Report

2021 Australian Business Assurance Report

SAI GLOBAL

Executive Summary

The global pandemic presented many challenges for our business community since early 2020. Lockdowns, border closures, the health crisis and economic issues caused an increasingly complex risk and compliance environment. To understand the challenges currently facing businesses, SAI Global conducted a survey of 328 Australian executives. We found that to deal with the challenges facing them such as disrupted supply chains (21% of respondents), reduced business opportunities (14%) and high risks (13%), businesses have had to react in agile ways.

More than three quarters of businesses have made changes to survive. One in five had to change their product or service offering, while more common changes included adjusting health and safety procedures (42%), implementing new technologies (40%) and reducing budgets and resources (36%).

Our team also investigated the opportunities that will emerge in the post-pandemic recovery. Businesses will focus on initiatives to increase efficiency: 46% will streamline processes to drive their recovery, 39% will invest in internal capabilities, 35% will integrate management systems and 30% will implement new technologies to minimise disruptions.

The lessons learned since the first quarter of 2020 also present an opportunity for businesses to build resilience for other challenges.

Climate change is one of the biggest threats to our current way of life. The global fight against climate change is an issue facing us all: governments, businesses and individuals. Over the last few years, as Australia has been battling bushfires, severe droughts and record temperatures, businesses have increasingly started to prioritise sustainability initiatives. On a scale of 1 to 100, businesses, on average, will put 57% more budget, time and people towards environmental sustainability. Businesses are largely focused on improving waste management processes (57%) and reducing their energy consumption (48%).

Cybersecurity is another challenge facing our business community – and it is on the rise. In the last year, there has been a 60% increase in ransomware attacks against Australian businesses[1]. The COVID-19 crisis caused a dramatic shift in the way we work, with government restrictions forcing many businesses to rapidly adapt to remote working models which, in turn, created a range of challenges for corporate cybersecurity. The digital transformation was fast-tracked to adapt to these changes, expanding cyber vulnerabilities for organisations. Alarmingly, 68% of businesses are vulnerable to a cybersecurity attack.

Cyberattacks not only affect operations, but expose companies to any number of legal, financial, compliance and reputational disasters. The prevalent fears among businesses are that a cyber security attack will lead to financial loss (36%) or loss of intellectual property (32%). It is key for businesses to mitigate risks, and for organisational leaders to ensure all employees are trained to be alert to potential threats. Almost half of employees say their organisation needs people who are trained to identify risks and a third want organisations to ensure cybersecurity skills are retained within the organisation.

Changes to working practices also made businesses rethink their employee health and safety policies. Working remotely presents a whole new set of challenges for businesses, as does mitigating the risk of infection among employees in workplaces that remained open. Managing the health and safety of employees and customers is one of the most important risks any business must manage, and COVID-19 has helped to bring occupational health and safety (OHS) back to the attention of leadership and management. Thankfully, businesses say they will put 62% more resources (such as budget, time and people) toward employee health and safety than they have done previously.

Changes to industrial manslaughter laws in certain states can place legal liability on the highest levels of an organisation, yet 45% of employees say their senior leaders have not fully prepared their organisation to be compliant, and only half say their senior leaders are responsible for managing company OHS. To reduce their risk of liability in case of a workplace fatality, the highest-ranking leaders in an organisation must be actively and directly involved in the establishment of health and safety systems.

As we look ahead, we expect some of the challenges of 2020 to continue as the world opens up and we learn to live with COVID-19. As we move into the new normal, businesses need to continue to look ahead and ensure they have the systems in place to reshape a better future and build resilience against new challenges.

[1] Ms Rachel Nobel, Director-General, Australian Signals Directorate, speaking at the Parliamentary Joint Committee on Intelligence and Security: https://www.aph.gov.au/Parliamentary_Business/Hansard/Hansard_Display?bid=committees/commjnt/27d1412f-0716-454a-9b40-c8e8276eb931/&sid=0005

About the Study

SAI Global conducted a survey of 328 Australian businesses – 80% of which are SAI Global customers – to understand the challenges currently facing organisations. The purpose of the study was to gauge the impact of the COVID-19 crisis on businesses and how they will drive post-pandemic recovery and opportunities.

