June 2026

Digital Out-of-Home Advertising Cyber Security Framework

Overview of Cyber Threat Scenarios, Security Outcomes and Responsibility Model

1 Contents

2 Version Control

Version	Changes	Author	Date
0.1	Creation of document	Skylight Cyber	12/06/2026
0.2	Addressing feedback	Skylight Cyber	19/06/2026
1.0	Addressed additional feedback and formatting issues	Skylight Cyber	05/08/2026

3 Background

Out-of-Home advertising has changed substantially over the past decade. Australia has been one of the fastest growing markets. What was once largely a market of static printed billboards and posters is now a digital channel, where DOOH screens now receive, store, fetch, and execute digital content from multiple parties across a complex supply chain. Programmatic trading, dynamic creative optimisation, third-party verification, and live data integrations have expanded what can be shown on screens and how quickly campaigns can be changed.

That evolution has brought the industry to a point where getting security right matters commercially, not just operationally. The industry's ability to give advertisers and agencies confidence in that chain, that what was approved is what plays and that it plays safely, is increasingly part of what makes DOOH an attractive and trusted channel.

3.1 Intent of this Framework

The Digital Out-of-Home Advertising Cyber Security Framework (the Framework) establishes shared cyber security expectations across the Australian DOOH supply chain. It is intended to strengthen confidence that campaigns are protected and give industry participants a consistent basis for demonstrating that protection.

The Framework defines the relevant threat landscape, the security outcomes the industry should collectively achieve, and the responsibilities of the parties that create, transfer, approve, schedule and render content. Its focus is the protection of content integrity, delivery chains, player environments and shared industry platforms against DOOH-specific threats.

Historically, supply chain assurance has relied on ISO/IEC 27001, SOC 2 and equivalent mechanisms as evidence that industry participants maintained sound general security practices. For example, SOC 2 is particularly relevant to third-party service providers in the supply chain, such as DSPs, SSPs, verification vendors and other technology platforms, that operate hosted systems or process customer data on an organisation's behalf, which is the operating model the standard is designed to assure. These mechanisms remain valuable baseline assurance, but do not by themselves address the DOOH-specific threats covered by this Framework. The Framework therefore complements, rather than replaces, existing supplier assurance requirements.

3.2 Who is this for

This document is written for OMA member organisations and the broader DOOH supply chain, including media owners, advertisers, media and creative agencies, DCO providers, verifiers, SSPs, DSPs, and CMS vendors. It assumes working familiarity with the DOOH industry but does not assume the reader is a security specialist. More granular technical guidance is provided in the Digital Out-of-Home Advertising Cyber Security Guidelines (hereby referred to as 'Guidelines').

3.3 Structure of this Framework

This Framework is organised into four parts:

- **What this Framework protects**: the assets, content types, delivery pathways, player infrastructure, and shared technology platforms in scope.
- **What this Framework defends against**: the integrity compromise scenarios the Framework is designed to address, including single-screen compromise, fleet-scale compromise, supplier compromise, data feed or CDN poisoning, runtime divergence, and supply chain package tampering.
- **How to protect against the threats**: the four outcomes the industry should collectively achieve to protect content integrity, preserve delivery chain integrity, secure the player environment, and prevent industry-wide compromise.

- **Assigning Responsibilities in the DOOH industry**: how accountability, responsibility, and enabling roles are assigned across the parties that create, modify, transfer, approve, schedule, and render DOOH content.

The Guidelines provides the detailed controls that address these security outcomes, including implementation guidance for how participants should apply them across their systems, workflows, suppliers, and delivery pathways.

3.4 Scope

This Framework is focused on cyber risks that could affect the integrity of what appears on DOOH screens, the chain that delivers content to those screens, the player environment that renders it, or the shared platforms on which the industry depends.

In scope are deliberate or malicious actions that could cause unauthorised content, code, instructions, or data to be displayed or executed. This includes compromise of media owner systems or player devices, compromise of shared suppliers or platforms, tampering with creative packages, manipulation of runtime data feeds or CDNs, and divergence between approved and observed runtime behaviour. While accidental errors are not the primary focus of the threat model, many of the same controls that preserve integrity against malicious action also reduce the likelihood and impact of misconfiguration, incorrect file handling, and unintended runtime behaviour.

Additionally, this Framework is not intended to cover all cyber security obligations of every participant. General corporate IT security, privacy, brand safety, content moderation, and broader operational resilience are out of scope. This includes scenarios where a full corporate or organisational breach of a participant enables screen manipulation, or where a malicious insider acts within their legitimate access rights to affect screen content. These represent general IT security and access governance failures that each participant is expected to manage as a baseline. This Framework addresses the DOOH-specific attack surface: the delivery chain, player environment, content packages, and shared industry platforms.

4 Digital OOH Cyber Security Framework on a Page

This Framework defines what the industry must collectively achieve to protect advertisers' content, delivery chains, player environments, and shared platforms.

Assets to Protect

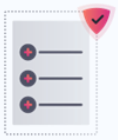
This Framework starts with the assets and workflows that must remain trustworthy for DOOH content to be safely displayed.

Creatives, Files and Packages	Delivery Chains	Player Device Infrastructure	Shared Industry Supplier Environment
Assets, creatives, templates and content packages prepared for display.	The workflows, approvals, transfers and handovers that move content from origin to screen.	The infrastructure and network used to display content.	The shared platforms, suppliers, integrations and services used across the DOOH ecosystem.

Threats to Protect Against

These are the compromise patterns the Framework is designed to prevent, detect, or contain across the DOOH ecosystem.

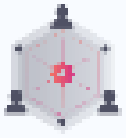
Player Environment Compromise	Shared Supplier Platform Compromise	Content and Delivery Chain Compromise
• Single screen compromise • Multiple-screen compromise	• Mass screen compromise across owners • Supply Chain Tampering	• Data Feed / CDN Compromise • Runtime Behaviour Compromise



Common Industry Security Outcomes to Address Threats and Protect Assets

The security outcomes define what the industry must collectively achieve to protect content, delivery chains, player environments, and shared platforms.

Protect Content Integrity	Preserve Delivery Chain Integrity	Secure the Player Environment	Prevent Industry-wide Compromise
What runs is what was reviewed.	What arrives is what was sent.	The screens stay under the operator's control.	Industry-wide compromise is controlled and prevented.



Roles and Responsibilities to Meet Outcomes

This Framework is applied through the commercial and operational relationships that connect the DOOH supply chain. Principal parties set expectations for the suppliers, platforms, and partners that create, deliver, verify, and display content.

Demand-Side Supply Chain Key Influencer: Advertiser	**Supply-Side Supply Chain** Accountable Principal Party: Media Owner
Influences: Creative Agencies, DCO, Verifiers, Demand-Side Platforms (DSP)	Oversees: CMS Vendors, Player Software Vendors, Supply-Side Platforms (SSP)

5 What the Framework Protects: Assets and Workflows in Scope

This Framework protects four classes of asset in the DOOH ecosystem: the content that flows through the system, the delivery chain that carries it, the player infrastructure that runs it, and the industry-wide technology platforms on which much of this depends. Each is the subject of one of the Framework's four security outcomes.

5.1 DOOH Creatives, Files and Content Package Types

The files below are typical of what is created, transferred, and stored across the DOOH delivery chain. Each type carries an inherent risk profile driven by three properties: whether the file executes code on the player, whether it makes external calls at runtime, and if it can be modified without detection. These properties determine what an attacker can do with each type.

This Framework recognises six content types:

- **HTML creative packages** are bundles of HTML, CSS, JavaScript, and assets that execute at the player.
- **DCO creative containers** are files that can call on stored creatives in external CDNs and/or dynamically pull ad content together on a player.
- **Verification HTML wrappers/containers** are executable packages produced by verifiers to operate alongside creative at play time.
- **Programmatic HTML wrappers/containers** are generated by demand-side platforms at delivery time and orchestrate which pre-approved creative plays.
- **MO-built dynamic content** is composed dynamically by the media owner from feeds they control.
- **Static assets** e.g. image and video files that carry no executable logic.

