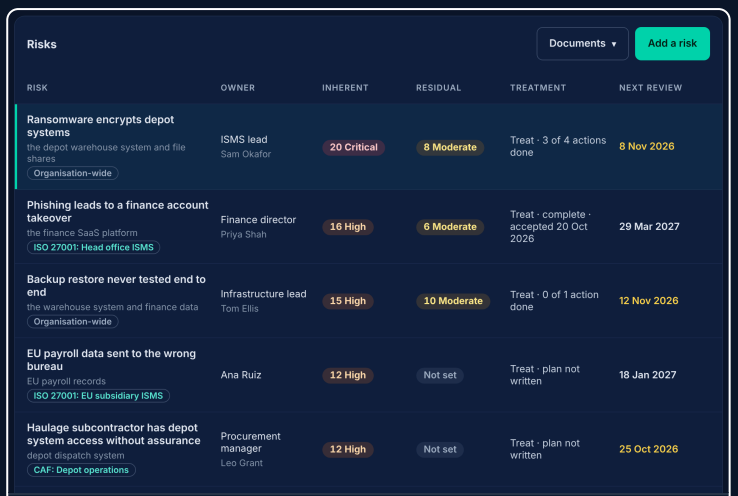
securitycompliancehub.io

RISK MANAGEMENT

Run your risks the way ISO 27001, ISO 42001 and the CAF expect

Your register, method, RACI, SoA, business assets and AI impact assessments, kept the way an auditor asks for them.

Certification and the CAF ask how you run risk between assessments: who owns each risk, how it was scored, what is being done, who accepted what is left, and when it was last looked at. The Risk management page keeps those records for your organisation or, for an MSP or vCISO, **for each client separately**. It runs on rules you can read and uses no AI, so it never counts against an allowance. **None of it waits for an assessment:** start here, and assess once your management system has taken shape.



The register. Each risk with its owner, its inherent and residual score on your own method, how its treatment is going and when it is next reviewed, labelled with the ISMS or essential function it belongs to. Illustrative data.

Register
PAGE 1

Every risk with its treatment, tracker actions and history.

Reviews
PAGE 2

Overdue and due in 30 days, the next date shown first.

Method
PAGE 2

Your scales, bands, acceptance and review intervals.

Accountability
PAGE 2

A RACI, complete on every row before it is approved.

Statement of Applicability
PAGES 2, 5

ISO 27001's 93 controls and ISO 42001's 38.

Business assets
PAGE 3

What you protect, in groups with owners. AI systems too.

Supplier risks
PAGE 4

From the Third Party Risk Hub, and kept current.

AI impact assessments
PAGE 5

Each AI system's harms, scored and kept current.

WHY IT LANDS ON YOUR DESK

What the standards ask, and where it is kept

ISO/IEC 27001:2022	ISO/IEC 42001	NCSC CAF	KEPT AS
5.3 Roles and responsibilities	5.3, A.3.2	A1.b	The RACI, approved by name, with its versions.
6.1.2 Risk assessment	6.1.2	A2.a	The method: how risks are scored and banded.
6.1.3 Risk treatment	6.1.3	A2.a	Treatment plans, accepted residual risk, each standard's SoA.
8.2, 8.3 Results	8.2, 8.3	A2.a	The register, every review and change in its history.
A.5.9, A.5.10 Assets	A.4.2–A.4.6	A3.a	Business assets in groups with owners; AI systems.
A.5.19 to A.5.22 Suppliers	A.10.3	A4.a	Supplier risks from the Third Party Risk Hub (page 4).
—	6.1.4, 8.4	—	AI system impact assessments (page 5).

Assessed, treated, reviewed and accepted

Your method, applied the same way to every risk, every time.

THE METHOD

- **Your own words** for the five likelihood and five impact levels, with impact described on up to five dimensions, such as money, operations and customers.
- **Where each band starts,** on the scores a 5 × 5 grid can make, and how often each band is reviewed.
- **An acceptance level,** and the role that must accept any residual risk above it.
- **Versioned.** A draft shows which risks would change band before anyone approves it by name.

Version 1, approved by name. Bands, acceptance and review intervals. Illustrative data.

Reviews come round on their own

A risk is reviewed by its inherent band while treatment is open, and by its residual band once it is done. Overdue and due-soon reviews are listed first. Closing a risk needs a note.

Acceptance by the right person

At or below your acceptance level the risk owner can accept the residual risk. Above it, only the role your method names can, and the name, role and date are kept.