We also sought to understand how businesses manage employee health and safety, including in the context of new industrial manslaughter laws that, in some states, place legal liability on organisations and their C-suite executives and company directors should their actions cause an employee fatality.

Aside from the challenges of the global pandemic, we also sought to gauge the response by businesses to two major threats currently facing them: climate change and cybersecurity attacks.

We surveyed organisations across a range of industries and business sizes: small businesses (1-50 employees), medium-sized businesses (51-100 and 101-500), and large businesses (501-1000 and more than 1001).

The largest industry represented in the respondent panel was manufacturing (17%), followed by construction and engineering (14%) and professional services (8%).

KEY DEMOGRAPHICS OF RESPONDENTS

328

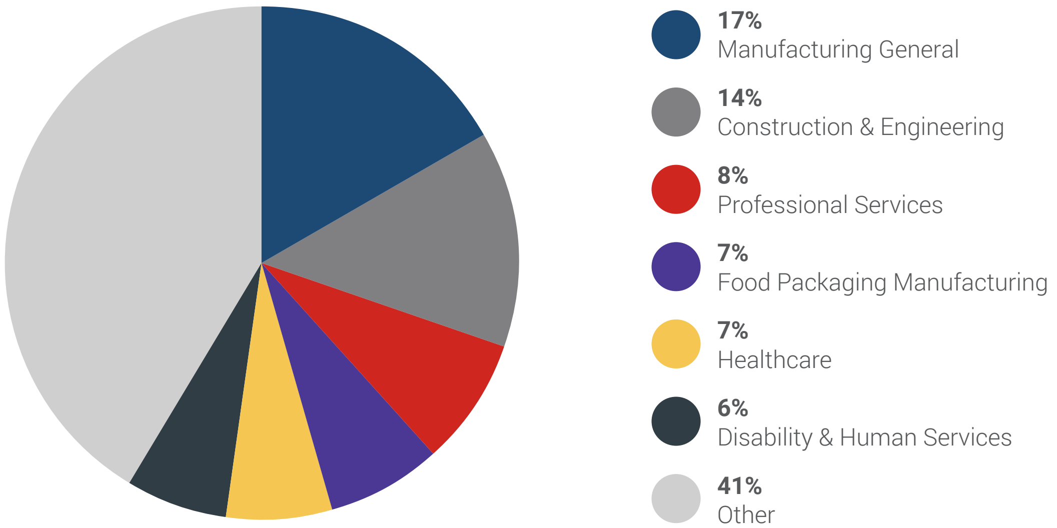
total respondents

Of these,

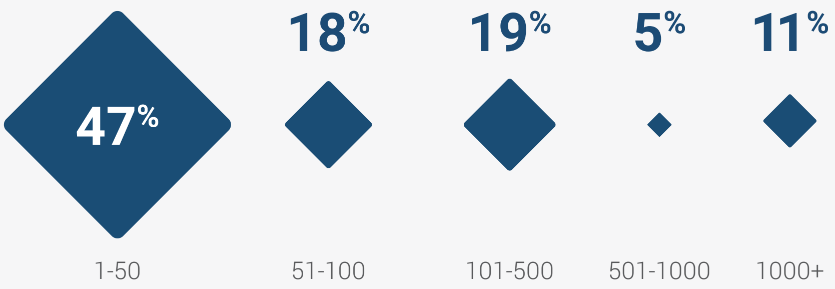
80%

are existing SAI Global customers

INDUSTRIES



KEY DEMOGRAPHICS OF RESPONDENTS BY BUSINESS SIZE (EMPLOYEES)



Problems Impacting Australian Businesses

The most common challenge currently facing businesses is impacted supply chains, according to one in five respondents.

