Business Leaders' Health & Safety Forum

ZERO HARM WORKPLACES

CEO Guide to Risk

WHAT GOOD LOOKS LIKE

Examples of Health & Safety Risk Management Tools

What others do

This guide provides examples of useful health and safety risk management tools.

These examples draw on international good practice and the experience of Forum members.

They are not exhaustive and are not meant to be prescriptive.

Their purpose is to share good practice to enable leaders to learn from each other.

They cover the following health and safety risk management tools:

Bow ties | Risk profile | Risk management policy | Risk assessment | Risk assurance

WHAT MATTERS

RISK | RELATIONSHIPS | RESOURCES

Bow tie method

This is an example of a risk analysis methodology called the 'bow tie'.

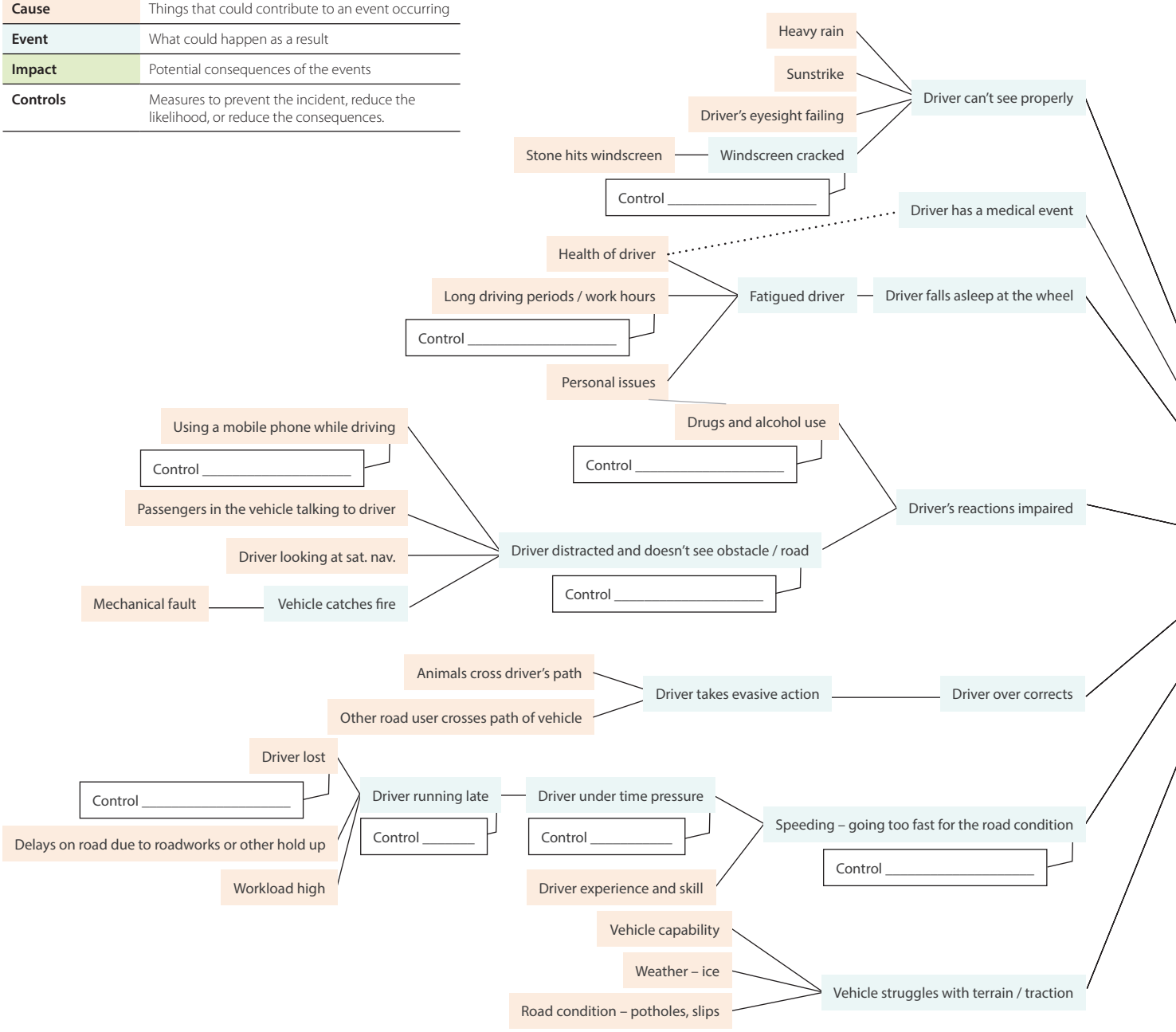
The bow tie helps you see where you have strong controls, where you might be over-controlled, and where you need to focus your attention.

