Restricted Content

Critical Risk Management

Implementation Toolkit for Large Organisations

2027

This toolkit helps large PCBUs sustain Critical Risk Management through everyday decisions, effective controls, clear accountability, and verification.

DRAFT

Restricted Content

Contents

Purpose, Audience and Scope 4
How to Use This Toolkit 4
The Seven Tools at a Glance 4
Templates, Worked Examples and Record Burden 5
How the Guide and Toolkit Work Together 5
Implementation Pathway 7
Readiness Checks for Phased Implementation 9
Tool 1: Accountability and Operating Model 10
Tool 2: Critical Risk Identification and Register 12
Tool 3: Critical Risk Assessment 13
Tool 4: Critical Control Decision and Standard 15
From control standards to evidence, confidence and decisions 18
Tool 5: Verification and Failure Response Plan 19
Part A: Annual Operational Verification Programme 19
Part B: Risk/Control-Specific Verification and Response 19
Tool 6: Assurance and Confidence 22
Assessing and explaining confidence 22
Supplementary example – energy isolation: verification trends and assurance confidence 23
Tool 7: Reporting, Learning, and Improvement 24
Part A: Reporting Performance and Confidence 24
Interpreting incident evidence 25
Part B: Turning Findings into Improvement 27
Capability Readiness Record 28
Implementation Readiness Checklist and Worked Example 29
Implementation Readiness Criteria 29
Appendix A: Tool 1 – Enterprise CRM Framework and Operating Model Record 33
Appendix B: Tool 2 – Critical Risk Register Template and Worked Example 34
Worked Example 35
Appendix C: Tool 3 – Critical Risk Assessment Template and Worked Example 36
Worked Example 37
Appendix D: Tool 4 – Critical Control Decision and Standard Templates and Worked Examples 39
Worked Example 41
Appendix E: Tool 5 – Verification Programme and Verification Plan Templates and Worked Examples 44
Part A: Annual Operational Verification Programme 44
Worked Example: Annual Verification Programme 45

Part B: Risk/Control-Specific Verification and Response 47
Worked Example 48
Risk-Based Assurance Programme 50
Worked Example: Risk-Based Assurance Programme 51
Worked Example: Mobile-Plant Assurance Across 12 Sites (primary example) 52
Worked Example: Periodic Performance and Confidence 53
Worked Example: Material Issue and Improvement Record 55

Appendix F: Tool 6 – Assurance and Confidence Template and Worked Example **50**
Tool 6 template: Risk-Based Assurance Programme 50
Tool 6 worked example: Risk-Based Assurance Programme 51

Appendix G: Tool 7 – Performance and Confidence Summary and Material Issue Record Templates and Worked Examples **53**
Tool 7A template: Periodic Performance and Confidence Summary 53
Tool 7B template: Material Issue and Improvement Record 55
Tool 7B worked example: Material Issue and Improvement Record 55

Appendix H: Capability Readiness Record – Template **57**

Restricted Content

Restricted Content

Purpose, Audience and Scope

Read this toolkit alongside *Critical Risk Management: A Good Practice Guide (2027)* (‘*the Guide*’). It translates the Guide’s principles into implementation decisions and records. Check applicable law, regulations, Approved Codes of Practice, and regulator guidance. Neither document replaces competent legal or technical advice.

This toolkit is for health, safety and wellbeing (HSW) professionals, technical specialists, and the operational and executive leaders accountable for the HSW of frontline leaders and workers. It provides templates and worked examples showing the evidence and decisions needed to implement and sustain Critical Risk Management (CRM).

It uses the Guide’s five **functions**: ***lead and govern; own, manage, verify and monitor; support, advise and challenge; assure***; and, where commissioned, ***review independently***. Any competent function – HSW, engineering, occupational hygiene or another specialist – may provide support and assurance, but never takes accountability for managing critical risks, controls and verification away from operational leaders, including executives.

In plain terms:

- Line leaders (‘Line 1’) own critical risks and verify controls.
- Support functions - such as HSW teams (‘Line 2’) – own the CRM framework, help and advise line leaders with CRM, sample critical controls, and provide a constructive test-and-challenge perspective on confidence that CRM is being effectively achieved.
- Assessments by fully independent internal or external specialists (‘Line 3’) are commissioned as necessary.

Reference to ‘*Line 1/2/3*’ is shorthand to who does what within CRM, not a prescribed structure.

Some organisations that meet the legal definition of a ‘large’ PCBU under the Health and Safety at Work Act 2015 may still find the small-PCBU toolkit a better fit.

How to Use This Toolkit

Read this first. This toolkit is implementation support for organisations that want more structure than the Guide alone provides. It is **not a prescribed operating model**, and its templates are **not mandatory forms**.

- The **seven tools** describe implementation decisions and provide usable example records.
- **Adapt them** to your risk profile, size, maturity, existing systems, and operating model.
- **Existing systems and records may already satisfy the intent.** Do not create duplicate systems or forms simply to mirror this toolkit.
- **Templates are adaptable examples. Worked examples** show one way of applying the method, not a required organisational model.
- **Protection needed for current work cannot be deferred** while implementation systems mature.

The Seven Tools at a Glance

Tools 1–4 decide what protection is required; Tools 5–7 check it works and drive decisions. Findings loop back to Tools 2–4. **Verification, response, and escalation never wait for later tools to mature.**

Restricted Content

Templates, Worked Examples and Record Burden

Each tool has guidance in the main body of this toolkit and a matching appendix containing an adaptable template. Most also include an illustrative worked example. Templates have a dark grey header (**Template: adapt to your organisation**); worked examples have a navy header (**worked example**).

One primary example – **mobile plant across a fictional 12-site network** – runs through Tools 2 to 7.

Before you complete or mandate any record, ask: **does it support an important decision, demonstrate control performance, make uncertainty visible, enable escalation, or help improvement?** If not, remove it, combine it with another record or make it optional.

- **Embed and reference.** Keep the information in your existing risk, engineering, verification, maintenance, incident, action-tracking and governance systems, linked by one risk/control ID. Refer to existing records rather than retyping evidence between tools.
- **The Guide is the normative source** for concepts and definitions; this toolkit shows ways to implement them.

How the Guide and Toolkit Work Together

The Guide explains good CRM practice; this toolkit proposes the practical decisions and activities needed to implement and sustain it in a large organisation.

The tools here follow a practical implementation roadmap rather than the order of the Guide. The table below maps sections of the Guide to the sections and tools in this toolkit.

Guide section	Toolkit location	Application
1. The problem and 3. Overview	Purpose and Scope; Pathway	Sets purpose, scope and the implementation cycle for preventing serious harm.
2. Legal context	Tools 1–3	Sets the enterprise method, applies both critical risk classification routes, and evidences the reasonably practicable control strategy.
4. Accountability, leadership and assurance	Pathway; Tools 1, 5–7	Assigns accountability, verification, reporting, governance decisions and objective assurance; capability maps to Section 8.
5. Identifying and assessing critical risks	Tools 2–3	Identifies, classifies and records scenarios, then assesses pathways and protection, updating the register from findings.
6. Selecting and defining critical controls	Tools 3–4	Applies the hierarchy to the reasonably practicable control strategy, designates critical controls, and approves performance standards.
6 (continued). Embedding controls and managing change	Tools 1, 4–5; Readiness; Maintain and Improve	Embeds controls in business decisions, assigns shared duties and change authority, verifies implementation and tests readiness.
7. Critical control verification, monitoring and assurance	Tools 5–6	Approves annual operational verification programmes and linked control plans; operational leaders monitor verification findings and other evidence for patterns and weaknesses; assurance separately tests the evidence and judges confidence. Control effectiveness (design capability) is established through competent technical assessment.

8. Capability	Pathway; Capability Record; Readiness	Demonstrates role-specific capability, records evidence and confirming roles, and reassesses readiness after work or evidence changes.
9. Measurement and reporting	Tools 6–7	Reports counts, proportions, coverage, effectiveness and limits alongside attributed assurance confidence, keeping performance and event learning distinct.
10. Preventing drift	Tools 5–7; Maintain and Improve	Uses verification, assurance, event learning, change, workarounds and emerging weaknesses to trigger review, escalation and improvement.

Restricted Content

Implementation Pathway

Guide link: Sections 3–10. Implementation is phased and iterative – not a requirement to finish every tool first. Use the ten stages on the following page as a menu to adapt, and check readiness before each rollout phase, expansion or material change.

Non-negotiable baseline at every phase

- Current critical risk exposure has **effective protection**, verified where relied on.
- **Accountability is clear** for each critical risk and control.
- Failed or uncertain protection triggers an **immediate response**: restrict affected work, restore, or use a verified effective alternative, and escalate.
- Phased development of the wider framework **never authorises unprotected work**.



Implementation Pathway: roles and completion evidence

	Stage	Roles	Completion evidence
1	**Mobilise and govern**	**Accountable:** CEO or delegated executive (CRM sponsor). **Delivery:** operational executives. **Support:** senior HSW leader.	Mandate, scope, governance, decision rights, resources and operational accountability agreed
2	**Establish the CRM framework**	**Accountable:** senior leader of the Line 2 function that owns the framework (HSW or equivalent). **Support:** technical, operational and assurance functions. **Approval:** sponsor / governance.	Usable framework approved: criteria, method, roles, records, verification, assurance, escalation
3	**Identify, classify and register critical risks**	**Accountable:** operational risk owner. **Support:** HSW / method adviser (e.g. HSW team). **Approval:** technical authority validates (e.g. engineering, process safety).	Scenarios, classification evidence, uncertainties and owners recorded
4	**Assess exposure pathways and current controls**	**Accountable:** operational risk owner. **Support:** operations, technical authorities, method advisers (e.g. HSW, engineering).	Work-as-done, pathways, controls and uncertainty assessed; required protection set; register updated
5	**Determine the reasonably practicable control strategy**	**Accountable:** operational risk owner. **Technical lead:** technical authority (e.g. HSW, engineering, process safety). **Support:** competent specialists.	Strategy justified independently of current practice, using the hierarchy, guidance and event learning
6	**Confirm critical controls and standards**	**Accountable:** operational risk owner. **Support:** designated operational managers. **Approval:** technical authority (e.g. engineering).	All four criteria evidenced; testable standards, owners and failure response approved
7	**Assess conformance and close gaps**	**Accountable:** operational risk owner. **Delivery:** designated operational manager. **Approval:** technical authority validates design.	Controls checked against standard; design effectiveness assessed technically; gaps owned with interim protection and escalation
8	**Implement verification and failure response**	**Accountable:** senior operational leader approves and resources the programme. **Delivery:** managers, supervisors, verifiers. **Support:** HSW, technical authorities.	Annual programme approved and resourced; failures escalated immediately
9	**Assure evidence and judge confidence**	**Assurance lead:** competent, objective Line 2 provider (e.g. HSW). **Action owner:** operations. **Independent review:** Line 3, where commissioned.	Risk-based assurance; coverage gaps visible; reasoned confidence with limits; action does not wait
10	**Report, learn and improve**	**Accountable:** operational leader. **Support:** Line 2 function integrates findings and updates the framework. **Decisions:** executives set priorities and resources.	Results, confidence and incidents drive action; weaknesses explicit; readiness reassessed
	Across the pathway: check readiness and improve	**Accountable:** operational executive. **Support:** HSW / technical advisers. **Improvement:** risk owners and managers.	**Next-phase prerequisites assessed; gaps owned; repeat before rollout, expansion or change. Readiness does not authorise individual work.**

Accountable **Delivery** **Support** **Approval**

HSW = HSW or an equivalent Line 2 function.

Across every stage: Involve affected workers, HSRs, frontline leaders, and contractors; share information, provide reasonable opportunities to contribute, consider views, and communicate decisions. Worker engagement, including through HSRs, never transfers the PCBU's duties or operational leaders' accountabilities to workers or representatives.

Readiness Checks for Phased Implementation

Before each rollout phase, expansion or material change, complete the readiness checklist in the appendix. For each one:

- **Define** the next step, its scope, the decision owner and the date.
- **Point to existing evidence** rather than re-describing it.
- **Give later requirements** an owner and a trigger.

Readiness never authorises individual work, and protection needed for current work cannot be deferred.

Restricted Content

Restricted Content

Tool 1: Accountability and Operating Model

Guide link: *Section 4: accountability, leadership, governance and assurance, with enterprise requirements supporting Sections 5–9.*

PCBUs should agree a clear CRM operating model early and adapt it as CRM implementation matures. Start with the **functions** required, then decide who is best placed to provide each. The visual below expands on the high-level CRM operating model in the Guide and reflects what may be envisaged within a large PCBU; it is illustrative and reflects good practice, but it is **not a prescribed organisational design**.

Two kinds of ownership. The HSW function, or an equivalent Line 2 function, **owns the CRM framework** – its method, standards and tools – and builds the capability to use it. Operational leaders at every level **implement the framework and own critical risks, controls and verification**. At all times, ownership of critical risks, controls and verification stays with line leaders.

When assigning roles, use the Capability Readiness Record (a cross-cutting resource for Tools 1–7) to confirm necessary CRM capabilities before people make CRM decisions or perform verification.



CRM decision rights to settle before improvement efforts start – record in your existing delegation documents		
Decision	**Who has authority (by role)**	**Safeguard**
Own and maintain the CRM framework (method, standards and tools)	HSW or an equivalent Line 2 function, approved by the executive governance forum.	Operational leaders implement the framework and own the critical risks, controls and verification it supports.
Accept ownership of the critical risk, its controls, resource requirements, and failure response	Named operational leader (site, area, or business unit/executive).	Support or assurance roles advise operational leaders; they do not take ownership of critical risks, controls or verification.
Approve CRM standards, designs, and alternative protection	Specific role with sufficient technical authority for that control type and with sufficient authority to guide the organisation; operational owner confirms it is practicable and resources it.	Approver is competent for this control type and has no personal or budget interest in operational work continuing without that control.
Authorise work to restart after failed, uncertain, or removed CRM protection	Operational owner of the affected work, after a competent verifier confirms effective protection (technical authority where design is affected).	Restart evidence recorded; due dates or plans never authorise exposure.
Judge the confidence the Line 1 verification activity and findings warrant	A sufficiently competent and objective function, team, or role (e.g., HSW, process safety, engineering).	Peer or external challenge for work the assurer helped design.
Resolve an issue that crosses business units or PCBUs	Lowest common accountable leader, then up to the executive who can resolve it.	Agree in advance who restricts work meanwhile. Allocation never transfers legal duties.

