WEBINAR RECORDED

PECB

AI Governance and Risk Management: Implementing ISO/IEC 42001 in Practice

AUGUST 27 | 3:00 PM CEST

Alexis Hirschhorn

CEO Acuna GRC

#GlobalLeadingVoices

AI GOVERNANCE AND RISK MANAGEMENT

Implementing *ISO/IEC 42001* in practice.

What we learned so far & How do we do it

Alexis Hirschhorn

CEO, Acuna GRC

3:00 PM CEST · 45 MIN

WHY NOW — THE MANDATE

The pressure *on the teams*

AI is already in production across the business, and the assurance questions have started. Auditors, clients, and regulators now ask what governs it.

THE HOT TOPIC

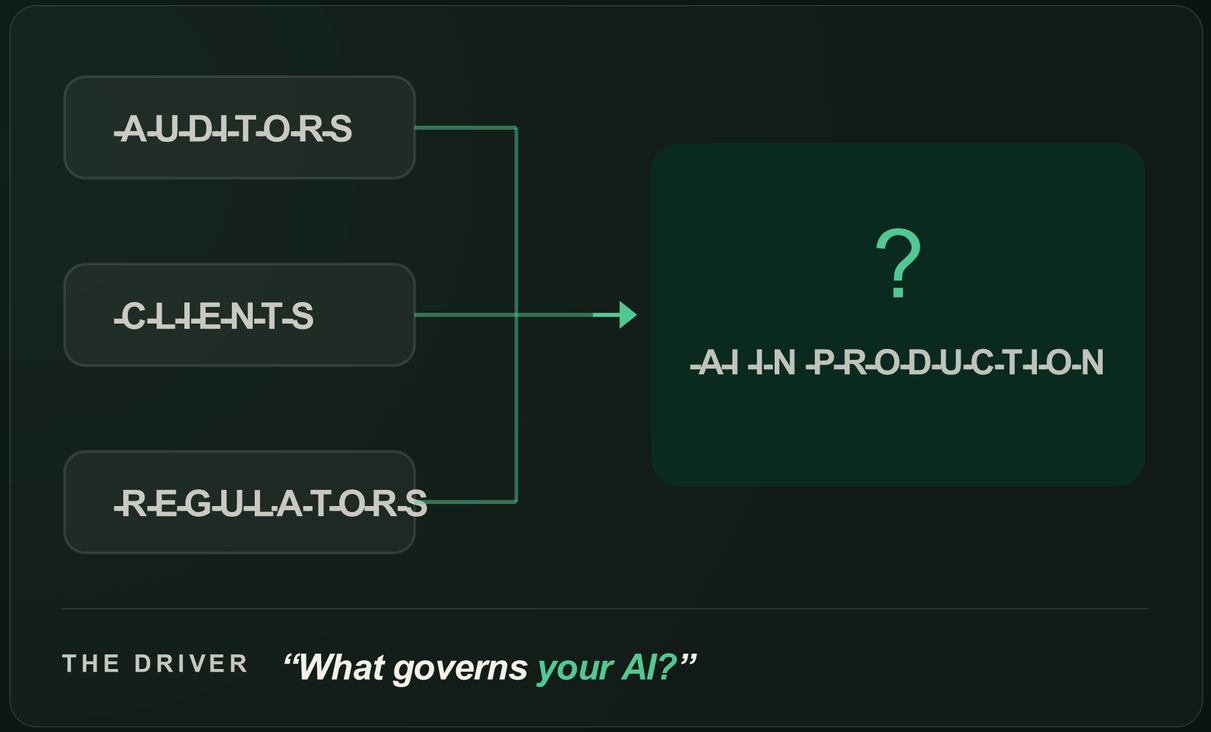
Vendor DDQs and audits now carry AI-specific sections.

AI, THE REALITY

Models in production with no management system around them.

EU AI ACT PRESSURE

Government require AI regulation and governance



OUR WORKED CASE — THE EXAMPLE

Meet *HireIQ.*

We'll carry one system through the whole session: HireIQ, a third-party AI tool you buy and deploy to screen and rank job applicants. You are the deployer.

WHAT IT DOES

Screens and ranks applicants

A vendor tool you procure, not one you build.

