ClearSkies™

CORE FUNCTION BRIEF

Regulatory Frameworks

A core function of the ClearSkies iISOC platform

One detection, mapped once through a shared technique language, evidences every regime that references it.

Contents

SECTION 1

Executive Summary

IN ONE SENTENCE.

Regulatory Frameworks is the core function that decomposes a regulation's obligations into MITRE ATT&CK techniques, so a single detection automatically produces evidence for every framework whose controls reference that technique, without separate mapping work per regulation.

Compliance evidence is conventionally assembled once a year under audit deadline pressure, framework by framework, because nothing links the same underlying control across the several regulations that reference it. An organization subject to five regimes maps the same control five separate times in five separate spreadsheets. A framework gets marked addressed in a tracker without a clear technical basis for the claim. And an organization operating across several jurisdictions has no single, current view of which frameworks are meaningfully covered rather than nominally listed.

Regulatory Frameworks answers this with a five-stage mechanism. Each supported framework's obligations are decomposed into the specific ATT&CK techniques that satisfy them. Every detection the platform raises already carries its technique identifier, attached by Detection Factory at the point of authoring. Because both use the same technique language, a firing detection is automatically attributed to every framework whose control set references that technique, continuously rather than seasonally. A relevance score indicates how directly a framework's technical obligations align to the platform's detection coverage, and a per-framework, board-ready evidence report is exported from the same underlying detections rather than assembled by hand.

That same shared language is what lets an organization operating across several jurisdictions see its actual, current coverage per region rather than a policy document's nominal list, because a new region's framework reuses a technique decomposition already in place wherever the same adversary behavior is regulated elsewhere.

THE FUNCTION IS PRECISELY SCOPED.

Regulatory Frameworks maps detections to regulatory obligations and reports the evidence. It does not attach the technique identifier itself, which is Detection Factory. It does not compute a risk score, which is the Risk Scoring Formula. And it produces evidence of specific controls firing, not a legal determination of compliance, which remains an organizational and legal judgment. Its evidence stands apart from the platform's data residency architecture, which is described in ClearSkies iISOC Data Sovereignty.

Five stages
Decompose, tag, attribute, score, report

Map once
One technique language across every supported region

Evidence, not assurance
A control that fired, not a compliance guarantee

SECTION 2

Why Manual Mapping Falls Short

Compliance evidencing is underinvested relative to the rest of the security operation, and the consequences surface as a scramble before an audit rather than as a single visible failure. Four failure modes explain why, and each is answered by a named stage of the mechanism in section 3.

2.1 The same control mapped by hand, once per framework

An organization subject to several regulations conventionally maps the same underlying control separately for each one, in separate spreadsheets, because nothing links the mappings through a shared technique language. The effort scales with the number of regulations rather than with the number of distinct controls actually in place.

2.2 Coverage claimed without a technical basis

A framework is marked addressed in a compliance tracker without a clear link to the specific detection that evidences it, so the claim cannot survive a specific auditor question about which control actually fired. The tracker records an intention rather than a demonstrated fact.

2.3 Evidence assembled once a year under deadline pressure

Mapping detections to a regulation's requirements is treated as an audit-season project rather than a continuous byproduct of running the security operation, so the evidence compiled is already stale relative to the current detection posture by the time an auditor reviews it.

2.4 A global footprint invisible per jurisdiction

An organization operating across several regions has no single, current view of which of the many frameworks it may be subject to are meaningfully covered by its actual detection coverage, as opposed to nominally listed in a policy document. A jurisdiction added after the initial compliance assessment is especially likely to be listed without being checked.

2.5 The cost of the workaround

The usual response is a compliance team or an external auditor re-deriving the same evidence from console exports and interview notes, once per framework, once per year. Cost scales with the number of regulations an organization is subject to, while the underlying problem, mappings that are not linked through a shared technique language, is untouched.

Industry research on compliance operations consistently finds audit preparation time dominated by manually re-deriving evidence framework by framework, though the specific figure for that cost, and for the share of it attributable to duplicate mapping work, is not yet sourced for this brief.

