Notify

How to choose, buy, and roll out health and safety software

notifytechnology.com

Contents

Introduction

If you're still managing health and safety on paper, across spreadsheets, or through a patchwork of tools, you've probably reached the point where 'good enough' no longer feels good enough.

You know a digital system could save time, improve visibility, and support a stronger safety culture - but the path from thinking about software to choosing the right platform and getting it embedded can feel like a lot. That's exactly what this eBook is here to support.

It brings together practical guidance to help you select, purchase, and implement health and safety software in a way that genuinely works for your organisation. Whether you're exploring options for the first time, replacing an outdated system, or restarting after a stalled project, the goal is the same: to help you make confident decisions, avoid common pitfalls, and build a rollout that delivers real engagement and measurable improvement.

The sticking points we hear most often

When safety teams start evaluating software, the same challenges tend to come up again and again:

- Turning a long wish list into a clear view of what you actually need
- Getting the right people aligned and securing buy-in beyond the health and safety team
- Working through procurement steps, reviews, and decision timelines without losing momentum
- Launching the system in a way people genuinely use (and that improves performance, not just reporting)

If any of that sounds familiar, you're in the right place.

What this eBook will cover

This guide will support you step-by-step, from early planning and scoping, through evaluation and purchasing, to rollout and long-term adoption.

It's organised into five chapters, covering eleven key stages. Along the way you'll find practical tips, common pitfalls to avoid, and real-world guidance drawn from specialists across our team, based on what we've seen work across hundreds of organisations going through the same journey.

You can read it cover to cover, or dip into the section that matches where you are right now.

Let's begin.

Why safety software matters

Health and safety isn't a 'nice to have'; it's a legal requirement. It's also one of the clearest signals of how well an organisation manages risk—and the consequences of getting it wrong are immediate, human, and expensive.

The reality is that safety incidents happen every day. In Great Britain, **124 workers** were killed in work-related accidents in 2024/25—that's roughly one fatality every three days[1]. And it doesn't stop there: the same year, an estimated **40.1 million** working days were lost due to work-related ill health and non-fatal injuries[1]. HSE's latest cost estimates put the total cost to Britain of workplace injuries and ill health at around **£22.9 billion**[1].

These aren't just headlines or statistics. They represent real people, real operational disruption, and real reputational and legal exposure—which is exactly why getting control of safety data and action management is so important.

124 workers were killed in work-related accidents in 2024/25

£22.9 billion[1] cost to Britain in workplace injuries and ill health

[1] https://www.hse.gov.uk/statistics/overview.htm

The hidden cost of patchwork safety systems

When organisations face these challenges, many start by building something that works well enough; a mix of spreadsheets, paper forms, and tools like Microsoft Forms. At first, it can feel workable. But over time, manual systems tend to create the same problems:

- Time drains and admin overload as reporting and follow-up becomes repetitive and inconsistent
- Errors and blind spots when information is duplicated, missing, or stored in different places
- Lost learning when near misses aren't captured, or trends are hard to spot across sites and teams
- Weak follow-through when corrective actions aren't assigned, tracked, escalated, and evidenced reliably
- Compliance pressure when you can't quickly demonstrate what happened, what you did, and whether it worked

In short: the risk isn't just the incident itself—it's what happens when you can't see issues early, respond consistently, or prove control.

What purpose-built safety software changes

The right health and safety software helps you move from reactive reporting to proactive prevention. It brings safety activity into one place, so you can:

- Act faster when hazards and incidents are reported
- Track actions properly (ownership, deadlines, reminders, evidence, escalation)
- Identify patterns across sites, teams, and categories before risks escalate
- Strengthen assurance with clearer records, better audits, and simpler compliance reporting
- Support a stronger safety culture by making it easier for people to engage and follow the right process

This isn't about going digital for the sake of it. It's about creating consistency, visibility, and accountability.

Expectations are rising

It's also worth being direct: the bar is moving. Clients, auditors, insurers, and supply chain partners increasingly expect evidence of robust safety management, and many organisations are already investing in modern systems to meet those expectations.

That means the decision to implement safety software isn't just an internal efficiency upgrade. It can protect commercial reputation, support tender requirements, reduce operational disruption, and strengthen long-term resilience.

Ultimately, health and safety software isn't just about ticking boxes. It's about protecting your people, your business, and your peace of mind—with a system that helps you do the right things consistently, and prove it.

[1] https://www.hse.gov.uk/statistics/overview.htm

Defining success criteria

Before you compare platforms, book demos, or build a business case, it helps to get one thing clear: what does ‘success’ actually look like for your organisation?

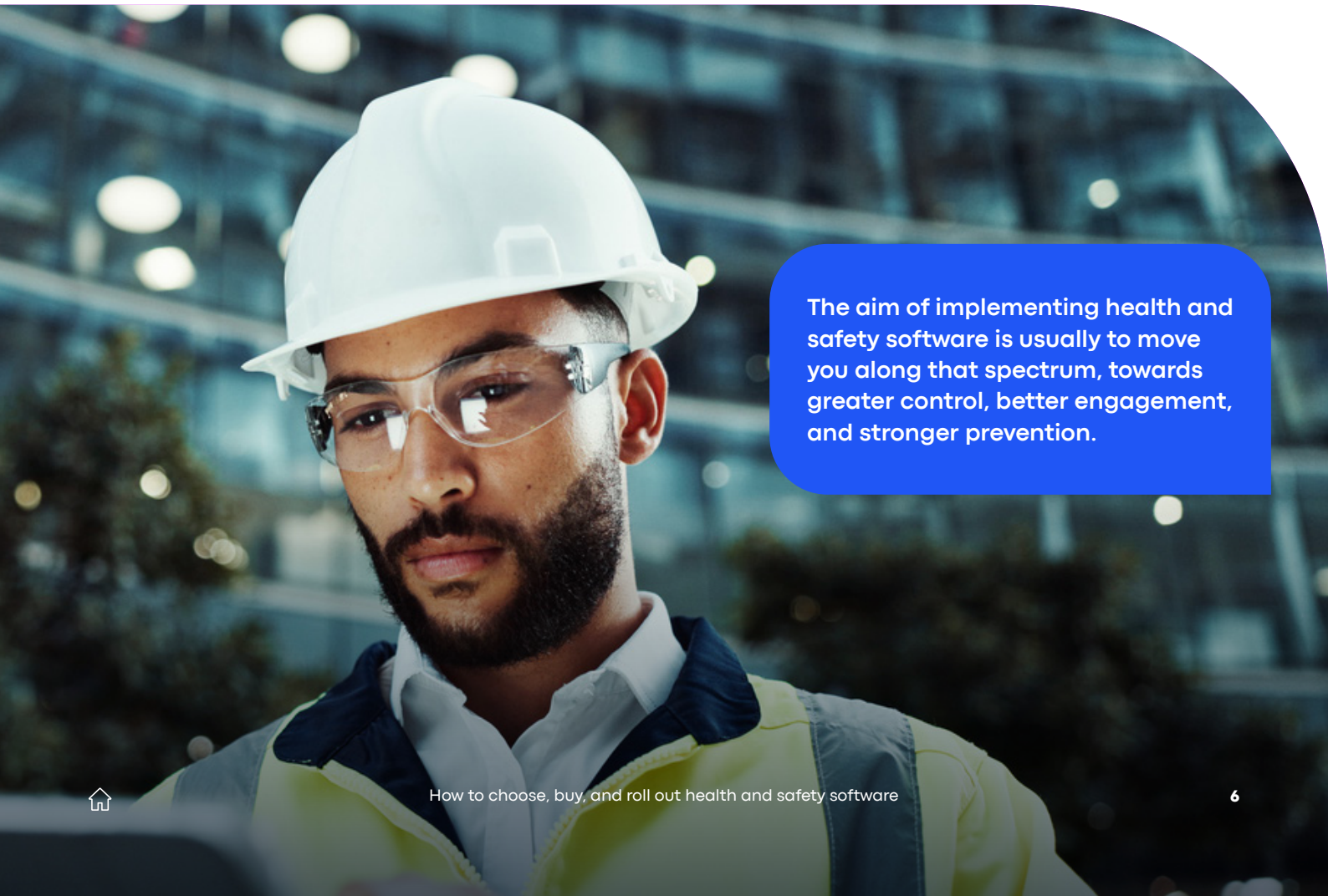
Without agreed success criteria, it’s easy to end up with a system that looks good in a demo but doesn’t solve the problems you’re trying to fix—or worse, becomes another tool people don’t use.