WHY IT'S HIGH-STAKES

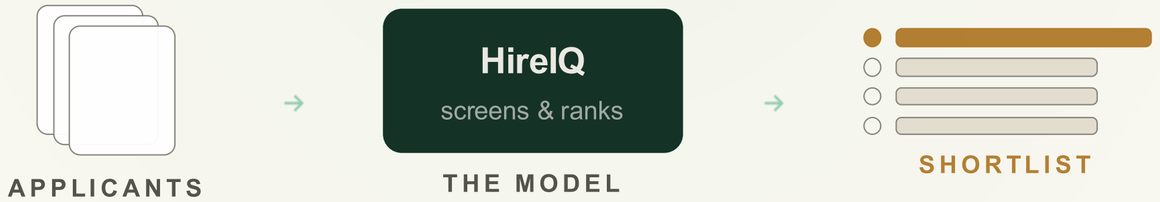
Livelihoods and bias

It affects people's livelihoods and can encode bias.

WHAT IS OUR ROLE

Deploying makes it yours

You didn't build it, but deploying it makes the duties yours.



THE THREAD

One system, followed end to end.

ONE WORKED EXAMPLE THROUGHOUT

YOUR ROLE — TWO ROLES, ONE OF THEM YOURS

Provider or *deployer?*

The EU AI Act splits two roles. You almost certainly sit on the deployer side, and that is where your obligations live.

PROVIDER · BUILDS / PLACES ON MARKET

- Builds or markets the AI system
- Technical documentation, conformity
- CE marking, EU database registration
- Declares the system fit for purpose

USUALLY YOUR VENDOR

↔

DEPLOYER · USES UNDER ITS AUTHORITY

- Uses the system per instructions for use
- Fundamental rights impact assessment
- Human oversight by competent people
- Monitors, logs, reports incidents

THIS IS YOU

The vendor's compliance is not yours. Like SOC 2: a supplier's certificate never makes you compliant. Deployer duties stay yours, whoever built the model.

SECTION 02 · THE STANDARD

You probably already *run this.*

The ISO/IEC 42001 shares the Annex SL Harmonized Structure with the ISO/IEC 27001. Clauses 4 to 10 are machinery you already operate.

IN THIS SECTION

Same structure, same disciplines, plus three genuinely new clauses.

Clauses 4–10 map from your ISMS
The delta: 6.1.2, 6.1.4, 8.4

CLAUSES 4 TO 10 — THE SCAFFOLD

The structure *you know.*

ISO/IEC 42001 uses the same Annex SL Harmonized Structure as ISO/IEC 27001. If you run an ISMS, clauses 4 to 10 are already familiar territory.

CLAUSES 4–5

Context & leadership

Scope, interested parties, top-management intent.

CLAUSES 6–7

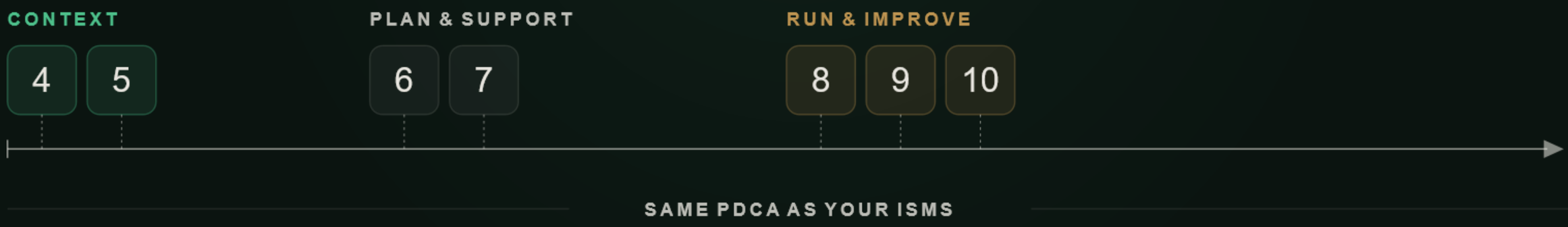
Planning & support

Risk, objectives, resources, competence.

CLAUSES 8–10

Operate, check, improve

Run it, audit it, correct it. Same PDCA.



