



## STRATEGIC WHITEPAPER

# SoReady™ The Continuity Layer for Major Events

Complementary positioning, modular architecture, security, universality and value for large-scale events.

### THESIS

SoReady connects requirements, data, dependencies, resources, risk, evidence and decisions. It preserves specialist systems and closes the gap between fragmented planning and demonstrable readiness.

# The gap is not a lack of tools

Major events already run on capable solutions. The break sits between them: divergent versions, invisible dependencies, late arbitration and scattered evidence.

## GAP 1

### Fragmentation

Every function optimises its own scope, without sufficient cross-cutting continuity.

## GAP 2

### Late decisions

Cross-impacts surface once the cost of correction has already grown.

## GAP 3

### Diffuse evidence

A readiness statement stays hard to explain, source and audit.

## RESPONSE

### Governed continuity

SoReady connects the useful objects without replacing their systems of authority.

## LEVEL 2 | UNDERSTAND

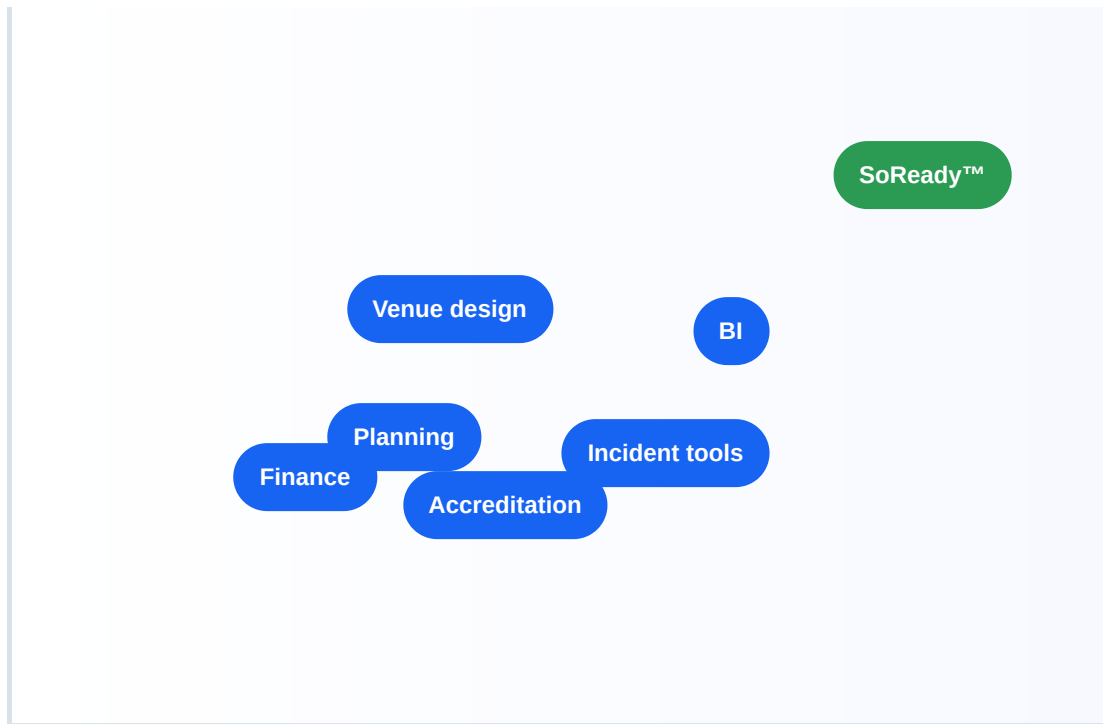
The functions of a major event are generally well equipped: finance, planning, accreditation, sport, security, logistics or documentation. Yet none of them alone carries the decisive question: can the whole thing work, on the planned date, with confirmed means and the required evidence? SoReady addresses this horizontal discontinuity. It makes visible the dependencies between domains, the contradictory information and the decisions left without an owner.

