Grant Thornton
An instinct for growth™

GRANT THORNTON NEW ZEALAND BUSINESS RISK SURVEY 2012/2013

Delivering value to your company through risk management

Contents

Executive summary

The Grant Thornton business risk survey provides a snapshot of risk management in New Zealand in 2012.

We look at organisations with a range of views and perspectives, from the private/corporate sector to not for profits and the public sector. Some have embraced risk, others are struggling, while a third group is just beginning their journey of managing their organisations' risks. The public and private sectors have similar representation across the three categories identified, while the not for profit sector are more heavily represented in the starting out category.

No matter what the perspective, one thing is clear: those who actively practice risk management feel the benefits, with almost all reporting that risk management delivers value to their organisation. This view is not only reflected but driven at boardroom level and those organisations that do value risk management expect further investment in risk management.

Senior management however, do not value risk management as much as boards, this is a consistent view across all sectors, although least pronounced in the private sector and most pronounced in the public sector. Interestingly, risk managers generally believe their senior management and board perceive they receive greater value from risk management than is justified by the quality of risk management activity in their organisation.

Three quarters of all public sector organisations and businesses have used external assistance at some point. Chartered accountants are the preferred professional provider (51%) followed by insurance brokers and boutique risk consultants at 33% each.

When we look at the practice of risk management we find the 'leaders' in risk management used more of the risk management approaches we surveyed than those 'behind' or 'starting out' in risk management.

i: Risk management segmentation: what is implemented?

	Behind		Starting out		Leaders	
	Yes	**No**	**Yes**	**No**	**Yes**	**No**
Risk standard	77%	20%	60%	38%	88%	9%
Software	27%	70%	17%	81%	61%	37%
KRIs	50%	50%	64%	36%	64%	36%
Quantitative analysis	23%	77%	26%	74%	36%	64%
Event analysis	82%	18%	92%	8%	84%	16%
External advisers	95%	5%	30%	70%	100%	0%
Risk profile usage	50%	50%	77%	23%	93%	7%

Note: The difference from 100% are those risk managers who don't know what their organisation has implemented.

Interestingly boards valued more detailed risk reporting (operational, project and divisional/business risks), while senior management valued strategic and top or largest risk reporting more, potentially contradicting the view that boards are focused on the big picture while management is focused on the detail.

New Zealand organisations should take comfort in the fact that many appear to appreciate the value risk management can bring to their organisation. This survey identifies that there are changes to approaches and reporting which can increase the value received from risk management.

What does a typical risk manager look like?

The typical private sector risk manager

The typical private sector risk manager has a strong financial focus. They are likely to be the CFO, CEO or have another financial role. Almost half in our survey are employed by international companies. Many are in the manufacturing, construction or financial services industries. A primary focus for these companies is credit risk – this is more prevalent than for other organisation types. Risk managers in the private sector are more likely to use external advisers to help with financial risk than other sectors. Insurance brokers are strongly represented among the advisers they have used.

The core risk management team in the private sector is fairly large (around seven part time and two full time risk managers); meanwhile, there are relatively few risk champions in the wider organisation. Risk reporting doesn't feature as prominently as in public sector organisations. The main risk reporting channels are used much less frequently in the private sector (eg, strategic risks to the board once every 45 days on average, versus once every 23 days in a public sector organisation).

The typical private sector risk manager is highly experienced, with 14 years' experience on average.

The typical public sector risk manager

The typical risk manager in a public sector organisation has a risk and audit, assurance or compliance role. Their risk management team have around two core members and 10 risk champions in the wider organisation.

The public sector is more likely to have an organisation-wide risk profile, which is also used for annual business planning and internal audit and assurance planning. The risk profile is more likely to include strategic risk: over half of public sector organisations include it, while other organisation types are less likely to include it.

Risk is widely reported in the organisation: operational risks are often reported to divisional management continuously and to the board monthly. Strategic risks and project risks are also reported to the board regularly.

Public sector organisations are more likely than others to adhere to a risk management standard (typically ISO 31000) and to use risk management software.

The typical not for profit risk manager

The typical risk manager in a not for profit has a small risk management team, with around two part-timers in the core team and around three risk champions in the wider organisation. They are often the CEO or CFO of the organisation or have other financial responsibilities – a third of their role is risk management. The organisations generally don't have an organisation-wide risk profile.

The organisations tend to be in the 'starting out' in risk management segment and have a less formal approach to risk management. Few adhere to a risk management standard or use software. Over a third say risk management is not well understood in their organisation. A substantial number of these organisations are part of global organisations.

Risk management segmentation

We have created three categories of organisational risk management based on how respondents described their organisations approach to risk management. We have matched approach/process attributes to these categories to gain insight into whether the leaders in risk management are doing things differently to the rest. We broadly segmented the respondent organisations into the following categories:

'Behind' on risk management (n=44)
- Often describe their organisation's approach to risk as 'piecemeal', 'not well-understood', 'less formal', 'reactive' and 'nice-to-have' rather than essential
- Less likely than others to have an organisation-wide risk profile (half of them do)
- Like the 'leaders', they are likely to use external advisers (typically these are chartered accountants), but they are used for a different range of activities to the 'leaders'

'Starting out' with risk management (n=53)
- This group is the least experienced with risk management, but they are positive about it and still likely to have an organisation-wide risk profile
- They are likely not to have ever used an external adviser (70% have not)
- Four in ten haven't adopted a risk management standard. Few use risk management software
- They often describe their approach as 'less formal' but nonetheless 'well-understood'

