# CoRsafe / AMCAS Audit Standard

## Audit program governance, delivery and assurance requirements

**Version published** July 2026

Version 1.0
Prepared for external publication
Aligned to the 2026 Master Code

AMCAS Master Code Auditing Service | CoRsafe

# Contents

**Important notice**

This document explains the audit program, the way audits are delivered, and the quality controls applied to the program. It is intended to support consistent audit practice and provide auditees, customers and supply chain participants with transparency about audit expectations.

This document and the CoRsafe / AMCAS audit programs are provided as a private, industry-led audit and assurance framework only. They are intended to support consistent audit practice and assessment of selected transport safety systems and controls against the program criteria.

They do not constitute legal advice, regulatory advice, statutory accreditation, regulator approval, certification of legal compliance, or a defence to any claim, investigation, prosecution or enforcement action. To the maximum extent permitted by law, NTI Limited makes no representation, gives no warranty or guarantee, and provides no indemnity in connection with participation in the program, completion of an audit, closure of a non-conformance, or issue of a report or certificate. None of those matters should be taken to mean that an Audited Party complies with any law, code, regulator guidance, customer requirement, contract requirement or other obligation.

The program may be informed by the 2026 Master Code and other transport safety concepts, but it does not purport to perfectly align with, reproduce, replace or satisfy any law, code or regulatory requirement. Legal obligations differ between jurisdictions, including HVNL participating jurisdictions, Western Australia, the Northern Territory and New Zealand, and nothing in this document should be read as stating or implying that those obligations are the same, equivalent or fully addressed by the program.

Audits are limited by scope, sampling, timing, access, evidence provided, records reviewed, sites observed, personnel interviewed and auditor judgement at the time of audit. Audit outcomes are program findings only and are not legal findings, regulatory findings, or guarantees of ongoing compliance, safety performance, control effectiveness or future conduct.

The Audited Party remains responsible for identifying and meeting its own legal, safety, operational, contractual, insurance, customer and supply chain obligations, and for designing, implementing, monitoring and maintaining its own systems, controls and corrective actions. To the maximum extent permitted by law, NTI Limited is not responsible for any reliance placed on this document or any audit outcome, or for the acts, omissions, advice, conduct, negligence, representations or decisions of any auditor. Nothing in this notice excludes any liability, right or remedy that cannot lawfully be excluded.

# 1. Introduction and program overview

The CoRsafe and AMCAS industry-led assurance programs are designed to assess how businesses manage safety and Chain of Responsibility (CoR) risks arising from heavy vehicle transport activities. It supports businesses across Australia and New Zealand including carriers, consignors, consignees, loading and unloading sites, distribution centres, producers, retailers, logistics businesses and other entities that influence or control transport activities.

These programs have been designed to assess the presence, suitability, implementation and effectiveness of a business' processes, systems and controls relating to their 'transport activities'. This is facilitated through a structured, risk-based assessment program, tailored to the business based on its role/s, the types of activities it's involved in, and any unique hazards or risks related to its industry sector. The intent is to support clearer audit expectations, structured supply chain assurance and continuous improvement in safety management practices.

The audit program does not constitute an accreditation scheme or statutory certification scheme, and the completion of an audit does not provide any form of legal defence to any prosecution or regulatory action, and not does it, in itself, demonstrate or guarantee compliance with any applicable laws, regulations or statutory obligations. However, the steps taken to prepare for an audit, the evidence reviewed during the audit, and the corrective actions taken after an audit may assist an auditee in demonstrating a proactive and systematic approach to risk management.

## 1.1 Relationship between CoRsafe and AMCAS

CoRsafe operates as a software provider, with a vision to create a safer and more sustainable future for the whole transport and logistics industry, enabled through a digital-first approach for scalable adoption and expansion. A component of the CoRsafe program has been an audit standard, aligned to the 'CoRsafe Guide'.

In 2023, CoRsafe acquired the 'Australian Master Code Auditing Service' (AMCAS) program, previously facilitated by the Australian Logistics Council. The program was run independently after this, with additional investment from CoRsafe to improve quality and consistency of the program.

The aim of both the CoRsafe and AMCAS programs is closely aligned, and following the release of the 2026 Master Code, both programs were reviewed and industry stakeholders engaged. This process considered how best to reflect the updated guidance, provide support to industry, and importantly, reduce the burden of compliance and duplication across industry.

As a result of this process, both programs have now been aligned, and cross-recognition enabled regardless of the program a business undertakes, provided relevant certification eligibility requirements are satisfied. For the purposes of this document, references to the audit program mean the common audit model used for onsite assessments under either CoRsafe or AMCAS programs. An Onsite Audit may be eligible for AMCAS Certification where all applicable criteria are assessed as Met, all non-conformances are closed within the permitted timeframe, no Critical Safety Finding remains under review, QA requirements are satisfied, and CoRsafe confirms certification eligibility. Audit results below 100% will receive an audit report only and do not result in AMCAS Certification.

## 1.2 Use of terminology

The term 'Audited Party' is used throughout this standard. An Audited Party may be a CoRsafe customer, a historic AMCAS subscriber, a carrier, non-truck operator, customer site, business unit, supply chain partner or other organisation being assessed under the audit program, regardless of who initiated the audit.

# 2. Purpose of the audit program

The purpose of the audit program is to provide a consistent, independent and evidence-based method for assessing how an Audited Party manages transport safety risks. The program aims to:

- Support businesses to understand and manage transport safety risks across their operations and supply chains.
- Provide customers and supply chain partners with a structured assurance process that may assist their own assurance and due diligence activities.
- Assess, based on available evidence, whether relevant systems and controls appear to be present, suitable, operating and effective.
- Identify non-conformances and improvement opportunities.
- Promote consistent interpretation of the 2026 Master Code and related industry guidance.
- Provide a robust pathway to AMCAS Certification where all applicable criteria are met
- Provide a documented program pathway to AMCAS Certification where all applicable certification requirements are met.

The audit program is intended to be practical and risk-based. It recognises that different businesses perform different transport activities, have different levels of influence and control, and require different audit effort depending on the complexity and maturity of their operations.

# 3. Scope and alignment to the 2026 Master Code

Heavy Vehicle safety in Australia and New Zealand is governed by different legal frameworks that establish both specific and broad-spectrum obligations for businesses, individuals, and extended supply chains. This, in combination with other legislated safety requirements (i.e. occupational, environmental, etc.) form a part of a business' safety obligations where their activities influence or control how a heavy vehicle may be used.

