



The Dead Runtime Problem

CUSS 1, CUSS 2, and the shared liability for airport kiosks after 31 December 2025

IATA deprecated the CUSS 1.x specification on 31 December 2025. Kiosk estates still running it depend on software that no vendor patches, on equipment the airport owns, for applications the airport does not control. Under NIS2 the airport and the airline are each liable, and the estate only becomes supportable when both have moved to CUSS 2.

AUDIENCE	Airline and airport IT, security, procurement, and compliance leadership
SCOPE	Common-use self-service check-in kiosks (CUSS 1.x and CUSS 2)
JURISDICTION	European Union primary; comparable regimes noted
CLASSIFICATION	Public

CONTENTS

1. Table of Contents

2.	<i>SUMMARY.....</i>	<i>3</i>
3.	<i>THE DEPENDENCY.....</i>	<i>4</i>
4.	<i>OWNERSHIP</i>	<i>5</i>
5.	<i>TIMELINE.....</i>	<i>6</i>
6.	<i>NUANCE.....</i>	<i>7</i>
7.	<i>THE STALEMATE.....</i>	<i>8</i>
8.	<i>DIRECTIVE (EU) 2022/2555</i>	<i>9</i>
9.	<i>ENFORCEMENT EXPOSURE.....</i>	<i>10</i>
10.	<i>THE ECONOMICS</i>	<i>11</i>
11.	<i>GLOBAL OUTLOOK</i>	<i>12</i>
12.	<i>NEXT STEPS</i>	<i>13</i>

2. SUMMARY

Summary

IATA deprecated the CUSS 1.x specification on 31 December 2025. Applications and platforms still built to it depend on browser and plugin technologies whose vendors stopped issuing security patches between 2015 and 2023. NIS2 names both the airport managing body and the air carrier as essential entities, and requires each to show that it handles vulnerabilities and manages supply chain risk. Neither can show that on software that nobody patches.

The estate becomes supportable only when the airport has provisioned a CUSS 2 platform and every airline on that platform has migrated its application to it. Until both are true, the airport keeps a deprecated runtime enabled, and every carrier on that estate shares the surface it sits on, including the carriers that have already done the work.

Migrating costs a defined amount once. Not migrating costs an administrative fine scaled to global turnover, a mandated audit at the entity's own expense, and the migration afterwards.

3. THE DEPENDENCY

What are CUSS 1 and CUSS 2?

CUSS, Common Use Self Service, is the IATA standard that lets several airlines share one physical check-in kiosk. The airport provisions a platform on that kiosk. Each participating airline supplies an application that runs on the platform.

CUSS 1.x defined that application as a client built for the browser and plugin technologies of its time. CUSS 2 replaced the model with current web technology: HTML5, WebSocket, OpenAPI, OAuth 2, and TLS 1.2 or later. Those components are maintained, patched, and testable by ordinary security tooling.

Applications built to CUSS 1.x expect a browser and plugin environment that has since been retired in full.

COMPONENT	STATUS	VENDOR SUPPORT ENDED
Internet Explorer 11	End of life	2023
Microsoft Silverlight	End of life	2021
Adobe Flash Player	End of life	2021
Adobe Shockwave	End of life	2019
Oracle Java 7	End of life	2015

End of life means no security patches. A vulnerability disclosed against any of these components today will never be fixed by the party that wrote it. Whatever mitigation exists is a compensating control layered around a defect that stays open permanently, on a device that touches passenger identity documents, passenger name records (PNR) and, at many installations, payment.

WHY THE SHARED MODEL AMPLIFIES THIS

A common-use kiosk carries several airlines on one platform. A single unmigrated application keeps the deprecated runtime enabled for that kiosk, and therefore for every other carrier whose passengers use it, for the airport that owns the equipment, and for the platform vendor that has to support it. One carrier's decision sets the security posture for everyone on the estate.

4. OWNERSHIP

Who owns what on a shared kiosk

A common-use kiosk has three layers, and different parties procure them under different contracts. Confusing the layers is what makes this look like an airline problem.

LAYER	PROVISIONED BY	SUPPLIED BY
Kiosk hardware and peripherals	Airport operator	Kiosk manufacturer
CUSS platform and client runtime	Airport operator	CUSS platform vendor
Check-in application	Each participating airline	Airline or its IT supplier

The deprecated runtimes sit in the middle layer. The airport procures that layer, operates it on its own estate, and keeps it on the older version because airline applications in the layer above still require it. The defective component is therefore on equipment the airport owns, held there by software the airport does not control.