Input (what is required to begin)	**Decision (what must be decided)**	**Output (what must be in place by the end)**
Enterprise mandate, Guide principles, and organisational context	How will CRM be governed, owned, and technically supported across the PCBU?	Approved CRM framework, documented decision rights, and CRM operating model

Template: Appendix A. The *T1 Enterprise CRM Framework and Operating Model Record* captures the enterprise decisions behind this tool in one place: mandate and scope, how critical risk is defined and assessed, accountabilities and technical decision rights, existing record systems, local adaptation, business decision-gates and shared duties, and governance reporting. Use it to record decisions or reference existing governance documents if they already hold them.

Use it to record decisions or reference existing governance documents if they already hold them.

Handoff: CRM mandate, framework, ownership, technical approvals, and reporting agreed → identify risks in Tool 2.

Restricted Content

Tool 2: Critical Risk Identification and Register

Guide link: *Sections 2 and 5: legal classification routes, identifying/describing critical risks.*

PCBUs must identify and classify serious harm scenarios with workers, contractors, and operational leaders; refine entries through Tool 3. HSW or another competent function may facilitate this work, but the operational owner remains accountable for it. Protective action must not await completed records.

A **serious harm scenario** describes what could happen, to whom, and in what circumstances. **Exposure** pathways then explain how harm could occur, including through repeated or prolonged exposure.

PCBUs should consider both critical risk classification routes in Guide Section 2 when identifying their critical risks: association with an applicable Schedule 1A hazard; or another hazard where occurrence of the risk (i.e., the scenario) is likely to cause death, notifiable injury or illness, a notifiable incident, or a listed occupational disease. This assessment should cover routine and non-routine work, maintenance, shutdowns, abnormal conditions, and work involving shared PCBU responsibilities.

PCBUs should not impose arbitrary limits on the number of critical risks they document – all that exist should be identified.

Key tips and advice as you work through the critical risk identification process:

- Use one consistent critical risk ID across assessment, control, verification, and reporting records.
- Do not exclude qualifying critical risks because events relating to them are rare, existing controls seem effective, or because of an internal risk matrix score or rating for them.
- Describe exposure across relevant sites, tasks, shifts, assets, operating conditions, and contractor interfaces.
- Use role titles, not individual names, for ownership wherever possible.
- Specify the next action and event-based review triggers rather than relying on an annual review alone.

Tip – enterprise register and local context, without duplicate systems. An enterprise critical risk register can hold the agreed CRM scenarios, classification, owner, risk ID, and standards.

Input (what is required to begin)	Decision (what must be decided)	Output (what must be in place by the end)
Enterprise criteria, work-as-done evidence, and serious-outcome information	Which serious-harm scenarios meet the critical risk threshold**?**	CRM register entries with classification evidence, owners and visible uncertainties

Template and worked example: Appendix B. The *Tool 2 register template* records each serious-harm scenario in one place. It covers:

- The critical risk ID
- the serious harm scenario and its exposure pathways
- the classification route used and supporting evidence for the final classification
- the operational owner
- any visible uncertainties
- the next action and event-based review triggers.

The worked example shows how the primary mobile-plant scenario (CR-02) is recorded. Use the tool to record each scenario, or reference your existing risk register if it already holds this information. Go to **Appendix B**.

Handoff: Record the scenario, classification basis and owner, then assess pathways and protection in Tool 3. Update the register as findings develop.

Restricted Content

Tool 3: Critical Risk Assessment

Guide link: *Sections 5 and 6: assessing exposure and control needs, applying the hierarchy and determining reasonably practicable protection.*

For each serious harm scenario identified in Tool 2, a multidisciplinary team should assess the exposure pathways, existing controls and required protection. The findings from this work should refine the PCBU's critical risk register scope or classification. The HSW team – or another CRM methodology specialist – may facilitate this process, with technical specialists validating risks and/or controls within their authority and workers testing their practicality. The operational risk owner remains accountable for their CRM plan, necessary resources, and implementation.

PCBUs should start by assessing whether elimination for each critical risk is reasonably practicable. If it is not, select the strongest suitable combination of controls through the hierarchy, then confirm that those controls can protect against the exposure, foreseeable failures, and dependencies associated with that risk. Complex risks – such as those relating to process safety – may need deeper specialist analysis.

PCBUs should base the assessment on what is known, or ought reasonably to be known, including law, codes, guidance, standards, and technical practice. Organisational preferences, budgets, risk appetite statements, and risk-matrix or investment thresholds do not, by themselves, establish what is or is not reasonably practicable. PCBUs should consider cost last when assessing what is reasonably practicable: rejecting an option on cost grounds requires evidence of gross disproportionality that could be defended to an external party – or to the officers of the PCBU – should that decision be tested.



Key tips and advice:

- Start with Tool 2's serious harm scenario, then assess actual work (routine and non-routine), foreseeable variations in how work is undertaken, and contractor interfaces.
- Test options in local conditions; use technical and external evidence to identify suitable controls and benchmarks.
- Take both existing and proposed controls into Tool 4 for assessment as to whether they are 'critical' or 'supporting' controls; do not automatically label them as critical controls beforehand.
- Treat uncertainty, missing evidence, and differences between existing and required controls as gaps requiring action.
- Give every interim control, improvement, investment decision, and escalation an accountable role and due date.

Tip – "credible". Support the judgement with relevant technical and operational expertise, industry experience, and comparable serious events – not a subjective sense of whether something "could" happen. Rarity or a good recent record does not make a serious scenario less credible.

Decision required
Determine the reasonably practicable control strategy. Current practice establishes the starting point, not the benchmark for adequacy.

Input (what is required to begin)	Decision (what must be decided)	Output (what must be in place by the end)
Tool 2 scenario, critical risk classification basis, uncertainties, and work evidence	How could serious harm occur, and what is the reasonably practicable control strategy to manage that scenario?	Agreed control strategy for specific risk/s, gaps, candidate critical controls, and risk register updates

Template and worked example: Appendix C. The Tool 3 template records, for each Tool 2 scenario, how serious harm could occur, the protection required, current controls, gaps and improvement actions, and carries candidate critical controls into Tool 4. The worked example assesses the mobile-plant scenario. Use it to record each assessment, or reference your existing risk assessment if it already holds this information. Go to **Appendix C**.

Handoff: Update Tool 2 from assessment findings; take required protection, gaps and candidate controls into Tool 4. Protective action does not wait.

Restricted Content

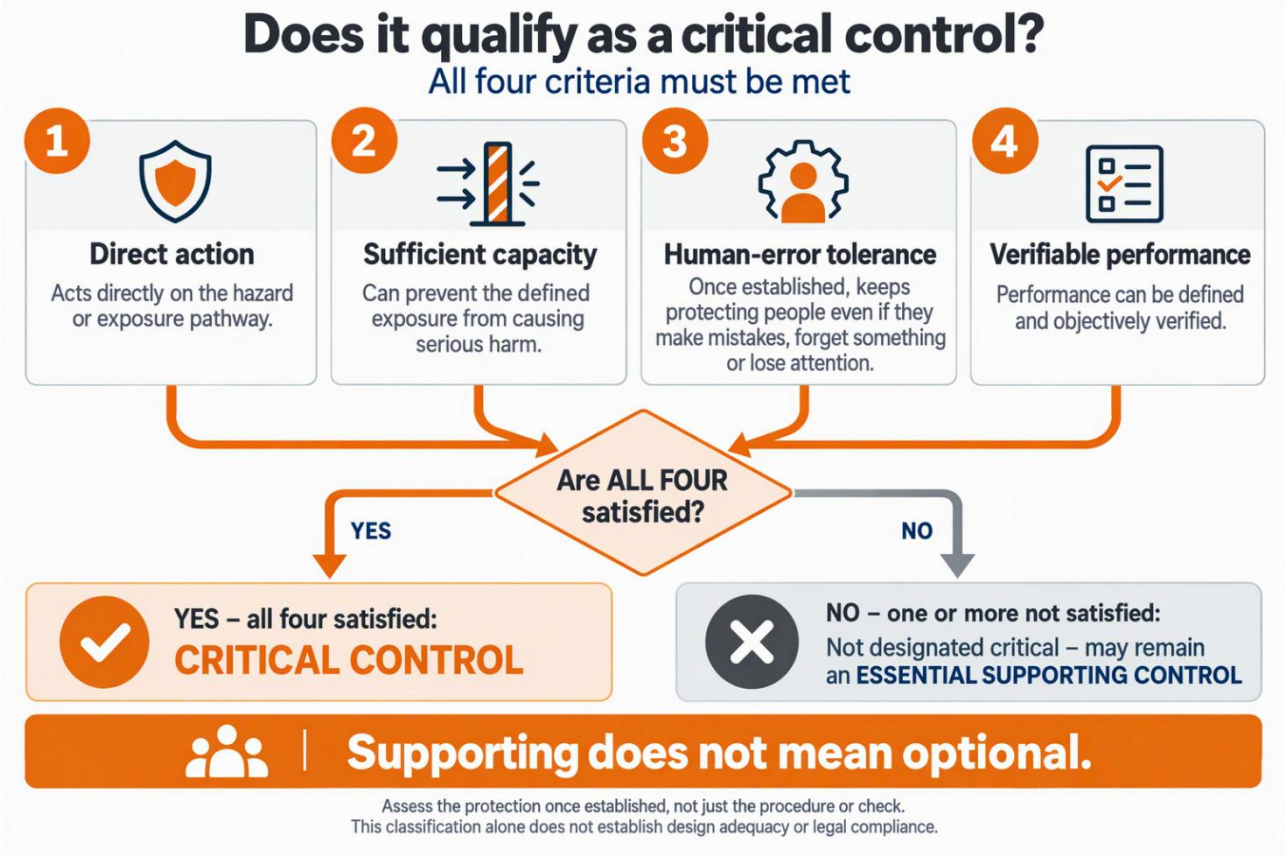
Tool 4: Critical Control Decision and Standard

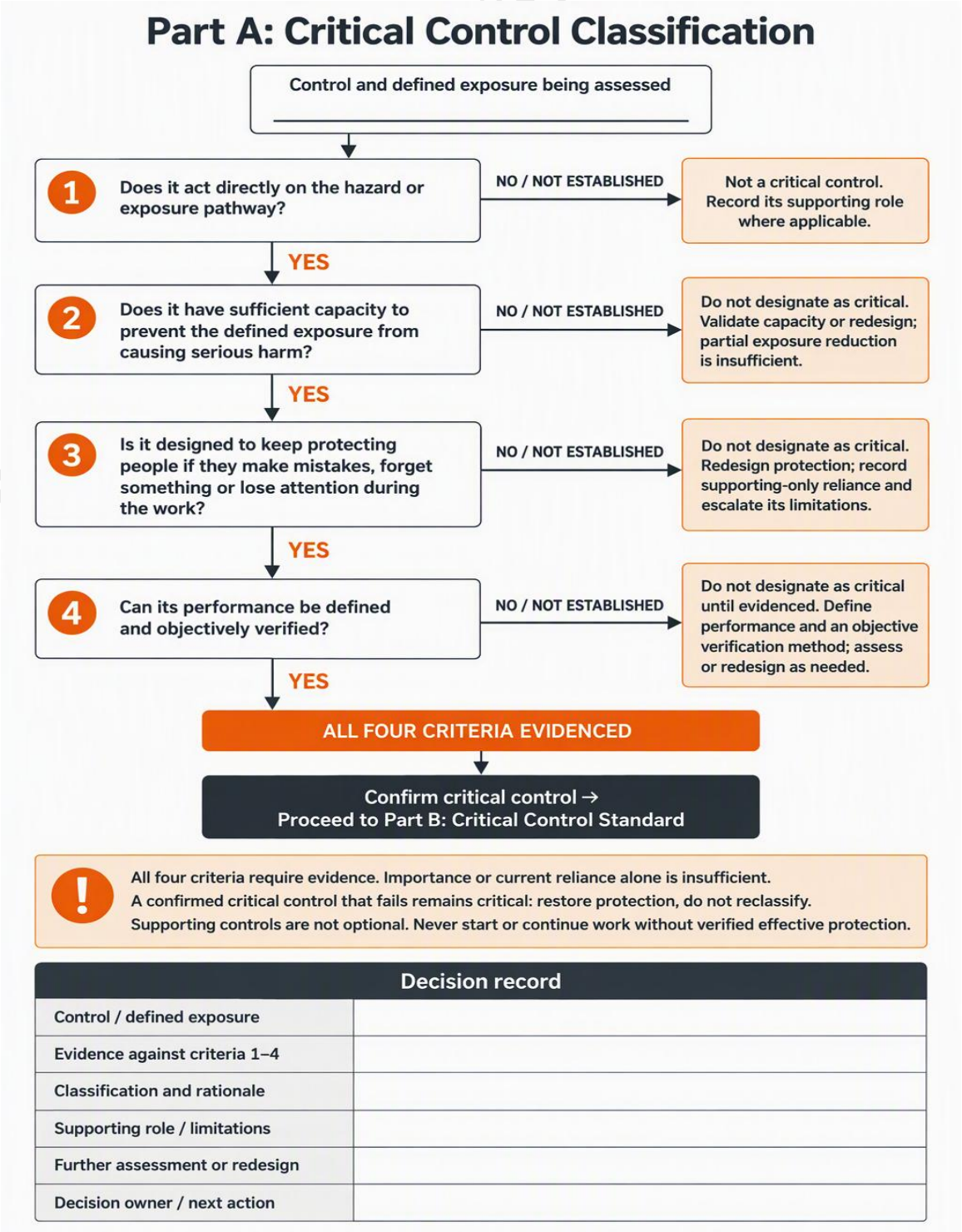
Guide link: *Section 6: designating critical controls, distinguishing supporting controls and defining performance, ownership and change requirements.*

Operational representatives and technical specialists should jointly assess whether each candidate control is a critical control or a supporting control; Tool 4A on the next page provides a clear decision flowchart. Competent specialists then develop the control standards (Tool 4B), and the delegated technical authority approves technical requirements as appropriate. Operational owners assess the applicability of those controls within their operations and own the resourcing, implementation, and response to failure of those controls. Workers and designated operational managers contribute to this by testing practicality, dependencies, and workarounds.

Decision before standard: Use the four criteria below to assess each candidate control, then complete Tool 4B for those that have been confirmed as critical controls.

Supporting controls first. Most controls in a CRM strategy are likely to be supporting controls such as training, procedures, permits, supervision, and signs or alarms that depend on a person responding. 'Supporting' does not mean a control is optional, unimportant, or unnecessary. Supporting controls can still be essential, need a clear purpose, owner, and checks, and the failure of a supporting control may require work to stop. In this toolkit, a control is designated 'critical' only if it meets all four criteria below.





Do not designate as critical unless all four criteria are supported by evidence. Importance, current reliance or procedural status alone is not sufficient.