Reactive, compliant, proactive: where are you today?

Most organisations sit somewhere along a spectrum:

- **Reactive:** action happens after something goes wrong—an incident, an audit issue, a complaint, or a fine.
- **Compliant:** the basics are in place (policies, checklists, audits), but the process is often manual and fragmented.
- **Proactive:** safety is managed with visibility and consistency—using data and employee engagement to spot risks early and prevent incidents.

Put simply: reactive organisations focus on what has already happened. Proactive organisations focus on what hasn’t happened yet, so they can stop incidents before they occur.



The aim of implementing health and safety software is usually to move you along that spectrum, towards greater control, better engagement, and stronger prevention.

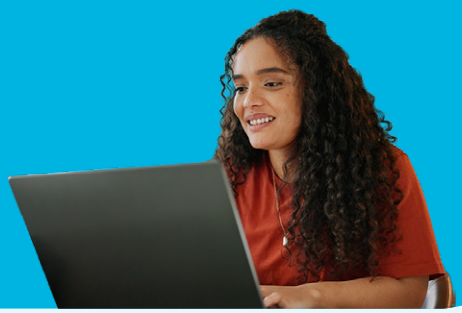
A practical 3-step process to define success

1

Step 1: Establish your baseline

Start with an honest picture of how things work today This gives you two benefits:

- ✓ You can pinpoint what needs to change, and
- ✓ You can prove improvement later



Use prompts like these:

Engagement and reporting

- Are you capturing safety insights from frontline teams consistently?
- Are reports coming from a wide range of people or just the same few?
- Are near misses and hazards easy to report, or do they get skipped?

Performance and visibility

- What do your key rates or indicators tell you (e.g., incident frequency, severity, trends)?
- Can you visualise safety performance in one place?
- Can you compare sites, departments, or contractors to prioritise action?

Actions and follow-through

- Are corrective actions clearly assigned, tracked, escalated, and evidenced?
- How often do actions go overdue, and why?

Admin and assurance

- How much time is spent inputting, checking, cleaning, and reporting on data?
- How much effort goes into gathering evidence for audits, claims, or investigations?
- Do you have a clear, reliable audit trail?

Tip: Do a quick process audit with your team. Note what's working, what's missing, and where the pain points show up most often.

What to capture in your baseline

- Current reporting volume (incidents, hazards, near misses, observations)
- Average time to close actions
- % actions overdue
- Time spent each month on admin and reporting
- Audit preparation time (and where evidence typically lives)
- Any recurring issues (same sites, same hazard types, same root causes)

2 Step 2: Consider your digital maturity

Your success criteria should fit your organisation's readiness, not just where you want to be eventually.

Ask

- How comfortable are teams with new tools and new ways of working?
- What training, onboarding, and ongoing support will be needed?
- What functionality is essential from day one vs. phase two?
- Which standards or regulations must the software support (e.g., ISO 45001), and where do your current processes struggle to evidence this?

This step is important because it protects you from choosing something too complex to adopt or choosing something that can't support you in 12–24 months.

3 Step 3: Define success (clearly, and in measurable terms)

Now set the outcomes you want to achieve and make them concrete.

A helpful question is: "In 12 months, how will we know this project has worked?"

Success criteria often include outcomes like:

- Better engagement from frontline teams
- Increased reporting of near misses and safety observations
- Faster close-out of corrective actions
- Fewer incidents and reduced absenteeism
- Less time spent on admin and more time spent on coaching, training, and improvement
- Stronger audit readiness and a clearer evidence trail

Make your success criteria SMART

To keep expectations aligned (and make buy-in easier), document goals using the SMART framework:

S **Specific**
What exactly will improve?

M **Measurable**
How will you track it?

A **Achievable**
Is it realistic with your resources and timeline?

R **Relevant**
Does it tie to your actual risks and priorities?

T **Time-bound**
By when?

Examples of SMART success criteria

- Increase near-miss reporting by **30%** within 6 months, with reporting coming from at least 4 departments.
- Reduce average corrective action close-out time from **40 days to 30 days within 12 months**.
- Cut monthly safety reporting admin time by **25% within 3 months of rollout**, freeing time for site engagement.
- Achieve **90% on-time completion** of corrective actions within 9 months.
- Create a single, consistent audit trail so audit evidence can be produced within **24 hours**, not days.

Why this step helps you get buy-in

Having clear success criteria doesn't just guide software selection, it strengthens the internal case for investment.

Leaders respond to outcomes that are measurable and grounded in business impact: time saved, risk reduced, assurance improved, operational disruption avoided. When you can link your success criteria to cost, capacity, and risk exposure, it becomes much easier to secure support and to keep momentum through procurement and rollout.

Pinpointing your software requirements

Once you've defined what success looks like and identified the problems you're trying to solve, the next step is to get clear on what you need your software to do.

This is where a well-built wish list pays off. It helps you compare solutions fairly, avoid being swayed by a slick demo, and make sure the system you choose genuinely supports how your organisation operates.

