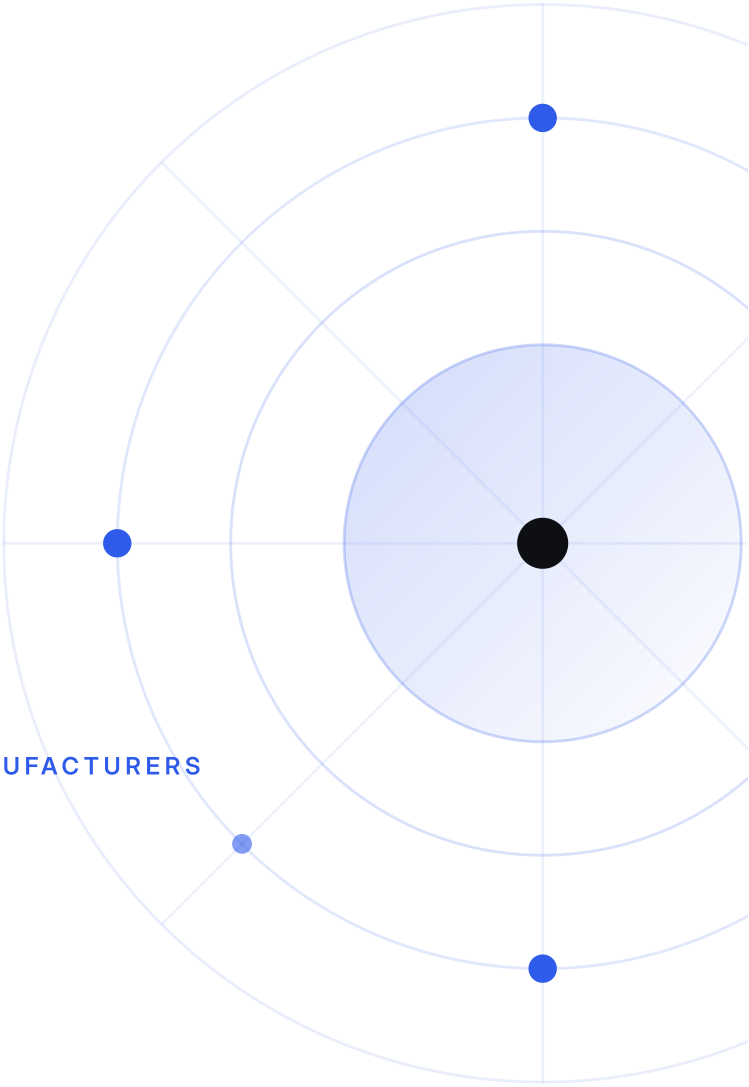
Aspirica

PLAYBOOK
EDITION 1.0 · NOVEMBER 2026



A PRACTICAL PLAYBOOK FOR MID-SIZED MANUFACTURERS

Technology Mastery

How to rescue, modernise and secure the systems a manufacturing business runs on, without a full-time technology executive.

Gareth Rooney

Fractional CIO and CTO · CIO 100 UK 2025 and 2026 · C|CISO

Published by Aspirica Ltd
aspirica.co.uk

About this playbook

This playbook sets out the method I use to take over a struggling technology function in a mid-sized manufacturer, find out what is really wrong, and leave the business with systems, security and people that can carry its growth.

It is written for owners, managing directors and finance directors of manufacturing businesses with roughly 50 to 1,000 staff: companies large enough to depend completely on their systems, but rarely large enough to employ a full-time Chief Information Officer. It is also written for the technology managers inside those businesses, and for other fractional executives who want a tested way of working.

The method comes from eighteen years of leading technology in organisations of this size, first as an employee and since 2021 as a fractional CIO and CTO serving several organisations at once. Every organisation in this playbook is described by its sector and size rather than its name, and no client's confidential information is included.

How to use it

- **Part 1** describes the problem and how to recognise it early.
- **Part 2** is the method itself: four stages, eight areas of assessment, and the rules I use to decide what to do first.
- **Parts 3 and 4** cover the two subjects boards now ask about most: cybersecurity and artificial intelligence.
- **Part 5** covers people and governance, which is where most programmes are won or lost.
- **Part 6** shows the method in practice. **Part 7** notes what changes for manufacturers in the United States.
- **The toolkit** at the back contains the templates. You are free to copy and use them.

> **Free to use.** You may copy, share and adapt this playbook and its toolkit, including for commercial use, provided you credit "Technology Mastery, Gareth Rooney, Aspirica Ltd". It is general guidance, not advice for any particular business.

© 2026 Gareth Rooney and Aspirica Ltd. Edition 1.0, published November 2026. Aspirica Ltd is registered in England and Wales, company number 12394752.

CONTENTS

Contents

1	Why mid-sized manufacturers struggle with technology	3
2	The method: Discover, Assess, Recommend, Plan	5
	Eight principles · The eight areas · Rescue, restart or stop · Triage · Options · Partners · Roadmap	
3	Owning security	11
4	Artificial intelligence: govern first, then adopt	13
5	People and governance: build to replace yourself	15
6	The method in practice	17
7	Notes for manufacturers in the United States	20
8	If you only have this playbook	22
T	The toolkit: seven templates	23
	Sources · About the author	31

98%

of U.S. manufacturing firms are small businesses (SBA Office of Advocacy, 2025)

35%

of small and medium-sized U.S. manufacturers employ a cybersecurity leader (MxD, 2024)

5 yrs

in a row as the most targeted industry for cyber attacks (IBM X-Force, 2026)

PART 1

Why mid-sized manufacturers struggle with technology

The problem is rarely the technology. It is that nobody senior owns it, and the business has no spare people to put it right.

A mid-sized manufacturer runs on a handful of core systems. The enterprise resource planning (ERP) system plans production, buys materials, runs the warehouse, and ships and invoices orders. Around it sit the customer relationship management (CRM) system, the website and e-commerce, electronic data interchange with customers and suppliers, and the reporting the board relies on. When those systems struggle, the whole business struggles with them.

The first signs of trouble

Trouble almost always shows first as a **bottleneck**. One part of the business cannot keep up, and the backlog creates knock-on problems elsewhere. At one schoolwear manufacturer I worked for, the old order system could process about 1,500 orders a day at peak. Above that, processing overran and created backlogs that took weeks to clear: late deliveries, chased invoices and unhappy customers, all from one constraint.