The third criterion does not exclude people having a role in relation to the installation or effective application of the specific control. People routinely design, install, operate, maintain, and verify critical controls. The test is whether – once implemented – the control would continue to work effectively even if a person made a mistake or failed to respond perfectly.

A supporting control does not become critical simply because it is the strongest control a PCBU has available and a critical control that fails remains a critical. A failure requires the PCBU to restore protection, not reclassify the control.

Work does not continue without effective protection while a better control is pursued. Where no control meets all four criteria and management of the risk is therefore dependent solely on supporting controls, this reliance should be made visible to leaders and officers so that they can understand where further risk reduction improvement and/or innovation may be warranted.

Input (what is required to begin)	**Decision (what must be decided)**	**Output (what must be in place by the end)**
Agreed control strategy and candidate critical controls	Does each control meet all four criteria, and what control specific standard must it meet?	Classified controls, approved control specific standards, and conformance gaps with accountable owners

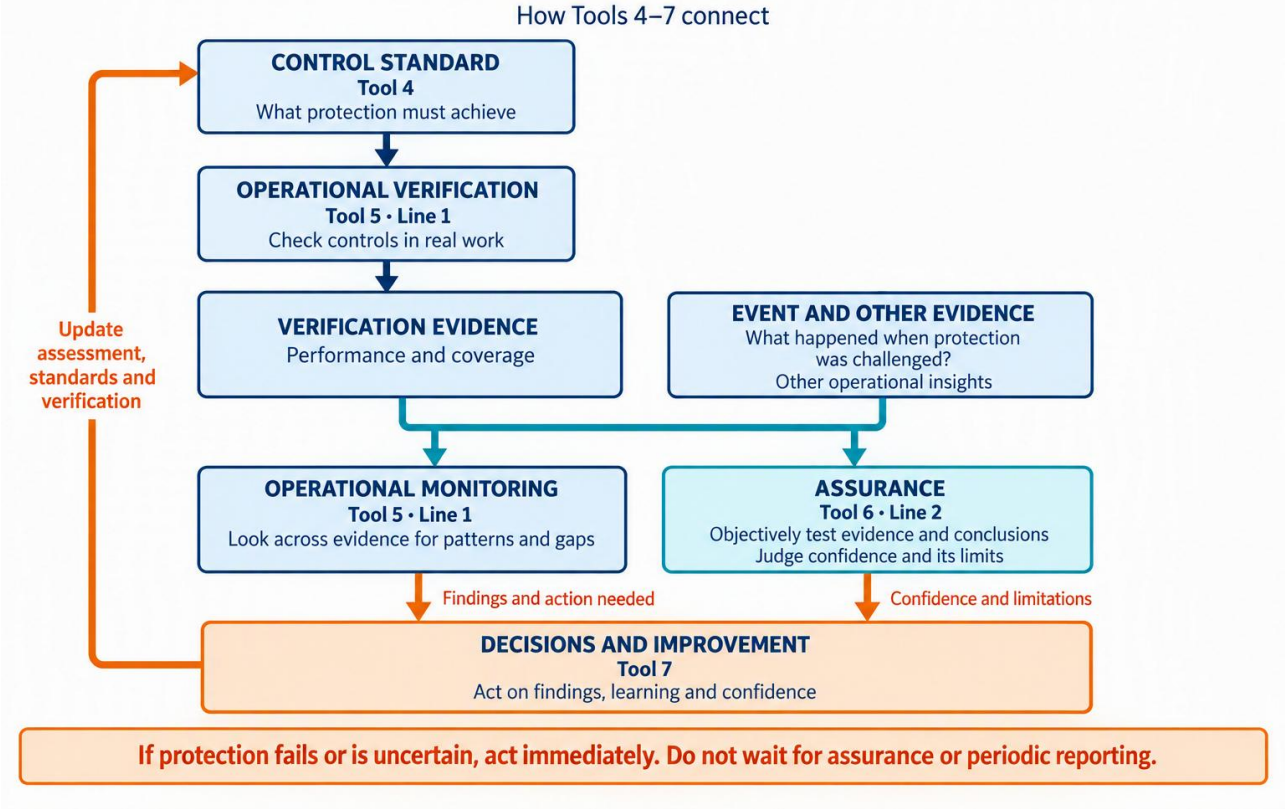
Templates and worked examples: Appendix D. Part A (Tool 4A Critical Control Decision Record) tests each candidate control against the four criteria and records the classification and evidence. Part B (Tool 4B Critical Control Standard) defines the approved performance requirements, verification, ownership, and response, and records conformance and remaining gaps. The worked examples apply both to mobile-plant control CC-02.1.

Use them to record each decision and standard or reference your existing control or engineering records if they already hold this information.

Handoff: Critical controls classified, standards technically approved, actual conformance assessed, and remaining gaps controlled with accountable owners → complete Tool 5.

From control standards to evidence, confidence and decisions

Tools 5–7 build on the critical-control standards established in Tool 4. Operational verification (Tool 5) establishes what was found when protection was checked, and operational leaders monitor those findings alongside wider evidence, including what incidents show about whether controls worked. Assurance (Tool 6) gives a confidence rating of how far that reporting can be relied on. In Tool 7, leaders read both together to make decisions and improve protection.



Restricted Content

Tool 5: Verification and Failure Response Plan

Guide link: *Section 7: objective critical control verification, monitoring and response where protection is absent or ineffective.*

Verification needs to work at two connected levels. The **annual operational verification programme** sets the overall scope, coverage, resources and oversight for a business area (Part A). The **risk/control-specific plans** translate approved critical-control standards into the checks required in real work (Part B).

Operational managers develop both levels with HSW and relevant technical support. The accountable senior operational leader for a business area – including relevant executive leaders - should approve the annual programme and its resources. Managers and supervisors then deliver it through competent, designated verifiers, with technical authorities approving specialist methods where required.

Update the programme and plans when exposure, controls or evidence materially change. Annual planning and approval never delay urgent verification or protective action.

Input (what is required to begin)	Decision (what must be decided)	Output (what must be in place by the end)
Approved critical control standard and known conformance gaps	What evidence will demonstrate performance, and what happens if it fails?	Approved annual programme, linked risk/control-specific plans, and predefined failure response

Part A: Annual Operational Verification Programme

Part A brings the risk/control-specific plans together into one risk-based programme for the business area. Senior operational leaders use it to judge whether planned verification provides sufficient volume, coverage, quality and capability for the actual exposure, and whether the resources needed to deliver it are available. Make any coverage or resource gaps explicit, with owners and escalation.

Template and worked example: Appendix E. T5A provides an adaptable programme record and worked example.

Part B: Risk/Control-Specific Verification and Response

Each risk/control-specific plan translates an approved critical control standard into the checks needed to establish whether the control is present and meeting its performance requirements. Map every check to a defined requirement and specify the method, evidence, competent verifier, frequency, coverage and response for a pass, fail, or cannot verify result.

Verify close to control use through observation, approved testing, or measurement, informed by workers' experience of normal, abnormal, and changing work. Feed practical issues, recurring failures, and changes in operating conditions back into the critical risk assessment, control standard and annual programme.

Key tips and advice:

- Set clear **pass, fail, or cannot verify** criteria.
- Base frequency on exposure, control reliability, consequences, previous failures, and change.
- Test performance against approved requirements – not simply whether checks were completed.
- Prioritise critical controls. Check supporting controls where their failure undermines protection, but do not treat their performance as proof that critical controls work.

Dynamic work – controls established for each task or shift

Where a control must be established for each task, job, or shift, verification operates at two **Line 1** levels:

- **At the work:** before and during the task, confirm that the required control is in place and meeting its performance requirements. Record this in the permit, job, or pre-start system already in use.
- **Across the work:** include a risk-based sample of tasks, shifts, and conditions in the operational verification programme to confirm that protection is being applied consistently across the exposure.

Set coverage by risk, considering task type, site, shift, contractor, consequence, previous findings, and change. Increase it after triggers such as a new task, crew change, high-potential incident, or failed result.

If required protection cannot be confirmed before work starts, the work does not start.

Line 2 assurance remains separate: it tests whether the Line 1 verification evidence and conclusions can be relied on.

Failure response. If a check fails or protection cannot be confirmed, the operational owner restricts the affected work, restores protection or uses an approved, verified alternative, and escalates immediately. Work restarts only after a competent verifier confirms effective protection, with technical authority approval where the design is affected. Due dates and improvement plans never authorise exposure to unprotected work.

Template and worked examples: Appendix E. T5B links each check to an approved requirement and defines the evidence, verifier, timing, coverage and failure response. The examples show the Site A plan and one completed check.

Monitoring Verification Performance and Findings

Operational leaders should look across verification results over time, not simply count completed checks. Review **delivery, coverage, findings and recurring weaknesses**, alongside other relevant evidence such as observations, breaches, incidents and near misses, maintenance records and worker insight.

The illustrations below show two useful examples of Line 1 monitoring performance views. The first shows how an organisation could present control-performance findings and known coverage gaps at a site. The second shows how an organisation could present verification delivery, findings and coverage across a network over time. **Neither is an assurance rating**, and neither establishes acceptable failure levels.

Critical control verification performance

Fictional example | Line 1 | Site A | Month 1

Control	Pass	Fail	Cannot verify	Total	Pass/total	Coverage gap
Physical separation	36	2	2	40	90%	Night delivery
Energy isolation	17	2	1	20	85%	Shutdown work
Machine guarding	20	0	0	20	100%	Night shift
Loading exclusion	7	2	1	10	70%	Contractor arrivals

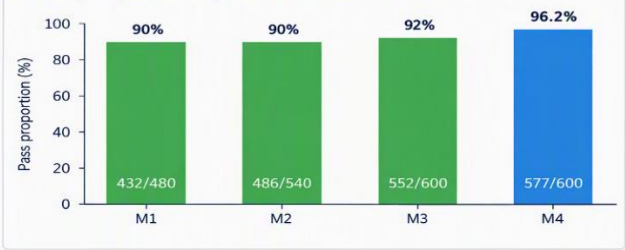
Pass/total colour key: Red <80% | Amber 80–89% | Green 90–94% | Blue ≥95%: validate depth and rigour | Grey: no checks

High results can be genuine. Investigate scope and checking quality; do not assume poor rigour. These bands are not acceptable failure levels. Restrict affected work when protection fails. Assurance confidence is reported separately by Line 2.

Critical control verification trends

Fictional example | Line 1 | 12 sites | Months 1–4





Last month (M4) by site

Metric	Site A	Site B	Site C	Site D	Site E	Site F	Site G	Site H	Site I	Site J	Site K	Site L
Completed checks	50	50	50	50	50	50	50	50	50	50	50	50
Passed checks	48	47	49	46	48	50	45	49	47	50	48	50
Pass proportion	96%	94%	98%	92%	96%	100%	90%	98%	94%	100%	96%	100%

All 12 sites reported; night-shift coverage complete at 10/12 sites.

More checks and higher pass rates do not establish full coverage.
Blue ≥95% prompts checks of depth, coverage and rigour—not automatic confidence. Respond immediately to material failures.

All checks, including cannot verify, remain in the denominator. Site mix and scope held constant. Fictional reporting bands—not acceptable failure limits.

Read unusually high results with care. High pass proportions may be genuine, but they should prompt a check of verification depth, coverage, and evidence quality where other evidence points the other way. Missing conditions, shifts or work types remain coverage gaps even where planned check volumes are achieved.

Tool 6 then provides the separate Line 2 test of whether this evidence and the conclusions drawn from it can be relied upon. Tool 7 brings verification, assurance and incident learning together for enterprise decisions and improvement.

Handoff: Use verification evidence in Tool 6 assurance and Tool 7 Part A reporting; material issues and event learning enter Tool 7 Part B. Verification, response and urgent escalation continue without waiting for assurance.

Restricted Content

Tool 6: Assurance and Confidence

Guide link: *Sections 4 and 7: objective assurance, confidence in control performance, and the quality of operational verification.*

Objective assurance (test and challenge), often called Line 2 assurance, tests how much confidence leaders and governance layers can have the Line 1 verification system, including what it is checking and reporting. HSW, engineering, occupational hygiene, process safety, other technical specialists, or another competent function may provide it. Assurers use risk-based sampling to test whether critical controls are in place and performing as required, whether operational (Line 1) verification appears sound, and whether the Line 1 findings can be relied on. Where practicable, compare Line 2 sample findings with the corresponding Line 1 results to identify material differences in what each is finding. Investigate differences in context, including scope, timing, conditions, methods and sample selection; the size of a difference is a signal for investigation, not by itself a measure of confidence or proof that either result is wrong.

The assurance provider combines evidence across sites and critical risks into a **reasoned, evidence-based confidence judgement**. It is not calculated from verification completion or pass rates, and it explains material differences and gaps rather than averaging grades. It weighs control performance, verification quality, coverage, technical evidence, incident learning (including failed safely and failed lucky), unresolved weaknesses, and uncertainty.

Assessing and explaining confidence

Confidence reflects the evidence for the sites, risks, and period assessed – not a guarantee of safety.

- **High confidence:** Line 1 verification has appropriate coverage, quality, and volume Its findings are consistent with incidents and other relevant evidence, giving high confidence that Line 1 is checking the right things, identifying material weaknesses and reporting an accurate picture.
- **Moderate confidence:** Line 1 verification provides a useful picture, but gaps in coverage, quality or volume, or some differences with other evidence, reduce confidence that it is consistently identifying and reporting material weaknesses.
- **Limited confidence:** Significant weaknesses in Line 1 verification, major coverage or evidence gaps, or conflicts with incidents and other evidence mean there is limited confidence that Line 1 is identifying material weaknesses and reporting an accurate picture.
- **Not assessed:** There is not yet enough assurance evidence to make a confidence judgement about Line 1 verification and reporting.

State the assessment date, scope, limitations, reasons for any change, and findings that would lower the rating. Keep material concerns and coverage gaps visible.

Key tips and advice:

- **Plan coverage by risk, not by formula.** Use consequence, exposure, control reliability, verification quality, change, incident evidence, previous findings, and uncertainty to decide what to assess, where, how deeply, and how often; record the reasoning, but keep it proportionate to the risk.
- **Make coverage gaps visible.** Record deferrals as gaps, not completed assessments, and show their effect on confidence.
- **Use competent, sufficiently objective assurers.** Obtain peer or external (to the team) challenge for controls the assurer helped design or operates.
- **Respond and escalate.** Add focused checks after high-potential incidents, repeated failures or change.