The AIMS runs *on a loop.*

PLAN · CLAUSES 4–6

Context, leadership, AI risk & impact, objectives.

DO · CLAUSES 7–8

Resources, operate, run impact assessments.

CHECK · CLAUSE 9

Monitor, internal audit, management review.

ACT · CLAUSE 10

Nonconformity, corrective action, improve.

The standard, *in figures.*

The shape of ISO/IEC 42001:2023: a management system you scope, control, and certify.

7

CLAUSES

Clauses 4–10: the management system.

38

ANNEX A CONTROLS

Reference set, chosen via SoA.

9

OBJECTIVES

Objectives A.2 to A.10.

2

AUDIT STAGES

Stage 1 then Stage 2 to certify.

Shared	6.1.2 / 6.1.4 / 8.4	Your set	Shared
HARMONIZED STRUCTURE	AI-SPECIFIC DELTA	STATEMENT OF APPLICABILITY	REUSES YOUR ISMS

Two standards, *one scaffold.*

ISO/IEC 27001

Information security

Confidentiality, integrity, availability

93 Annex A controls across 4 themes

ISO/IEC 42001

AI management

AI impact, fairness, transparency, oversight

38 Annex A controls across 9 objectives

SHARED

Annex L / Harmonized Structure

Clauses 4–10

27001 — THE OVERLAP

What maps *straight across.*

CLAUSE 6

Risk management

Risk assessment and treatment: same discipline, AI subject.

CLAUSES 9–10

Audit & improve

Internal audit, management review, corrective action.

ANNEX A

Suppliers

Third-party assessment; extended to model and data vendors.

ANNEX A

Access control

Access control and change control transfer directly.

REUSE

Your ISMS habits, already earning.

SAME DISCIPLINES, NEW SUBJECT

WHAT 27001 NEVER ASKED — THE DELTA

Three new *clauses.*

The real delta is three sub-clauses with no ISMS equivalent. They shift the question from risk-to-you to harm-to-others.

6.1.2

AI risk

Risk to the organisation meeting its objectives.

6.1.4

Impact process

Define how you assess harm to individuals and society.

8.4

Perform it

Run the impact assessment, retain the results.

THE PIVOT

Risk to you, harm to others.

NO ISMS EQUIVALENT

How the delta clauses *connect.*

PLAN · CLAUSE 6

DO · CLAUSE 8

6.1.2

AI risk

Risk to the org meeting its objectives.

→

6.1.4

Impact process

Define how you assess harm to people & society.

→

8.4

Perform it

Run the impact assessment; retain results.

→

SoA

Your control set

Select Annex A controls; justify exclusions.

SECTION 03 · ANNEX A

38 controls, *9 objectives.*

Annex A (A.2 to A.10) is a reference set, not a checklist. You select via a Statement of Applicability driven by risk and impact.

IN THIS SECTION — 12 MIN

The control catalogue, two deep-dives, and the SoA that ties it together.