Signs you can see from the board

- Spreadsheets running alongside the ERP system, because people no longer trust it.
- Month-end taking longer every quarter.
- Stock figures nobody believes, and buffer stock to compensate.
- Peak periods that end in backlogs measured in weeks.

Signs inside the technology team

- A systems project that has been "nearly live" for more than a year.
- Knowledge held by one or two people and written down nowhere.
- Unsupported servers and software still running core processes.
- Security tools that are paid for but never switched on.

Why mid-sized manufacturers end up here

I have seen every one of the following causes, often several at once:

- **No one at board level owns technology.** It sits under the finance director as one responsibility among many, or with an IT manager who is not in the room when the business decides where it is going.

- **The wrong partner, chosen the wrong way.** Implementation partners are often chosen on day rate or a single demonstration, without testing their experience of the sector.
- **Under-investment**, especially in the unglamorous work: replacing unsupported platforms, testing backups, documenting systems.
- **No spare people.** When a large company has a systems problem, it can move people onto it. A mid-sized manufacturer has to keep producing and shipping with the same staff, so there is nobody to bail it out.

Why programmes stall

Most of the programmes I have been asked to rescue had not failed for technical reasons. They had run out of energy:

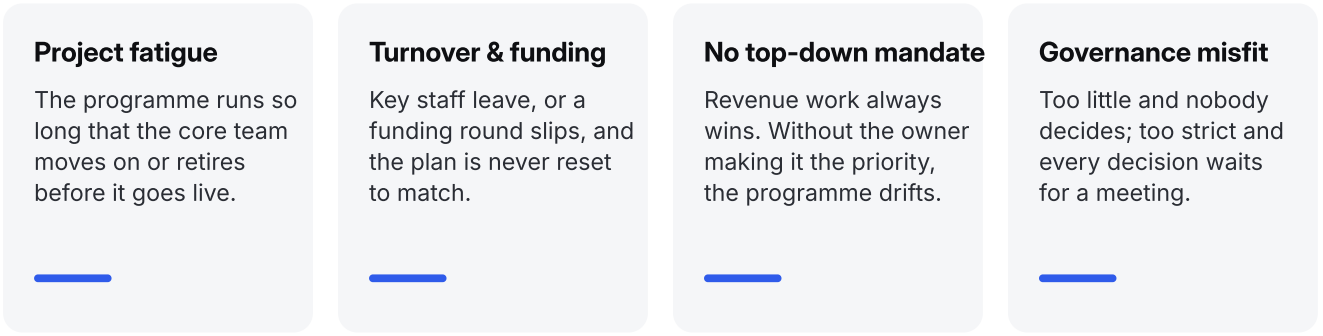


Figure 1. The four reasons I most often find behind a stalled systems programme.

> **Why this matters beyond the company.** Small businesses make up more than 98 percent of U.S. manufacturing firms, and only 35 percent of small and medium-sized manufacturers employ a dedicated cybersecurity leader. These companies supply larger manufacturers and critical infrastructure. When their systems fail or are breached, the effect travels along the supply chain.

The answer for most of these businesses is not a full-time executive they cannot justify. It is a share of an experienced one, working to a clear method, who builds the business's own capability and then steps back. The rest of this playbook describes that method.

PART 2

The method: Discover, Assess, Recommend, Plan

A whole-of-technology review in the first thirty days, then a costed plan the board approves and the business can deliver.

Every engagement starts the same way. Before I change anything, I build a complete picture of the business's technology and judge it against where the business is going, not against an abstract standard. The output is a review the board can act on, usually within the first thirty days.



Figure 2. The four stages. The first three normally complete within thirty days and end in a board playback; the plan then runs for 12 to 24 months.

Stage 1: Discover

I talk to the people who run the business before the people who run the technology: the owner or managing director, the finance director, operations, sales and customer service, then the IT team and the key suppliers. I visit the sites, because a factory floor shows things a system diagram does not. I collect the costs, the contracts and licences, the policies, and any earlier reviews. Each review records how much evidence it rests on: the people interviewed, sites visited, and systems and documents reviewed.

The first question is always where the business is going: acquisitions, new plants, new markets, a sale. Technology is judged against that ambition.

Stage 2: Assess

I rate the business in eight areas, each against good practice for a company of its size. Each area receives a rating and a priority. The ratings go on one page, so the board sees the whole picture at a glance.

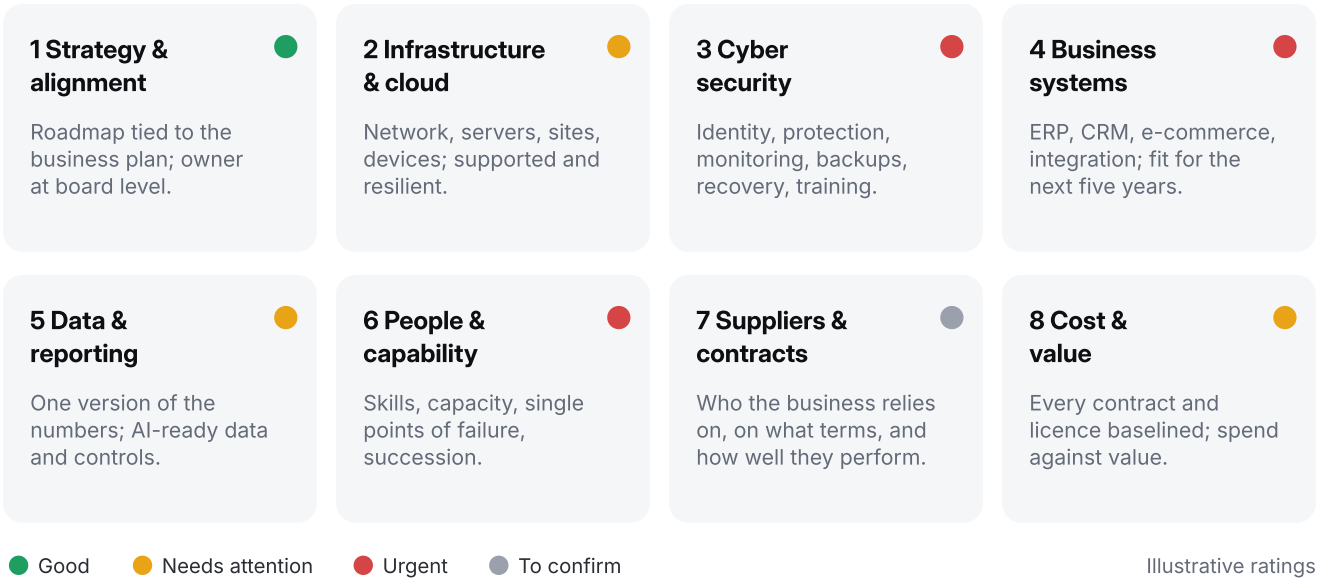


Figure 3. The eight areas of assessment. Each area is rated and given a priority (high, medium or low). The blank scorecard is Tool 1 in the toolkit.