In these jurisdictions, the concept of CoR is prevalent – and usually refers to the idea that risks to the public, the environment and infrastructure, particularly where heavy vehicles are involved due to the increased consequences of heavy vehicle related incidents, can be adequately managed when everyone works together to ensure safety.

Please note, this program is informed by the 2026 Master Code, recognised industry guidance and high-level transport safety concepts relevant to heavy vehicle activities. Legal obligations differ between HVNL participating jurisdictions, Western Australia, the Northern Territory and New Zealand. References in this standard to Chain of Responsibility, Primary Duty, transport activities, duty holders, controls or the Master Code should be read as program concepts unless the relevant law expressly applies. This standard is not a comprehensive legal compliance matrix for any jurisdiction and should not be relied on as a complete or definitive statement of legal obligations.

Significant consequences for individuals and businesses may also apply, where 'parties in the chain' aren't doing everything, so far as is reasonably practicable, to ensure the safety of their transport activities.

There also exists specific duties relating to areas such as:

- **All jurisdictions** – mass, dimension, loading/load restraint
- **Varied across jurisdictions** – fatigue, vehicle standards
- **HVNL / Land Transport Act (NZ)** – speed
- **Land Transport Act (NZ)** – licencing

The audit program has been designed to provide support for most businesses or individuals across Australia and New Zealand where CoR applies, but draws heavily upon the 2026 Master Code, recognised as a Registered Industry Code of Practice under HVNL. The Master Code as a common reference point regardless of legal relevance provides an independent, industry informed resource exploring hazards, risks and controls relative to heavy vehicles that be used to support businesses assess the robustness of their safety, risk and operational systems.

As such, and to avoid using broad language, the information and references are largely reflective of the approach and requirements under HVNL. The program conceptually incorporates key legal requirements in Western Australia, Northern Territory, New Zealand, and all states participating under HVNL have been represented, however, does not purport to be a complete or definitive statement of legal obligations, and therefore businesses should still seek their own advice regarding their specific circumstances and obligations.

This guide has also been prepared without assigning specific obligations or controls to any particular party as has previously been the accepted approach. To determine if a control is relevant to a business, the business should first consider if they are involved in the relevant transport activity, and then determine how the control may apply to their circumstances. Where using the CoRsafe platform to assess/audit your business, additional tasks have been designed to help assign specific activities/controls to a business as part of the review process.

The audit program will also be reviewed on an ongoing basis based on industry feedback, changes to relevant legislation, updates to the Master Code, and any other stage where review is required. Minor changes based on any review will be tracked and added into the program. Any major changes, like those following the release of the 2026 Master Code will be consulted before being implemented.

# 4. Audit Categorisation

The program is designed to assess how an auditee has identified, assessed and managed transport safety across 9 core elements:

| No. | Audit element | What the element considers |
|---|---|---|
| 1 | **Leadership and Commitment** | How a business' leadership establishes, demonstrates, and maintains accountability for safety and CoR. |
| 2 | **Risk Management** | How a business proactively and systematically identifies, assesses, and controls risks associated with their transport activities and broader supply chain operations. |
| 3 | **People** | How a business ensures all personnel involved in transport activities are competent, fit for work, and supported to meet their safety obligations. |
| 4 | **Assurance, Monitoring and Improvement** | How a business measures performance, verifies that systems are working as intended, and drives continuous improvement. |
| 5 | **Safety Systems** | How policies, procedures, standards, records and document controls support transport safety. |
| 6 | **Transport Operations** | How a business ensures the operational tasks and decisions closely linked to heavy vehicle movements on-road enable safe and compliant outcomes. |
| 7 | **Site Activities** | How a business controls risks related to heavy vehicles and drivers while at a site, including loading, unloading, queuing and traffic management. |
| 8 | **Working With Other Businesses** | How a business manages risks involving suppliers, contractors, subcontractors, customers and other parties. |
| 9 | **Specialised Activities** | How sector-specific or higher-risk transport activities are managed where relevant. |

The audit criteria are activity-driven. Not every question will apply to every Audited Party. Applicability is determined by the transport activities performed by the Audited Party, having regard to the nature, scale and complexity of those activities, and the extent to which the Audited Party has the capacity to influence or control it has over the relevant risk.

Further guidance on the structure of the audit program can be found within the 'CoRsafe Guide', published within the CoRsafe portal. The CoRsafe portal, which includes the ability to self-assess against the audit standard for free and request an audit against the program, can be accessed at https://app.platform.cor-safe.com.au

# 5. Program governance and responsibilities

CoRsafe, as program owner, is responsible for the governance, maintenance and continuous improvement of the audit program. CoRsafe will:

- Promote participation and support businesses across the supply chain.
- Maintain the audit standard, audit questions, guidance material and digital audit platform.
- Review and update the program in line with the Master Code, relevant legislation, recognised industry guidance and program performance data.
- Maintain a list of approved auditors and manage auditor appointment, onboarding, performance and quality controls.
- Manage audit initiation, platform access, reporting workflows and certification processes.
- Receive audit program fees and manage payment arrangements with approved auditors.
- Investigate complaints, manage disputes and support resolution of process issues.
- Maintain appropriate confidentiality over information obtained through audit activities.
- Use aggregated and deidentified audit information to identify program trends, common non-conformances and improvement opportunities.

CoRsafe may issue supporting procedures, guides, schedules, platform instructions, auditor guidance notes or customer-facing materials to support this standard. Subject to applicable law and any signed agreement between the relevant parties, this standard governs audit delivery. Any intended departure from this standard should be documented in writing by CoRsafe and communicated to affected parties where relevant.

# 6. Audit principles

Audits are conducted in accordance with the following principles:

- **Evidence-based:** findings should be based on sufficient and appropriate evidence, having regard to the circumstances, as determined by the auditor.
- **Risk-based:** audit scope and depth must reflect the activities, risks, controls and maturity of the Audited Party.
- **Independent:** auditors must act objectively, manage conflicts of interest, and remain free from undue influence by the Audited Party, customer, program owner, commercial interests, or any other party.
- **Consistent:** auditors must consider how observations and gathered evidence apply to the audit criteria, and assess accordingly. Observations or evidence that do not correlate with the criteria may be recorded, but should not impact how the criteria is assessed.
- **Practical:** the audit should assess how controls operate in real business conditions, not only whether documents exist.
- **Improvement-focused:** non-conformances must identify the system or control issue that requires correction in a way that enables the Audited Party to consider how they might address it.
- **Transparent:** the Audited Party must understand the audit scope, method, evidence needs, findings, non-conformances and next steps.

