for my Learning Tribe x

Ten steps to safe IT control of AI

What a CTO sets up before the people side of AI transformation starts. A sheet for every step.



Juliette Denny
Founder, Zavmo
juliettedenny.com

read this before you coach a single person

Who pays for the tokens? Answer that first.

The gap nobody plans for

We talk about AI transformation as a people job. Coach everyone, train everyone, get them using it. That part matters, and it is the part I love.

Then picture the Monday after the coaching. Someone in finance builds a workflow that checks invoices. It runs on tokens every day. Who approves the spend? Which data can it read? Who checks it before it goes live? In the organisations I talk to, there is rarely a process for any of it. And the better the coaching works, the more of these arrive.

this is the Monday problem

So the people side fails on the IT side. Here is how it usually goes.

1. **People use their own accounts.** Company data ends up somewhere you cannot see, audit or delete.
2. **Data goes into the wrong tool.** Nobody said which data is allowed where, so everybody guesses.
3. **A bill arrives that nobody planned.** Tokens are a running cost, and no team owns the line.
4. **AI writes code to nobody's standard.** If the standard is not written down, AI cannot follow it.
5. **A change reaches live without a review.** The pipeline was built for people working at people speed.

ask finance about number 3

How this workbook helps

Ten steps, one page each. Every page says what to set up, gives you a sheet to fill in, and says how you know it is done.

Work through it with your heads of engineering, security, data and finance. Start with the self-check on page 4, then fix the lowest score first.

When all ten are done, the coaching has somewhere to land.

Ten steps, four stages

the boring bits are the safe bits

Do them in this order. The ground first, then the rules, then the guard rails, then the door. Each step has its own page.

A Set the ground

1. **Choose** Approved tools, company accounts p5
2. **Classify** What data goes where p6
3. **Budget** Tokens are a cost line p7

B Write the rules down

4. **Document** Write down how you work p8
5. **Standardise** Standards a machine checks p9
6. **Design** One library of parts p10

C Put up the guard rails

7. **Gate** Every change through the pipeline p11
8. **Contain** What AI may do on its own p12
9. **Record** An audit trail you can show p13

D Open the door

10. **Open** One front door for new ideas p14

✓ Then the people

Coaching and mentoring for everyone. Last issue's workshop guide takes each team through six steps, one task at a time: Spot, Document, Agree, Trial, Share, Learn.

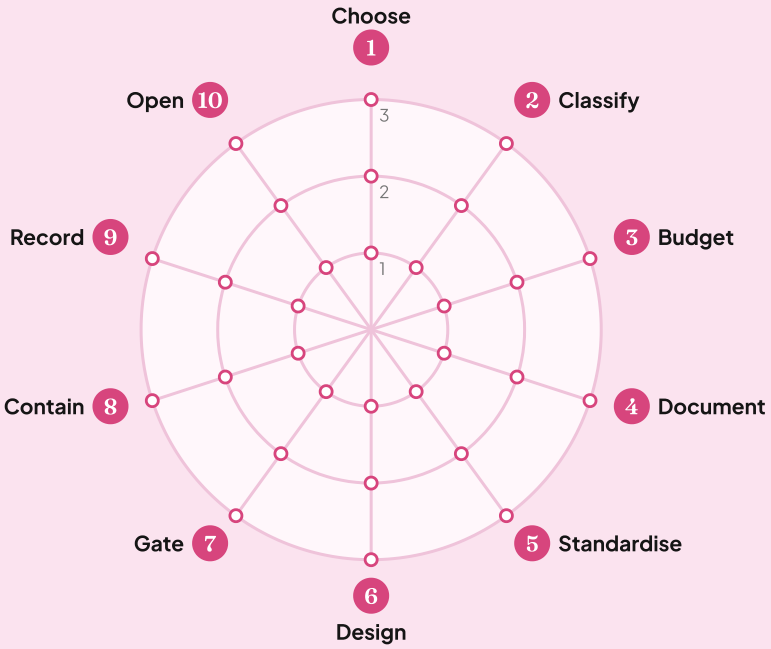
Start here

Where are you now?

3 means a machine checks it. Not a person.

Score each step from 0 to 3. Be harsh. A rule that is written down is a rule a person can forget. A rule a machine checks is one AI cannot skip.