For each area I record what is working as well as what is not. Boards act faster on a review that recognises the strengths of their team. I then set out the remedial actions needed to move every area to green, with a rough effort and timescale for each.

Eight principles

The same principles decide almost every judgement in the method:

1 **Judge technology against where the business is going**

A system that is adequate today can be the main obstacle to an acquisition or a new plant. The business plan sets the standard.

2 **Find the root cause before prescribing the remedy**

A stalled programme can look the same whether the system, the partner or the internal team is at fault. The cure is different for each.

3 **Triage: fix what could stop the business first**

Production and transactions come first, then anything customer-facing, then everything else.

4 **Own security, and hand the operation to specialists**

Someone senior must own cyber risk. Wherever possible, the round-the-clock work is backed out to a managed security service provider.

5 **Choose partners for sector experience, through a scored tender**

A partner who has done it before in your sector is worth more than a lower day rate.

6 **Get approval to spend to the plan**

The board approves a costed plan once, then governs progress against it, rather than approving every purchase.

7 **Right-size the governance**

Enough structure to make decisions quickly; never so much that every decision waits for a meeting.

8 **Always build to replace yourself**

A fractional leader succeeds when the business no longer needs them for day-to-day leadership.

Rescue, restart or stop

When a programme is in trouble, the instinct is to add money or people. Sometimes that is right. Often it makes things worse. I first establish which of three things is at the root of the problem, and only then choose the remedy.

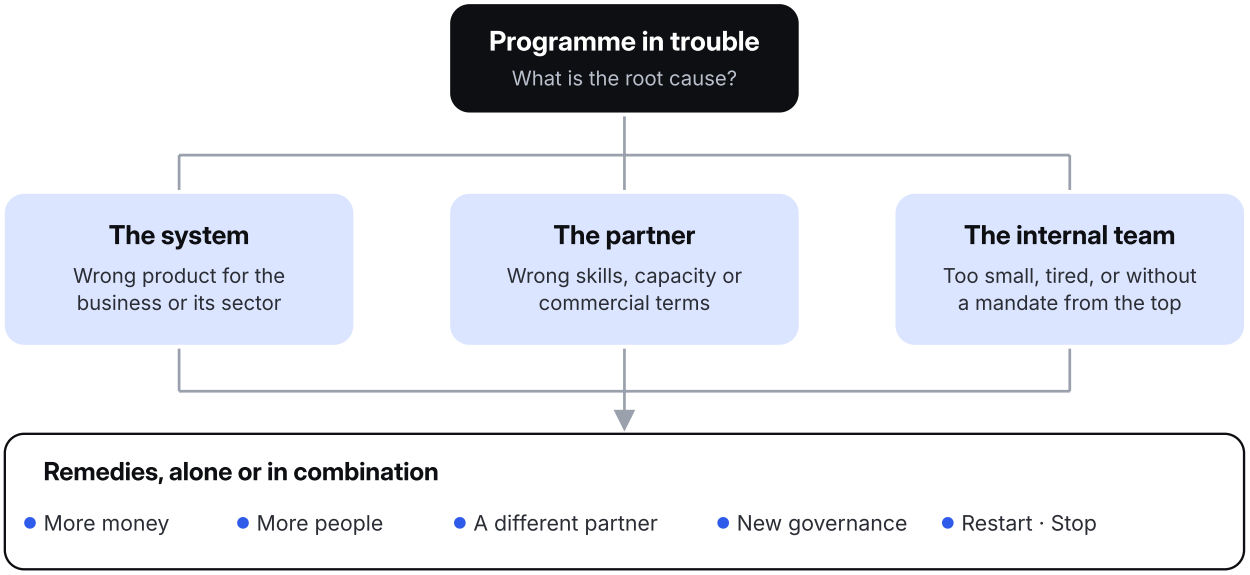


Figure 4. Diagnose first. The same symptoms can have three different causes, each with a different cure.

The evidence that decides it: whether the product still fits the business and its sector; how much of the work is done and what it would cost to finish compared with starting again; whether the partner can deliver with the right support; and whether the business still wants the outcome. When the internal team is the root cause, the cure is usually a combination: an explicit mandate from the owner, backfill so key users can give the programme proper time, and governance that makes decisions quickly.

Triage: what to fix first

A review usually finds more problems than the business can fix at once. I triage them in a fixed order:

1. **Anything that could stop production or transactions.** If the business cannot make, ship or invoice, nothing else matters.
2. **Critical security exposures**, which can stop the business just as completely.
3. **Anything customer-facing**: ordering, delivery promises, service.
4. **Quick wins** that build confidence in the programme.
5. **The strategic programme**: the platform for the next five years.

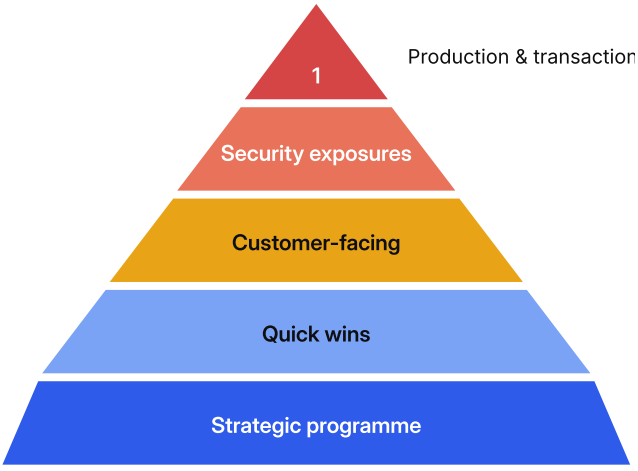


Figure 5. The triage order. Higher levels are fixed first, but the strategic programme starts planning in parallel.