# 7. Audit types and delivery models

To accommodate different audit purposes and applications, the audit program includes a desktop/remote audit, and an onsite/hybrid audit.

Due to limitations on verifying evidence, particularly when considering implementation and effectiveness, desktop/remote audits are not eligible for AMCAS certification regardless of the score achieved. The audit criteria is also reduced, focusing predominantly on the presence and suitability of systems, policies and procedures of the Audited Party relative to their roles, sectors and activities. Desktop/remote audits are called 'CoRsafe Smart Audits'.

Onsite Audits have been categorised into 3 'levels', though the rigour and assessment expectations for each level remain the same. The different levels are intended to reflect the additional time required to conduct an audit on businesses, depending on the Audited Party's size, risk profile, transport activities, business complexity and assurance needs.

Certification eligibility is determined only in accordance with this standard. A certificate, where issued, is limited to the stated audit scope, site or sites, audit type, audit date, criteria version and validity period. Desktop or remote assessments are not eligible for AMCAS Certification because they do not include mandatory onsite verification.

The different audit types available under the audit program are outlined below.

| Audit Type | Audit Level | Description | Certificate outcome |
|---|---|---|---|
| **CoRsafe Smart Audit** | Desktop / Virtual | An online-only assessment suitable for businesses seeking to demonstrate the presence and suitability of their safety management systems, policies, procedures and records. It is suitable for low-risk operating environments, due-diligence checks of other businesses, or independent documentation reviews. | No certificate. A report is issued. |
| **Onsite Audit** | 1-Day | A hybrid audit with mandatory onsite verification **over 1 day**, suitable for most carriers and non-truck operators with straightforward transport activities and established records. | Eligible for AMCAS Certificate if 100% is achieved. |
| | 2-Day | A hybrid audit with mandatory onsite verification **over 2 days**, suitable for large carriers and non-truck operators with high exposure to heavy vehicles, or smaller operators with complex arrangements. | Eligible for AMCAS Certificate if 100% is achieved. |
| | 3-Day | A hybrid audit with mandatory onsite verification **over 3 days**, suitable for large, multi-site or highly complex businesses, including those with extensive contractor networks, high-risk activities or significant influence across their supply chain. | Eligible for AMCAS Certificate if 100% is achieved. |

If the audit level of an onsite audit is not suitable for the Audited Party, it can be changed provided more than 14 days' notice is provided, subject to auditor availability.

If it becomes apparent that the Audited Party requires a level of audit greater than what was originally selected on/after the date of the audit, CoRsafe must be notified immediately and all efforts will be made to assess the

appropriate audit level and availability of auditor to complete. Additional costs will apply, so parties requesting audits are encouraged to carefully consider the appropriate audit level before booking.

## 7.1 CoRsafe Smart Audits (Desktop)

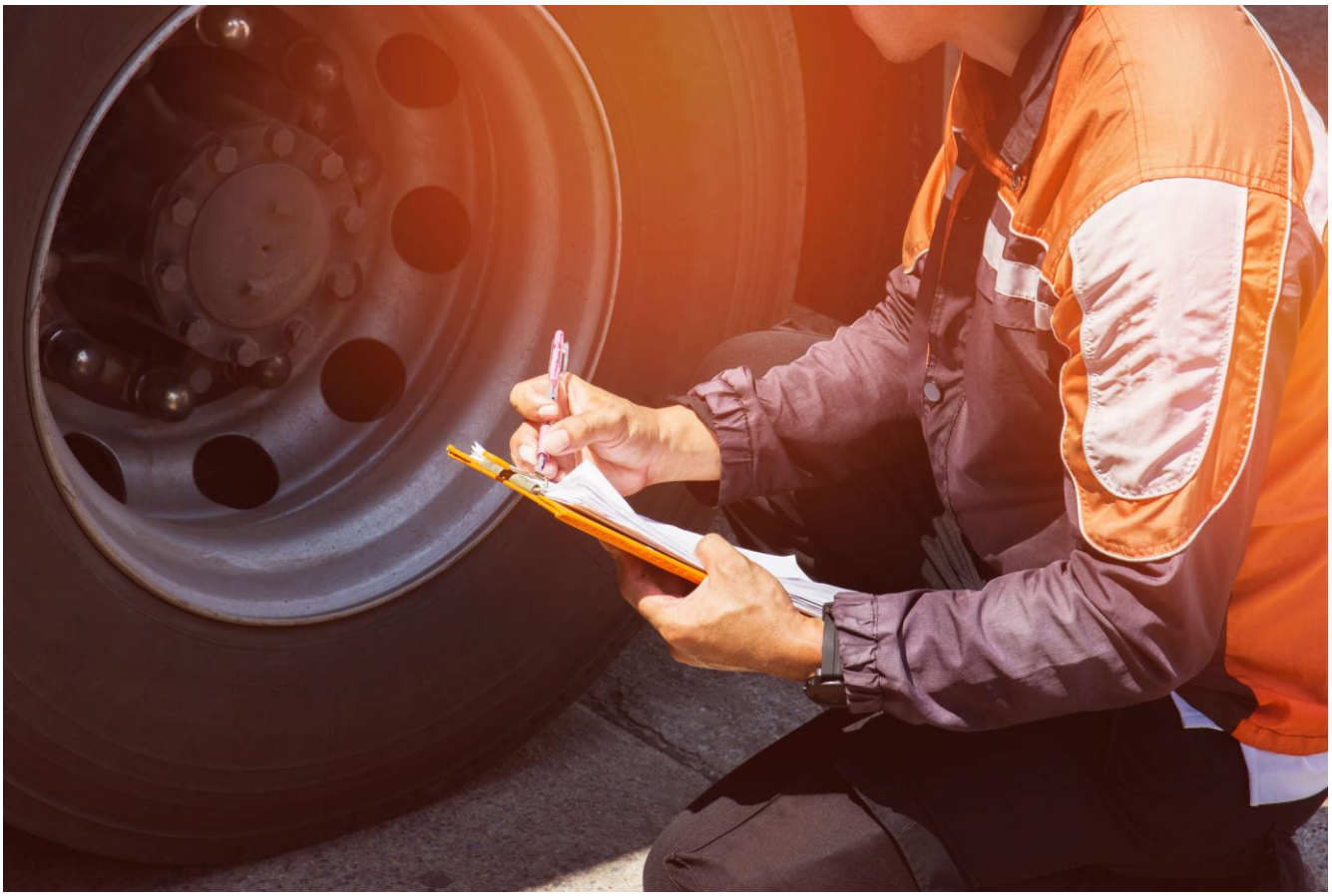
A CoRsafe Smart Audit is delivered through CoRsafe's online platform. It focuses on elements that can reasonably be demonstrated digitally, including the presence and suitability of policies, procedures, records, registers, review processes and other safety management system evidence.

