Risk management, step by step

From a blank page to records an auditor can follow: for your own organisation, or for each client you look after.

This guide takes the Risk management page in the order the work is usually done. Each step says what to do, which tab it's on, what ISO 27001, ISO 42001 and the CAF ask for, and how you know you're done, with a box on doing the same for a client if you're an MSP or vCISO. The page runs on rules you can read and uses **no AI**, so nothing here counts against an analysis allowance. And **none of it waits for an assessment**: start here, and assess once your management system has taken shape.

NOT ONE SIZE FITS ALL

Your risk method, not ours

No two organisations weigh risk the same way. A haulier counts impact in depots out of action, a clinic in patients affected, a software company in customers it can't serve. The Hub doesn't hand you a fixed matrix: **you set the scales, the bands and the rules for treating and accepting risk**, and it applies them the same way to every risk, every time.

How risk is scored
Your words for each of the five likelihood and five impact levels, with impact described on up to five dimensions of your own: money, operations, customers.

Where each band starts
The scores at which Moderate, High and Critical begin on the 5 × 5 grid.

What you will accept
The residual score you're prepared to accept, and the role that must accept anything above it.

How often you look again
Each band's review interval, from a week to two years, or a date set on a single risk.

How each risk is treated
Treat, transfer, accept or avoid; the controls you choose; the actions behind them and a target date.

Who does what
A RACI started from ISO 27001, ISO 42001, the CAF or a blank page, then renamed, added to and cut down.

You also name your asset classification levels (two to six of them), and any ISMS, AIMS or essential function that works differently can have **a method and RACI of its own**. Every change is a new version, approved by name, and shows first which risks it would move.

THE EIGHT STEPS

In the order the work is done

	STEP	WHERE	YOU END UP WITH
1	**Roles and the risk method**	Accountability, Method	An approved RACI and a risk method in your own words
2	**Scopes, if you have several**	My Hub, then every tab	A view, a Statement of Applicability and documents for each ISMS, AIMS or essential function
3	**Business assets**	Business assets	What you protect, in groups with owners, classification and criticality
4	**Raise risks**	Register	Every risk with an owner, including those your suppliers bring
5	**Score and treat**	Register	Inherent and residual scores, treatment plans, acceptances by the right person
6	**Statement of Applicability**	Statement of Applicability	An approved SoA for each ISMS (93 controls) or AIMS (38)
7	**Review and keep current**	Reviews	Reviews on time, and every change in each risk's history
8	**Hand it to the auditor**	Documents, Audit Pack	Eight documents, and notes under each assessment question they support

1 **What to do** — In order, with the page's own button names.

✓ **Done when** — How you know the step is finished.

YOU DECIDE **Yours to set** — Not fixed by the Hub.

MSP **For an MSP or vCISO** — Doing the step for a client.

BEFORE YOU START

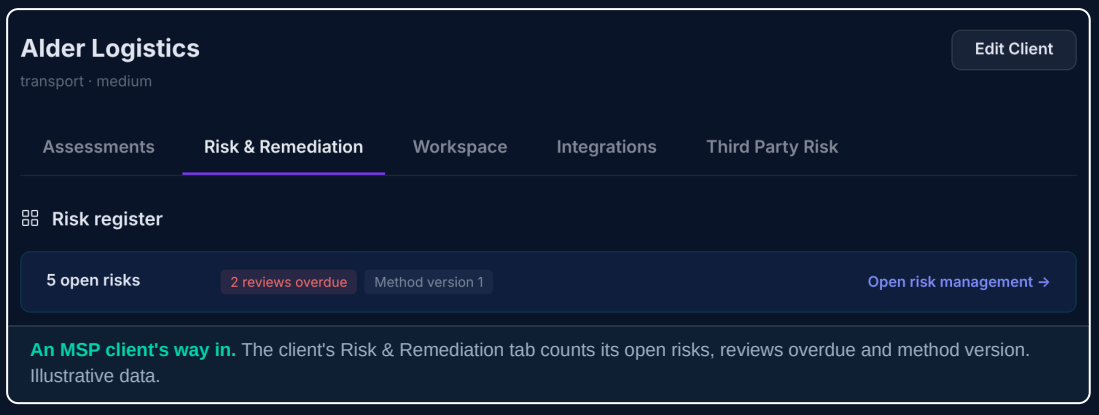
Where the page is, and who can change it

YOUR ORGANISATION

- **Open it** from My Hub: Risk & Remediation, then **Open risk management** on the Risk Register card.
- **Who can change it:** anyone on the Assessment Bundle, a specialist plan or an MSP plan. On a Team plan everyone works on the same records, and a read-only member sees them and changes nothing.
- **Supplier risks** need Risk Operations: the Assessment Bundle with the Third Party Risk Hub.