A useful way to structure your thinking is the Plan–Do–Check–Act (PDCA) cycle. It's a practical framework used to reduce risk and drive continual improvement, and it's also a core part of ISO 45001.

Use PDCA to shape your requirements

Here's what PDCA looks like in a health and safety context:

- **Plan:** Identify risks, set objectives, and define the policies and processes needed to manage safety effectively.
- **Do:** Put controls into practice - train staff, implement procedures, provide resources, and engage workers.
- **Check:** Monitor performance through inspections, audits, and incident reviews to confirm controls are working.
- **Act:** Take corrective and preventative action, update your approach, and continuously improve.

When you're evaluating software, ask: how well does this system support each stage of PDCA, in the real world, day to day?

The core features most organisations need

Every organisation will prioritise differently, but these are common foundations that support consistent safety management:

- **Incident Reporting:** Mobile-friendly, quick to complete, with photo uploads and clear next steps.
- **Audit and Inspection Management**: Schedule inspections, capture findings, and follow through on actions.
- **Risk Assessments:** Simple to create, assign, review, and keep up to date - with clear ownership and sign-off.
- **Method Statements/RAMS:** Easy creation, sharing, and access for teams in the field.
- **Action Tracking:** Assign, monitor, evidence, escalate, and close out actions to ensure accountability.
- **Document Management:** Central storage for important documents, with version control and controlled access.
- **Dashboards and Reporting:** Real-time visibility of trends, hotspots, and performance indicators.

Tip: As you list features, keep linking back to your success criteria. If a feature won't help deliver the outcomes you defined, it may not be a priority right now.

The ‘difference makers’ for your organisation

Beyond the basics, certain capabilities can make or break adoption, depending on your environment and workforce. Consider questions like:

- Do teams work in low or no-signal areas (e.g., tunnels, remote sites, offshore)? If so, offline functionality can be essential.
- Do you have a diverse workforce where English isn’t everyone’s first language? If so, multi-language support can improve reporting quality, engagement, and clarity.
- How much tailoring do you need? Will a standard setup work, or do you need configurable workflows, incident types, and investigation fields that help you capture root causes properly?

These features may not sound exciting in a demo, but they often determine whether the system becomes part of daily operations or quietly falls back into ‘something we do for audits’.

Nice-to-haves

Some capabilities can be valuable, but don’t need to be prioritised from day one. For example:

- **Asset Management:** Track equipment, inspections, defects, and service history with reminders and escalation.
- **Safety Training Management:** Assign, deliver, and record training to maintain compliance and competence.
- **Permit to Work:** Manage permits for high-risk activities and ensure controls are applied consistently.

If these aren’t urgent now, you can note them as future requirements. Make sure the software can support them later (or integrate cleanly with what you already use).

Emerging capabilities

Many providers are now introducing AI-powered tools. Used well, these can reduce manual effort and improve visibility.
For example, AI may help with:

- Generating summaries, reports, or briefings faster
- Highlighting patterns in incident and observation data
- Improving search and retrieval of key information across the system

The important thing is to treat this as part of your broader requirements: What problem does it solve? How does it save time, reduce risk, or improve decision-making?

One platform, or multiple tools?

It’s also worth thinking about your overall approach:

- Do you want an all-in-one platform that covers most requirements in one place?
- Or a best-of-breed setup, using separate specialist tools for separate needs?

Best-of-breed tools can work but they often create challenges with integration, duplicated data, inconsistent reporting, and extra admin. Over time, that can become costly and inefficient. For many organisations, simplicity and consistency win.

Build the wish list collaboratively

Finally: don't build your requirements in isolation. Involve stakeholders early, not just for input, but to reduce resistance later. In fact, the more likely someone is to block change, the earlier it's worth engaging them.

You'll typically want perspectives from:

- **Frontline workers -** the people reporting hazards, near misses, and incidents
- **Site/branch managers -** overseeing day-to-day operations and action close-out
- **Regional/area/divisional leaders -** comparing performance across sites and prioritising improvements
- **The H&S team -** analysing trends, managing assurance, and driving prevention
- **Executives -** shaping policy, investment decisions, and organisational priorities

With the right voices involved, your wish list becomes more than a list of features. It becomes a shared definition of what 'good' looks like, and a practical tool for choosing the right solution.

Choosing the right health and safety software

Once you're clear on your success criteria and you've built a realistic wish list, the next step is finding a solution that fits your organisation in practice, not just on paper.

This stage is about moving from 'what's out there?' to 'which options are genuinely worth our time?'

Start broad, then narrow quickly

Begin with simple, targeted research. Search engines are still one of the fastest ways to understand the market, especially if you use search terms that match your sector and priorities. For example:

- 'Health and safety software for manufacturing'
- 'Incident reporting software'
- "ISO 45001 safety management system software'
- 'Near miss reporting app'
- 'Safety audit and inspection software'

Tip: As you research, note recurring providers, common feature sets, and any strong differentiators that line up with your requirements.

Use comparison sites and reviews (carefully)

Comparison sites can help you build a shortlist faster because they bring together product summaries, feature breakdowns, and user reviews in one place. Sites like G2 are commonly used for this.

A word of caution: reviews are useful, but they're not the full story. Pay attention to:

- Whether reviewers sound similar to your organisation (industry, size, complexity)
- Repeated themes (both positive and negative)
- Comments about implementation, support, and ease of use (often more revealing than feature lists)

Use AI to accelerate the shortlist

AI tools can help you cut through volume, especially when you're reading dozens of reviews or comparing similar vendors.

For example, you might use tools such as ChatGPT, Google Gemini, or Perplexity to:

- Summarise common pros/cons across customer reviews
- Group vendors by strengths (e.g., 'strong reporting', 'best for multi-site', 'good offline capability')
- Turn your wish list into a shortlist of likely matches

Example prompt:

'Based on these requirements (X, Y, Z), suggest a shortlist of health and safety software options for a company with 200+ employees operating across multiple sites.'

AI won't replace your judgement, but it can save time and help you focus attention where it matters.

You can also use it like a search assistant to explore the market and refine your shortlist as you go.

Demos: where the shortlist becomes real

Once you have a shortlist, book demos. Most providers offer a walkthrough or live demo. This is where you'll quickly learn whether the platform will work for your teams. The key is to make demos realistic. Before the call, prepare a few scenarios based on your actual workflows. For example:

- Logging an incident from a mobile device, including photos and key details
- Assigning and tracking actions, including reminders, evidence upload, and escalation
- Pulling a monthly trend report or dashboard view in a few clicks
- Running an inspection or audit, capturing findings and converting them into actions
- Finding evidence for an audit, quickly and consistently

A strong demo should show how the software handles these end-to-end, not just how it looks on screen.