A Smart Audit does not include onsite verification, operational observation or face-to-face testing of practices. It is therefore a lower-assurance assessment than an Onsite Audit and is not suitable where the purpose of the audit is to verify implementation of controls in practice, investigate a safety concern, or determine eligibility for AMCAS Certification.

## 7.2 CoRsafe / AMCAS Audits (Onsite / Hybrid)

Onsite Audits are delivered using a hybrid model. The auditor may review evidence before the onsite component, conduct interviews remotely or in person where appropriate, undertake mandatory onsite verification, record findings in the platform, issue the audit report through the platform, raise non-conformances in the platform and close non-conformances in the platform.

Onsite Audits must include sufficient onsite time to verify relevant operational practices, interview personnel and observe activities where those activities are material to the audit scope. The onsite component must not be reduced to a document review only.



# 8. Audit timing, duration and effort categories

Audit duration includes all work required to deliver the audit, including planning, scoping, document request and review, interviews, onsite verification, evidence review, audit findings, reporting, non-conformance raising and included non-conformance review activity. Travel and administrative arrangements may be managed separately. All costs associated with travel are charged 'at-cost', and additional allowances may apply. For a copy of the allowance schedule, which is reviewed annually, please contact CoRsafe.

| Category | Indicative duration / delivery | Included NC closure reviews |
|---|---|---|
| **CoRsafe Smart Audit** | Audited Party given a total of 28 days to upload evidence, and an additional 28 days to respond to any gaps. Audit report and status of any non-conformances managed in CoRsafe platform. | As required |
| **Onsite Audit** | Audited Party able to upload evidence prior to audit date. Auditor spends time on site, based on Audit Level (as per below). Audit report and status of any non-conformances managed in CoRsafe platform. | Up to 10 |
| **1-day** | 4-8 hours onsite, depending on how much evidence is uploaded and able to be reviewed prior to the audit date. | |
| **2-day** | **Predominantly onsite:** 12-16 hours onsite over 2 days, depending on how much evidence is uploaded and able to be reviewed prior to the audit date.<br><br>**True hybrid (preferred):** 6-8 hours onsite, and 6-8 hours remotely reviewing uploaded evidence. | |
| **3-day** | As per arrangement with audited party, across a 3-day period. | |

Where the number of non-conformances exceeds the number of included closure reviews for the relevant audit type, the Audited Party may be required to pay additional amounts for the auditor to review evidence submitted against those additional non-conformances. Any additional payment requirement does not extend the required timeframes for submission of corrective action evidence unless CoRsafe confirms otherwise in writing.

# 9. Audit scope, site sampling and use of other audit programs

The audit scope must be confirmed by the auditor before the audit begins. The scope must identify the Audited Party, the site or sites to be assessed, the industry sectors related to the Audited Party, and the different roles the Audited Party holds.

## 9.1 Site-based audit outcomes

An audit is against the audited site or sites, not the whole of the business. Audit reports and certificates must not be represented as evidence of whole-of-business performance unless there has been sufficient site sampling to provide confidence that the management system is implemented and operating effectively across the business.

## 9.2 Multi-site organisations

For multi-site organisations, a site sampling approach may be used where sites operate under a common management system, perform similar activities, and are subject to central governance and corrective action control. Where sites operate under materially different systems, risk profiles or local controls, separate audits or increased sampling may be required.

Where site sampling is used, 25% of selected sites should be chosen randomly where possible. The remaining sites should be selected to reflect the greatest reasonable variation in risk and operations, including site size, transport volume, shift patterns, contractor use, historical findings, incidents, complaints, maturity, geography and whether sites are permanent, temporary or virtual.

The default sample size is the square root of the total number of relevant sites, rounded up to the next whole number. Where a multi-site organisation who has previously been audited and obtained AMCAS certification across their business requests a new audit across their organisation, the sample may be reduced to 0.8 times the square root of the total number of sites, rounded up to the next whole number. CoRsafe may require a higher sample where risk, complexity or prior performance warrants it.

*Multi-site organisation sample size = $\sqrt{}$total number of sites*

## 9.3 Use of other audit programs

The audit program recognises that other credible heavy vehicle, transport safety or CoR-related audit programs may provide relevant evidence. A current TruckSafe audit or a post 1 August 2026 Heavy Vehicle Accreditation (HVA) audit (General Safety Accreditation and Alternative Compliance Accreditation) may be accepted as evidence against relevant audit criteria, provided the audit is current, independent, relevant to the criterion being assessed, and supported by sufficient documentation.

Where an Audited Party has completed one of these programs in the previous two years, the program owner and auditor should consider whether an additional audit is required, whether the scope can be reduced, or what the appropriate audit duration is. Acceptance of another audit program does not automatically result in certification under this audit program.

If the reason for the audit is a specific safety concern, incident, customer concern, regulatory issue or other risk trigger, the full audit scope should be conducted regardless of any other audit program that applies to the business. Other audit evidence may still be considered, but it must not replace reasonable enquiry into the safety concern that triggered the audit.

# 10. Audit criteria, applicability and scoring

Audit criteria are written as statements, used to assess whether the Audited Party has present, suitable, operating and effective systems and controls for the relevant transport activities.

The criteria are designed to assess the Audited Party's processes and systems for ensuring the safety of their transport activities, with respect to the relevant activities, hazards and risks identified in the 2026 Master Code and other industry guidance.

Audit criteria do not reflect any specific control, or establish an expectation that any specific control in the 2026 Master Code are adopted, though they may reference relevant controls to support the Audited Party when considering what they might reasonably do to ensure the safety of their transport activities.

Each applicable criteria is assessed as either 'Met' or 'Not Met'. Some criteria may also be marked as 'Not Applicable'. Partial scoring is not used. Audit findings may also identify maturity observations where controls meet minimum requirements but could reasonably be strengthened. This should be identified in the audit report, but not impact the criteria assessment.

| Assessment | Meaning | Consequence |
|---|---|---|
| Met | The auditor has sighted sufficient and appropriate evidence to reasonably conclude that the criteria is satisfied. | **N/A** |
| Not Met | The auditor has not sighted sufficient and appropriate evidence to reasonably conclude that the criteria is satisfied, or the evidence shows the system or control is not suitable or effective. | **A non-conformance is raised.** |
| N/A | The criteria does not apply because the Audited Party does not perform, control or influence the relevant activity, risk or control. | **Excluded from scoring.** |

The final audit score is calculated as the number of Met criteria divided by the number of applicable criteria, expressed as a percentage. Criteria assessed as N/A are excluded from the score.

