blocco del percorso o intervento con lead time significativo.
MEDIA	Miglioramento necessario ma pianificabile senza bloccare immediatamente le altre attività.
BASSA	Hardening, qualità dell'evidenza o ottimizzazione con impatto limitato nel breve periodo.

6. Deliverable

Deliverable	Contenuto	Formato indicativo
Management Summary	Stato generale, top finding, decisioni richieste e roadmap 30/60/90 giorni	PDF/DOCX
CRA Technical Evidence Pack	Baseline, architettura, SBOM summary, attack surface, risk assessment tecnico, mapping, finding e remediation	PDF/DOCX
SBOM snapshot	Inventario software legato alla release valutata; machine-readable se tecnicamente ricostruibile	CycloneDX/SPDX + tabella
Findings register	ID, area, evidenza, impatto, priorità, owner, stato e target release	XLSX/CSV o allegato al report
Evidence index	Elenco delle evidenze ricevute/prodotte con versione e riferimenti	Allegato al Pack

Consegna riutilizzabile
Il cliente può usare il materiale come input alla propria documentazione tecnica, alle review interne, al lavoro del consulente compliance e, se applicabile, alla preparazione della valutazione di conformità. Il fabbricante resta responsabile della completezza e validità finale.

7. Esclusioni e limiti

- Parere legale o determinazione vincolante del campo di applicazione del CRA.
- Certificazione, marcatura CE, dichiarazione UE di conformità o attività riservate a organismi notificati/autorità.
- Penetration test completo, red team, laboratorio accreditato, safety assessment o verifica EMC, salvo incarico separato.
- Analisi del cloud/backend, app mobile o infrastruttura del cliente se non espressamente inclusi nel perimetro.
- Garanzia che il prodotto sia privo di vulnerabilità; l'assessment fotografa evidenze e rischi nel perimetro/tempo concordato.
- Monitoraggio continuativo delle vulnerabilità dopo la consegna, salvo servizio ricorrente separato.

8. Ruoli e responsabilità

Attività	Silicon LogiX	Cliente / fabbricante
Definizione baseline	Facilita e documenta	Conferma prodotto, versioni, uso previsto e varianti
Fornitura materiale	Indica requisiti minimi	Fornisce evidenze complete e autorizzazioni necessarie
Assessment tecnico	Esegue analisi nel perimetro	Rende disponibili referenti tecnici e chiarimenti

Attività	Silicon LogiX	Cliente / fabbricante
Finding e priorità	Formula finding tecnici e remediation	Valida vincoli di prodotto e assegna owner
Decisioni di conformità	Fornisce evidenze tecniche	Mantiene la responsabilità delle decisioni, dichiarazioni e procedura applicabile
Remediation	Può implementare su incarico separato	Approva modifiche, release e test di accettazione

9. Piano operativo e change control

Fase	Output	Gate
A · Baseline & discovery	Scope confermato, evidence request, product map	Baseline firmata/congelata
B · Technical assessment	SBOM, attack surface, control review, risk evidence	Review tecnica con team cliente
C · Reporting	Pack, management summary, findings register, roadmap	Consegna e comment cycle
D · Remediation (opzionale)	Patch/feature, secure update, hardening, process tooling	Nuova release + delta verification

Change control. Nuove varianti, componenti, servizi o release emersi dopo il congelamento della baseline vengono registrati come change request o open point. Questo evita che il report mescoli evidenze riferite a prodotti diversi.

10. Accettazione, riservatezza e gestione materiale

- NDA disponibile prima della condivisione di repository, chiavi, credenziali, schemi e materiale riservato.
- Le credenziali di test devono essere dedicate e revocabili; non vanno utilizzate credenziali di produzione se non strettamente necessario e autorizzato.
- Le copie locali del materiale vengono gestite secondo il canale e il periodo di conservazione concordati con il cliente.
- La versione finale del documento viene identificata da codice, revisione, baseline prodotto e data di emissione.

Approvazione del perimetro

Per il cliente	Per Silicon LogiX
Nome / ruolo: _____	Nome / ruolo: _____
Data / firma: _____	Data / firma: _____

A. Evidence Request Checklist

Area	Da richiedere
Product	Part number, HW revision, serial/sample, intended purpose, deployment environment
Firmware	Release ID/hash, bootloader, build config, toolchain, release notes
Source/Build	Repository snapshot, manifest/lock files, CI/CD, reproducible build instructions
Dependencies	Open-source/third-party components, licenses, vendor libraries, binary blobs
Interfaces	Ethernet/Wi-Fi/BLE/USB/UART/JTAG, exposed ports/services, protocols
Identity	Accounts, roles, credentials, key/certificate provisioning and rotation
Update	Package format, signing, verification, rollback, recovery, distribution channel
Logging	Security events, audit trail, time source, export/retention
Vulnerability	CVD policy, contact, triage, vulnerability tracking, advisories
Lifecycle	Support period rationale, release cadence, EOL/EOS and decommissioning

Riferimenti normativi e informativi

Regolamento (UE) 2024/2847 (Cyber Resilience Act) — testo ufficiale EUR-Lex: Regulation (EU) 2024/2847

Commissione europea — Cyber Resilience Act: pagina ufficiale

Commissione europea — guidance CRA C(2026) 5252: Guidance C(2026) 5252

Verificato al 16/08/2026. La guidance non vincolante della Commissione C(2026) 5252 del 27/07/2026 è inclusa tra i riferimenti; atti di esecuzione, standard armonizzati, common specifications e guidance successivi devono essere riesaminati prima di ogni incarico reale.