CSFAAS

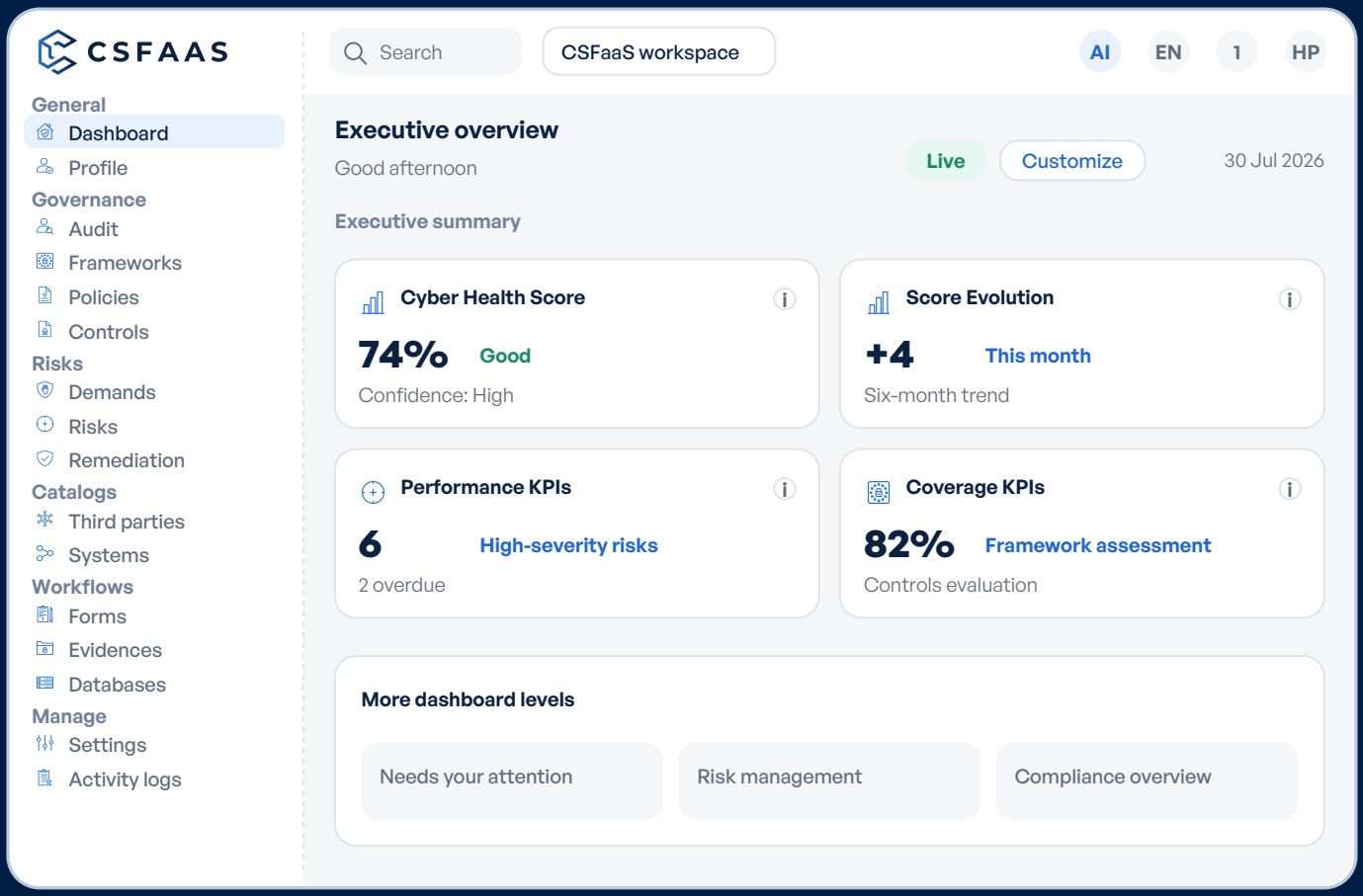
Whitepaper

Cybersecurity Governance that stays alive.

AI & API by Design

CSFaaS connects requirements, ownership, risk decisions and evidence in one permission-scoped GRC workspace.

Build the programme. Run the work. Prove the outcome.



Product view with example values.

Explore CSFaaS

csfaas.com

July 2026

EXECUTIVE CONTEXT

The problem is not another checklist. It is operational continuity.

Cyber security programmes now span standards, frameworks, regulations and assurance schemes. The hard part is not reading each requirement. It is keeping decisions, owners, assets, risks and evidence connected as the organisation changes.

Fragmented work

Requirements, evidence and actions live in separate tools, creating duplicate effort and conflicting status.

Evidence drift

Files outlive their context. Teams cannot quickly show which version supports which control, audit or review.

Unclear accountability

Ownership, due dates, exceptions and approvals are difficult to see across the programme.

Point-in-time reporting

A static report may describe yesterday while risks, suppliers, controls and evidence continue to change.

