Safety in program design

www.pwc.com.au

Contacts

Canberra

David Vrancic
Partner
+61 (2) 6271 3320
dave.vrancic@au.pwc.com

Brian McBride
Director
+61 (2) 6271 3291
brian.mcbride@au.pwc.com

Les Haines
Director
+61 (2) 6271 3295
les.haines@au.pwc.com

About the authors

Dave Vrancic is a Canberra-based Partner with PwC. He has 15 years consulting experience in management and engineering, where he has led strategic engagements in program design and execution, systems engineering process and program life cycle cost analysis, regularly providing advice and program recommendations to senior executives. Prior to his consulting career he was a senior engineer in the Royal Australian Air Force, where he gained extensive practical experience in system safety improvement and airworthiness.

Brian McBride is a Director in PwC's government practice in Canberra. He has 30 years' experience working on large-scale technologically complex programs across Defence and civil government. Brian's areas of expertise includes program management, systems engineering, assurance of safety critical and high integrity systems, safety management systems, and regulatory systems.

Les Haines is a Director in PwC's government practice in Canberra. He has more than 25 years of experience in consulting and management in civil government in Australia and internationally. His expertise is in the people component of organisational capability and programs, with a specific focus on work health and safety, program safety, workforce analysis and planning, human systems integration and human factors analysis.

Executive summary

*The **Report of the Royal Commission into the Home Insulation Program** found that the deaths of four young men working on the program could have been avoided had the program been properly devised, designed and implemented. The report also found that, contrary to the contention of Federal Government officials who designed the program, safety risks associated with the program could have been controlled.*

This finding reinforces what the aerospace, automobile, ship-building and construction industries have known, accepted and practised for decades – that lives, time and money can be saved by 'designing out' safety risks before programs are implemented.

In these industries, managing the risks to health and safety is an integral part of a 'cradle to grave' program management discipline. Commonly referred to as the 'Program Lifecycle', this discipline governs the conception, design, building, supply, use, maintenance and disposal of materiel items, vehicles and facilities.

The introduction of the WHS Act (2011) has generated increased effort into improving safety. Many government organisations in Australia have focussed on improving their safety compliance and processes. However, by itself this is not enough – relying solely on compliance and process can actually skew safety thinking and actions in ways that work against management of program safety risks. Effort also needs to be applied to achieve a proactive stance on prevention of harm and encouraging the 'STOP, THINK, PLAN, ACT' behaviours on which sound safety performance depends.

PwC believes that health and safety should be accorded the same priority in program management as quality, risk and schedule. Critical to this, and to ensuring continuous improvement in safety capabilities in organisations more generally, senior executives in government should focus on:

- establishing and sustaining effective safety leadership
- shifting their organisations from compliance-focused, process-driven safety models to proactive, principles-based models
- taking an evidence-based approach to WHS capability assessment and building
- taking a lifecycle approach to program safety
- embedding upstream safety thinking, decision-making and action in program design
- building a 'Risk Sensible' appetite and culture in all safety thinking and decision making
- setting rigorous safety performance measures and targets and hold people accountable for achieving them
- embedding closed-loop safety information processes along the program lifecycle.

Safety in the program lifecycle

When most people think about work health and safety (WHS), they think about activities conducted in workplaces such as offices, factories, wharves, power plants and transport hubs to keep employees safe. These activities typically include identifying and controlling hazards, responding to and reporting safety incidents, providing healthcare for work injuries and illness, supporting rehabilitation and providing compensation. We call this 'downstream safety'.

However, there is another critical side to safety that involves 'designing out' hazards that create workplace risks before they become embedded in the workplace. This concept, which we call '*upstream safety*' but is often referred to as 'safe design', is commonly reinforced by strong government regulatory regimes and has been widely accepted and practised in the aerospace, automobile, mining, shipbuilding and construction industries for decades.

In these sectors, safety is an integral part of a 'cradle to grave' program management discipline that governs the conception, design, building, supply, use, maintenance and disposal of materiel items, vehicles and facilities – commonly referred to as the 'program lifecycle'. For these industries, the need to embed critical safety decision-making and action early in the program lifecycle is unchallenged, because experience has shown it saves lives, time and money.