FOR AN MSP OR VCISO CLIENT

- **Open it** from the MSP Portal: the client, Risk & Remediation, then **Open risk management**. The page says **Client:** and the client's name.
- **Each client's records are its own**: method, RACI, register, SoA, assets and documents. Nothing is shared between clients.
- **Your team** sees only the clients they're given. A Viewer sees everything and changes nothing.
- No AI, so a client's three analyses a month are untouched.



An MSP client's way in. The client's Risk & Remediation tab counts its open risks, reviews overdue and method version. Illustrative data.

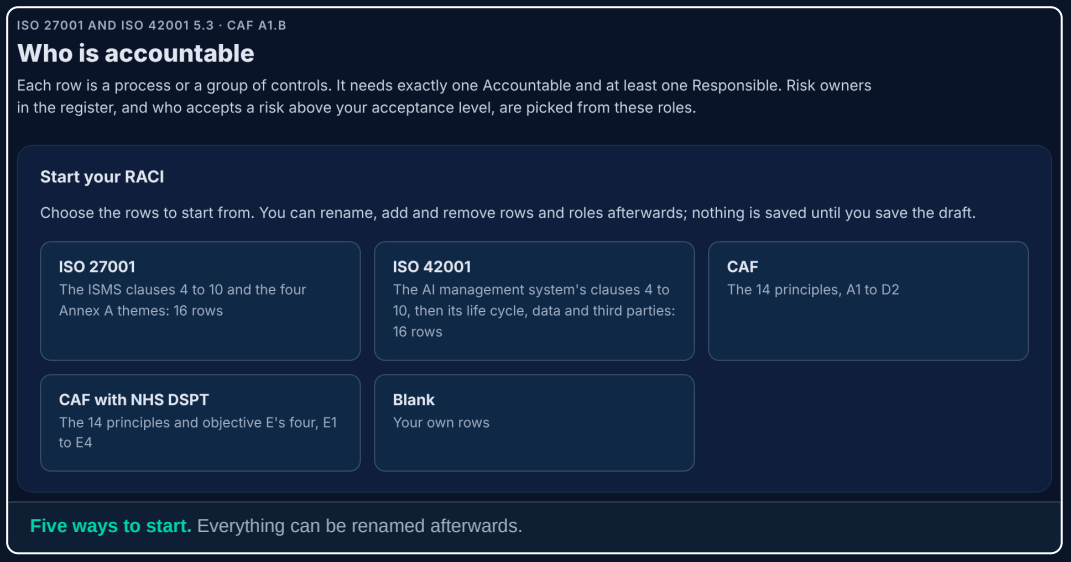
STEP 1 OF 8 Tabs: **Accountability**, then **Method**

Roles and the risk method

ISO 27001 and ISO 42001 5.3 and 6.1.2 · CAF A1.b and A2.a

Start with the RACI: **risk owners, and the role that accepts risk above your level, are picked from its roles**.

1. **Choose the rows to start from:** ISO 27001's or ISO 42001's 16, the CAF's 14 principles, the CAF with the NHS DSPT's four more, or a blank page.
2. **Name the roles:** a title, who holds it and an email. Rename, add or remove rows and roles until it matches how you're organised.
3. **Click each cell** to cycle R, A, C and I. Every row needs exactly one Accountable and at least one Responsible.
4. **Save the draft** as you go, then **Approve as version 1** with the approver's name. A draft can be incomplete; approval can't.



Five ways to start. Everything can be renamed afterwards.

