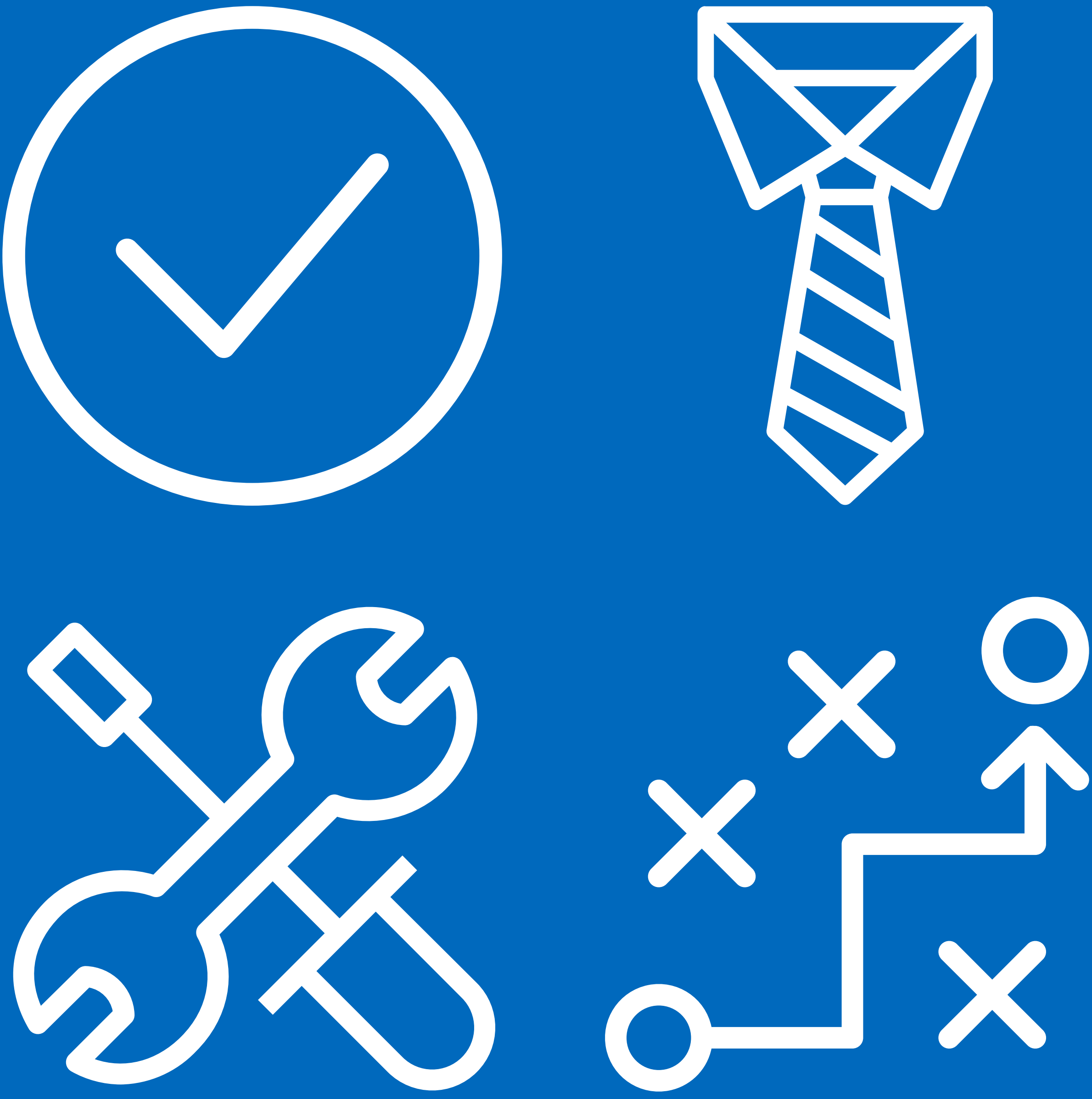
noggin

Business Continuity

Making Sense of Risk Management: Best-practice risk management tools and strategies for the era of threats



Why ramp up risk management practices today

What's the value of risk management? If it wasn't clear before, business interruption is a matter of when not if. Without even factoring in the pandemic, the measured risk of disaster-related closings of business facilities has increased precipitously. Meanwhile, business interruptions themselves have only become more expensive.

Worse still, interruption isn't the only serious business risk requiring sustained senior management oversight. From public and operational security to occupational health and safety, risk vectors continue to grow, as the wider macroeconomic environment just gets more difficult for business.