#	Step	0	1	2	3	Owner
1	**Choose** Approved tools, company accounts	☐	☐	☐	☐	
2	**Classify** What data goes where	☐	☐	☐	☐	
3	**Budget** Tokens are a cost line	☐	☐	☐	☐	
4	**Document** Write down how you work	☐	☐	☐	☐	
5	**Standardise** Standards a machine checks	☐	☐	☐	☐	
6	**Design** One library of parts	☐	☐	☐	☐	
7	**Gate** Every change through the pipeline	☐	☐	☐	☐	
8	**Contain** What AI may do on its own	☐	☐	☐	☐	
9	**Record** An audit trail you can show	☐	☐	☐	☐	
10	**Open** One front door for new ideas	☐	☐	☐	☐	



The scores

- 0 Nothing in place
- 1 Started
- 2 Written down
- 3 A machine checks it

Mark each score on its spoke, then join the dots. The dents are where to start.

Total, out of 30: _____

Lowest step: _____

Step 1 of 10 · Set the ground

1 Choose

Approved tools, company accounts

one tool done well beats five done badly

People will use AI whether you approve it or not. So pick the tools you back, buy company accounts and switch on single sign-on. Then a person who leaves takes nothing with them.

○ Approved
Company account, single sign-on, a named owner.

● On trial
One team, a spend limit and an end date.

● Not allowed
Say so in writing, and say why.

Tool	What for	Company account	Single sign-on	Owner	○ Yes	● Trial	● No
		☐	☐		☐	☐	☐
		☐	☐		☐	☐	☐
		☐	☐		☐	☐	☐
		☐	☐		☐	☐	☐
		☐	☐		☐	☐	☐
		☐	☐		☐	☐	☐
		☐	☐		☐	☐	☐
		☐	☐		☐	☐	☐
		☐	☐		☐	☐	☐

Done when

- ☐ There is one list of approved tools, and everyone knows where it is.
- ☐ Every approved tool uses company accounts and single sign-on.
- ☐ Each tool has an owner, by name.

Step 2 of 10 · Set the ground

2 Classify

What data goes where

if in doubt, it's restricted

Not all data is equal. Sort yours into three levels, then decide which level each tool can take. Write it on one page that people will actually read.

Open

Public

Website copy, published reports, anything already out in the world.

Internal

Inside the company

Plans, code, meeting notes, anything you would not post but would not panic about.

Restricted

Personal, client or secret

Customer records, salaries, health data, passwords and keys.

Approved tool	○ Open	● Internal	● Restricted	Who signs off an exception
	☐	☐	☐	
	☐	☐	☐	
	☐	☐	☐	
	☐	☐	☐	
	☐	☐	☐	
	☐	☐	☐	
	☐	☐	☐	
	☐	☐	☐	
	☐	☐	☐	

Done when

- ☐ Every kind of data you hold has a level.
- ☐ Every approved tool says which levels it may take.
- ☐ Restricted data has a named owner who signs off any exception.

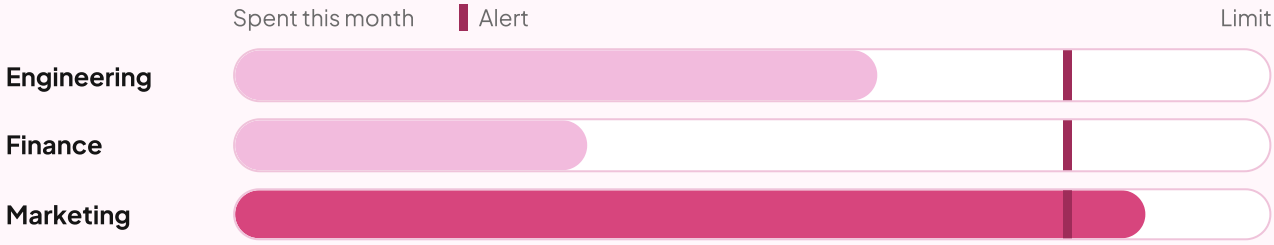
Step 3 of 10 · Set the ground

3 Budget

Tokens are a cost line

say who pays. Out loud.

Every AI workflow runs on tokens, and tokens cost money. Most finance teams have no line for them yet. Give each team a monthly limit, an alert before they reach it, and one way to ask for more. The better your people get, the bigger the bill. That is success, so plan for it.



An example. Marketing has passed its alert, so the budget owner hears about it before the limit, not after.

1. A team asks for more
2. The budget owner decides
3. The limit changes
4. Spend reviewed monthly

Team	Monthly limit	Alert at	Budget owner	Spent last month

The budget line sits in: _____

Reviewed every month by: _____

Done when

- [ ] Every team using AI has a limit and an alert.
- [ ] Finance has a line for tokens.
- [ ] Somebody looks at the spend every month.