You can use it to create a high-level picture of all the risks in your business. Or you can use it to detail all the risk controls needed for a particular work activity.

It can also help you check that the 'hierarchy of controls' has been used to ensure workers have the highest level of protection *(First try to eliminate the risk; second try to minimise it; lastly look at administrative controls like PPE, training etc).*

Key:

Cause	Things that could contribute to an event occurring
Event	What could happen as a result
Impact	Potential consequences of the events
Controls	Measures to prevent the incident, reduce the likelihood, or reduce the consequences.

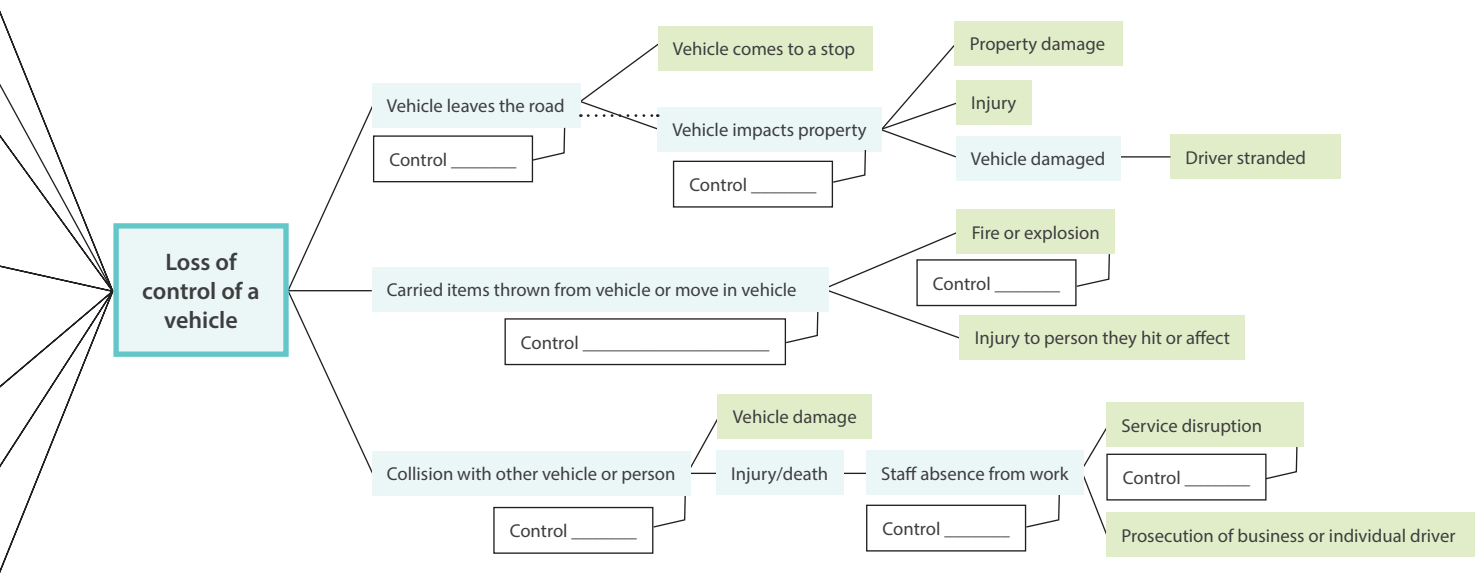


Risk velocity:

Measures how fast an incident goes from cause to impact. Understanding risk velocity is important because it affects the balance of controls you need to put in place. If the impact of an event will happen fast you need more prevention controls. If the impacts will take longer to occur you can make more use of controls aimed at preventing and reducing consequences

Loss of control while driving

- Below is an example of how a bow tie could be used to identify risks and controls related to driving.
- The bow tie identifies potential *events* that can occur while driving, along with their potential *causes* and *impacts*. Identifying the events, causes and impacts helps you think about all the *controls* you can put in place.
- **To keep things simple this example doesn't include the controls.** There are a lot of them and what's appropriate will depend on circumstances. But it provides prompts in key places where you might want to insert controls.
- Controls on the left hand side of the diagram aim to *prevent* or *reduce the likelihood* of an event. Controls on the right aim to help *reduce the impact* and help you *recover faster*.
- This bow tie was used to populate the Risk Profile on pages 4/5.