Each content type introduces or increases the cyber risk to the DOOH industry and is the subject of Outcome 1 (Protect Content Integrity).

5.2 Delivery Chains from Creation to Screen

Content reaches a screen through a chain of parties — originated by one, possibly modified by others in transit, ultimately stored, scheduled, and played by the media owner. The chain is important as it carries integrity risk: any file or package passing through multiple hands creates opportunities for substitution, modification, or tampering between the point of approval and the point of execution.

Three pathways exist in the Australian DOOH ecosystem.

- **Direct delivery pathway**: Creative is commissioned under a direct commercial relationship between the advertiser (or its agency) and the MO, built by a creative or DCO agency, and the package handed to the MO with a window to review it before it is scheduled to a screen. An independent verifier may collect play telemetry for the advertiser.
- **Programmatic delivery pathway**: Creative is pre-approved by the media owner and cached on the player before auction time. Time slots are bought and sold through real-time auctions. The DSP bids on behalf of the advertiser, the SSP runs the auction, and the programmatic wrapper instructs the player which pre-approved creative package to display when the auction resolves. An independent verifier may collect play telemetry for the advertiser.
- **MO-internal delivery pathway**: The MO produces content in-house and runs it on its own screens. No external commercial party is involved.

Each pathway involves a different set of parties, a different set of handovers, and a different chain of custody. The integrity of these pathways is the subject of Outcome 2 (Preserve Delivery Chain Integrity).

5.3 Player Device Infrastructure

Player infrastructure is the system that schedules, manages, and runs content at the screen. It comprises three layers:

- **The physical device** hosting the screen and its computing hardware;
- **The CMS platform** that schedules content, manages playout, and provides the operational surface the media owner administers and;
- **The network** that connects them and, in many architectures, allows the player to fetch content, data, or runtime instructions from external sources during playout.

This infrastructure is the subject of Outcome 3 (Secure the Player Environment).

5.4 Industry-wide Technology and Vendor Environment

Several platforms in the DOOH supply chain serve many parties at once. **CMS vendors** operate the same platform across multiple media owners. **Demand-side and supply-side platforms** intermediate between many advertisers and many media owners. **Verifiers** run detection and measurement infrastructure spanning the industry. **DCO** providers create and coordinate dynamic content ads across multiple screens and media owners. While these platforms appear elsewhere in the Framework as participants or technology enablers in the chain or the player infrastructure, the industry technology and vendor environment represents a shared attack surface that can affect multiple media owners simultaneously.

This shared industry ecosystem is the subject of Outcome 4 (Prevent Industry-wide Compromise).

6 What the Framework Defends Against: Cyber Threat Landscape of the DOOH Industry

The DOOH industry has shifted from delivering static creatives only to delivering code on digital outdoor screens. The increase of programmatic delivery, dynamic creatives, and third-party measurement wrappers all introduce executable content, such as HTML, JavaScript, and runtime data calls, onto player devices that face the public. As a result, this shift has changed the cyber risk profile of the industry materially.

6.1 Threats this Framework is Designed to Counter

While the preceding section defines the assets and workflows this Framework protects, this section defines the threat scenarios that could compromise them. The impact this Framework is concerned with is the integrity of what appears on screen. Confidentiality and availability risks, such as data exfiltration or ransomware, are not the focus and the defining harm in DOOH and this Framework is unauthorised or altered content reaching a public display.

As a result, the scenarios are grouped around three broad compromise patterns: operator-side compromise, shared supplier compromise, and content or file compromise. Together, these scenarios describe the recurring ways unauthorised content, code, instructions, or data could reach a DOOH screen.

Type of Threat	Description	Threat Scenarios	Relevant Assets Affected
Player Environment Compromise	Compromise of systems, credentials, devices, or operational processes controlled by a media owner or operator, enabling an attacker or insider to alter what is displayed on one or more screens and/or compromise the integrity and availability of the player device itself.	S1: Single Screen Compromise S2: Multi-screen compromise via media owner-managed infrastructure or software	Player Device and Environment
Shared Supplier Platform Compromise	Compromise of a supplier, platform, integration, or technology provider used across multiple participants in the DOOH supply chain.	S3: Mass compromise via supplier platform or organisation S6: Supply Chain Tampering	Delivery Chain Industry-wide Technology and Vendor Environment
Content and Delivery Chain Compromise	Tampering with creative assets, HTML/JavaScript, media files, runtime data feeds, or CDN-hosted content before or during delivery to screen.	S4: Data feed / CDN poisoning S5: Runtime Behaviour Divergence S6: Supply Chain Tampering	Creatives, Files and Content Package Types Delivery Chain

6.2 Cyber Threat Scenarios

From these threat types, six recurring patterns of compromise are relevant across the DOOH supply chain. These scenarios are not exhaustive, but they cover the patterns this Framework is designed to address.

Real-world examples that illustrate these patterns are included in Appendix: Real-world Examples. They are provided as contextual examples to show how similar compromise patterns have occurred in digital signage, advertising technology, and related content-delivery environments.

6.2.1 S1: Single screen compromise

An individual screen has its content substituted via physical access to the player, credential compromise, file substitution at the player level, or insider action by someone with legitimate scheduling access. Additionally, it may be compromised to affect its device integrity or availability, such as installation of crypto-miners or botnet recruitment. The commercial impact is limited to that screen. The reputational impact can be substantial if the content is offensive, politically charged, or damaging for an advertiser.

6.2.2 S2: Multi-screen compromise via media owner-managed infrastructure or software

A single compromise of media owner credentials, API keys, fleet management tools, or programmatic scheduling integration propagates to many screens simultaneously. The result is a fleet-scale incident with content appearing across dozens or hundreds of screens at once.

6.2.3 S3: Mass compromise via supplier platform or organisation

A breach of a shared supplier - the CMS vendor's platform, an SSP's platform, or a verifier's back-end - propagates across multiple media owners simultaneously. The result is industry-scale; a single compromise can reach every media owner using that supplier.

6.2.4 S4: Data feed / CDN poisoning

Creative that pulls data from external sources at runtime is fed corrupted, manipulated or unauthorised content. The compromise may occur at the data origin, at a CDN serving the feed, in transit, at a third-party data provider, or through accidental misconfiguration. The screen renders whatever the corrupted feed returns, including content the media owner never approved.

6.2.5 S5: Runtime behaviour divergence

Creative that passed approval review behaves differently when it actually runs in production. The divergence may be deliberate (environment-aware evasion, time-delayed activation, obfuscated payloads, runtime-fetched executable code) or unintentional (silent version updates, behaviour changes after multi-party wrapping). The screen displays content or behaviour that was not part of what was reviewed.

6.2.6 S6: Supply chain package tampering

Creative is modified between the point of approval and the point of execution. The modification may occur in transit, at rest in storage, via email distribution, by same-filename substitution at the destination, through compromise of a supplier's build pipeline, or in programmatic configurations where the creative is fetched at play time with no inspection window. It may also occur through legitimate update mechanisms used to push minor revisions to already-approved creatives, where the update path bypasses the original approval gate. The screen executes something other than what was approved.

Out of Scope Scenarios

Threat scenarios where the mechanism of compromise is a full organisational or corporate breach of a participant, rather than a targeted attack on the DOOH delivery chain itself are out of scope. For example, a ransomware attack that encrypts a media owner's corporate network, or a nation-state intrusion that compromises a supplier's internal systems broadly, may incidentally create a path to screen content, but that path is a consequence of a general IT security failure, not a DOOH-specific threat. Similarly, a malicious insider with legitimate, authorised access to scheduling or CMS systems, acting within their normal access rights, falls outside the threat scenarios this Framework addresses. The controls in this Framework assume that general corporate security, access governance, and insider risk programs are maintained as a baseline by each participant.