## LEVEL 3 | GO DEEPER

The value does not come from a new central data-entry point, but from a governed link between sources of authority. Measure the reduction in manual reconciliation and the arbitration lead time.

# Complementary by design

SoReady sits above transactional and specialist systems, below executive decision-making: a layer of governance, readiness and correlation.



## GOVERNANCE POINT

SoReady does not claim to redo finance, planning, CAD, BIM or accreditation. It makes their contributions coherent, explainable and actionable.

## LEVEL 2 | UNDERSTAND

SoReady's positioning rests on one discipline: not reproducing the depth of specialist tools. The financial system stays authoritative for commitments; planning for dates; document management for documents; sport solutions for their own objects. SoReady assembles the reading management needs: obligations, states, impacts, reservations, evidence and decisions. This complementarity reduces migration risk and allows progressive adoption.

## LEVEL 3 | GO DEEPER

The map is conceptual, not a product ranking. Integration requires an owner, a frequency, a status and a conflict rule for every data point.

# From data to a demonstrable decision

Value appears when the chain preserves the authority of the source, exposes the relationships and places arbitration at the right level.



## GOVERNANCE POINT

AI can extract, explain, challenge and draft. Rules compute; the human validates; the system traces.

## LEVEL 2 | UNDERSTAND

An isolated piece of data does not produce a reliable decision. It must be qualified, linked to an object and checked against applicable rules. The SoReady chain preserves the path from source to evidence: who supplied the information, which version was valid, what calculation ran, and who arbitrated. This continuity makes it possible to explain a decision after the fact and to revisit it when its context changes.

## LEVEL 3 | GO DEEPER

Systematically separate fact, calculation, AI proposal and decision. A rollback must restore the business state and its history, not just the display.

# A modular architecture put back in order

Modules are organised in layers: governance, reference data, planning and resources, then event operations.

## 01 - GOVERNANCE

### **Security, functional and technical administration**

Identities, roles, policies, audit, configuration, supervision and built-in user assistance.

## 02 - KNOWLEDGE

### **Document management/OCR, reference data and automated population**

Document reading, controlled extraction, provenance, validation and reference data.

## 03 - PREPARATION

### **Planning, contention, risk, budget, BOM and infrastructure**

Dependencies, capacities, costs, means, calculations and readiness by object.

## 04 - OPERATIONS

### **EOS, EDF, external flows, reporting and command centre**

Observation, event correlation, assisted summaries and traced decisions.

## LEVEL 2 | UNDERSTAND

The order of the modules reflects an order of trust. Governance and security define first who can see, modify or validate. The knowledge layer turns documents and reference data into sourced facts. Preparation connects planning, infrastructure, FoP, resources, budget, BOM, VIK and risk. Finally, the EOS and the Event Data Fabric support operations. Modules can be activated separately, but they share the same grammar of objects and evidence.

## LEVEL 3 | GO DEEPER

Avoid module silos: stable identifiers, versioned data contracts and a shared audit log. Functional and technical administration remain distinct.

# Thirteen capabilities, a single chain of trust

The breakdown distinguishes functional modules, cross-cutting services and the technology foundation.

| Order | Capability                           | Role in the chain                                  |
|-------|--------------------------------------|----------------------------------------------------|
| 01    | Governance / security                | Rights, responsibilities, policies, evidence       |
| 02    | Document management / OCR            | Documents into sourced, validatable facts          |
| 03    | Reference data / external flows      | Authorities, versions, mappings, quality           |
| 04    | Infrastructure / calculation engines | Venues, spaces, capacities, scenarios              |
| 05    | FoP / materials / consumables        | Needs, configurations, turnover, availability      |
| 06    | Planning / contention                | Dependencies, transitions, collisions, capacities  |
| 07    | Budget / BOM / VIK / workforce       | Costs, contributions, resources and arbitration    |
| 08    | Risk Assessment / readiness          | Exposure, treatment, evidence, gates               |
| 09    | EOS / EDF                            | Event state and operational correlations           |
| 10    | AI-assisted reporting                | Sourced summaries, files, decisions                |
| 11    | Cross-checked AIs                    | Extraction, contradiction, simulation, explanation |
| 12    | User assistance                      | Integrated, governed contextual help               |
| 13    | Administration                       | Business CRUD, operations, RBAC/MAC by criticality |