While Australia comparatively escaped some of the worst impacts of the COVID-19 crisis, many of Australia's major trading partners were heavily impacted, causing myriad difficulties across the supply chain. In the early stages of the crisis, restrictions in China and then subsequently in other countries, meant production slowed. Transportation was also affected. Increased customer demand for goods purchased online, coupled with the reduced import capacity at ports around the world due to restrictions, caused further disruptions in supply chains and increased the cost of goods.

Australia's international and state border closures helped to soften the impact of the global pandemic locally, but they impacted the flow of goods and supply chains. Border closures and lockdowns also greatly reduced corporate travel, which led to reduced business opportunities – a problem 14% of organisations are currently facing.

In this unprecedented COVID-19 climate, it is no surprise the third most common problem facing organisations is high risks (13%).

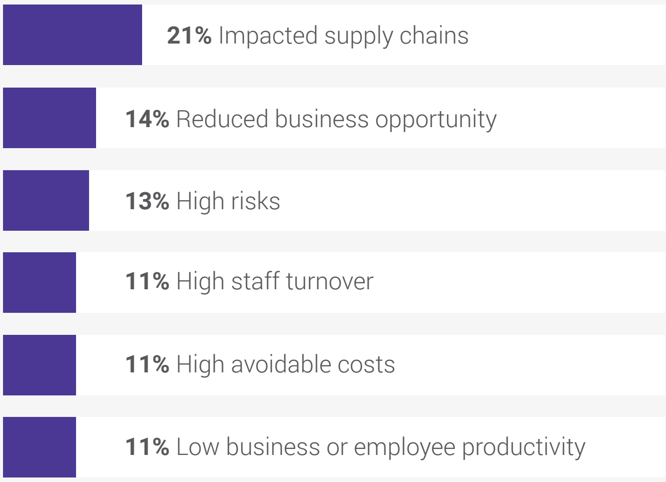
HOW BUSINESS PIVOTED DURING THE PANDEMIC TO SURVIVE

Businesses need to be agile to survive and adapt to the ever-changing COVID-19 environment. We found that more than three quarters of businesses made changes during the pandemic to survive.

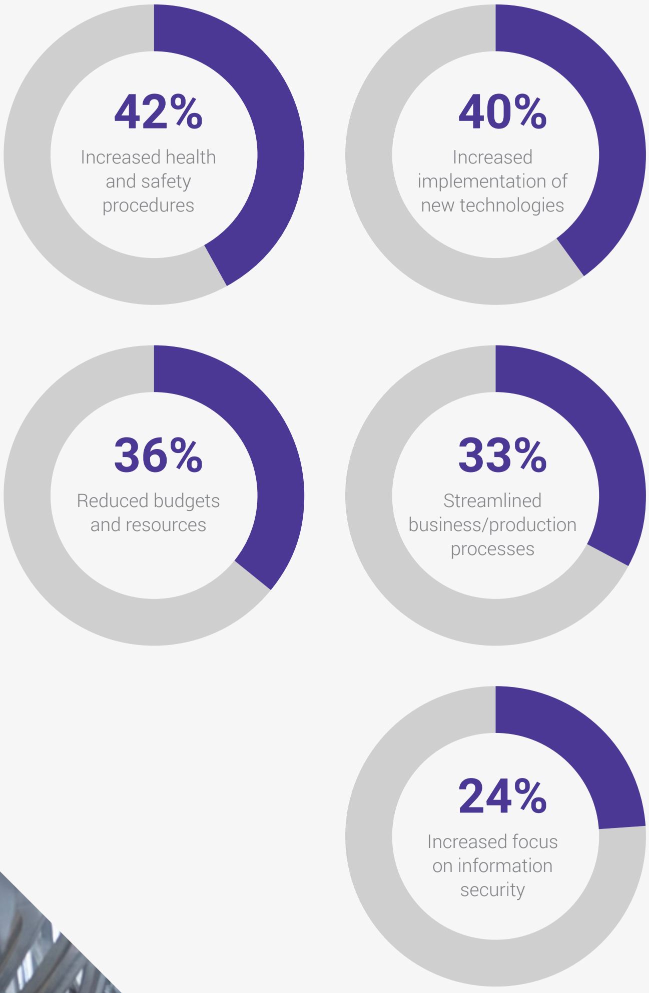
We asked organisations what initiatives they implemented: the most common response was increasing health and safety procedures (42%), followed by increasing implementation of new technologies (40%) and reducing budgets and resources (36%).