Stage 3: Recommend

I rarely present a single answer. Boards make better decisions, and own them, when they can see the alternatives. I set out three strategic options, usually a version of **stabilise** (fix what is broken, minimum change), **modernise** (replace the weakest platforms) and **consolidate** (move to one integrated platform), and score them against weighted criteria agreed with the board.

Criterion	Weight	Stabilise	Modernise	Consolidate
Business fit & scalability	30%			
Risk reduction	20%			
Total cost of ownership	20%			
Speed to value	15%			
Delivery risk & capacity	15%			
Weighted score (out of 5)		**3.20**	**3.40**	**3.50**

Figure 6. An example options appraisal. Each option is scored 1 to 5 on each criterion (for cost and delivery risk, 5 means lowest cost or effort). Close scores are normal: the appraisal shows the board what it is trading off, and the recommendation explains how to manage the weaknesses of the preferred option, for example by phasing it to the business's capacity.

The recommendation then sets out the team needed to deliver it, the partners to appoint, and an investment summary with ranges rather than false precision. Ranges are firmed up when tender responses arrive.

Choosing systems and partners

For a manufacturer, the choice of ERP and implementation partner is the largest technology decision of the decade. I score every candidate product, including the incumbent, on the same six criteria, and I give real weight to sector experience: a partner that has implemented the product for manufacturers like yours will avoid mistakes a generalist will make at your expense.

Criterion	What I look for
Vendor size and strength	Scale, financial strength and commitment to the product line.
Adoption	Installed base among companies like yours, and depth of the local partner market.
Independent reviews	Ratings from independent user-review services, read for patterns, not averages.
Current technology	Cloud model, update cycle, integration options, reporting and AI capabilities.
Remaining supported life	How long the product will be developed and supported.
Fit	Fit to the business's processes, sector, number of companies and countries, and growth plans.

A short, competitive tender

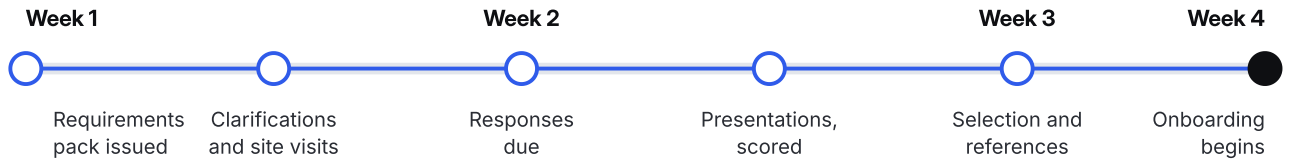


Figure 7. A typical tender for a managed service or implementation partner: four well-regarded, sector-relevant suppliers, a written requirements pack, and a decision within about three weeks.

The most common mistakes I see: choosing on day rate; letting the software vendor choose the partner; skipping reference calls with companies of similar size; signing without a clear statement of work and exit terms; and assuming the partner will supply the business's own product owners and testers. Those roles must come from inside the business.

Stage 4: Plan

The plan turns the recommendation into a sequenced roadmap, an investment summary, the principal risks, and a short list of decisions the board must take, each with an owner and a date. I ask the board to approve the plan and the spending that goes with it. From then on, governance tracks delivery against the plan rather than re-approving each step.

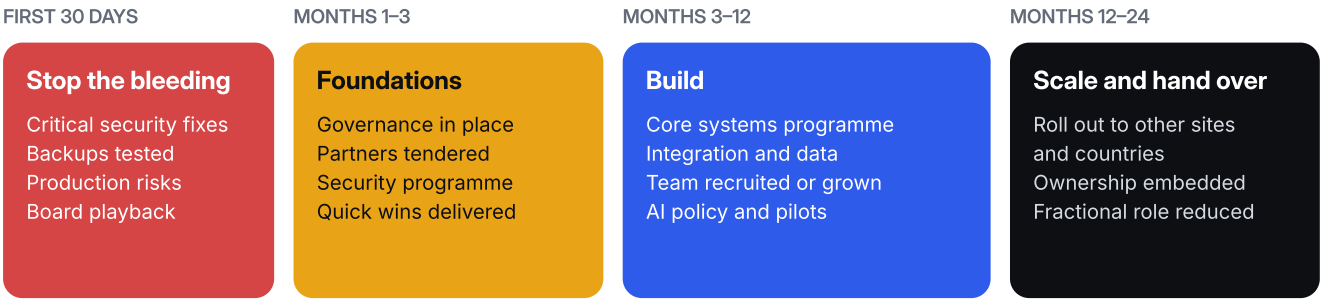


Figure 8. The shape of a typical roadmap. Timing depends on the decisions, funding and people available; for a multi-site or multi-country group the build stage usually runs site by site.

PART 3

Owning security

In a mid-sized manufacturer, cyber risk is a business risk that someone senior must own. The work itself is best done by specialists.

You have to own security and resolve the issues in priority order. Most mid-sized manufacturers cannot staff a round-the-clock security operation, and should not try: wherever possible, I back the operational work out to a managed security service provider (MSSP), and keep ownership, priorities and board reporting in the business.

What I find most often is not a lack of tools. It is tools that have been paid for but never switched on: multi-factor authentication licensed but not enforced, endpoint protection installed on some devices but not others, servers exposed to the internet that need not be, and backups that have never been test-restored. Most of the first month's work is configuration, not new spending.

The first 30 days

Critical fixes

- ☐ Reset any accounts showing signs of compromise
- ☐ Enforce multi-factor authentication for every user
- ☐ Remove servers and services from the public internet where they need not be there
- ☐ Remove unnecessary administrator rights, including suppliers'
- ☐ Lock down external file sharing
- ☐ Fix failed backups and test a restore

Then, over 3 to 9 months

- ☐ Security baselines for devices, email and cloud
- ☐ Endpoint protection switched on everywhere
- ☐ Round-the-clock monitoring and response (MDR) through a specialist partner
- ☐ A benchmark against a recognised framework, and a penetration test
- ☐ Policies, staff training and a tested recovery plan
- ☐ A recognised certification where customers ask for one

A common language: NIST CSF 2.0

I map the security programme to the six functions of the NIST Cybersecurity Framework 2.0, which the U.S. National Institute of Standards and Technology designed to be used by any organisation, "regardless of its size, sector, or maturity". In the United Kingdom, I also benchmark against the National Cyber Security Centre's Cyber Assessment Framework. Using a published framework lets the board, insurers and customers understand the position without technical translation.