5. TIMELINE

The deadline has already passed

This is often discussed as a future migration. IATA deprecated the CUSS 1.x specification on 31 December 2025, so the first deadline is already behind us.

Deprecation changes the compliance position rather than switching anything off. Kiosks running CUSS 1.x did not stop working, and many are in service today. What changed is that the specification no longer carries the standing of a current standard, while the runtimes it depends on had already lost vendor support years earlier.

Airports set their own dates for withdrawing CUSS 1.x from their estates, and they are under no obligation to wait for any particular carrier. An airline that has not migrated is exposed to a schedule it does not control.

WHAT DEPRECATION DOES TO THE COMPLIANCE ARGUMENT

Before 31 December 2025, an operator running CUSS 1.x was running a current if ageing standard. After that date it is running a specification its own standards body has retired, on runtimes their vendors retired years earlier. Under Article 21 the question a supervisory authority asks is whether the measures are appropriate to the risk. A retired specification on unpatchable components is difficult to defend as appropriate.

6. NUANCE

Not every Airline or Airport is affected

The distinction matters, and it gets lost whenever this subject is raised. It applies on both sides of the house.

Airlines

A meaningful number of carriers have already rebuilt their kiosk applications against CUSS 2 and moved off the deprecated stack. They absorbed the cost and ran the project.

Airports

A number of airports have already provisioned CUSS 2 platforms, and some have set dates for withdrawing CUSS 1.x from their estates. Others have not begun, and a few have no published position.

Neither group should be grouped with the estates that have not moved. An audit exists precisely to tell these populations apart: at a given airport, on a given kiosk, for a given airline application. The answer is rarely uniform across an operator's whole footprint, which is why “we are fine” is not an answer a compliance function can rely on without evidence.

7. THE STALEMATE

Why neither party can fix this alone

An airline can rebuild its application against CUSS 2 and still not deploy it, because the airports it serves have not provisioned a platform that supports it.

An airport can provision a CUSS 2 platform and still have to keep the CUSS 1.x runtime enabled, because one or more carriers on its estate have not migrated. Enabling it for one carrier enables it for the terminal.

Each side waits for a signal from the other, and neither has a commercial reason to move first. The airline sees no point building for a platform that is not there. The airport sees no point withdrawing a runtime its carriers still need. While they wait, the shared estate stays at the security posture of its least migrated tenant, and both parties are separately liable for it.

THE END STATE IS NOT PARTIAL

A CUSS estate is supportable only when the airport has provisioned the CUSS 2 platform and every airline operating on it has migrated its application. Until both halves are true, the airport still runs a deprecated runtime, and every carrier on that estate still shares the surface it sits on. A carrier that migrated early carries the same shared exposure as the carrier that has not started, for as long as the platform has to support both.

This is why the migration is a scheduling problem between parties rather than a technical one. Bridging arrangements exist so that a platform can carry CUSS 2 and CUSS 1.5 applications at the same time, which lets either side move before the other is ready. What bridging does not do is remove the deprecated runtime. It buys an orderly transition, and it only pays off if both sides use the time to finish.

8. DIRECTIVE (EU) 2022/2555

What NIS2 requires

NIS2 names the air transport sector (air carriers, airport managing bodies, and traffic management operators) among its **essential entities**. Four provisions bear directly on the kiosk estate.

Art. 21(2)(e)	Security in acquisition, development and maintenance , including vulnerability handling and disclosure. Difficult to evidence when the upstream vendor stopped issuing fixes years ago.
Art. 21(2)(d)	Supply chain security , covering the security posture of direct suppliers and service providers. The platform an airport buys, and the application an airline supplies onto it, are both this relationship.
Art. 23	Incident reporting on a fixed clock : an early warning within 24 hours, a full notification within 72 hours, and a final report within one month.
Art. 20	Governance and management accountability : Management bodies must approve the risk-management measures, oversee their implementation, and undergo training. This does not delegate to the IT function.

Article 21 applies whether or not an incident has occurred. It is a standing obligation to demonstrate that the measures in place are appropriate and proportionate to the risk, and an estate running unpatchable components on a retired specification is a finding on inspection.

9. ENFORCEMENT EXPOSURE

Where the exposure lands, and what it costs

It lands in more than one place

The airport managing body and the air carrier are separately designated. One incident at one kiosk can therefore produce two regulatory exposures, against two entities, under the same directive, plus a supply chain finding against the platform vendor under Article 21(2)(d).

