

AUS & NZ

Lone & Remote Worker Safety BUYER'S GUIDE

How to choose and implement the right solution for your organisation

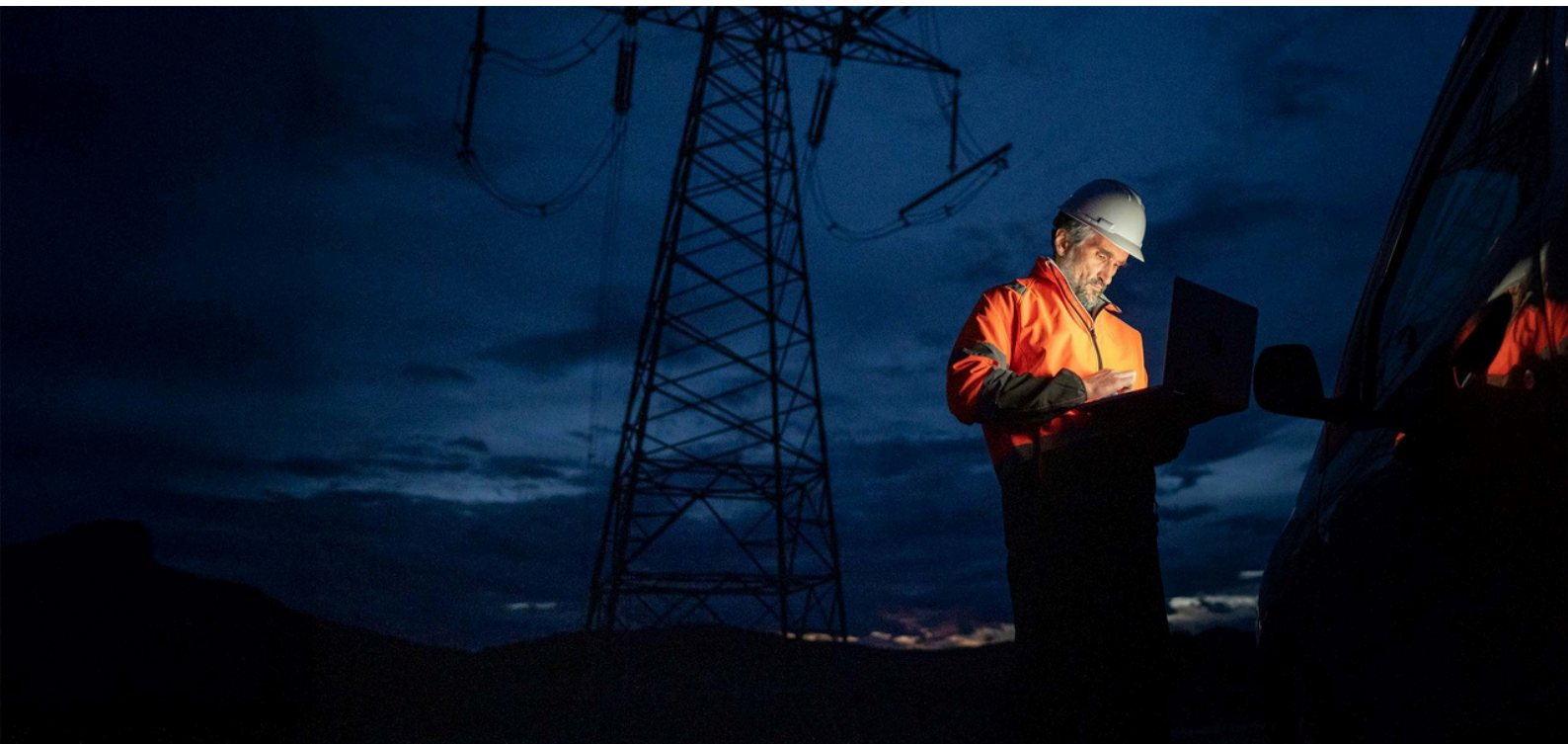


Table of Contents



01

Introduction

05

Vendor Evaluation

02

Know Your Risk Profile

06

Compliance Checklist

03

Solution Types Explained

07

Implementation Fundamentals

04

Which Solution Do I Need

08

Technology Glossary

01 INTRODUCTION

If you are responsible for people who work alone in the field, on the road, visiting clients, or in remote locations, this guide is for you.

Each year, serious injuries and fatalities occur when workers are isolated, travelling, or working without immediate support. In many of those cases, the organisation had a safety solution in place. The measures just didn't perform as expected under real conditions.

The question that matters

“Would our solution still work if something went seriously wrong?”

Most organisations ask: do we have a lone and remote worker safety solution? The harder question is whether it would actually work in a real emergency. Through coordinating incident responses, we see the same gaps appear repeatedly not failures of intent, but failures of design.



The Three Failure Modes

Through coordinating incident responses, we see the same gaps appear repeatedly not failures of intent, but failures of design.



Activation Failure

Falls, medical events, vehicle incidents and confrontations can leave a worker unable to press a button. Any solution relying entirely on manual activation has this gap.



Coverage Failure

Cell coverage fails in buildings, remote areas, and more often than organisations realise. A cellular device with no signal at the point of an incident is the same as no device.



Monitoring Failure

An alert sent to a colleague's phone, an unwatched portal, or an inbox that fills with spam is not monitored. The alert exists. The response doesn't.

Failure Mode

The worker couldn't activate an alert

Coverage dropped at the location of the incident

Alerts went to people who weren't monitoring

What this means in practice

Falls, medical events, vehicle incidents and confrontations can all leave a worker unable to press a button. Any solution that relies entirely on manual activation has this gap.