Input (what is required to begin)	Decision (what must be decided)	Output (what must be in place by the end)
Verification results, technical and incident evidence, and the approved assurance programme	How much confidence can be placed in Line 1 verification and reporting, and what limits that confidence?	Reasoned confidence judgement with coverage gaps, limits and required actions

Template and worked example: Appendix F. The Tool 6 template sets out a risk-based assurance programme: scope, review priorities and timing, sampling and evidence, resources and approval, confidence reporting and follow-up. The worked example shows the mobile-plant programme across 12 sites and how the confidence judgement is reached.

Use it to plan and record assurance, or reference your existing audit or assurance planning systems if they already hold this information. Go to **Appendix F**.

The supplementary example below uses energy isolation to show how a confidence judgement is reached and explained. Tool 7 then shows how to communicate that judgement alongside changing performance and required decisions.

Supplementary example – energy isolation: verification trends and assurance confidence

This short supplementary example is separate from the mobile-plant dataset. It shows how Line 1 and Line 2 results, attributed confidence, reasons and a decision can be presented over time. Different samples are signals to investigate, not proof of bias.

Verification trends and assurance confidence

Fictional example | Line 1 and Line 2 | Energy isolation | January–June

Energy isolation during permitted maintenance

Checks meeting isolation performance requirements



Sample size (n)	Jan	Feb	Mar	Apr	May	Jun
Line 1 checks (n)	40	40	40	40	40	40
Line 2 checks (n)	20	20	20	20	20	20

June judgement

Volume and coverage
Moderate, unchanged
Night-shift gaps.

Verification quality
Limited, declining
Recurring record/evidence weaknesses.

L1/L2 alignment
Limited, declining
Investigate scope, timing and missed defects.

Overall confidence
Limited, declining
Material evidence gaps unresolved.

Basis: repeat gaps and weaker L2 findings; night-shift coverage incomplete.

Decision: restore deficient isolations, test verification quality and extend coverage.

Different samples are signals to investigate, not proof of bias. Pass rates are not population estimates or confidence grades. Fictional example only.

Handoff: Carry confidence reported by the identified Line 2 provider, evidence limits and required actions into Tool 7 alongside operational verification results. Routine reports, restrictions and urgent escalation do not wait for a new assurance assessment.

Preprinted Content

Tool 7: Reporting, Learning, and Improvement

Guide link: *Section 9: measurement, reporting, escalation and event learning, with Section 10 informing signals of emerging weakness and drift.*

Tool 7 is where leaders see what Tools 5 and 6 produce and decide what to do about it. Operational leaders report what they are doing, finding and seeing: verification activity and results, patterns and weaknesses, other evidence such as incidents and near misses, and the actions they are taking. The Line 2 function, such as the HSW team, adds its confidence rating of how far that reporting can be relied on, with its reasons, limits and any weak signals. Leaders and governance groups read the two together, ask for further evidence where needed, and decide what must improve. Leaders act on what the combined picture shows, including escalating issues that exceed local authority or resources. Failed or uncertain protection is different: it requires immediate response under Tool 5 and does not wait for periodic reporting.

Operational managers and leaders report their area's verification activities, results, patterns and responses to the next leadership level. The relevant Line 2 confidence rating travels with that report, attributed to the Line 2 function and not altered by Line 1. The Line 2 function brings together the enterprise picture and the Line 2 confidence assessments for operational, executive, and governance groups. These groups set priorities and resources and require evidence that critical risk management is effective and weaknesses are being resolved.

Input (what is required to begin)	Decision (what must be decided)	Output (what must be in place by the end)
Monitored verification results and wider evidence (Tool 5); Line 2 confidence rating and weak signals (Tool 6); uncertainty and recurring patterns	What do the results, and the confidence in them, require us to decide, resource or improve, and who can resolve it?	Decisions with accountable owners, wider learning, and effectiveness checks

Templates and worked examples: Appendix G. Part A (T7A Periodic Performance and Confidence Summary) brings Line 1 performance, coverage, patterns and action effectiveness together with the attributed Line 2 confidence rating, its reasons and limitations, and the decisions required. Part B (T7B Material Issue and Improvement Record) records a material issue, the response, the decision or escalation needed, the owner, and the effectiveness check. The worked examples show the mobile-plant periodic performance and confidence summary and the Site A material-issue record.

Use them to report and record decisions, or reference your existing reporting and action-tracking systems if they already hold this information. Go to **Appendix G**.

Part A: Reporting Performance and Confidence

Part A is one report, not two. Operational leaders report what they are verifying, finding and acting on. The Line 2 confidence rating sits within that report so readers can see how far the findings can be relied on. Line 2 keeps authorship of its rating; Line 1 does not set or edit it.

One report: what Line 1 found, with Line 2's confidence in it	
Line 1 report (Tool 5), owned by operational leaders:	**Line 2 confidence rating (Tool 6), reported by the objective assurance provider:**
• Verification activity, coverage and results • Patterns and weaknesses, including incidents, near misses and failed safely / failed lucky events • Actions taken and whether they worked • Decisions or resources needed	• Rating: **High / Moderate / Limited / Not assessed** • Reasons, limits, and coverage gaps • Relevant Line 2 sample findings and material differences from Line 1 • Systemic patterns and weak signals
How leaders use the report: Where Line 1 findings, relevant Line 2 samples and other evidence broadly align, reliance is stronger. Where they differ materially, investigate why, considering differences in scope, timing, conditions, methods and sample selection. Do not assume that either result is more accurate simply because it is higher or lower, and do not average them into a combined score. The Line 2 confidence rating reflects the assurance provider's judgement across all relevant evidence, not the size of the difference alone.	

Line 2 may also see patterns that Line 1 cannot see from within one area, such as repeated weaknesses across sites or business units or in the quality of verification itself. It shares these with Line 1 and reports them alongside its confidence rating.

More adverse findings being reported after implementing new or better verification or assurance systems may reflect better detection, not necessarily worsening controls or a deterioration in safety. Line 1 and 2 teams should investigate before drawing conclusions, comparing previous and current results only where controls, scope, methods, and working conditions are sufficiently similar. PCBUs should address ineffective protection regardless of the explanation.

Interpreting incident evidence

Assess **high-potential incidents** by their credible potential for serious harm, whether or not harm occurred. Record the controls involved and the evidence supporting the conclusion:

- **Failed safely:** A critical control performed its defined function and prevented serious harm.
- **Failed lucky:** A required critical control was absent or ineffective, and chance prevented serious harm.
- **Not established:** There is insufficient evidence to determine what prevented harm.

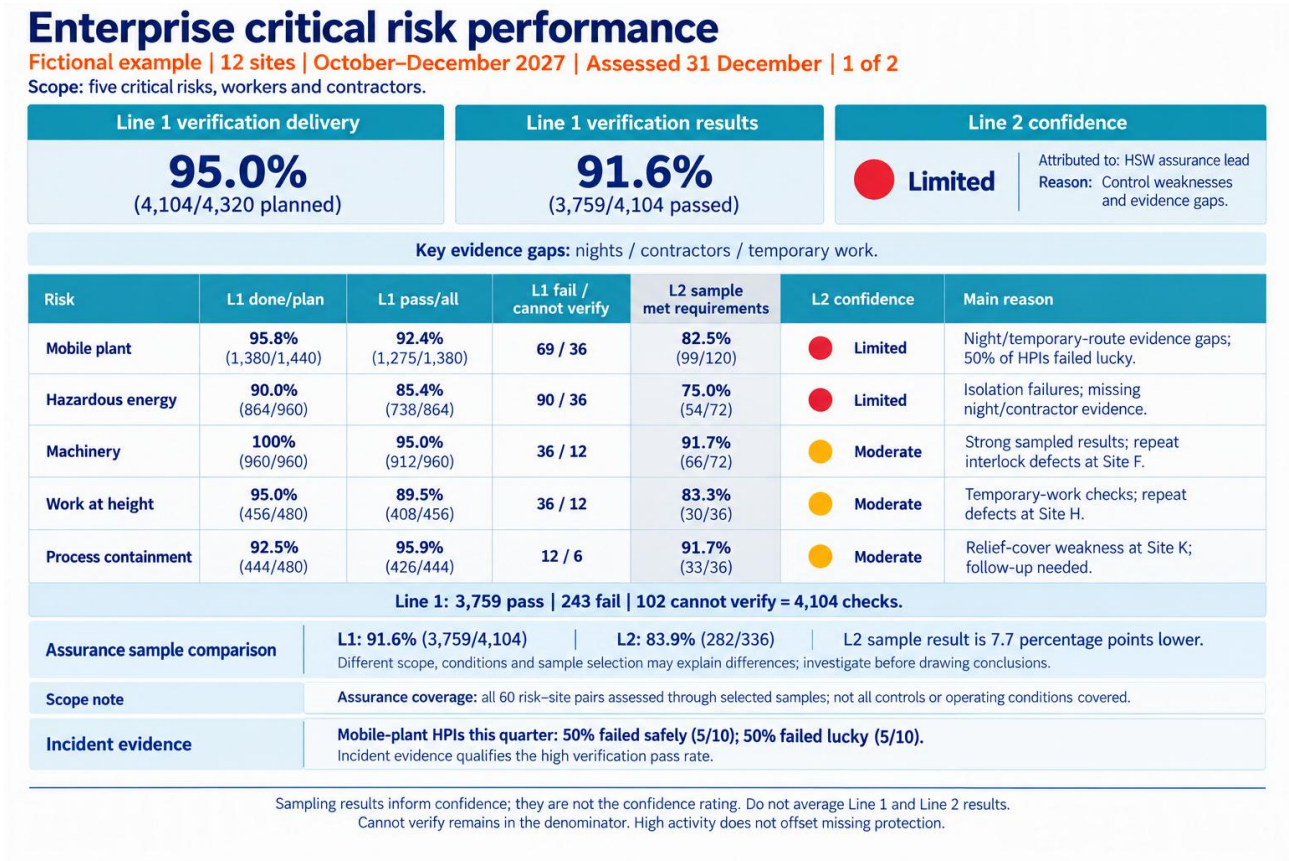
Record actual serious-harm events separately; they are neither failed safely nor failed lucky. The worked examples in Appendix G calculate the failed-safely rate using all reported incidents in scope, including actual serious-harm and not-established cases. Count each event once, but record both failed and effective controls where findings are mixed. Record uncertainty, restored protection and learning. A verification defect alone is not an incident.

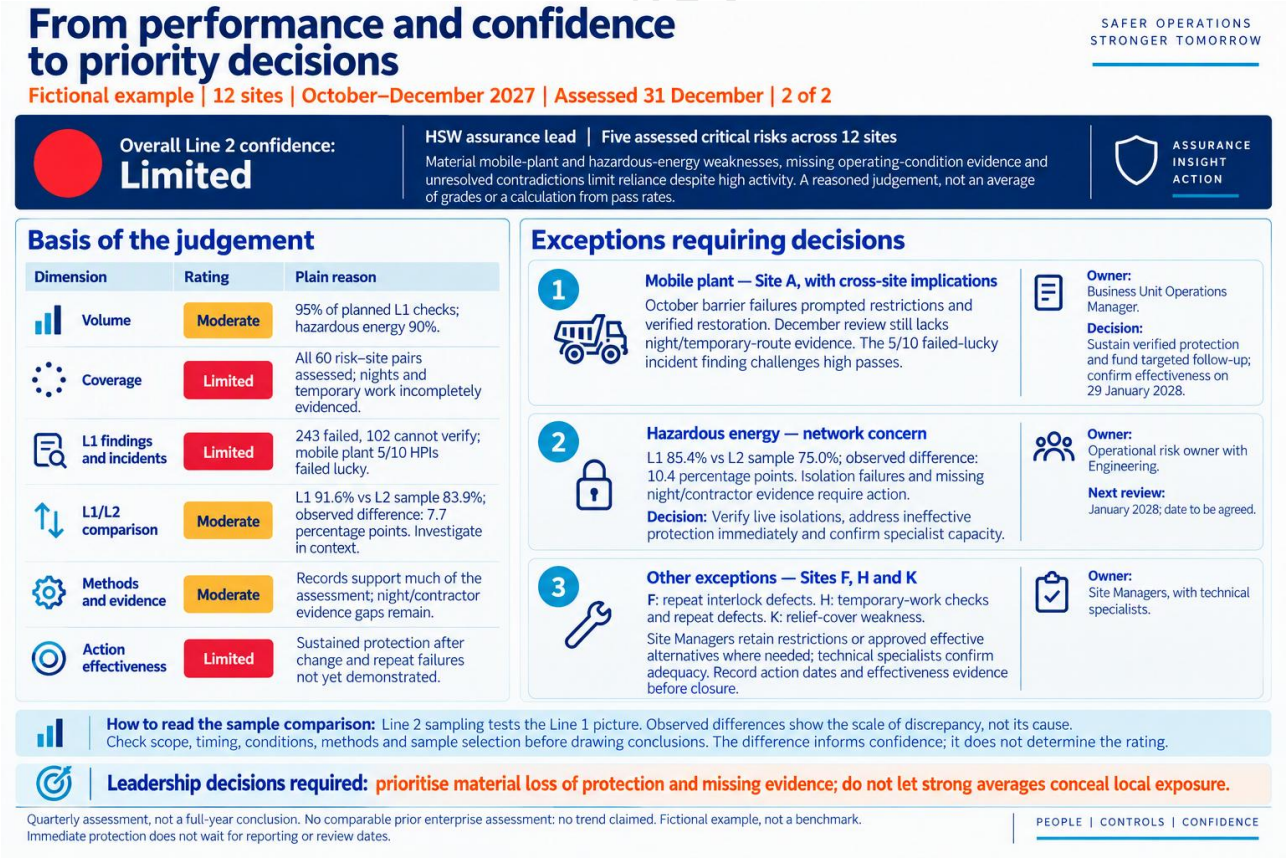
Show incident counts and proportions by critical risk, including cases classified not established. Explain changes in exposure, incident types, classification practices and small samples. Present incident trends separately from verification results, but consider both when assessing control performance and confidence.

Handle failed-safely and failed-lucky proportions with care. They are **descriptive learning measures**, not standalone safety-performance scores, rankings or targets. They are vulnerable to reporting and classification effects – a stronger reporting culture can add events, investigation depth varies, numbers are often small, and “not established” may be used inconsistently. Read them with counts, exposure, event mix and any reporting changes, validate classifications, and do not set targets for them.



The following two illustrations show how operational performance, event learning and Line 2 confidence can be brought together in one report and then used to identify decisions and improvements required.





Part B: Turning Findings into Improvement

Part B turns what Part A shows into action. Where a pattern, weakness, or event needs a decision, resources, or wider improvement, record it, give it an accountable owner, and escalate it if it is beyond local authority.