7 How to Protect the Industry: DOOH Cyber Security Outcomes

This Framework articulates the outcomes that the industry must collectively action to mitigate and control the risk associated with the six cyber threat scenarios.

There are four overarching outcomes that protect the DOOH advertising supply chain:

- Protect Content Integrity
- Preserve Delivery Chain Integrity
- Secure the Player Environment
- Prevent Industry-wide Compromise

The outcomes aim to protect the end-to-end creative start to digital screen flow, as well as industry-wide security outcomes.

Appendix: Security Outcome to Threat Scenario Mapping further maps each outcome to the six threat scenarios.

7.1 Outcome 1 — Protect Content Integrity

What runs is what was reviewed.

The integrity of what runs on a screen is preserved against deliberate adversarial action. What is displayed, fetched, and executed on a screen matches what was approved at review, and is resilient to attempts to substitute, alter, or subvert it, including by parties that originated the content.

1.1 Approval visibility

A file or package can be independently assessed, or relevant parties can receive adequate attestation to what the file will do before approving it for screens.

1.2 Execution integrity

The code and content executing on the player are what was approved. An external attacker or a compromised staff or upstream party cannot cause different code or content to execute.

1.3 External dependency control

What the file fetches or calls at runtime, internally or externally, is bounded to what was approved, and the data those sources return can be verified as authentic and unaltered between the source and the player.

1.4 Runtime containment

The file's execution is bounded to its intended scope. It cannot break out to affect other content, the player itself, or the broader environment.

1.5 Runtime detection

Divergence between approved behaviour and observed behaviour is detected at play time and reported to parties with the authority to act on it.

7.2 Outcome 2 — Preserve Delivery Chain Integrity

What arrives is what was sent.

The integrity of the file between origin and execution is preserved against deliberate adversarial action. The file delivered to the player can be traced back to the originator's release through a chain of attributable handovers and modifications and is resilient to attempts to substitute or alter it outside that chain.

2.1 Verifiable origin

The originator establishes a verifiable record of the file at release, against which downstream parties can confirm authenticity.

2.2 Custody preservation

At each handover between parties in the chain, the file received matches the file sent. Attempts to substitute or alter the file between parties are prevented or detected.

2.3 Modification visibility

Where a file is modified in transit by parties whose role is to modify it (verifier wrapping, programmatic wrapping, or other approved augmentation), the modifications and their authors are tracked, so that approved modifications can be distinguished from any others.

7.3 Outcome 3 — Secure the Player Environment

The screens stay under the operator's control.

The integrity of the player environment is preserved against deliberate adversarial action. The infrastructure that schedules, manages, and runs content is operated only by authorised parties, and is resilient to attempts to compromise, tamper with, or subvert it.

3.1 Physical integrity

The device's physical state remains as deployed and is resilient to tampering or substitution.

3.2 Player device environment segregation

The systems that schedule, manage, and run content on screens are isolated from the broader environments of the operator or any connected parties, and are resilient to attempts to propagate compromise across that boundary.

3.3 Authorised system access

Access to the systems that schedule, manage, or play content is limited to authorised parties acting within their authorised scope.

7.4 Outcome 4 — Prevent Industry-wide Compromise

Industry-wide compromise is controlled and prevented.

The integrity of DOOH screens and supporting platforms across the industry is preserved against deliberate adversarial action targeting shared infrastructure. Platforms on which multiple parties depend on must enable the controls required for the security outcomes to be delivered and contain compromise so that a breach of any single platform or of a single tenant does not cascade across the industry.

4.1 Control enablement

Shared platforms provide the technical capability required for the security outcomes to be delivered and are resilient to attempts to circumvent them.

4.2 Blast radius limitation

Compromise of a shared platform, or of a single tenant within it, is contained. Its impact does not propagate to other parties.

8 Assigning Responsibilities in the DOOH Supply Chain

8.1 Understanding the DOOH Supply Chain & Chain of Custody

This section identifies the parties and the custody handoffs that define how creative reaches each screen. This was gathered from interviews with various stakeholders conducted in April to June 2026.

The first defines the supply chain itself, that is the parties that combine to deliver creative from development start to screen. The second is the delivery chain and subsequent chain of custody, that is how the creative package moves between those parties, where it changes hands, and where each handoff creates an opportunity for integrity to be preserved or lost.

8.1.1 Supply Chain Participants

The parties in the DOOH supply chain divide into two groups, distinguished by the kind of accountability they hold for what reaches the screen.

8.1.1.1 Principal Parties

These are the parties whose accountability for what reaches the screen cannot be fully transferred to another party. The advertiser owns the brand on the creative and the media owner owns the screen and the audience relationship. They face the audience, regulators, and the public directly when compromise occurs, and they hold the commercial principal position through which the Framework's obligations flow to the rest of the chain.

- *Advertiser*. The brand whose message is being communicated. The advertiser is the originator of intent and the commercial principal for the chain that follows.
- *Media owner*. Operates the physical screen network, the players that drive each screen, the network connecting them, and the workflow that approves what content is permitted to play. The media owner holds the audience relationship and the public-facing brand on the asset.

8.1.1.2 Supply Chain Partners

These are the parties that provide the services or operate the infrastructure required to deliver creative from origination to execution. They are contracted into the chain by one of the principal parties, directly or through programmatic intermediaries, and carry significant technical responsibility for delivering the Framework's outcomes within their domain. This Framework's expectations of these parties are enforced through the contracts the principal parties hold with them.

- *Media agency / Creative agency*: Plans and buys advertising inventory on behalf of the advertiser and designs and produces advertising creative on behalf of the advertiser.
- *DCO provider*: Assembles personalised creative at runtime using data feeds and contextual triggers.
- *Verifier*: Provides independent telemetry or collects telemetry on whether advertising played as intended.
- *SSP (Supply-Side Platform)*: Represents media owners in programmatic auctions and runs the auction and returns the winning ad selection to the player.
- *DSP (Demand-Side Platform)*: Represents advertisers in programmatic auctions and submits bids and supplies and confirms the creative to play if won.
- *CMS vendor*: Provides the platform media owners use to schedule, distribute, and manage content across their player fleets.

8.1.2 Participant's role and accountabilities by demand-side vs supply-side supply chain

The two principal parties hold commercial leverage over a different segment of the supply chain, and accountability follows that leverage.

To ensure that the outcomes are met, it is recommended that each principal party is responsible for influencing or enforcing requirements through their direct and indirect commercial relationships. For instance, the advertiser is responsible for outcomes depending on the demand-side chain and the media owner for those depending on the supply-side chain.

The following table summarises the two segments, the principal party and their commercial relationships.

Supply Chain Segment	Party	Influences
Demand-side *Originates content and routes it to the point of delivery*	Advertiser	• Creative/Media Agency • DCO Provider • DSP (as a fourth party) • Verifier (as a fourth party)
Supply-side *Receives content and delivers it to the screen*	Media Owner	• CMS vendor • SSP

Each principal's accountability or influence is exercised through their contractual relationships with the parties in their segment. They are expected to embed the Framework's outcomes and security controls as security requirements within those contracts, monitor compliance, and manage the residual risk arising from their segment.

8.1.2.1 Overall Oversight and Governance

OMA carries the coordinating responsibility in setting the baseline requirements, promoting adoption, and providing the collective leverage that individual procurement cannot generate alone.

8.1.3 Chain of Custody by Pathways

Chain of custody describes who has practical control over a creative package, wrapper, data dependency, or player environment at each point between creation and display. In this Framework, responsibility follows that control. Each delivery pathway has different custody points, approval windows, runtime dependencies, and commercial relationships, which changes who can prevent, detect, or respond to compromise.