A history that can't be rewritten

Every review, every change of score, status, owner or treatment, and every acceptance is kept in the risk's history. A saved review can't be edited or deleted.

STATEMENT OF APPLICABILITY

93 controls, with or without an assessment

Each control says whether it applies, why, how far it is implemented and which risks it treats, and it is approved by name once every control is decided and justified. **No assessment is needed.** Once you finalise one, **Pre-fill** fills in the controls nobody has set, never changes one a person set, and shows where the two differ. An AIMS has ISO 42001's own (page 5).

CONTROL	WHAT IT COVERS	APPLIES	IMPLEMENTATION	JUSTIFICATION AND SOURCE
ORGANISATIONAL CONTROLS (A.5)				
A.5.1	A top-level security policy and topic policies, approved, published and reviewed	Yes	Implemented	Treats risks in the risk assessment From the assessment, 14 Oct 2026
A.5.2	Security roles and responsibilities defined and assigned	Yes	Implemented	Treats risks in the risk assessment From the assessment, 14 Oct 2026
A.5.3	Conflicting duties separated to reduce misuse or error	Yes	Implemented	Treats risks in the risk assessment From the assessment, 14 Oct 2026
A.5.4	Managers require staff and contractors to follow security policy	Yes	Implemented	Treats risks in the risk assessment From the assessment, 14 Oct 2026
A.5.5	Contacts kept with regulators, law enforcement and other authorities	Yes	Implemented	Treats risks in the risk assessment From the assessment, 14 Oct 2026
A.5.6	Membership of security forums and specialist groups	Yes	Implemented	Treats risks in the risk assessment From the assessment, 14 Oct 2026
A.5.7	Threat information gathered, analysed and acted on	Yes	Partly implemented	Treats risks in the risk assessment From the assessment, 14 Oct 2026
A.5.8	Security built into every project, from start to finish	Yes	Implemented	Treats risks in the risk assessment From the assessment, 14 Oct 2026
A.5.9	An owned, current inventory of information and the assets that hold it Your asset register: 4 groups in use, all owned, reviewed within 12 months.	Yes	Implemented	Treats risks in the risk assessment From the assessment, 14 Oct 2026
A.5.10	Rules for acceptable use of information and assets Your asset register: 4 groups in use, all owned, reviewed within 12 months.	Yes	Implemented	Treats risks in the risk assessment From the assessment, 14 Oct 2026

Where each value came from. A.5.9 and A.5.10 show your asset register as evidence, without changing their status. Illustrative data.

ACCOUNTABILITY

Start the RACI from ISO 27001's clauses and Annex A themes, ISO 42001's, the CAF's 14 principles (with the NHS DSPT's four more), or blank rows. Risk owners, and the role that accepts risks above your level, are picked from its roles.

MORE THAN ONE ISMS OR AIMS?

Each named ISO 27001 or ISO 42001 scope and CAF essential function has its own view of the register, its own Statement of Applicability and its own Audit Pack. A risk to the whole organisation shows in every scope, labelled Organisation-wide. A scope can have its own risk method and RACI, or use the organisation's.

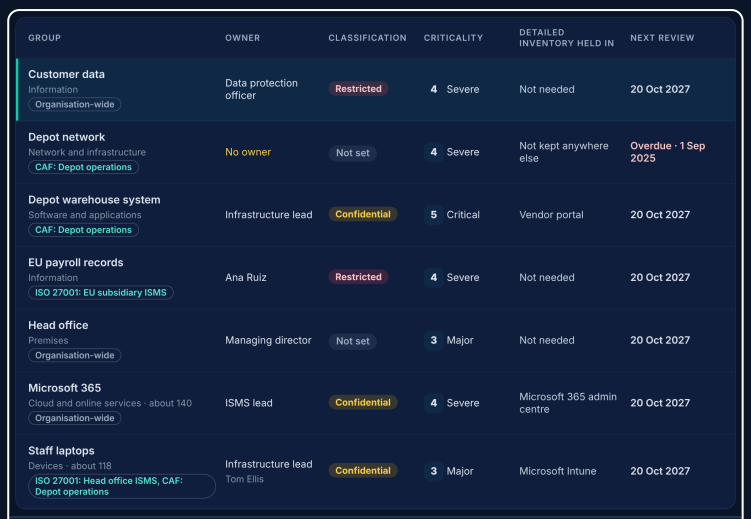
securitycompliancehub.io

BUSINESS ASSETS

Know what you protect, without another asset database

ISO 27001 A.5.9 and CAF A3.a, in groups with owners.