Risk management 'leaders' (n=67)
- Often describe their organisation's approach to risk as 'formalised', 'proactive' and 'comprehensive'
- All of the 'leaders' have experience with external advisers, and are much more likely to use boutique consultants than others
- They are likely to use risk management software, and one in two have adopted the ISO 31000 standard
- The organisations generally have full time risk managers and risk champions in the wider business

These segments are referred to where relevant throughout this report. For demographics of risk managers who completed the survey refer to pages 39 - 40 under survey methodology.

ii: Risk management segmentation by sector

Sector	Behind	Starting out	Leaders
Public	33%	25%	42%
Private	20%	33%	47%
Not for profit	28%	72%	0%

There is little difference in risk management segmentation in the public and private sector and despite the apparent difference in the not for profit sector, this is probably more to do with the size and scale of the not for profits that responded to the survey, than how they have embraced risk management.

iii: Risk management segmentation - what is implemented?

	Behind		Starting out		Leaders	
	Yes	**No**	**Yes**	**No**	**Yes**	**No**
Risk standard	77%	20%	60%	38%	88%	9%
Software	27%	70%	17%	81%	61%	37%
KRIs	50%	50%	64%	36%	64%	36%
Quantitative analysis	23%	77%	26%	74%	36%	64%
Event analysis	82%	18%	92%	8%	84%	16%
External advisers	95%	5%	30%	70%	100%	0%
Risk profile usage	50%	50%	77%	23%	93%	7%

Note: The difference from 100% are those risk managers who don't know what their organisation has implemented.

Overall we can see the 'leaders' display the highlighted attributes more than the 'behind' group and those 'starting out'. 'Leaders' are significantly more likely to use risk management software, follow a risk management standard, use external advisers and utilise an organisation-wide risk profile.

Event analysis is common across all three categories and most common among those 'starting out'. The use of key risk indicators (KRI's) and an organisational risk profile is proportionately more for those 'starting out' than those in the 'behind' segment.

The 'starting out' segment is significantly less likely to use external advisers than the 'leaders' and those 'behind' in risk management. Interestingly, 95% of those 'behind' in risk management use external advisers. We explore each of these attributes in more detail in the body of this report.

Segmentation background

Delivering a useful segmentation is both an art and a science. We arrived upon the segmentations in this report using a 'blind' computerised process (a programme calculated several natural groupings of the respondents). The programme uses a clustering algorithm which is closest to Proc FastClus and K-means Clustering. It looks at all the responses that interviewees gave and calculates how similar those interviewees are overall and produces a number of possible solutions. It is then the role of the researcher, who is familiar with the data and what it means, to choose the most useful solution for our needs.

Attitudes towards risk

Risks are becoming more numerous or more severe

When organisations compare their current situations to 12 months ago, about half are facing more risks or more severe risks. Undoubtedly the perceived risks are amplified by the state of the global economy and national and international events such as the Christchurch earthquakes, Japanese tsunami and on-going unrest in the Middle East.

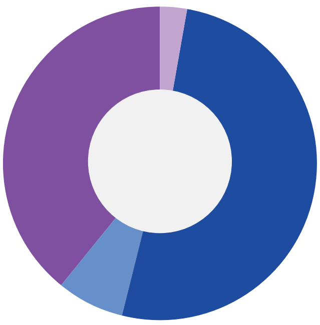
Perceived risks are higher among public sector organisations (six in ten). The changing political environment is potentially driving the public sectors' response to risk. The public sector continues to go through significant change and consolidation of resources and services. It faces a significant challenge to do more with less, a challenge which appears to be viewed as increasing their risk exposure.

Surprisingly, the not for profit organisations had the highest proportion reporting a decrease in risks, (however, it is important to note that the data used had a low base size of 14 interviewees). With the financial climate squeezing donation funding, changed government funding mechanisms and increasing demand for their services, we expected not for profits to report increasing risks.

Businesses in the private sector are more likely than their public sector peers to report no change in the number of risks versus a year ago (52% versus 28%).

1: Organisations' perceived risks

Q: Compared with twelve months ago, is your organisation facing either more risks and/or more severe risks, or is it facing fewer risks and/or less severe risks?



Base: all surveyed (n=174)

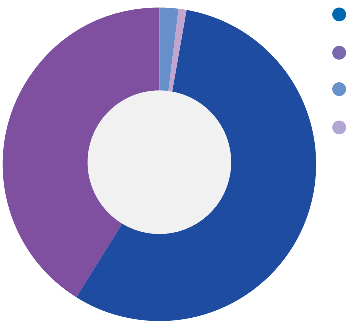
iv: Organisations' perceived risks by sector

	Public sector	Private sector	Not for profit sector
More or more severe risks	61%	39%	50%
Fewer or less severe risks	5%	8%	21%
No change	28%	52%	29%
Can't say	6%	1%	0%

Risk management delivers value but many senior managers don't see it

Almost everyone we surveyed believes risk management delivers value to their organisation. About six in ten believe risk management delivers significant value, while four in ten believe it delivers some value. Private businesses were more likely to view risk management as delivering significant value, about seven in ten. Not for profit organisations tend to be more likely to perceive risk management as delivering some value.

2: Value of risk management
Q: We'd like to know if risk management delivers value to your organisation: in your opinion, does risk management deliver



Base: all surveyed (n=174)

Most believe their organisation's senior management team does not value risk management as much as their board or audit committee does.