Cell coverage fails in buildings, remote areas, and more often than organisations realise during travel. A cellular device with no coverage at the point of an incident is the same as no device.

An alert sent to a colleague's phone, an unwatched portal, or an inbox that fills with spam is not monitored. The alert exists. The response doesn't.



Your Obligations | Plain English

This section is a practical interpretation of common regulatory expectations. It is not legal advice. Organisations should seek independent advice for their specific circumstances.

Under health and safety legislation in both Australia and New Zealand, directors and officers must exercise due diligence, not just to have a system in place, but to be satisfied it is fit for purpose. Regulators assess whether a system performed when it was needed, not whether it existed.

In practical terms this means being satisfied that your solution addresses all three failure modes above, not just one or two.

Test your current solution

Use these three questions as a sense-check before working through the rest of the guide. They are not about blame, they are about identifying gaps before an incident does.

Question	Answer	Gap to address
Can it work if the worker cannot activate it? Medical emergencies, falls, vehicle incidents, and confrontations can leave workers unable to press a button. <i>Consider: Does your solution include automated detection, fall detection, no-movement alerts, or scheduled welfare checks?</i>	☐ Yes ☐ No	Failure mode: Activation
Does it work everywhere your people actually go? Many incidents happen while travelling, inside buildings, or in areas with unreliable cellular coverage. <i>Consider: Do you know where your coverage gaps are, and does your solution account for them?</i>	☐ Yes ☐ No	Failure mode: Coverage

Question

Is someone actively monitoring alerts 24/7?

An alert is only useful if it is seen immediately and acted on by someone trained to respond.

Consider: If an alert triggered right now who would receive it, and would they be awake, trained, and able to act?

Answer

☐ Yes ☐ No

Gap to address

Failure mode:
Monitoring

Interpreting your answers

LOW RISK

3 Yes answers

Test regularly, and review as conditions change, exercise.

MODERATE RISK

2 Yes answers

Identifiable gaps that should be addressed.

HIGH RISK

1 or fewer

This is where most organisations sit when they first work through this exercise.



If you're unsure after working through this, that's normal. Most organisations are. That's exactly where we start
[CONTACT US FOR A COVERAGE RISK ASSESSMENT →](#)

Common misconception:

"We have coverage everywhere"

This is almost always false. Coverage maps show theoretical signal, not real-world performance at your workers' actual locations.



02 KNOW YOUR RISK PROFILE

The three failure modes don't affect all workers equally.

Before choosing a solution, you need to understand which gaps are most likely for your specific workforce and which would be most consequential if they appeared.



Factor	Key question	Which failure mode it drives
Coverage	Do your workers always have reliable cell coverage, or do they travel through gaps or work in areas with no coverage at all?	Coverage failure — a cellular device cannot send an alert it cannot transmit
Environment	Do workers face physical hazards (height, vehicles, rugged terrain) or risk from animals and/or other people?	Activation failure — physical injury or confrontation can make manual activation impossible
Worker type	How do your people move through their day — mobile, fixed-site, or genuinely remote?	Monitoring failure — isolated workers have no one nearby to notice when something goes wrong. Remote workers face greater risk due to longer response times and genuine isolation. Urban lone workers can also be at risk the general public rarely intervene in a confrontation.

Scenario

What this means

Solution direction

Always in reliable cell coverage

Cellular or app-based solution is viable

Cellular wearable or app

Sometimes out of cell coverage

The gap matters more than the percentage. If workers perform high-risk tasks outside coverage, even occasionally a cellular-only solution is not sufficient.

Assess the risk level of the gap, then decide

Frequently or always out of coverage

A cellular solution will fail at exactly the moment it is most needed

Satellite device required

Inside buildings with no cell signal

No cell coverage inside a building is the core issue. A cellular device may still transmit an alert ... with "Wearable pendant + external bridge system: The worker wears a device on their body that communicates via industrial grade radio link to a bridge placed outside the building which maintains a connection to the network (cellular or satellite), ensuring alerts are sent immediately. For large or multi-story buildings, consider indoor locator beacons to speed up locating the worker.

Satellite device required

Environment and worker type

Each row below maps a risk factor to the failure mode it creates and what the solution needs to address.

Risk factor	Failure mode created	What the solution must do
Working at height, vehicle operation, or physical injury risk	Activation — an incapacitated worker cannot press a button	Automated fall detection and no-movement alerts. The device must raise an alert without any action from the worker.
Rugged, wet, or physically demanding conditions	Coverage — a device that fails physically creates the same gap as one with no signal	IP65–67 rating minimum. SAR certified. Designed for field use, not office use.
Hazardous environments (gas, fuel, explosives)	Activation — a standard device may not function, or may cause ignition	Intrinsically safe (IS-rated) device. A legal requirement in some environments.
Low supervision night shifts, remote fixed sites, lone working in buildings	Monitoring — no one nearby to notice that something has gone wrong	Scheduled welfare check-ins and automated no-movement detection. Professional 24/7 monitoring.

Most organisations have more than one risk profile

Map your worker groups before selecting any technology. A field technician, a social worker on home visits, and a remote infrastructure worker may each expose a different failure mode and require a different solution.



03 SOLUTIONS EXPLAINED

There are four solution categories. There are primary device types; the fourth, bodycams, is an emerging complement, not a standalone solution. Each addresses the three failure modes differently. Understanding where each one falls short is as important as understanding what it does well.