A.5 impact and A.7 data and the applied HireIQ's SoA, worked live

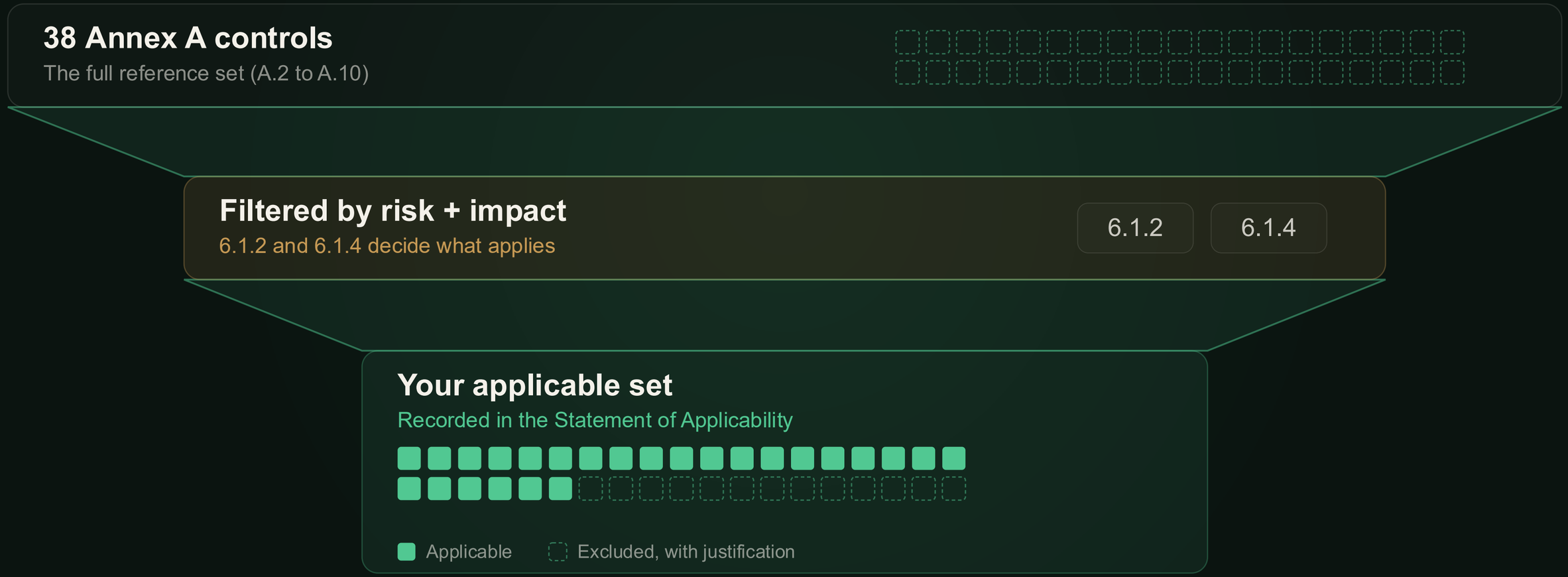
A.2–10 — ANNEX A

Nine objectives, *thirty-eight controls.*

A.2 Policies related to AI	A.3 Internal organization	A.4 Resources for AI systems
A.5 Assessing AI impacts	A.6 AI system life cycle	A.7 Data for AI systems
A.8 Information for parties	A.9 Use of AI systems	A.10 Third-party relationships

A.5 and A.7 (highlighted) are the objectives with **no ISO 27001 equivalent**: impact assessment and data governance.

From 38 controls *to your set.*



STATEMENT OF APPLICABILITY — THE BRIDGE

From 38 *to yours.*

The SoA turns 38 reference controls into HireIQ's control set. Each control: applicable or not, justified, implemented or not. Exclusions need a reason.

DRIVEN BY ASSESSMENT

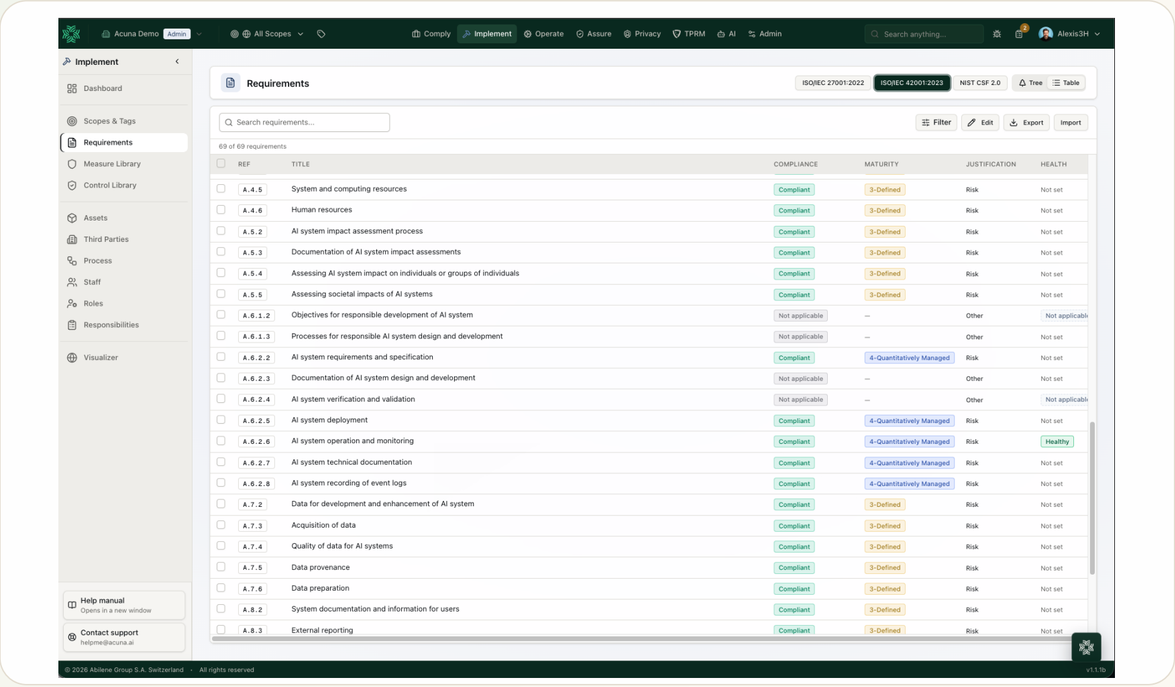
Risk and impact decide what applies, not a template.