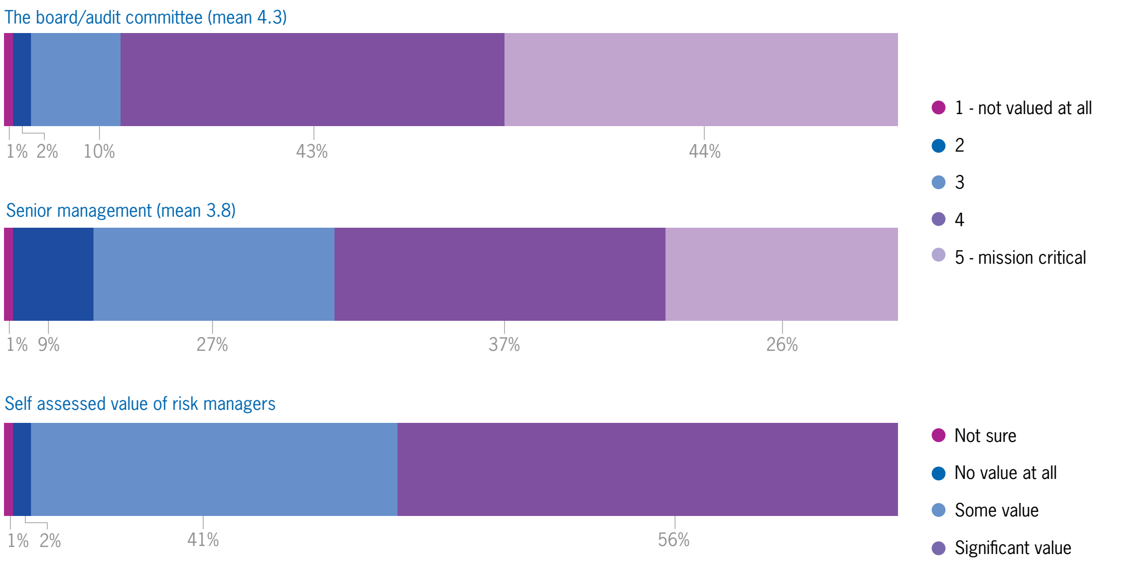
On a scale of 1 to 5, where 1 is risk management is 'not valued at all' and 5 is risk management is considered 'mission critical', respondents believe that their senior management teams value risk management at 3.8 on average. They also believe their boards or audit committees value risk management at 4.3, significantly higher than the senior management rating.

The 'behind' on risk management segment feels that senior management view risk management as having less value, being noticeably lower than the total sample with an average rating of 3.4.

Management attitudes appear to have a strong influence on the organisations' approach to risk, reflective of the importance of the 'tone of the top'.

3: Perceived value of risk management in organisations

Q: On a scale of 1 - 5, where 1 means risk management is not valued at all and 5 means risk management is mission critical, to what extent do senior management and the board/audit committee in your organisation value risk management?



Base: all surveyed (n=174)

Note: the perceived value of boards, audit committees and senior management, and the self-assessed value of risk management use different measurement bases so the results should be considered indicative only.

v: Perceived value of risk management in organisations by sector

		Public sector		Private sector		Not for profit sector	
Value		The board/ audit committee	Senior management	The board/ audit committee	Senior management	The board/ audit committee	Senior management
Low value	1 - not valued at all	0%	1%	3%	1%	0%	0%
	2	1%	11%	0%	5%	14%	14%
Low value sub-total		1%	12%	3%	6%	14%	14%
Neutral	3	9%	33%	12%	20%	7%	29%
High value	4	46%	35%	41%	40%	36%	36%
	5 - mission critical	44%	20%	44%	34%	43%	21%
High value sub-total		90%	55%	85%	73%	79%	57%

Boards and audit committees across all sectors are happy with the value that risk management delivers to their organisations. Interestingly senior management in both the public and not for profit sectors are not so comfortable with the value being delivered to their organisations.

If we compare the views of the risk managers to those of their senior management and boards (noting that the results are not directly comparable because of differing measurement scales being used), we find the following:

vi: Risk management viewed by organisation

	Significant value/high value	Some value/ neutral	Don't deliver value/ low value
Risk managers	56%	42%	2%
Senior management	63%	36%	1%
Board	87%	12%	1%

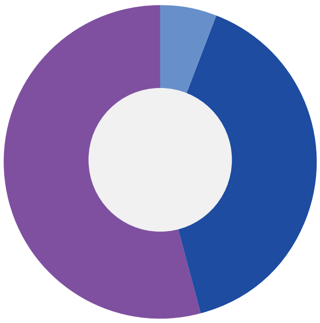
While not conclusive, it appears that risk managers' perception of the value they deliver is closely correlated to the views of senior management regardless of the value their board gain from risk management.

The difference between senior management and board perceptions of the value gained from risk management is consistent across all sectors, but the difference is greatest in the public sector.

Net increase in risk management budgets

A significant proportion of those surveyed report that their risk management budget increased over the past 12 months (two in five). About half report no change in their budgets, and very few report a decrease in budget. The private sector is significantly more likely than other organisations to report an increase in budget (56%).

4: Risk management budget: past 12 months
Q: Over the past twelve months, have risk management budgets and resources in your organisation generally increased or decreased?