STEP 1, CONTINUED Tab: **Method**

Say how you assess risk, in your own words

5. **Start version 1**. Say what each likelihood level means to you (“Expected within the next year”) and what each impact level means on each dimension you choose.
6. **Set where Moderate, High and Critical start**, the acceptance level and the role above it, and how often each band is reviewed.
7. **Approve as version 1**. Until you do, the defaults apply as version 0. A later version shows which risks would change band, and their review dates, before anyone approves it.

Impact

Scored at the worst of the 3 dimensions

#	NAME	MONEY	OPERATIONS	CUSTOMERS AND DATA
1	Minor	Under £10k	Hours of disruption	No customer data
2	Moderate	£10k to £50k	A day at one depot	Internal data only
3	Major	£50k to £250k	Several depots for a day	Some customer data
4	Severe	£250k to £1m	Most depots for days	Customer data, reportable
5	Critical	Over £1m	Operations stop	Large breach, regulator action

Impact in the company's own terms. Money, operations, and customers and data, scored at the worst of the three. Illustrative data.

Where each band starts

The grid can only make 1 to 6, 8, 9, 10, 12, 15, 16, 20 and 25

Critical	20	20 to 25 Grid scores: 20, 25
High	12	12 to 19 Grid scores: 12, 15, 16
Moderate	6	6 to 11 Grid scores: 6, 8, 9, 10
Low	1	1 to 5 Grid scores: 1, 2, 3, 4, 5

5	10	15	20	25
4	8	12	16	20
3	6	9	12	15
2	4	6	8	10
1	2	3	4	5

The heat map

Acceptance

Acceptance level (residual score) 5

Above it, accepted by **Managing director**

The role comes from the RACI: today, Elaine Morris.

How often each band is reviewed

Critical	every 30 days
High	every 90 days
Moderate	every 180 days
Low	every 365 days

The rules that follow from it. Where each band starts, what you accept and who accepts above it, and how often each band comes back. Illustrative data.

YOU DECIDE The level names and what each means, up to five impact dimensions, the three band cut-offs, the acceptance level and its role, and four review intervals (7 to 730 days). **Not one is fixed by the Hub.**

✓ **Done when** the Accountability and Method tabs both show version 1, approved by name.

FOR AN MSP OR VCISO CLIENT

Build each client's RACI from the client's own people. Keep the Accountable with someone at the client, and add your practice as a role where you do the work, as “vCISO (Harbourline IT)” here.

Agree the method's words with the client: their money, their operations, their customers. A template that suits one client rarely suits the next.

Approval is the client's. Type the name of the person at the client who approved it, not yours.

ROWS FROM ISO 27001		ISMS lead Hannah Ward Change	Board-level owner Martin Cole Change	IT lead Jo Patel Change	vCISO (Harbourline IT) Alex Rowan Change	CHECK
4.3	Scope of the ISMS	× R	A	I	C	✓ Complete
5.2	Information security policy	× R	A	C	C	✓ Complete
6.1.2	Risk assessment	× R	A	C	I	✓ Complete
6.1.3 e	Risk treatment plan	× R	A	I	C	✓ Complete
6.1.3 d	Statement of Applicability	× R	A	I	C	✓ Complete
6.2	Objectives and plans	× R	A	C	I	✓ Complete

A client's RACI, with the vCISO as a role. Illustrative data.

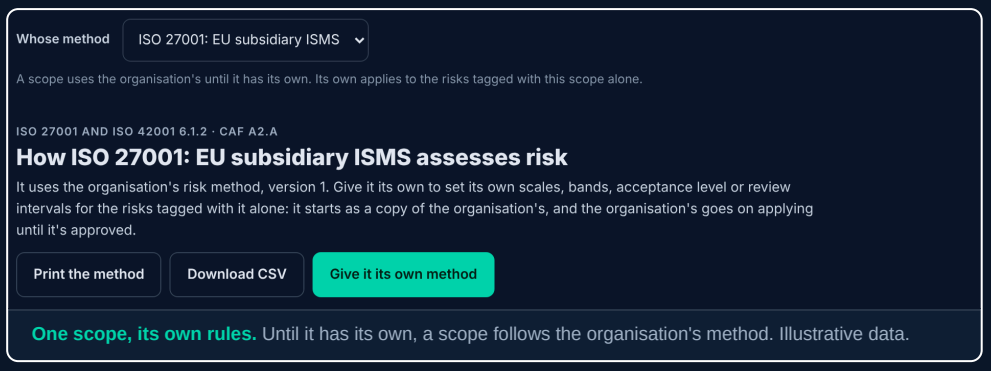
STEP 2 OF 8 Start in **My Hub**; then every tab

Scopes, if you run more than one

ISO 27001 and ISO 42001 4.3 · the CAF's essential functions

Skip this step if you have one ISMS, one AI management system (AIMS) or one essential function.