The Business assets tab holds the information your ISMS protects and the assets that hold it: "Customer data", "Staff laptops, about 120", "the finance system". Each group has an owner, a classification on your own levels, a criticality on your method's impact scale, where it is held and the scopes it supports, and comes round for review every 12 months unless you set a date. **A risk can name the groups it affects**, and each group lists its risks.



GROUP	OWNER	CLASSIFICATION	CRITICALITY	DETAILED INVENTORY HELD IN	NEXT REVIEW
Customer data Information Organisation-wide	Data protection officer	Restricted	4 Severe	Not needed	20 Oct 2027
Depot network Network and infrastructure CAF: Depot operations	No owner	Not set	4 Severe	Not kept anywhere else	Overdue · 1 Sep 2025
Depot warehouse system Software and applications CAF: Depot operations	Infrastructure lead	Confidential	5 Critical	Vendor portal	20 Oct 2027
EU payroll records Information ISO 27001: EU subsidiary ISMS	Ana Ruiz	Restricted	4 Severe	Not needed	20 Oct 2027
Head office Premises Organisation-wide	Managing director	Not set	3 Major	Not needed	20 Oct 2027
Microsoft 365 Cloud and online services · about 140 Organisation-wide	ISMS lead	Confidential	4 Severe	Microsoft 365 admin centre	20 Oct 2027
Staff laptops Devices · about 118 ISO 27001: Head office ISMS, CAF: Depot operations	Infrastructure lead Tom Ellis	Confidential	3 Major	Microsoft Intune	20 Oct 2027

Groups, not items. Each group of software, cloud services, devices or network kit says which tool holds its item-level list. Illustrative data.

WHY IT ISN'T A CMDB

- **No item-level fields:** no serial number, hostname, IP or MAC address, licence key, warranty or purchase date, and up to 300 groups.
- **No discovery or sync.** Device-by-device detail stays in Intune, your RMM or a spreadsheet, and the register names where.

SUGGEST GROUPS

From your technology stack, Microsoft 365's Intune count or CrowdStrike Falcon's device count, and common information groups. Nothing is added until you tick it.

IMPORT FROM A SPREADSHEET

Columns are matched by heading, and a preview comes first. Any other column never leaves your browser, and a list of individual devices is turned away.

FOR THE AUDITOR

Eight documents, printed, as CSV and in the Audit Pack

Risk assessment process and criteria	**6.1.2 · A2.a**	The method in force, its version and approval.
Risk register and assessment results	**8.2 · A2.a**	Both heat maps and every risk, for one scope or all.
Risk treatment plan and results	**6.1.3, 8.3**	Each plan, its tracker actions and the acceptances.
Statement of Applicability	**6.1.3 d**	The controls of one ISMS (93) or AIMS (38).
Roles and responsibilities (RACI)	**5.3 · A1.b**	The roles and who does what.
Inventory of information and associated assets	**A.5.9 · A3.a**	The groups by type; its CSV imports again.
Suppliers and their risks	**A.5.19–5.22 · A4.a**	With the Third Party Risk Hub: each supplier and its risks.
AI system impact assessments	**42001 6.1.4, 8.4**	Each AI system's harms on your method's scales.

For MSPs and vCISOs: each client has its own records, opened from its Risk & Remediation tab. Team members see only their clients; Viewers see everything and change nothing.

Screens are the shipped product showing a fictional company; names and figures are illustrative. Included wherever the Risk Register is: the Assessment Bundle, MSP plans and the specialist plans.

securitycompliancehub.io

SUPPLIER RISKS

Where your suppliers meet your risk register

The Third Party Risk Hub finds supplier risk, the register runs it, and each keeps the other current.

Risk Operations puts the Assessment Bundle, with this risk register, and the **Third Party Risk Hub** on one subscription. The hub sends each supplier a questionnaire and checks its answers against Risk Purview's external scan. Apart, a supplier risk is typed into the register once and goes stale. Together, **it starts from the supplier's own record, and the register hears when the supplier changes.** Rules decide each step, and nothing is raised, rescored or closed by itself.