JUSTIFY EVERYTHING

An excluded control still needs a defensible rationale.

FIRST DOC OPENED

The SoA is where every assessor starts.



38 REFERENCE CONTROLS TO YOUR SET

SECTION 04 · IN PRACTICE

From standard *to operations.*

How to operationalize the controls, with the impact assessment and register.

IN THIS SECTION — 10 MIN

Deep dives into the impact assessment, the third-party and data element and the register

A.5 impact and A.7 data, then the workflow guard in Acuna AIM

ACUNA AIM — THE MODULE

The operational *layer.*

Acuna already held both framework catalogs. What was missing was a concept of the AI system itself. AIM adds that operational layer: one register, two regime lenses.

`/ai/systems`

AI system register

Lifecycle to “approved for use”, risk tier, warnings.

`/ai/assessments`

Impact assessments

Structured assessment, frozen once approved.

`/ai/oversight`

Human oversight

Who can override or suspend each system.

`/ai/provenance`

Model provenance

Derived live from your supplier module.

`/ai/incidents`

AI incidents

Serious incidents carry a 72h notification clock.

The register and the impact assessment are where **enforcement lives.** That is what we will look at live.

OBJECTIVE A.5 · CLAUSE 6.1.4 — DEEP DIVE

Impact, *assessed.*

As deployer, you run this even though the vendor built the model. It asks who HireIQ could harm: rejected applicants, protected groups, people never asked.

INTENDED USE

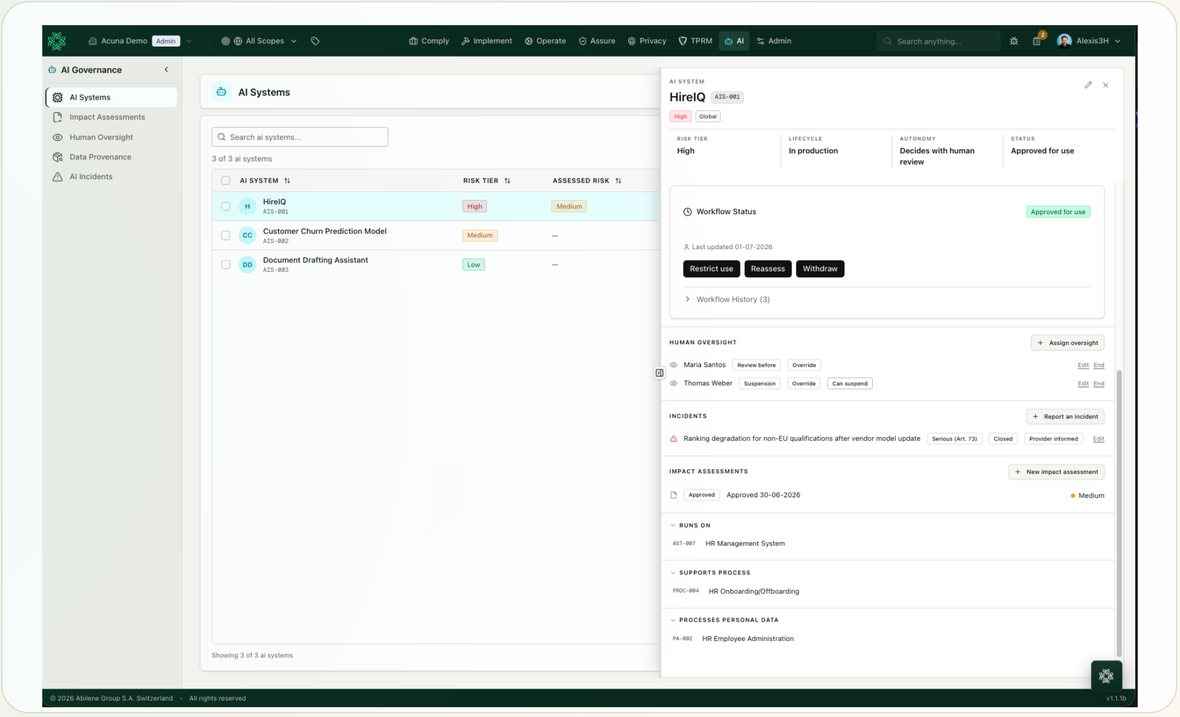
You run the structured assessment; the vendor cannot do it for you.