1. **In My Hub**, on the ISO 27001, ISO 42001 or CAF card, choose **+ Add another scope** and name it, such as “EU subsidiary ISMS”. Name the main run too.
2. **Tick the scopes** each risk and asset group belongs to. Tick none for the whole organisation: it shows in every scope, labelled Organisation-wide.
3. **Filter** the Register and Reviews by scope. Each scope has its own Statement of Applicability, and its assessment's Audit Pack carries its own documents.
4. **A scope that works differently** can have its own method or RACI: pick it under “Whose method” and choose **Give it its own method**. It starts as a copy of the organisation's.



One scope, its own rules. Until it has its own, a scope follows the organisation's method. Illustrative data.

FOR AN MSP OR VCISO CLIENT

The client's Assessments tab has **+ Add another scope** on its ISO 27001, ISO 42001 and CAF tiles, so one client can run several ISMSs or essential functions, each with its own register view and SoA.

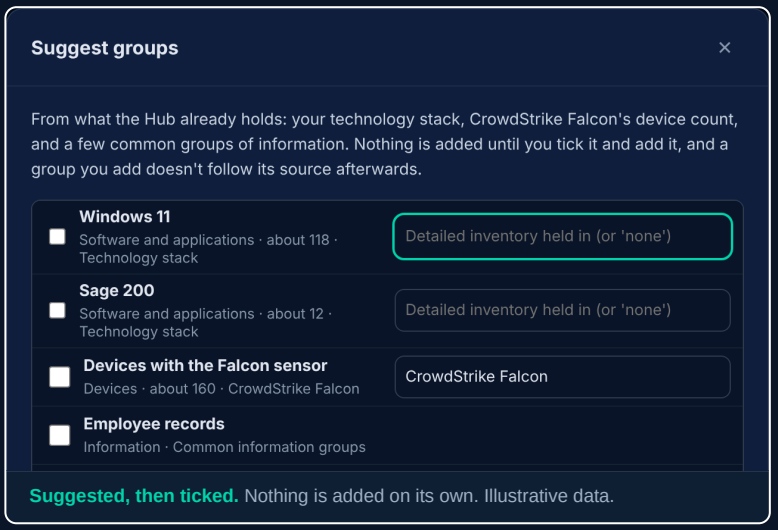
STEP 3 OF 8 Tab: **Business assets**

Business assets: what you protect

ISO 27001 A.5.9 and A.5.10 · ISO 42001 A.4.2 to A.4.6 · CAF A3.a

Groups, not items: “Customer data”, “Staff laptops, about 120”, “the finance system”. Device-by-device detail stays in Intune, your RMM or a spreadsheet, and the group says where.

1. **Classification and reviews**: **name your classification levels**, two to six, and how often groups are reviewed (yearly unless you change it).
2. **Suggest groups** from your technology stack, Microsoft 365's Intune count, CrowdStrike Falcon's device count and common information groups. Nothing is added until you tick it.
3. Or **Import from a spreadsheet**: download the template and check the preview. A list of single devices is turned away.
4. **Give each group** an owner from your RACI, a classification, a criticality on your impact scale and where it's held. Add each AI system with its purpose, models, data and people.



Suggested, then ticked. Nothing is added on its own. Illustrative data.

✓ **Done when** every group in use has an owner and none is overdue for review.