1 · The hub finds it

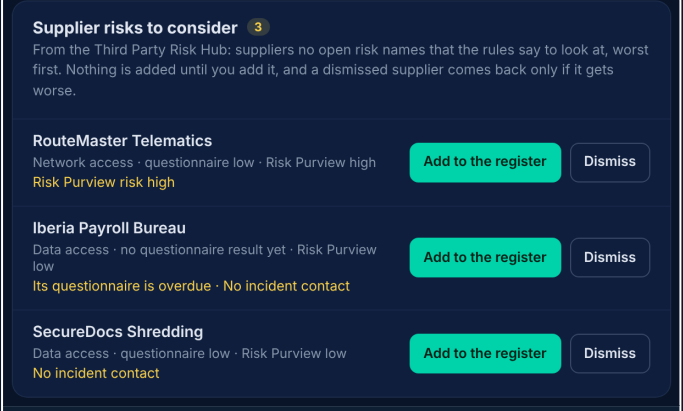
Suppliers no open risk names are suggested, worst first, with the reason: a critical Risk Purview finding, a high level with access to your systems or data, an overdue questionnaire or reassessment, no incident contact. A dismissed supplier comes back only if it gets worse.

2 · The register runs it

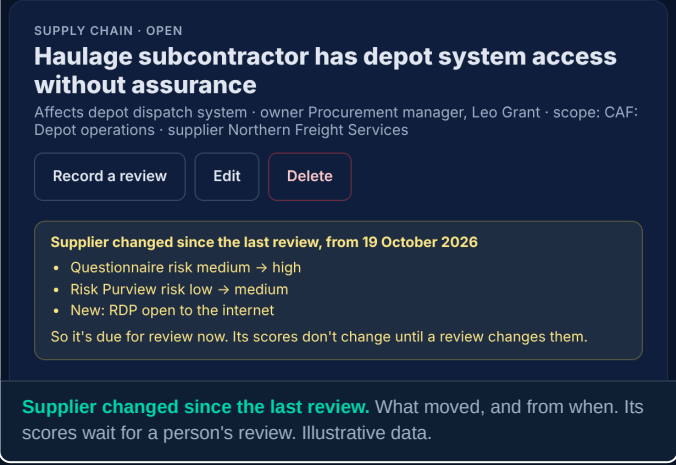
Add to risk register opens a risk filled in from the supplier's record. Its starting impact comes from the most critical business asset group naming the supplier, else its access; its likelihood from its levels. Owner, treatment and review follow your method, with the supplier's own open fixes alongside.

3 · Each keeps the other current

When a supplier gets worse (a level up, a score 10 lower, a new critical finding, a reassessment due), its risks say what moved and fall due for review that day. Each supplier's card in the hub shows its open risks and the highest band.



Supplier risks to consider. On the Register tab, each with the rule that put it there. Illustrative data.



Supplier changed since the last review. What moved, and from when. Its scores wait for a person's review. Illustrative data.

FOR THE AUDITOR

Supplier evidence beside the questions it answers

QUESTION	REF	THE NOTE UNDER IT GIVES
ISO 27001 supplier relationships	A.5.19–5.22	Suppliers with system, network or data access assessed in 12 months; whether each supplier risk has an owner and a treatment; your supplier security policy.
CAF risk management	A2.a	The open risks that name suppliers.
CAF supplier assessment	A4.a	The suppliers assessed in the last 12 months and scanned by Risk Purview in the last 30 days.
CAF supplier contracts	A4.a	What suppliers say their contracts include, such as incident notification, and the incident contacts given.

A note never fills in an answer, and says what the records can't show: the CAF notes support Partially Achieved at most. **Suppliers and their risks**, the seventh document, lists every supplier with its access, latest results, its own open fixes and the open risks naming it, printed, as CSV and in the ISO 27001, ISO 42001 and CAF Audit Packs.

BUSINESS ASSETS NAME THEIR SUPPLIER

Pick a group's supplier from the hub, or type one that isn't in it. The inventory then prints the supplier's access and levels beside the group.

FOR MSPS AND VCISOS

A client's risks name only that client's suppliers, and the client card in the MSP Portal counts the risks that name suppliers.

Screens are the shipped product showing a fictional company; names and figures are illustrative. Supplier risks need both halves: Risk Operations, the Assessment Bundle with the Third Party Risk Hub, or an MSP plan with the Third Party Risk add-on. With the hub alone, a supplier's card says the register comes with Risk Operations.

securitycompliancehub.io

ISO 42001 · AI MANAGEMENT

An AI management system, run the same way

ISO/IEC 42001's risks, Statement of Applicability, AI systems and impact assessments, beside your ISMS.