Contracts between the parties can allocate cost. They cannot allocate the regulatory duty. A supervisory authority looks at the entity it designated, not at that entity's supplier agreements.

What the sanctions are

Art. 34(4)	Essential entities: administrative fines up to €10,000,000 or 2% of total worldwide annual turnover for the preceding financial year, whichever is higher.
Art. 34(5)	Important entities: up to €7,000,000 or 1.4% of total worldwide annual turnover , whichever is higher.
Art. 32	Supervisory and enforcement measures: binding instructions, mandated audits at the entity's expense, orders to bring conduct into compliance, orders to inform affected customers, and public disclosure of the infringement .
Art. 32(5)–(6)	Operational and personal sanctions: suspension of a relevant certification or authorization, and a temporary prohibition on named individuals exercising management functions .

EXPOSURE STACKS

A kiosk compromise that reaches passenger data engages GDPR notification duties and a separate penalty regime with its own turnover-based ceiling, alongside any contractual liability between carrier, airport, and platform vendor. These regimes run in parallel, and satisfying one does not discharge the others.

The financial ceiling is the headline. In practice the measures that concentrate board attention are the mandated audit at the entity's own expense, the published finding, and the possibility of individual management prohibition, because no insurance policy meaningfully transfers them.

10. THE ECONOMICS

Migration is the cheaper side of the ledger

The argument against migrating has always been cost and disruption. That argument was easier to sustain while the counterweight was an abstract risk of compromise. The counterweight is now a retired specification, a named regulatory obligation, and penalties scaled to turnover.

Compare the two sides on their structure rather than on any single number.

MIGRATING: BOUNDED, ONE-TIME	NOT MIGRATING: OPEN-ENDED, RECURRING
• Application rebuild or port onto CUSS 2, or platform provisioning on the airport side • Certification against CUSS 2 and integration testing • Phased rollout and staff familiarization • Scope known in advance, schedulable against existing release cycles • Mostly a software-layer change; in many estates the kiosk hardware is unaffected • Produces the Article 21 evidence as a by-product	• Administrative fines scaled to global turnover, per infringement, per designated entity • Mandated external audit at the entity's own expense • Compensating controls maintained indefinitely against defects nobody will fix • Assessment findings that cannot be closed • Incident response on a 24 and 72-hour statutory clock • Possible suspension of authorization and management prohibition • Airports withdrawing CUSS 1.5 on dates you do not control • The migration still has to happen afterwards

One column is a project with a defined end. The other recurs every year the estate stays as it is, and it does not remove the obligation to migrate; it adds the penalty on top of it.

THE QUESTION FOR THE BOARD

Not what migration costs, but what it costs to migrate now against migrating later plus everything that accrues in between. On those terms, deferral is a financing decision rather than a saving.

11. GLOBAL OUTLOOK

Not a European problem with a European fix

The European Union is first here, and it is not alone. Comparable critical-infrastructure cyber obligations are in force or advancing in several major aviation markets, built on similar logic: designate critical entities, mandate risk management and supply chain assurance, impose reporting deadlines, attach penalties.

UNITED KINGDOM	NIS Regulations and the civil aviation authority's cyber assessment framework, with further legislation widening scope.
AUSTRALIA	Critical infrastructure security legislation placing aviation within its designated sectors.
CANADA	Critical cyber systems protection legislation on closely comparable principles.
SINGAPORE	Cybersecurity Act framework for critical information infrastructure, including transport.
UNITED STATES	Transportation security directives for aviation operators, alongside federal incident reporting requirements.
GULF AND ASIA-PACIFIC	National critical-infrastructure cyber regimes advancing across several major hub markets.
GLOBAL	International civil aviation policy continues to push cyber resilience as a sector-wide obligation.

CUSS itself is a global standard, which makes the operational point simpler than the legal one. An airline runs one kiosk application across every market it serves, and an airport runs one platform for every carrier that touches it. A finding in one European hub describes code and configuration already deployed everywhere else. Remediating once to the strictest applicable standard costs less than remediating to each standard in turn as it arrives.

12. NEXT STEPS

Questions worth asking this quarter

These are deliberately answerable, and they are split by who can answer them. If the responsible party cannot answer from existing records, that gap is the first finding.

For the airport, about the platform you provision

- 01 Which CUSS version does each platform on our estate implement, by terminal and by kiosk?
- 02 Is the CUSS 1.x runtime still enabled anywhere, and which carriers require it?
- 03 What is our published date for withdrawing CUSS 1.5, and have we told our carriers?
- 04 What does our platform vendor contract say about CUSS 1.x support, and for how long?