Remember, you're assessing the provider too

It's easy to focus only on features, but implementation and ongoing support often determine success. During demos, ask about:

- Onboarding and implementation support (what's included)
- Customer support model (hours, response times, channels)
- Whether support is local/UK-based (if that matters to your organisation)
- Typical implementation timelines and what helps them go smoothly
- How they handle configuration, training, and change management

You're not just buying software; you're entering a working partnership. The right fit is as much about the team behind the product as the platform itself.

Compare options with a simple evaluation matrix

A basic comparison matrix keeps decision-making fair and helps you justify recommendations internally.

Rate each vendor against your priorities, such as:

- Alignment to your must-have requirements
- Ease of use for frontline teams
- Interface and user experience (especially on mobile)
- Flexibility and configuration options
- Reporting and dashboards
- Implementation approach and support model
- Total value for money (not just licence cost)

This is also a good moment to include stakeholders who will be affected by the change - especially those who'll use the system day-to-day.

Always prioritise adoption

Finally, a practical truth: the best system is the one people will actually use.

If the platform is hard to navigate, too slow, or feels like extra admin, reporting will drop and follow-through will suffer, no matter how advanced the features look. When in doubt, prioritise:

- Simplicity and speed
- Mobile usability
- Clear workflows that mirror real operations
- Strong support and implementation guidance

Building stakeholder buy-in

Choosing health and safety software is rarely just a safety team decision. One of the biggest hurdles is getting buy-in, especially when budgets sit across different departments, or when technology spend is tightly controlled.

In larger organisations, safety software often touches multiple functions: Health & Safety, Quality, Legal, Finance, HR, Operations, and IT. It's also common for IT to have a strong voice in procurement and platform decisions, while training budgets may sit with HR, and operational budgets may sit elsewhere.

The result? Sometimes safety ends up belonging 'nowhere' and projects stall. The key is to involve the right people early and speak their language.

Start with the stakeholders who shape the decision.

Senior leadership (CEO/MD/Directors)

At the top of the organisation, leaders are balancing competing priorities and multiple teams asking for investment. Some will already understand the importance of better safety systems. Others will need a clearer business case.

It can be tempting to rely on 'worst case scenario' arguments - fines, prosecutions, reputational damage. Those risks are real, but fear alone rarely builds lasting support. What tends to work better is combining:

- **Evidence** (current risks, gaps, inefficiencies)
- **Business context** (operational impact, audit readiness, supply chain expectations)
- **A clear ROI story** (time saved, risk reduced, disruption avoided)

Helpful framing: *"This isn't just a system change. It's a way to reduce risk, improve performance, and strengthen assurance across the business."*

HR

HR teams can be powerful allies because they're deeply involved in engagement, communication, training, and change management - all of which directly affect adoption. When you speak with HR, focus on how better safety systems support:

- Workforce wellbeing
- Retention and employee experience
- Consistent training and competence
- Employer brand and trust

HR also tends to understand budget cycles and internal approval routes, which can help you navigate the process more smoothly.

IT

IT stakeholders typically care most about:

- Security and data protection
- Scalability and reliability
- Integration with existing systems
- User access and identity management
- Support burden

The strongest approach here is partnership. Emphasise the shared goal: a secure, well-governed platform that people actually use.

Also make the 'IT benefit' explicit. The right system can reduce the support burden by removing spreadsheets, email chains, workarounds, and shadow processes that create risk and extra admin.

> **Helpful framing:** *"We want something that's secure and easy to support, but also simple enough that frontline teams adopt it without friction."*

Finance

Finance teams want clarity, and they'll often ask the questions other stakeholders avoid. Be ready to explain:

- The cost model (licensing, onboarding, implementation, training)
- Contract terms and risk (renewals, exit terms, data ownership)
- ROI and value for money
- How this reduces exposure to operational and financial risk

Link the investment to tangible costs the business recognises: incident disruption, absenteeism, claims, insurance implications, audit hours, and wasted admin time.

Handling objections

Even with the right stakeholders involved, you may still hear objections. The goal isn't to 'win an argument', it's to reduce uncertainty and keep momentum. Common objections may include:

- "We already have a system" (usually meaning spreadsheets and shared drives)
- "This is just compliance"
- "We can't prioritise this right now"
- "It's too expensive"
- "IT won't support it"

A useful response is to bring the conversation back to outcomes:

- What risks are we currently carrying because of how we manage safety?
- What's the operational cost of delays, duplication, and missed follow-through?
- What happens if we can't evidence control quickly - for an audit, a client, an incident, or an insurer?

Remember: poor systems create real costs, such as downtime, injuries, lost productivity, reputational impact, and lost talent. Framing the discussion around business resilience helps move it beyond box-ticking.

A simple approach to building buy-in

When engaging each stakeholder group, ask yourself:

- What do they care about most?
- What might make them resist?
- What would success look like from their perspective?
- What's the best way to involve them? (A short one-pager, a workshop, a demo invite, or a quick risk/ROI summary?)

Tailor your message and your method. People support what they feel included in and what they understand.

Practical ways to involve stakeholders early

- Run a short requirements workshop with Safety, Ops, IT, HR, and Finance
- Share a one-page summary of the current pain points and desired outcomes
- Invite key stakeholders to demos with real scenarios, not generic walkthroughs
- Agree decision criteria up front (e.g., security, usability, reporting, configurability, ROI)
- Identify one senior person who can unblock decisions if timelines slip

Creating a business case

If you want to secure budget for health and safety software, you need more than a product shortlist.

You need a clear, credible business case that helps decision-makers quickly answer three questions:

- **Why now?**
- **What happens if we don't act?**
- **What outcomes will we deliver if we do?**

A strong business case typically balances four angles: legal, moral, financial, and commercial. This is because different stakeholders care about different risks and rewards.

1. The legal case: health and safety isn't optional

At its simplest, organisations have legal duties, and failing to meet them can lead to regulatory attention and formal enforcement.