SECTION 3

How Regulatory Frameworks Works

Regulatory Frameworks is one continuously operating mechanism native to the TDIR core, not an annual mapping exercise. A regulation's text enters at one end, and continuous, per-framework evidence leaves at the other.

> *Figure 1. The five-stage evidencing mechanism.*

3.1 The five stages

Each stage is named once here and referenced by name throughout the rest of this brief, paired with the failure mode from section 2 that it answers.

STAGE	WHAT HAPPENS	THE FAILURE MODE IT ANSWERS
Decompose	A supported framework's obligations are decomposed into the specific MITRE ATT&CK techniques that represent the adversary behavior it requires an organization to defend against and evidence.	The same control mapped by hand, once per framework
Tag	Every detection the platform raises already carries its ATT&CK technique identifier, attached by Detection Factory at the point of authoring, not added afterward for compliance purposes.	Coverage claimed without a technical basis
Attribute	A firing detection is automatically attributed to every framework whose control set references its technique, continuously, without manual tagging.	Evidence assembled once a year under deadline pressure

STAGE	WHAT HAPPENS	THE FAILURE MODE IT ANSWERS
Score	Each framework carries a relevance score indicating how directly its technical monitoring obligations align to the platform's detection coverage.	Coverage claimed without a technical basis
Report	A per-framework, per-region evidence export is produced from the same underlying detections, current as of the moment it is generated.	A global footprint invisible per jurisdiction

A single detection can satisfy several frameworks at once precisely because Decompose and Tag share the same technique language. Attribute is the stage where that shared language turns into evidence for every applicable regime simultaneously.

3.2 How a mapping is judged

Quality is measured rather than assumed, on definitions a provider can report and a customer can audit. The measures below are reported natively and per tenant. They are defined here because the same metric name is measured differently by different vendors, and target values are agreed per engagement rather than asserted.

MEASURE	THE DEFINITION USED	WHAT A POOR VALUE TRIGGERS
Mapping completeness	A framework's technique-based obligations with at least one live, validated detection attached, as a share of the total.	A review of the gap against the Detection Factory coverage matrix.
Attribution latency	Elapsed time between a detection firing and its evidence being attributed to every referencing framework.	Investigation of the specific stage introducing the delay.
Citation currency	Supported frameworks with citation and version confirmed current within the defined review period, as a share of the catalog.	Prioritized legal and compliance review of the stale citation.
Frameworks evidenced per detection	The average number of distinct frameworks a single detection's evidence satisfies at once.	A review of whether the decompositions in place are too narrow to share techniques.
Time to onboard a new jurisdiction	Elapsed time from adding a framework's technique decomposition to its appearance in reporting.	A review of the decomposition backlog against the regions a tenant actually operates in.

MEASURE	THE DEFINITION USED	WHAT A POOR VALUE TRIGGERS

Mapping is not compliance. ***A framework this function evidences at a high relevance score is a technical mapping, not a legal determination. A specific detection firing is a fact the platform can produce. Whether an organization is compliant with a given regulation is a judgment the organization and its counsel make, informed by that evidence rather than replaced by it.***

SECTION 4

Regulatory Frameworks in the Platform

4.1 What it draws on, what it writes back, and what it does not do

What it draws on. The ATT&CK technique identifier Detection Factory attaches at authoring time, and the decomposition of each supported framework's legal or standards text into the technique set that satisfies it, reviewed on a defined cadence. Each is an input to a specific stage rather than a capability this function generates.

What it writes back. Per-framework evidence records and relevance scores, published into the shared model, and the board-ready reports generated from them. KPIs and SLAs may draw on the reporting cadence for its own audience-matched delivery. The relationship is one way: nothing returned to this function changes a mapping already published, and Decompose changes only when a framework's underlying text changes. An internal compliance review and an external audit draw on the same evidence records rather than on separate copies.

What it does not do. It does not attach a technique identifier to a detection, which is Detection Factory's authoring stage. It does not compute a risk score or decide a response. And it does not determine or assure legal compliance, only that a specific, technique-mapped control fired. Residency is a platform-level architecture property: this function evidences framework alignment whatever configuration is in place.