This section summarises the responsibility logic for the three delivery pathways. It does not document every operational process or file transfer method. Those mechanics are set out in Appendix: Understanding of Delivery Chains. For the responsibility model, the key distinction is who controls the asset at approval, at handover, during storage or distribution, and at runtime.

The table below is a summary view that identifies the main party or parties with custody or control in each pathway and the primary Framework outcomes engaged at that point.

This custody view explains why responsibility is not assigned uniformly across all parties. A participant's role depends on whether it originates the content, modifies it, transfers it, stores it, controls the player environment, or operates a shared platform used by others. The next section translates this custody model into accountable, responsible, and enabling roles for each Framework outcome.

Pathway	Segment	Party with custody, control or enabling technology	Asset or control surface	Primary outcome(s)
Direct delivery	Demand-side	• Creative agency / DCO provider	• Original creative package	• Protect Content Integrity
		• Verifier (where it wraps creative)	• Original creative package • Wrapped creative package	• Protect Content Integrity • Preserve Delivery Chain Integrity
	Supply-side	• CMS / player software vendor	• Approved or wrapped creative package • Player and CMS copies • Control of player devices	• Prevent Industry-wide Compromise • Secure the Player Environment
		• Media Owner	• Approved or wrapped creative package • Player and CMS copies	• Protect Content Integrity • Preserve Delivery Chain Integrity • Secure the Player Environment
Programmatic delivery	Demand-side	• Creative agency / DCO provider	• Original creative package	• Protect Content Integrity
		• Verifier (where it wraps creative)	• Original creative package • Wrapped creative package	• Protect Content Integrity • Preserve Delivery Chain Integrity
		• DSP	• Programmatic wrapper / decisioning instructions	• Protect Content Integrity • Preserve Delivery Chain Integrity • Prevent Industry-wide Compromise

	Supply-side	• SSP	• Programmatic wrapper / decisioning instructions	• Protect Content Integrity • Preserve Delivery Chain Integrity • Prevent Industry-wide Compromise
		• CMS / player software vendor	• Approved or wrapped creative package • Programmatic wrapper / container • Player and CMS copies • Control of player devices	• Prevent Industry-wide Compromise • Secure the Player Environment
		• Media Owner	• Approved or wrapped creative package • Programmatic wrapper / container • Player and CMS copies	• Protect Content Integrity • Preserve Delivery Chain Integrity • Secure the Player Environment
MO-internal delivery	Supply-side	• Media Owner	• MO-created creative package • Player and CMS copies	• Protect Content Integrity • Preserve Delivery Chain Integrity • Secure the Player Environment

8.2 Assigned Responsibilities

Responsibility in this Framework follows control, custody, and commercial leverage. A party is accountable where it bears the consequence of failure and has the ability to require controls through its own systems or commercial relationships. A party is responsible where it performs the activity needed to preserve the relevant security outcome. A party is an enabler where it provides the technical capability needed by others.

8.2.1 Summary of Accountable, Responsible and Enabling parties

This section divides the responsibilities into these categories: accountable, responsible, enabler and key influencer.

- *Accountable*: The party that bears the consequence if the outcome fails. The accountable party holds commercial leverage over the parties that perform the work and exercises accountability through contractual enforcement, including translating outcomes into contractual requirements, monitoring compliance, and managing residual risk.
- *Responsible*: The party that performs the action required to deliver the outcome. Multiple parties may share responsibility across different aspects of the same outcome.
- *Enabler*: The party that provides the technical capability without which the responsible party cannot deliver the outcome. The enabler does not perform the action itself.
- *Key Influencer*: The party that exercises influence through procurement requirements, contractual expectations, and supplier selection rather than through direct operational control.

Appendix: Definitions of Participants and Assigned Responsibilities describes the higher-level responsibilities of each participant. Further specific security control requirements will be documented in more detail in the Guidelines.

8.2.1.1 Outcome 1 — Protect Content Integrity

Accountability for content integrity follows the chain. The advertiser commissions production can influence what their chain produces. The media owner operates the screen and is accountable for what executes there. At the boundary where a file is presented for approval and accepted onto a screen both accountable parties and their chains must contribute: the producer makes the file assessable, and the media owner operates the gate and the runtime that holds the producer to what was approved.

Beyond the gate, control over what the content fetches, what it can reach within the player, whether data returned by those sources is authentic and unaltered, and whether divergence is detected at play time rests with the media owner.

Sub-outcome	Accountable	Responsible	Enabler
1.1 Approval visibility	• Advertiser (Key Influencer) • Media Owner	• Media Owner	• Creative Agency • DCO • Verifier
1.2 Execution integrity	• Advertiser (Key Influencer) • Media Owner	• Creative Agency • DCO • Verifier	• CMS / player software vendor
1.3 External dependency control	• Advertiser (Key Influencer) • Media Owner	• Creative Agency • DCO • Verifier	• CMS / player software vendor
1.4 Runtime containment	• Media Owner	• Media Owner	• CMS / player software vendor

1.5 Runtime detection	• Media Owner	• Media Owner	• CMS / player software vendor

8.2.1.2 Outcome 2 — Preserve Delivery Chain Integrity

Accountability for delivery chain integrity follows the chain. The advertiser commissions origination and needs assurance for what their chain produces and passes downstream. The media owner receives the file and is accountable for its preservation through the supply-side chain to the screen. Every party that holds the file during its passage is a custodian during that segment, preventing substitution while it sits with them and detecting substitution at handover. Where parties whose role is to modify the file in transit do so (e.g. the verifier wrapping for verification, the DSP wrapping for programmatic delivery) they attest to those modifications so downstream custodians can distinguish approved augmentation from any other change.

Sub-outcome	Accountable	Responsible	Enabler
2.1 Verifiable origin	• Advertiser (Key Influencer) • Media Owner	• Creative agency • DCO • DSP • SSP • Verifier	• N/A
2.2 Custody preservation	• Advertiser (Key Influencer) • Media Owner	• Creative agency • DCO • DSP • SSP • CMS Vendor	• N/A
2.3 Modification visibility	• Advertiser (Key Influencer) • Media Owner	• Verifier	• N/A

8.2.1.3 Outcome 3 — Secure the Player Environment

The player environment sits entirely on the media owner's side of the chain. The media owner operates the physical security of the device, the segregation between the screen systems and the broader environments they connect to, and access control over who can schedule, manage, or play content. Where other parties connect into this environment (e.g. the CMS vendor as platform operator, the verifier when extracting play data) they operate segregation on their side of the boundary so that compromise in their broader corporate environment is not exposed through the integration.

Sub-outcome	Accountable	Responsible	Enabler
3.1 Physical integrity	• Media Owner	• Media Owner	• N/A
3.2 Player device environment segregation	• Media Owner	• Media Owner • Player software vendor	• N/A
3.3 Authorised system access	• Media Owner	• Media Owner	• CMS/player software vendor

8.2.1.4 Outcome 4 — Prevent Industry-wide Compromise

Industry-wide compromise is a different failure mode from compromise of any single chain. The risk arises where many parties depend on the same platform — a CMS, a DSP, an SSP, a verifier — and a single breach can cascade across them. Accountability is shared in two forms: shared platform providers are accountable for the security and containment properties of the platforms they operate and media

owners and advertisers are accountable for using procurement and contractual leverage to require those properties from the providers they depend on.

Sub-outcome	Accountable	Responsible	Enabler
4.1 Control enablement	• Media Owner • Advertiser (Key Influencer) • CMS / player software vendor • DSP • SSP • Verifier	• CMS / player software vendor • DSP • SSP • Verifier	• N/A
4.2 Blast radius limitation	• Media Owner • CMS / player software vendor • DSP • SSP • Verifier	• CMS / player software vendor • DSP • SSP • Verifier	• N/A

9 From Framework to Implementation

This Framework defines what the DOOH industry needs to protect, the compromise scenarios the industry should plan for, and which parties are accountable, responsible, or enabling for each security outcome.