LEVEL 2 | UNDERSTAND

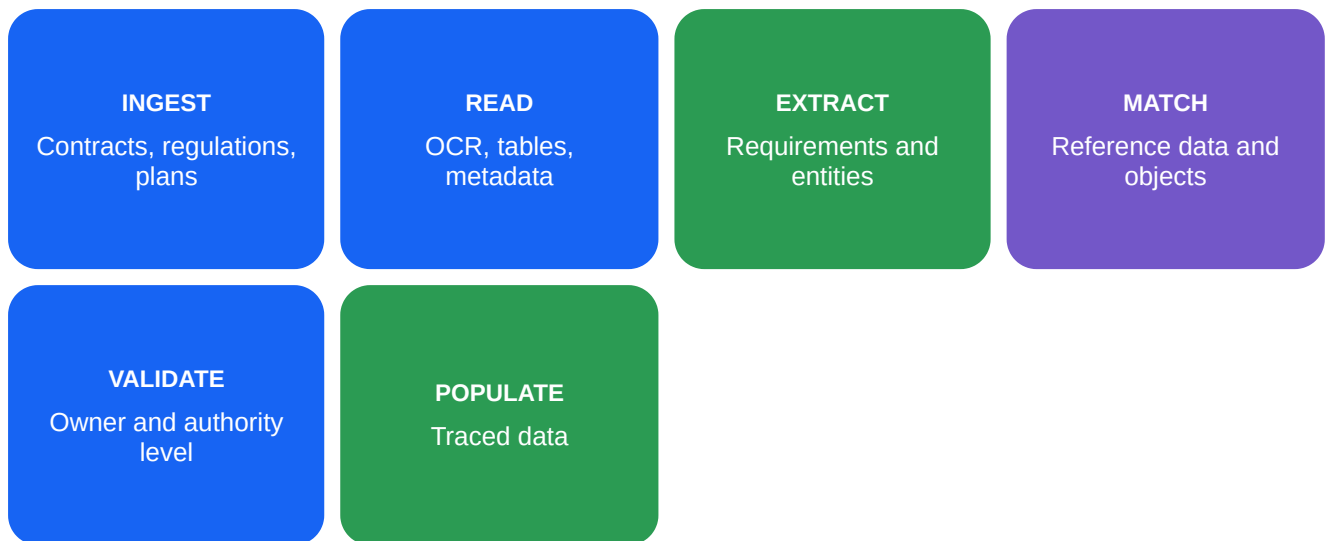
The breakdown does not describe thirteen juxtaposed applications. It exposes the capabilities needed to move from a documentary obligation to an opening condition, then to a live situation. Budget, BOM, VIK and workforce give substance to the means; planning and contention verify their availability; Risk Assessment measures exposure; EOS/EDF observes the signals. Reporting and cross-checked AIs make this information readable, without modifying certified data on their own.

LEVEL 3 | GO DEEPER

Business CRUD is subject to rights. For critical or certified information, apply separation of duties, dual validation and RBAC/MAC where required.

# From document to actionable context

Document management/OCR does not silently fill the system. It proposes facts, keeps the evidence and organises their validation.



## GOVERNANCE POINT

No automated extraction becomes an operational truth without provenance, status and control suited to its criticality.