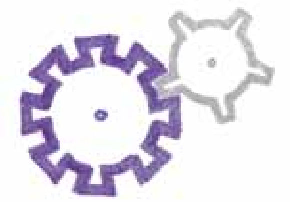


vii: Risk management budget past 12 months by sector

Sector	Increased budget	No change to budget	Decreased budget
Public	27%	62%	11%
Private	56%	41%	3%
Not for profit	29%	71%	0%

Risk managers tend to be optimistic about their future risk management budgets: about a third of the organisations believe they will get an increase in budget in the next 12 months. Six in ten believe there will be no change and, again, very few believe they will get a budget decrease. There is an apparent correlation between the perceived value of senior management and the increase or decrease in the risk management budget.

The public sector, whose senior management is perceived to value risk management the least by respondents, has the lowest expectation of increased budgets. While the private sector, whose management see greater value in risk management, have the highest expectation of increased budgets. We note there will be a number of other factors influencing budgets across the sectors. However, the private sector is more likely to feel risk management is 'essential' than public sector organisations. Public sector organisations are more likely than the private sector to see risk management as 'not well-understood'.



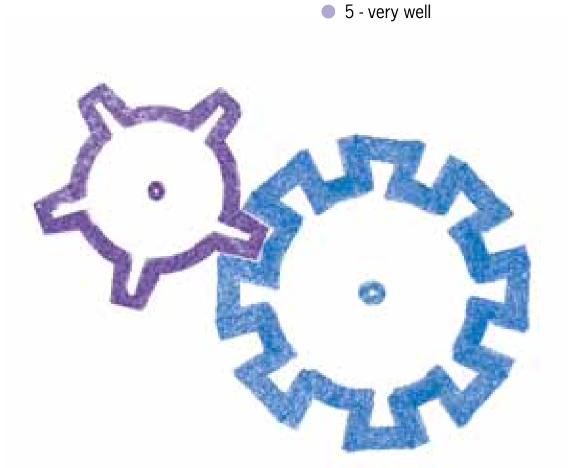
Most feel their organisations are managing risks well

On a scale of 1 to 5, where 1 is managing risks 'very poorly' and 5 is managing risks 'very well', the average organisation's rating is 3.5.
There is no significant correlation between how well the organisation is actually managing their risks and the senior management or board perception of value from risk management, with a greater perception of value than is indicated by the results below. Interestingly, while 53% of organisations believe they are managing their risk well or very well, 62% of organisations believe they are doing the right amount of risk management.

5: Organisations' risk management ratings
Q: On a scale of 1-5 where 1 means very poorly and 5 means very well, how well do you feel your organisation manages risk overall?

Organisations' risk management rating (mean 3.5)

Base: all surveyed (n=174)

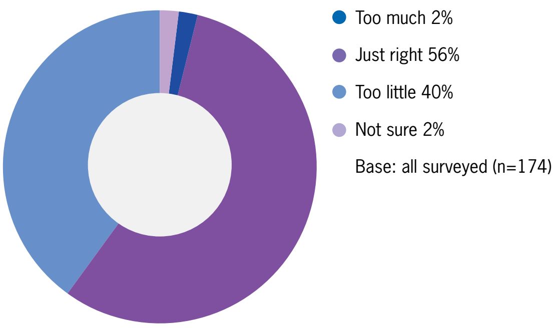


Two in five feel they do too little risk management

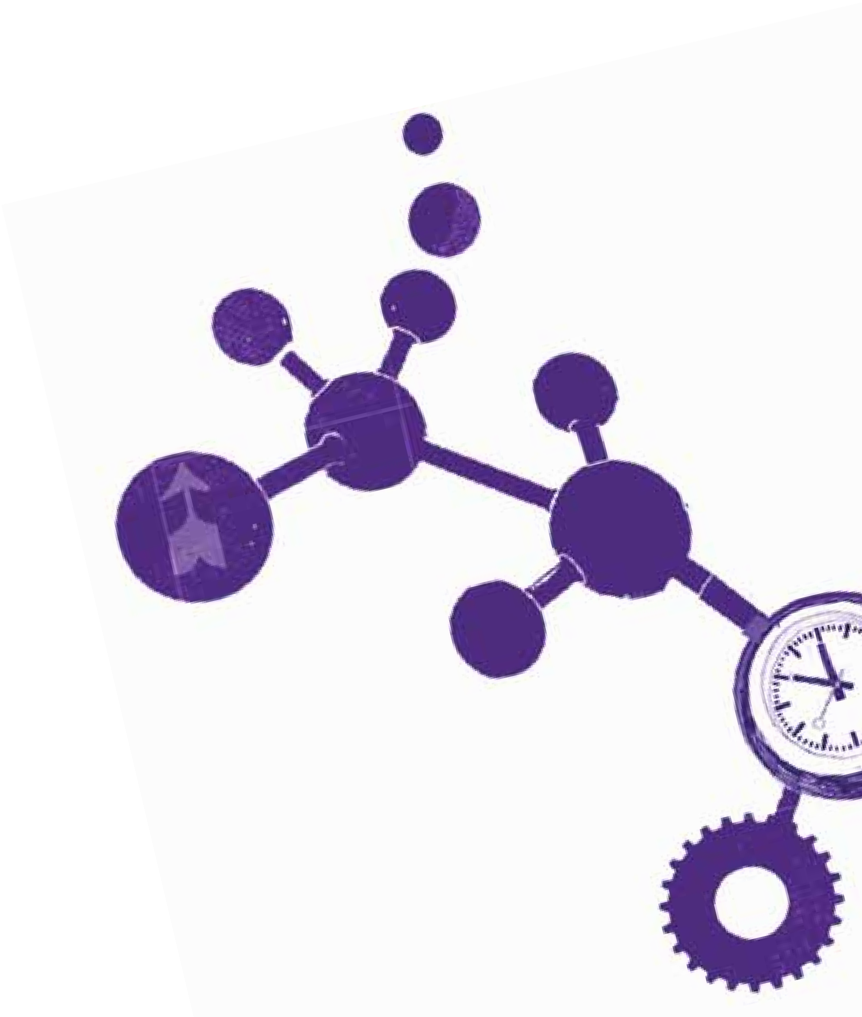
When we asked if the level of risk management in their organisation is right, half feel it is. However, two in five feel that their level of risk management is too little. Almost no one believes that their organisation does too much risk management. The private sector is more likely to say their organisations' risk management is just right, at about seven in ten. Organisations without a risk profile are more likely to say they are doing too little, at about six in ten.