The Guidelines translates this model into practical control guidance. It sets out the specific controls expected for each outcome, the implementation tiers for those controls, and the artefacts participants can use to demonstrate execution, including attestations, vendor questionnaires, evidence expectations, and testing scopes.

Participants should use this Framework as the reference model for accountability, and Guidelines as the operational playbook for implementation. Together, the two documents provide the DOOH industry with a common language for cyber risk, a consistent set of expectations across the supply chain, and a practical path for improving security without requiring each party to solve the same problem independently.

10 Appendix: Real-world Examples

This appendix provides public examples and adjacent cyber incidents that illustrate the threat scenarios used in the Framework. Some examples are direct DOOH or digital signage incidents. Others are close analogues from web advertising, CDN compromise, or software supply chain compromise where the same technical pattern applies to DOOH.

These examples show three practical lessons for the Framework. First, public-facing screens create reputational impact even when only one device is affected. Second, the systems that manage or distribute content create a much larger blast radius than the screens themselves. Third, executable content and runtime dependencies change the assurance problem from "was this file reviewed" to "is the content that runs on the player still the content that was reviewed".

10.1 Digital billboard, Brisbane, 2022

Maps to: S1 - Single screen compromise

In November 2022, a digital billboard on Milton Road in Brisbane displayed inappropriate content for several minutes on a Sunday morning before the operator's technicians shut it down. Public reporting described a single affected screen, but the incident generated national media coverage because the content was displayed in a public, high-traffic location.

Why it matters for DOOH. A single-screen incident may have limited operational scale, but public exposure can be immediate. The practical causes can include physical access to the player, weak local administration controls, exposed remote access, compromised credentials, or insider misuse. The incident illustrates why individual player devices still require physical integrity, local hardening, and rapid takedown capability even where broader platform controls are strong.

10.2 Fast-food chain digital menu board compromise, Canada, 2025

Maps to: S2 - Mass compromise via operator-managed infrastructure

In April 2025, Mary Brown's, a Canadian quick-service restaurant chain, reportedly had menu boards and drive-through screens across approximately 300 stores display political messages simultaneously. Public reporting attributed the incident to a breach affecting a third-party digital signage provider used to operate the chain's in-store screen estate.

Why it matters for DOOH. Although this was retail digital signage rather than roadside DOOH, the impact pattern is directly relevant: one control plane or signage management integration was able to affect many public-facing screens at once. For a media owner, the equivalent path would be the compromise of CMS credentials, fleet management tooling, scheduling integrations, API keys, or deployment workflows that can push content to a large screen estate.

10.3 Compromise of trusted external library through online advertising company, 2019

Maps to: S3 - Mass compromise via supplier infrastructure, S6 - Supply chain package tampering

In January 2019, Magecart Group 12 compromised Adverline, a French online advertising company, by injecting skimming code into a third-party JavaScript library Adverline provided for retargeting advertising. Every e-commerce site that embedded Adverline's script automatically loaded the malicious code on the next request, and the skimmer harvested payment card details from checkout forms across the customer base before discovery.

Why it matters for DOOH. Adverline's role as a supplier concentrated the risk as it produced the library, distributed it through its own infrastructure, and held the implicit trust of every consumer embedding its tag. DOOH suppliers (CMS vendors, SSPs, media agencies, verifiers) sit in the same position, controlling

either or both the artefacts they produce (creative packages, wrappers, bundled libraries) and the infrastructure that distributes them (multi-tenant platforms, auction backends, tag-serving systems). Compromise at either point lets altered code reach every consuming player through legitimate channels, with no compromise of the player or a media owner's infrastructure required. The consequences depend on where the compromise sits. Supplier-level compromise enables manipulation of scheduling, decisioning, telemetry, and verification data across every tenant, plus exfiltration of supplier-held data. Package-level compromise enables arbitrary code execution on every consuming player, ranging from altered content through to reconnaissance, beaconing, exfiltration, breakout from the rendering context, lateral movement, and persistence on the device.

10.4 Trusted News Source Feed Compromise, 2013

Maps to: S4 - Data feed / CDN poisoning

In April 2013, attackers compromised the Associated Press Twitter account and posted a false breaking news update claiming explosions at the White House had injured President Obama. The post came from a trusted news source and was consumed by automated trading systems within seconds, briefly wiping around US$136 billion from the S&P 500 before the hoax was identified.

Why it matters for DOOH. The same pattern applies to dynamic DOOH content where screens automatically render information, templates, scripts, or assets from a trusted upstream source. If an attacker compromises a data feed, CDN-hosted asset, hosted template, or other runtime dependency, they can cause screens to display content that was never approved, such as a fake headline, altered price, manipulated weather alert, or substituted creative element. The player and CMS may behave as designed, but the trusted source they retrieve from is no longer trustworthy.

10.5 Web malvertising and cloaking

Maps to: S5 - Runtime behaviour divergence, S6 - Supply chain package tampering

The web advertising industry has seen ad cloaking for years. In these campaigns, an ad creative or landing page appears benign during review but behaves differently once live, often based on time, geography, browser properties, referrer, sandbox indicators, or the identity of the reviewer. The same technical pattern is relevant to DOOH wherever HTML creatives, verification tags, DCO logic, or programmatic wrappers execute code on the player.

Why it matters for DOOH. In DOOH, the objective is not necessarily end-user malware. The more relevant objectives are unauthorised content display, unauthorised audience or measurement data collection, evasion of media owner review, runtime fetching of unapproved code, or interference with the player or CMS environment. This is why approval-time review alone is insufficient for executable creative. Runtime controls and runtime detection are required to confirm that what plays matches what was approved.

11 Appendix: Security Outcome to Threat Scenario Mapping

Sub-Outcome	S1 Single Screen Compromise	S2 Multi-screen Compromise via MO	S3 Mass Compromise via Supplier	S4 Data Feed/CDN Poisoning	S5 Runtime Behaviour Divergence	S6 Supply Chain Tampering
Protect Content Integrity						
1.1 Approval visibility					●	●
1.2 Execution integrity					●	
1.3 External dependency control				●	●	
1.4 Runtime containment					●	
1.5 Runtime detection					●	
Preserve Delivery Chain Integrity						
2.1 Verifiable origin						●
2.2 Custody preservation			●			●
2.3 Modification visibility			●			●
Secure Player Environment						
3.1 Physical integrity	●					
3.2 Player device environment segregation		●	●			
3.3 Authorised system access	●	●	●			
Prevent Industry-wide Compromise						
4.1 Control enablement	●	●	●	●	●	●
4.2 Blast radius limitation			●			

12 Appendix: Understanding of Delivery Chains

12.1 Direct delivery pathway

Custody in direct delivery is short and linear. A creative agency or DCO provider creates the original creative package and transfers it to the media owner, either directly or through a verifier that wraps the creative for measurement. The media owner then holds custody through approval, storage, scheduling, distribution to players, and playout. The CMS or player software vendor may provide the enabling technology for storage, distribution, and player control, but the media owner controls the operational pathway.