A criteria must not be marked N/A where the Audited Party has indirect influence over the activity through contracts, rates, scheduling, loading requirements, site access conditions, customer requirements, operational pressure, supply chain arrangements or other business practices. N/A decisions may be reviewed through the quality assurance process.

# 11. Evidence, interviews and audit depth

The Audited Party is responsible for providing appropriate and sufficient evidence to support the audit. Where evidence is insufficient, the auditor should make reasonable further enquiries. If sufficient evidence is still not available, the relevant criterion must be assessed as 'Not Met'.

The auditor must record enough information to demonstrate what was reviewed, what was tested and why the score was given. Audit comments should be clear, specific and evidence-based. They should not simply repeat the question or state a conclusion without describing the basis for that conclusion.

## 11.1 Evidence expectations

Evidence may include policies, procedures, standards, risk assessments, contracts, registers, meeting records, training records, monitoring data, incident records, corrective action records, maintenance records, journey plans, load records, site observations, photographs, interview responses and other verifiable information. The same evidence may support more than one criterion where it is relevant and sufficient.

The audit design does not separate documentation scoring from in-practice scoring. Instead, criteria are designed to ask more targeted questions that require auditors to consider both system design and evidence of implementation where relevant.

## 11.2 Audit depth

An Onsite Audit should include:

- **Review** of relevant policies, procedures, records and other evidence
- **Reasonable enquiry** into the Audited Party's transport activities and CoR roles
- **Interviews** with personnel who understand or perform the relevant tasks
- **Testing** of relevant parts of the safety management system
- **Onsite observation** of relevant operational activities where available and material
- **Clear recording** of evidence, findings, non-conformances and report conclusions

While audit programs for large, complex or high risk Audited Parties may take additional time, the depth of the audit program should not change.

Any increases to audit depth should be proportionate to the increased size or complexity of the organisation, not a change in how the criteria are applied/assessed.

## 11.3 Record Sampling

To sufficiently answer some audit criteria, records may need to be reviewed (i.e. runsheets/work diaries, maintenance records, transport documentation, training records, etc.). Where this is required, auditors are expected to review a sample of this documentation, at a minimum based on the record types below.

If the Audited Party does not have enough records to meet the below requirements, 100% of available records should be reviewed.

**Record type:**
Employee or maintenance records

**Sample size:**
10% or 10 records from the last 12 months, whichever is the greater.

**Record type:**
Transport Documentation

**Sample size:**
10% or 30 records from the last 3 months, whichever is the greater, capped at 50 records.

## 11.4 Interviews

Auditors must not rely solely on documentation to determine whether a management system is operating. Interviews should be targeted at personnel who perform, supervise or govern the tasks being assessed. Auditors should ask open questions, avoid leading questions, explain the purpose of the interview, and where practical conduct interviews where the relevant work is performed.

Where a finding appears to be isolated or systemic, the auditor should test that conclusion through further enquiry where reasonable. This may include interviewing additional personnel, reviewing further records or observing similar activities in another area of the site.

Recordings of interviews do not have to be captured within the audit report, but any discussion that influences how a criteria is assessed should be summarised as part of the auditor's findings.

# 12. Conducting the audit

Audits must be conducted through the approved digital audit platform unless CoRsafe approves an alternative process. The platform is used to initiate audits, upload or review evidence, record findings, generate reports, raise non-conformances, receive corrective action evidence and close non-conformances. An excel file can be downloaded in the CoRsafe platform and later re-uploaded if the audit is being conducted in an area where internet is not reliably available.

## 12.1 Initiating an audit

Any business can initiate an audit against any other consenting business through the CoRsafe platform, or by contacting CoRsafe. The CoRsafe platform can capture the Audited Party, audit type, preferred date of audit, and allocated auditor. The business requesting the audit may choose a preferred auditor, or elect to have an auditor allocated on their behalf.

If a preferred auditor selected by the requesting company does not accept the audit within 3 business days, CoRsafe will contact the requesting company to see if an alternative auditor can be used, the date changed, or explore other options.

## 12.2 Preparing for an audit

The Audited Party will be able to review the audit in the CoRsafe platform. The platform will also help guide them on activities that can assist in preparing for the audit, including uploading evidence to the platform.

For onsite audits, the auditor should also review any information uploaded by the Audited Party, and can start marking any criteria that can be assessed digitally. Desktop audits are conducted entirely through the platform and therefore uploading evidence and reviewing evidence is required.

For onsite audits, the auditor must also make contact with the Audited Party at least 7 days before the audit date where practicable. This is to encourage attendance by relevant personnel, go over the expected evidence/how time will be spent on site, and to ask if there are any site access/induction requirements.

## 12.3 Opening meeting for an onsite audit

The opening meeting should include the relevant nominated representative, senior management where appropriate, and personnel who may be involved in the audit. The auditor should confirm the audit purpose, scope, method, timing, information needs, interview arrangements, onsite verification plan, communication pathway, and process for non-conformances and close-out.

## 12.4 Generating audit findings

Audit findings must be based on evidence obtained during the audit. The auditor must understand the Audited Party's business processes, review relevant records, test the management system, discuss the system with personnel, and observe work practices where required. Findings must be recorded in the platform against the relevant criterion.

## 12.5 Closing meeting

At the completion of the audit, or at the end of each audit day for multi-day audits where appropriate, the auditor should conduct a closing meeting with the nominated representative. The closing meeting should summarise the audit findings, explain any non-conformances, provide an opportunity to clarify misunderstandings, outline the close-out process and confirm key timeframes.

## 12.6 Critical safety findings

While most audit findings will be managed through the normal non-conformance process, some findings may indicate a serious or immediate transport safety concern requiring additional review.

A Critical Safety Finding may exist where the auditor identifies circumstances that, in the auditor's reasonable opinion, indicate:

- An immediate or significant risk to the safety of any person.
- A systemic failure of safety controls relating to transport activities.
- Evidence suggesting deliberate falsification, concealment or manipulation of records relied upon for the audit.
- A serious incident, recurring event or pattern of behaviour that has not been appropriately identified, assessed or managed by the Audited Party.
- Any other circumstance that may materially affect the integrity of the audit process or confidence in the Audited Party's ability to manage transport safety risks.