6: Organisations' risk management levels

Q: Is your level of risk management right for your organisation, or is it too much or too little?



72% of private sector organisations think they do the right amount of risk management, compared with 56% of public sector organisations. Among the public sector respondents, 41% thought their organisation was doing too little risk management, significantly more than the 25% of private sector organisations who thought they were doing too little risk management.



Processes

Risk management standards

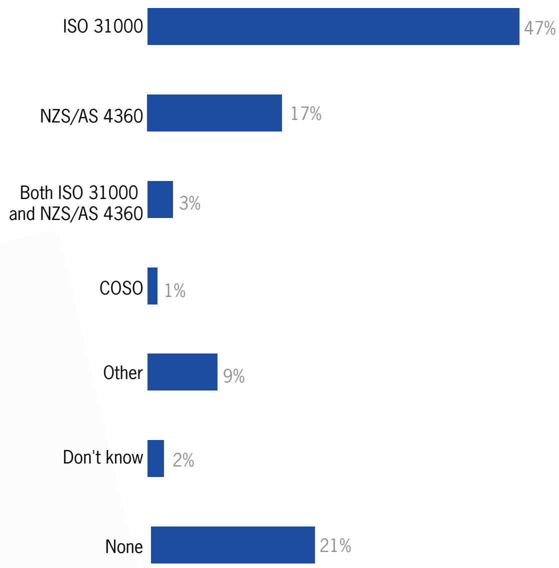
In order to understand how risk management works within different organisations we now look at tools and processes they currently have in place. Three out of four organisations (77%) have adopted a risk management standard, with ISO 31000 being mentioned most often.

The boards of organisations that adopt risk management standards value risk management more than those of organisations who have not adopted them. Organisations with a risk management standard are generally larger, with an average of 2.3 full time risk managers, while those without have an average of 0.7 full time risk managers.

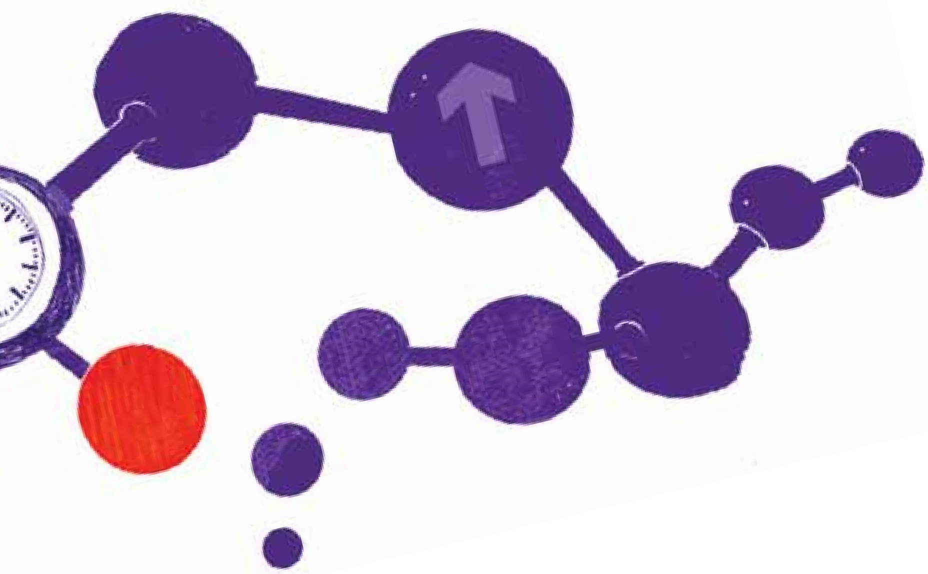
ISO 31000 is used by almost two-thirds of businesses that use a risk management standard. There is an on-going association with NZS/AS 4360: approximately one-fifth of businesses responded that their organisation uses NZS/AS 4360, and 3% mentioned both. Of concern are the 21% who have not adopted any standards.

7: Risk management standard adopted

Q: Many organisations adopt a risk management standard such as ISO 31000 or NZS/AS 4360. Which, if any, risk management standard has your organisation adopted?