Risk Profile

This is a way for critical risk information to be presented to you, in a way that is relevant for your position and broad span of control. It has been populated following the completion of a bow tie analysis.

The profile contains information to enable you to interrogate the management of the risk, to ensure consistency in standards and approach across the business, and to understand the performance of the business in respect of this risk. It enables you to have a conversation with the business and with your Board about specific critical risks, as part of good management and due diligence.

There will be additional layers of detail that sit beneath this risk profile that are owned by your direct reports, managers, front line supervisors and staff. That information (risk assessments, task analysis, job safety analysis) will ensure the understanding and management of this risk is relevant to the specific activities and tasks undertaken through the layers of your business. That information should align with the information you are provided with in a risk profile like the one presented here.

Driving

Risk description *(Definition of this risk, who is exposed, where and when exposure occurs)*	• There's a risk people could be harmed while driving to and from work, to jobs and meetings, and to site visits. Drives can be long because we are based in Timaru and cover a large region. People also occasionally drive to places like ports and commercial sites, off-road in rural areas, and in places with extreme temperature fluctuations, ice, snow and sunstrike. • The driving therefore requires on and off-road capability, and involves the use of various types of vehicles. • Our people are also driven by others – including taxi drivers, stakeholders, and clients and workers of businesses we work with. • All staff who drive for work are exposed, particularly those who drive in remote locations or off-road.	**Inherent risk level**	**High**
What we know about this risk in our business	We've had 4 driving-related incidents in the past 5 years. These involved property damage and minor injury. Investigations indicated that fatigue was a key contributory factor.	**Residual risk level**	**High**
What we know about this risk in our operating environment	Driving is a known work-related risk. About 300 people are killed on NZ's roads every year. There are about 300 injuries per 100,000 of the population.	**Is this risk within tolerance**	**Yes**
Our business objectives potentially impacted by this risk	Deliver the service on time every time	**Our confidence in control**	**Moderate**
Risk owner	GM Operations		

Note, the information in the 4th column will relate to your company's risk matrix and risk tolerance process

Key risk event: Loss of control of a vehicle during a work activity

Causes	Potential consequence / Impacts
The following could lead to an event: • Distracted or impaired driver; driver speed; driver vision compromised by conditions • Mechanical fault; tyre blow out; fire or explosion in vehicle • A person or animal crosses driver's path causing an accident • Driver unable to handle vehicle or conditions, or vehicle not suitable for terrain.	Potential impacts: • Injury/death to driver or other person • Driver stranded; driver unable to work due to injury; service disruption • Vehicle damage; property damage • Prosecution; increased insurance costs; reputational damage.

Controls: How we manage this risk

Brief control description *(What's in place to manage the risk)*	Further information about control	Control in place and working?	Brief control description *(What's in place to manage the risk)*	Further information about control	Control in place and working?
Driving/working time restrictions, and break/rest and overnight requirements to manage fatigue risk	Fatigue Policy	**Yes**	Defensive and Advanced Driver Training provided to all drivers		**Yes**
Recruitment process asks if any health issues could impact ability to drive	Employment Relations Policy	**No**	First aid training provided to staff	Emergency Procedures	**No**
We visually check our vehicles before using them	Driving Policy	**Yes**	First aid kits in all vehicles and there is a process to maintain these		**Yes**
Purchase of safe fleet – ANCAP 5 Star plus vehicles for the terrain	Procurement Policy	**Partially**	We have a process to know where all our staff are so if anything happens we will know quickly and can send help	Lone/Remote worker Procedures	**Partially**
We have good relationships and discussions to ensure we are managing workloads, conflicts, health issues and fatigue	Employment Relations Policy	**No**	Commercial insurance required for all fleet and personal vehicles used for work	Insurance Policy	**No**
All vehicles have regular service and WoF	Asset Register	**Yes**	All tickets and fines investigated. Must be paid for by person who incurred them	Investigation Policy	**Yes**
All staff have hands-free kits and GPS		**Partially**	Vehicles have snow chains and drivers know how to use them	Driving Policy	**Yes**
We check the licences of all staff required to drive	NZTA check	**No**	Items in our vehicles are secured so they can't move in transit	Driving Policy/ Procurement Policy	**No**
We require drug and alcohol testing if there is an accident	Drug and Alcohol Policy	**Yes**	Vision tests are available for staff required to drive	Website	**Yes**
Staff assess weather, road conditions, site access needs, journey time and route prior to departing		**Yes**	Emergency assistance available through AA or equivalent	Driving Policy	**Yes**
Physical maps and GPS available to prevent staff getting lost		**No**	Fleet vehicles have warning triangles and high visibility vests in the boot, and water/food if travelling to remote areas	Driving Policy	**No**