Organisations can also choose between purchasing components separately (device, monitoring, platform) or procuring a complete integrated system. That decision is covered at the end of this section.

	App-based Smartphone + App - Cell / WiFi	Cellular wearable Dedicated device + cell	Satellite device Dedicated device + Iridium
Failure mode 1: if the worker can't activate an alert	Automated detection rarely available	✓ Fall detection + no-movement on quality devices	✓ Fall detection + no-movement on quality devices
Failure mode 2: if coverage drops	✗ No cell coverage = no signal	✗ No cell coverage = no signal	✓ Works anywhere with sky view
Failure mode 3: if nobody is monitoring	Difficult – app compliance is hard to verify; alert delivery via SMS/email is unreliable	Supported – requires graded monitoring station with API integration	Supported – requires graded monitoring station with API integration
Works inside buildings	Limited	Yes, with 1–3 min polling rate	No – needs sky view; bridge + pendant required

	App-based	Cellular wearable	Satellite device
	Smartphone + App - Cell / WiFi	Dedicated device + cell	Dedicated device + Iridium
Compliance and audit trail	Difficult to verify	✓ Automatic device logging	✓ Automatic device logging
Hardware cost	Low — uses existing phone	Medium	Medium to high
Best suited for	Lower-risk, urban workers where all three failure modes are low probability	Mobile workers with reliable cell coverage and moderate-to-high risk	Remote or high-consequence work where coverage failure cannot be accepted



Want to see how your current system performs against these criteria?
[**ASK FOR A FAILURE MODE AUDIT →**](#)

App-based: which failure modes it creates

Activation failure: the app must be launched by the worker before each shift. If it isn't, there is no protection. Compliance is almost impossible to verify at scale.

Coverage failure: GPS tracking drains battery approximately 30% faster, more on older devices. A flat battery creates the same gap as no coverage.

Activation failure: in a confrontation, there is unlikely to be time to unlock a phone, open the app, and activate an SOS. A phone is also the first thing an attacker will demand or disable. A dedicated wearable device is significantly harder to neutralise.

Coverage failure: iOS and Android updates can break app functionality without warning, silently removing protection until someone notices. Hardware variation also creates uneven coverage, different phone models have different antenna quality, so one device may receive a signal where another does not.



Cellular wearables: what the specs mean

These specifications map directly to the three failure modes. An undersized spec in any row creates a gap.

Specification	What to look for	Which failure mode it addresses
Automated detection	Fall detection, no-movement alerts, and scheduled welfare checks all active and configured	Activation — the device raises an alert without the worker doing anything
Polling rate (standard)	1–3 min location update during normal operation	Coverage — a recent breadcrumb trail is the only way to locate a worker who has entered a building and GPS has been lost
Polling rate (in alarm)	Continuous or significantly faster location updates once an alert is triggered. Ask specifically: does it just send location when in alarm, or does it increase tracking frequency?	Coverage — if a worker is running or being driven after triggering an alert, a standard 3-minute poll is not sufficient to track their movement
Location accuracy	+/- 5m minimum	Coverage — location accuracy determines whether responders can find the worker at a specific spot, not just in a general area
Battery life	15+ hours at the intended polling rate not standby time	Coverage — a dead device in the field is the same as no device
IP rating	IP65 minimum; IP67 preferred	Coverage — a device that fails physically creates the same gap as one with no signal
Network	4G LTE hardware. Not just SIM type. 3G is decommissioned in AU and NZ. 5G offers no advantage for lone worker safety and increases power consumption. No current lone worker devices operate on 5G.	Coverage. A device without true 4G LTE hardware will fail in the field.

Specification	What to look for	Which failure mode it addresses
SAR certification	NATA-approved test lab certificate	Not a failure mode — a worker safety and regulatory compliance requirement. Not all devices sold in NZ/AU meet this standard.
Two-way voice	Auto-answer on incoming call is the preferred configuration the monitoring station calls the device and it answers automatically. Auto-dial (device calls out) is an alternative but risks call queues, voicemail, and the call not being answered. Hands-free essential. Some devices support one-way voice (monitoring station can hear but worker cannot hear operator) which can be useful to avoid escalating a confrontation.	Monitoring — the operator can speak with or listen in to the worker without the worker needing to initiate. Call recording by the monitoring station provides evidence in legal proceedings and training. Hands-free keeps the worker's attention on safety, not the device. A good operator providing updates on how far away Emergency Services are is a genuine comfort in a real incident.

Satellite: the Iridium question

Satellite addresses failure mode 2 (coverage) completely. It does not automatically address failure modes 1 or 3 those still require automated detection and professional monitoring.

Coverage: the only satellite network with true global coverage and message-forwarding technology is Iridium. If a device does not use Iridium, ask specifically what gaps exist and what happens when a message fails to transmit.

Activation: automated detection capabilities vary significantly between satellite devices. Some include automated fall and no-motion detection; others support automated welfare checks and geo-fence entry/exit alerts. Confirm which detection features are active and configured on any device you consider, not just listed as available.

Two-way communication: two-way messaging is available on quality satellite devices. Two-way communication is a requirement under HSWA in both NZ and AU: 'effective means of communication must be in place.' Confirm this is supported and tested.

Monitoring: a satellite alert still needs someone to receive and act on it. The same graded monitoring station requirement applies as for cellular devices.

Bridge + pendant: for work inside buildings without cell coverage, a pendant worn by the worker connects to a hub outside or in the vehicle, transmitting via satellite. Pendant frequency must be 915–928 MHz (legal range for NZ/AU). Confirm that the pendant's location is transmitted separately from the hub's location if only the hub GPS is sent, responders are directed to the vehicle, not to the worker inside the building.