An AI management system (AIMS) is a scope like an ISMS: its risks are scored by your method and owned from your RACI, which can start from ISO 42001's own rows. What ISO 42001 adds is kept here too, by rules, **with no AI deciding anything**.

Its own Statement of Applicability

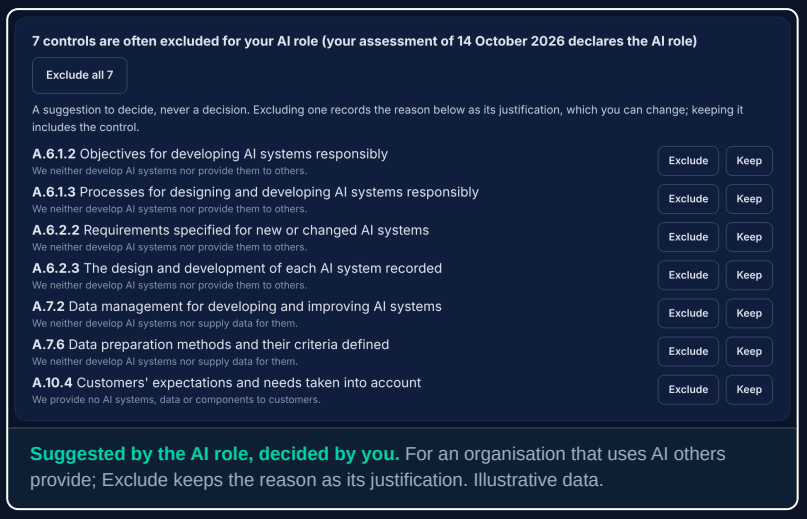
ISO 42001's 38 controls, pre-filled from your assessment. Those often excluded for its AI role are suggested, with the reason; nothing is excluded until you choose.

AI systems in Business assets

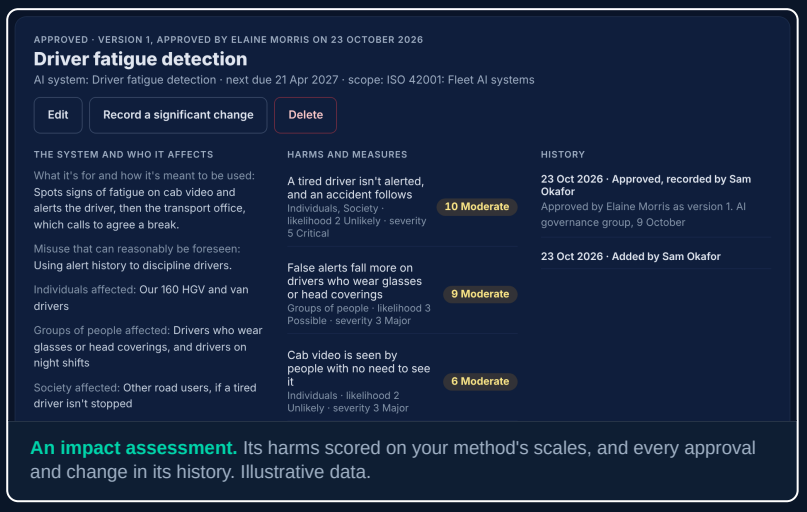
Each AI system with what it's for and its models, data, tools, computing and people (A.4.2 to A.4.6). Not a model card.

Impact assessments, kept current

Who each AI system affects and its harms, scored on your method and approved by name. Due again by your method, or at once after a significant change.



Suggested by the AI role, decided by you. For an organisation that uses AI others provide; Exclude keeps the reason as its justification. Illustrative data.



An impact assessment. Its harms scored on your method's scales, and every approval and change in its history. Illustrative data.

FOR THE AUDITOR

Notes under the ISO 42001 assessment, and its Audit Pack

QUESTION	REF	THE NOTE UNDER IT GIVES
Impact assessment	6.1.4, 8.4, A.5.2–A.5.5	Those approved and current, and AI systems without one.
Resources for AI systems	A.4.2–A.4.6	The AI systems' owners and each resource they record.
Roles, risk, treatment	5.3, 6.1.2, 6.1.3, 8.2, 8.3	The AIMS's RACI, method, register, plans and SoA.
Suppliers	A.10.3	The suppliers your AI systems name: Partially implemented at most.

Screens are the shipped product showing a fictional company; names and figures are illustrative. A note never fills in an answer. An impact assessment here isn't a DPIA or a fundamental rights impact assessment: it names the one that covers the same system. ISO 42001 certification isn't conformity with the EU AI Act.