

Sky Matrix

Forensic Audit - Conformity Report

Against Sky_Matrix_Forensic_Audit_Report_2026-07-23 | compiled 27 July 2026

Configuration under test: application 2026-07-27-batch80 | licence worker 2026-07-27-batch34

All statements below were verified against the live production copy served from skymatrix.biz, not against the working tree. The check is re-runnable as 8 Working\verify-audit-full.ps1 and reports 46 of 46 assertions passing. The published user guide is verified separately by 8 Working\pdf_tagging.py.

1 Summary

Group	Range	Position	Status
Critical	C-01 to C-04	4 of 4 closed and verified in production	CLOSED
Security	S-01 to S-10	10 of 10 closed and verified in production	CLOSED
Operational	O-01 to O-18	18 of 18 closed and verified in production	CLOSED
Accessibility	Section 10	9 of 9 closed and verified in production	CLOSED

Release position. All 32 numbered findings are closed and verified in production. The audit's release block was raised on the numbered findings together with four governance workstreams: privacy and DPIA, the EFB safety case, WCAG 2.2 AA conformance, and modularisation with a regression corpus. Those remain outstanding and require counsel or operator input rather than code; they are listed in section 6. **This report does not by itself lift the release block.**

2 Critical findings

ID	Finding	What was changed, and why it closes the finding	Status
C-01	Malicious PDF can execute JavaScript in the Sky Matrix origin (CVE-2024-4367).	PDF.js upgraded 3.11.174 to 4.2.67 (patched), loaded as an ES module with CSP origin-pinning. isEvalSupported:false set on all seven getDocument calls as defence in depth. Verified on a real iPad.	CLOSED
C-02	Imported or shared content can execute as same-origin code.	esc() now escapes quotes and backticks as well as angle brackets. The document preview iframe is sandboxed with neither allow-same-origin nor allow-scripts, so an imported HTML or SVG file can no longer reach localStorage, IndexedDB, the licence or the PIN hash.	CLOSED
C-03	TAF engine can issue a false no-hazard conclusion.	The all-clear ternary is gone. Three explicit branches: hazard in window, hazard elsewhere in the TAF, or neither. The last states that this is not an all-clear and points at the raw TAF. Fails safe.	CLOSED
C-04	Revised OFP can erase active-flight state.	Flight identity no longer includes the OFP revision number, so loading a revision keeps captured times, actuals, notes and rest, and raises an alert instead of resetting.	CLOSED

3 Security findings

ID	Finding	What was changed, and why it closes the finding	Status
S-01	Unauthenticated /blocked returned 10 live device IDs with wildcard CORS.	The endpoint now requires a device parameter and returns a boolean for that device only. An unauthenticated caller receives no list.	CLOSED
S-02	Licence and device values appear in sync and FR24 query strings.	The licence code moved out of the query string into the POST body for /sync/get and /fr24/lookup. Query strings are written to edge logs, browser history and Referer headers; the credential no longer travels there. GET is retained temporarily for older installed builds.	CLOSED
S-03	4-digit SHA-256 PIN is brute-forceable; stored content is not encrypted.	PBKDF2-SHA256, 210,000 iterations, salted per device, measured about 108 ms per guess, so the 4-digit space takes roughly 18 minutes and six digits about 30 hours rather than milliseconds. New PINs must be 6 to 8 digits and obvious sequences are refused. Escalating delay after three failures and a 15-minute lockout after ten, persisted so relaunching the app does not reset the allowance. Legacy PINs still verify and are upgraded transparently. 16 of 16 unit tests pass.	CLOSED
S-04	No CSP, frame protection, referrer, permissions or HSTS headers.	Full header set delivered via public/_headers, the only mechanism that reaches Workers Static Assets, since headers set in the router are bypassed for static files.	CLOSED
S-05	PDF.js, Tesseract and Mammoth load without SRI.	SRI added to the classic CDN script. An ES module import cannot carry an integrity attribute, so CSP origin-pinning covers the PDF.js module.	CLOSED
S-06	No robust size, page or count limits for PDFs, images or shared payloads.	Hard limits applied before parsing: 60 MB, 1,200 pages and 400,000 text items across the document. All are far above any real flight plan, and each fails fast with a plain explanation instead of locking the tab.	CLOSED
S-07	Last-seen day can heal downwards; raw device date controls expiry.	The effective day is now the later of the device clock and the highest day ever seen, and that floor is only ever lowered against trusted internet time, never against the device clock it exists to defend against. Rolling the tablet date back no longer revives an expired licence.	CLOSED
S-08	Six-digit share codes require server throttling, expiry and one-time use.	Expiry of 15 minutes and single use were already enforced. Added: 12 accept attempts per device and 30 per IP per 15 minutes, plus a cap of 10 codes minted per device per hour. Walking the 900,000-code space is no longer feasible.	CLOSED
S-09	Service worker can install without the required dependency cache.	Assets split into required and optional. Any required asset failing to cache now rejects the install, leaving the previous good worker in place. The app can no longer report itself offline-ready having cached nothing.	CLOSED
S-10	Background remains focusable and in the accessibility tree behind the lock screen.	The application layer is marked inert and aria-hidden whenever a gate screen is shown, and restored on entry. Tab order, find-in-page and screen readers can no longer reach the briefing behind the lock.	CLOSED