Key tips and advice:

- Record immediate action already taken; escalate urgent concerns without waiting.
- Escalate major loss of protection, repeated failures, unresolved uncertainty, or resource and deadline constraints that prevent effective protection.
- Close actions only when evidence confirms the intended improvement - not simply completion.

Maintain and Improve the Critical Risk Management System

Guide link: *Section 10: preventing drift, responding to change and recurring weakness, and improving controls and the wider system.*

Review failures, repeated problems, changes, workarounds and declining confidence without waiting for the scheduled review. Drift occurs when protection weakens or safety margins narrow, including through greater reliance on supporting controls or individual judgement.

Use findings and learning to check that the risk profile still reflects actual work and that controls, verification, capability, reporting and assurance remain adequate. Examine assumptions, design, workload and competing pressures with workers, using objective evidence. Assign improvement actions, verify their effectiveness before closure and restrict affected work while protection is uncertain.

Handoff: Use findings and learning to update Tools 1–7 and capability evidence. Recheck readiness before each rollout phase, expansion or material change—not as a final approval after Tool 7.

Restricted Content

Capability Readiness Record

Cross-cutting resource for Tools 1–7

Guide link: *Section 8: role-specific capability demonstrated in practice and reviewed when work, controls or evidence change.*

Capability is a requirement throughout Tools 1–7, not a final step after reporting. Use this record as roles are assigned and before people make CRM decisions, perform verification or provide assurance. People should understand relevant serious-harm pathways, control requirements and how to respond when protection weakens. Confirm capability before decisions or verification through observed practice and, where appropriate, realistic abnormal-work scenarios—not training alone.

Reassess after changes or adverse findings. Leaders provide learning time and constructive support. **Use existing competency, authorisation and training records** as evidence where they show demonstrated practice; record only who confirmed capability, the evidence reference, gaps and reassessment triggers, and use this in implementation readiness decisions.

Where roles are combined, assess each function separately. An HSW title does not establish technical authority, and technical authority does not establish assurance objectivity. Where independent Line 3 review is commissioned, confirm that the reviewer has the competence and independence required for the scope and maintain a reporting route independent of the functions being reviewed.

Input (what is required to begin)	Decision (what must be decided)	Output (what must be in place by the end)
Defined role accountabilities, required CRM capabilities and evidence of demonstrated practice	Can priority roles perform their CRM functions in practice?	Confirmed capability for priority roles, with gaps, actions and reassessment triggers

Template: Appendix H. The *Capability Readiness Record* records the capability required for priority CRM roles, the evidence demonstrating readiness, who confirmed it, and any gaps or actions. Use existing competency, authorisation and training records as evidence rather than recreating them here.

Restricted Content

Implementation Readiness Checklist and Worked Example

Cross-cutting resource for phased implementation

Guide link: *Sections 4 and 7–9. Use this checklist as described under "Readiness Checks for Phased Implementation". Readiness is a decision about whether to proceed with the defined implementation step. It neither proves continuing effectiveness nor authorises individual work.*

Implementation Readiness Criteria

Assessment scope: [phase/sites/risks] · **Proposed next step:** [activity] · **Decision owner/date:** [role/date]. For each criterion record **ready for this phase**, **gap requiring action**, **required later** or **not ready**. For later requirements, record the later phase, owner and trigger/date; do not defer protection needed now.

Keep this short. In the evidence column, point to the existing record (approved framework, programme approval, capability confirmation, test result) rather than repeating it. Complete only the criteria relevant to the next step. If your governance system already records these decisions, use it.

Template: adapt to your organisation – TR Implementation Readiness Assessment

Criterion	Expectation when relevant to this phase	Status	Evidence / gap / action
Enterprise framework	Critical risk criteria, methodology, accountabilities, technical approval rules, records, reporting, assurance and local adaptation requirements are approved and usable.	[ready / gap / later / not ready]	[insert]
Ownership	Operational owners are assigned for risks, controls, verification and improvement.	[ready / gap / later / not ready]	[insert]
Critical risk visibility	Both classification routes are applied without arbitrary exclusions. Workers and contractors inform scenarios/pathways, including shared interfaces and chronic illness, and receive decisions. Assessment findings update register scope, classification and uncertainties.	[ready / gap / later / not ready]	[insert]
Reasonably practicable control strategy and gap closure	Technical/external evidence justifies required protection; gaps have owners for interim protection, improvement, investment and escalation.	[ready / gap / later / not ready]	[insert]
Control clarity	Evidence supports all four designation criteria. Responsibility for design, provision, use, maintenance and verification is clear. Failed critical controls retain their designation, and any reliance on supporting controls alone is explicit.	[ready / gap / later / not ready]	[insert]

Verification readiness	The senior operational leader has approved and resourced the annual programme and linked risk/control plans. Competence, methods, frequency, volume, coverage and evidence quality are demonstrated. Test failure response and authorised, verified restart, including necessary supporting-control failures.	[ready / gap / later / not ready]	[insert]
Capability	Priority roles have demonstrated the capability required for their assigned CRM functions in practice, with gaps, interim arrangements and reassessment triggers recorded.	[ready / gap / later / not ready]	[insert]
Reporting and escalation	Reports show Line 1 verification activity, coverage, findings, patterns, event learning and action effectiveness, alongside the attributed Line 2 confidence rating, reasons and limitations. Relevant Line 2 sample findings and material differences from Line 1 are visible where useful. Decisions, owners and escalation are clear.	[ready / gap / later / not ready]	[insert]
Change management	Changes that could affect risks or controls, whether permanent, temporary or gradual, are assessed before approval. Operational and technical decision rights are clear, and performance is verified after implementation.	[ready / gap / later / not ready]	[insert]
Assurance	A competent, objective Line 2 provider has a risk-based assurance programme addressing applicable critical risks and sites, with sampling depth and timing based on exposure, control reliability, verification quality, change, incidents, findings and uncertainty. Material coverage gaps and their effect on confidence are explicit; triggered reviews respond to emerging evidence. Commissioned Line 3 review remains separate.	[ready / gap / later / not ready]	[insert]
Governance	Executives act on priorities and resources; officers exercise due diligence through evidence and challenge, not positive dashboards or general audit results alone.	[ready / gap / later / not ready]	[insert]
Gap management	Remaining gaps are classified, owned, controlled and escalated.	[ready / gap / later / not ready]	[insert]
Overall readiness decision		[ready / ready with managed gaps / not ready] [decision owner, conditions and review date]	

System readiness does not authorise individual work. Managed gaps require verified protection, owners, conditions and timely review; absent, ineffective or unverified protection blocks affected work. Use competent supervision or restrict activities until capability is demonstrated.

Mobile-plant example — readiness to continue rollout
Phase-specific decision, repeated as implementation and evidence develop—not a final stage after reporting.

This assesses readiness to continue the mobile-plant CRM rollout with managed gaps—not completion of the full control set, continuing effectiveness or permission for individual work.

Worked Implementation Readiness Assessment		
Criterion	**Status**	**Evidence / gap / action**
Enterprise framework	Ready	Enterprise CRM framework approved by the Executive HSW Forum on 30 September 2027, including the method, decision rights and technical approval requirements. Current version published in the enterprise HSW system.
Ownership	Ready	Business Unit Operations Manager and Site Manager accountabilities recorded in the approved CRM framework; local owners confirmed for all 12 sites before rollout. Escalation authority is documented.
Risk and CC-02.1 clarity	Ready	The scenario, CC-02.1 standard and owners are approved. Loading/reversing (P2) records and speed assessment remain outstanding; this is not the full control set.
Reasonably practicable control strategy and gap closure	Gap	Interim separation is verified. The Engineering Technical Authority completes the P2 decision and standard and speed assessment by 30 November 2027. Do not rely on speed limitation until validated. Site Managers retain verified loading exclusion or restrict work.
Verification	Gap	Control-specific plans are in use. Confirm the annual programme's approval, resources and consistent change-triggered checks across all sites by 15 December 2027. Add night-delivery checks by 7 November; review Site A effectiveness on 8 November 2027.
Capability	Gap	Capability Readiness Record confirms demonstrated practice for priority roles at 10 of 12 sites. Practical demonstrations remain outstanding at two sites, due by 30 November 2027. Until then, competent personnel perform or directly supervise those functions. Briefing alone does not demonstrate capability.
Reporting and escalation	Ready	Quarterly performance and confidence reporting format approved for business-unit leadership, showing Line 1 findings with the attributed Line 2 confidence rating. Immediate failure escalation route is documented and has been briefed to Site Managers.
Governance	Ready	Executive HSW Forum and business-unit leadership reporting routes are recorded in the approved CRM framework. Decision rights and escalation routes are confirmed, including executive decisions on priorities and resources.
Change management	Gap	Roles and triggers are defined. By 15 December 2027, test all sites' approval before planned removals or layout changes and verification afterwards, plus immediate assessment and re-verification after impacts.

Assurance	Ready	HSW assurance lead appointed and Q1 mobile-plant assurance review completed on 31 October 2027, testing scope, methods and reporting and identifying coverage gaps. Follow-up scheduled for 29 January 2028. This demonstrates assurance capability for the assessed scope, not high confidence in all work.
Gap management	Ready	Open rollout gaps are recorded in the business-unit action tracker with accountable owners, due dates and temporary protection. Site Managers review immediate protection weekly; overdue or unresolved protection gaps escalate to the Business Unit Operations Manager.
Overall decision		**Ready with managed gaps - Business Unit Senior Leader, 31 October 2027.** Continue rollout, not unprotected work. Verify protection, including P2 exclusion, before work starts or continues. Maintain temporary controls and weekly review; meet deadlines and escalate breaches immediately. Review night coverage on 8 November and remaining conditions on 15 December 2027.

Restricted Content

Appendix A: Tool 1 – Enterprise CRM Framework and Operating Model Record

Guide link: Section 4, with enterprise requirements supporting Sections 5–9.

This record is the enterprise-level companion to Tool 1. Complete it once for the organisation, and review it when the mandate, structure, critical risk profile or technical authorities change. Where a row is already covered by an existing document, enter a reference rather than repeating the content. The template is an adaptable example, not a mandatory form.

Template: adapt to your organisation – T1 Enterprise CRM Framework and Operating Model Record	
Mandate, scope and approval	[enterprise mandate, scope, sponsor, approval forum, pace and resources]
Critical risk definition and methodology	[definition, inclusion threshold, assessment method, required evidence and review triggers]
Accountabilities and technical decision rights	[owner of the CRM framework (HSW or equivalent Line 2 function); operational owner of each critical risk and control; programme approval and resourcing; technical approval including alternative protection; restart authority; who provides support and objective assurance, with self-review safeguards; escalation routes, including across business units or PCBUs. Reference existing delegation documents.]
Records and systems (use what exists)	[existing systems holding each record, owners, and how they link by risk/control ID. Define new records only where none meets the intent.]
Local adaptation and change control	[what may be adapted locally; what changes to risks, controls, standards or operating arrangements require technical, operational or enterprise approval; and how framework updates are governed]
Business integration and shared duties	[link business decision gates. Agree responsibilities across PCBUs for control provision, use, maintenance, verification, change communication and escalation. Consult, cooperate and coordinate; allocation does not transfer legal duties.]
Governance information and decisions	[Identify governance forums, reporting frequency, evidence, escalation routes and decisions. Officers need evidence of priorities, defined and resourced controls, reliable verification and sustained improvement – not activity counts, audit results or green dashboards alone. See Guide Section 4 and its governance-guide reference.]

Appendix B: Tool 2 – Critical Risk Register Template and Worked Example

Use this template to record each serious-harm scenario, its classification basis, owner and next action. Adapt it to your organisation, or reference your existing risk register where it already holds this information.

The worked example follows the primary mobile-plant scenario (CR-02) across the fictional 12-site network. All figures and dates are fictional; validate all detail against actual work.

Template: adapt to your organisation – T2 Critical Risk Register Entry	
Critical risk ID	[insert]
1. Define the serious-harm scenario	
Serious-harm scenario	[describe hazard → how exposure occurs → person affected → serious outcome, including repeated/prolonged exposure; see Guide Appendix A]
Credible consequence	[insert]
Critical risk classification basis	[record consideration of both classification routes: Schedule 1A applicability and the serious-outcome route; identify the applicable route(s), specific criterion, supporting evidence and rationale under Guide Section 2, including Schedule 2 of the Accident Compensation Act 2001 for listed disease. Assess consequence, not frequency]
Where exposure exists	[sites, tasks, people, shifts, assets, operating conditions and contractor/shared-PCBU interfaces; record scope uncertainties for Tool 3]
2. Confirm the basis and ownership	
Evidence, contributors, and decisions	[sources, technical evidence, contributors, issues, decisions and unresolved concerns; how decisions were communicated]
Operational owner	[insert]
3. Maintain and progress the entry	
Status / next action	[classification/assessment status, uncertainty, next action, owner and date; update from Tool 3 findings]
Review trigger	[insert]

Mobile plant example - progress
[REGISTER] → Assessment → Critical control decision → Standard → Verification → Assurance → Reporting and learning

Worked Example

Primary example (Tools 2–7): mobile plant, CR-02, in a fictional 12-site distribution network. Baseline 1 October 2027; review 31 October 2027; 90-day follow-up 29 January 2028. Illustrative only; not technical or legal validation.

Illustrative worked example – Critical Risk Register Entry (primary example: mobile plant)	
Critical risk ID	CR-02
1. Define the serious-harm scenario	
Serious-harm scenario	Person struck or crushed by moving mobile plant during vehicle movements, loading or unloading.
Credible consequence	Fatality, life-altering crush injury or amputation.
Critical risk classification basis	Critical under the serious-outcome route: a loaded forklift striking/crushing a pedestrian is likely to cause fatal or notifiable injury, regardless of frequency or current controls. Both routes were considered; inclusion does not depend on an unverified Schedule 1A reference.
Where exposure exists	All 12 sites: yards, docks, warehouses and contractor delivery areas, especially reversing, peak movements, maintenance, non-routine work and temporary routes.
2. Confirm the basis and ownership	
Evidence / source	Site walk-throughs and worker input; vehicle–pedestrian near miss reports; contractor interface review; traffic management assurance findings; relevant industry serious event learning.
Operational owner	The Business Unit Operations Manager owns the risk and implementation across the enterprise. Site Managers own local protection, supported by Logistics and Engineering.
3. Maintain and progress the entry	
Status / next action	Identified at all 12 sites; detailed assessment pending. HSW facilitates Tool 3, Engineering assesses options, and operational and contractor representatives test practicality. The Business Unit Operations Manager approves priorities after technical validation. Findings update this entry.
Review trigger	Review after changes to traffic, loading, plant or contractors; failed verification; serious or high-potential events involving inadequate protection; assurance findings; or weakened or bypassed separation.