FOR AN MSP OR VCISO CLIENT

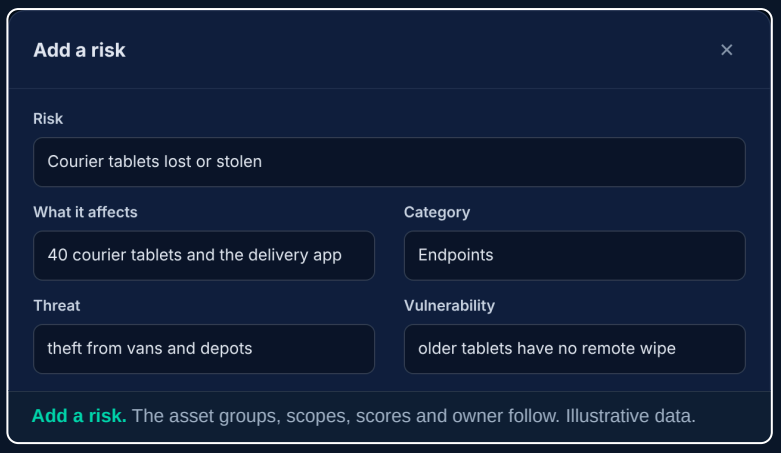
Suggestions read **the client's** Microsoft 365 or CrowdStrike Falcon, connected on the client's Integrations tab, and the client's own spreadsheet imports the same way.

STEP 4 OF 8 Tab: **Register**

Raise your risks

ISO 27001 and ISO 42001 6.1.2 · CAF A2.a

- **Add a risk** for anything an assessment can't see: a supplier you depend on, a building, the one person who knows the systems. Tick its asset groups and scopes.
- **From My Hub: + Add to Risk Register** on a cross-framework risk signal or a Remediation Tracker card. It starts from the signal's band; adjust it.
- **From your suppliers** (Risk Operations): **Supplier risks to consider** lists those no open risk names, worst first, and fills a risk in from the supplier's record.
- **Nothing is raised by itself.**



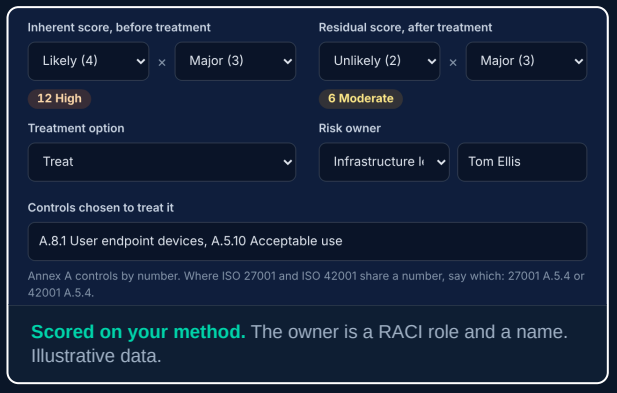
Add a risk. The asset groups, scopes, scores and owner follow. Illustrative data.

STEP 5 OF 8 Tab: **Register**

Score and treat each risk

ISO 27001 and ISO 42001 6.1.2 d–e, 6.1.3, 8.2 and 8.3 · CAF A2.a

1. **Inherent score:** likelihood × impact on your scales, before treatment.
2. **Choose how to treat it** and name the controls by number (A.8.13): each then lists the risk on the SoA.
3. **Link up to 10 Remediation Tracker actions** and set a target date. The register counts those done.
4. **Residual score:** where the risk will sit once treatment is done.
5. **Accept the residual risk**: the owner can at or below your acceptance level; above it, only the role your method names. Name, role and date go into the history.



Scored on your method. The owner is a RACI role and a name. Illustrative data.

The result: both scores, the plan, who must accept what's left, the history. Illustrative data.

FOR AN MSP OR VCISO CLIENT: STEPS 4 AND 5

Add a client's risks on the page or from **the client's** findings: **+ Add to Risk Register** on a Risk Scenarios row of the client's Risk & Remediation tab, or on the client's Remediation Tracker cards, adds it to the client's register. With the Third Party Risk add-on, so does **Add to risk register** on a supplier in the client's portfolio.