Risk scholars Howard Kunreither and Michael Useem offer a few reasons why. They highlight a number of cross-industry trends exacerbating business risk across the globe. Those trends include:

- Growing interdependency
- Shorter-term (management) thinking
- Increased regulation
- Greater geographical clustering
- Higher probability of systemic shock
- New calls for transparency

So, how do companies succeed in this volatile business environment? They develop proactive, forward-looking risk management strategies, processes, and systems to cope with and anticipate profound shifts in business risk.

A risk management overview

Having a firm grasp of the fundamentals of risk and risk management certainly helps, here. For starters, any risk, defined as the expression of possible loss due to a hazard, has three basic components. Those include:

1. Probability of occurring
2. Severity
3. Exposure of people and equipment

Risk itself can be further sub-categorised. There's not just the risk you identify using your analytical tools, but also the risk you have yet to find. The sum of identified and unidentified risk makes up your total risk profile.

Meanwhile, there're varying degrees of risk within the category of identified risk: acceptable and unacceptable risk. Acceptable risk, as the name implies, is the risk you tolerate once you've applied controls to manage your risk profile.

Controls are the actual strategies and tools you'll use to manage risk, either to mitigate risk or eliminate it altogether. An effective control will reduce or eliminate at least one risk component.

Unacceptable risk, on the other hand, is the portion of identified risk that you simply can't accept. As such, unacceptable risk should be eliminated or at least actively controlled.

Residual risk, encompassing acceptable risk and unidentified risk, is the amount of total risk that remains after your risk management efforts have been brought to bear.

Risk management terms can be tough to get straight. Here is a simple risk management glossary.

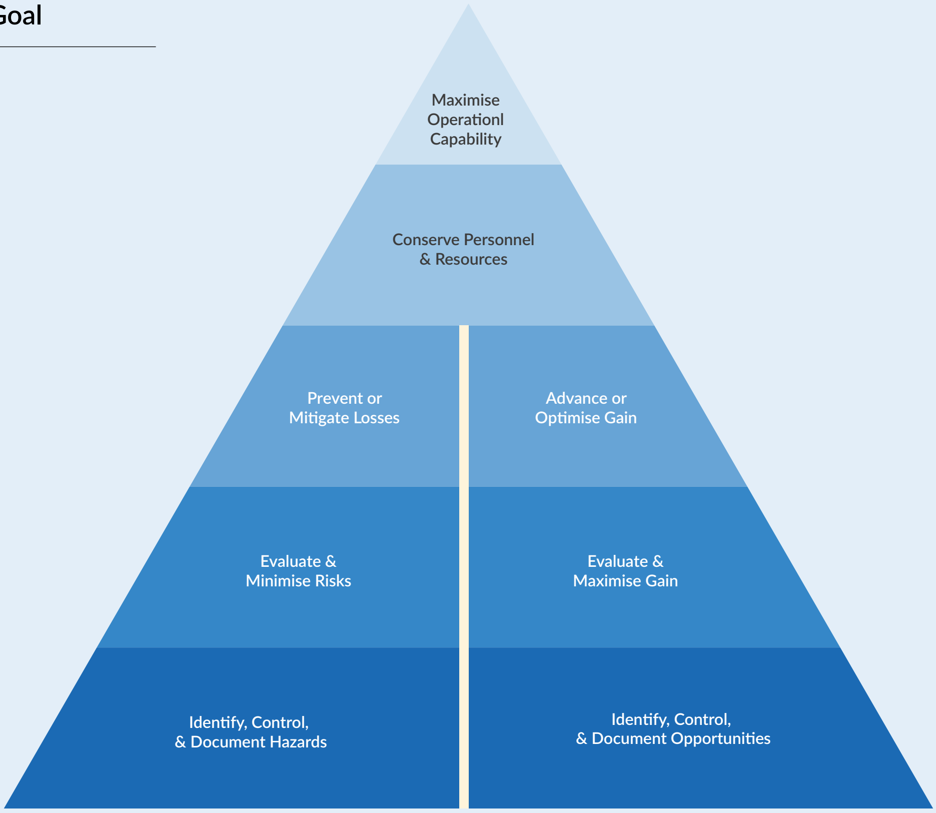
- **Hazard.** Any real or potential condition that can cause degradation, injury, illness, death, or damage to or loss of equipment or property.
- **Risk.** An expression of possible loss due to a hazard in terms of severity (usually qualitatively categorised) and probability (also qualitatively categorised).
- **Identified risk:** Subset of risk that has been determined to exist using analytical tools. The time and cost of analysis, the quality of the risk management program, and the state of the technology involved affect the amount of risk that can be identified.
- **Unidentified risk:** Subset of risk that has not yet been identified. Some risk is not identifiable or measurable.
- **Total risk:** The sum of identified and unidentified risk.
- **Acceptable risk:** The part of identified risk that is allowed to persist after controls are applied. Risk can be determined acceptable when further efforts to reduce it would cause degradation of the probability of success of the operation, or when a point of diminishing returns has been reached.
- **Unacceptable risk:** The portion of identified risk that cannot be tolerated but must be either eliminated or controlled.
- **Residual risk:** The portion of total risk that remains after management efforts have been employed. Residual risk comprises acceptable risk and unidentified risk.