Sample content

Appendix C: Tool 3 – Critical Risk Assessment Template and Worked Example

Use this template to assess each serious-harm scenario from Tool 2: how harm could occur, the protection required, current controls, gaps and improvement actions. Adapt it, or reference your existing risk assessment if it already holds this information. The worked example assesses the mobile-plant scenario (CR-02). All figures and dates are fictional.

Template: adapt to your organisation – T3 Critical Risk Assessment Worksheet	
1. Define the scenario and exposure pathways	
Serious-harm scenario	[carry forward Tool 2 ID, scenario and classification; update the register and recheck both classification routes where findings change the scenario, scope, or classification]
Causes and exposure pathways	[identify how each pathway develops and link controls to it]
Required protection (before looking at current controls)	[state the protection each pathway requires to prevent serious harm, drawing on law, standards, technical practice and event learning]
2. Map the controls relied upon	
Existing preventive controls	[map controls to pathways, stating function, deployment, evidence and dependencies]
Mitigative / emergency controls	[map consequence-reduction measures to pathways. Preventive/mitigative is function; critical/supporting is designation. Response measures are not automatically critical.]
3. Determine the reasonably practicable control strategy	
Reasonably practicable control strategy and evidence	[Describe the control combination and evidence that it provides sufficient protection, including candidate critical controls' capacity, abnormal conditions, foreseeable failures and dependencies. Reference relevant law, codes, guidance, standards and specialist validation. Record input from users, maintainers, workers and contractors, and how decisions were communicated.]
Higher-order options not adopted and decision rationale	[Record options, availability and suitability, evidence for non-adoption, any gross-disproportion assessment, approval, remaining protection and uncertainty, and review trigger. Recording a decision does not prove adequacy.]
Candidate critical controls for Tool 4	[existing or proposed controls for assessment against Tool 4's four criteria; include controls whose capacity or other designation criteria still require evidence. Do not designate them critical here.]
4. Compare current and required states and plan gap closure	
Current-state gaps, vulnerabilities and uncertainty	[record absent, weak, variable or unproven controls and relevant dependencies or evidence gaps]

Interim protection, actions, owner, due date and escalation	[state immediate restrictions or alternative protection, improvement or investment action, accountable role, date and escalation route]

Mobile plant example - progress
Register → **[ASSESSMENT]** → Critical control decision → Standard → Verification → Assurance → Reporting and learning

Worked Example

This example assesses Tool 2's mobile-plant scenario, refining its pathways without changing its classification. Findings update the register. Validate all detail against actual work.

Illustrative worked example – Critical Risk Assessment (primary example: mobile plant)	
1. Define the scenario and exposure pathways	
Serious-harm scenario	Person struck or crushed by moving mobile plant during vehicle movements, loading, or unloading.
Causes and exposure pathways	**P1 - Shared routes:** pedestrians enter vehicle operating areas or uncontrolled crossings. **P2 - Loading/reversing:** restricted visibility, obstructed sightlines and unfamiliar contractor routes expose people. **P3 - Changed protection:** barrier impact/removal, open gates or temporary routes create access to moving plant.
Required protection	**P1:** continuous engineered separation of people and plant, with controlled crossings. **P2:** physical exclusion of people during loading and reversing. **P3:** separation maintained through damage, removal and temporary change.
2. Map the controls relied upon	
Existing preventive controls	**P1:** Barriers at four sites and designated crossings, supported by markings and warnings. **P2:** Loading exclusion at designated bays, one-way routes and installed speed limiters. Cameras, warnings, instructions rely on human response. **P3:** Gate controls, supported by change approval, defect reporting and pre-start checks. Gaps are listed below; Tool 4 determines which controls qualify as critical.
Mitigative / emergency controls	**P1–P3:** First aid, communications, coordination and emergency access support response; they do not prevent contact. Before classifying emergency stops as critical, assess their response time, performance and reliance on people.
3. Determine the reasonably practicable control strategy	
Reasonably practicable control strategy and evidence	**P1:** Continuous engineered separation and controlled crossings. **P2:** Physical exclusion during loading and reversing; assess additional speed limitation. **P3:** Maintain fixed barriers and controlled crossings. Before removal or route changes, install and verify an engineering-approved equivalent; repair damage before exposure resumes. Engineering review and operator/contractor workshops support the strategy; human-dependent warnings remain supporting controls. MP-DB-01 sets operating limits and local validation requirements.
Higher-order options not	Trials and supplier review found automatic braking incompatible with the mixed fleet and unreliable at screened cross-aisles (MP-OD-02). Engineering rejected

adopted and decision rationale	network-wide use on suitability, not cost. The Business Unit Operations Manager approved separation, crossings and loading exclusion. Keep compatible local applications and alternatives under review; reassess after fleet/layout changes or newly validated technology. Do not rely on the rejected system; maintain verified protection while considering alternatives.
Candidate critical controls for Tool 4	**Separation/crossings:** CC-02.1 covers P1/P3 only. **Loading exclusion (P2):** Complete a separate Tool 4 decision and standard, with a linked Tool 5 verification plan. **Pending assessment:** Engineering assesses speed limitation; do not count it as protection until validated. Site Managers maintain verified loading exclusion or restrict affected work while actions remain outstanding.
4. Compare current and required states and plan gap closure	
Current-state gaps, vulnerabilities and uncertainty	Across 12 sites: eight lack barrier sections (P1); three have gates left open and five lack evidence of temporary-route reviews (P3); four lack evidence that contractors understand routes and two have incomplete alarm-maintenance evidence (P2). Sites may appear in several groups. Speed limitation is not yet validated and cannot count as protection.
Interim protection, actions, owner, due date and escalation	**Immediate protection - from** 1 October 2027**:** Site Managers restrict affected work until equivalent separation is verified, maintain verified loading exclusion (P2), and authorise restart only after verification. **Delivery and oversight:** The Business Unit Operations Manager owns delivery, capital escalation and weekly evidence review. **Site deadlines - 2027:** Engineering: barriers by **30 November**. Logistics: gates/routes by **31 October**. Maintenance: alarm evidence by **15 October**. **Technical approval:** The Engineering Technical Authority approves designs and alternatives, and completes the P2 decision and standard and speed-limitation assessment by **30 November 2027**.

Restricted Content

Appendix D: Tool 4 – Critical Control Decision and Standard Templates and Worked Examples

Use these templates to decide whether each candidate control is critical (T4A), then to define its approved standard, verification, ownership and response, and record conformance and remaining gaps (T4B). Adapt them, or reference your existing control or engineering records if they already hold this information. The worked examples apply both templates to the mobile-plant control CC-02.1. All figures and dates are fictional.

T4A: Complete one record for each candidate control. Designate a control critical only where all four criteria are supported by evidence

Template: adapt to your organisation – T4A Critical Control Decision Record	
Candidate control assessed	[insert]
Acts directly on the hazard or exposure pathway?	[yes / no - evidence and rationale]
Sufficient capacity to prevent the defined exposure from causing serious harm?	[yes / no - evidence and rationale]
Designed to keep protecting people despite mistakes, forgetting or loss of attention?	[yes / no - evidence and rationale]
Performance can be defined and objectively verified?	[yes / no - evidence and rationale]
Classification and rationale	[record classification and evidence against all four criteria, with further assessment or redesign where needed. Explain any reliance on supporting controls alone, its limitations, improvement and leadership visibility. Never downgrade a critical control because it has failed.]
Supporting control requirements	[if supporting: required status, purpose, owner, performance requirements, checks, and failure response. Where protection depends solely on supporting controls, record the limitations, required improvement and leadership visibility.]

Approve the performance standard before writing verification questions. **Make each requirement observable or measurable** – what a verifier would see, test or measure, against what limit or reference – so two competent verifiers reach the same result. “Barriers are adequate” is generic; “every section is anchored with all fixings present and within design-basis limits, with no pedestrian access gap” is verifiable. Carry gaps, interim protection and escalation needs into Tool 5.

T4B: Complete this for each confirmed critical control. Map every check to a requirement, then record conformance and any remaining gaps.

Template: adapt to your organisation – T4B Critical Control Standard	
1. Link and define the control	
Critical risk / serious-harm scenario	[risk ID, serious-harm scenario and pathways addressed]
Critical control	[write the control in practical, observable terms]
Control purpose	[define the protective function, e.g. preventing lane entry or release; one function suffices, but all four designation criteria apply]
Where it applies	[sites, tasks, assets, conditions and interfaces]
2. Define what effective performance looks like	
Technical basis / design validation	[evidence/approval that control meets all four critical control criteria. Define exposure, demands, operating envelope, abnormal conditions, failures and dependencies. see Guide Appendix B.]
Performance requirements	[observable or measurable requirements R1, R2…: what is seen, tested or measured, against which limit or reference. Retain these requirement codes in Tool 5 and map every verification check to them.]
Verification method	[observation, test, measurement, system check or inspection]
Verification frequency	[before work / during work / scheduled / event-triggered / risk-based]
Evidence required	[what must be observed, recorded, tested or measured]
3. Assign accountability and response	
Operational owner	[accountable owner; provision, use, maintenance and verification roles; authority to approve restoration or alternatives; responsibilities shared across PCBUs]
Technical authority / approver	[insert role]
Response if not effective	[stop, modify, restore, escalate or use approved alternative effective control]
Change assessment	[assess permanent, temporary or gradual changes to exposure, controls, interfaces, roles or resources before approval.]
Review trigger	[change, failure, event, assurance finding, technical update or repeated verification issue]
Control Conformance and Remaining Gap Record	
Conformance with approved standard	[record whether the control is present and conforms, fails or cannot be verified, with evidence and uncertainty. Assess design adequacy separately. Retain critical designation and assign restrictions, restoration and verified restart.]
Remaining gaps, interim protection	[record absent, degraded, variable or unverified requirements and any immediate restriction or effective alternative protection]
Action, investment, owner, escalation	[record corrective action or investment, accountable role, due date, escalation route and evidence required for closure]

Mobile plant example - progress
Register → Assessment → **[CRITICAL CONTROL DECISION] → [STANDARD]** → Verification → Assurance → Reporting and learning

Worked Example

This example covers one Site A control (CC-02.1), not the full control set. Loading/reversing protection (P2) needs separate records; speed limitation cannot count as protection until assessed. The acceptance schedule tracks outstanding installations across the 12 sites.

Illustrative worked example – Critical Control Classification (primary example)	
Control assessed	CC-02.1: engineered fixed barriers and controlled crossings separating pedestrian routes from mobile plant areas.
Acts directly on the hazard or exposure pathway?	**Yes.** Barriers prevent pedestrian access through P1/P3 pathways. Controlled crossings prevent conflicting pedestrian and vehicle movements at permitted openings.
Sufficient capacity to prevent the defined exposure from causing serious harm?	**Yes.** The approved design basis (MP-DB-01) validates capacity, anchoring, foundations and geometry against defined vehicle demands to prevent serious-harm contact. Crossings prevent conflicting movement. Appearance alone does not prove capacity.
Designed to keep protecting people despite mistakes, forgetting or loss of attention?	**Yes.** Barriers protect despite distraction or defined route deviations. Crossings prevent conflicting access without relying on instructions, and gate failure blocks access. Damage or removal requires restrictions and competent assessment before restoration.
Performance can be defined and objectively verified?	**Yes.** Design and installation-acceptance evidence confirm capacity. Inspections check dimensions, fixings, continuity and condition; approved tests check crossings and failure behaviour. Requirements R1–R4 link to checks V1–V4.
Classification and rationale	**Critical - CC-02.1.** Evidence supports all four criteria. Engineering approved MP-DB-01; the Business Unit Operations Manager endorsed network use. Each installation must also meet the approved design. Damage is a control failure, not grounds for reclassification.

Illustrative worked example – Critical Control Standard (primary example)	
1. Link and define the control	
Critical risk / serious-harm scenario	Person struck or crushed by mobile plant during movement, loading or unloading.
Critical control	CC-02.1: continuous fixed barriers separate pedestrian routes from mobile plant areas; controlled crossings prevent conflicting movement at access points.
Control purpose	Prevent pedestrian entry into mobile plant operating areas.
Where it applies	Warehouse aisles, loading docks, dispatch yards and contractor delivery interfaces where pedestrian routes adjoin mobile plant areas.
2. Define what effective performance looks like	

Technical basis and design validation	The approved design basis (MP-DB-01) defines vehicle demands, geometry, foundations, capacity and fail-safe crossings. The acceptance schedule (MP-AC-01) tracks accepted and outstanding installations across 12 sites; Site A's record (A-01) confirms conformance. Operator and contractor input shaped delivery access. Routine checks do not validate design.
Performance requirements	**R1:** Barriers are continuous, securely anchored and free of pedestrian access gaps, meeting MP-DB-01 vehicle-contact demands. **R2:** Controlled crossings prevent simultaneous conflicting movements. **R3:** Gate/control failure leaves access unavailable. **R4:** Temporary removal requires an approved, verified equivalent separation arrangement. The validated design maintains protection under defined distraction and route-deviation scenarios.
Verification method	Confirm MP-DB-01 installation acceptance, then follow Tool 5: **V1 → R1:** Inspect continuity, anchoring and condition. **V2 → R2:** Apply the approved safe crossing test. **V3 → R3:** Competent technical verifier conducts the controlled failure test. **V4 → R4:** Check approval, field separation and restart evidence before exposure. Suspected damage requires restrictions and competent assessment, not informal capacity testing.
Verification frequency	**V1:** Each shift; monthly documented inspection. **V2:** Pre-start and scheduled approved tests. **V3:** Approved interval; after relevant maintenance/change. **V4:** Every removal, before exposure. Re-verify after impact, failure, change or relevant events; use approved technical intervals and Tool 5.
Evidence required	Record each R/V result with location, conditions and date: V1 installation/inspection; V2 crossing tests; V3 failure tests; V4 approval, equivalent separation and restart. Retain defect, restriction and restoration evidence and photographs. Tool 5 assigns verifiers.
3. Assign accountability and response	
Operational owner	Site Managers**:** Own protection and authorise verified restart. Logistics**:** Provides and applies controls; Site A Logistics coordinates deliveries. Maintenance**:** Maintains controls. **Designated** supervisors**:** Verify performance. Business Unit Operations Manager**:** Owns rollout. Engineering**:** Approves requirements and restoration. **Delivery PCBU:** Is responsible for complying with access requirements.
Technical standard authority / approver	Engineering technical authority approves the barrier standard and any equivalent control; HSW provides CRM method challenge.
Response if not effective	Stop pedestrian access or plant movement. Restore the barrier or install an approved equivalent before resuming work. Escalate repeated, systemic or resource-dependent failures.
Changes requiring assessment and approval	Layout, barrier, plant, loading, temporary-route or contractor-interface changes require Site Manager assessment and Engineering technical-authority approval before implementation, then re-verification before normal work.
Review trigger	Review after traffic or plant changes; impact, failure or unauthorised removal; failed verification; an event where chance - not effective protection - prevented serious harm; repeated gate defects; assurance findings; or updated engineering requirements.