Emerging Technology:

Satellite Networks and the Fringe Cover Problem

A critical and underappreciated coverage risk is what happens at the fringe: one bar of signal that is not enough to make a call or send a text, but enough to prevent a device from switching to satellite mode. In that scenario, the worker has no options. This is a real-world gap, not a theoretical one.

Emerging satellite networks (Direct-to-Cell)

New satellite-to-mobile technologies — including Starlink Direct-to-Cell and AST SpaceMobile aim to allow standard mobile phones to connect directly to satellites.

As of 2026:

- Limited to SMS and low-bandwidth messaging in select regions
- Latency and reliability vary significantly
- No integration with dedicated lone worker safety devices
- No established track record in emergency response scenarios
- Starlink is still awaiting regulatory approval to launch a second-generation constellation capable of harnessing additional radio spectrum; phone manufacturers also need to update chipsets to support it
- Current bandwidth constraints make these technologies unsuitable for critical safety use



What this means in practice:

These technologies may reduce some coverage gaps in future. They do not currently replace purpose-built satellite safety devices. They should be treated as a supplementary layer, not a primary safety control.

Procurement guidance:

Ask vendors whether their solution relies on emerging satellite networks. Confirm what happens when messages fail or are delayed. Do not assume coverage equals reliability in an emergency context.

Consideration	Detail
When relevant	Workers who face confrontation or aggression risk: social workers, healthcare, parking enforcement, frontline retail, and security. Best deployed alongside a primary lone worker device.
What they address	Confrontation deterrence. Evidence collection. Live streaming to a monitoring station (device-dependent).
What they don't address	Activation failure: a bodycam does not raise an alert. Coverage failure: a bodycam does not transmit location. A primary device is still required.
Privacy obligations	Significant. Workers and members of the public must be informed. Recording policies must comply with the Privacy Act in both NZ and AU. Review with legal counsel before deploying.
Practical limitations	Battery life is typically 8–12 hours. Storage and footage management require a defined policy. Device selection, positioning, and activation protocols must be trained.

Bodycam deployment requires a standalone policy

Before deploying bodycams, document: when recording is active, how footage is stored and accessed, who can review it, how long it is retained, and how workers and members of the public are notified. This is a separate document from your lone worker safety policy.

Complete systems vs. component purchasing

Organisations have two broad approaches to building a lone worker safety solution.

Approach	What it means	Considerations
Complete integrated system	A single vendor supplies the device, monitoring platform, response centre, and reporting as a managed service. One contract, one point of accountability. Note: SIM and network costs are typically included in the managed service fee confirm this is the case and what is covered.	Benefits: simpler procurement, integrated reporting, single point of accountability for incidents. The vendor owns the end-to-end performance of the solution. Risks: vendor lock-in, migration complexity if you change providers. Evaluate contract exit terms carefully.
Component purchasing	Device from one vendor, monitoring from another, platform integration managed separately. The network (SIM and data) would need to be purchased direct by the customer from a network provider.	Benefits: flexibility to use best-in-class components, easier to switch individual elements. Risks: integration gaps between components can create failure modes of their own. Who is accountable if a device raises an alert that the monitoring platform doesn't receive? Establish this contractually before going live. An internal resource will also be required to manage all suppliers, bills, and services across the solution.

The accountability question

Whether you choose a complete system or component approach, establish in writing who is responsible if an alert is raised and not acted on. In a component model, this requires explicit contract language with each vendor. In a complete system, it is typically the provider's responsibility to confirm this is stated in the agreement.

04 WHICH SOLUTION DO I NEED?

Most organisations get this wrong: here's why

The most common mistake is choosing a solution based on what workers do most of the time, not on what they do when they're most at risk. A worker who spends 90% of their day in reliable cellular coverage and 10% in a remote location still needs a solution that works in that 10% because that's often exactly when something goes wrong.

Work through the flowchart below for each worker group in your organisation. Different roles may point to different solutions.



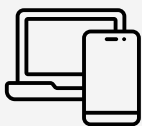
Monitoring

24/7 graded station · API · response



Network

cellular · satellite · fringe coverage



Device

hardware · fall detection · IP rating

A gap in any one layer is the same as no solution.