Source: Federal Aviation Administration

A central question of risk management is how much risk is too much risk? Risk management, of course, is all about identifying, evaluating, and determining the risks to which your company is exposed and coming up with policies, processes, and procedures to manage those identified threats.

But you simply can't run a business without courting some level of risk. Even if you could identify every single risk, it would require a significant outlay of resources to control all of them. As you can imagine, allocating that number of resources to risk management would have significant opportunity costs for running the business as a whole.

Risk Management Goal


Maximise Operationl Capability
Conserve Personnel & Resources
Prevent or Mitigate Losses
Advance or Optimise Gain
Evaluate & Minimise Risks
Evaluate & Maximise Gain
Identify, Control, & Document Hazards
Identify, Control, & Document Opportunities

Source: U.S. Federal Aviation Administration

The challenges of effective risk management

Limited resources for controlling identified risks aren't the only stumbling blocks to effective risk management. In this day and age, businesses are confronting new risk types all the time.

The sheer pace and volume of change are overwhelming risk teams, quickly rendering their existing processes and frameworks outmoded. It doesn't help that many of those existing risk management processes and frameworks are disjointed, disconnected, and overly manual

The lack of a comprehensive, integrated approach to operational risk management specifically wreaks havoc on teams who lack the internal (communications) tools to properly integrate their knowledge base of risk into their systems for managing risk.

In turn, risk managers don't get visibility into companywide risk. Instead, they only get a fragmented view of (section-specific) risk. Despite the high probability of contagion between business lines, team-specific processes to identify, assess, manage, monitor, and report on risk proliferate, with the following consequences:

- ✗ Teams are less able to identify priorities that will help them stay ahead of risk.
- ✗ Processes become more reactive and less effective.

Add to that, risk management is just hard. Even teams who deploy best-practice processes can easily find themselves at a preparedness deficit. Just the sheer surfeit of emerging risks, including public health and safety threats, can expose major skills and capabilities gaps.

On the other side, the cost of ineffective risk management can be prodigious. Get risk management wrong and the business might suffer from workplace injuries and accidents, productivity loss, damaged assets and products, even significant financial penalty.

The cost of an on-the-job accident alone adds up quickly. Companies will have to shell out to train replacements, repair equipment, pay higher insurance premiums, while also losing time, prestige, and sacrificing employee morale.

Effective risk management practices

So, what can be done, especially if you can't adequately control all of your company's identified risks? We live by the mantra that risk is inevitable. Trade-offs in risk management are inevitable. To make better-informed trade-offs, though, stakeholders will need to operate with a strategic, business perspective in mind. That means anchoring their risk management practices within a larger, organisational context.

It starts at the top. For, only business leaders can align their company's risk appetite with its risk management aims.

But first, those same executives will have to promote greater risk management awareness and risk transparency. Business leaders will also have to empower staff to contribute their own ideas in order to improve risk processes and controls.

Further, you'll only get that kind of risk management culture with a robust reporting culture. Here, executives have to invest in the appropriate integrated risk and work safety management software that will enable teams to fully assess and document risks, including detailed information on why certain identified risks were accepted (and others not). Additional best practices include:

- ✓ Limit risk decision making to leaders who have the power to allocate resources
- ✓ Have clear organisational objectives
- ✓ Identify risk roles and responsibilities
- ✓ Put a support structure in place
- ✓ Deploy early warning systems
- ✓ Ensure risk decisions go through a clear review cycle

Integrate operational risk management practices into your planning efforts

A central theme of operational risk management is that risks are more easily assessed and managed in the planning stage of any given operation, rather than during implementation and execution. It's during the latter phase when changes become more expensive and time consuming.

Operational risk management, however, is an actual process of its own of risk assessment, decision making, and implementation (of controls). Here, then, are the stages of the operational risk management lifecycle:

Risk identification. The identification stage consists of isolating all potential operational risks, whether recurring risks or potential one-offs. Risk identification involves staff across the business, not just C-suite executives.