Illustrative worked example – one requirement from protective function to Tool 5 verification (CC-02.1)			
1 Protective function	**2 Performance requirement**	**3 Evidence it is met**	**4 Tool 5 verification**
Prevent pedestrians entering mobile plant operating areas, even if someone is distracted or takes a shortcut.	**R1:** Every barrier section is continuous (no pedestrian access opening), anchored with all fixings present and undamaged, within MP-DB-01 limits.	MP-DB-01 design validation; installation acceptance record A-01; inspection checklist with photos of defects.	**V1 → R1:** inspect each section each shift; documented monthly inspection (see the complete check in Tool 5).
Keep access unavailable if a gate or control fails.	**R3:** On loss of power, signal or control, the gate defaults to closed and access-blocking.	Fail-safe design specification; controlled failure test recorded by a competent engineering verifier.	**V3 → R3:** controlled failure test at the approved interval and after relevant maintenance or change.

Restricted Content

Appendix E: Tool 5 – Verification Programme and Verification Plan Templates and Worked Examples

Use these templates to set the annual operational verification programme for a business area (T5A), then to define the checks and failure response for each risk and control (T5B). Adapt them, or reference your existing verification and maintenance systems if they already hold this information. The worked examples follow the mobile-plant programme across 12 sites, the Site A plan for CC-02.1, and one complete verification check. All figures and dates are fictional.

Part A: Annual Operational Verification Programme

T5A: *Complete one programme for each business area each year. It needs senior operational approval and resourcing; annual approval never delays urgent checks.*

Template: adapt to your organisation – T5A Annual Operational Verification Programme	
Scope and ownership	[business area, year, sites, risk/control IDs, programme reference/version and operational managers responsible for delivery; record exclusions and unresolved gaps]
Schedule and volume	[for each risk/control stream: linked detailed plan, responsible manager, frequency/trigger, monthly or quarterly expected checks and exposure-based rationale; distinguish routine, specialist and triggered checks]
Coverage and quality	[sites, shifts, tasks, assets, contractors, abnormal/temporary work; sampling basis, approved methods, competent verifiers, evidence requirements and quality-review arrangements; no target pass rate]
Resources and support	[verifier time, specialist capacity, training, systems and funding; confirm availability, technical approvals and HSW support; assign any shortfall an owner, deadline and escalation]
Review and response	[local and senior review frequency; expected versus completed checks, coverage gaps, evidence quality, findings and action effectiveness; immediate failure response and escalation; updates after change, failure or new evidence]
Annual approval	[accountable senior operational leader, date, decision and review date; confirm scope, volumes, coverage, quality, capacity and resources against exposure.]

Worked Example: Annual Verification Programme

This extract follows the primary mobile-plant example across 12 sites. It shows an approved annual operational verification programme, not completed verification results. Other critical risks would have their own streams using the same pattern.

Illustrative worked example – Annual Operational Verification Programme (primary example: mobile plant)	
Scope and ownership	**Area:** Distribution Centres – 12 sites. **Period:** October 2027 – September 2028. **Owners:** Site Managers submit local schedules; Logistics and Maintenance Managers lead their verification activities. **Scope shown:** Mobile plant (CR-02). Other applicable critical risks follow the same pattern in their own streams.
Schedule and volume	**Mobile plant – Logistics Managers:** Check active routes each shift and every barrier section and crossing monthly across all 12 sites. Linked CC-02.1 plans also require pre-start crossing checks, approved specialist tests, checks before temporary removal and re-verification after impact, failure or change. Maintain verified P2 loading exclusion; do not rely on speed limitation until validated. Site Managers submitted numeric local volumes and linked detailed plans for approval on 15 December 2027, based on routes, assets, shifts and work orders. Approved specialist intervals are used rather than arbitrary quotas.
Coverage and quality	Cover all sites, shifts, tasks and asset groups, including night deliveries, shutdowns, temporary routes and contractors. Competent designated verifiers use approved methods and record **pass, fail or cannot verify**, with evidence against each requirement. Managers review evidence quality monthly with Engineering/HSW support. **No pass-rate target.** Line 2 assurance remains separate.
Resources and support	**Site Managers:** Confirm competent verifier hours, relief cover, engineering tests and system costs. **Engineering:** Approves specialist methods. **HSW:** Supports planning. **Resources confirmed:** Routine verifier capacity and approved specialist testing are resourced. Night coverage and specialist-capacity shortfalls remain recorded actions with owners and escalation to the Business Unit Operations Manager; they do not permit unprotected work.
Review and response	**Immediately:** Supervisors restrict affected access or movement after failed or cannot verify results. Restore protection or an approved effective alternative; a competent verifier confirms performance and the Site Manager authorises restart. **Weekly:** Site Managers compare expected and completed checks and address coverage gaps. **Monthly:** The Business Unit Operations Manager reviews delivery, coverage, evidence quality, findings and action effectiveness. **Update/escalate:** Revise schedules after change, failure or new evidence; escalate urgent failures and unresolved capacity gaps immediately.
Annual approval	Approved by the Business Unit Operations Manager on 15 December 2027 for the October 2027 - September 2028 programme, subject to the recorded coverage and capacity actions. Resources confirmed for routine verification and approved specialist testing. Night coverage and specialist-capacity gaps remain recorded actions and do not

	permit unprotected work. Programme review scheduled following the 29 January 2028 assurance follow-up, with earlier review after material change, failure or new evidence.

Restricted Content

Content

Part B: Risk/Control-Specific Verification and Response

T5B: Complete one plan for each risk and control. Map every check to an approved requirement and record pass, fail or cannot verify.

Template: adapt to your organisation – T5B Risk/Control-Specific Verification and Response Plan	
1. Link verification to the control standard	
Critical risk	[scenario, pathways, risk/control IDs; business area, annual programme reference, operational plan owner and approval]
Critical control requirements	**R1:** [one observable or measurable requirement] **R2:** [next requirement] **R3:** [continue as needed; retain these codes in the approved standard]
2. Define the verification	
Verification question / method	**V1 → R1:** [question, method and pass/fail/cannot verify criteria] **V2 → R2:** [separate question and method] **V3 → R3:** [continue; map every requirement and split checks where methods differ]
Evidence required	[record results and objective evidence against each R/V code, with location, conditions, defects and response]
Verifier	[competent role for each V code]
Frequency / trigger	[timing for each V code: before/during work, scheduled, event or change triggered]
Coverage and sampling basis	[for controls established for each task/shift, state what must be confirmed at the work and where that evidence is recorded. For programme verification, compare expected and completed checks and show risk-based coverage by site, shift, task, asset, contractor and operating condition, with gaps and response.]
3. Respond and review	
Failure response and escalation	[immediate restrictions, restoration/verified alternative, restart authority and escalation thresholds]
Review owners and frequency	[local manager and senior programme approver; review frequency for delivery against the annual programme, volume, coverage, evidence quality, findings, recurrence and action effectiveness; decisions, updates and escalation]

Operational response: Do not start or continue work where required critical protection is absent, ineffective, or unverified, including failure of necessary supporting controls. Restore required protection or authorise and verify an effective alternative before restart. Record evidence, verifier, restart authority and conditions; plans or due dates never authorise exposure.

Do not proceed unless effective protection is verified. A failed or cannot verify result requires the predefined operational response.

Mobile plant example - progress
Register → Assessment → Critical control decision → Standard → **[VERIFICATION]** → Assurance → Reporting and learning

Worked Example

This Site A plan sits within the business-area annual programme; it is not the programme itself. Each approved requirement has a separate check. Preserve differences in method, timing and competence in the plan and results.

Illustrative worked example – Control-Specific Verification and Response Plan (primary example)	
1. Link verification to the control standard	
Critical risk	CR-02**, Site A:** Person struck or crushed by mobile plant during movement, loading or unloading. **CC-02.1** addresses separation and crossings for **P1/P3**, not the full scenario. **Area:** Distribution Centres, Site A. **Programme:** October 2027–September 2028 approved 15 December 2027. **Plan owner:** Logistics Manager. **Local approver/date:** Site Manager, 15 December 2027.
Critical control requirements	**R1:** Barriers are continuous, anchored and free of pedestrian access gaps, meeting MP-DB-01 design limits. **R2:** Controlled crossings prevent conflicting movements. **R3:** Gate/control failure blocks access. **R4:** Before temporary removal, approve and verify equivalent separation. The validated design protects against foreseeable distraction and route deviation.
2. Define the verification	
Verification question / method	**V1 → R1:** Are barriers continuous, anchored and undamaged? Inspect against the approved checklist and installation records; refer damage for competent assessment. **V2 → R2:** Do crossings prevent conflicting movement? Use the approved safe test. **V3 → R3:** Does failure block access? A competent engineering verifier uses the approved controlled test. **V4 → R4:** Is approved equivalent separation installed and verified before exposure? Check approval, field conditions and restart evidence. Record each check separately as **pass, fail or cannot verify** against approved criteria.
Evidence required	Record each R/V result, location and inspection/test evidence, plus defects, restrictions and restoration. Photograph defects, changes and repairs. Do not use informal tests to establish structural capacity.
Verifier	**V1:** Area Supervisor; Logistics Manager/delegate for monthly inspections. **V2:** Trained designated verifier. **V3:** Competent engineering verifier. **V4:** Competent designated verifier; Engineering approves the alternative.
Frequency / trigger	**V1:** Each shift; documented inspection monthly. **V2**: Pre-start functional check; approved tests as scheduled. **V3:** At approved technical intervals and after maintenance or change. **V4:** Before exposure at every temporary removal. Re-verify affected requirements after impact, failure, change or a relevant event. Follow the approved standard's technical intervals.

Coverage and sampling basis	**Coverage:** Check Site A's active routes each shift and every barrier section and crossing monthly. Include nights and temporary work. **Monitor and report:** Compare completed with expected checks by requirement, route and shift; feed results into the 12-site programme. **Protection gaps:** Restrict affected work where protection is missing.
3. Respond and review	
Failure response and escalation	**Stop and restore:** For a **fail or cannot verify** result, stop affected access or movement. Restore separation or an Engineering-approved equivalent. **Verify and restart:** A competent verifier confirms performance. The Site Manager authorises restart and records the evidence and conditions. **Escalate:** Escalate repeated, systemic, uncertain or resource-dependent failures.
Review owners and frequency	**Logistics Manager:** Develops the local plan. **Site Manager:** Coordinates delivery; reviews weekly and resolves repeat failures and overdue actions. **Business Unit Operations Manager:** Is responsible for approving and resourcing the annual 12-site programme; reviews delivery, volume, coverage, evidence quality, trends and action effectiveness monthly. **Technical authorities:** Approve specialist methods. Escalate urgent failures immediately.

Restricted Content

Appendix F: Tool 6 – Assurance and Confidence Template and Worked Example

Use this template to record each assurance assessment: what was tested, what the evidence showed, where coverage is incomplete, and the confidence the evidence warrants. Adapt it, or reference your existing assurance records if they already hold this information. The worked example shows how the confidence judgement is reached for the mobile-plant risk. All figures and dates are fictional.

Risk-Based Assurance Programme

The assurance lead documents priorities, questions, controls and evidence to be sampled, methods, reviewer, timing and reporting. A review may cover one or several sites. Use existing audit or assurance planning systems if they can hold this information.

Template: adapt to your organisation – T6 Risk-Based Assurance Programme	
Scope and purpose	[business area, period, programme owner and decisions informed; critical risks and sites in scope and the basis for coverage decisions]
Reviews and timing	[for each risk/site grouping: priority and depth (consequence, exposure, control reliability, verification quality, change, incident evidence, findings, uncertainty); timing, selected controls, reviewer and brief; triggered reviews; **coverage-gap list** – what is not assessed, why, and the effect on confidence]
Sampling and evidence	[sample size, selection rationale and limitations – not every control must be tested. Assess control effectiveness and Line 1 verification volume, coverage, methods and response using field checks, approved tests, technical records, worker input and action evidence. Compare matched Line 1 and Line 2 findings where practicable; investigate material differences in context, including scope, timing, conditions, methods and sample selection. Differences inform the confidence judgement; they do not determine it.]
People, resources and approval	[competent reviewers separate from the routine checks assessed; specialist support, time, budget, programme approver and date. Obtain peer or external challenge of own designs. Record shortfalls and approved deferrals as coverage gaps. Keep commissioned Line 3 and its independent reporting route separate]
Confidence and reporting	[audiences and dates; integrate volume against plan, coverage, evidence quality, Line 1 and Line 2 findings, recurring weaknesses and action effectiveness into overall confidence. State assessed scope, material differences, limits, unassessed areas, further checks and decisions; do not average grades or conceal weaknesses]
Response and follow-up	[immediately escalate absent or ineffective protection, repeated failures, material uncertainty and unresolved resource constraints. Assign actions, owners, dates and effectiveness evidence; assurance confirms effectiveness before closure. Update the programme without displacing priority coverage or verification schedules]

Worked Example: Risk-Based Assurance Programme

Illustrative worked example – Risk-Based Assurance Programme (primary example: mobile plant)	
Scope and purpose	**Area/period:** Distribution Centres, 12 sites; October 2027–September 2028. **Owner:** HSW assurance lead (or other competent provider). **Coverage basis:** Mobile plant (CR-02) is shown. Coverage follows consequence, exposure, control reliability, verification quality, change, incident evidence, findings and uncertainty; gaps are shown, not hidden.
Reviews and timing	**Q1 priority (mobile plant, all 12 sites):** High consequence, shared pedestrian exposure, Site A barrier failures and recent change justify early, deeper sampling of separation, crossings, restoration and change controls. Review Site A findings on **31 October 2027**; follow up on **29 January 2028**. **Later quarters:** other critical risks, sequenced by the same factors; weak verification evidence, repeat findings or incident signals bring sites forward. **Coverage-gap list:** any risk/site combination not assessed in the year, why, and the effect on confidence.
Sampling and evidence	**Mobile-plant brief:** Sample field protection, design/installation records, gate tests, defect photos, change approvals, Line 1 checks, worker/supervisor input and action logs. Include nights, deliveries and temporary routes. Test Line 1 coverage, methods, high pass rates, restoration and recurrence. Compare matched findings where possible, allowing for scope, timing and methods; investigate differences alongside incident and other risk evidence. Document selection and limits for each site/risk; do not infer that every control was tested.
People, resources, and approval	**Reviewers:** Competent HSW assurance personnel separate from local implementation and routine checks, with technical specialists as needed. Obtain peer or external challenge when assessing controls they helped design. **Resources:** Reviewer time, specialist capacity, budget and schedule confirmed for the approved programme; any subsequent shortfall or deferral is recorded as a coverage gap and escalated. **Approval:** Programme approved by Chief Operations Officer on 15 July 2027. Leadership separately commissions Line 3 Internal Audit or independent review where required, with an independent reporting route.
Confidence and reporting	HSW integrates verification delivery, coverage, evidence quality, Line 1/2 findings, recurring weaknesses and action effectiveness across sites and risks. Report overall confidence, material differences, limits and decisions to operational owners and business-unit leadership; escalate material uncertainty to the executive HSW forum and relevant officers. State assessed scope and dates; show unassessed areas and further checks. Site/risk judgements support the overall view, not an average of grades. Do not extrapolate beyond the evidence or conceal material weaknesses.
Response and follow-up	**Immediately:** Escalate open access gaps, ineffective interim controls, unprotected work, repeated failures, material uncertainty or unresolved resource constraints. **Actions:** The Business Unit Operations Manager owns corrective delivery; Site Managers own local protection. Record owners, dates and effectiveness evidence. **Follow-up:** The HSW assurance lead tests night-delivery and temporary-route protection before closure; the **29 January 2028** review checks sustained improvement, not permission to defer action.