One in five (19%) businesses changed their product or service offering.

THE BIGGEST PROBLEM FACING BUSINESS:



THE CHANGES BUSINESSES MADE DURING THE PANDEMIC TO SURVIVE:



Looking Ahead: Post-Pandemic Recovery

The pandemic caught many businesses unprepared and brought unexpected impacts. While many organisations suffered losses or had to pivot their offerings in response to the pandemic, 31% of businesses say they thrived.

The pandemic accelerated changes in consumer and business behaviours: employees went home, businesses introduced new technologies to adapt, and consumers went online. These changes are likely to continue in a post-COVID-19 world.

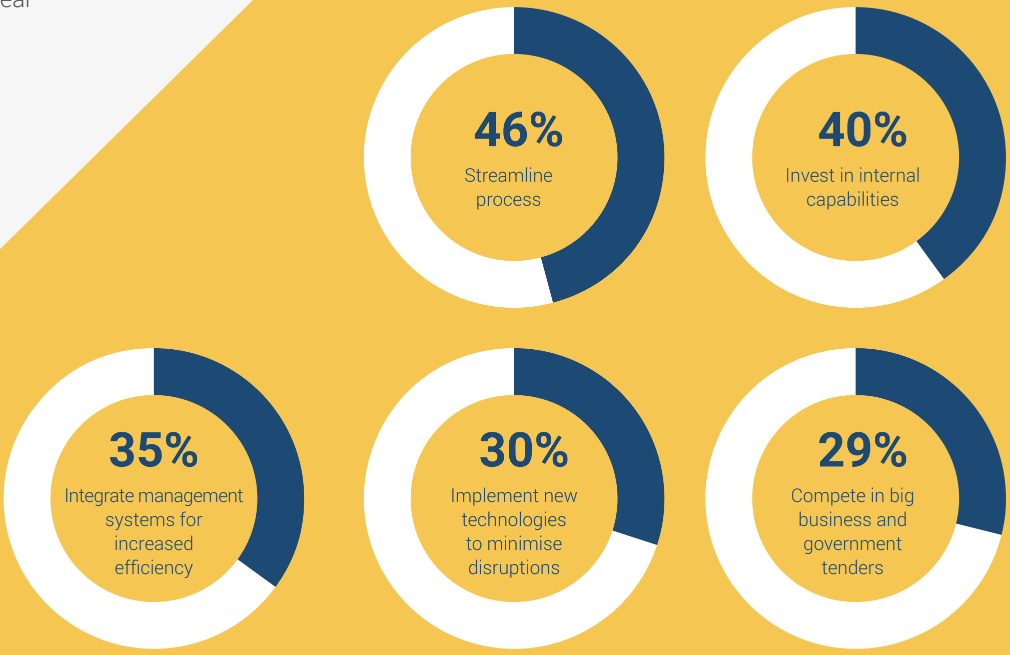
It also gave some businesses an opportunity to reset. Now, the recovery is a chance for businesses to reconfigure and look ahead to the opportunities that are available as we steer out of the global pandemic.

When asked how businesses will drive recovery and opportunity, the most common answers were around improving efficiency: 46% will streamline processes, 40% will invest in internal capabilities, 35% will integrate management systems and 30% will implement new technologies to minimise disruptions.

50% of businesses will focus on business recovery

31% of businesses said they thrived last year

WHAT INITIATIVES WILL YOUR ORGANISATION IMPLEMENT TO DRIVE BUSINESS RECOVERY AND OPPORTUNITY LOOKING AHEAD?



In Focus: Employee Health & Safety

Our survey did a deep dive into three risks that we believe pose significant threats to businesses: employee health & safety, environmental sustainability, and cybersecurity.