But the need to consider safety early in the lifecycle has not been so widely adopted and practised in private and public sector non-materiel programs. This is particularly the case for many government programs in Australia. These programs, commonly directed at achieving high priority government policies, are often large, complex and costly. They generally involve the design and delivery of services, products or a combination of both, and have multiple touch-points on complex stakeholder communities involving elected representatives, government officials, service providers and citizens.

Exhibit 1: The program lifecycle
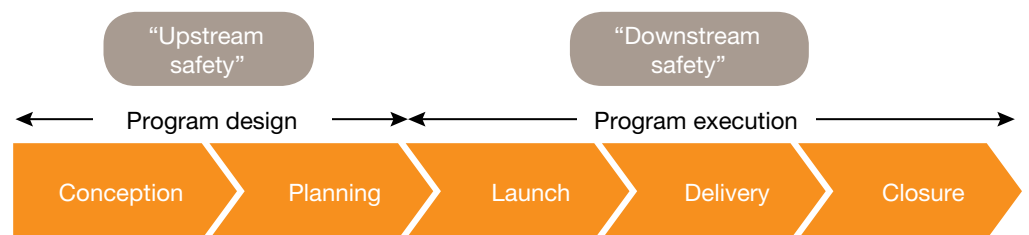
This has been brought into sharp focus in Australia with the release of *Report of the Royal Commission into the Home Insulation Program (HIP)*[1]. The report was commissioned as a result of the deaths of four young men working on the HIP, a very ambitious program to install insulation in the ceilings of 2.2 million Australian houses in two and a half years. The Royal Commission found that these deaths could have been avoided had the program been properly devised, designed and implemented. The report also found that the contention of the federal government officials who designed the program – namely, that the program's WHS risks were the regulatory responsibility of the states implementing the program, and not theirs – was unjustified and unreasonable[2].

[1] Report of the *Royal Commission into the Home Insulation Program*, Ian Hanger, AM QC, 29 August 2014.

[2] Ibid p3

Why early and effective safety thinking is critical

The WHS Act (2011) and the harmonisation of WHS legislation across most states and territories raised the bar significantly for work health and safety in Australia, by, for example:

- making the tasks of duty holders non-transferable; in other words, each person is responsible for influencing and controlling the safety issues involved in their duties

- requiring duty holders to *eliminate* risks to health and safety, so far as is reasonably practicable (SFAIRP), and if it is not reasonably practicable to do so, to minimise those risks SFAIRP

- introducing additional duties for *upstream safety* for those involved in designing and installing, manufacturing, importing or supplying plant, substances or structures for workplaces

- extending protection to cover the safety of all workers, and to the general public who may be affected by work activities

- introducing significant new fines and prison sentences for breaches for organisations and individuals.

But as important as ensuring legislative and regulatory compliance is, it is not the only reason for ensuring safety thinking is embedded throughout the program lifecycle. Other reasons include:

- **The moral imperative** – it is the right thing to do in terms of the 'contract' between government and its citizens who either deliver a program or receive the products and services of the program.

- **The program effectiveness imperative** – getting safety right from the outset helps ensure a program's intended outcomes are actually achieved, and not diluted by predictable and preventable safety issues.

- **The economic imperative** – early and judicious investment in safety in government actually saves money, by minimising preventable death, illness and injury among those delivering or receiving program services. It also boosts workforce productivity and reduces the costs of treating, rehabilitating and compensating affected people.

WHS driven solely by a legislative or compliance imperative can help avoid fines and prison sentences for some government officials. However, it can actually skew safety thinking and actions in ways that work against the core objective of any organisational safety system, driving down the incidence of preventable workplace deaths, injuries and illnesses.

The key – less process, more proactivity

Compliance-driven approaches to safety generate large numbers of policies, procedures and processes that typically result in process overload.