Engagement and communication *How we've engaged people on this risk*	This risk assessment has been developed with our workers		
Additional resource need *(Equipment, processes, training, money etc)*	Additional support required for a 3-month term to undertake a review of assets, PPE and training	**Monitoring this risk**	• Service and maintenance performance • Number and dollar amount of property / vehicle damage claims • Number of traffic fines, along with incident learning outcomes

Risk Management Policy

Here is an example of a risk management policy for a fictional business, ABC Ltd. A risk management policy is a document that states your objectives and commitment to risk management. It explains why this is important to you, and what your expectations for risk management are. It outlines the roles and responsibilities and accountabilities for risk management at a high level – and can be used to communicate your intent and expectations clearly across the business.

The identification and effective management of *ABC Ltd* risks are a priority of the Board and the Audit and Risk Committee. This Risk Management Policy assists the Board in fulfilling its risk assurance and audit responsibilities.

Introduction

Risk management is a critical business discipline that reduces uncertainty in the achievement of business objectives, and strengthens and complements other corporate governance initiatives.

Effective management of risk is essential for us to achieve our goals and objectives and to satisfy key external stakeholder expectations.

Managing risk reduces uncertainty associated with business performance and gives us greater freedom to plan and use resources for innovation and measured risk taking.

Managing risk directly contributes to our profitability by reducing additional costs and assisting to improve certainty around revenue achievement.

Policy Statement

1. The approach to governance in *ABC Ltd* is set out in the Board and Board Committee Charters and related documents.
2. *ABC Ltd* is committed to proactively and consistently managing risk in order to:
   - enhance and protect *ABC Ltd*'s value by delivering on our commitments and meeting stakeholders' expectations;
   - allow *ABC Ltd* to pursue opportunities in an informed way and aligned with the Board's risk appetite; and
   - ensure a safe and secure environment for *ABC Ltd* people (employees and contractors), partners and customers.
3. A robust risk management framework is a valuable strategic tool. It enables *ABC Ltd* to proactively manage risk, by setting out disciplines that can be embedded in day-to-day business operations and decision-making processes.

Key concepts

4. ***Risk*** is anything that has the ability to impact on our ability to achieve *ABC Ltd*'s goals and objectives and is therefore interconnected with *ABC Ltd*'s business plan and strategy. Risk is assessed in terms of a combination of the impact and likelihood of an event occurring, and can be categorised according to the areas it could potentially impact. These are:
   - commercial/financial sustainability;
   - performance of core services;
   - stakeholder confidence/reputation;
   - preparedness to manage and respond to a crisis situation;
   - people safety and resource availability; and
   - regulatory/contractual.
5. ***Enterprise-wise risks*** are the key risks facing *ABC Ltd* and are identified and reviewed by the Audit and Risk Committee twice a year. The Board, through the Audit and Risk Committee, regularly monitors the executive's management of these enterprise-wise risks.
6. ***Risk appetite*** describes *ABC Ltd*'s tolerable levels of risk. It draws together risk metrics and risk management so they can be translated into everyday business decisions, reporting and discussions. Risk appetite is set by the Audit and Risk Committee and reviewed annually. It sets the boundaries which form a dynamic link between strategy, target setting and risk management.
7. ***Risk management*** is the process through which risk is managed and includes risk identification and reporting through to risk mitigation and allocating risk ownership.

Background

8. *ABC Ltd* is committed to ensuring rigorous risk management processes are in place.
9. To implement risk management effectively, it must be integrated into *ABC Ltd*'s business operations, projects and decision-making processes. It is part of our mindset and integral to the way we do things.