4 Operational findings

ID	Finding	What was changed, and why it closes the finding	Status
O-01	Deltas over 12 hours wrap negative or become unavailable.	elapsedFwd() replaces signed(), using trip time to disambiguate. Sectors longer than 12 hours no longer display as negative or as dashes. Nine unit cases including the 12-hour boundary.	CLOSED
O-02	RVSM and configured checks at the same minute can suppress each other.	dueChecks() returns every check due and they are shown together. Acknowledgement is keyed by kind and minute rather than minute alone, so dismissing a fuel check can no longer silently dismiss an unseen RVSM altimetry check.	CLOSED
O-03	Location starts before an explicit cockpit action or unlock.	A one-time explanation and opt-in before location is touched, the choice remembered, and a persistent Location in use badge whenever the watch is live, which can be tapped to stop it. Arming by hand also records consent.	CLOSED
O-04	Three speed fixes; no altitude, on-ground, accuracy or hysteresis check.	Fixes worse than plus or minus 150 m cannot drive the state machine. Take-off requires at least 60 m climb above the recorded aerodrome elevation, or 60 s above 100 kt where the device reports no altitude, which is longer than any rejected take-off. Landing requires 60 s below 100 kt and below 15,000 ft, so a GPS dropout in the cruise cannot stamp a touchdown. START and LDG remain the primary method.	CLOSED
O-05	Offsets of 12 hours or more are rejected and worst device errors may be unflagged.	The 12-hour rejection is removed. It discarded the correction in precisely the most dangerous case while still displaying internet UTC as verified. Corrections are now applied and a large one is called out as severe, warning that anything captured offline will carry the same error.	CLOSED
O-06	No facility class, augmentation or operator FTL scheme; short-trip wrap.	No window is offered below 90 minutes trip time, and any span longer than trip minus 30 minutes is refused with a reason instead of drawn. The modulo previously wrapped a reversed window into a roughly 24-hour rest plan. An explicit amber notice states that this splits a window and does not assess FTL legality.	CLOSED
O-07	Missing AI coverage can be represented as complete agreement.	A field counts as verified only when both readers produced a value. Fields the AI returned nothing for are listed as cross-check incomplete rather than shown as a clean tick.	CLOSED
O-08	Acceptance key omits OFP number; warnings can be hidden without correction.	The data-quality acceptance key now includes the OFP release, so a revision re-raises its own warnings instead of arriving pre-dismissed. This is deliberately the opposite of C-04: flight identity excludes the release so captured times survive, while acceptance includes it so checks do not.	CLOSED
O-09	Reserve treatment is incomplete and a 3% tolerance may conceal error.	Final reserve, hold and tankered fuel are parsed and summed. Tolerance tightened from 3% of ramp fuel, which is thousands of kilos on a long-haul, to 1% capped at 1,000 kg. Both the tolerance and the components compared are now stated in the message.	CLOSED
O-10	Build errors are swallowed while the briefing may still be declared ready.	The build call is no longer wrapped in a silent catch. A failure is recorded, reported in the status line, and raises a red banner at the top of the briefing stating that the content may be incomplete and must not be used.	CLOSED
O-11	Year ignored, month approximated, categories dropped and results truncated.	Three defects, all producing a green tick on an active NOTAM. The year was captured then discarded, so a 20 DEC to 15 JAN window compared as an end before its own start. wxNow(), which drives the NOTAM chips the pilot taps, supplied a 1-based month against 0-based NOTAM months and dropped the day of month entirely. Now a single absolute ordinal on both sides, the flight year inferred as whichever candidate places it nearest the NOTAM start, reversed windows returning neutral rather than green, an optional end-date year, and no 600-character truncation. 15 unit cases including a	CLOSED