Base: all surveyed (n=174)

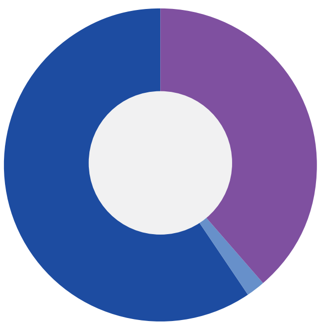


Risk management software used by around four in ten organisations

Almost six out of ten organisations use no form of risk management software. This is consistent across the public and private sectors, but in the not for profit sector nine out of ten organisations do not use software. Larger organisations are more likely to use software than smaller organisations. The boards and senior management of organisations that use some form of risk management software value risk management slightly more than those that don't.

Organisations that use software also rate themselves as being slightly better at risk management. If organisations have used a boutique risk management consultant they are significantly more likely to use some form of software than those who have used other or no external advisers.

8: Software use among organisations
Q: Which, if any, risk management software do you use?



viii: Software use among organisations by sector

Sector	Risk management software	None	Don't know/ no response
Public	44%	55%	1%
Private	38%	59%	3%
Not for profit	7%	93%	0%

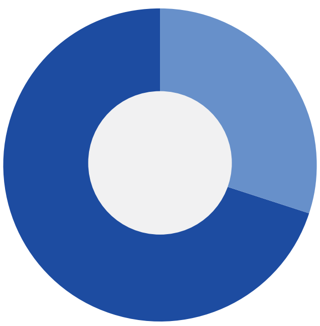
Quantitative techniques

In those organisations which use quantitative techniques, risk management is valued more by their boards and senior management. The same is true for organisations' overall risk management rating (how well or poorly the respondent believes their organisation manages risk). The larger the organisation the more likely they are to use quantitative techniques. Private sector organisations are also more likely to use quantitative techniques than public sector organisations, and twice as likely to use quantitative techniques than not for profit organisations.

Key risk indicators (KRIs)

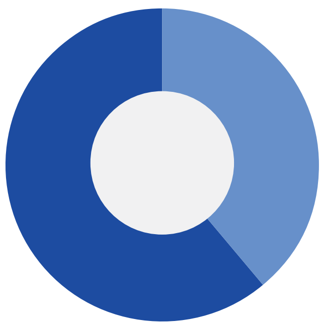
KRIs are used by around six out of ten organisations. The 'behind' segment on risk management is less likely to use KRIs: only one in two. Organisations with an environmental risk focus are more likely to use KRIs: around seven out of ten do. Organisations that have used insurance brokers or boutique risk management consultants are more likely to use KRIs than those that haven't. Boards and senior management of organisations who use KRIs value risk management significantly more than those that don't. Organisations that use KRIs also tend to have larger risk management teams. Private sector organisations are slightly more likely to use KRI's than public or not for profit sector organisations.

9: Quantitative techniques used among organisations
Q: Does your organisation use quantitative risk assessment techniques?



Base: all surveyed (n=174)

10: KRI use among organisations
Q: Does your organisation use key risk indicatiors (or KRIs) to monitor risks?



Base: all surveyed (n=174)

ix: Quantitative techniques used among organisations by sector

Sector	Use quantitative techniques	Don't use quantitative techniques
Public	27%	73%
Private	37%	63%
Not for profit	14%	86%

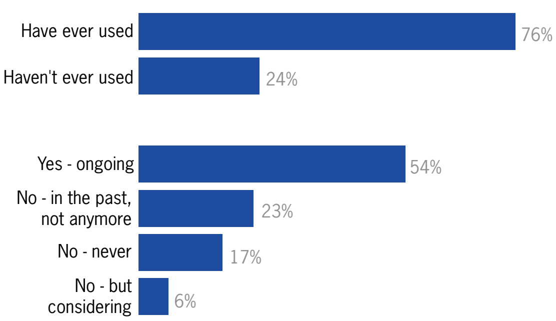
x: KRI use among organisations by sector

Sector	Use KRIs	Don't use KRIs
Public	58%	42%
Private	65%	35%
Not for profit	61%	39%

External support

Three in four organisations use some form of external adviser for risk management. About half the organisations surveyed are currently engaged in on-going external support. About one in five have used an external adviser in the past but no longer do so, and a similar proportion have never used external advisers before.

11: External adviser use among organisations
Q: Does your organisation ever use external professional advisers in risk management?



Base: all surveyed (n=174)

xi: External adviser use among organisations by sector

	Public sector	Private sector	Not for Profit sector
Have ever used	80%	76%	57%
Haven't ever used	20%	24%	43%
Yes ongoing	52%	60%	36%
No - in the past, not anymore	28%	16%	21%
No - never	14%	19%	29%
No - but considering	6%	5%	14%

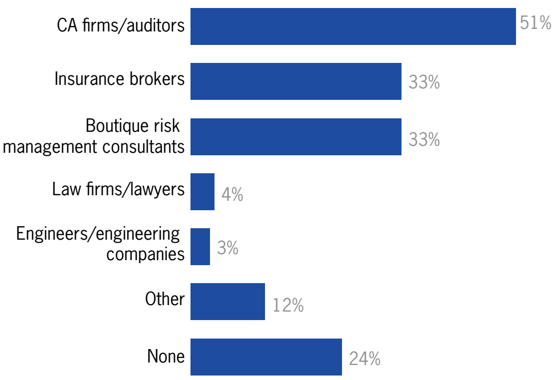
Not for profit organisations have lower-than-average usage of external advisers for risk management, at around one in two. Over three-quarters of both businesses and public sector organisations have used external advisers; businesses have slightly higher on-going usage, boosted by the number using insurance brokers.