FORESEEABLE HARM

Bias against protected groups; opaque rejections.

OVERSIGHT & CONTEST

Who can override it, and how a person challenges a decision.



OBJECTIVE A.7 · DATA — DEEP DIVE

Data, *governed.*

As deployer you control the input data you feed HireIQ and must demand training-data provenance from the vendor. Bias hides in both.

QUALITY & BIAS

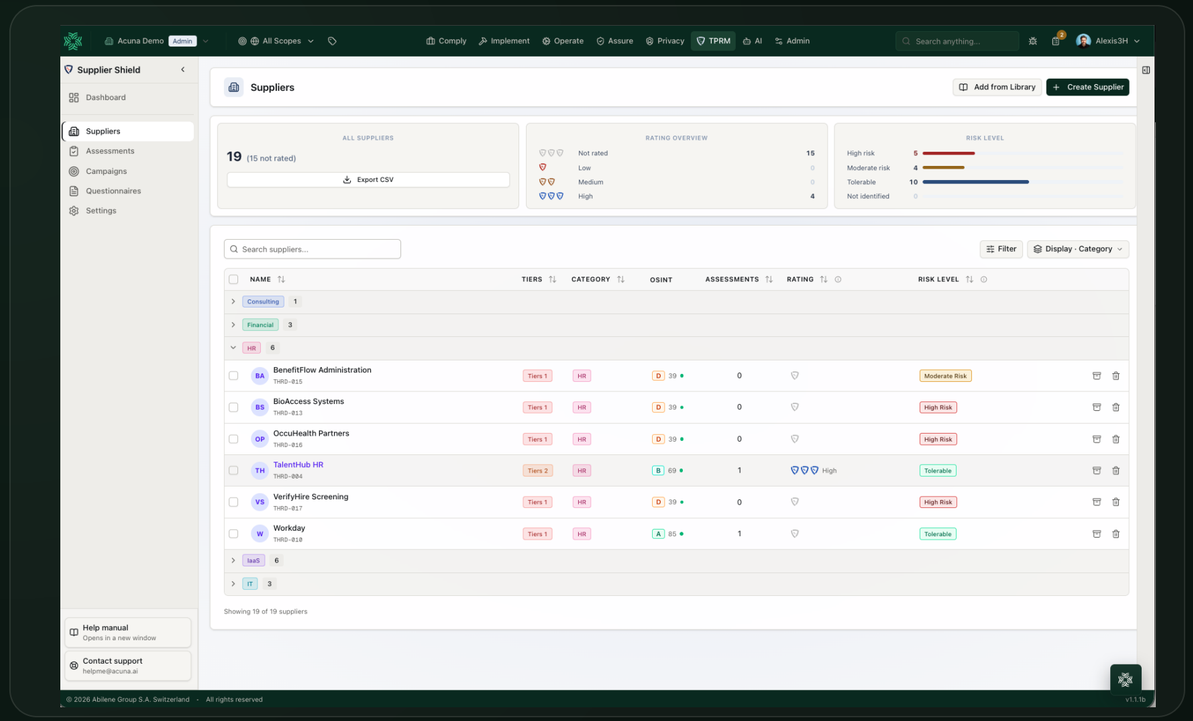
Your input data: relevant and representative?