12.1.1 Direct delivery - verifier wraps creative

Parties involved:

- Creative agency (may include DCO)
- Media Owner
- Verification provider

#	Process	Parties involved	Custody or control surface
1	Creative package is created	Creative agency / DCO	Original creative package
2	Creative package is uploaded to verifier platform or transferred to verifier for wrapping	Verifier	Original creative package Wrapped creative package
3	Media owner receives or downloads wrapped creative package from verifier	Verifier Media owner	Wrapped creative package
4	Media owner approves, stores, schedules, distributes, and plays the creative	Media owner CMS / player software vendor (enabling technology)	Approved or wrapped creative package Player and CMS copies Control of player devices

12.1.2 Direct delivery - verifier does not hold content custody

Parties involved:

- Creative agency (may include DCO)
- Media owner

#	Process	Parties involved	Custody or control surface
1	Creative package is created	Creative agency / DCO	Original creative package
2	Creative package is transferred directly to media owner or uploaded to media owner-controlled CMS	Media owner	Original creative package
3	Media owner approves, stores, schedules, distributes, and plays the creative	Media owner CMS / player software vendor (enabling technology)	Approved creative package Player and CMS copies Control of player devices

Pathway-intrinsic properties:

- The MO has a review window before the creative plays, and conducts that review with full knowledge of which advertiser and creative agency authored the file
- Creative is scheduled by the MO and played at fixed times

12.2 Programmatic delivery pathway

In the programmatic pathway, creative is approved and cached before auction time, while runtime selection is driven by programmatic wrappers, containers, or decisioning instructions. The DSP bids on behalf of the advertiser, the SSP resolves the auction for the media owner's inventory, and the player renders a pre-approved cached creative or container according to the runtime instruction it receives.

12.2.1 Programmatic onboarding - creative approval and cache population

Parties involved:

- Creative agency / DCO
- DSP / SSP
- Media owner and verifier, where applicable

#	Process	Parties involved	Custody or control surface
1	Creative package is created	Creative agency / DCO	Original creative package
2	Creative package is submitted through programmatic or verifier workflow for media owner pre-approval	DSP / SSP Verifier, where it wraps creative	Original creative package Wrapped creative package, where applicable
3	Media owner reviews and approves creative as eligible for programmatic display	Media owner	Approved or wrapped creative package
4	Media owner or CMS caches approved creative to player devices before auction time	Media owner CMS / player software vendor (enabling technology)	Approved or wrapped creative package Player and CMS copies Control of player devices

12.2.2 Programmatic auction and runtime decisioning

Parties involved:

- DSP
- SSP
- Media owner

#	Process	Parties involved	Custody or control surface
1	DSP bids into SSP auction on advertiser's behalf	DSP SSP	Auction and decisioning data No creative file transfer
2	SSP resolves auction and produces runtime decisioning	SSP DSP, where applicable	Programmatic wrapper / container Decisioning instructions

	instruction or programmatic wrapper / container		
3	Programmatic wrapper / container is delivered to media owner, CMS, or player environment	SSP / DSP Media owner CMS / player software vendor (enabling technology)	Programmatic wrapper / container
4	Media owner or CMS distributes wrapper / container to player devices	Media owner CMS / player software vendor (enabling technology)	Programmatic wrapper / container Player and CMS copies Control of player devices
5	Wrapper / container calls DSP or SSP at runtime for playback instructions	DSP / SSP Media owner player environment	Runtime decisioning instructions External dependency
6	Player renders the cached approved creative according to the runtime instruction	Media owner CMS / player software vendor (enabling technology)	Cached approved creative package Programmatic wrapper / container Player environment

Pathway-intrinsic properties:

- The MO has a review window before the creative plays
- The programmatic HTML wrapper is the active code surface at runtime, while the creative could be static or dynamic. The wrapper executes on the player, makes a runtime call back to the DSP/SSP for selection instructions, and pulls a cached creative for display. The creative is essentially "as-approved" provided cache integrity holds.

12.3 MO-internal delivery pathway

In the MO-internal pathway, the media owner creates content in-house and runs it on its own screens. There is no external originator and no external handover in the content chain, but the media owner still relies on its CMS, player devices, and any supporting vendor technology to store, schedule, distribute, and render the content.

Parties involved: Media owner. CMS / player software vendor may be an enabling technology provider.

#	Process	Party(ies) involved	Custody or control surface
1	Media owner creates creative package internally	Media owner	MO-created creative package
2	Media owner approves, stores, schedules, distributes, and plays the creative	Media owner CMS / player software vendor (enabling technology)	MO-created creative package Player and CMS copies Control of player devices

Pathway-intrinsic properties:

- The MO is both author and operator
- Without external commercial leverage, internal separation of duties (between the team building the content and the team approving it) becomes the substitute control

13 Appendix: Definitions of Participants and Assigned Responsibilities

This appendix provides a participant view of the responsibility model. It lists the outcomes and sub-outcomes for which each participant is accountable, responsible, or an enabler.

13.1 Advertiser

The advertiser is the principal party on the demand side. Its influence is exercised through the parties it commissions or selects to create, package, verify, and place creative into the delivery chain.

Role	Sub-outcome	What the party should do
Key Influencer	1.1 Approval visibility	Require the creative agency, DCO provider, verifier, and other demand-side partners to provide enough information for the media owner to assess the creative before approval. This includes declaring executable code, runtime calls, data sources, external dependencies, and any wrapping or modification applied before handover.
Key Influencer	1.2 Execution integrity	Ensure the demand-side chain produces creative that executes consistently with what was submitted for approval. The advertiser should require its partners to prevent hidden code, unauthorised substitution, and post-approval changes that would alter what runs on the player.
Key Influencer	1.3 External dependency control	Require demand-side partners to identify and control the external feeds, scripts, APIs, CDNs, and hosted assets the creative depends on at runtime. The advertiser should ensure those dependencies are approved, stable, and not capable of changing the screen output outside the agreed behaviour.
Key Influencer	2.1 Verifiable origin	Require the originator of the creative to create a verifiable record of the released file or package. This record should allow downstream parties to confirm that the artefact they receive is the one released by the demand-side chain.
Key Influencer	2.2 Custody preservation	Ensure demand-side partners protect the creative while it is in their custody and during handover to the media owner, SSP, DSP, verifier, or other recipient. The advertiser should require controls that prevent or detect substitution before the creative leaves the demand-side chain.
Key Influencer	2.3 Modification visibility	Require any party that modifies, wraps, optimises, or packages creative to make those changes visible and attributable. The media owner and other downstream parties should be able to distinguish approved augmentation from unauthorised tampering.
Key Influencer	4.1 Control enablement	Select agencies, DCO providers, DSPs, verifiers, and other demand-side suppliers that can support the Framework's control requirements. The advertiser should translate the relevant outcomes into contractual and procurement requirements for its supplier chain.

13.2 Media owner

The media owner is the principal party on the supply side and operates the screen estate, CMS workflow, player environment, and approval gate. Its accountability is broad because it controls the environment in which content is accepted, scheduled, and rendered.

Role	Sub-outcome	What the party should do
Accountable and responsible	1.1 Approval visibility	Operate the approval gate and define what evidence is needed before content is approved for screen. The media owner should require visibility of executable code, external dependencies, data feeds, wrapping, runtime calls, and other behaviour that may affect what appears on the screen.
Accountable	1.2 Execution integrity	Ensure the content accepted onto the screen estate is the content that executes on the player. The media owner should operate controls that prevent unauthorised replacement, stale or altered cached copies, and unapproved changes after approval.
Accountable	1.3 External dependency control	Set boundaries for what approved content may fetch, call, or execute at runtime. The media owner should require dependencies to be declared and should use network, player, and CMS controls to restrict content to approved sources.
Accountable and responsible	1.4 Runtime containment	Ensure creative execution is constrained to its intended scope and cannot interfere with other content, the player, CMS integrations, or the broader network. The media owner should implement sandboxing, least privilege, network restrictions, and isolation appropriate to the player environment.
Accountable and responsible	1.5 Runtime detection	Detect when content behaves differently from what was approved or expected at play time. The media owner should monitor player behaviour, runtime calls, content execution, and screen output where feasible, and ensure alerts reach teams with authority to act.
Accountable	2.1 Verifiable origin	Require a verifiable origin record before accepting content into the supply-side chain. The media owner should validate that the received package, or an attestation about it, can be traced back to the party that released it.
Accountable	2.2 Custody preservation	Protect content while it is in the media owner's systems, CMS, storage, and player fleet. The media owner should prevent or detect substitution during upload, approval, storage, scheduling, distribution, cache population, and playout.
Accountable	2.3 Modification visibility	Ensure any approved modification after receipt is recorded, attributable, and distinguishable from tampering. This includes internal edits, format conversion, wrapper changes, programmatic packaging, and other workflow changes before playout.
Accountable and responsible	3.1 Physical integrity	Protect player devices and screen infrastructure from physical tampering, replacement, unauthorised local access, and unauthorised peripherals. The media owner should maintain