Where a Critical Safety Finding is identified, the auditor must notify CoRsafe as soon as reasonably practicable. CoRsafe may undertake further review of the circumstances and determine whether additional action is required. Identification, review or escalation of a Critical Safety Finding does not transfer responsibility for safety controls, legal compliance, incident response, mandatory reporting or operational decision-making from the Audited Party or any other duty holder to CoRsafe or the auditor.

Depending on the nature of the finding, CoRsafe may:

- Require additional evidence or clarification.
- Expand the audit scope.
- Require additional site verification activities.
- Suspend completion of the audit pending further review.
- Require a follow-up audit.
- Refer the matter for independent review.

The existence of a Critical Safety Finding does not automatically determine the final audit outcome. However, certification will not be granted while a Critical Safety Finding remains under review or where CoRsafe determines that additional assurance activities are required before an audit outcome can be finalised.

Where an immediate risk to health or safety is identified, the auditor may pause audit activities, notify the nominated site representative and follow site safety procedures. The Audited Party remains responsible for determining and implementing immediate controls and any required regulator, emergency service, customer or internal notifications.

# 13. Non-conformances and close-out

A Non-Conformance (NC) must be raised for each applicable criteria assessed as 'Not Met'. An NC should focus on the system, control, evidence or implementation gap that caused the criterion to be assessed as 'Not Met'.

The NC should be clear enough for the Audited Party to understand what has not been demonstrated and what type of evidence may be required to close the NC. The auditor may provide broad examples of suitable evidence or measures, but must not design the corrective action, provide consultancy, or compromise independence.

Unless otherwise agreed in writing, the Audited Party must submit corrective action evidence within 28 days of receiving the final audit report containing the NC.

An Audited Party may request an extension for NC closure by contacting CoRsafe. CoRsafe will review the circumstances of the request, and at their discretion, which may include discussions with the auditor and Audited Party, approve an extension of up to 90 days from when they received the final audit report containing the NC.

All NCs must be closed within the agreed period for certification eligibility. Where NCs remain open after the agreed period, the audit will close with the score and outcome achieved at that time.

Where a corrective action can be completed and verified during the audit, the auditor may close the NC during the audit. Where implementation needs to be observed or tested, the auditor may require additional evidence, further interviews or a revisit to the site. Depending on the nature of the NC, and the difficulty in reviewing the corrective action, closure of some NCs may incur additional cost.

# 14. Reports and certificates

The audit report is the formal record of the audit. It must identify the Audited Party, scope, site or sites audited, audit type, audit date, auditor, applicable criteria, findings, score, non-conformances, evidence reviewed and any limitations or assumptions relevant to the audit outcome.

CoRsafe Smart Audits result in a report only and do not result in certification. Onsite Audits result in a report and may result in AMCAS Certification if all applicable criteria are assessed as Met, and the final audit score is 100%.

Audit results below 100% receive a report only. No certificate will be issued unless and until all applicable criteria are assessed as Met within the permitted close-out timeframe and the program owner confirms certification eligibility.

A certificate or report must not be used to represent whole-of-business performance unless the audit scope and site sampling provide sufficient coverage of the business. When considering audit certificates or reports, the roles and sectors related to the Audited Party should be considered.

# 15. Ongoing monitoring and continuous improvement

An audit provides an assessment of the Audited Party's systems, controls and transport activities at a point in time. While an audit may provide assurance regarding the evidence reviewed and activities observed during the audit, it does not guarantee ongoing compliance, future performance, or the continued effectiveness of safety controls after the audit has been completed.

The Audited Party remains responsible for continuously identifying, assessing and managing transport safety risks, and for ensuring that systems and controls remain suitable, implemented and effective as business activities, risks and operating environments change.

Businesses are expected to monitor their performance on an ongoing basis, including through activities such as:

- Internal reviews and self-assessments.
- Monitoring of incidents, hazards, complaints and near misses.
- Review of corrective actions and improvement opportunities.
- Periodic review of policies, procedures, risk assessments and operational controls.
- Management review of transport safety performance and emerging risks.
- Verification that implemented controls remain effective and appropriate.

Businesses may also use the CoRsafe platform to undertake additional self-assessments, review changes to their transport activities, monitor performance across audit elements, and identify areas requiring improvement. These activities can assist businesses in maintaining an up-to-date understanding of their transport safety systems and preparing for future audits.

Ongoing monitoring and review are important components of effective safety management and should be undertaken regardless of the outcome of any audit, report or certification issued under this program.

# 16. Use of Artificial Intelligence

CoRsafe and approved auditors may use artificial intelligence tools to support audit administration, quality assurance and report preparation, provided those tools are used responsibly, securely and under human oversight. AI may be used to assist with activities such as improving the clarity of audit notes, refining the wording of findings, preparing executive summaries, identifying inconsistencies in draft reports or supporting quality assurance review. AI must not be used to make audit decisions, determine audit outcomes, assess evidence, replace professional judgement, or independently generate audit findings or reports.

Any use of AI must occur within an approved and appropriately protected environment that maintains the confidentiality and security of Audited Party information. Sensitive, confidential or commercially sensitive information must not be entered into unmanaged or unsecured AI tools. Auditors remain responsible for the accuracy, completeness and appropriateness of all audit records, findings and reports, including any content that has been supported or refined using AI. All AI-assisted content must be reviewed and approved by a competent person before being relied upon or issued.

# 17. Quality assurance program

Quality assurance (QA) is a core part of the audit program. It is used to promote consistent audit practice, improve report clarity, identify auditor calibration needs, detect quality issues and strengthen confidence that audits are being carried out in line with this standard.

## 17.1 QA review coverage

CoRsafe will apply mandatory, sample-based and triggered quality assurance reviews. As a minimum:

- The first two audits completed by each newly approved auditor will be reviewed.
- All 3-day Onsite Audits will be reviewed.
- At least 10% of completed audits per quarter will be reviewed, excluding audits already subject to mandatory review.
- Triggered reviews may be conducted where there is a complaint, dispute, unusual result, unusual N/A use, high number of NCs, no NCs in a high-risk context, new or unusual audit scope, safety concern, auditor performance issue, or other concern identified by CoRsafe.

## 17.2 QA review focus

The intent of quality assurance is not to override the auditor's judgement or to re-perform the audit. The review is intended to determine whether the auditor's recorded comments, evidence references and findings support the score provided, and whether the report is sufficiently clear, consistent and complete.