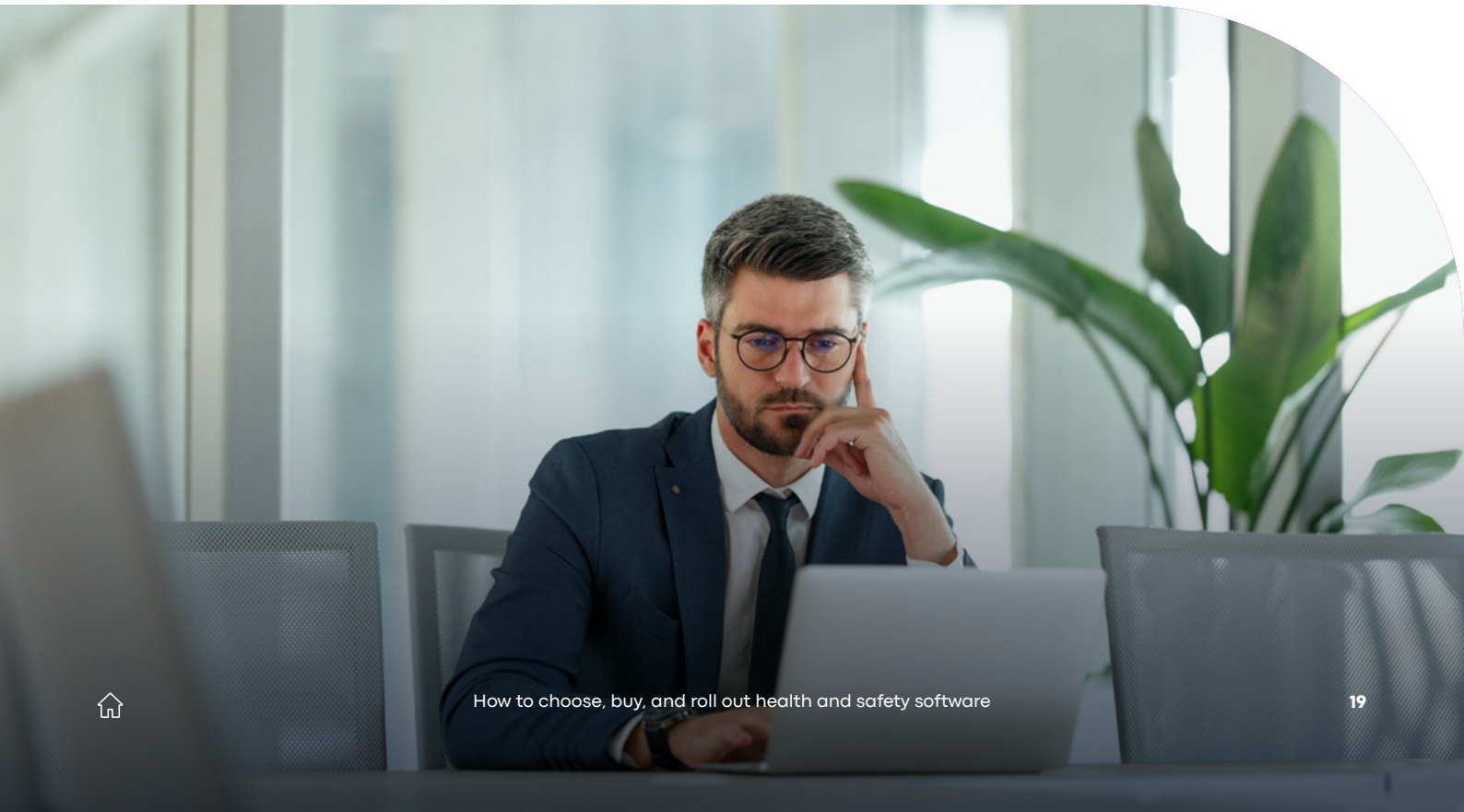
HSE's approach includes enforcement notices and prosecutions that can result in convictions - both of which are publicly recorded.

When you're framing the legal case, keep it grounded and practical. You're not trying to scare people; you're highlighting exposure and control.

Useful prompts to explore internally:

- Have we had any near misses that could have been much worse?
- Are we confident we can evidence controls, training, actions, and decisions if we're audited or investigated?
- Where are we currently relying on individuals' inboxes, spreadsheets, or knowledge to prove compliance?

The message: software reduces risk by improving consistency, visibility, and audit trails.



2. The moral case: people notice what you prioritise

Most leaders don't need convincing that safety matters. But the moral case becomes powerful when you link it to culture and trust:

- People are more likely to report issues when it's easy and the follow-through is visible.
- Teams engage more when they believe action will be taken.
- A strong safety culture supports wellbeing, retention, morale, and employer brand.

This part of the business case is about reinforcing a simple truth: good systems make it easier for people to do the right thing, every day.

3. The financial case: quantify what incidents and inefficiency really cost

This is where your business case becomes hard to ignore because it turns 'safety improvement' into tangible costs.

HSE publishes appraisal values (unit cost estimates) that can help you put credible numbers against injuries and ill health. For example, HSE's average costs to employers per case are estimated at **£111,000 for a workplace fatality** and **£7,500 for a non-fatal injury** involving **7+ days'** absence (2023/24 values, 2024 prices).

You can use these as reference points, then strengthen the case with your own internal data:

- Your incident volumes and trends
- Average time to close actions
- Admin hours spent compiling reports and evidence
- Audit preparation time
- Contractor management overhead
- Recurring issues and repeat events

The message: even small reductions in incidents, admin time, or disruption can fund the investment and the benefits stack over time.

A simple ROI starting point

- Estimate your annual number of 7+ day absence injuries (or lost-time incidents).
- Multiply by an indicative cost per case (e.g., HSE's employer cost estimate).
- Add internal hidden costs you can quantify (e.g., overtime, temporary cover, rework, investigation time, audit hours).
- Then model a conservative improvement scenario (e.g., 'reduce severity incidents by 10–20%', 'cut action close-out time by 30%', 'save X admin hours per month').
- You don't need perfection, but a credible estimate shows value.

4. The commercial case: safety impacts reputation and revenue

In many sectors, safety performance affects:

- Tender success and prequalification
- Client audits and assurance expectations
- Insurer confidence and terms
- Investor and board-level risk management
- Supply chain status (being 'approved' to operate)

This is the part of the story that helps leaders see safety software as more than an internal improvement project. It becomes a way to protect revenue, reduce disruption, and strengthen credibility with external stakeholders.

The message: if you can't demonstrate control clearly and consistently, you create commercial risk, even if your real-world performance is strong.

Pull it together: what a 'good' business case looks like

You don't need a 20-page document. In many organisations, a strong one- to two-page case (plus supporting data) is more effective.

A useful structure is:

1. The problem today (what's broken/slow/risky/inconsistent)
2. The impact (risk + cost + time + assurance gaps)
3. The outcomes we're targeting (your success criteria, SMART where possible)
4. The recommended approach (what you're buying + implementation support)
5. Cost and timeline (including internal effort)
6. Risks and mitigations (adoption, training, data migration, change management)
7. How we'll measure success (12-month view)

The four lines to include in almost every business case

- **Legal:** We need stronger, faster evidence of control and compliance.
- **Moral:** We want a culture where reporting is easy and follow-through is visible.
- **Financial:** Incidents and inefficiency have real cost and prevention pays back.
- **Commercial:** Safety performance affects trust, audits, and our ability to win and retain work.

A final tip: Keep it outcome-led

Software features matter but budgets are approved for outcomes.

If you keep your business case anchored on what the organisation will gain (time back, risk reduced, assurance strengthened, engagement improved), you'll speak to every decision-maker in a language they understand - and you'll make it much easier to get the software approved.