ID	Finding	What was changed, and why it closes the finding	Status
		regression line printing old equals green and new equals red.	
O-12	Fractional and P6SM parsing can misclassify flight category.	P6SM matched nothing and every fraction was hard-coded to 0.5, so quarter-mile LIFR and three-quarter-mile visibility both read as 0.5. Three ordered patterns now handle whole plus fraction, bare fraction and whole values, with M and P prefixes.	CLOSED
O-13	Public CORS proxies add ungoverned operational dependencies.	Retained as a last resort by operator decision, but no longer silent. When a reply arrives via a public relay the weather panel names the host and states that Sky Matrix has no agreement with it and the data is unverified.	CLOSED
O-14	Static or current offsets do not reliably represent scheduled flight dates.	Local time now comes from the browser IANA timezone database for the scheduled instant, rather than a static summer-time offset applied to the current moment. Verified across DST for CDG, LHR, JFK, DOH, KHI and SYD. The static offset survives only as a fallback and anything derived from it is marked approximate.	CLOSED
O-15	Nearest-waypoint and linear fuel fallbacks can materially mislead.	Distance flown is now the position projected onto the route, choosing the leg with the smallest cross-track. The previous nearest-waypoint method was demonstrated 300 NM out mid-route and non-monotonic. Beyond 150 NM cross-track the app declares itself off-route and says so rather than inventing a figure. Plan fuel is interpolated from the nav log printed fuel column instead of a ramp-minus-trip straight line. The card states that every figure is a projection and that the FMS and EICAS are the source of truth.	CLOSED
O-16	n_flow is read instead of nl_flow; actual distance may be omitted.	Corrected to nl_flow. The element referenced never existed, so distance flown was silently absent from the end-of-flight summary.	CLOSED
O-17	Load-another clears localStorage but retains the IndexedDB PDF blob.	The stored OFP document is now deleted before the reload, and the reload waits for that delete to complete. A flight plan carries other crew members' names and rosters, so it must actually be erased.	CLOSED
O-18	Drill codes called classes; no clear edition, source or operator precedence.	Relabelled throughout as ICAO emergency response drill codes and explicitly distinguished from UN hazard classes. The source, the ICAO Doc 9481 structure, is stated together with a standing notice that Sky Matrix holds no controlled copy, tracks no amendments, and that the aircraft ERG and the operator's dangerous goods manual take precedence over anything shown.	CLOSED

