Business Leaders' Health & Safety Forum

ZERO HARM WORKPLACES

CEO Guide to Risk

DIGGING DEEPER

Detailed questions to assess the effectiveness of your health and safety risk management

Take a closer look

This guide will help CEOs dig deeper into the effectiveness of their health and safety risk management.

It is a companion to the Forum's *CEO Guide to Risk* – which supports CEOs to assess their current performance, in discussion with their directors and teams.

The *Digging Deeper* questions can then be used to examine particular areas of performance in much more depth.

The questions cover three essentials of good health and safety risk management:

- Setting expectations
- Enabling the work
- Monitoring outcomes

WHAT MATTERS

RISK | RELATIONSHIPS | RESOURCES

Digging Deeper Questions: Setting expectations

Setting clear expectations is essential for good health and safety risk management. This sets the tone for how risks will be managed. Use these questions to dig deeper into how well your organisation has communicated its commitment, expectations and approach to managing health and safety risks.

Have we articulated our commitment and attitude to health and safety risk management, relevant to our business objectives and context?

Have we **clearly defined our business objectives**, against which we can consider the impact of health and safety risks?

Have we **defined and understood our operating environment**, including the social, environmental, regulatory, competitive and political context, and our internal capability and capacity?

Have we, with our board, **articulated our commitment** to health and safety risk management?

Have we, with our board, **defined our attitude** to health and safety risk management - including setting our risk appetite and risk tolerance for health and safety?

Have we set clear expectations for the management of health and safety risks?

Have we developed clear **criteria for health and safety risk management** to help us understand the magnitude of risk and the potential impact? These criteria should cover:

- The nature, causes and consequences, and how they will be measured
- How the 'likelihood' of an event occurring will be defined (e.g. qualitatively or as a quantitative probability)
- The timeframe of interest
- How the level of risk will be determined
- The level at which the risk becomes tolerable
- Whether combinations of risks should be taken into account, and if so how, and which combinations should be considered?

Have we **defined clear roles, responsibilities, accountabilities and authority** for health and safety risk management? Including:

- The risks people are accountable for, and how people will be held accountable
- Expectations for managing risks and how risks should be managed
- Reporting and escalation requirements for risks that go beyond tolerance levels
- Authority for accepting the aggregated and interlinked level of risk in our activities.

Have we ensured **good governance and infrastructure arrangements** for risk management data and information? Including:

- Does our infrastructure (IT, storage, communication) enable visibility of risk assessment and risk controls across our business?
- Are records and information transparent and accessible across our business?
- Are learnings (including incidents, defects and inquiries) collated centrally?

Have we developed a consistent approach to risk management across our business?

Does our risk management approach (framework and process) help us and our board **consider health and safety risk as an integrated part of business risk?**

Does our approach help us **cascade and communicate our attitude to health and safety risk?**

Does our approach to health and safety risk management help us **identify, anticipate, assess, manage and monitor risks to health and safety?** Do we:

- Use a range of risk identification and assessment methodologies?
- Consider what is needed to support things to go right, as well as how to avoid things going wrong?
- Prepare for how we will recover when things do go wrong?
- Clearly define how we assess risk (e.g. based on severe but plausible, or most likely, outcome)?

Digging Deeper Questions: Enabling the work

Enabling the work is essential to ensure your expectations become reality. Use these questions to dig deeper into how well your organisation understands and controls its risks, and whether risk management is properly resourced.

Have we identified and assessed risks to health and safety?

Are we continually **applying our risk management approach** and identifying existing and emerging risks (acute, chronic and catastrophic)? Have we considered risk related to:

- Our locations, activities, or use of equipment, plant and substances?
- Our supply chain?
- Change (people, environment, business activity, strategy) including acquisitions and mergers?
- Our leadership decisions, and strategy development and business planning?
- Our procurement approach or design processes?

Are we **meaningfully and continually involving our people and others** (from our supply chain, our sites or service delivery partners) in the identification and assessment of risk?

Are we applying our defined risk criteria to identify **the critical health and safety risks** that demand the attention of senior leaders and directors?

Do we **understand our critical risks?** This includes:

- The operational context the risk exists in (internal and external)
- Sources of potential harm and when, why and how exposure occurs
- Who is exposed to the risk
- How fast an event will occur once set in motion (risk velocity), and therefore how much time we have to respond
- How multiple risks might interact
- The impact of specific risks
- Which risks are outside our tolerance levels.

Have we removed or managed critical risks that can kill or cause permanent injury/life-shortening ill health?

Are we continually assessing how to **remove critical risks**, or how to prevent, detect, mitigate and recover, to bring the risk within our tolerance levels?

- Do we involve our people, and for key issues our board, in a meaningful way in this process?