In organisations suffering policy and process overload, workers struggle to even know what policies and processes exist, let alone read, understand and comply with them. Also, the 'way things work' usually do not fully follow the policies and procedures. This problem besets government bureaucracies in general and actually stifles the proactive 'STOP, THINK, PLAN, ACT' behaviours on which sound safety performance depends. Effective safety processes that are complied with are a necessary but not sufficient condition for strong safety performance. Excessive and exclusive reliance on process and compliance to achieve safety outcomes can relegate safety thinking to a second order priority rather than keeping it front of mind where it should be.

In government programs, safety risk management is often considered as part of the overall risk management approach – as it should be. But in our experience, much government risk and assurance activity at both the enterprise and program levels, is very heavy on process but light on insight. Critical safety information, like other risk information, and safety processes, gets lost in the detail.

Senior executives and program managers in government are typically not short of risk information. In fact, they are often overwhelmed by endless risk matrices, risk registers, traffic light reports, dashboards and so on – much of which they can't make sense of, or draw actionable insight from. Too often, capturing risks in registers and reports becomes an end in itself rather than part of a learning cycle to devise and embed remediation and enhance behaviour. That is, the action often stops once the safety risk is noted in the register, when the desired result is for action to continue until the mitigation has been implemented and the risk has been effectively managed.

Organisations that take safety seriously treat it as a journey of continuous improvement. They understand where they are at in terms of their WHS performance, articulate clearly where they aspire to be, and put in place the initiatives to close their safety capability gaps. For example, the Department of Defence has adopted a WHS capability maturity model (*Exhibit 2*) that serves as a framework for its continuous WHS improvement journey.

It is only when organisations apply frameworks like this, and aspire and act to achieve levels of WHS capability beyond a mostly reactive, process-driven, compliance-focused approach (*level 2 in Exhibit 2*) to one that is more principles-based and embraces proactivity and behavioural safety (*level 3 and beyond*) that the real benefits of improved safety performance begin to be harnessed.

At a proactive level of WHS maturity, the whole organisation accepts and adopts a Zero Harm objective and the requirement to reduce safety risks (including program safety risks) SFAIRP and to ensure controls are in place to manage accepted residual risks. Safety management systems and policies are clear, simple, readily understood and actionable. Leaders have a strong and informed focus on safety, clear safety performance measures are established and targets set, and line management is held accountable for achieving them.

Proactivity in safety thinking and action is particularly relevant to the design phases of the program lifecycle (*Exhibit 1, page 7*), for it is here that upstream safety decisions lay the foundations for downstream safety success. It is also much cheaper to change the design to reduce risks in the conception and planning stages, with mitigation costs often escalating to very high (and often unaffordable) levels once programs are in delivery.

Exhibit 2: Levels of WHS capability maturity[3]

1 Reactive	2 Managed	3 Proactive	4 Learning	5 Leading
Absence or fragmented and disconnected management system with resulting confusion of intent, priorities, roles and preferred practices. Safety culture is characterised as reactive.	Compliance-oriented WHS management system, with associated auditing regimes, Safety culture is characterised as compliant.	Alignment, closed-loop improvement and linkages across the organisation established, with associated emphasis on prevention. Safety culture is characterised as systematic.	Whole-of-organisation capability established with WHS embedded into business and related management systems. Improvement is holistic, innovative and integrating. Safety culture characterised as learning.	Leading WHS is externally focused and foundational to organisational capability and success. Safety culture is characterised as mindful.

The elements of proactive upstream safety

So what does upstream safety involve? For senior government executives and staff engaged in program design it means:

- thinking of safety risk management as something more than simply an administrative requirement to help programs proceed through approval decision gates, and being more likely to argue for a safety risk to be controlled rather than accepted

- ensuring that stakeholders and team members recognise the inherent value of safety to program capability, and embed safety as a cultural facet of how business is done

- assessing safety risks in a richly informed, evidence-based and continuous way from the earliest stages of a program

- where there is a need to make trade-off decisions between the prevention of injury and other objectives such as process efficiency, product fitness or facility productivity, doing so in a fully-informed way

- understanding as completely as possible the full safety risk profile of a program across all lifecycle stages from program outset, developing a full picture of hazards, people at risk, and the controls required to either eliminate the hazards or reduce the risks to health and safety to an acceptable level SFAIRP