Step 4 of 10 · Write the rules down

4 Document

Write down how you work

AI is a new starter every morning. This file is its induction.

AI follows what is written down, and nothing else. If how you work lives in people's heads, AI will guess. Every code base needs a short file written for AI: how we work here, what this connects to, what never to touch.



README
What this is, and how to run it.



AI instructions
How we work here. What never to touch.



The map
What runs where, and what connects to what.



Decisions
Why it is built like this, and when we chose.

Code base	README	AI instructions	The map	Decisions	Last checked
	☐	☐	☐	☐	
	☐	☐	☐	☐	
	☐	☐	☐	☐	
	☐	☐	☐	☐	
	☐	☐	☐	☐	
	☐	☐	☐	☐	
	☐	☐	☐	☐	
	☐	☐	☐	☐	
	☐	☐	☐	☐	

Done when

- ☐ Every active code base has an AI instructions file.
- ☐ There is one map of what runs where.
- ☐ Each file says when it was last checked.

Step 5 of 10 · Write the rules down

5 Standardise

Standards a machine checks

the linter never gets tired

A coding standard that lives in a senior developer's head never reaches an AI. Write it down. Then hand it to a machine to check on every change, so nobody has to remember.

1. **Written down**
   One place, plain words.

2. **A machine checks it**
   On every change, every time.

3. **It blocks the merge**
   Break it and the change cannot land.

Standard	Written where	Tool that checks it	Runs on every change	Blocks the merge
			☐	☐
			☐	☐
			☐	☐
			☐	☐
			☐	☐
			☐	☐
			☐	☐
			☐	☐
			☐	☐
			☐	☐

Done when

- ☐ Your standards are written in one place.
- ☐ A machine checks them on every change.
- ☐ A change that breaks one cannot merge.

Step 6 of 10 · Write the rules down

6 Design

One library of parts

reuse the button!

Ask AI for a new screen and it will happily invent a new button. Then another. Atomic design stops that. Build small parts once, combine them into bigger ones, and tell AI to use the parts you already have.



Atoms
A colour, a font, an icon

Molecules
A search box

Organisms
A card, a header

Templates
A layout, no content

Pages
The real thing

Our design system lives in:

Who owns it:

Colours and fonts are set in:

AI is told to use it in:

Part	Atom to page	Where it lives	AI uses it
			☐
			☐
			☐
			☐
			☐
			☐
			☐
			☐

Done when

- ☐ There is one library of parts, and AI is told to use it.
- ☐ Colours and fonts are set in one file, nowhere else.
- ☐ A new part needs a person's approval.

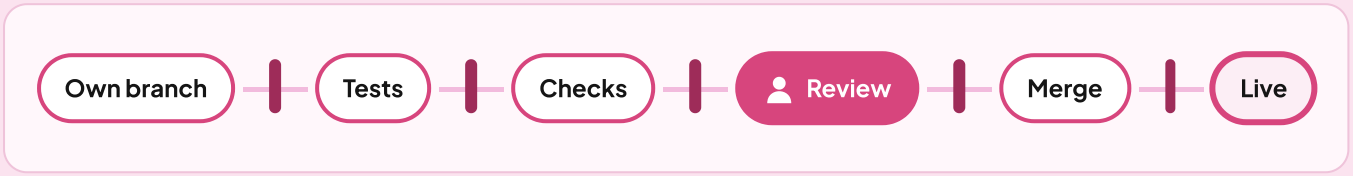
Step 7 of 10 · Put up the guard rails

7 Gate

Every change through the pipeline

AI writes faster than anyone can read. The pipeline reads first.

AI writes code fast. That is the point, and it is also the risk. Every change goes the same way: its own branch, automatic checks, a person's review, then merge. Nobody, human or AI, pushes straight to live.



Each bar is a gate. A change that fails one stops there, whoever or whatever wrote it.

Our pipeline

- [ ] The main branch is protected. Nobody pushes to it directly.
- [ ] Tests run on every change.
- [ ] A security scan runs on every change.
- [ ] A person reviews every change AI writes.
- [ ] Live is deployed from main, and only from main.
- [ ] We have rolled back a bad change, on purpose, to prove we can.

Required check	What it catches	Owner

Done when

- [ ] Nothing reaches live without passing the pipeline.
- [ ] Every AI change has a named human reviewer.
- [ ] A rollback has been tested, not just planned.