		deployment records, tamper controls, and operational procedures to identify and respond to physical compromise.
Accountable and responsible	3.2 Player device environment segregation	Keep player systems isolated from broader corporate, supplier, and third-party environments except through controlled pathways. The media owner should segment networks, restrict management channels, and prevent compromise from propagating into or out of the player environment.
Accountable and responsible	3.3 Authorised system access	Limit access to CMS, scheduling, player management, APIs, and operational tooling to authorised users and systems acting within their required scope. The media owner should enforce strong authentication, role-based access, privileged access controls, and auditability.
Accountable	4.1 Control enablement	Procure and operate CMS, player, SSP, verification, and other supply-side platforms that can support the Framework's control requirements. The media owner should require suppliers to provide the technical controls needed for approval, integrity, containment, detection, and auditability.
Accountable	4.2 Blast radius limitation	Require shared platforms and integrations to limit the impact of a supplier, tenant, credential, or integration compromise. The media owner should ensure supplier platforms cannot allow compromise of one customer, campaign, or integration to cascade across the screen estate or the wider industry.

13.3 Media agency / Creative agency

The media agency or creative agency is responsible for the creative artefact it produces or manages. This includes making the creative assessable, preserving its integrity before handover, and ensuring executable behaviour and external dependencies are consistent with what is presented for approval.

Role	Sub-outcome	What the party should do
Enabler	1.1 Approval visibility	Provide the information needed for the media owner and advertiser to understand what the creative will do before it is approved. This includes documenting code, assets, data sources, external calls, dynamic behaviour, and any third-party components included in the package.
Responsible	1.2 Execution integrity	Build and release creative so that the code and content executed on the player match what was submitted for approval. The agency should prevent unauthorised code insertion, hidden runtime behaviour, post-approval substitution, and uncontrolled updates.
Responsible	1.3 External dependency control	Use only approved and declared external dependencies in the creative. The agency should vet external dependencies and avoid uncontrolled third-party scripts, unstable hosted assets, or runtime calls that could change what appears on screen without re-approval and ensure external dependencies support integrity verification of the data they return.
Responsible	2.1 Verifiable origin	Create or support a verifiable release record for the creative package. Downstream parties should be able to confirm that a received file matches the agency's released version.

Responsible	2.2 Custody preservation	Protect creative while it is being built, stored, exported, and transferred to the next party. The agency should use controlled repositories, access controls, secure transfer methods, and checks that prevent or detect substitution before handover.

13.4 DCO provider

The DCO provider constructs or personalises creative using data inputs. Its responsibilities arise where that logic, its external dependencies, or its custody of creative can change what the player ultimately renders.

Role	Sub-outcome	What the party should do
Enabler	1.1 Approval visibility	Explain how the DCO logic determines what appears on screen and what inputs influence that decision. The provider should make templates, decision rules, runtime calls, data feeds, and fallback behaviour visible enough for approval.
Responsible	1.2 Execution integrity	Ensure the DCO package and runtime logic execute as approved and cannot be altered to produce unauthorised creative variants. The provider should control template changes, code releases, and version updates that affect screen output.
Responsible	1.3 External dependency control	Control the data feeds, APIs, CDNs, scripts, and hosted assets used by the DCO package at runtime. The provider should validate inputs, restrict sources, define safe fallback behaviour, and prevent upstream data changes from causing unauthorised screen content.
Responsible	2.1 Verifiable origin	Create a verifiable record of the DCO package, template, or configuration released into the delivery chain. This allows downstream parties to confirm the package and configuration they receive are the approved versions.
Responsible	2.2 Custody preservation	Protect packages, templates, and configurations while they are stored or transferred through the DCO platform. The provider should prevent or detect unauthorised modification of any artefact that affects what the player renders.

13.5 Verifier

The verifier provides independent measurement or confirmation of what played. Where verification is tag-based or otherwise executes code with the creative, the verifier also affects runtime behaviour and shared-platform risk.

Role	Sub-outcome	What the party should do
Enabler	1.1 Approval visibility	Make verification code, tags, wrapping behaviour, data collection, and runtime calls visible to the media owner and advertiser before approval. The verifier should provide enough detail for parties to assess what the wrapper does when it runs on the player.
Responsible	1.2 Execution integrity	Ensure verification code executes only the measurement behaviour that was approved. The verifier should prevent unauthorised tag changes, hosted script substitution, and runtime logic that changes creative display or player behaviour beyond the agreed scope.

Responsible	1.3 External dependency control	Control the verifier-hosted services, scripts, APIs, and telemetry endpoints that the verification code calls at runtime. The verifier should ensure those dependencies cannot be used to alter creative output or introduce unapproved behaviour and ensure the integrity of data returned by verifier-hosted endpoints can be verified by downstream parties.
Responsible	2.1 Verifiable origin	Where the verifier releases a wrapper or tag, establish a verifiable record of the wrapper and the original creative it was applied to. This supports downstream confirmation that the wrapper is the approved verifier output.
Responsible	2.3 Modification visibility	Record and attest to any modification, wrapping, or augmentation applied to creative for verification purposes. The verifier should make its changes attributable so the media owner can distinguish approved wrapping from tampering.
Accountable and responsible	4.1 Control enablement	Operate verification platforms that support the Framework's integrity, visibility, and runtime control requirements. The verifier should provide customers with the controls and evidence needed to safely use verification tags, APIs, and telemetry services.
Accountable and responsible	4.2 Blast radius limitation	Design and operate verifier platforms so that compromise of one tenant, campaign, tag, or backend component does not cascade to other media owners or advertisers. The verifier should isolate tenants, protect hosted scripts, and limit the reach of platform-level compromise.

13.6 SSP (Supply-Side Platform)

The SSP operates supply-side programmatic infrastructure and is a custodian for programmatic delivery. It is also a shared platform whose compromise could affect multiple media owners.

Role	Sub-outcome	What the party should do
Responsible	2.1 Verifiable origin	Preserve the link between programmatic creative, its approved identity, and the party that submitted or authorised it. The SSP should support evidence that the creative or wrapper offered to the media owner is the one approved for that campaign or demand path.
Responsible	2.2 Custody preservation	Protect creative, wrappers, auction outputs, decisioning instructions, and delivery metadata while they are in the SSP's custody. The SSP should prevent unauthorised substitution or manipulation between bid resolution and delivery to the media owner or player environment.
Accountable and responsible	4.1 Control enablement	Provide the controls needed for media owners to enforce approval, integrity, auditability, and safe programmatic delivery. This includes tenant controls, access controls, integrity checks, logging, and clear integration boundaries.
Accountable and responsible	4.2 Blast radius limitation	Contain compromise within the affected tenant, campaign, integration, or component. The SSP should prevent a breach of one buyer, seller, credential, API integration, or platform service from affecting unrelated media owners or campaigns.

13.7 DSP (Demand-Side Platform)

The DSP operates demand-side programmatic infrastructure and can affect the origin, custody, and runtime selection of programmatic creative.