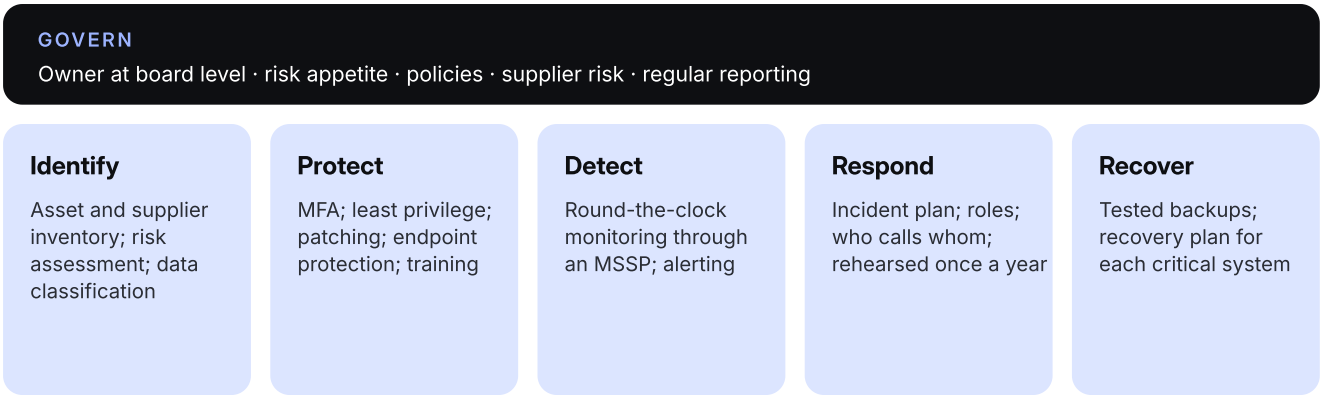


Figure 9. The security programme organised by the six functions of NIST CSF 2.0. Govern sits across all of them.

Reporting cyber risk to a board

Boards need a small number of measures, reported the same way every time: the framework benchmark score and its trend; the cloud security score where the business uses Microsoft 365 or similar; backup health and the date of the last successful test restore; the status of access reviews; open high-risk findings and their owners; and any incidents since the last meeting. The risk register should say plainly which risks the board is treating and which it has chosen to accept.

> The test of good security reporting is simple: could the board explain its cyber risk to its insurer, its largest customer and its bank?

At a schoolwear manufacturer I worked for, a ransomware attack was contained and the business was trading again the same day, because backups were tested and the recovery steps were known. That is the outcome this part of the method is designed to produce.

PART 4

Artificial intelligence: govern first, then adopt

Manufacturing is behind most industries in using AI. The way to catch up safely is to get control of it first.

In the manufacturers I work with, generative AI is already in use, often without anyone deciding that it should be. Agentic AI, where software agents carry out tasks rather than just answer questions, is in its infancy: a handful of trials at most. A serious effort is needed to bring AI into the production side of these businesses, but it has to start with control.

The U.S. Federal Reserve reported in April 2026 that about 18 percent of U.S. firms had adopted AI by the end of 2025, and that the largest firms have the highest adoption rates. Smaller manufacturers risk falling further behind, and the ones that adopt AI without controls risk exposing customer and product data.

Step 1: get control

When I review a business, the AI area is often rated "at risk" for the same reasons: staff using unapproved AI services with company data ("shadow AI"); no acceptable-use or AI policy; and nobody knowing which AI licences and tools are in use. The fixes are straightforward:

1. **Audit** the AI tools and licences in use across the business.
2. **Publish** an AI and acceptable-use policy that staff can understand in five minutes.
3. **Agree an approved toolset** and keep a register of AI services and what data each may use.
4. **Classify sensitive data** and switch on data-loss prevention, so the policy is enforced, not just written.

Step 2: adopt where the value is

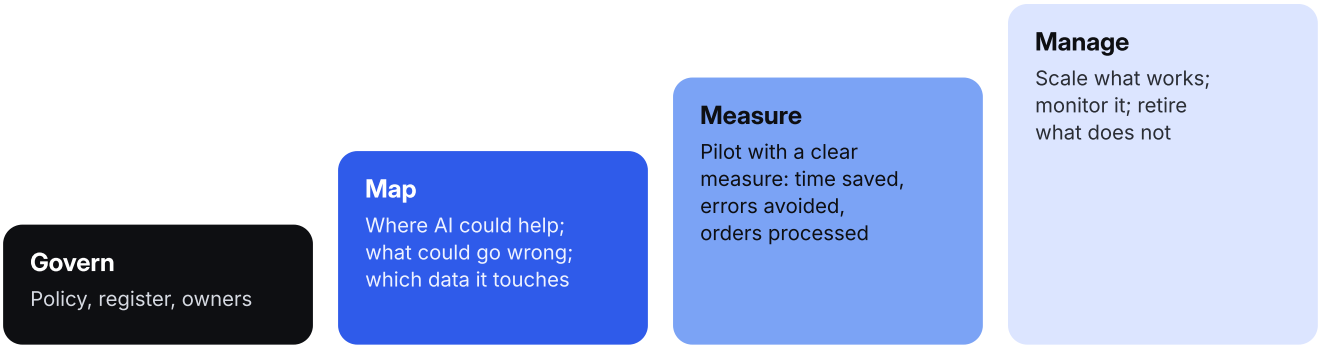


Figure 10. Adoption steps, using the four functions of the NIST AI Risk Management Framework: Govern, Map, Measure and Manage.

The best first uses are repetitive, document-heavy tasks with a measurable outcome:

IN USE

Order intake

At an office furniture manufacturer, an agentic AI process imports government orders at the sales end, removing manual re-keying into the business systems.

IN USE

Bid and tender analysis

At an international engineering consultancy, an AI agent built into the CRM system analyses bids and tenders, cutting the team's time on that work by more than 60 percent.

NEXT

Production and quality

Scheduling, maintenance prediction and quality inspection on the shop floor: the area where manufacturers have most to gain and have done least.

NEXT

Supplier and finance documents

Matching supplier statements, invoices and delivery notes, and handling routine mailbox queries.