Navigating procurement

Once you've built stakeholder support and have a clear business case, the next step is procurement. For many organisations, this is where progress can slow down, not because anyone is trying to block the project, but because there are multiple checks to complete and several teams involved.

The good news - procurement doesn't have to be daunting. With the right preparation, you can keep momentum and move from 'approved' to 'implemented' far more smoothly.

Step 1: Get clarity on your internal process

Start by mapping the route. Every organisation is slightly different, but procurement usually requires sign-off from some combination of IT, Procurement, Legal, Finance, and Information Security.

Ask early:

- Who needs to sign off and in what order?
- Is there a standard vendor onboarding process?
- Are there templates for SaaS due diligence or a vendor questionnaire?
- What are the typical lead times for reviews and approvals?
- Are there thresholds (e.g., contract value) that trigger extra governance?

This might feel admin heavy, but knowing the process upfront prevents surprises later.

A simple procurement map to create

1. **Key stakeholder/budget owner approval**
2. **IT/InfoSec review**
3. **Procurement review (commercials, vendor onboarding)**
4. **Legal review (terms, SLA, data processing)**
5. **Final approval + purchase order/signature**

Step 2: Be ready for the four questions most organisations ask

Most procurement processes are designed to confirm a handful of core things. If you can answer these clearly and quickly, everything becomes easier.

1) Is the software secure?

Expect questions about security controls, data protection, access management, hosting, backups, and incident response.

2) Is the vendor stable?

Organisations often want confidence the supplier will still be around in 2–3 years, and able to support you long-term.

3) Are the contract and SLA clear?

This includes service levels, support response times, uptime commitments, and what happens if things go wrong.

4) Is there a plan for data migration and exit?

Procurement teams increasingly want clarity on how you'll migrate data in, and how you'd leave if you ever needed to - including data ownership, export formats, and timelines.

What to request from vendors early

- Security documentation (e.g., policies, certifications if available)
- Data protection information (e.g., DPA, sub-processors, hosting location)
- SLA/support model (hours, response times, escalation)
- Onboarding and migration approach (what's included, responsibilities)
- Exit terms (data export, retention, deletion, timelines)

Step 3: Partner closely with IT (and make it easy for them)

IT teams are often asked to validate security and technical fit, so involve them early and treat them as partners in success.Typical topics to cover include:

- Integrations (if needed)
- Access controls and user provisioning
- Authentication options (e.g., SSO)
- Data hosting and governance
- Reporting needs and data exports
- Device compatibility (especially mobile use on site)

The smoother the relationship here, the faster decisions tend to move.

Step 4: Build relationships with Legal and Procurement

Legal and procurement aren't there to slow you down - they're there to reduce risk for the organisation. The fastest projects are usually the ones where these teams are engaged early, kept informed, and given complete information.

A practical approach:

- Let them know what you're aiming to achieve and why it matters
- Share key dates or deadlines (if there are any)
- Be responsive and transparent when questions come up
- Ask what 'good' looks like from their perspective

And lean on your vendor. They onboard new customers regularly, so they should be able to:

- Provide documentation quickly
- Respond to questionnaires
- Suggest standard clauses and terms
- Support contract and security conversations
- Keep momentum with preparation and pace

Procurement feels slowest when it becomes reactive - when questions appear late, documents are missing, or stakeholders aren't aligned.

When you're proactive, the opposite happens - reviews run in parallel, blockers surface early, and the project moves forward with less friction.

The more prepared you are at this stage, the faster you'll move from selecting a platform to actually implementing it and starting to see results.

Planning your implementation

You've chosen your health and safety software. Now the work that really determines success begins - implementation.

The biggest mistake organisations make at this stage is treating implementation like a straightforward tech install. In reality, introducing a new safety system often requires changes to habits, workflows, and expectations. Depending on your organisation, it can be as much a change programme as it is a technology project.

That's why planning matters. Not just for IT and the Health and Safety team, but for your people, your sites, and the way work actually gets done.

Start by aligning with your provider

Before you build your internal plan, get clarity from your software partner on the practicalities.

Ask:

- How does onboarding work? What are the steps, and what's expected from your team?
- What's the typical go-live timeline? What affects speed, and what are realistic milestones?
- Who supports us post-launch? What does 'support' include, and how do users access it?
- These answers help you plan resourcing properly and avoid last-minute surprises.

What to confirm upfront

- Implementation approach (phased vs. big bang)
- What's included vs. paid extras (configuration, training, migration)
- Roles and responsibilities (who does what)
- Support model after go-live (hours, channels, response times)
- Any prerequisites (devices, SSO setup, permissions, site readiness)

Build the right project team

A strong rollout needs ownership and input. Bring together a small project group that can make decisions and keep momentum.

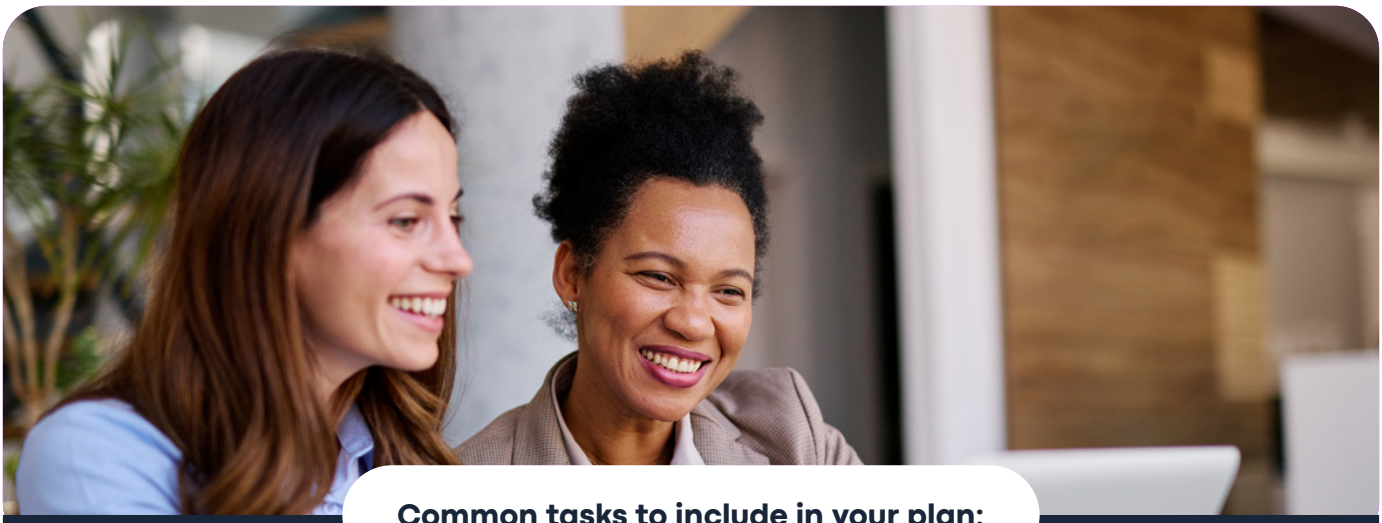
Typical roles include:

- **Project lead (often a Safety Manager) -** keeps the plan moving, coordinates stakeholders, and owns outcomes
- **IT support -** oversees security, access, integrations, and technical governance
- **Operational representatives/frontline input -** ensures workflows are usable in real settings, not just in theory
- **Optional but valuable:** HR/communications support for training and engagement, and a senior individual to unblock decisions

The aim is simple: make sure the system works for the people who will actually use it.