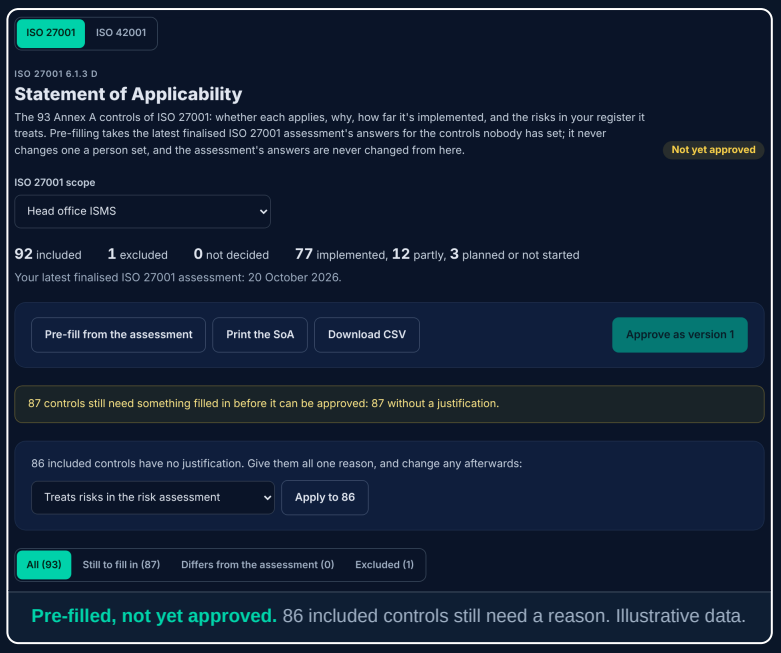
Accepting a risk is the client's decision: record the client's role holder, not yourself.

STEP 6 OF 8 Tab: **Statement of Applicability**

The Statement of Applicability

ISO 27001 6.1.3 d (93 controls) · ISO 42001 6.1.3 d (38 controls)

1. **Pick the standard and the scope.**
2. **Assessed already? Pre-fill from the assessment** sets the controls nobody has and never changes one a person set. “Differs from the assessment” shows where they disagree.
3. **Not yet?** Set each control by hand: whether it applies, how far it's implemented, and why.
4. **Give included controls one reason** in a click, then change any. A control a risk's treatment names is justified by it.
5. **For an AIMS**, the controls often excluded for your AI role are suggested with the reason. Nothing is excluded until you choose.
6. **Approve as version 1** once every control is decided and justified.



Pre-filled, not yet approved. 86 included controls still need a reason. Illustrative data.

FOR AN MSP OR VCISO CLIENT

Pre-fill reads **the client's** latest finalised run for that scope, so finalise the client's assessment first, from its Assessments tab.

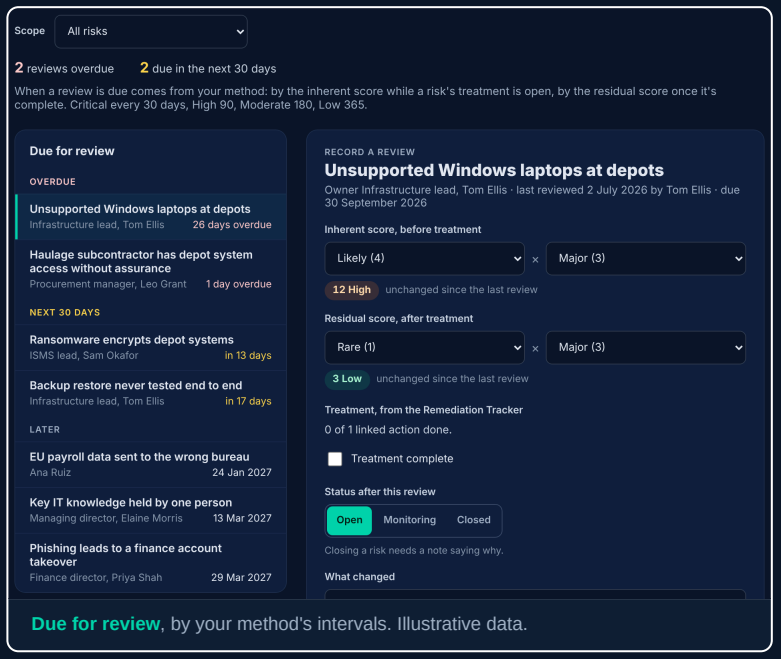
STEP 7 OF 8 Tab: **Reviews**

Review, and keep it current

ISO 27001 and ISO 42001 8.2 and 8.3 · CAF A2.a

1. **Open Reviews:** overdue first, then the next 30 days. The tab shows how many are due.
2. **Record a review**: the scores now, whether treatment is complete, the status (closing needs a note) and what changed.
3. **Leave the next date empty** to follow your method: the inherent band's interval while treatment is open, the residual band's once it's done.