The International Labour Organisation (ILO) estimates that 2.3 million people die every year from work related accidents and disease[2]. Managing the safety of employees and customers is one of the most important risks all businesses must manage.

New industrial manslaughter laws legislated in Victoria, Queensland, Western Australia, the Northern Territory and the Australian Capital Territory.place legal liability on organisations and people, including C-suite executives and company directors, should their actions cause the death of an employee. Yet, our survey revealed that 45% of employees say their organisations have not made adequate changes to prepare for new industrial manslaughter laws. However, larger companies have taken more action: only 29% of large enterprises (more than 1001 employees) say no improvements have been made by senior leaders to fully protect the organisation.

Among businesses that are not fully protected, 30% have ot made any changes to be compliant and 15% have made some improvements, but not adequately to fully protect the organisation.

The highest-ranking leaders in an organisation must be actively and directly involved in the establishment, review of, and training around workplace safety systems to reduce their risk of personal liability and prosecution in case of a workplace fatality. Yet, one third of executives say their senior managers and leaders are not responsible for managing OHS in their organisation.

The most effective method of ensuring compliance with the new laws is certification to the latest international OHS standards. Thankfully, businesses say they will put 62% more resources (such as budget, time and people) toward employee health and safety than they have done previously.

45%

45% of businesses may not be fully protected against new industrial manslaughter laws.

29%

Only 29% of larger businesses (more than 1001 employees) are vulnerable.

62%

Businesses will, on average, put 62% more resources toward employee OHS.

33%

33% of respondents say their senior managers and leaders are not responsible for managing OHS in their organisation.

[2] International Labour Organization (ILO): https://www.ilo.org/moscow/areas-of-work/occupational-safety-and-health/WCMS_249278/lang--en/index.htm

In Focus: Environmental

A silver lining of the pandemic is that it shifted our current trajectory and allowed us to rethink our future.

As it recovers, Australia's business sector believes it can rebuild in a more sustainable way and focus more on environmental sustainability than it has done previously. On a scale of 1 to 100, businesses, on average, will put 57% more budget, time and people toward this goal.

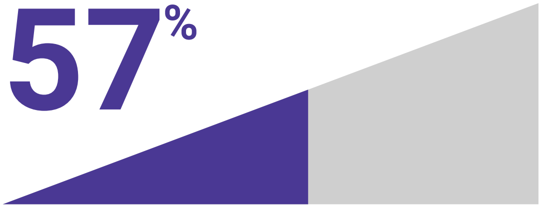
The majority (85%) of businesses are already taking measures to reduce their environmental impact. Almost three in five businesses are reducing waste management processes including reusing, refurbishing, recycling and disposal.

Organisations are also focused on reducing their emissions. Almost half of businesses are reducing their energy consumption, 24% are increasing local sourcing and 23% are reducing travel and product transportation.

Almost a third of businesses are reviewing their environmental policy. Adopting an environmental management system will improve an organisation's ability to develop and implement policies to deliver environmentally responsible and sustainable business practices.

SUSTAINABILITY GOALS

57%



On a scale of 1 to 100, businesses on average will put 57% more budget, time and people toward their environmental sustainability goals

THE TOP FIVE CHANGES BUSINESSES ARE UNDERTAKING TO IMPROVE THEIR ENVIRONMENTAL IMPACT:

57% **ONE**
Improving waste management process including reuse, refurbish, recycle and disposal

48% **TWO**
Reducing energy consumption

31% **THREE**
Reviewing their environmental policy

24% **FOUR**
Increasing local sourcing

23% **FIVE**
Reducing travel or product transport emissions

In Focus: Cybersecurity

Each year sees thousands of cyber attacks on businesses of all sizes in Australia. They pose an increasing threat to businesses and can be detrimental to an organisation if they result in data breaches, loss of income and/or loss or consumer trust.

The rapid change to remote working meant businesses had to scramble to install or adapt new technologies to aid the transition to working from home. The use of home WiFi networks and some employees having to use their own unprotected devices left companies open to a greater range of risks than ever before.