GUARDIAN ANGEL SAFETY
Safety when it matters most

CONTACT US

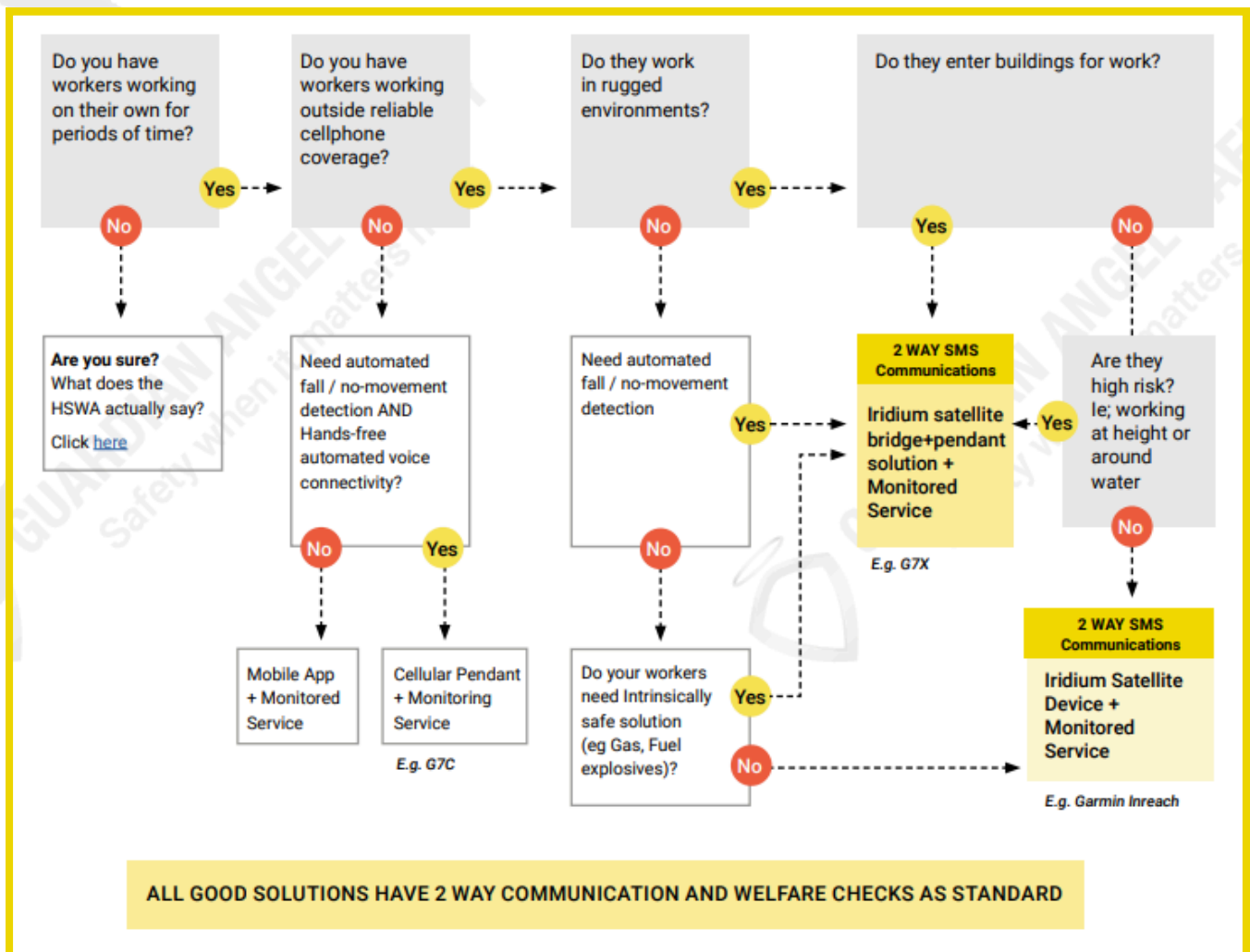


Reading this chart

Start at the left: Do your workers work alone for periods of time?

Follow the Yes/No branches through coverage, environment, and risk factors.

Most organisations will find different worker groups land in different places; more than one solution may be required.



ALL GOOD SOLUTIONS HAVE 2 WAY COMMUNICATION AND WELFARE CHECKS AS STANDARD

05 VENDOR EVALUATION

Once you know which solution type you need, use these questions to assess vendors. Vague or evasive answers are a red flag.

Key questions to ask

Area	Ask this	A strong answer looks like...
Device quality	What is the IP rating? Can you provide a SAR certificate from a NATA-approved test lab? Is the device certified for intrinsically safe (IS) environments where required?	IP65–67 confirmed. SAR certificate provided on request, not just claimed.
Network	Is this a true 4G LTE hardware device? Will it work after 2G/3G decommissioning?	Hardware generation confirmed, not just SIM type. 3G is already decommissioned in AU and NZ.
Automated detection	What triggers an alert without the worker activating it?	Fall detection, no-movement/man-down, and scheduled welfare checks all specified clearly and confirmed as active by default.
Polling rate	What is the polling rate in normal operation? What happens when an alert is triggered – does tracking frequency increase?	1–3 min standard. Faster polling confirmed in alarm mode so a mobile worker can be tracked if running or being driven. Minimum +/- 5m location accuracy.
Battery life	What is battery life at a 1–3 minute polling rate?	15+ hours at the intended polling rate – not standby time.

Area	Ask this	A strong answer looks like...
Configuration	Can device settings be updated over the air? Can detection thresholds be adjusted?	Yes - tilt angles, polling rate, and detection thresholds all adjustable remotely.
Two-way voice	Does the device auto-answer incoming calls from the monitoring station, or does it auto-dial out? Is call recording standard? Is one-way voice available?	Auto-answer on incoming call is the stronger configuration — avoids call queues and voicemail. Call recording confirmed as standard. Hands-free operation confirmed.
Monitoring station	Is the centre graded or ISO certified? Is it staffed 24/7 with dedicated response software? What are the business continuity arrangements? How often are operators trained? Is there a schedule for regular internal or external audits to verify procedures and compliance?	Graded centre confirmed. Purpose-built response software, not a watched portal. Multiple redundant providers for internet, phones and power. Backup centre available if the building must be evacuated. Operator training schedule documented. Audits conducted regularly to ensure compliance and effectiveness, with records available for review.
Emergency Services	In Australia, do you hold an Alpha Code?	Alpha Code confirmed for AU operations.
Data and privacy	Where is data stored? Who has access? How are breaches handled?	Data residency stated. Privacy policy addresses NZ Privacy Act 2020 and AU Privacy Act 1988.
Device longevity	Where is the device manufactured? What are the warranty terms? What is the vendor's roadmap for this device?	Clear warranty terms stated. Vendor demonstrates ongoing investment in the platform — not a device that risks becoming unsupported and unreplaceable (an 'orphan product').
Cyber security	How is the platform secured? Where is data hosted? What is the process for a data breach?	Documented security model for the cloud platform. Data hosted in NZ or AU, or with explicit data residency confirmation. Breach notification process compliant with local Privacy Act requirements.