5 Section 10 - Accessibility and cockpit human factors

ID	Finding	What was changed, and why it closes the finding	Status
10.1	84 labels, none using for; only four controls wrapped and four aria-labels.	72 labels bound to their controls with a for attribute, giving every one a programmatic name and making the label itself a hit target.	CLOSED
10.2	Four modals lack dialog role, modal state and programmatic title.	All four now carry role=dialog, aria-modal=true and aria-labelledby pointing at their title element.	CLOSED
10.3	Background remains focusable and in the accessibility tree.	Closed together with S-10: the application is inert and aria-hidden behind any gate screen.	CLOSED
10.4	Clickable div elements lack role, tabindex and key handling.	Clickable non-button elements are promoted once and again on every DOM change, receiving role=button, a tab stop and Enter or Space activation, so core functions are reachable without a pointer.	CLOSED
10.5	Only the AI wait uses aria-live.	Nine status and error regions now announce: load status, licence messages, PIN and login errors, restore, received-plan status, GPS hint and nav hint. Assertive for errors, polite for status.	CLOSED
10.6	8.5 to 11 px text and small padding are common.	No type below 11 px remains, with 14 declarations raised. Interactive controls have a 44 px minimum height, and a text-size control scales the whole interface up to 160% for glare, vibration or low vision.	CLOSED
10.7	#5a6b86 on #0e1726 measured about 3.32:1, below the 4.5:1 benchmark.	Both failing tones, measured at 3.32:1 and 4.23:1, replaced with #8296b5 which measures 5.97:1 against the application background. All remaining text tones were re-measured and pass.	CLOSED
10.8	Reduced-motion handling covers only one overlay.	A global prefers-reduced-motion rule now disables all animation, transition and smooth scrolling across the application, and the behaviour is described to the pilot under Display and accessibility.	CLOSED
10.9	Public user guide PDF is not tagged.	The published guide is now a tagged PDF. reportlab has no structure-tree support, so 8 Working/pdf_tagging.py supplies both halves: marked-content sequences written into the page streams as each block is drawn, and a structure tree attached afterwards with pikepdf. The live file carries 62 content-bearing structure elements (12 H1, 9 H2, 29 P and 12 lists as L/LI/LBody), one per visible block, a parent tree indexing every page, a role map, document language en-GB, a document title and DisplayDocTitle so a reader announces the title rather than the filename. Verified against the copy served from skymatrix.biz.	CLOSED

6 Outstanding - governance workstreams

These were raised alongside the numbered findings. None is a code defect; each needs a decision, a document or an external party.

Ref	Workstream	Position	Status
6.1	Privacy notice, DPIA and UK GDPR / PECR control gaps.	Requires legal review of what is collected (email, device identifier, pilot profile, usage counters and position handling) and a published privacy notice and retention schedule. The technical groundwork is in place: position never leaves the device, GPS consent is recorded, and the device-identifier disclosure is closed.	OPEN
6.2	EFB safety case and operator approval evidence.	Requires the operator. Sky Matrix is presented throughout as reference only and subordinate to the released OFP, the FMS and the aircraft ERG, which supports but does not substitute for a safety case.	OPEN
6.3	WCAG 2.2 AA formal conformance.	The section 10 defects are closed, but a formal conformance statement needs an independent audit using assistive technology on the target device.	OPEN
6.4	Modularisation and a regression test corpus.	The application remains a single file with inline scripts, which is why the CSP must still permit unsafe-inline. Unit coverage now exists for the highest-risk logic (NOTAM validity, GPS phase, PIN storage, distance projection, METAR category and long-haul time), and every deploy is gated on a syntax check of all inline script blocks.	OPEN

7 Verification method

- Every claim was checked against the copy served from the public edge with a cache-busting parameter, because edge caches had previously made a good deploy look like a failed one.
- Behavioural logic was unit-tested wherever a string check would not prove correctness: NOTAM validity (15 cases, including a regression line showing the old code returning green for an active NOTAM), PIN storage and throttling (16 cases, including legacy upgrade and measured cost per guess), distance flown along a doglegged route (monotonicity across the whole route), METAR flight category, long-haul elapsed time, and timezone conversion across DST.
- Two verification scripts produced false failures during this work: one matched an explanatory comment rather than the control it described, and one relied on PowerShell variables being case-sensitive, which they are not. Both were corrected, and tests now assert on identifiers and elements rather than prose.
- Endpoints were exercised live where possible. The document-open receipt endpoint was confirmed to accept a well-formed receipt and reject a malformed device, and the admin endpoints were confirmed to return 401 without a token.
- Deploys of the licence worker and the site are issued as separate commands and each is re-verified at the edge after propagation, because chaining them has previously left one deployed and the other silently not.