If *ABC Ltd* does not manage its risk effectively, this may result in shareholder dissatisfaction, loss of revenue or increased costs (including from investigations, litigation, penalties or damages), other loss of shareholder value, negative publicity, reputational damage, the potential loss of customers or injury to *ABC Ltd*'s people and partners.

Objectives

10. The key objectives of this policy are to:
    - Ensure that all *ABC Ltd* people are aware of their responsibility to manage risk.
    - Mandate one framework for the management of risk in *ABC Ltd*. Our framework:
      - ensures the Board sets the risk appetite and reviews the enterprise-wise risks annually;
      - integrates risk management in line with the Board's risk appetite into our structures, policies, processes and procedures; and
      - delivers regular enterprise wide risk review and monitoring.

- We will maintain and adhere to a risk management framework that ensures:
  - the risk management process is evident whenever key decisions are made;
  - risks are identified and evaluated;
  - effective responses and control activities are developed for these risks; and
  - there is appropriate monitoring and timely re-evaluation of risks.
- Ensure that the CEO and the executive team have discretion to select the approach they use to manage risk within the guidance provided in our framework.
- Mandate regular measurement and reporting on the efficiency and effectiveness of our risk management processes.
- Encourage balancing the level of control implemented to mitigate identified risks with our commitment to comply with external regulation and governance requirements and our value and growth aspirations.
- Meet or exceed IOD best practice standards for risk management processes and related governance.

Risk Management Framework

11. The objective of our risk management framework is to ensure we operate within our agreed risk tolerance and risk limits. We do this by the:
    - effective and efficient continuity of operations;
    - safeguarding of our assets;
    - preservation and enhancement of our reputation;
    - reliability of internal and external reporting;
    - compliance with applicable laws and regulations.

Creating and maintaining a culture consistent with our risk tolerance is an important element of operational risk management, as are our selection and recruitment processes.

Roles and Responsibilities

12. The roles and responsibilities in relation to this policy are as follows:

ABC Ltd Board of Directors

- Reviewing the effectiveness of the implementation of the risk management and internal control system.
- Promoting a culture of proactively managing risks, setting _ABC Ltd_'s risk appetite and reviewing _ABC Ltd_'s enterprise-wise risks annually.
- Through the Audit and Risk Committee, provides oversight and monitoring, including through receipt of regular reporting from management on our risks.

Chief Executive

- Promoting a culture of proactively managing risks, aligned with this policy and the Board's risk appetite.
- Reviewing _ABC Ltd_'s principal risks regularly and regularly reporting to the Audit and Risk Committee regarding that review and, at other times by exception, reporting on any changes to the rating of enterprise-wide risks.
- Monitoring of action plans to mitigate risks rated as critical and high on a premitigation basis.

Chief Financial Officer

- Providing a single framework for risk management in _ABC Ltd_ consistent with this policy and the Board's risk appetite.
- Facilitating regular reviews and updates to the CEO and to the Audit and Risk Committee.

CEO and executive

- Providing leadership in _ABC Ltd_ for risk management by:
  - Identifying, managing, updating and monitoring risks.
  - Creating a focus on risk awareness and management for their teams.
  - Ensuring that key decisions are made taking into account risk factors.
  - Ensuring that mitigations are in place and are effective.

All _ABC Ltd_ People

13. Appropriately identify and manage the risks in their area of work.

Supporting Functions

14. The Risk and Assurance Manager will provide the framework to enable the identification of compliance obligations and the compliance controls embedded in the business that ensure our obligations are met. Wherever possible the risk and compliance frameworks will be aligned.

15. Independent assurance providers, including business assurance, external audit and regulators undertake periodic reviews to assess:
    - the effectiveness of internal processes and controls for managing risk; and
    - the effectiveness of relevant aspects of _ABC Ltd_'s risk management implementation as appropriate.

Ownership and Review

Approver: _ABC Ltd_ Board

Reviewer: Audit and Risk Committee

Ownership: CEO

Review: Annual or as needed.

Risk Assessment

The risk assessment matrix shown below is an example of a common type of risk matrix used by business. The information contained in the matrix for likelihood and consequence, across all the categories, needs to be set by you and your Board and executive team. These are the risk criteria. They must be relevant to your business objectives, and used to help you to maximise opportunity and minimise loss.