4.2 A worked example

The chain below is illustrative and technically representative rather than drawn from a named engagement. A detection fires for credential abuse consistent with valid-account techniques on an internet-facing system. Tag confirms the detection already carries its technique identifiers, attached when Detection Factory authored the rule. Attribute recognizes that both techniques are referenced by the control sets of three supported frameworks operating in the tenant's region, a data-protection regulation, a financial operational-resilience regime and an international security standard, and links the single detection to all three. Score reflects a highly relevant control area for two of the three and a

supporting one for the third. Report includes the detection, its timestamp and its technique mapping in the next scheduled export for each framework, and the same detection remains available to any framework added later that references either technique.

4.3 Delivery across many tenants

A framework's technique decomposition is maintained once and applies to every tenant subject to it, so onboarding a customer into a new jurisdiction means applying an existing decomposition rather than building a new mapping. What travels between tenants is that decomposition; what never travels is one tenant's detections, evidence records or reports.

Because the function is switched on with the platform rather than deployed separately, time to value is a matter of enabling the relevant frameworks rather than an onboarding project. In the first week, a tenant's existing detections are attributed against every decomposition already enabled for its region, so a first evidence export is available immediately. Through the first month, mapping completeness becomes visible against each enabled framework's obligations, surfacing any gap for Detection Factory to prioritize. At steady state, citation currency and attribution latency are tracked as ongoing measures.

SECTION 5

MITRE ATT&CK as the Shared Technique Language

MITRE ATT&CK is what makes cross-framework evidencing possible. Every supported framework is expressed as the set of techniques that represent the adversary behavior it requires an organization to defend against, and every detection already carries the technique identifier Detection Factory attached. Because the same language underlies both sides, mapping is a lookup rather than a translation exercise performed by hand.

Mapping is not coverage. A technique referenced in a framework's control set and matched to a live detection is claimed evidence. Whether that specific detection has been exercised in a purple-team run or validated against MITRE Engenuity ATT&CK Evaluations is the claimed-versus-demonstrated distinction the Detection Factory brief owns. This function inherits that distinction and states which of the two applies, rather than presenting every mapped technique as equally proven.

A representative set of supported frameworks appears below rather than the complete catalog, which is maintained live and available through platform reporting.

REGION	REPRESENTATIVE FRAMEWORKS	WHAT THEY REQUIRE DETECTION COVERAGE FOR
European Union and Europe	GDPR (EU 2016/679, Art. 32), NIS2 (EU 2022/2555), DORA (EU 2022/2554)	Security of processing, network and information security, and financial operational resilience, spanning both a general data-protection regulation and two sector-specific regimes.
Middle East	SAMA cybersecurity framework, UAE NESA, Qatar National Information Assurance	Financial-sector and national-assurance security monitoring obligations, each issued by a national regulator rather than a shared regional body.
International standards	ISO/IEC 27001 and 27002, PCI DSS, CMMC 2.0	Information security management, payment-card data protection and defense-sector maturity, none of them tied to a single jurisdiction.
North America	HIPAA Security Rule, NIST Cybersecurity Framework 2.0	Health-data safeguards and general cybersecurity outcome reporting, the latter widely referenced outside North America as well.

Relevance scores are illustrative of the model and dependent on the methodology behind them, so a specific figure is confirmed before use with a customer and reviewed alongside the citation currency check in section 3.2. A framework still in draft or pending is marked as such rather than presented as settled law, and adding one to the catalog reuses an existing decomposition wherever the same behavior is already regulated elsewhere.

SECTION 6

Questions Raised in Evaluation

The questions below recur in buyer evaluations, each answered directly against the mechanism described in section 3.

QUESTION, AS A BUYER ASKS IT	ANSWER
Does mapping to a framework mean the organization is compliant with it?	No. It produces evidence that specific technique-mapped controls fired. A compliance determination is a legal and organizational judgment this function does not make.