- identifying and applying a hierarchy of controls to reduce safety risks SFAIRP, working through elimination, substitution, engineering controls, administrative controls and personal protective equipment – and continually monitoring the effectiveness of those controls as new risk information and implementation safety incident experience becomes available

- developing and maintaining a program 'safety argument' which becomes an evolving body of evidence throughout the program lifecycle, supporting and continuously re-affirming the assertion that the program is safe

- continually reviewing the safety argument in the light of new information and evidence, to identify any unmitigated hazards, and designing and implementing new controls in response

- identifying and describing residual, and hence accepted, risks and their controls at the point of program launch (*Exhibit 1, page 5*) and communicating them to the deliverers and customers of the program

- putting in place closed loop processes to monitor safety performance and incident experience throughout the program lifecycle, and feeding that back to inform and adapt the program design.

In our view, a valid and well documented safety argument[4] should be the central integrating element aimed at assuring program safety. It becomes an on-going, continuously evolving body of knowledge about the hazards and associated risks of the program and the effectiveness of controls implemented to mitigate them.

[4] A safety argument is broader than just the individual or summary safety cases of design.

Another critical element of upstream safety happens at the design stage, when program designers and officials carefully think through the implementation of the program and envisage:

- the sorts of things that could go wrong given the current knowledge at the design stage of the risks
- the availability and likely effectiveness of proposed controls
- the nature and extent of the exposed population.

This sort of detailed preparation is fundamental to the design of an effective program safety performance and incident reporting system that will provide leading indicators of a new risk emerging or something going wrong. Effective closed-loop control of program safety in the execution phase involves investigating and getting to the root causes of actual accidents, but also tracking the incidents, hazardous conditions and unsafe acts that typically precede them (*Exhibit 3*).

Exhibit 3: 'Heinrich's Triangle'– the relationship between low-level safety deviations and accidents[5]

1 accident

30 incidents

300 hazardous conditions

1,000 unreported "unsafe acts"
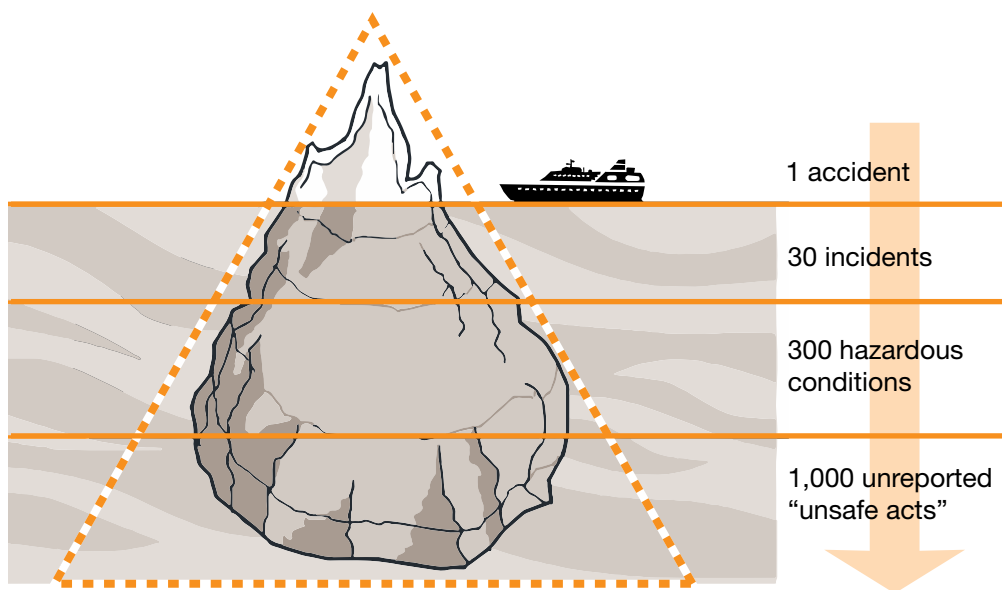
James Reason's 'Swiss-Cheese Model' provides yet another perspective on through-program safety management. Reason[6] hypothesised that most accidents can be traced to one or more failures of safety defences through the program lifecycle (*Exhibit 4, page 15*). Defences against failure are signified as a series of barriers, represented as slices of cheese. The holes in the slices represent weaknesses in individual parts of the system and vary in size and position across the slices. The system produces failures when a hole in each slice momentarily aligns, permitting, as Reason says, "a trajectory of accident opportunity", so that a hazard passes through holes in all of the slices, leading to a failure.