## LEVEL 2 | UNDERSTAND

OCR is only the first step. SoReady must distinguish detected text, proposed fact and validated information. A requirement extracted from a regulation is matched to a discipline, a venue, a date and an owner; the original excerpt stays accessible. When a version changes, the system identifies the affected objects instead of silently overwriting the previous knowledge. Automated population thus becomes a controlled accelerator, not a source of opacity.

## LEVEL 3 | GO DEEPER

Keep the document, page, zone, hash, extraction date, model used and validation status. A value without provenance stays a proposal.

# Anticipating collisions before the event

The contention engine cross-references calendar, spaces, resources, capacities, turnover and dependencies. Budget and BOM give substance to arbitration.

## TIME

### Planning & transitions

Milestones, sequences, changeover times and critical paths.

## CAPACITY

### Contention

Conflicts across venues, teams, assets, transport and suppliers.

## MEANS

### BOM / FoP

Equipment, consumables, configurations and availability.

## ECONOMY

### Budget, VIK and workforce

Costs, in-kind contributions, resources, pooling and decisions.

## LEVEL 2 | UNDERSTAND

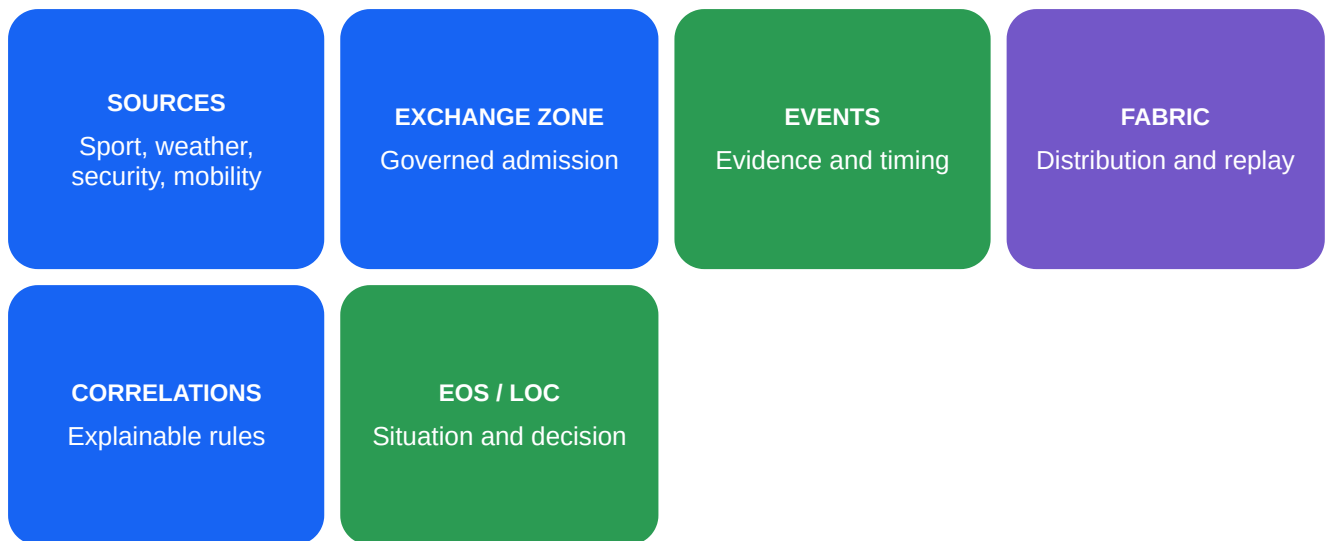
Contention appears when the same resource is promised to several incompatible sequences: space, team, equipment, transport, power or turnover time. The engine cross-references calendars with real capacities and dependencies. It does not stop at flagging a collision; it prepares arbitration options with their effects on budget, VIK, workforce and readiness. Management can then decide before the conflict reaches operations.

## LEVEL 3 | GO DEEPER

Calculation rules must be deterministic, versioned and testable. AI can explain the options, never invent an available capacity.