We found that, alarmingly, 68% of Australian businesses believe they are vulnerable to a cybersecurity attack or are not sure if they are vulnerable to a cybersecurity attack – and this vulnerability is more common among larger businesses: 65% of businesses with under 100 employees feel vulnerable, compared with 77% of businesses with more than 501 employees.

The myth that only larger businesses are the target of cyberattacks can lead to a false sense of security among small and medium-sized businesses. Approximately 144 reports of cybercrime relating to small business were reported every day to the Australian Cyber Security Centre in 2019, costing small businesses an estimated $300m per year[3].

Financial loss (chosen by 36% of respondents) is the most common fear for businesses when a cyberattack takes place, followed by the fear of losing intellectual property (32%). Almost one fifth (18%) worry about losing brand reputation and trust, yet only 7% of businesses worry that they will lose customers.

To mitigate the risk of cybersecurity attacks, 47% of businesses say they need to ensure skilled people are trained to identify and raise potential threats, while only 33% say they need to ensure that cybersecurity skills and knowledge are retained within the organisation.

The changing nature of how we work means cyberattacks have become increasingly sophisticated – from email phishing scams and hacktivists (hackers fighting for social and political issues) to data fraud involving disgruntled malicious employees, and cyberattacks on users of video conferencing services, both through data theft and unapproved access to virtual meetings. Businesses must now educate everyone in their organisation to be alert.

THE BIGGEST FEAR FOR BUSINESSES WHEN IT COMES TO A CYBERSECURITY ATTACK:

36%

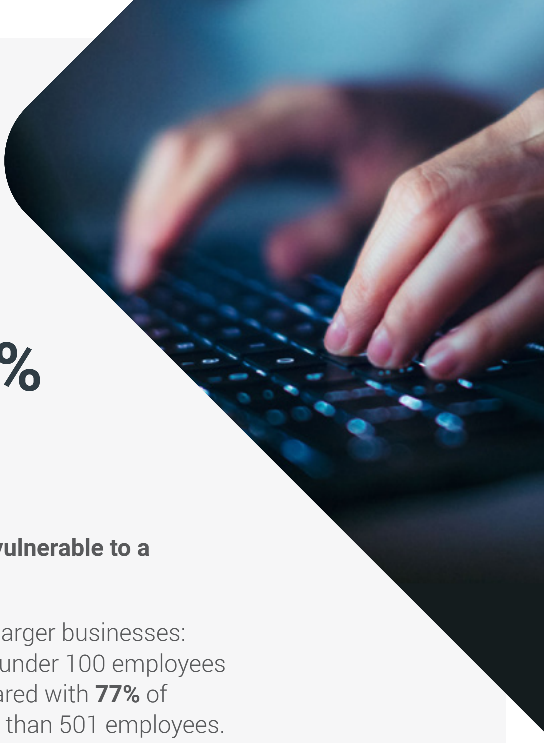
Financial loss

32%

Loss of intellectual property

18%

Loss of brand reputation and trust in the brand



68%

68% of business are vulnerable to a cybersecurity attack

This is higher among larger businesses: **65%** of business with under 100 employees feel vulnerable, compared with **77%** of businesses with more than 501 employees.

TO MITIGATE THE RISK OF CYBERSECURITY ATTACKS, BUSINESS SAY THEY NEED TO:

47%

Ensure skilled people are trained to identify and raise potential threats

40%

Ensure the organisation has the best cybersecurity technology, and it is updated

33%

Ensure that cybersecurity skills and knowledge are retained within the organisation

[3] Australian Institute of Criminology, 2021, 'Statistical Bulletin 34' https://www.aic.gov.au/sites/default/files/2021-07/sb34_estimating_the_cost_of_pure_cybercrime_to_australian_individuals.pdf

How businesses are using standards to solve their problems

The COVID-19 crisis caused a disruption and created an opportunity for companies to reconfigure and transform their operations. The way employees work has changed for good, new automation and digital technologies have been rapidly introduced, and a chance to rebuild back more sustainably means companies need to ensure quality internal operations.