Red flags



Cannot provide a SAR certificate, or says one 'isn't required'



Pricing quoted as device cost only, with no transparency on monitoring, data, or ongoing fees



Monitoring described as 'someone watches the portal' not dedicated response software



Cannot specify which automated detection features are active by default vs. requiring manual configuration



After-hours alerts route to a mobile phone



Cannot provide warranty terms or a clear answer on how long the device line will be supported, a risk of ending up with an orphan product that cannot be updated or replaced



Critical alerts delivered by SMS or email only, both are vulnerable to spam filters and delays



Monitoring station cannot document business continuity arrangements: redundant internet, phones, power, and a backup centre



Cannot confirm 4G LTE hardware, only SIM type



Device polling rate in alarm is the same as normal operation; location is only sent on activation, not continuously



If any of these sound familiar

[CONTACT US BEFORE YOUR NEXT RENEWAL →](#)



GUARDIAN ANGEL SAFETY
Safety when it matters most

CONTACT US



Total cost of ownership

Cost component	Notes
Device purchase or lease	Compare outright vs lease. Leasing shifts replacement cost to the vendor but may include lock-in.
SIM / data plan	Cellular devices require a SIM. Satellite devices charge per message high polling rates increase cost significantly.
Monitoring station fees	Typically a monthly per-device fee. Confirm what is included: 24/7 staffing, Emergency Services liaison, reporting. Confirm if unlimited alerts are included or if there are extra charges for high volumes.
Platform / portal access	Some vendors charge separately for reporting, API integration, or portal access.
Training	Initial and ongoing. Ask whether this is included or billed separately.
Device replacement	What is the expected device lifespan? What are the terms if a device fails in the field?
Ongoing Support and Maintenance	Check what's included: Support helpdesk / ticketing system availability to flag hardware and platform support and service level agreements (SLA). Ask whether this is included in the cost or billed separately.



06 COMPLIANCE CHECKLIST

Compliance with health and safety legislation is a floor, not a ceiling. Meeting the legal minimum does not mean your solution will perform when it is needed. This section covers both your legal obligations, and the practical test that sits above them.

The fit-for-purpose test

Following a serious incident, regulators ask one central question: did the organisation take reasonably practicable steps to prevent this? A system that existed but relied solely on manual activation, failed in the location of the incident, or was not actively monitored is likely to be found insufficient even if it appeared compliant on paper.

Use these three questions as your primary compliance test before turning to the legislation tables below.

Question: failure mode

Can it work if the worker cannot activate it? Failure mode: Activation

Does it work everywhere your people actually go? Failure mode: Coverage

Is someone actively monitoring alerts 24/7? Failure mode: Monitoring

What compliance looks like in practice

This looks like: automated detection. fall detection, no-movement alerts, or scheduled welfare checks — is configured and tested.
A gap exists when: the solution relies entirely on the worker pressing a button.

This looks like: coverage has been mapped against actual working locations, and gaps have been addressed by the solution design.
A gap exists when: coverage gaps are known but accepted without mitigation.

This looks like: a graded monitoring station with dedicated response software and documented business continuity receives alerts via API.
A gap exists when: alerts go to a staff member's phone or a portal that requires someone to be watching it.

Legislative obligations

The tables below summarise the primary obligations under health and safety and privacy legislation in both countries. This is a practical reference not legal advice.

H&S obligation	New Zealand (HSWA 2015)	Australia (Model WHS Act)
Duty to manage risk	PCBUs must eliminate or minimise risks so far as is reasonably practicable	Same duty under the Model WHS Act adopted in most states and territories
Officer due diligence	Officers must take reasonable steps to ensure the organisation meets its duties — including verifying that controls are effective	Same obligation under Model WHS Act s.27. Personal liability applies.
Fit for purpose test	WorkSafe assesses whether controls were reasonably practicable — not just whether they existed	Same test. Regulators have prosecuted organisations where systems existed but failed in practice.
Lone and remote worker obligations	PCBUs must identify risks specific to lone and remote work and implement controls. HSWA 2015 and the Health and Safety at Work (General Risk and Workplace Management) Regulations 2016 require that an effective means of communication is in place for isolated or remote workers. Workers must be able to summon assistance in an emergency. A monitoring system must be established where workers are working alone in circumstances that may put them at risk.	Same obligation under the Model WHS Act and WHS Regulations. Regulation 48 (Remote or isolated work) requires PCBUs to manage risks of remote or isolated work, including ensuring an effective means of communication is available. Workers must be able to call for assistance at any time. The PCBU must prepare, maintain and implement a system for monitoring the health and safety of workers who are working remotely or in isolation.

Privacy obligation

Inform workers

New Zealand (Privacy Act 2020)

Workers must be told that location data is collected and for what purpose

Limit data use

Data collected for safety purposes cannot be used for other purposes (e.g. performance monitoring) without separate consent

Breach notification

Mandatory notification to the Privacy Commissioner and affected individuals for serious breaches

Vendor obligations

Your vendor must also comply. Confirm data residency, access controls, and breach procedures.