What I warn against. Buying AI tools before the data underneath is sound; pilots without a measure of success; and letting AI make decisions about customers, safety or quality without a person accountable for the outcome.

PART 5

People and governance: build to replace yourself

Technology problems are the easier part. People are always the most difficult part, and the part that decides whether the change lasts.

In a fractional role you always build to replace yourself. From the first month, I am asking who will lead this technology when I step back, and what they need to get there.

If the talent is already there

Bring it on. Give people real responsibility under supervision: running supplier meetings, presenting to the executive team, owning part of a tender or a roll-out. At one national sports governing body I worked with, two members of the internal team were promoted into head-of-department roles.

If it is not

Build a profile of what the business needs and recruit for it. The review sets out two or three alternative team structures, compares them on cost, capacity and risk, and recommends one: for example a full-time IT director supported by the right mix of in-house staff, partners and contractors.

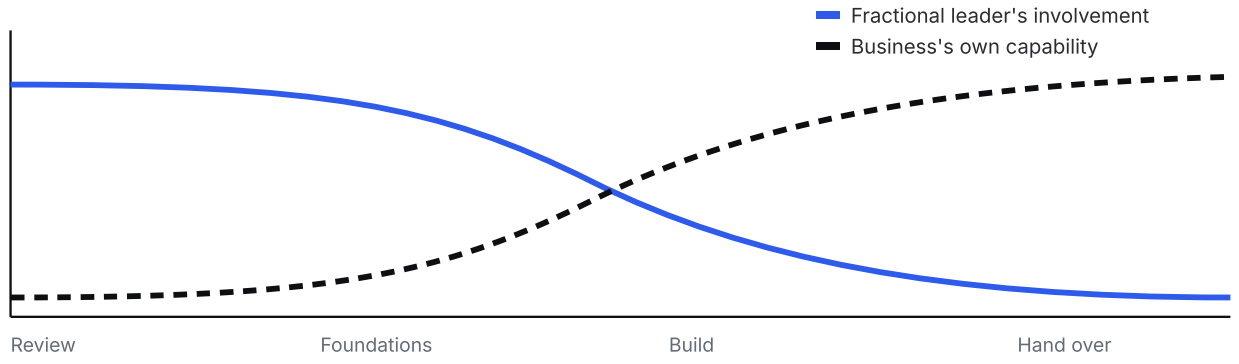


Figure 11. Building to replace yourself: the fractional role is designed to shrink as the business's own capability grows.

A lesson learned. In my experience the technology has rarely been the reason a programme fell short; the people structure has. In the past I have got a structure wrong and lost good people, or not achieved the outcome I wanted. What I do now: design the structure around the people the business actually has, involve them before roles change, and plan succession before anyone is moved.

Right-sized governance

Governance exists to make decisions quickly and to keep the board informed. A typical rhythm for a mid-sized group has three levels, but it must be sized to the company and the task: a 60-person business may need one monthly meeting; a multi-site group in the middle of an ERP programme needs all three.

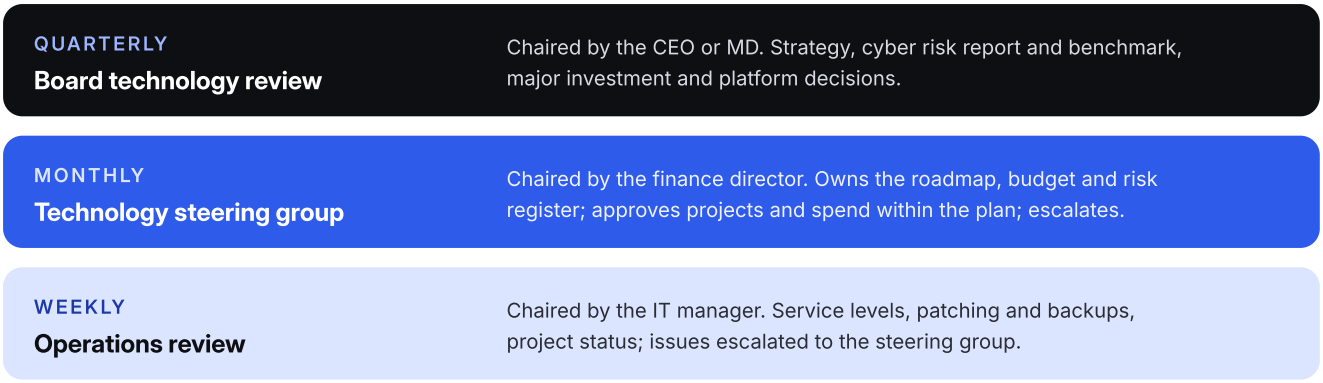


Figure 12. A three-level governance rhythm. Tool 5 in the toolkit sets out the attendees and papers for each.

Two practices make the biggest difference. First, a single page of **decisions required**, each with an owner and a date, so the board knows exactly what it is being asked to do. Second, an explicit statement of **which risks the board is treating and which it accepts**. Unowned risks are where programmes and businesses get hurt.

PART 6

The method in practice

Four engagements over eighteen years, from an in-house role at a 100-person manufacturer to a fractional role at a large office furniture manufacturer with factories in the UK and the U.S.

Schoolwear and sportswear manufacturer · about 100 staff · 2008 to 2017 · IT and Development Manager, then IT Director and company director

Manufacturing business: replacing the system that capped growth

The business designed, produced and supplied sportswear and schoolwear direct to schools across the United Kingdom. Its ageing mail-order system capped peak processing at about 1,500 orders a day. I led its replacement with Microsoft Dynamics AX in two phases, covering finance, sales, purchasing, production, the warehouse and e-commerce; set the digital strategy that made it the first schoolwear business in its market to sell online through a secure digital platform; moved the company into a new 40,000 square foot site; and prepared the technology due diligence for its sale in 2016.

2,700
orders a day at peak, up from about 1,500

0 days
of trading lost in the 2011 relocation

Same day
recovery from a ransomware attack

The ERP programme was delivered on time and to budget, and HM Revenue and Customs accepted it for research and development tax relief as the development of new technology.

Schoolwear and sportswear group · about £75 million turnover, 360 staff · 2016 to 2020 · Group IT Director

Retail and wholesale group: one platform for a group growing by acquisition

After that business was sold, I ran IT for the acquiring group and became its Group IT Director. The group was growing by acquisition under private-equity ownership on systems that could not support that growth. I wrote a five-year IT roadmap tied to its five-year business plan, delivered an end-to-end Microsoft Dynamics AX 2012 R3 implementation across manufacturing, wholesale, retail and online, and led the technical integration of three acquired high-street retailers.