Key:

Critical	Immediate action required by the executive and Board with detailed planning, allocation of resources and regular monitoring
High (H)	High risk, senior management attention needed
Medium (M)	Management responsibility must be specified
Low (L)	Monitor and manage by routine procedures
Very Low (VL)	Managed by routine procedures

People
Information
Property
Economic
Reputation
Capability

	Chance	Probability	Frequency		
Likelihood	Is expected to occur in most circumstances	>95%	Has occurred 9 or 10 times in the past 10 years in this organisation or circumstances are in train that will almost certainly cause it to happen	E	Almost Certain
	Will probably occur in most circumstances	>65%	Occurred more than 7 times over 10 years in this organisation or circumstances are such that it is likely to happen in the next few years	D	Likely
	Might occur at some time	>35%	Has occurred in this organisation more than 3 times in the past 10 years or occurred regularly in similar organisations or is considered to have a reasonable likelihood of occurring in the next few years	C	Possible
	Could occur at some time	<35%	Has occurred 2 or 3 times over 10 years in this organisation or similar organisations	B	Unlikely
	May occur only in exceptional circumstances	<5%	Has occurred or can reasonably be considered to occur only a few times in 100 years	A	Rare

	Consequence				
	Minor injury or first aid treatment	Injury requiring treatment by medical practitioner and/or lost time from workplace.	Major injury / hospitalisation	Death or irreversible, life-altering harm	
	Compromise of information otherwise available in the public domain	Minor compromise of information sensitive to internal or sub-unit interests	Compromise of information sensitive to the organisation's operations	Compromise of information sensitive to organisational interests	Compromise of information with significant ongoing impact
	Minor damage or vandalism to asset	Minor damage or loss of <5% of total assets	Damage or loss of <20% of total assets	Extensive damage or loss of <50% of total assets	Destruction or complete loss of <50% of total assets
	1% of budget organisational division or projected budget as relevant	2-5% of annual budget	5-10% of annual budget	>10% of budget	>30% of project or organisational annual budget
	Local mention only. Quickly forgotten. Freedom to operate unaffected. Self improvement review required	Scrutiny by executive, internal committees or internal audit to prevent escalation. Short term local media concern. Some impacts on local level activities	Persistent national concern. Scrutiny required by external agencies. Long term 'brand' impact	Persistent intense national public, political and media scrutiny. Long term 'brand' impact. Major operations severely restricted	International concern, government inquiry or sustained adverse national/ international media
	Minor skills impact. Minimal impact on non-core operations. The impact can be dealt with by routine operations	Some impact on organisational capability in terms of delays, systems quality but able to be dealt with at operational level	Impact on the organisation resulting in reduced performance such that targets are not met. Organisation's existence is not threatened, but could be subject to significant review	Breakdown of key activities leading to reduction in performance (eg. service delays, revenue loss, client dissatisfaction, legislative breaches)	Protracted unavailability of critical skills/people. Critical failure(s) preventing core activities from being performed. Survival of the project/activity/organisation is threatened

	Insignificant	Minor	Moderate	High	Extreme

Risk Assurance

The risk assurance matrix below is a way for you to consider consequence and control assurance together. This provides you with a picture of how well the risks are being controlled – and can be more useful in health and safety than a matrix that purely considers consequence and likelihood.

Key:

Critical	Immediate action required by the executive and Board with detailed planning, allocation of resources and regular monitoring
High (H)	High risk, senior management attention needed
Medium (M)	Management responsibility must be specified
Low (L)	Monitor and manage by routine procedures
Very Low (VL)	Managed by routine procedures

Risk assurance matrix (taken and adapted from *SafeWork Australia*)

			Consequence				
			Insignificant	Minor	Medium	High	Extreme
1	Risk eliminated or insignificant	Cost effectiveness	very low	very low	low	low	low
2	Controls are in place, to the full extent reasonably practicable		very low	low	medium	medium	medium
3	Satisfactory – controls seem adequate, but better controls are available		low	medium	high	high	critical
4	Existing controls are inadequate		medium	medium	critical	critical	critical
5	Risk is uncontrolled		medium	medium	critical	critical	critical

Risk Tolerance

Risk tolerance can be articulated in many ways- through tables, descriptions and through methods like the one here. Using a slider system like this can support risk understanding across multiple domains – helping you to integrate health and safety into normal business decisions.