QA reviews may consider whether:

- The audit scope and applicable activities were clearly defined
- N/A ratings were justified
- Met ratings were supported by sufficient and appropriate evidence
- Not Met ratings were clearly explained and linked to the relevant criterion
- Comments describe the evidence sighted rather than simply stating conclusions
- The audit report is clear, professional and internally consistent
- The number and nature of NCs are plausible given the evidence recorded
- The audit appears to have been delivered to the expected depth for the audit type
- Any certificate recommendation is supported by the final audit result and scope

## 17.3 Auditor calibration and program improvement

CoRsafe may use QA outcomes to provide auditor feedback, require report corrections, identify training needs, conduct calibration sessions, update guidance material, modify audit questions or review program controls. Where a material audit quality concern is identified, CoRsafe may require further review, additional evidence, auditor retraining, suspension from audit allocation, or other appropriate action.

Artificial intelligence (AI) may be used as part of the quality assurance program. This may include analysis of audit reports, comparison of comments and scores, identification of unusual patterns, trend analysis across multiple audits, review of recurring non-conformances, and support for auditor calibration. AI-assisted review does not remove the need for human oversight of quality assurance decisions.

Any utilised AI will be limited to closed environments to ensure the privacy of all information is maintained.

# 18. Disputes, complaints and review of findings

The Audited Party should raise any questions about findings with the auditor during the audit or closing meeting where possible. If the issue cannot be resolved, the Audited Party may request review through CoRsafe.

A dispute or complaint may relate to audit process, auditor conduct, scope, interpretation of criteria, evidence considered, scoring, N/A treatment, non-conformance wording, report clarity or certification outcome. CoRsafe may review the audit record, seek further information from the auditor and Audited Party, appoint an independent reviewer, or require further evidence or clarification.

The dispute process is not intended to enable an Audited Party to negotiate findings. Findings will only be changed where CoRsafe is satisfied that the original finding was not supported by the evidence, relevant evidence was not reasonably considered, the criteria was misapplied, or a process issue materially affected the audit outcome.

# 19. Auditor approval, competence and standards

Only auditors approved by CoRsafe can conduct audits against this audit program. To qualify to become an auditor against this audit program, applicants must meet the requirements in the table to the right and below.

Auditors must exercise due care, diligence and professional judgement. They must provide accurate, timely and sufficiently detailed information, participate in site induction and safety processes, work within their area of expertise, and attend any reasonable training as directed by CoRsafe.

Auditors must complete audit reports and platform records in line with the service levels below:

- Response to requests for audits within the CoRsafe platform within 3 business days
- Draft audit reports submitted within 5 business days of audit completion
- Audit report finalised within 5 business days of submitting the draft audit report
- NCs closure/response within 5 business days of having received evidence from the Audited Party

| | |
|---|---|
| **Qualifications** | • Completion of a nationally recognised or equivalent Lead Auditor course aligned with the current version of ISO 19011 (e.g., ISO 9001, ISO 45001, or integrated management systems). |
| **Industry Experience** | • Minimum 3 years of relevant supply chain / transport industry experience and capability, OR auditing experience of safety systems in other industries |
| **Technical Competencies** | • Knowledge, understanding and application of Heavy Vehicle National Law, or WA, NT or NZ equivalent Chain of Responsibility legal frameworks.<br>• Knowledge, understanding and application of the 2026 Master Code. |
| **Audit Experience** | • Experience undertaking audits within the last 2 years (i.e. TruckSafe, HVA) or nomination and supervision from and already approved auditor for the first 2 audits. |
| **Insurances** | • Insurance limits outlined in Auditor Agreements relating to:<br>  ○ Public Liability Insurance<br>  ○ Professional Indemnity Insurance<br>• Worker's Compensation where directly employing workers, or any other case as required by law. |

# 20. Conflict of interest and auditor rotation

Auditors must act independently and objectively. An auditor must not conduct an audit where the auditor has a direct or indirect financial interest, commercial relationship, personal relationship, or other interest that may reasonably be perceived to affect impartiality.

An auditor must not accept an appointment to audit an Audited Party where the auditor has provided consultancy services to that Audited Party within the previous two years. An auditor must not assist or advise an Audited Party in designing, implementing or closing corrective actions arising from an audit conducted by that auditor.

Auditors must not conduct more than two consecutive audits for the same Audited Party at the same site. After two consecutive audits, a different auditor must be appointed unless CoRsafe approves an exception due to exceptional circumstances and records the reason for that decision.

Auditors must not accept inducements, favours or instructions that could influence, or be perceived to influence, an audit outcome, audit finding or response to a non-conformance.

# 21. Confidentiality and use of information

Auditors, CoRsafe and any person involved in the audit process must maintain appropriate confidentiality over information obtained through audit activities. Information must only be used for delivering, administering, assuring, reporting on and improving the audit program, unless disclosure is required by law, authorised by the relevant party or permitted under an applicable agreement. Information obtained through audit activities must be handled using reasonable security controls, retained only for legitimate program purposes and disclosed only on a need-to-know basis. CoRsafe may use aggregated and reasonably deidentified audit information for program reporting, trend analysis, auditor calibration, quality assurance, industry insights and continuous improvement. Nothing in this standard requires an Audited Party to waive legal professional privilege.

Where AI-assisted tools are used, the program owner will apply appropriate governance controls for information handling, access and confidentiality.

# 22. Change of company name or business structure

Where an Audited Party changes its company name, trading name, ABN, ACN or equivalent business identifier within 12 months of an audit, it may request that the program owner consider issuing an updated report or certificate in the new name.

CoRsafe may require a statutory declaration or equivalent director statement confirming that the change has not resulted in operational changes, change of control, new sites, material changes to transport activities or other changes that would affect the audit outcome. CoRsafe may also require current company extracts or other documents it considers necessary.

An updated report or certificate will not normally be issued where the change relates to a merger, acquisition, change of control, new site, materially different operations or any other circumstance where CoRsafe considers that the previous audit no longer reasonably reflects the Audited Party’s activities or risk profile.