[5] Herbert Heinrich was an American industrial safety pioneer. He published *Industrial Accident Prevention, A Scientific Approach* in 1931. A key finding from his analysis became known as 'Heinrich's Law': that in a workplace, for every accident that causes a major injury, there are 30 accidents that cause minor injuries and 300 accidents that cause no injuries. Because many accidents share common root causes, addressing more commonplace accidents that cause no injuries can prevent accidents that cause injuries. Heinrich's work is the basis for the theory of behaviour-based safety.

[6] "The Contribution of Latent Human Failures to the Breakdown of Complex Systems", *Philosophical Transactions of the Royal Society of London*, James Reason, 1990.

Exhibit 4: Reason's 'Swiss-Cheese Model' – potential failure of safety defences

Program design → | ← Program execution →

| Conception | Planning | Launch | Delivery | Closure |

eg. Lack of the safe operating concept/safe design limit for the system

e.g., Lack of planning for hazard and risk reduction activities across the program. No safety performance measures and criteria established ie. defining what is SFAIRP

eg. Lack of hazard reduction to SFAIRP

Unsafe act or condition with the potential for harm during operation

Program stage

Safety defences, barriers and controls

Hole in safety defences, barriers and controls

Upstream safety and risk appetite

Embedding effective, proactive safety risk thinking in senior executive decision-making in government organisations is not easy – particularly when it comes to upstream safety.

Many senior government officials with huge workloads struggle with making sense of the mass of information presented to them – including information on risks they should be managing. As mentioned earlier, they are typically not short of risk information. In fact, they are often overwhelmed by it, and can't make sense of, nor draw actionable insight from it.
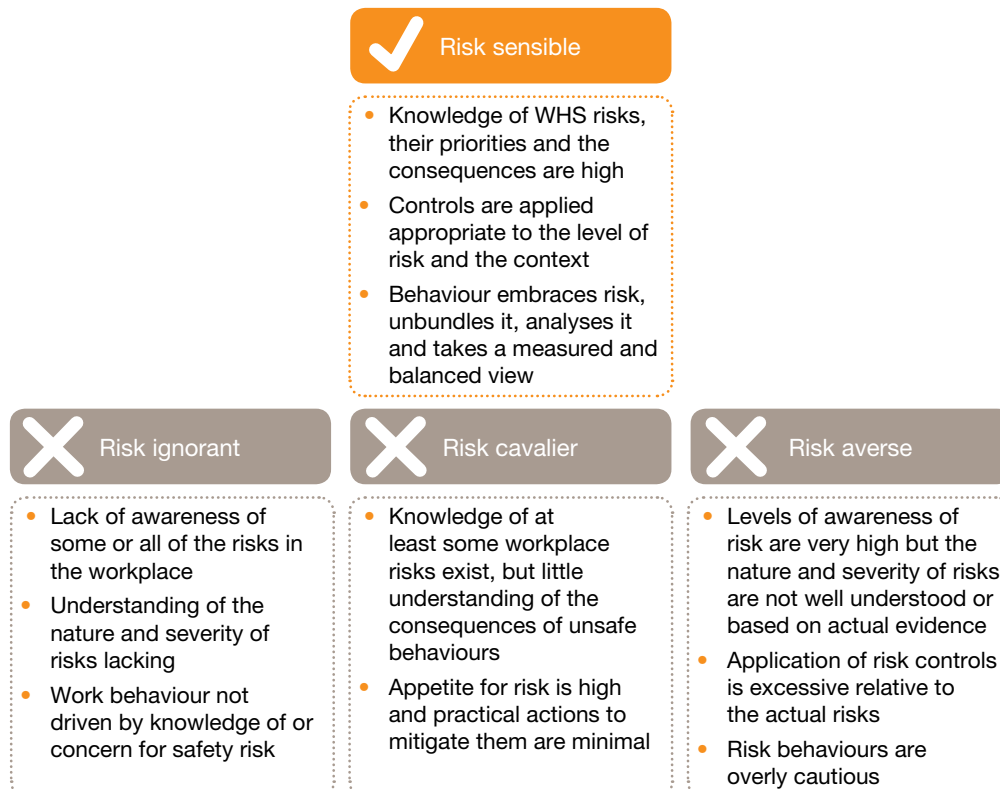
This problem is compounded by a focus by many of their staff on complying with processes rather than delivering outcomes, working in a safety risk information environment that is rich on data but low on insight, and a reluctance by some to increase a risk rating or escalate it when it might adversely impact program momentum, increase costs or not align with a dominant program view.