Australia (Privacy Act 1988)

Same requirement under the Australian Privacy Principles (APPs)

Same under APP 6

Mandatory notification under the Notifiable Data Breaches scheme

Same. Confirm vendor holds a current Privacy Policy and can demonstrate compliance.



Before you go live - checklist

Grouped by what matters most. The first group is the fit-for-purpose test. The second is the legal and administrative minimum.

Item	Done
Will it actually work? – the three failure modes	
Activation failure addressed – automated detection configured and tested: fall detection, no-movement alerts, or welfare check-ins active	☐
Coverage failure addressed – coverage mapped against actual working locations, gaps identified and designed around	☐
Monitoring failure addressed – 24/7 graded monitoring station confirmed with dedicated response software, not a watched portal or a mobile phone	☐
All three tested together: full alert path tested end-to-end: device → monitoring station → Emergency Services, in real operating conditions	☐
Legal and administrative requirements	
Workers informed in writing of location monitoring and its purpose	☐
Privacy policy updated to reflect location data collection	☐
Data use formally limited to safety purposes and documented	☐
Vendor data residency and breach procedures confirmed in writing	☐
Officer-level sign-off on solution design and risk assessment obtained	☐
Incident response procedure documented and distributed to relevant staff	☐
Regular review schedule established (minimum annually)	☐

07 IMPLEMENTATION FUNDAMENTALS

Most implementations fail quietly not with a dramatic breakdown, but with a slow drift away from the conditions that made the solution work on day one. Coverage changes. Roles change. Devices go unconfigured. Nobody tests the alert path after the first week. The steps below are ordered by where we most commonly see things go wrong.

Phase	Action	Action
Map	Identify all worker groups and risk profiles before selecting any technology	All three — a solution chosen before workers are mapped will have activation, coverage, or monitoring gaps that only become visible in a real incident.
Select	Use the decision flowchart in Section 4. Pilot with a small group in actual working locations before full rollout.	All three — a solution chosen before workers are mapped will have activation, coverage, or monitoring gaps that only become visible in a real incident.
Configure	Set polling rates, detection thresholds, and monitoring contacts before devices leave the building	Activation — a device issued with default settings may not trigger an automated alert. Coverage — an unchecked polling rate creates a location gap.
Inform	Tell workers what data is collected, why, and how it will be used. Get written acknowledgement.	Monitoring — workers who understand the system are more likely to report when something isn't working, before a gap becomes an incident.
Train	Train workers on device use. Train alert-recipients separately on response procedures.	Monitoring — alerts going to people who aren't actively monitoring is almost always a training gap, not a technology gap.



Phase	Action	Action
Test	Test the full alert path, device to monitoring station to Emergency Services, before going live. Then test again in six months.	All three failure modes. This is the only step that confirms activation detection works, coverage is real, and monitoring is actually active. It is the only way to answer: would it still work if something went seriously wrong?
Review	Review coverage, incident history, and device performance at least annually	All three, coverage changes, roles change, monitoring arrangements lapse. A solution that addressed all three failure modes last year may not today.

Ongoing review triggers

Trigger	What to check
Annually (minimum)	All three failure modes: automated detection still active and configured; coverage still appropriate; monitoring confirmed active. Privacy policy and alert path up to date.
When worker roles or locations change	Activation and coverage: does the new role or location expose a different failure mode? Are detection thresholds and coverage still appropriate?
After any incident or near-miss	Which failure mode appeared: activation (worker couldn't trigger or was triggered too late), coverage (signal or location gap), or monitoring (alert not seen or acted on)?
After a phone OS update (app-based)	Coverage and activation: iOS and Android updates frequently break app functionality, silently removing protection until someone notices.
When network changes occur	Coverage: confirm device compatibility. 3G is now decommissioned in both NZ and AU; 4G LTE hardware is required.

“Would our solution still work if something went seriously wrong?”

If you can answer yes with confidence, automated detection active, coverage gaps addressed, 24/7 monitoring in place, and the full alert path tested in real conditions, you're in a strong position.

If you can't, that's where we start.

 AUS (07) 4800 0011

 NZ 09-886 7075

 info@guardianangelsafety.co



08 TECHNOLOGY GLOSSARY

A reference guide to the technical terms used in this guide and in lone worker safety conversations generally. Terms are listed alphabetically.

Term	What it means
4G LTE	Fourth-generation mobile network standard. The current baseline for lone worker devices. 'LTE' (Long Term Evolution) is the technical specification. Important distinction: a 4G SIM in a 2G or 3G hardware device is not a 4G device. Ask vendors to confirm hardware generation, not just SIM type.
5G	A code issued by Australian emergency services that allows monitoring stations to identify themselves as professional operators when calling 000. Monitoring stations holding an Alpha Code receive priority handling. Relevant in vendor evaluation for Australian operations. Important: only Australian-based monitoring stations are eligible for an Alpha Code, overseas-based stations cannot obtain one. Confirm the monitoring station is Australian-based if Alpha Code priority handling is required.
API integration	Application Programming Interface integration. A technical connection that allows a lone worker device platform to send alerts directly to a monitoring station's response software, rather than via SMS or email. API integration is more reliable and faster. The preferred standard for professional monitoring.
Bridge + pendant	A configuration for indoor satellite use. A pendant worn by the worker transmits a short-range radio signal to a hub (the bridge) placed outside the building or in a vehicle, which then transmits via satellite. Required when workers are inside buildings without cell coverage. Pendant frequency must be 915–928 MHz in NZ and AU. Confirm that the pendant's own location is transmitted separately from the hub's GPS location — if only the hub location is reported, emergency responders will be directed to the vehicle or building entrance, not to where the worker is inside.
Cellular wearable	A dedicated wearable safety device that transmits via mobile cell networks. Also referred to as a lone worker device or satellite device (when satellite-capable). Distinct from app-based solutions in that the device is purpose-built for lone worker safety and does not rely on a smartphone.