Create a realistic rollout timeline

Implementation goes smoothly when it's broken into clear stages. Assign ownership and actions for each stage, and be honest about timing. Rushing usually creates the problems you'll spend months fixing later.



Common tasks to include in your plan:

- Define workflows (incident types, actions, approvals, escalation)
- Set up users, roles, and permissions
- Configure reporting and dashboards aligned to success criteria
- Decide what data to migrate
- Create quick-start guidance for end users
- Schedule training sessions
- Agree success measures for the first 30/60/90 days

Communicate early - and make it relevant

Before go-live, make sure teams understand what's changing, why it matters, and what's in it for them (less admin, quicker follow-up, clearer reporting, easier access).

Keep messaging practical and human, especially for frontline workers. People are more likely to engage when they can see how the new process makes their day easier and safer.

Consider a pilot group

A small pilot can be a smart way to build confidence and improve the rollout. Invite a representative group to test key workflows and share feedback. Their experience helps you:

- Spot friction early
- Refine training and guidance
- Build internal advocates who can support others after launch

Put support in place from day one

Even the best software needs support around it - especially in the first few weeks.

Plan for:

- A clear "who to contact" route for questions and troubleshooting
- Short help guides or quick-reference pages
- Internal champions (people who can help others)
- Vendor support resources (e.g., Help Centre/ Knowledge Base)

When users feel supported, engagement increases naturally because the system feels safe and easy to use, even when people are learning.

Implementation isn't just switching software on

A well-planned rollout doesn't just activate a platform. It gives people the confidence to use it, and it sets the foundation for consistent reporting, stronger follow-through, and measurable improvement.

That's what turns a purchase into a successful safety programme.

Configuration considerations

Before you go live, you need to make sure the system is set up to work for your organisation - your sites, your teams, and your real-world processes.

Good configuration isn't about making the platform look nice. It's about removing friction, building trust, and making it easier for people to report issues and follow through.

1. Decide what data needs to be migrated (and what doesn't)

Start with your existing data and agree what should move into the new platform. Depending on your setup, this might include:

- Incident and near-miss history
- Risk assessments
- Audit and inspection templates
- Action logs
- Training records and competence evidence
- Assets or equipment registers (if relevant)

Two practical principles help here:

- **Migrate what you need to run and report -** If the data is still relevant for trend analysis, auditing, or continuity, it's often worth bringing across.
- **Don't migrate clutter -** Old, incomplete, duplicated, or inconsistent data can make the new system harder to trust from day one.

Quick migration questions

- What do we need for day-to-day operations from day one?
- What do we need for reporting and benchmarking (e.g., last 12–24 months)?
- What do we need for audits, investigations, or insurance evidence?
- What can stay archived in a read-only format outside the system?

2. Map your workflows and configure around reality

Next, focus on workflows: how work will move through the system. Start by mapping your current processes, such as:

- How incidents, hazards, and near misses are reported
- How investigations are initiated and completed
- How corrective actions are assigned, tracked, evidenced, and closed
- How escalations work when actions become overdue or high risk
- How approvals and reviews happen (if needed)

Then configure the system to match the steps that actually happen in real life, not just what's written in a policy.

This is also a good time to simplify. If your current workflow has grown complex because of manual workarounds, the new system can be an opportunity to streamline.

3. Use customisation carefully - make it familiar, not complicated

Most platforms offer some level of configuration: terminology, forms, categories, dashboards, and reporting. When done well, this can make the system feel familiar and relevant from the outset.

Aim for:

- Language that matches how your organisation speaks (site names, departments, role titles)
- Forms that collect the right level of detail
- Dashboards that reflect your success criteria and the decisions you need to make
- Incident categories that help you understand root causes and trends over time

Involve frontline users early

Frontline teams can spot friction quickly - confusing questions, unnecessary steps, missing options, or anything that makes reporting slower than it needs to be. If adoption is your goal, their input at this stage is invaluable.

4. Test the system before launch

Before you roll out, test workflows end-to-end using realistic scenarios. For example:

- Reporting a hazard or near miss on a mobile device
- Submitting an incident with photos
- Assigning an action and checking reminders/escalation
- Completing an investigation and closing out actions with evidence
- Pulling a simple dashboard or monthly trend report

Testing isn't just a tick-box. It's how you catch the practical issues that would otherwise show up after go-live.

What "good testing" looks like

- Use real scenarios from different sites/teams
- Test on the devices people actually use
- Involve both admin users and frontline reporters
- Confirm reporting outputs match what leadership expects
- Fix friction before launch, not after

Configure for culture, not just compliance

Ultimately, the goal isn't simply to 'set up' the system. It's to configure it in a way that supports your safety culture and makes life easier for your teams.

When configuration is right, reporting becomes easier, follow-through becomes stronger, and the system becomes part of daily work - which is where the real impact happens.

Making safety software stick

A successful launch is only the beginning. The real value comes when people use the system day in, day out - when reporting becomes normal, actions get closed consistently, and safety insights are visible across the organisation.

It's tempting to assume that if you buy new software and tell people to use it, adoption will follow naturally. In reality, it rarely works that way. People don't change behaviour because a tool exists - they change when it feels useful, easy, and trusted.

So how do you build genuine engagement?

1. Make it relevant

Start by showing colleagues what's in it for them. End users don't engage with systems because they help the business produce reports. They engage when the system helps them do their job more safely and with less friction.

Practical examples work best:

- Reporting an incident or hazard in under a minute from a mobile device
- Uploading a photo so an issue can be acted on quickly
- Raising a concern that protects a colleague
- Seeing that actions are assigned and followed through, not ignored

The key is to position the platform as something that makes life easier and enables safer decisions. Tone matters too. If reporting feels like blame, people will avoid it. If it feels like prevention and improvement, people will use it.

2. Create feedback loops

One of the fastest ways to increase engagement is also one of the simplest: close the loop. When someone reports a hazard, near miss, or accident, tell them what happened next:

- What action was taken?
- What was changed?
- What was learned?
- What's being done to stop it happening again?