PROVENANCE

No black box: get documentation, or don't deploy.

PREPARATION

Provenance derived live from your supplier module.



RUNNING THE AIMS — IN OPERATION

One register, *every framework.*

An AIMS lives or dies on evidence and upkeep. Run 42001 on the same platform as your ISMS so controls, evidence, and audits stay in one place.

LIVING INVENTORY

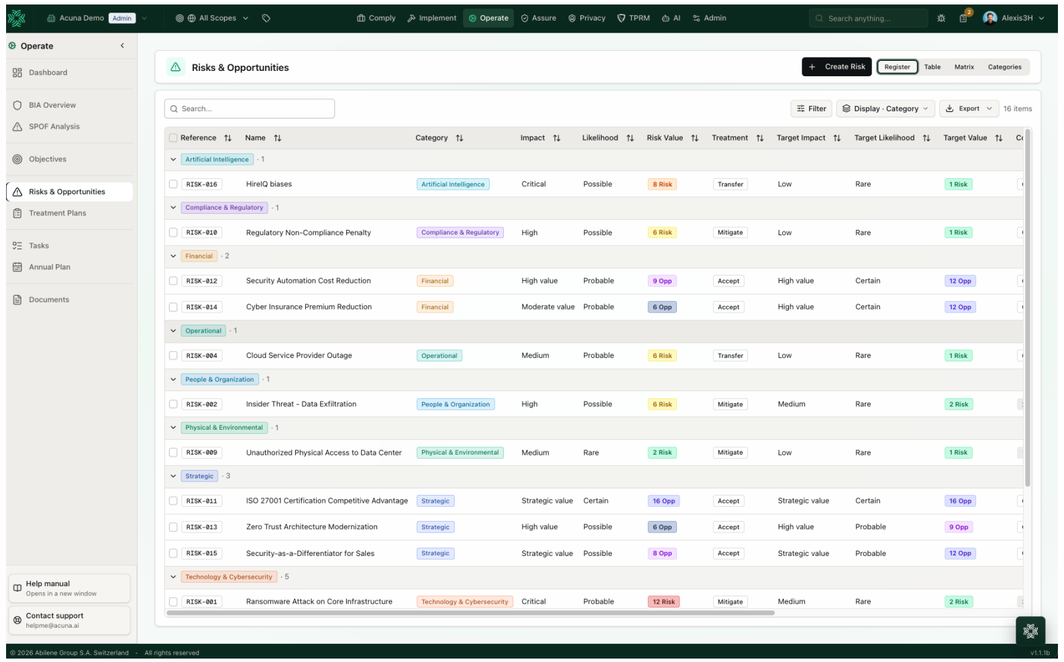
Use cases, risk tier, impact status in one register.

SHARED CONTROLS

Map 42001 to 27001 once; reuse evidence across both.

AUDIT-READY

A.10 third-party controls are the deployer's home base.



ENFORCEMENT — THE MODULE

The workflow *is the control.*

The governance control is not a policy document. It is a guard in the workflow: a system cannot be approved for use until an approved impact assessment exists.

1 REGISTER
AI system created
Not yet approved

→

2 ASSESS
Run the assessment
Submit for review

→

3 BLOCKED
Approve-for-use refused
The guard fires

→

4 APPROVE
the assessment
Status: completed

→

5 APPROVED
System approved
for use

> *“This AI system needs an approved impact assessment before it can be approved for use.”*

The message the platform shows at step 3. The workflow guard is the governance control, enforced on screen.

ENFORCED ON SCREEN

THANK YOU FOR YOUR TIME

Questions?

Ask anything about scoping an AIMS, the delta clauses, or running 42001 alongside your ISMS.

ah@acunagrc.com

ACUNAGRC.COM

SCAN TO CONNECT ON LINKEDIN

Alexis Hirschhorn

CEO, Acuna GRC · LinkedIn