260
users across four sites on one ERP system, live in 2019

~8 weeks
to bring each acquired retailer onto group systems

30+
retail locations integrated into the group

Over its owner's investment period from 2015 to 2021, the group more than doubled revenue and profit and grew to 32 stores with about 40 percent of sales online, as published by its private-equity owner.

National sports governing body · about 260 staff · fractional CIO 2022 to 2023; fractional CTO from 2026

National governing body: resetting a programme after two failed attempts

Two earlier attempts at a digital transformation programme had failed, the organisation was under financial pressure, and cybersecurity was a red risk on its register. I reset the programme with a new delivery partner, retendered the managed IT service, implemented a CRM system, introduced managed detection and response, and set up a technology risk committee. Three years later the organisation asked me back. Since then I have stabilised the delivery partner, restarted go-lives of further major modules, reduced the issue backlog, recruited six staff, and closed the gaps in governance.

£45k
a year saved on the managed service, with 25% fewer support tickets

+15%
sales conversion after the CRM went live for about 20 users

2
internal team members promoted to head of department

Office furniture manufacturer · more than 1,000 staff · UK and U.S. factories · fractional CIO from 2026

Manufacturing business: restarting an ERP programme and planning for growth

This office furniture manufacturer makes furniture in the UK and the United States. Its Microsoft Dynamics 365 programme across two plants had stalled through project fatigue and a lack of business prioritisation. My review covered twelve areas and set out eight decisions for the board and a 24-month roadmap, the UK first and then the U.S. business. The programme has been restarted on an accelerated timeline, and the target architecture is designed to support the group's growth ambitions.

~900
users on the restarted ERP programme across two plants

£80k
a year licence saving from the move to Hyper-V

UK + US
24-month roadmap, with the U.S. rollout to follow the UK

Other results, described without names

Organisation	Result
Consumer brand, about 140 staff, UK and U.S.	Integration platform replaced the EDI layer, saving about £120,000 a year; eight stores moved to one platform; three warehouse moves (two UK, one U.S.) with no lost trading.
Glass recycler with four plants	AI-based safety and security monitoring across five sites; injuries down 40 percent as behaviour changed; support brought in-house, saving about £96,000 a year.
Leisure trust with 20 sites	Systems consolidated, saving about £200,000 compared with the legacy set-up; first internal IT team built.
International engineering consultancy	Whole-of-market ERP and CRM selection; AI agent in the CRM cut bid-analysis time by more than 60 percent.

PART 7

Notes for manufacturers in the United States

The method is the same. The context, the rules and some of the risks are different.

My view of U.S. manufacturing so far has been from the parent company's side: UK groups with American factories and subsidiaries. The U.S. businesses face different challenges from the UK ones, and in some areas I have found real weaknesses.

What I have seen

- U.S. subsidiaries with no in-house IT at all, relying on one person and an ad hoc managed service provider.
- Industry-specific ERP systems split across several databases, partly used and costly to run.
- Rollouts that wait until the parent company's own programme is finished, leaving the U.S. business behind.
- Equally, managed security in some U.S. businesses that is stronger than in their UK parent.

Why it matters

- Small businesses make up more than 98 percent of U.S. manufacturing firms.
- Only 43 percent of U.S. manufacturers employ a cybersecurity leader, falling to 35 percent among small and medium-sized ones.
- The FBI recorded 355 ransomware complaints from the critical manufacturing sector in 2025, second only to healthcare.
- CISA designates critical manufacturing as one of sixteen critical infrastructure sectors.

U.S. requirements the method must cover

Requirement	What it means for a mid-sized manufacturer
Defense supply chain: DFARS 252.204-7012 and CMMC	Manufacturers that supply the U.S. defense supply chain and handle controlled unclassified information must protect it to the 110 requirements of NIST SP 800-171. The CMMC program began its first phase, contractor self-assessment, on 10 November 2025. Mandatory third-party assessments (phase 2) were suspended in July 2026 pending a review, but the underlying obligations remain, and prime contractors can still require certification from their suppliers. Treat readiness as a commercial requirement.
NIST CSF 2.0 and the AI RMF	The voluntary federal frameworks this method already uses for security and AI, recognised by U.S. customers and insurers.

Cyber insurance	Insurers increasingly require multi-factor authentication, tested backups and endpoint monitoring before they will quote, which are the first 30 days of Part 3.
State privacy laws	Several states have their own consumer data laws. Map where customer and employee data is held before choosing systems and AI tools.
Manufacturing Extension Partnership	NIST's network of MEP centres serves small and medium-sized manufacturers in every state and is a natural partner for training and support.

PART 8

If you only have this playbook

Much of this method needs specialist knowledge. Two parts do not, and they are where every improvement starts.

THIS MONTH

1. Rate your business on the eight areas

Use Tool 1. Give each area a red, amber or green rating and one sentence of evidence. Be honest about "to confirm": not knowing is itself a finding. Share it with your board.

THIS MONTH

2. Set up a monthly steering group

Use Tool 5. Chaired by the finance director or owner, with your IT lead and key suppliers. Start a risk register and a decisions-required page (Tool 6) at the first meeting.

When to bring in specialist help

- Any area rated red, especially cybersecurity or business systems.
- A systems programme more than six months late, or with a partner relationship under strain.
- An acquisition, new plant or new country on the horizon.
- A customer, insurer or defense prime asking for evidence of security you cannot provide.
- Staff using AI tools and nobody knows which ones.

The remaining tools (partner selection, options appraisal, tendering and AI) are included so that whoever you bring in, internal or external, works to a recognised standard.

THE TOOLKIT

Seven templates

Copy them, adapt them, and use them with your board. Please credit "Technology Mastery, Gareth Rooney, Aspirica Ltd".

Tool	Template	Use it to
1	Eight-area scorecard	Rate your technology on one page
2	System and partner suitability scorecard	Compare ERP, CRM or partner options on the same basis
3	Options appraisal	Score strategic options against weighted criteria
4	Tender plan and requirements pack	Run a short, fair, competitive tender
5	Governance terms of reference	Set up the weekly, monthly and quarterly rhythm
6	Decisions required and risk register	Put clear decisions and risks in front of the board
7	AI policy starter and AI register	Get control of AI before you scale it

TOOL 1

Eight-area scorecard

Rating: Good · Needs attention · Urgent · To confirm. Priority: H, M or L.