For the airline, about the application you supply

- 05 Which CUSS version is each of our kiosk applications certified against?
- 06 Which client-side runtime does each application depend on, and when was it last patched?
- 07 Is a CUSS 2 build available today, and what is blocking deployment at each airport?
- 08 Which of the airports we serve have set a CUSS 1.5 withdrawal date?

For both parties, on regulation and governance

- 09 Which of our locations fall under NIS2 or an equivalent regime, and under which classification?
- 10 What compensating controls carry the risk today, and who signed them off?
- 11 Can we produce the Article 21 evidence pack for the kiosk estate if a supervisory authority asks tomorrow?
- 12 Does our incident response plan meet the 24-hour and 72-hour clocks for an incident originating at a shared kiosk, and who notifies whom between airport and airline?
- 13 Has the board reviewed and approved the risk position on this estate, as Article 20 requires?

And one for procurement on both sides: when a new kiosk or platform is offered, ask which CUSS version the software implements and which runtime it depends on. New hardware does not imply new software.

A deprecated interoperability standard should not become a shared regulatory liability.

CUSS 2 has been available for years and CUSS 1.x has been deprecated since December 2025. What has been missing is a reason compelling enough for both sides to schedule the work in the same window. Regulators have supplied one, and they are not confining it to Europe.

Important Notice

Disclaimer and Limitation of Liability

Please read this notice carefully. It applies to the whole of this document and to any summary, presentation, or extract derived from it.

Interpretation, not authority

The commentary in this whitepaper represents Elevation AI's own interpretation and summary of the referenced regulations, directives, and industry specifications as at the date of publication. It is not an official statement of, and has not been endorsed or reviewed by, the European Commission, any national supervisory or competent authority, any civil aviation authority, IATA, or any other standards or regulatory body. Specification status and deprecation dates are as published by the relevant body and are subject to change. Where this document and any official text diverge, the official text governs in all cases.

Not legal, regulatory, or professional advice

Nothing in this document constitutes legal, regulatory, compliance, financial, insurance, or other professional advice, and no attorney-client, advisory, or fiduciary relationship is created by its distribution or by any person reading or relying on it. Regulatory obligations under NIS2 are given effect through national transposition and supervisory practice, and therefore vary by member state and by entity classification.

Independent due diligence is required

Airlines, airport operators, ground handlers, platform providers, and any other reader remain solely responsible for determining their own regulatory classification, obligations, deadlines, and risk exposure. Each organization should carry out its own independent assessment of its estate and obtain advice from qualified legal counsel and security professionals licensed in each jurisdiction in which it operates before taking, or refraining from taking, any action.

No warranty as to accuracy or currency

This document is provided on an “as is” and “as available” basis. While it has been prepared in good faith and with reasonable care, Elevation AI makes no representation or warranty of any kind, express or implied, as to the accuracy, completeness, currency, or fitness for any particular purpose of its contents. Regulations, specifications, product support lifecycles, and enforcement practice change over time, and Elevation AI is under no obligation to update this document to reflect any such change.

Exclusion of liability

To the fullest extent permitted by applicable law, Elevation AI, its affiliates, and their respective directors, officers, employees, and agents accept no responsibility or liability whatsoever for any loss, damage, cost, expense, penalty, fine, claim, or other consequence of any kind, whether direct, indirect, incidental, special, consequential, or arising from loss of profit, revenue, data, business, goodwill, or anticipated savings, suffered by any person or organization acting, or refraining from acting, in reliance on any information contained in this document. Nothing in this notice excludes or limits any liability that cannot lawfully be excluded or limited.

No commitment or offer

This document is provided for general information and discussion purposes only. It does not constitute an offer, a solicitation, a warranty of any product capability, or a contractual commitment of any kind by Elevation AI, and it does not vary the terms of any existing agreement between Elevation AI and any party.

Third-party names and marks

Product names, standards, specifications, and organization names referenced in this document, including CUSS and IATA, are used for identification and factual commentary only, and remain the property of their respective owners. Their use does not imply any affiliation with, sponsorship by, or endorsement from those owners.

SUMMARY OF THIS NOTICE

This whitepaper is Elevation AI's interpretation of the applicable standards and regulations, offered to inform your own assessment. It is not legal advice and it is not a substitute for it. Airlines and airports must conduct their own due diligence and take their own professional advice, and Elevation AI cannot be held responsible for any consequence of any action taken, or not taken, on the basis of this material.

© 2026 ELEVATION AI. ALL RIGHTS RESERVED.