New technologies have also led to an information revolution. Consumers have access to more information about an organisation's values, products and operations. The climate of increasingly demanding customer expectations means businesses need to deliver an impressive and transparent customer result. Meeting increasing customer expectations (chosen by 60% of respondents) is the largest driving force for an organisation to certify to a standard or scheme. Being required by government and other tenders or contracts (57%) was close behind, followed by the need to improve their products or service quality (52%).

Two thirds (67%) of the businesses surveyed have certified to a quality management system. An efficient quality management system, managed by a qualified organisational stakeholder, improves performance and internal efficiency, identifies inconsistencies and problems and recognises ways to resolve them.

A third (31%) of businesses have certified to OHS management systems, which provide a framework to establish OHS policies, processes and documentation to control the factors that could affect the health and safety of workers and customers.

To help achieve the goals set out in an organisation's environmental policy, environmental management systems – to which 29 per cent of businesses in the survey have certified to – is a set of business processes and documentation which control the conditions and factors impacting the environment, including air, water, land, natural resources, flora, fauna, human and their relationship, to achieve sustainability and respond to the changing environment.

Implementing management systems can streamline business processes, improve an organisation's performance and demonstrate their ability to meet the needs of their customers.

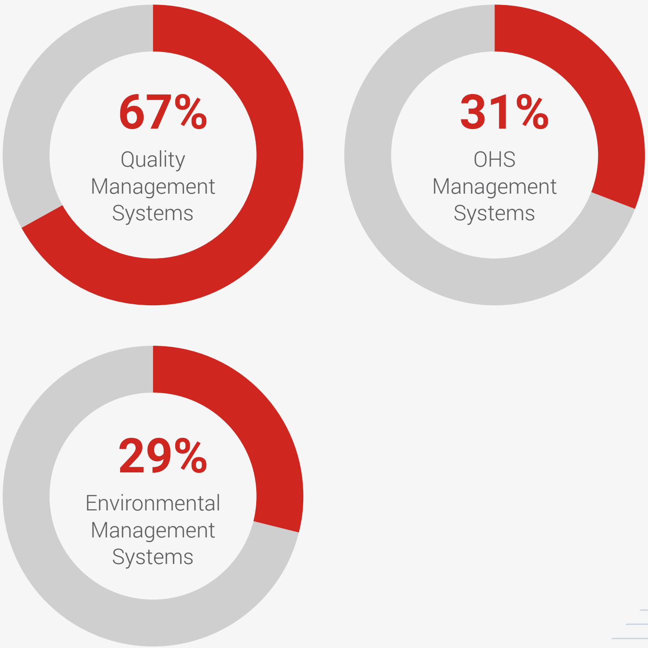
BUSINESSES ARE MOST LIKELY TO CERTIFY TO A STANDARD OR SCHEME DUE TO:

60% Meeting increasing customer expectations

57% Being required by government and other tenders and contracts

52% To improve their product or service quality

THE TOP THREE MANAGEMENT SYSTEMS, STANDARDS OR SCHEMES THAT ORGANISATIONS ARE CERTIFIED TO:



About SAI Global

At SAI Global Assurance, we understand the organisational challenges of building stakeholder trust and confidence at all stages of maturity. We work with organisations to help them meet stakeholder expectations for quality, safety, sustainability, integrity and desirability in any market and industry worldwide, while embedding a critical risk-based thinking and a continuous improvement culture.

SAI Global Assurance has offices in 21 countries and services clients globally, delivering more than 125,000 audits and training more than 100,000 students through its Assurance Learning courses each year.

Our services include:

- Audit and Inspection – An accredited certifying body with respected and independent expert auditors
- Learning and Training – Extensive range of accredited courses to support career advancement, career change or enhanced industry expertise
- Product Certification – Third-party certification against known standards for product conformance
- Business Advisory – An independent team to support business improvement and control, including your supply chains

Contact Us

For more information, or to find out how SAI Global Assurance can support your organisation, visit **saiassurance.com.au**

SAI GLOBAL