Area	What good looks like	Current position and evidence	Rating	Priority	Owner
Strategy and alignment	Roadmap tied to the business plan; a board-level owner				
Infrastructure and cloud	Supported, resilient, segmented; nothing exposed without reason				
Cyber security	MFA enforced; monitored round the clock; tested recovery				
Business systems	Supported ERP and CRM that fit the next five years; integrated				
Data and reporting	One version of the numbers; data classified and controlled				
People and capability	Enough capacity; no single points of failure; succession				
Suppliers and contracts	Every critical supplier under contract, measured and reviewed				
Cost and value	All contracts and licences baselined; spend reviewed yearly				

Evidence base: people interviewed _____ · sites visited _____ · systems reviewed _____ · documents reviewed _____

TOOL 2

System and partner suitability scorecard

Score each candidate 1 to 5 on each criterion (5 = strongest). Include the incumbent system as a candidate.

Criterion	Incumbent	Option A	Option B	Option C
Vendor size and strength				
Adoption (installed base, partner market)				
Independent reviews				
Current technology				
Remaining supported life				
Fit (processes, sector, entities, growth)				
Partner sector experience				
Overall score				

Questions to ask every partner

- Which manufacturers like us have you implemented in the last three years, and may we call two of them?
- Who exactly will work on our project, and for what share of their time?
- What do you need from our people, by role and hours a week?
- How do you handle change requests, and what are the exit terms?

TOOL 3

Options appraisal

Agree the criteria and weights with the board before scoring. Score 1 to 5 (for cost and delivery risk, 5 = lowest cost or effort). Weighted score = sum of weight × score.

Criterion	Weight	Option 1 Stabilise	Option 2 Modernise	Option 3 Consolidate
Business fit and scalability	30%			
Risk reduction	20%			
Total cost of ownership	20%			
Speed to value	15%			
Delivery risk and capacity	15%			
Weighted score	**100%**			

For each option, record

- Indicative cost range (one-off and yearly), timescale, and the people needed
- The main risks and how they would be managed
- What the business could do, and could not do, at the end of it

TOOL 4

Tender plan and requirements pack

When	Step	Owner
Week 1	Issue the requirements pack to four shortlisted, sector-relevant suppliers	
Week 1–2	Clarification questions answered to all; site visits	
Week 2	Written responses due	
Week 3	Presentations, scored by a panel against Tool 2; reference calls	
Week 3	Selection, approval and contract	
Week 4	Onboarding begins	

Requirements pack contents

- [ ] The business: what it makes, sites, users, growth plans
- [ ] Scope and service levels required
- [ ] Current systems, suppliers and known issues
- [ ] Security requirements and the framework you work to
- [ ] Commercial model, contract length and exit terms
- [ ] How responses will be scored, and the timetable

TOOL 5

Governance terms of reference

Right-size this: a smaller business may need only the monthly steering group.

Forum	Chair and attendees	Papers	Decides
Weekly Operations review	IT manager; service provider; project manager; site leads	Tickets and service levels; patching and backup status; project progress	Day-to-day priorities; what to escalate
Monthly Steering group	Finance director (chair); fractional CIO or IT director; IT manager; business leads	Roadmap status (RAG); budget against plan; risk register; security measures; decisions required	Projects and spend within the approved plan; risks to treat or escalate
Quarterly Board review	CEO or MD (chair); board; finance director; CIO	Strategy update; cyber risk report and benchmark; major investment cases	Platform decisions; investment; risks the board accepts

TOOL 6

Decisions required and risk register

#	Decision required	Why now	Owner	By
1				
2				
2				
3				

#	Risk	Likelihood	Impact	Treat or accept	Owner
1					
2					
2					
3					

TOOL 7

AI policy starter and AI register

Five rules for staff

1. Use only the AI tools on the approved list.
2. Never put customer, employee, pricing or design data into an unapproved tool.
3. A named person is accountable for anything AI produces that leaves the business or affects safety, quality or a customer.
4. Check AI output before relying on it.
5. Ask before adding a new AI tool; tell us if you have been using one.

AI register

Tool or service	Owner	Use	Data allowed	Status

SOURCES

Sources

1. U.S. Small Business Administration, Office of Advocacy. *Facts About Small Business: Manufacturing Statistics 2025*. March 2025.
2. MxD with APCO. *Behind the Firewall: Assessing Cyber Resilience in US Manufacturing*. 2024 (survey of 750 manufacturers, November–December 2023).
3. IBM X-Force. *2026 Threat Intelligence Index*, report highlights.
4. Federal Bureau of Investigation, Internet Crime Complaint Center. *2025 IC3 Annual Report*. April 2026.
5. Cybersecurity and Infrastructure Security Agency. Critical Manufacturing Sector.
6. Board of Governors of the Federal Reserve System. "Monitoring AI Adoption in the U.S. Economy". *FEDS Notes*, 3 April 2026.
7. National Institute of Standards and Technology. *The NIST Cybersecurity Framework (CSF) 2.0*, NIST CSWP 29. February 2024.
8. National Institute of Standards and Technology. *Artificial Intelligence Risk Management Framework (AI RMF 1.0)*, NIST AI 100-1. January 2023.
9. U.S. Department of Defense. Cybersecurity Maturity Model Certification program rule (32 CFR Part 170) and DFARS 252.204-7021; status of phase 2 as reported in July 2026.



ABOUT THE AUTHOR

Gareth Rooney

Gareth Rooney is a fractional Chief Information Officer and Chief Technology Officer who leads technology for several mid-sized organisations at once through his company, Aspirica. He has led technology functions since 2008: as IT Director and a company director of a schoolwear manufacturer, as Group IT Director of a £75 million schoolwear and sportswear group, and since 2021 for eleven organisations with turnover from £2 million to £200 million, including manufacturers in the UK with U.S. operations.

He was named in the CIO 100 UK in 2025 and 2026. He holds EC-Council's Certified Chief Information Security Officer (C|CISO) and the Certified CIO – Foundation, completed the Oxford Artificial Intelligence Programme at Saïd Business School, University of Oxford, and is a member of BCS, The Chartered Institute for IT.

Contact: gareth@aspirica.co.uk