Chartered accountants most common source of external advice

Among those who have used external advice, half have used a chartered accountancy firm. A third have used an insurance broker and the same proportion have used a boutique risk management consultant. One in four haven't used any type of external support.

12: External support type

Q: What sort of external professional advisers have you used in risk management?



Base: all surveyed (n=174)

Chartered accountancy firms have the highest level of on-going usage for external advice (a third currently use chartered accountants in risk management). Current usage of insurance brokers is at one in four and boutique risk management consultants are currently used by about one in five.

Organisations that used external support in the past, but not any more, were most likely to have used chartered accountancy firms or boutique risk management consultants.

Organisations use external providers to support a variety of activities including: risk management, audits, business continuity planning, technology risk, IT security, strategic, project, legal and financial risk to name but a few. On average, an individual organisation uses advisers for two activities.

The scale of the organisation predicts, to some degree, the type of external support they use. Organisations that have used boutique risk management consultants have slightly larger numbers involved in risk management than those organisations that have used chartered accountants or insurance brokers.

xii: Approach attributes by external adviser type

	Use chartered accountant		Use broker		Use boutique	
	Yes	**No**	**Yes**	**No**	**Yes**	**No**
Risk standard	73%	24%	74%	25%	82%	14%
Software	42%	58%	40%	58%	51%	46%
KRIs	65%	35%	67%	33%	65%	35%
Quantitative analysis	32%	68%	33%	67%	23%	77%
Event analysis	80%	20%	81%	19%	82%	18%
Risk profile usage	76%	24%	81%	19%	81%	19%

Note: The difference from 100% are those risk managers who don't know what, if any, external advisers have been used.

Organisations that use boutique risk management consultants are the most likely to adopt a risk management standard and risk management software, but are the least likely to use quantitative techniques. However, overall there appears to be a consistency of approach adopted by organisations that utilise external advisers, regardless of the source of the external advice.

Best practice ideas

Risk management standards such as ISO 31000 and COSO give organisations a benchmark and a way of keeping up with international practices – an aspect which is key for some of the risk managers we surveyed.

Professional advisers, especially chartered accountants, are frequently mentioned as a source of best practice ideas. Chartered accountants are particularly commonly mentioned among privately owned businesses.

The New Zealand Society for Risk Management is a commonly mentioned source of best practice. Other membership organisations are helpful to smaller groups of risk managers; eg, the Institute of Chartered Accountants and Institute of Internal Auditors.

Journals, websites and seminars provide a good source of best practice information by which risk managers keep up to date. Many subscribe to websites to receive regular news.

Those in the public sector tend to look to their peers in similar organisations for best practice. Software providers also provide best practice ideas to a handful of organisations.

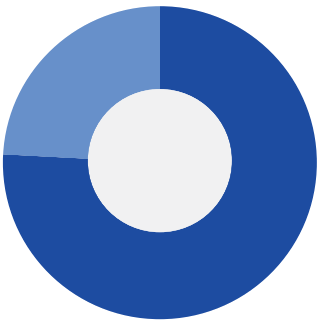
Monitoring risk

Risk profiles widely used and updated regularly

The majority of organisations surveyed produce an organisation-wide risk profile – about three quarters. There are differences in the usage of organisational risk profiles across the three sectors, with the public sector most likely to use a risk profile. The private sector is slightly less likely to utilise risk profiles and the not for profit sector is significantly less likely.

13: Organisation-wide risk profile use

Q: Does your organisation produce an organisation-wide risk profile? By risk profile we mean a summary of all the risks (or the key risks) an organisation faces – we're interested in the reporting of a consolidated risk position/profile (as compared to a business unit risk profile).



Base: all surveyed (n=174)

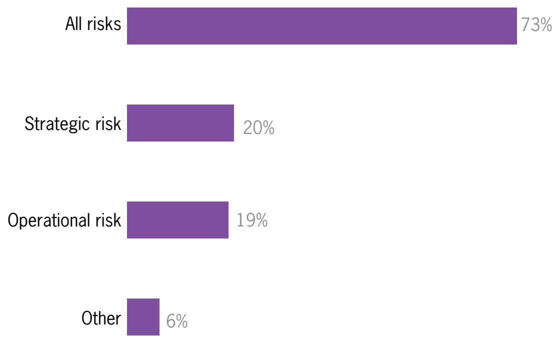
xiii: Organisation-wide risk profile use by sector

Sector	Yes	No
Public	84%	16%
Private	71%	29%
Not for profit	57%	43%

Three in four of these organisations produce risk profiles to cover all risks. One in five organisations produce risk profiles to cover strategic risk only, with similar numbers doing so for operational risk. 93% of organisations have a risk profile that covers strategic risks.

14: Risk profile coverage

Q: Which, if any, of these does your organisational risk profile cover? Would you say it covered all risks, or, you can choose more than one.