# 23. Related documents

This framework, if read in isolation, may not reflect the entirety of the audit program approach. It should be considered in conjunction with:

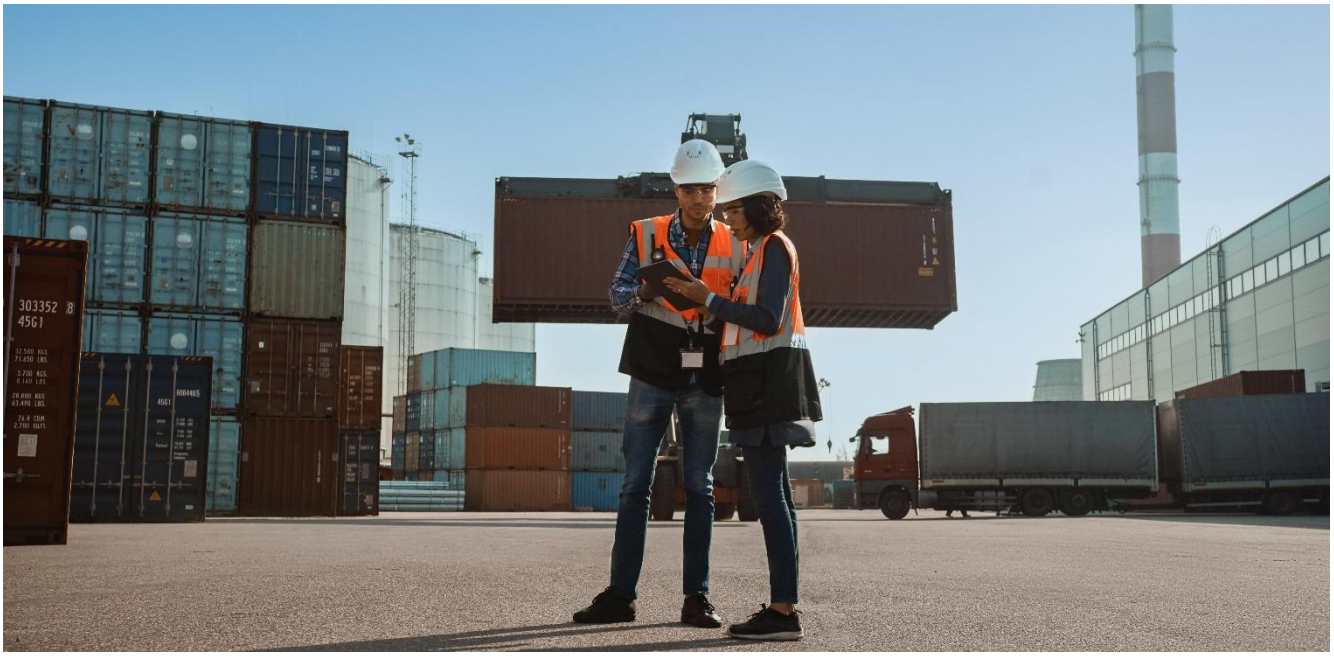
- The related audit questions, criteria, auditor guidance and mapping back to the 2026 Master Code
- The 2026 Master Code
- The CoRsafe Guide
- For auditors, the Auditor Code of Conduct, Auditor Agreements, and any related Agreement Schedules

# 24. Program review and version control

The audit program will be reviewed periodically to reflect changes in the Master Code, relevant legislation, recognised industry guidance, audit practice, platform capability, customer feedback, auditor feedback, QA outcomes and aggregated program data.

Each revision of the Master Code, or any replacement Master Code, will trigger a whole-of-program review. Minor changes based on any review will be tracked and added into the program. Any major changes, like those following the release of the 2026 Master Code will be consulted before being implemented.

| Version | Summary of review | Date of issue | Next scheduled review | Approved by |
|---|---|---|---|---|
| **1.0** | Creation of CoRsafe & AMCAS Audit Framework –<br>• Retiring of the CoRsafe Audit Framework (2024);<br>• and the AMCAS Audit Framework (2024) | 1 July 2026 | 1 July 2028 | CoRsafe |



# Appendix A – Definitions

| Term | Definition |
|---|---|
| **Audit** | A systematic, independent and documented process for obtaining evidence and evaluating it objectively to determine the extent to which audit criteria are fulfilled. |
| **Audit criteria** | The requirements or outcome statements against which audit evidence is assessed. |
| **Audit evidence** | Records, statements of fact, observations, interview responses or other verifiable information relevant to the audit criteria. |
| **Audit finding** | The result of evaluating audit evidence against audit criteria. |
| **Audit scope** | The extent and boundaries of the audit, including the Audited Party, site or sites, activities and criteria included. |
| **Audited Party** | The business, site, business unit, carrier, non-truck operator, customer, subscriber or supply chain partner being audited. |
| **Auditor** | An individual approved by the program owner to conduct audits under this standard. |
| **CoRsafe Smart Audit (Desktop)** | An online-only desktop assessment delivered through the platform. |
| **Onsite Audit / Hybrid Audit** | An onsite or hybrid audit that includes mandatory onsite verification and may be delivered as a 1, 2 or 3-day audit. |
| **Non-Conformance (NC)** | A finding raised where an applicable criterion is assessed as Not Met. |
| **Transport activities** | Activities, including business practices and decisions, associated with the use of a heavy vehicle on a road, including contracting, scheduling, packing, loading, unloading, consigning, receiving goods or managing premises. |

*Definitions in this appendix are for the purposes of this audit program only. They do not replace, amend or limit any definition under applicable law.*

# Appendix B – CoR roles and transport activity mapping

The audit criteria relate to the Audited Party's transport activities and the role or roles it performs in relation to those activities. It is the work performed, influence exercised or control held by the Audited Party that determines the relevant audit scope, not the Audited Party's job title, business description or contractual label.

| Role / activity type | Indicative description | |
|---|---|---|
| **Operator** | A business or person that... | ...uses, has control over, or is responsible for trucks or buses (GVM ≥ 4.5t). |
| **Employer** | | ...employs heavy vehicle drivers |
| **Prime Contractor** | | ...engages self-employed heavy vehicle drivers |
| **Consignor** | | ...arranges, requests or influences the transport of goods by road. |
| **Consignee** | | ...receives goods unloaded from heavy vehicles. |
| **Loader** | | ...loads, supervises loading, manages loading activities or controls premises where loading occurs. |
| **Unloader** | | ...unloads, supervises unloading, manages unloading activities or controls premises where unloading occurs. |
| **Loading Manager** | | ...is responsible for, or manages a site, where more than 5 heavy vehicles are loaded / unloaded each day. |
| **Scheduler** | | ...schedules transport tasks, delivery windows, driver work or vehicle use. |
| **Packer** | | ...packs, prepares, palletises or otherwise prepares goods for transport, including in containers. |
| **Specialised activity** | A business involved in specialised or higher-risk activities such as containers, livestock, dangerous goods, OSOM, construction, recovery or passenger transport. These activities may also relate to other Registered Industry Codes of Practice. | |

Where there is any conflict with the above representation of the different roles / activity types and any legal definition, the legal definition must be referred to.

An Audited Party may perform more than one role and participate in multiple specialised activities. Incorrect or incomplete identification of activities may result in an incomplete audit and may affect the reliability of the audit outcome.

All audit reports and certificates will reflect the audited site, the selected roles, and relevant industries with specialised activities.