Mobile plant example - progress
Register → Assessment → Critical control decision → Standard → Verification → **[ASSURANCE]** → Reporting and learning

Worked Example: Mobile-Plant Assurance Across 12 Sites (primary example)

This example shows how HSW combines mobile-plant findings across 12 sites to assess overall confidence. It covers October–December 2027, assessed on 31 December, using samples of controls and working conditions.

The assessment brings together verification coverage and quality, Line 2 sample findings, incident evidence, unresolved weaknesses and uncertainty to reach and explain the confidence judgement. Differences between Line 1 and Line 2 results require investigation in context, not conclusions based on pass rates alone. The judgement covers mobile plant, not all critical risks.

Mobile-plant assurance across 12 sites

Fictional example | Oct–Dec 2027 | Assessed 31 Dec 2027

CRITICAL RISK MANAGEMENT TOOLKIT
SAFER PEOPLE SAFER OPERATIONS

Sites assessed
100%
(12/12)

Line 1 completion
95.8%
(1,380/1,440)

Pass results: Line 1 | Line 2
92.4% (1,275/1,380) | **82.5%** (99/120)
Line 1: 69 fail, 36 cannot verify. Line 2: 13 fail, 8 cannot verify.
Denominators include all outcomes.

Site results

Site	L1 completion	L1 pass	L2 pass	Confidence and reason	
A	91.7% (110/120)	90.0% (99/110)	80% (8/10)	Limited	Night/temporary-route evidence missing.
B	100% (120/120)	96.7% (116/120)	90% (9/10)	Moderate	Restart evidence incomplete.
C	95.8% (115/120)	93.9% (108/115)	80% (8/10)	Moderate	Contractor work under-sampled.
D	100% (120/120)	98.3% (118/120)	90% (9/10)	High	Key conditions covered; closure verified.
E	83.3% (100/120)	85.0% (85/100)	60% (6/10)	Limited	Shifts/change checks missed.
F	100% (120/120)	95.0% (114/120)	90% (9/10)	Moderate	Repeat defects after actions.
G	91.7% (110/120)	90.0% (99/110)	70% (7/10)	Limited	Maintenance evidence inconclusive.
H	100% (120/120)	97.5% (117/120)	90% (9/10)	Moderate	Lasting improvement untested.
I	95.8% (115/120)	93.0% (107/115)	80% (8/10)	Moderate	Temporary-route sample too small.
J	100% (120/120)	96.7% (116/120)	90% (9/10)	High	Coverage sound; restoration verified.
K	91.7% (110/120)	80.0% (89/110)	70% (7/10)	Limited	Night-work evidence missing.
L	100% (120/120)	90.0% (108/120)	100% (10/10)	Moderate	Sample misses non-routine work.

Incident evidence tests the pass-rate picture

50% of reported mobile-plant high-potential incidents were classified failed lucky.
Required critical controls were absent or ineffective; chance prevented serious harm.
This weakens confidence despite 92.4% verification passes.

Additional fictional assumption: incident count and prior-period comparison not provided; no trend or failed-safe percentage inferred. Validate classifications, affected controls and current protection.

What informs the overall judgement

Dimension	Judgement	Evidence and further checks
Verification volume	Moderate	95.8% completed; explain 60 missed checks and address shortfalls.
Coverage	Limited	All sites assessed, but nights, contractors and temporary work under-sampled. Check missing conditions.
Line 1 findings and incident evidence	Limited	92.4% passed; 69 fail and 36 cannot verify. Failed-lucky evidence contradicts broad reassurance. Investigate event causes, recurring defects and affected controls.
Line 1 / Line 2 comparison	Moderate	92.4% versus 82.5%: 9.9 percentage points. Different samples limit comparison; match checks and investigate missed defects. Misalignment not yet established.
Methods and evidence quality	Moderate	Some records cannot confirm performance; improve testing and objective evidence.
Action effectiveness	Moderate	Restoration shown; verify sustained improvement and prevention of repeat failures.

Dimension grades are illustrative judgements, not numerical thresholds; overall confidence is not an average.

OVERALL CONFIDENCE: LIMITED
Failed-lucky incidents and material coverage gaps outweigh reassurance from high pass rates.
Restore and verify protection; investigate contradictory evidence.

Key actions
Operations: maintain verified controls or restrict affected work; resolve incident-related and repeat weaknesses.
HSW: validate incident evidence, sample missing conditions and test action effectiveness.
Follow-up: 29 January 2028; urgent action does not wait.

Scope: mobile plant across 12 sites—not all critical risks. Controls/conditions sampled, not every control.
Site A October subset: L1 36/40; L2 8/10. No comparable prior network assessment; no trend claimed.

Restricted content

Appendix G: Tool 7 – Performance and Confidence Summary and Material Issue Record Templates and Worked Examples

Use these templates to report performance, coverage and confidence for a period (T7A), then to record each material issue, the response and decision required, and the effectiveness check (T7B). Adapt them, or reference your existing reporting and action-tracking systems if they already hold this information. The worked examples show the mobile-plant periodic performance and confidence summary and the Site A material-issue record. All figures and dates are fictional.

T7A: *Complete one summary for each reporting period. Report Line 1 performance and findings with the attributed Line 2 confidence rating, keeping the underlying evidence and its limitations visible.*

Template: adapt to your organisation – T7A Periodic Performance and Confidence Summary	
Scope and period	[risk/control IDs, sites/work and dates; measure definitions and reporting owner]
Volume and coverage	[compare completed checks with the approved annual programme's expected volume and coverage; explain shortfalls, omitted exposure and action. Show sites, shifts, tasks, assets and conditions. Meeting volume targets alone does not establish adequate coverage or quality.]
Line 1 control performance	[show pass, fail and cannot verify counts, the proportion meeting requirements and its denominator. Reference evidence and material failures; inconclusive findings are not passes.]
Patterns and exposure	[identify recurring weaknesses, differences between controls or sites, changing conditions and comparability limits. Label incident insights separately.]
Action effectiveness	[record restored protection, unresolved issues and evidence that completed actions improved protection; link Part B]
Line 2 confidence and assurance insight	[attributed confidence rating: High / Moderate / Limited / Not assessed; provider and assessment date; reasons, material limitations and coverage gaps; relevant Line 2 sample findings and material differences from Line 1; systemic patterns or weak signals. Differences inform the confidence judgement but do not determine it.]
Limitations and decisions required	[state remaining uncertainty, further checks and decisions, resources or escalation needed, with accountable owner and review date.]

Worked Example: Periodic Performance and Confidence

The illustration below shows how Line 1 verification performance, event evidence and action, together with the attributed Line 2 confidence view, can be presented in one report for the primary mobile-plant example. It demonstrates one way of applying T7A; adapt the presentation to existing organisational reporting rather than creating a separate report solely for this toolkit.

Mobile plant: reporting for leaders

Fictional example | 12 sites | Oct–Dec 2027 | five evidence streams, no single score

Verification delivery and coverage

95.8%

of planned checks completed (1,380/1,440).

Gaps: night, contractor and temporary-route work under-sampled.

Control-performance findings

1,275	69	36
pass	fail	cannot verify

(92.4% pass; all outcomes in the denominator)

Event evidence (high-potential incidents)

10 events

5	5	0
failed safely	failed lucky	not established

Descriptive learning, small numbers, no target.

Assurance confidence and limits

LIMITED

HSW assurance lead, 31 Dec 2027.
Night and temporary-route evidence missing.
Assurance sample 82.5% (99/120) – investigate the difference.

Leadership decisions required

- Sustain verified protection or restrict affected work.
- Fund targeted follow-up.
- Direct a night, contractor and temporary-route coverage check.
- Confirm effectiveness 29 Jan 2028.

Challenge the high pass rate: 92.4% pass sits alongside 5/10 failed-lucky events and Limited confidence.

Investigate – do not read as reassurance.

T7B: *Complete one record for each material issue. Assign an owner and an effectiveness check before closing it.*

Template: adapt to your organisation – T7B Material Issue and Improvement Record	
1. Describe the issue and evidence	
Exposure or control issue	[describe the critical risk, control weakness or change in exposure]
Evidence / uncertainty	[state what is known, the evidence source and what remains uncertain]
Recurring theme or learning	[record recurring or cross-site implications. For incidents, state serious-harm potential, the challenged control, actual performance, evidence distinguishing protection from chance, the conclusion or "not established", uncertainty and learning.]
2. Respond and decide	
Immediate response	[action taken to restore protection, restrict work or manage uncertainty]
Decision / escalation required	[decision, forum, resource, technical input, assurance or priority required]
3. Assign ownership and confirm effectiveness	
Accountable owner	[insert role]
Due date / effectiveness check	[due date, evidence required to confirm effectiveness, review date and reporting route]

Mobile plant example - progress
Register → Assessment → Critical control decision → Standard → Verification → Assurance → **[REPORTING AND LEARNING]**

Worked Example: Material Issue and Improvement Record

Site A - October 2027; review 31 October: All 40 targeted checks were completed: 36 passed, two failed and two were inconclusive, giving a 90% pass proportion. Despite meeting the volume target, checks missed night deliveries. Failures prompted restrictions and verified restoration; evidence gaps remain. The Site Manager assigned night checks to Logistics by 7 November, with effectiveness reviewed on 8 November 2027. The Business Unit Operations Manager directed a 12-site night-coverage check; Line 2 reported Limited confidence.

This completed Part B record shows how Site A's verification findings led to immediate protection, cross-site action and effectiveness checks.

Illustrative worked example – Material Issue and Improvement Record (primary example: Site A)	
1. Describe the issue and evidence	
Exposure or control issue	Two failed verifications found gaps in fixed pedestrian barriers at loading bays, allowing access to active mobile plant areas.
Evidence / uncertainty	**Known:** gaps were directly observed; one followed barrier impact and one followed temporary removal. Gate checks elsewhere passed. **Uncertain:** whether similar removals or impact damage exist at other sites.

Recurring theme or learning	Barrier changes can bypass separation controls without triggering re-verification. Treat impact, removal and layout change as mandatory review triggers across all sites.
2. Respond and decide	
Immediate response	Closed affected pedestrian routes, installed temporary physical separation and restricted plant movement until effective barriers were restored and verified. Maintain verified protection while permanent repairs are completed.
Decision / escalation required	Business-unit leadership funds permanent repairs and approves the cross-site review. Operational owners restore protection and apply impact, removal and change triggers. The framework owner updates requirements with technical approval; assurance tests effectiveness.
3. Assign ownership and confirm effectiveness	
Accountable owner	Business Unit Operations Manager; Site Managers own local restoration and verification.
Due date / effectiveness check	Permanent repairs by 30 November; cross-site review by 15 December 2027. These deadlines do not permit unprotected work. Close only after re-verification, with no open barrier gaps and evidence that related actions are effective. Line 2 samples on 29 January 2028, 90 days after the 31 October review.

Restricted Content

Appendix H: Capability Readiness Record

Use this template alongside the Capability Readiness Record section in the main body. It records the capability required for priority CRM roles, the evidence demonstrating readiness, who confirmed it, and any gaps or actions. Use existing competency, authorisation and training records as evidence where they already demonstrate the required capability, rather than duplicating them here. Use the resulting capability gaps and interim arrangements in implementation readiness decisions.

Where roles are combined, assess each CRM function separately. Where independent Line 3 review is commissioned, confirm that the reviewer has the competence and independence required for the scope.

Template: adapt to your organisation – TC Capability Readiness Record

Role	Capability to demonstrate	Evidence of readiness	Confirmed by	Gap / action
Worker / contractor	Ability to apply required controls in the work and recognise, stop or escalate when protection is absent, degraded, bypassed, ineffective or cannot be verified.	Field demonstration or observed work.	Frontline leader	[insert]
Frontline leader	Ability to verify controls against their requirements, respond appropriately to failure and coach the work team.	Observed verification and scenario response.	Operational leader	[insert]
Operational leader	Ability to develop risk-based verification programmes and plans, review delivery and evidence quality, act on patterns and escalate gaps. Senior leaders also need to judge programme adequacy and resource it.	Decision record, field review or scenario exercise.	Operational executive	[insert]
Technical authority	Technical capability to define or approve control requirements, evaluate technical evidence, make or validate material technical decisions, and identify when specialist input is required.	Technical review, approval record or observed technical decision.	Designated technical leader	[insert]
HSW function	Capability to shape and apply the CRM methodology, facilitate and challenge implementation, integrate enterprise insight and provide or coordinate objective assurance where assigned.	Facilitation observation, decision challenge or assurance calibration.	Senior HSW leader	[insert]

Restricted Content

Resource / change decision-maker	Ability to assess how resource or change decisions could affect critical-risk exposure and protection, and identify when technical input or escalation is required.	Observed decision, scenario exercise or decision record showing consideration of critical-risk implications and any required technical input or escalation.	Delegated executive or competent assurance / technical lead	[action, owner, date]
Line 2 Assurance provider	Capability and objectivity to test Line 1 evidence, compare relevant Line 1 and Line 2 findings, investigate material differences and uncertainty, and make a reasoned confidence judgement.	Assurance sample, comparison with relevant Line 1 evidence and documented confidence rationale.	Senior assurance lead or competent reviewer independent of the assurance work being assessed.	[action, owner, date]