# Understanding the event as it unfolds

The EOS carries the operational state; the EDF admits heterogeneous signals, qualifies them and enables cross-domain correlation without erasing the authority of the sources.



## GOVERNANCE POINT

The EDF is an evolving event data fabric. Routing details, thresholds, models and proprietary rules are not exposed.

## LEVEL 2 | UNDERSTAND

The EOS provides an operational representation of the event; the EDF feeds it qualified events from heterogeneous domains. Between the source and the business state, a governed exchange zone checks the identity, form, authority, sensitivity and timing of the signal. Accepted events stay attached to their evidence and can be distributed, replayed or isolated. Correlation then surfaces a situation that no single source, taken alone, could reveal.

## LEVEL 3 | GO DEEPER

Observational architecture by default. No external flow writes directly into the business core; OT and life-safety systems keep their own chain of action.

# The Event Data Fabric is a complete module, not a simple connector

Its role covers the full lifecycle of a signal: admission, qualification, evidence, distribution, replay, correlation and operational control of flows.

## TRUST BOUNDARY

### Admission and isolation per flow

Source identity, authority, sensitivity, limits, format controls and independent shutdown.

## EVIDENCE & QUALITY

### Validation, quarantine and provenance

Original or probative reference, timestamping, version, status and visible handling of rejects.

## SERVICE CONTINUITY

### Durable distribution, deduplication and replay

Independent consumers, recovery after interruption, store-and-forward and reconciliation.

## EVENT INTELLIGENCE

### Canonical contract and explainable correlations

Comparable events, versioned rules, contextualised impacts and EOS feed.

# Ten domains, one cross-cutting view

The design base covers several dozen flow families, ten major operational domains and multi-domain correlation scenarios. This scope is extensible and is not a fixed promise.

**SIGNAL****Sport + results**

Programme, session status, timing and associated evidence.

**CONTEXT****Weather + mobility**

Forecasts, alerts, transport, traffic and arrivals.

**SITUATION****Security + crowd + medical**

Access, density, incidents and response capacity.

**CONTINUITY****OT + IT + logistics**

Power, network, equipment, services and turnover.

**LEVEL 2 | UNDERSTAND**

Sport, results, weather, mobility, crowd, medical, security, OT, IT, logistics and media evolve at different rhythms. The value of the EDF is to preserve this diversity while giving it a common timeline. The demonstration scope covers several dozen flow families and multi-domain scenarios; it remains extensible. The value lies less in the number of connectors than in the ability to qualify the freshness, confidence and operational impact of each signal.

**LEVEL 3 | GO DEEPER**

Every feed has an owner, an authority, a sensitivity, a simulated/sandbox/real mode, a quarantine and an independent kill switch.

# Security is included - but is not just an event standard

ISO 20121 addresses responsible event management; it is not a cybersecurity standard. SoReady aligns with a portfolio of complementary frameworks, without claiming certification.

| Reference             | Contribution                    | SoReady coverage                            |
|-----------------------|---------------------------------|---------------------------------------------|
| ISO 20121:2024        | Responsible event management    | Objectives, stakeholders, improvement       |
| ISO 31000:2018        | Risk management principles      | Risk Assessment, treatments, escalation     |
| ISO 22301:2019        | Business continuity             | Scenarios, recovery, exercises, evidence    |
| ISO/IEC 27001:2022    | Information security management | Identities, IT risks, audit, controls       |
| ISO/IEC 42001:2023    | AI management systems           | AI roles, risks, monitoring, accountability |
| OWASP / NIST AI RMF   | Application and AI risks        | Threats, tests, technical governance        |
| WCAG 2.2 / W3C PROV-O | Accessibility and provenance    | Usable interfaces, traceable facts          |

LEVEL 2 | UNDERSTAND

Security runs through the product: identity, rights, confidentiality, integrity, availability, continuity and audit. ISO 20121 structures responsible event management but does not on its own cover cybersecurity. ISO/IEC 27001, ISO 22301 and the OWASP frameworks therefore complete the approach; ISO/IEC 42001 addresses AI governance. SoReady can support the evidence and controls of a programme, without turning this alignment into a certification claim.

