EXECUTIVE DELIVERABLE

CRA Technical Assessment - Management Summary

Sintesi decisionale per management, product owner e responsabili R&D

FAC-SIMILE DIMOSTRATIVO

Titolo	CRA Technical Assessment - Management Summary
Codice	SLX-CRA-MGMT-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 — Management Summary
Codice documento	SLX-CRA-MGMT-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 executive
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. Executive snapshot

Conclusione di readiness. IG-200 possiede controlli utili già implementati, ma non è opportuno considerare chiusa la preparazione tecnica. Cinque gap richiedono intervento, con priorità immediata su SBOM e build provenance, catena di update/recovery, protezione debug e vulnerability handling.

Dominio	Stato	Messaggio per il management
Architettura & baseline	OK	Prodotto/versione e trust boundary sono identificabili.
SBOM & dipendenze	GAP	È disponibile uno snapshot CycloneDX ricostruito; manca una SBOM generata dalla build e legata deterministicamente alla release.
Update & recovery	GAP	Recovery non applica la stessa autenticazione dell'OTA.
Access control & hardening	PARZIALE	Web identity da completare; JTAG/UART e configurazione di produzione da governare.
Vulnerability handling	GAP	CVD, security contact e release gate devono essere formalizzati.
Lifecycle evidence	PARZIALE	Support period dichiarato ma non ancora motivato/documentato.

Decisione richiesta
Autorizzare una remediation tecnica in due tranche: (1) chiusura dei prerequisiti critici entro la prossima release; (2) automazione delle evidenze e consolidamento del lifecycle entro 90 giorni.

2. Prodotto e perimetro

Figura 1 — Perimetro tecnico valutato nel fac-simile.

Incluso	IG-200 HW Rev. B, IGOS 2.4.1, U-Boot 2024.01, Linux 6.1 LTS, Gateway Core 3.2.0, Web UI 1.8.2, interfacce e update A/B.
Escluso	Backend cloud, infrastruttura aziendale, assessment legale, certificazione/CE, penetration test completo.

Metodo	Review documentale + verifica tecnica selettiva + evidence mapping + gap analysis.
Uso previsto del report	Pianificazione R&D, input a qualità/compliance, definizione budget/priorità e tracciamento remediation.

3. Top 5 findings e impatto

ID	Finding	Impatto business/tecnico	Priorità
IG200-F-001	Recovery image non verificata come il normale update A/B	Rischio di firmware non autorizzato; blocca la coerenza dell'update chain.	ALTA
IG200-F-002	JTAG/UART di produzione non governati	Aumenta il rischio in caso di accesso fisico e complica l'hardening di produzione.	ALTA
IG200-F-004	CVD/security contact assenti	Il produttore non ha un canale/processo strutturato per ricevere e gestire vulnerabilità.	ALTA
IG200-F-007	Nessun vulnerability gate di release	Possibile rilascio senza evidenza formale sulla valutazione di vulnerabilità note.	ALTA
IG200-F-003	SBOM di release non deterministica	Tracciabilità manuale, rischio di mismatch tra documento e build effettiva.	ALTA

4. Roadmap 30 / 60 / 90 giorni

Orizzonte	Obiettivo	Azioni	Indicatore di chiusura
0–30	Ridurre i rischi che hanno priorità alta	Uniformare image verification; avviare SBOM pipeline; definire debug production policy, CVD/contact e vulnerability release gate	Negative update tests superati; policy approvate; checklist release attiva
30–60	Rendere le evidenze ripetibili	SBOM automatica; service inventory; logging security; auth hardening	SBOM collegata a IGOS; inventario servizi; event coverage; test account protections
60–90	Consolidare lifecycle e documentazione	Support period rationale; decommissioning instructions; retest e closure report	Lifecycle memo; docs aggiornate; finding chiusi con evidence ID

5. Decisioni e ownership

Decisione	Owner suggerito	Da completare entro
Confermare HW Rev. B e IGOS 2.4.1 come baseline della remediation	Product + R&D	Kick-off remediation

Decisione	Owner suggerito	Da completare entro
Approvare la modifica della catena update A/B e recovery	Firmware lead	Prima di IGOS 2.5.x
Definire policy di debug/provisioning di produzione	HW + Manufacturing	Prima del nuovo lotto
Nominare owner vulnerability handling e security contact	Management/Product	Prima del 11/09/2026 per il runbook di reporting
Approvare support period rationale e responsabilità di manutenzione	Product/Management	Durante consolidamento lifecycle

Cosa cambia per il management
L'assessment trasforma un tema regolatorio generico in un backlog tecnico assegnabile: prodotto/versione, finding, owner, priorità, evidence richiesta e target release. Questo permette di stimare effort e responsabilità senza confondere assessment tecnico e decisioni legali.

6. Cosa riceve il cliente

Deliverable	Utilizzatore principale	Scopo
Management Summary	Management / Product	Decisioni, priorità, budget, owner
CRA Technical Evidence Pack	R&D / Quality / Compliance	Evidenze tecniche, mapping, finding e closure
SBOM snapshot	R&D / Release / Security	Tracciabilità componenti e dependency monitoring
Findings register	Project/Product owner	Pianificazione e tracking remediation

Supporto Silicon LogiX
Su incarico separato, la stessa analisi può proseguire con implementazione firmware/software, secure update, bootloader, hardening, SBOM automation, logging, vulnerability tooling e verifica di chiusura dei finding.

7. Limitazioni e riferimenti

- Questo documento non certifica la conformità del prodotto e non sostituisce la documentazione tecnica completa del fabbricante.
- I risultati sono validi soltanto per la baseline e il perimetro indicati.
- Gli aspetti legali, la classificazione del prodotto e la procedura di conformità devono essere validati dalle figure competenti.
- Il fac-simile contiene dati inventati e non deve essere presentato come assessment di un cliente reale.

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.