QUESTION, AS A BUYER ASKS IT	ANSWER
How current are the framework citations?	Reviewed on a defined cadence, and citation currency is one of the measures in section 3.2. A framework still in draft or pending is marked as such rather than presented as settled law.
What does the relevance score mean?	It indicates how directly detection coverage aligns to a framework's technical monitoring obligations. It is illustrative of the model rather than a certified audit score.
Does this function decide which detections fire?	No. Detection Factory authors and tags detections. This function consumes the technique identifier already attached and never adds one of its own.
Does compliance evidencing depend on where data is stored?	No. Data residency and sovereignty are platform-level architecture properties held by ClearSkies iISOC Data Sovereignty. This function evidences framework alignment whatever residency configuration is in place.
Does reporting depth vary by what a customer pays for?	Commercial packaging is a decision made elsewhere. This function evidences whatever frameworks are enabled for a tenant, at the same depth in every case.
What happens when a regulation is amended?	Decompose is rerun against the amended text, and only the affected technique set changes. Detections already attributed under the unchanged obligations are unaffected.

SECTION 7

The Benefits

Compliance evidencing is where a security operation either produces the record or asks to be taken at its word, and the outcomes are countable: how many regimes one detection evidences, how much of a framework's obligations have a live detection behind them, and whether the evidence an auditor reads is current or reconstructed.

7.1 At a glance

BENEFIT	WHAT PRODUCES IT
One detection evidences every regime that references it	Decompose and Tag share the same technique language, so Attribute links a firing detection to every framework at once.

BENEFIT	WHAT PRODUCES IT
A coverage claim has a technical basis behind it	Every attributed detection carries the technique identifier Detection Factory attached at authoring.
Evidence is current rather than reconstructed	Attribute runs continuously as detections fire, so Report exports what is true at the moment it is generated.
A gap is visible before an auditor finds it	Mapping completeness, defined in section 3.2, measures obligations with no live detection attached.
A new jurisdiction costs a decomposition, not a project	An existing technique decomposition is reused wherever the same adversary behavior is regulated elsewhere.
The limit of the claim is stated, not implied	Evidence of a control firing is distinguished from a compliance determination throughout, in sections 3.2 and 5.

7.2 What changes, and for whom

A continuous, technique-linked evidence base changes what each role spends time on, and what each role can defend under audit.

ROLE	WHAT CHANGES
Compliance analyst	Works from a live, technique-linked evidence report rather than reconstructing one from console exports before an audit.
SOC manager	Mapping completeness and citation currency become visible, manageable numbers rather than an assumption checked once a year.
CISO and risk	A per-framework, board-ready report replaces a compliance tracker's checkbox, with a technical basis behind every claim.
Service provider practice lead	A customer entering a new jurisdiction is mapped once against an existing technique decomposition rather than requiring bespoke work per regulation.

7.3 What sets it apart

▸ **Mapped once, evidenced everywhere.** A single detection's technique attribution satisfies every framework that references it, so the cost of adding a regime is a decomposition exercise rather than a parallel mapping project.

▸ **Coverage measured, not asserted.** A relevance score and a mapping-completeness figure replace a tracker's checkbox, so a gap is visible before an auditor finds it rather than after.

▸ **Continuous, not seasonal.** Evidence accumulates as detections fire rather than being assembled under deadline pressure, so a report is never older than the detection posture it describes.

> **THE VALUE IN ONE LINE.**
>
> Manual mapping produces a document that says a control exists. A shared technique language produces the detection that fired, the technique it carried and every regime that technique answers, from the same record, on the day the auditor asks.

SECTION 8

Summary

Regulatory Frameworks is how the platform turns its own detections into regulatory evidence. It is one core function among twelve, scoped to a five-stage mechanism that runs continuously inside the TDIR core rather than as an annual mapping project performed by hand.

▸ Decompose, tag, attribute, score and report replace framework-by-framework manual mapping.

▸ The technique identifier this function consumes is attached by Detection Factory, which authors and tags every detection.

▸ A single detection is attributed to every framework whose control set references its technique, continuously rather than seasonally.

▸ A mapped, firing control is a fact the platform produces. Whether that satisfies a given regulation stays a judgment the organization and its counsel make.

▸ The function maps and reports, and leaves detection authoring, scoring, response and commercial structure to the functions and decisions built for them.

Forward-looking statement: any statement about future capability is forward-looking and non-binding, and capability described in the present tense is capability available at the publication date, subject to the deployment configuration in force. This document describes evidencing and reporting capability and does not constitute legal advice on any customer's regulatory obligations.