Term

What it means

Fall detection

An automated feature that detects a sudden change in movement consistent with a fall and raises an alert without the worker activating anything. Typically uses accelerometer data. Sensitivity and tilt thresholds are configurable on quality devices. Not all fall detection implementations are equally reliable, ask vendors for false positive and false negative rates.

Geo-fence

A virtual boundary defined in the monitoring platform. When a worker's device crosses the boundary (entering or exiting), an alert or notification is triggered. Used for site access monitoring and remote location management.

GPS

Global Positioning System. A satellite-based navigation system operated by the US military and available for civilian use. Provides location coordinates via signals from a constellation of GPS satellites. Accurate outdoors with clear sky view; degrades or fails inside buildings, underground, and in dense urban canyons. Most lone worker devices use GPS for location tracking.

HSWA

Health and Safety at Work Act. New Zealand's primary workplace health and safety legislation, enacted in 2015. Places duties on PCBUs and officers to manage risk so far as is reasonably practicable. The equivalent legislation in most Australian states and territories is the Model WHS Act.

IP rating

Ingress Protection rating. A two-digit standard (IEC 60529) that rates a device's resistance to solids and liquids. The first digit rates dust resistance (6 = dust-tight). The second rates water resistance (5 = water-jet resistant, 7 = immersion up to 1m). IP65 is the minimum standard for field-use lone worker devices. IP67 is preferred for wet or submersion-risk environments.

Iridium

A satellite network operated by Iridium Communications Inc. The only satellite network with true global coverage, including polar regions. Uses a constellation of 66 low-earth-orbit satellites. Uniquely offers message-forwarding technology: if a message cannot be immediately received, the network retries until a satellite picks it up. The standard network for professional satellite lone worker devices.

IS-rated (Intrinsically Safe)

Intrinsically Safe certification. Indicates a device has been certified safe for use in environments where flammable gases, vapours, or dusts are present. Standard electronic devices can cause ignition in these environments. IS certification is a legal requirement in certain hazardous industries. Lone worker devices used in oil and gas, mining, or chemical environments must carry IS certification.

Term

What it means

Man-down / no-movement detection

An automated alert triggered when a device detects no significant movement for a defined period. Distinct from fall detection: man-down detects inactivity rather than a sudden impact. Useful for medical events, unconsciousness, or situations where the worker is incapacitated without a fall. Detection window and sensitivity are configurable on quality devices.

Monitoring station (graded)

A professional alarm receiving centre (ARC) that monitors lone worker alerts and coordinates responses. A graded centre has been assessed against a recognised standard (such as NZS 4517 in NZ or AS 2201.2 in AU) for physical security, staffing, technology, and business continuity. Grading is the professional standard — not all monitoring services are graded.

NATA

Person Conducting a Business or Undertaking. The legal entity that carries primary health and safety duties under HSWA (NZ) and the Model WHS Act (AU). In practice, this is usually the employing organisation. PCBUs must eliminate or minimise risks to workers so far as is reasonably practicable.

Polling rate

The frequency at which a lone worker device reports its location to the monitoring platform. A 1–3 minute polling rate means the platform receives a location update every 1–3 minutes. A faster polling rate produces a more accurate breadcrumb trail but drains battery faster and increases data costs on satellite devices. Always ask vendors to quote battery life at your intended polling rate, not standby time.

SAR certification

Specific Absorption Rate certification. SAR measures the rate at which the human body absorbs radio frequency energy from a device. A SAR certificate from a NATA-approved lab confirms the device meets safe radiation exposure limits. Not all devices sold in NZ and AU carry this certification. It is a worker safety requirement, not just a regulatory checkbox.

Satellite device

A lone worker device that transmits via satellite rather than (or in addition to) cellular networks. Provides coverage in areas with no cell network. Quality satellite lone worker devices use the Iridium network. Satellite transmission has higher latency than cellular and higher per-message data costs.

Term

What it means

Starlink

A low-earth-orbit satellite internet service operated by SpaceX. As of 2026, Starlink is not used as a transmission network for lone worker safety devices. It provides broadband internet rather than the low-bandwidth message delivery used by Iridium. This may change as the technology evolves — monitor vendor claims carefully.

Two-way voice

A feature that allows a monitoring station operator to initiate a call to a lone worker device, or to listen to the device's environment, without the worker needing to initiate anything. Auto-answer on incoming call is the preferred configuration — the operator calls the device and it answers automatically, avoiding call queues and voicemail. Auto-dial (device calls out) is an alternative but risks the call being lost in phone system loops. Some devices support one-way voice, where the monitoring station can hear the worker but the worker cannot hear the operator — useful in confrontation scenarios where operator noise might escalate the situation, while still allowing the worker to hold the device to their ear if it is safe. Call recording by the monitoring station provides evidence in legal proceedings and for training. Hands-free operation is essential — it allows the worker to focus on safety without holding a device. Two-way communication is a requirement under HSWA in both NZ and AU.

Welfare check-in

A scheduled, automated prompt sent to a worker at defined intervals, requiring a response to confirm they are safe. If the worker does not respond within a defined window, an alert is raised. Addresses the monitoring failure mode for low-supervision environments. Interval and response window are configurable.