The root causes of situations like this are typically an immature safety culture, including a poorly defined, communicated and reinforced safety risk appetite.

Sir Charles Haddon-Cave conducted a detailed inquiry into the causes of a crash of a Royal Air Force Nimrod XV230 that suffered a catastrophic mid-air fire while on a routine mission in Afghanistan in 2006, killing all 14 service personnel on board. In his seminal report, he identified four ways that we, as humans, typically engage with safety issues (*Exhibit 5*). He argued that if a 'Risk Sensible' approach had been adopted and applied throughout the program lifecycle of the Nimrod, the disaster would most likely not have occurred.

In our experience, 'Risk-Sensible' is not the typical risk appetite prevailing in the design and execution of major Australian government programs.

Exhibit 5: Haddon-Cave's 'Four States of Man'[7]

✓ **Risk sensible**
- Knowledge of WHS risks, their priorities and the consequences are high
- Controls are applied appropriate to the level of risk and the context
- Behaviour embraces risk, unbundles it, analyses it and takes a measured and balanced view

✗ **Risk ignorant**
- Lack of awareness of some or all of the risks in the workplace
- Understanding of the nature and severity of risks lacking
- Work behaviour not driven by knowledge of or concern for safety risk

✗ **Risk cavalier**
- Knowledge of at least some workplace risks exist, but little understanding of the consequences of unsafe behaviours
- Appetite for risk is high and practical actions to mitigate them are minimal

✗ **Risk averse**
- Levels of awareness of risk are very high but the nature and severity of risks are not well understood or based on actual evidence
- Application of risk controls is excessive relative to the actual risks
- Risk behaviours are overly cautious

Embedding safety effectively in program management

How do current approaches to program management commonly applied by Australian government organisations need to change to ensure programs are safely implemented?

Apart from organisations like the Department of Defence whose approach to program safety is influenced by its responsibilities to safely design, acquire, sustain and dispose of large, high-cost and very complex military platforms that may be in service for several decades, very few government organisations take a lifecycle approach to safety. As a result, critical safety decisions with downstream consequences that should occur early in the life of a program might not be made, or might be inadequately informed.

