

## v3.4-SEC-006 – Certification Scorecard, Security KPI & PenTest Disclosure

Document Title	Certification Scorecard, Security KPI & PenTest Disclosure
Version	v3.4
Document ID	v3.4-SEC-006
Date	2025-03-22
Author	Take Back Your Data – Security Standards Office
Document Type	Public / Certification / Internal

### 1. Purpose & Scope

This document defines the certification scoring model, security KPIs and penetration testing disclosure format required for MaxOneOpen forks. It ensures that all certified systems undergo standardized, transparent and repeatable security evaluation.

### 2. Scorecard Structure

- Max score: 70 points (score  $\geq 64$  required for certification)
- Sections include: architecture, runtime, isolation, communication, resilience, audit
- Each item must be verifiable by documentation and runtime trace
- No self-assigned scores allowed; certification requires third-party validation

### 3. Security KPI Definitions

Metric	Target	Certification Trigger
MTTD (Detection Time)	< 60s	Fail if avg > 5min
MTTR (Recovery Time)	< 180s	Fail if avg > 15min
Breach Scope	< 1 twin / user	Fail if lateral escalation
Audit Proof Latency	< 5s	Fail if non-reproducible

### 4. PenTest Disclosure Format

- PenTests must be performed by external party or community DAO
- Report must include: scope, methods, outcome, patch timeline
- All unresolved findings must be disclosed
- Retests are required after architectural changes

### 5. Certification Relevance

Security scorecard, KPI adherence and PenTest disclosure are mandatory for MaxOneOpen certification. No fork can be certified without third-party trace validation and reproducible metric proofs.