CSFaaS turns requirements into a shared operating model

Framework elements link to controls and policies; systems and third parties provide context; structured demands turn concerns into assessed risks and remediation; evidence, audits and reviews close the loop. The same workspace supports practitioners, management and assurance without creating a second source of truth.

- **Efficiency**
  Reuse controls, mappings and evidence instead of rebuilding the same proof for each programme.
- **Assurance**
  Keep evidence, decisions and review history attached to the objects they support.
- **Accountability**
  Make owners, workflow stages, due dates, exemptions and approvals visible.
- **Collaboration**
  Coordinate work through scoped access, activity, notifications and selected real-time collaboration features.

Scope note CSFaaS supports governance and certification preparation; it does not certify organisations or guarantee compliance.

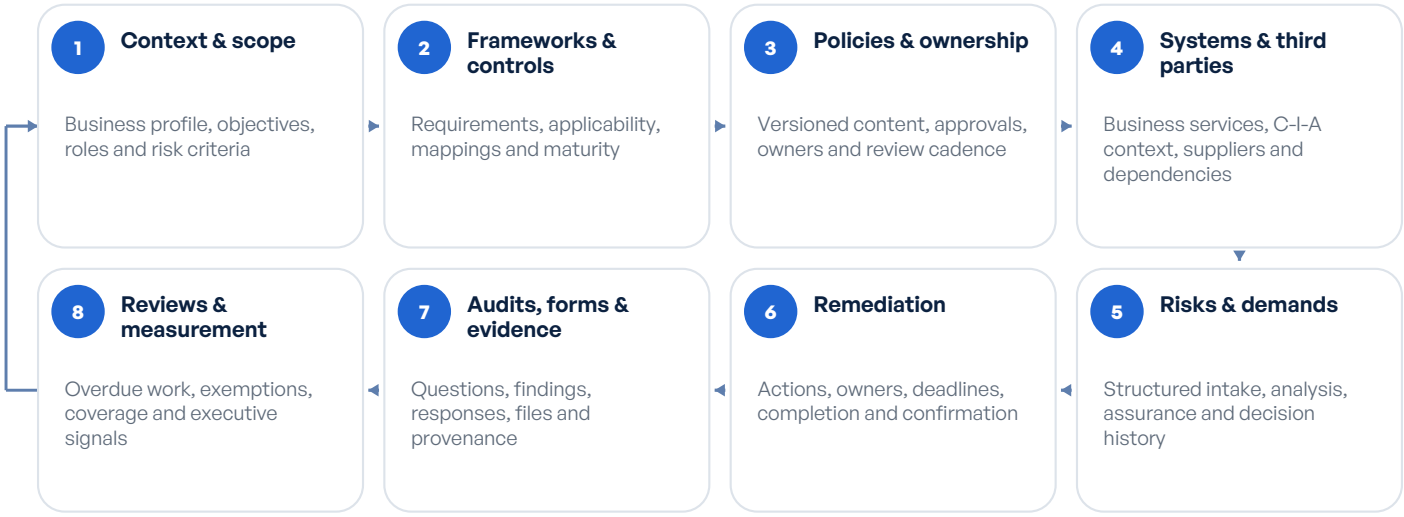
THE OPERATING MODEL

One connected model. A continuous operating rhythm.

CSFaaS treats governance as a cycle of context, decisions, execution and proof. Each domain remains distinct, but relationships let work performed in one place strengthen the rest of the programme.

STANDARD	FRAMEWORK	REGULATION	ASSURANCE
ISO 27001	NIST CSF	NIS2 / DORA	SOC 2

These sources have different legal and assurance roles. CSFaaS connects their requirements without treating them as interchangeable.



OPERATING RHYTHM

01

Scope

Choose the programme boundary, starting points, data model and decision rights.

02

Operate

Assign owners, run workflows, collect evidence and keep work moving.

03

Prove

Use linked evidence, audit records and review history to answer assurance questions.

04

Improve

Feed findings, overdue items and posture signals back into priorities and treatment.

THE CONNECTED PLATFORM

Twelve workflows. One evidence graph.

The platform keeps specialist workflows focused while preserving the relationships needed for reporting, assurance and change control.

Frameworks

Hierarchical requirements, applicability, maturity, mappings and framework reporting.

Policies

Collaborative authoring, versions, approvals and links to controls and requirements.

Controls

A shared control library with implementation status, owners, evidence and review cadence.

Demands

Structured risk intake with direct, analyst and assurance workflow modes plus SLAs.

Risks

Configurable qualitative analysis, treatment context and exposure-aware prioritisation.

Remediation

Owned actions, deadlines, completion states and confirmation against the originating need.

Systems

An information-system register with C-I-A context and links to risks and third parties.

Third parties

Tiering, assessment context, related systems, questionnaires and review schedules.

Audits

Campaigns, questions, findings, recommendations, actions and report generation.

Forms

Reusable questionnaires for internal teams, third parties and auditees.

Evidence

Files and links associated with the relevant object, response or content version.