Risk assessment. Once identified, risks must be added to a risk register where they are to be assessed based on a number of factors, like how likely the risk is to occur, how frequently the risk will occur, and the potential risk exposure to human and non-human assets if the risk is not managed. The use of a risk matrix, an established risk assessment methodology, is a standard way of prioritising risks by likelihood and consequences. The severity of each risk can then be assessed separately, either as inherent, target, or residual risk, using a common methodology. At the end of the evaluation, risk is traditionally categorised as very high, high, medium, low, or very low.

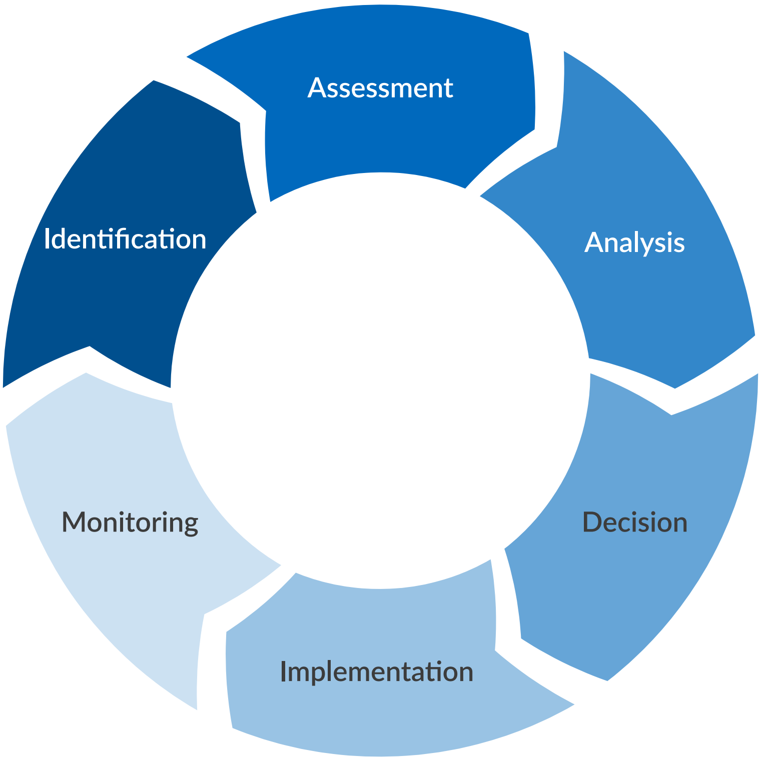
Analysis. In analysing risk, teams will consider which risk controls (if any) to put in place. Additionally, teams will provide decision makers with a thorough risk analysis, a clear cost and benefit evaluation, as well as outlines of possible alternative measures to take.

Decision. Based on the analysis furnished, decision makers will choose the best control (or combination of controls).

Implementation. Carrying out the decision taken requires having a plan for applying the selected controls. Adequate time and resources must also be allocated for any control measure to be successful. In addition, implementing controls requires clearly communicating your plan to everyone involved.

Monitoring. Implementation, however, isn't the end of the story. Once they're put in place, controls will have to be consistently monitored to ensure they are working as expected.

The operational risk management lifecycle



Invest in the right integrated risk management and work safety management software to mitigate risk

Not all hazards lend themselves to this level of operational risk management. Rather, more time-critical risk management makes use of an abbreviated lifecycle, in which teams skip straight to assessing the situation, before balancing resources, communicating risks and intentions, implementing controls, and (finally) debriefing.

So, what level of operational risk management makes the most sense for your business? The frustrating answer is it depends. It depends on any number of factors, none more important than available time and resources.

What we can say, though, is the best operational risk management frameworks balance prevention and response. They also put a high premium on continuously improving the efficiency of control systems so as to support larger business objectives. Getting there takes eliminating redundant and overlapping controls, as well as issuing specific guidelines on how to perform best-in-class root cause analyses – at least in the short term.

In the longer term, integrated risk management and work safety management software will be absolutely integral to developing a strong operational risk management culture at your business. Such a platform would bundle operational risk tracking and incident management functionality into the same solution, making incident response more efficient.

Cross-linking hazards with incidents (in the same solution) gives teams the history and intelligence needed to trigger necessary changes in risk management plans and processes, as well as helps teams identify where controls might have failed to achieve desired outcomes.

That's not all. What other capabilities matter? Download our purchaser's guide to work safety management software to find out.

Source

[i.] *Howard Kunreuther and Michael Useem, Oxford University Press: Mastering Catastrophic Shock: How Companies Are Coping with Disruption.*