Step 8 of 10 · Put up the guard rails

8 Contain

What AI may do on its own

I learned this one the hard way. Two agents, one folder.

Decide what AI can do on its own before it does it. Write three lists: on its own, with a person's approval, never. Keep production keys away from it. Give each agent its own workspace, so two agents never write in the same place.

On its own

- Read the code
- Run the tests
- Draft a change on its own branch

With a person's approval

- Merge a change
- Add a new package
- Spend past its limit

Never

- Hold production keys
- Push straight to live
- Delete live data

Action	○ On its own	● With approval	● Never	Agreed by
	☐	☐	☐	
	☐	☐	☐	
	☐	☐	☐	
	☐	☐	☐	
	☐	☐	☐	
	☐	☐	☐	
	☐	☐	☐	
	☐	☐	☐	
	☐	☐	☐	
	☐	☐	☐	

Done when

- ☐ The three lists are written down and agreed.
- ☐ No AI tool can reach production keys or passwords.
- ☐ Each agent works in its own space.

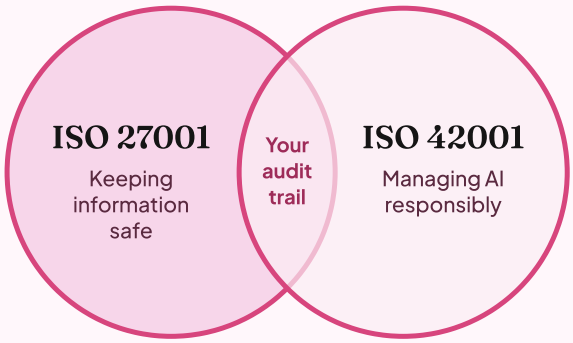
Step 9 of 10 · Put up the guard rails

9 Record

An audit trail you can show

the auditor will ask. Be ready.

One day somebody will ask what AI changed, and who said yes. Keep the answer. If you hold ISO 27001, map AI to the controls you already have. ISO 42001 is the standard written for managing AI.



1. **Who asked?**
2. **What changed?**
3. **Who approved it?**

Three answers for every AI change. If you can give all three, you can show an auditor.

Control or rule	What AI changes about it	Evidence we keep	Owner

Done when

- [ ] Every AI change can be traced back to a person.
- [ ] Logs are kept for as long as your policy says.
- [ ] Your next audit includes AI.

Step 10 of 10 · Open the door

10 Open

One front door for new ideas

make it easy to say yes

Once people are trained, ideas arrive fast. Give them one front door: a short form, one owner and a quick answer. A slow door teaches people to go round it.

1 An idea › **2 The front door form** › 3 The owner decides › 4 Rules and budget set › 5 Trial › 6 Live

At step 3 the answer is yes, no or not yet. A no comes with a reason. A not yet comes with a date.

The front door form

Photocopy this. Or turn it into your real one.

Your name and team: _____

The task, in one sentence: _____

How often it happens: _____

The tool you want to use: _____

Who checks what comes out: _____

Rough cost per month: _____

What it saves: _____

What could go wrong: _____

The data it uses ○ Open ☐ ● Internal ☐ ● Restricted ☐

Decision Yes ☐ No ☐ Not yet ☐ By: _____ Date: _____

Done when

- ☐ Everybody knows where the front door is.
- ☐ Every request gets an answer within a set time.
- ☐ Approved ideas get a budget line and a reviewer.

Ready for the people

When every step scores a 3, sign it off. Then start the coaching. People can learn a new workflow on Tuesday and know exactly how to get it approved on Wednesday.

Ready

1. Choose
2. Classify
3. Budget
4. Document
5. Standardise
6. Design
7. Gate
8. Contain
9. Record
10. Open

CTO: _____ **Head of security:** _____

Finance: _____ **Date:** _____

Start on Monday

1. Take the self-check with your heads of engineering, security, data and finance.
2. Pick your lowest score and give it an owner, by name.
3. Answer one question in writing. Who pays for the tokens?

Now the people side

Last issue's workshop guide, **The journey to becoming an AI first organisation**, takes each team through six steps, one task at a time, with the people who do the work.

The Future Fluency check tells each person whether to start at Level 3 or Level 5.

zavmo.ai/future-fluency-check

now coach everyone!



I would love to know which step was hardest. Tell me what broke. For the next one, join Juliette's Learning Tribe on LinkedIn.

Juliette