Reviews

Ownership coverage, periodicity, upcoming and overdue work, validation and exemptions.

CROSS-CUTTING CAPABILITIES

- Dashboard and Cyber Health Score
- Activity, notifications and followed items
- English, French and Spanish interfaces
- Business profile, catalogues and parameters
- Multi-workspace roles and per-item access
- Dark mode and TOTP two-factor authentication

GOVERNANCE IN MOTION

From work to proof - with ownership built in.

The value of a GRC system appears between modules: when a request becomes a decision, a decision becomes an action, and completed work remains reviewable later.

1 Request

Capture context, scope, stakeholders and confidentiality.

2 Analyse

Apply the configured method, roles and priority SLA.

3 Decide

Record review, approval, exceptions and rationale.

4 Remediate

Assign actions, dates, complexity and evidence.

5 Verify

Confirm completion, review outcomes and retain history.

Work together, deliberately

- Owners, comments, activity and notifications keep the next action visible.
- Supported rich-text fields can be co-edited with conflict-safe collaboration; live cursors and selected-item presence help teams coordinate other work.
- Selected module views refresh as work changes, within the workspace boundaries configured for that part of the product.

Keep proof attached

- Evidence is linked and, where relevant, stamped to the object, version or response it supports.
- Time-limited signed access avoids turning evidence storage into a public shared drive.
- Audit questions, findings, recommendations and actions remain connected to their campaign.

Review the operating system

- Review schedules, validations and exemptions distinguish maintained governance from one-time setup.
- The unified events feed combines in-app activity with API and MCP access visibility where enabled.
- Dashboards surface posture and data-confidence signals without replacing the underlying evidence.

Executive measurement with context

The Cyber Health Score combines selected posture indicators configured for the workspace; a separate Confidence Score reflects data coverage.

Heat maps, deep links and overdue views let readers move from a signal to the records behind it.

Example score; actual results vary.

PLATFORM API / MCP / AI

AI that inherits your permissions - not a bypass.

CSFaaS exposes a canonical Platform API v2 and an MCP server for supported AI clients. Both converge on the same invariant: the caller acts as a real user, inside one workspace, under current membership, the credential's role scope and PostgreSQL row-level security.

01	02	03	04	05
User or client	**Explicit authorisation**	**API v2 / MCP**	**RLS and workflow guards**	**GRC data**
Browser session, supported MCP client or user-bound API key	OAuth 2.1 selects workspace, roles and read-only or read/write access	Validates the request and creates a short-lived workspace-pinned identity	Confine data, enforce membership, credential scope and workflow permissions	Returns or changes only the resources authorised for that caller

Read-only by default

Read/write must be explicitly granted to the credential or OAuth consent.

No service-role bypass

The Platform API holds no service-role key; normal data access remains RLS-scoped.

Workspace kill switch

An administrator can disable API and MCP access for the workspace.

Guarded writes

Supported writes use strict schemas, workflow rules, dry-run and idempotency controls.

Access visibility

API and MCP request access is captured on a best-effort basis for the data-access console.

Revocable access

Keys and OAuth grants can be revoked; membership is checked per request and role grants are re-evaluated on issue or refresh.

Bring your own assistant, keep the programme boundary

Use plain business questions to explore risks, frameworks, controls, audits, evidence, reviews and related work. With read/write authorisation, supported tools can create or update records and perform governed workflow actions. The assistant does not receive database credentials and cannot expand its own permissions.

Platform API reference

MCP connection guide

ADOPT AND OPERATE

Start with scope. Grow into continuous assurance.

A credible implementation begins with decision rights and data boundaries, not with bulk configuration. CSFaaS can then expand as evidence, workflows and integrations mature.

01

Frame

Create the workspace, business profile, roles, starting frameworks and risk model.

02

Connect

Map controls and policies; declare systems, third parties, owners and review cadence.

03

Operate

Run demands, remediation, forms, audits and evidence collection in the same model.

04

Extend

Use dashboards, scheduled reviews, exports, API v2 and MCP where they add value.

Tenant isolation

Browser and API database access uses PostgreSQL RLS; API sessions add a restrictive workspace pin.

Identity and roles

Workspace roles, per-item grants and optional TOTP protect sensitive workflows.

Controlled evidence

Workspace-scoped storage, entity/version stamping and time-limited access preserve provenance.

Recorded activity

Database-emitted activity events and the gated access console support operational traceability.

Delivery options without freezing the architecture into this paper

The standard service is delivered as SaaS. Enterprise engagements can be scoped separately, including published flexible deployment options subject to technical and commercial confirmation. DarkProtect can add managed compliance, advisory and security-assessment support.

contact@csfaas.com

SOURCE AND SCOPE

Product and architecture facts were reviewed against the CSFaaS codebase and public product surfaces on 30 July 2026. Confirm current catalogue and commercial details with the CSFaaS team.

Build a living Cybersecurity GRC programme

Start a workspace or book a guided review of your governance, risk and assurance operating model.

Start with CSFaaS

Book a conversation