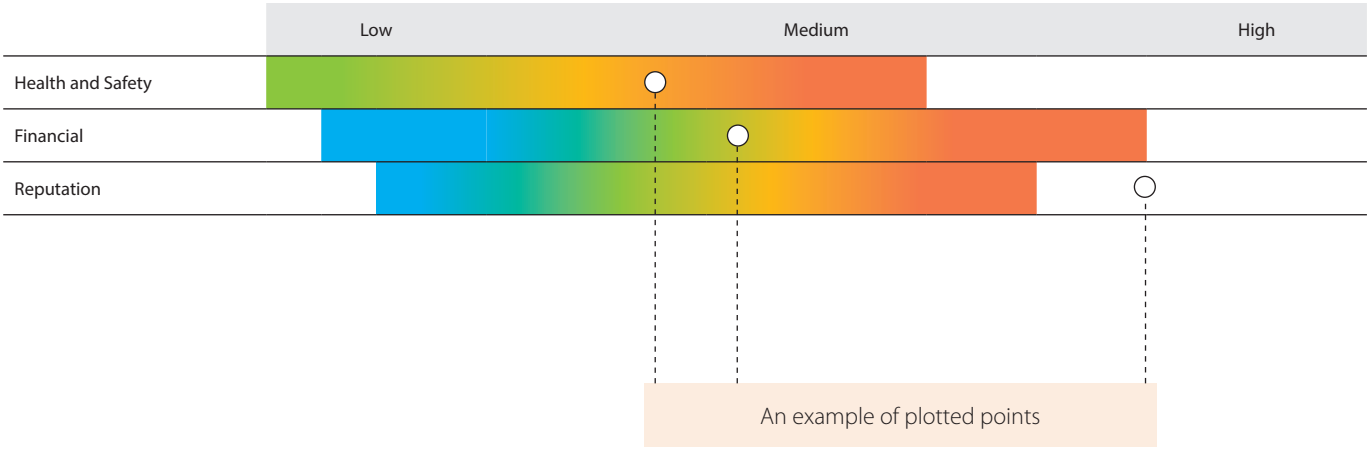
Driving Risk:

Example uses content from bow tie method (pages 2-3) and the risk profile (pages 4-5).
Risk level is taken from the Risk Assessment matrix (pages 8-9).

Key:

	Beyond tolerance (pursuing or retaining too much risk)
	High alert, monitor closely and bring within tolerance
	Within tolerance
	Beyond tolerance (not pursuing or retaining enough risk)

Tolerance Graph:



Key risk concepts explained

Risk appetite: The degree of risk an organisation will accept and pursue to achieve its objectives. Provides a framework for making decisions about which risks will be accepted and sets boundaries for the organisation's activities.

Risk tolerance: This is the *maximum level of risk a business is willing to operate within*. Risk tolerances translate risk appetite into operational limits for the day-to-day management of risks.

Risk framework: This enables effective implementation of the risk management process. It is the glue that gives cohesion and consistency to risk management efforts.

Risk profile: An organisation's entire risk landscape, reflecting the nature and scale of its risk exposures in each relevant category of risk.

Key risk controls: Controls which are critical to the management of a risk. The performance of key risk controls should be monitored.

Escalation requirements: Sets out the process for when and how critical risks should be brought to the attention of those accountable for the risks – who can decide what to do.

Risk criteria: Defines the causes and consequences of the risk, and how they will be measured. Sets out how the level of risk will be determined, the views of stakeholders, and the level at which the risk becomes acceptable. Covers how the 'likelihood' of the risk occurring will be defined, and timeframes for any consequences. States whether combinations of risks should be considered and, if so, which combinations.

Risk velocity: How fast a risk travels from the initiating event to the consequence. Indicates how much time you will have to respond, and therefore if your controls are appropriate.

Recovery control: A control that helps you recover if an event occurs, or lessens the consequences. E.g. a fall arrest harness.

Risk control effectiveness: Whether a risk control operates in a consistent, repeatable and defined way.

Want more?

This guide is part of the Forum's *Monitoring What Matters* series – which supports CEOs to lead on the three pillars of good health and safety – Risk, Relationships, Resources.

For more information visit www.zeroharm.org.nz and see:

- *CEO Guide to Risk – W*hich supports CEOs to understand their current performance and offers suggestions for how to improve.
- *Digging Deeper* – Detailed questions to assess the effectiveness of your health and safety management.
- *Monitoring What Matters* – A guide to monitoring health and safety that includes suggested performance measures for risk, relationships and resourcing.

More information: see www.zeroharm.org.nz or email info@zeroharm.org.nz