When workers see that reporting leads to real change, they keep reporting. When they feel it disappears into a void, engagement drops. You can reinforce this with regular updates:

- "You said, we did" summaries
- Recent hazards identified
- Lessons learned and quick wins
- Reminders that actions are being completed

A simple message that works

"If you spot something, report it quickly. We'll follow up, and you'll hear what happens next."

3. Keep it simple - remove friction wherever you can

If reporting takes too long, requires too many fields, or is hard to do on the devices people actually use, adoption will stall. Make it easy to do the right thing:

- Keep forms short and relevant
- Use clear categories and plain language
- Ensure mobile reporting works smoothly
- Avoid "optional" steps that feel mandatory in practice
- Make it obvious what happens after submission

A good rule of thumb: if someone can't report a hazard quickly during a busy shift, the process isn't designed for reality.

4. Recognise and reinforce the right behaviours

Recognition builds momentum, and it doesn't have to be complicated. You might:

- Give shout-outs to teams who spot and report hazards proactively
- Recognise sites that improve action close-out rates
- Celebrate meaningful contributions (not just volume)
- Share examples where reporting prevented an incident

Some organisations also use light gamification to keep safety visible, for example, friendly competition between sites, or progress dashboards showing improvements over time. Be careful with metrics however - you want to encourage quality reporting and meaningful follow-through, not a rush to hit numbers.

Recognition ideas that encourage real impact

- 'Best catch of the month' (a hazard spotted early)
- 'Fastest meaningful fix' (action closed with evidence)
- 'Most improved site/team' (better reporting and better close-out)

5. Build a network of champions

Engagement doesn't happen by accident. It needs advocates - people who reinforce the new way of working, answer questions, and keep momentum going after the initial launch.

Choose champions across teams and sites (not just within health and safety) and empower them to:

- Demonstrate how to report quickly
- Encourage reporting without blame
- Support colleagues who are less confident with new tools
- Share feedback on what's working (and what isn't)
- Celebrate progress and keep safety visible

Make it a tool people want to use

The more you involve your workforce, recognise contributions, and keep processes simple, the more the system becomes something people choose to use because it helps them.

That's when you start to see the real return: better visibility, stronger follow-through, and a safety culture where prevention becomes part of everyday work.

Measuring success

Once your system is in use, you can start measuring success, starting with clear KPIs.This is where many organisations miss an opportunity. They implement a platform, then only look at the data when it's time for a monthly report or a board update.

But the real value comes when you use your metrics regularly to spot risks early, prioritise action, and keep momentum going.The simplest place to start is to revisit the success criteria you set at the beginning of this process. Ask:

- Are reports being submitted faster and more consistently?
- Are actions being closed out quicker, with better follow-through?
- Are more hazards and near misses being identified before they escalate?
- Is visibility improving across sites, departments, or contractors?

A good platform will support this with dashboards and reporting that makes progress visible.

Choose KPIs that reflect what you're trying to improve

Not all safety metrics are equal. The most useful KPI sets include a balance of:

- Lagging indicators (what has already happened)
- Leading indicators (signals of prevention and engagement)
- Process measures (whether your safety system is being used effectively)

Lagging indicators (less is better)

These measures reflect harm and serious outcomes, and they help you understand risk exposure over time. Examples include:

- Number of incidents reported by type (accidents, injuries)
- High-impact incidents (e.g., RIDDOR-reportable cases, lost time injuries)
- Severity trends (e.g., injury severity, time lost)

Leading indicators (more is better)

Leading indicators can show engagement and early risk detection, which is what helps you prevent harm. Examples include:

- Near misses reported
- Safety observations logged
- Hazard reports submitted
- Proactive inspections completed
- Positive interventions (where someone prevented unsafe work).

Note

More leading indicators isn't automatically 'good', but becomes powerful when paired with meaningful follow-through.

Process measures (are we doing what we said we would do?)

These show whether the system is functioning and whether improvement is likely to be sustained. Examples include:

- Action close-out rates and time-to-close
- % of actions overdue (and by how long)
- Audit and inspection completion rates
- Repeat issues (same hazard types, same locations, same root causes)
- Reporting participation (is it broad, or only a few people?)

You may also track industry-recognised metrics such as:

- Accident Frequency Rate (AFR)
- Lost Time Incident Frequency Rate (LTIFR)

Use dashboards as decision-making tools, not just reporting tools

Dashboards shouldn't exist solely to create monthly slides. Used well, they help you:

- Identify trends early
- Compare performance across sites or teams
- Highlight hotspots (by activity, location, time, or hazard type)
- Prioritise action where it will make the biggest difference

Look for patterns such as:

- One site consistently outperforming others (and why)
- Spikes in a specific incident type
- Rising near misses without corresponding action close-out
- Recurring root causes that point to a training, maintenance, or process gap

Share insights widely (and close the loop)

Transparency builds engagement. When teams can see the impact of their reporting - hazards resolved, actions completed, risks reduced - it reinforces good behaviours and strengthens culture.

Sharing insights also encourages shared responsibility, because improvement stops being 'a safety team task' and becomes something visible across the organisation. A few practical ways to do this:

- Site dashboards displayed and discussed in team meetings
- Monthly highlights - wins, trends, and focus areas
- Learning summaries after incidents or repeat issues

Keep evolving your definition of success

Success isn't static. Once you have momentum, use your data to set new targets, refine workflows and reporting categories, identify where training or controls need strengthening, and focus on prevention, not just documentation.

The goal is to move from reactive management to proactive improvement - using evidence to guide decisions and build a culture of continuous learning.

Because dashboards aren't just reporting tools. They're decision-making tools. When used consistently, they help you make safety performance visible, actionable, and measurable over time.

Final thoughts

Thanks for reading! We hope this eBook has given you the clarity, tools, and confidence to take the next step, whether you're replacing an outdated system or moving to digital for the very first time.

Selecting and implementing health and safety software can feel like a big project, but the process becomes far more manageable when it's broken into clear stages, as detailed in the chapters of this eBook.

Most importantly, remember - software only delivers value when it's used. The goal isn't just to launch a platform, it's to create consistent reporting, stronger follow-through, better visibility, and a culture where prevention becomes the norm.

Your next step

If you'd like to explore what good can look like in practice, you may find it useful to see a safety platform in action.

If you want to see how Notify can help you proactively manage workplace risks - from reporting and action tracking to insights and continuous improvement - you can book a demo. Our friendly, expert team will be happy to walk you through the platform and answer any questions.

Good luck with your project.

Spark

Your AI-powered companion, for fast, high-quality post-incident analysis

On a mission to create a safer, healthier world of work

Talk to the team

hello@notifytechnology.com
(+44) 0330 390 0530
notifytechnology.com