Role	Sub-outcome	What the party should do
Responsible	2.1 Verifiable origin	Maintain a verifiable relationship between the advertiser, approved creative, campaign, and bid activity. The DSP should ensure creative submitted into the programmatic chain can be traced to an authorised demand-side release.
Responsible	2.2 Custody preservation	Protect creative assets, wrappers, campaign configurations, bid logic, and decisioning instructions while they are held or generated by the DSP. The DSP should prevent unauthorised substitution, campaign hijacking, or manipulation of what is selected to play.
Accountable and responsible	4.1 Control enablement	Provide the controls required for advertisers and downstream parties to use programmatic delivery safely. This includes access control, campaign-level integrity, audit logging, controlled creative updates, and integration controls with SSPs and verification providers.
Accountable and responsible	4.2 Blast radius limitation	Limit the impact of compromise of a buyer, campaign, credential, API integration, or DSP service. The DSP should prevent one compromised tenant or component from influencing unrelated campaigns, advertisers, SSP integrations, or downstream media owners.

13.8 CMS / player software vendor

The CMS or player software vendor provides the platform capability used to schedule, manage, distribute, and render content. Its role is strongest where platform capabilities enable controls or where a shared platform could create industry-wide exposure.

Role	Sub-outcome	What the party should do
Enabler	1.2 Execution integrity	Provide CMS and player capabilities that allow media owners to ensure approved content is the content that executes. This may include integrity checks, controlled deployment, versioning, cache validation, and prevention of unauthorised local or remote substitution.
Enabler	1.3 External dependency control	Provide technical mechanisms for media owners to restrict and monitor what content can fetch, call, or execute at runtime and mechanisms to verify the integrity of data returned by external sources before it is rendered. This may include allow-listing, network controls, content security controls, logging, and policy enforcement at the player or CMS layer .
Enabler	1.4 Runtime containment	Provide player software architecture that constrains creative execution and limits access to the operating system, other content, player management functions, and the broader

		network. The vendor should support sandboxing, isolation, and least privilege by design.
Enabler	1.5 Runtime detection	Provide telemetry and detection capability that helps media owners identify divergence between approved and observed runtime behaviour. This may include player logs, runtime call records, integrity events, content execution signals, and alerting interfaces.
Responsible	2.2 Custody preservation	Where the vendor stores, distributes, caches, or synchronises content through the CMS or player software, it must preserve custody integrity. The vendor should prevent unauthorised modification of content in storage, transit, cache, or deployment workflows.
Responsible	3.2 Player device environment segregation	Where the vendor provides or operates player software, it should support segregation between the player environment, management plane, customer networks, and vendor infrastructure. The software should not create uncontrolled paths for compromise to propagate across those boundaries.
Enabler	3.3 Authorised system access	Provide access control, authentication, authorisation, audit logging, and administrative separation capabilities for CMS and player management. The vendor should enable media owners to enforce least privilege and trace actions that affect screen content.
Accountable and responsible	4.1 Control enablement	Provide platform capabilities that enable media owners to meet the Framework's integrity, containment, detection, custody, and access outcomes. The vendor should maintain these capabilities as core security properties of the CMS and player product.
Accountable and responsible	4.2 Blast radius limitation	Design and operate the platform so that compromise of one tenant, screen fleet, credential, integration, or backend component does not cascade to other customers. The vendor should enforce tenant isolation, privileged access controls, secure update mechanisms, and platform-level monitoring.

14 Appendix: Glossary of Terms

The following is a list of definitions used in this Framework. For further industry definitions, refer to oma.org.au/glossary.

Term	Definition
API (Application Programming Interface)	A defined interface through which software systems exchange data or instructions. In DOOH, APIs connect CMS platforms, DSPs, SSPs, verifiers, data feeds, and player devices. Poorly controlled API access can enable unauthorised content changes at scale.
CDN (Content Delivery Network)	A distributed network of servers used to cache and deliver digital content - including creative assets, scripts, data feeds, and hosted files - to endpoints such as DOOH players. CDNs improve delivery speed and reliability but introduce a dependency that can be exploited if the hosted content is tampered with.
Chain of custody	The sequence of parties that hold, control, or modify a creative package between its origination and its execution on screen. Each handover in the chain is a point at which integrity can be preserved or lost. This Framework assigns responsibility based on which party holds custody at each stage.
CMS (Content Management System)	The platform used by media owners to schedule, manage, distribute, and control content across their player fleet. The CMS is the primary operational interface for approving what plays on screen and is a critical control surface for the security outcomes in this Framework.
Creative package	The complete set of files prepared for display on a DOOH screen, which may include HTML, CSS, JavaScript, image or video assets, manifests, and configuration files. The creative package is the primary unit of review and approval in the delivery chain.
DCO (Dynamic Creative Optimisation)	A technology and process by which advertising creative is assembled or personalised at or near runtime using data inputs such as time, location, weather, audience context, or other triggers. DCO providers manage the logic, templates, and data feeds used to construct these creatives.
DOOH (Digital Out-of-Home)	The digital subset of OOH advertising, delivered on screens that can receive, store, and display digital content. DOOH screens may execute code, fetch live data, and update content remotely, which distinguishes them from static OOH formats.
DSP (Demand-Side Platform)	A technology platform used by advertisers and their agencies to purchase advertising inventory programmatically. In DOOH, the DSP bids into SSP auctions on the advertiser's behalf and supplies or confirms the creative to play if the bid is won.
Dynamic content	Content that is assembled, personalised, or updated at or near the time of display, drawing on live or near-live data inputs such as time, temperature, pricing, or audience signals. Dynamic content introduces runtime dependencies not fully determined at approval time, creating additional integrity risk compared to static assets.
HTML (HyperText Markup Language)	The standard language used to structure and display content in web-based rendering environments. In DOOH, HTML creative packages bundle HTML, CSS, and JavaScript that execute on the player, making them the highest-

	risk content type due to their ability to run code and make external calls at runtime.
JavaScript	A programming language that executes in web-based rendering environments, including DOOH players. JavaScript within creative packages can fetch external data, call third-party services, and modify displayed content at runtime. It is the primary executable surface in HTML creative packages and verification wrappers.
OMA (Outdoor Media Association)	The peak industry body representing outdoor advertising companies in Australia. The OMA coordinates industry standards, guidelines, and frameworks including this Framework.
OOH (Out-of-Home)	Advertising displayed in public spaces outside the home, including billboards, transit shelters, street furniture, and retail environments. Encompasses both static printed formats and digital screens.
Programmatic	Automated buying and selling of ad space using data & algorithms
Runtime	The period during which a creative package is actively executing on a player device. Runtime behaviour includes fetching external data, calling APIs, rendering content, and any code execution triggered after the creative has been delivered and is playing. Runtime behaviour may differ from what was observed during pre-approval review.
Sandboxing	A security technique that isolates the execution environment of a process or application, limiting its ability to access the operating system, other applications, or the network beyond what is explicitly permitted. Sandboxing of creative execution on the player is a key control for runtime containment (sub-outcome 1.4).
SSP (Supply-Side Platform)	A technology platform used by media owners to make their DOOH inventory available for programmatic purchase. The SSP runs the auction, resolves bids, and returns the winning ad selection or decisioning instruction to the player.
Supply chain	The full set of parties, platforms, and workflows involved in creating, delivering, approving, and displaying DOOH advertising content - from the advertiser and their agencies through to the media owner's player devices. This Framework assigns accountability and responsibility across the supply chain based on each party's role and custody.
Verifier	An independent third party that collects telemetry or measurement data to confirm whether advertising played as intended. Verifiers may operate tag-based or wrapper-based measurement that executes on the player alongside the creative. In this Framework, verifiers are supply chain partners accountable for the integrity and containment of their own measurement code.
Wrapper / verification wrapper	An executable layer added around a creative package, typically by a verifier or DSP, that runs alongside the creative at play time. Wrappers collect measurement telemetry or carry programmatic decisioning instructions. Because wrappers execute code on the player, they are subject to the same integrity requirements as the creative itself.