What's more, program management approaches applied by these organisations sometimes do not call out safety as an outcome to be measured and managed in its own right. Instead, safety thinking, decision-making and action are typically bundled into risk management where critical safety issues that should be driving management decision making can be lost in the detail.
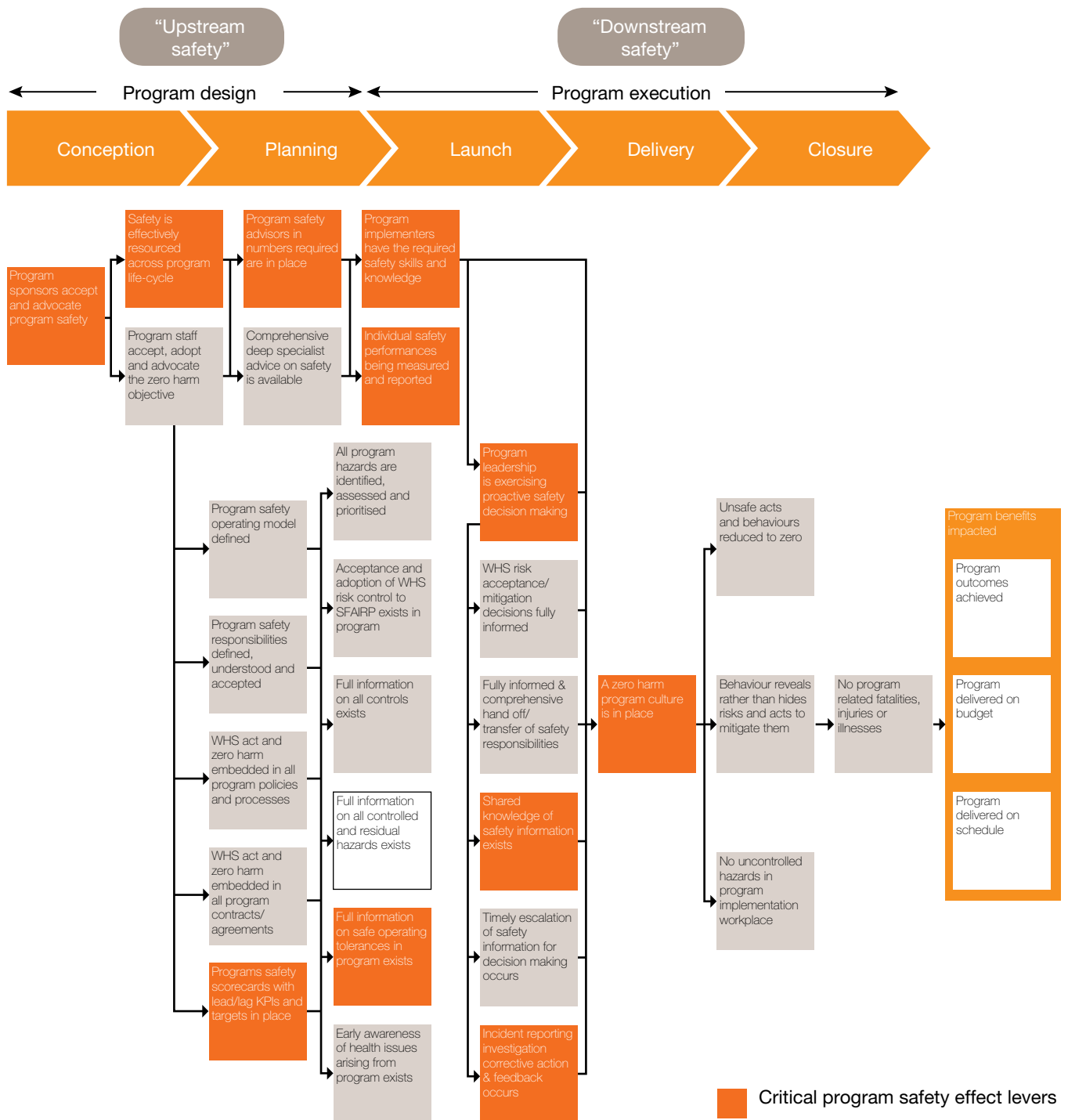
We believe that safety should be given the same priority in program management as cost, risk and schedule. This is particularly true in the program design stages of the lifecycle, where sound and timely upstream safety decision-making and action can save lives, time and money during program execution.

From our experience, better practice program safety involves proactively driving a sequence of linked safety effects along the program lifecycle to cumulatively deliver a safely delivered program (*Exhibit 6, page 14*). The effects that we see as more important than others we call 'Critical Safety Effect Levers'.

Central to delivering these key safety effects along the program lifecycle are:

- establishing and sustaining effective safety leadership
- treating organisational safety as a process of continuous improvement
- shifting the organisation from a compliance-focused approach to safety, whether it be in workplace safety or program safety, to a more proactive approach
- moving away from a process-driven safety management model to a more principles-based model
- taking an evidence-based approach to WHS capability building
- taking a lifecycle approach to program safety
- embedding a culture of upstream safety thinking, decision-making and action in program design
- building a 'Risk Sensible' appetite and culture in all enterprise level safety decision making
- setting rigorous safety performance measures (lead and lag indicators) and targets and hold people accountable for achieving them
- embedding closed-loop safety information processes along the program lifecycle.