LEVEL 3 | GO DEEPER

Distinguish product security, operational security and overall event security. Each has its own owner, risks and tests.

# Three levels of AI, one doctrine

The deployment level depends on sensitivity, latency, connectivity and sovereignty requirements.

## LEVEL 1

### Controlled external AI

Authorised data, minimisation, governed gateway, low-sensitivity uses.

## LEVEL 2

### Hybrid architecture

Routing by data class; private models for sensitive content; interchangeable specialised services.

## LEVEL 3

### Local / sovereign AI

Local or isolated engines, on-site context, offline continuity and reinforced operational control.

## LEVEL 2 | UNDERSTAND

The choice between external, hybrid or sovereign AI depends on the data and the context, not on an abstract technology preference. Public or low-sensitivity content can use a controlled service. Contractual, financial or operational data can be routed to a private environment. Critical functions or those with strong continuity requirements can run locally. An MCP-type tool gateway can preserve common access contracts. In all three cases: minimal context, visible sources, bounded actions and human validation.

## LEVEL 3 | GO DEEPER

Plan for languages, data residency, administration, keys, latency and degraded mode. Sovereignty is an end-to-end property; MCP does not relocate rights or business authority.

# A stable grammar, configurable rules

SoReady is universal because it models the invariants of a major event, then adapts taxonomies, evidence, authorities and workflows.

## WHAT

### Programme and obligations

Commitments, requirements, deliverables, rules and decisions.

## WHERE / WHEN

### Venues and sequences

Spaces, milestones, transitions, capacities and dependencies.

## WHO / WITH WHAT

### Responsibilities and means

Owners, workforce, budget, assets, suppliers and BOM.

## WHAT IF

### Risk and continuity

Scenarios, signals, treatments, tests and evidence.

## LEVEL 2 | UNDERSTAND

All complex events share invariants: programme, venues, sequences, owners, resources, rules, risks and evidence. SoReady stabilises this grammar, then configures the vocabulary and obligations of the context. An international competition emphasises disciplines and FoP; a summit, delegations and protocol; a festival, stages and permits. Universality therefore comes from a coherent core and explicit contextualisation, not from an impoverished generic model.

## LEVEL 3 | GO DEEPER

Version taxonomies, rules and evidence levels per event. A local configuration must not break the common core or the migrations.

# Open, administrable and governed

Acceptance of external flows is controlled. Functional administration configures the business; technical administration operates the platform; security runs through both.

## FUNCTIONAL

### **Taxonomies, rules, responsibilities, gates**

Configuration per event, disciplines, venues, functions and evidence levels.

## TECHNICAL

### **Connectors, availability, observability, backup**

Operations, supervision, version management, continuity and performance.

## SECURITY

### **Identities, separation of duties, audit, integrity**

Access controls, logging, human validation and incident handling.

## LEVEL 2 | UNDERSTAND

Openness to the outside is only reliable if the boundaries are administrable. Functional administration configures taxonomies, workflows, gates and responsibilities. Technical administration operates connectors, performance, backups and observability. Security enforces identities, separation of duties and integrity controls. This organisation makes it possible to accept external flows without delegating authority over the programme's objects to them.

## LEVEL 3 | GO DEEPER

Document configuration changes like production changes: author, reason, validation, effective date, test and rollback.

# Deploy along critical paths

Value is demonstrated on a precise scope, then extends without forcing a wholesale replacement of existing tools.



## GOVERNANCE POINT

Measures: sourced coverage, conflicts detected before execution, arbitration lead time, demonstrable gates and reduced reconciliation work.