Have we **set and communicated standards for each risk control**, in line with good practice, legal and industry standards? Have we:

- Identified key risk controls and defined parameters they should operate within?
- Understood the purpose of the control (prevention, protection, detection, recovery), what it controls and how, and the parameters that ensure it is consistent, reliable and timely?
- Defined how the control must be maintained or tested?
- Defined performance indicators for key risk controls?
- Ensured we account for the impact of social interactions and human factors on risk perception and response?

Do we **understand interactions between risks and risk controls?**

- In particular, where controls are dependent on each other, where they might interact or where they might exacerbate or transfer risks elsewhere?

Are we prepared to **respond to risk events and change?** Do we:

- Recognise the boundaries of health and safety in our operations?
- Understand when and how to respond?
- Have the capability to return to normal after a response?

Have we resourced the management of health and safety risk?

Are we defining and building the **organisational capabilities** needed to enable effective risk management on an ongoing basis? Have we:

- Identified the organisational capabilities needed now and in the future (including collaboration, trust, communication, flexibility, responsiveness etc.)?
- Got accessible, relevant and supportive risk management processes?
- Got the right tools, information and infrastructure to support risk management, and enable collaboration and communication across teams and locations?

Are we building **workforce capability and capacity** to manage risks on an ongoing basis? Have we:

- Got people with the capacity and capability (physical and psychological) to recognise and respond to unanticipated threats and opportunities?
- Created space for people to open up and discuss risk – even when things appear safe?
- Provided our people with relevant training and development?
- Built trust in all our relationships?
- Ensured everyone understands the degree to which they are permitted to expose the organisation to the consequences of a health and safety risk?

Do we provide **safe plant and equipment?** Do we:

- Regularly check there are no 'safer or healthier' alternatives?
- Inspect and maintain plant and equipment?
- Redesign our work to reduce equipment and plant risks?

Do we provide the right **information** at the right time, in the right way, to support people to manage risks in line with our expectations? This includes ensuring:

- Information about risk and risk controls is delivered in an understandable and accessible way
- Our communication processes are two-way.

Digging Deeper Questions: Monitoring Outcomes

Monitoring outcomes is essential to build confidence in your risk management and to maximise resilience. Use these questions to see how well your organisation monitors activity, verifies performance and looks for ways to learn and improve.

Do we monitor and verify risk management activity, and hold ourselves accountable to our commitment?

Does our **monitoring help us understand risk** related to our relationships, changes in operating conditions and activities? Does it:

- Help us **anticipate, respond and learn about risk?**
- Cover risk management activity right through our organisation, including by staff, contractors, management and the board?
- Help us understand the effectiveness of key risk controls, whether they are being implemented, and the capability and adaptability of our people?
- Have limitations, and do we understand what they are?
- Enable us to have effective governance conversations with our board?

Do we have **internal and external assurance mechanisms** in place for our risk management activity? Specifically, do we:

- Have an internal audit/review programme that verifies key risk controls are being implemented?
- Have an independent external audit/review programme reporting directly to our executive or board covering the implementation of controls?
- Involve workers and their representatives in the validation of risk controls at the operational level?

Are we **holding management and workers accountable** for meeting their risk management responsibilities? Do we hold:

- Our people accountable for monitoring the implementation of risk controls?
- Ourselves responsible for listening to the ideas, concerns and issues raised by our people?
- Ourselves accountable for learning from key events, information and ideas?

Do we reflect on the effectiveness of our risk management activity?

Do we **make time to collectively reflect** on our management of critical health and safety risks? Do we:

- Discuss our performance with our management team and people?
- Keep risk discussions alive when everything appears safe?

Do we **maintain the energy, space and motivation** for health and safety risk management? Do we:

- Create an environment where workers' ideas can be raised and acted on?
- Encourage and support people to get involved and allocate them time to do this?
- Show through our actions at the leadership and board level that we value the time people spend on risk management?
- Appreciate how our leadership decisions might put pressure on the time available for staff and contractors to work on risk management?

Do we assess and determine, with our board, whether our **attitude and approach to health and safety risk management is appropriate?**

- Are our risk appetite and risk tolerance appropriate to achieving our business objectives?
- Are our risk criteria appropriate and do they reflect our attitude towards risk?
- Do we involve everyone who would be considered an 'officer' under the Health and Safety at Work Act in the evaluation and understanding of health and safety risks?

Do we learn and improve our approach, based on our verification and reflection activity?

Do we have mechanisms to ensure we **learn** from why things work well, as well as why they fail? Have we:

- Defined when and why we will investigate incidents?
- Identified and understood how, when and why people adjust their actions to ensure work can be done safely?
- Shared information and learning across teams and locations?
- Inquired into why things go right most of the time?
- Learnt from others outside our organisation?

Do we **benchmark our risk management activity** in or outside our sector? Do we use this information to inform our decisions, change our approach, and help us to improve our risk management activity?

Do we **plan and update our health and safety risk management** based on information from our monitoring activity and learning forums?

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: Define the causes and consequences of the risk, and how they will be measured. Set 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.
- *What Good Looks Like* – Examples of health and safety risk management tools.
- *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