Exhibit 6: Program safety effect drivers

"Upstream safety"

"Downstream safety"

← Program design →   ← Program execution →

Conception | Planning | Launch | Delivery | Closure

Program sponsors accept and advocate program safety

Safety is effectively resourced across program life-cycle

Program safety advisors in numbers required are in place

Program implementers have the required safety skills and knowledge

Program staff accept, adopt and advocate the zero harm objective

Comprehensive deep specialist advice on safety is available

Individual safety performances being measured and reported

Program safety operating model defined

All program hazards are identified, assessed and prioritised

Program leadership is exercising proactive safety decision making

Unsafe acts and behaviours reduced to zero

Program benefits impacted

Program outcomes achieved

Program safety responsibilities defined, understood and accepted

Acceptance and adoption of WHS risk control to SFAIRP exists in program

WHS risk acceptance/ mitigation decisions fully informed

Behaviour reveals rather than hides risks and acts to mitigate them

No program related fatalities, injuries or illnesses

Program delivered on budget

WHS act and zero harm embedded in all program policies and processes

Full information on all controls exists

Fully informed & comprehensive hand off/ transfer of safety responsibilities

A zero harm program culture is in place

Program delivered on schedule

WHS act and zero harm embedded in all program contracts/ agreements

Full information on all controlled and residual hazards exists

Shared knowledge of safety information exists

No uncontrolled hazards in program implementation workplace

Programs safety scorecards with lead/lag KPIs and targets in place

Full information on safe operating tolerances in program exists

Timely escalation of safety information for decision making occurs

Early awareness of health issues arising from program exists

Incident reporting investigation corrective action & feedback occurs

■ Critical program safety effect levers

Strong leadership: The key to effective safety culture

Strong leadership is at the heart of an effective safety culture. If safety is given the proper status it deserves, then program leaders will also be afforded the time and resources needed to ensure that government programs are designed with, and maintain, a proactive safety culture and a 'Risk Sensible' risk appetite.

The key attributes of effective, proactive safety leadership involve:

- **Vision** – the proactive safety leader is able to 'see' what safety excellence would look like and conveys that vision in a compelling way throughout the program. She acts in a way that communicates high personal standards in safety, helps others question and rethink their assumptions about safety, and describes a compelling picture of the program safety vision.

- **Credibility** – the proactive safety leader fosters a high level of trust in her peers and reports. She is willing to admit mistakes with others, advocate for direct reports and the interests of the group, and gives honest information about safety even it if is not well received.

- **Collaboration** – the proactive safety leader works well with other people, promotes cooperation and collaboration in safety, actively seeks input from people on issues that affect them, and encourages others to implement their decisions and solutions for improving program safety.

- **Communication** – the proactive safety leader is a great communicator and encourages people to give honest and complete information about safety even if the information is unfavourable. She keeps people informed about the big picture in program safety, and communicates frequently and effectively up, down, and across the program.

- **Integration** – In her approach to business as usual the proactive safety leader considers workplace health and safety as an integral element of program performance and encourages integral consideration of safety on all operational matters.

- **Action-Orientation** – the proactive safety leader avoids being reactive when addressing program safety issues – she gives timely, considered responses to safety concerns, demonstrates a sense of personal urgency and energy to achieve safety results, and demonstrates a performance-driven focus by delivering results with speed and excellence.

- **Feedback and Recognition** – the proactive safety leader is good at providing feedback and recognising people for their accomplishments – she publicly recognises the contributions of others, uses praise more often than criticism, gives positive feedback and recognition for good performance, and finds ways to celebrate accomplishments in program safety. She creates a safety culture where safety issues are more likely to be raised and addressed, rather than ignored or concealed.

- **Accountability** – the proactive safety leader practises accountability – she gives people a fair appraisal of the efforts and results in safety, clearly communicates people's roles in the safety effort, and fosters the sense that every person is responsible for the level of safety in their part of the program.

www.pwc.com.au