## LEVEL 2 | UNDERSTAND

A useful deployment starts with a management question, for example the readiness of a cluster or the turnover of several disciplines on one venue. The first thirty days align objects, owners and sources; the next connect documents, dependencies and rules; the final step demonstrates a gate with evidence and arbitration. This pilot produces verifiable value and reveals data gaps before extending to all functions.

## LEVEL 3 | GO DEEPER

Define success metrics from the start: sourced coverage, decision lead time, anticipated conflicts, accepted evidence and reconciliation workload.

# What SoReady claims - and what it does not

The product strengthens control. It does not replace authorities, certified systems or the LOC's responsibilities.

## CLAIMS

### Continuity and evidence

Connect, control, explain, trace, assist and prepare.

## DOES NOT CLAIM

### Automatic certification

No standard, regulatory compliance or approval is claimed without a dedicated audit.

## PROTECTS

### Trade secrets

Detailed models, calculations, rules, thresholds, routing and configurations stay confidential.

## EMPOWERS

### Human decision

Sensitive actions remain subject to rights, validations and competent authorities.

## LEVEL 2 | UNDERSTAND

The product's credibility depends as much on its limits as on its capabilities. SoReady can check consistency, trace provenance, compute states and assist analysis. It does not replace the authority of a federation, a security service, an auditor or the LOC. It does not turn data into certification by simply passing it through the platform. Trade secrets stay protected while governance principles remain explainable.

## LEVEL 3 | GO DEEPER

Every commercial claim must distinguish available capability, required configuration, third-party integration, expected assurance and final responsibility.

# Turning readiness into a governance asset

SoReady preserves the depth of existing tools, adds the continuity they lack, and gives every decision its context, its evidence and its owner.

**SEE****Earlier**

Weak signals, coverage gaps and contradictions.

**CONNECT****More broadly**

Functions, venues, disciplines, means and events.

**DECIDE****More clearly**

Options, impacts, responsibilities and evidence.

**CAPITALISE****Beyond the event**

History, lessons learned and reusable assets.

**LEVEL 2 | UNDERSTAND**

Readiness becomes an asset once the board can question it: why is this object declared ready, what evidence demonstrates it, what reservation remains and who accepted it? SoReady creates this capacity for scrutiny and keeps the history of changes. After the event, the same corpus supports the debrief, the handover to future teams and the reuse of reference data. The platform thus connects immediate performance and organisational legacy.

**LEVEL 3 | GO DEEPER**

Assess readiness by conditions and evidence, never by an isolated percentage. Keep the accepted reservations and their authority.

# Frameworks used and scope of the claims

The references structure the analysis. They constitute neither a certification of SoReady nor an automatic validation of an event's compliance.

| Public reference      | Domain                       | Use in this document              |
|-----------------------|------------------------------|-----------------------------------|
| ISO 20121:2024        | Responsible event management | Governance and improvement        |
| ISO 31000:2018        | Risk management              | Treatment and residual exposure   |
| ISO 22301:2019        | Business continuity          | Scenarios, exercises and recovery |
| ISO/IEC 27001:2022    | Information security         | Identities, controls and audit    |
| ISO/IEC 42001:2023    | AI management systems        | Roles, risks and accountability   |
| NIST AI RMF / OWASP   | AI and application risks     | Threats and assurance             |
| W3C PROV-O / WCAG 2.2 | Provenance and accessibility | Traceability and inclusive use    |

LEVEL 2 | UNDERSTAND

The standards and frameworks cited provide complementary angles: event management, risk, continuity, security, AI, provenance and accessibility. They make it possible to check that the architecture does not overlook a major dimension. This document does not reproduce their normative content and does not claim to demonstrate compliance. Any certification is a matter of scope, a management system and a formal audit.

LEVEL 3 | GO DEEPER

Official references: [iso.org](https://www.iso.org), [nist.gov](https://nist.gov), [owasp.org](https://owasp.org) and [w3.org](https://www.w3.org). Check the edition applicable at the time of the project.