- **A supplier that gets worse** puts the risks naming it due that day.
- **Asset groups** come round yearly; AI impact assessments at your method's interval, or after a significant change.
- **Nothing is rewritten.** Every review, change and acceptance stays in the risk's history.



Due for review, by your method's intervals. Illustrative data.

YOU DECIDE How often each band comes back, and a date of its own for any risk that needs one.

FOR AN MSP OR VCISO CLIENT

Each client's Risk register card in the MSP Portal counts its reviews overdue. Look through your clients once a month, and record each review with the client's risk owner.

STEP 8 OF 8 Each tab's documents, and the **Audit Pack**

Hand it to the auditor

1. **Print, or download as CSV,** from the tab each document belongs to: the register, the treatment plan and the suppliers document from the Register tab's **Documents** menu; the method, the RACI, the SoA, the inventory and the AI impact assessments from their own tabs.
2. **Generate the Audit Pack** from your finalised ISO 27001, ISO 42001 or CAF assessment. It carries the documents in a risk management folder, for that assessment's scope.
3. **Read the notes** under each ISO 27001, ISO 42001 and CAF question: what your records support, and where your answer differs. A note never fills the answer in.

DOCUMENT	ANSWERS	FROM
Risk assessment process and criteria	6.1.2 · A2.a	Step 1: the method in force, its version and approval
Roles and responsibilities (RACI)	5.3 · A1.b	Step 1: the roles and who does what
Inventory of information and associated assets	A.5.9 · A3.a	Step 3: the groups by type; its CSV imports again
Risk register and assessment results	8.2 · A2.a	Steps 4 and 5: both heat maps and every risk
Risk treatment plan and results	6.1.3, 8.3	Step 5: each plan, its actions and the acceptances
Statement of Applicability	6.1.3 d	Step 6: one ISMS's 93 controls, or an AIMS's 38
Suppliers and their risks	A.5.19–5.22 · A4.a	Step 4, with the Third Party Risk Hub
AI system impact assessments	42001 6.1.4, 8.4	For an AIMS: each AI system's harms on your scales

FOR AN MSP OR VCISO CLIENT

Generate the Audit Pack from **the client's** finalised assessment, opened from the MSP Portal: it carries that client's documents, never another's. Print a client's register and treatment plan for its management review.

RUNNING AN AI MANAGEMENT SYSTEM TOO?

Step 1
Start the AIMS's RACI from ISO 42001's rows, with an AIMS lead and AI system owners.

Step 3
Add each AI system as an asset: what it's for, its models, data, tools, computing and people.

Step 6
ISO 42001's 38 controls, with the exclusions usual for your AI role suggested, never applied.

AI impact assessments
One system: who it affects and its harms on your scales, approved by name (6.1.4, 8.4).

AFTER THE FIRST PASS

A year with the register

Each month
Clear the Reviews tab, and look at any risk whose supplier changed.

Each management review
Print the register and the treatment plan; record decisions as reviews and acceptances.

When things change
A new scope, a new version of the method or RACI, a new supplier or AI system.

Each year
Review the asset groups; finalise the assessment, pre-fill the SoA and approve its next version.

Before the audit
Generate the Audit Pack, and read the notes under each question.

ACROSS A PORTFOLIO OF CLIENTS

Every client follows the same eight steps with its own records. Each client's Risk register card in the MSP Portal shows where it is: open risks, reviews overdue, the method version, risks naming suppliers and AI impact assessments. Give team members the clients they work on, as Editors or Viewers.

Screens are the shipped product showing fictional organisations; names and figures are illustrative. Clause numbers refer to ISO/IEC 27001:2022, ISO/IEC 42001:2023 and the NCSC CAF. Risk management is included wherever the Risk Register is: the Assessment Bundle, MSP plans and the specialist plans. Supplier risks need Risk Operations, or an MSP plan with the Third Party Risk add-on.