

Tier-1 Internet Exposure Register

Board Summary (Executive View)

What This Is

The Tier-1 Internet Exposure Register is the authoritative, continuously updated record of all externally reachable and identity-adjacent digital exposure surfaces whose compromise would constitute a material enterprise event. It converts internet exposure from an abstract technical risk into an owned, time-bound executive liability.

Why the Board Should Care

Modern enterprise breaches overwhelmingly originate from unknown, weakly authenticated, or third-party fronted internet exposure. Regulatory scrutiny increasingly focuses not on whether incidents occur, but on whether exposure was known, owned, monitored, and acted upon within defined time limits.

What Decisions the Board Is Being Asked to Endorse

1. Formal adoption of the Tier-1 Internet Exposure Register as a required governance control. 2. Mandated executive ownership for every Tier-1 exposure. 3. Approval of maximum acceptable unpatched exposure windows. 4. Requirement for kill-switch or isolation capability for Tier-1 identity-adjacent surfaces. 5. Continuous reporting of longest-open exposures and assumption expiries.

What This Prevents

- Unknown internet exposure • Orphaned ownership and vendor deflection • Open-ended patch delays • Identity blast-radius amplification • Evidence gaps during investigations • Inability to demonstrate due care to regulators

Board-Level Metrics (Reported Quarterly)

- Number of Tier-1 internet-exposed surfaces • Top 10 longest-unpatched exposures • Identity-adjacent Tier-1 exposures • Exposures lacking kill-switch capability • Risk acceptances approaching expiry

Technical Implementation Annex

Purpose

This annex defines the minimum technical controls, data feeds, and operational practices required to keep the Tier-1 Internet Exposure Register accurate, current, and defensible.

Required Data Feeds

- External attack surface discovery (DNS, IP ranges, certificate transparency)
- Cloud control plane inventories
- Identity platform exports (IdP, MFA, token services)
- WAF/CDN configuration state
- Vendor exposure attestations

Automation Rules

- New exposure automatically creates provisional Tier-1 entry
- Missing ownership escalates to default executive owner
- Exposure clocks run continuously until remediated or accepted
- Unverified exposures flagged after 30 days
- All changes logged and immutable

Operational Guardrails

No Tier-1 exposure may exist without an owner, defined patch window, logging enabled, and an isolation or kill-switch strategy. Vendor-hosted exposure does not transfer accountability.

Acknowledgement and Endorsement

By signing below, the undersigned acknowledge review of this document and endorse the Tier-1 Internet Exposure Register as an approved enterprise governance control. Signatures attest to awareness, oversight, and accountability—not delegation of responsibility.

Role	Name	Signature	Date
Board Chair			
Audit / Risk Committee Chair			
Chief Information Security Officer (CISO)			