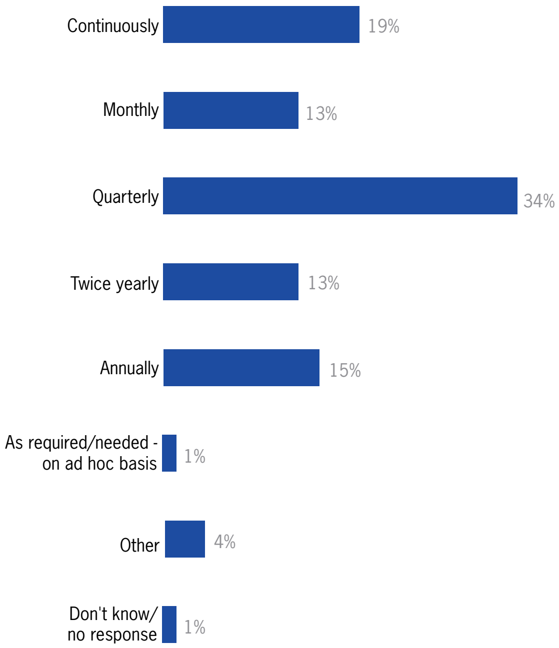


Base: all surveyed who have a risk profile (n=132)

Organisations typically update their risk profiles quarterly or less frequently. A substantial minority (19%) reported they update their risk profile continuously. Altogether the survey reveals that 32% of organisations update their profiles either continuously or monthly (13%). In our experience this takes a significant amount of time and resource and we question if this is the reality.

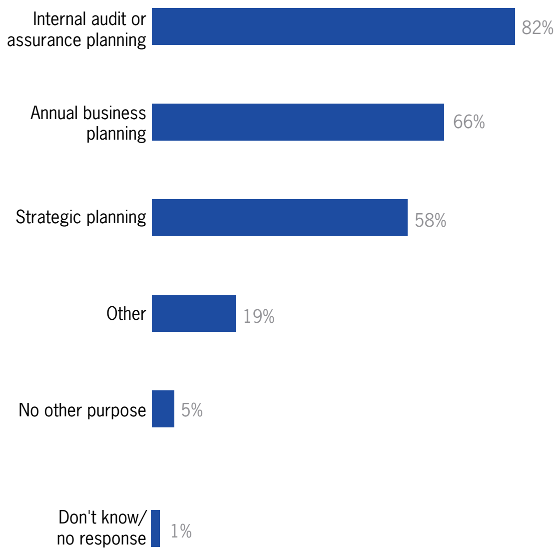
Public sector organisations are more likely to update at least quarterly. Businesses are more likely to update their risk profile less frequently, with most updating quarterly or less often.

15: Risk profile updating
Q: How often is your organisational risk profile updated?



Base: all surveyed who have a risk profile (n=132)

16: Risk profile additional usage
Q: Organisations sometimes use their risk profile for purposes other than risk management and reporting. Which, if any, of the following purposes does your organisation use the risk profile for?



Base: all surveyed who have a risk profile (n=132)

Almost all who produce a risk profile also use it for internal audits or assurance planning (eight out of ten). This is particularly popular in public sector organisations (nine in ten). Two-thirds of organisations use their risk profiles for annual business planning. Again, this increases for public sector organisations to about eight out of ten.

Eight out ten organisations prepare a risk profile but of those, one third don't use this to update their strategic or business planning. This begs the question: does the strategic or business planning process not include analysis of the organisation's risks, or are the risk profiles of insufficient quality to be relied upon for planning purposes?

xiv: Additional usage of risk profile by sector

	Public sector	Private sector	Not for profit sector
Internal audit or assurance planning (IA)	88%	73%	74%
Annual business planning (BP)	77%	51%	62%
Strategic planning (SP)	63%	53%	50%
Other	20%	19%	13%
No other purpose	1%	10%	12%

The public sector is more effective in utilising their risk profile for purposes beyond risk management than the private and not for profit sectors, with virtually all public sector respondents using their risk profile for purposes beyond risk management.

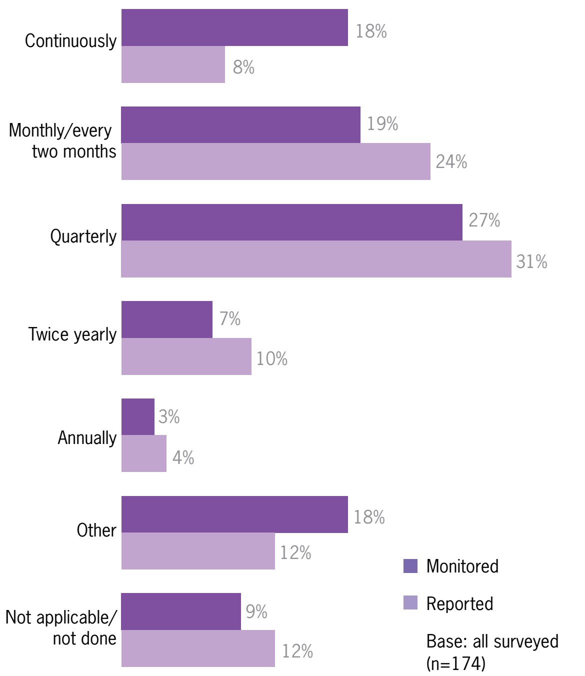
Around half of the private sector organisations utilise their risk profiles for business or strategic planning, with 20% of private sector respondents using their risk profile for internal audit planning but not business or strategic planning. One in ten use their risk profile solely for risk management in both the private and not for profit sectors.

Mixed management of high impact low likelihood risks

Organisations address very-high-impact but very-low-likelihood risks with a variety of approaches. About one in three monitors these risks quarterly. One in five monitors them monthly and another one in five continuously. These organisations, however, do not report the risks as frequently. Significantly fewer organisations report them continuously than those that do, moving instead to reporting either monthly or quarterly.

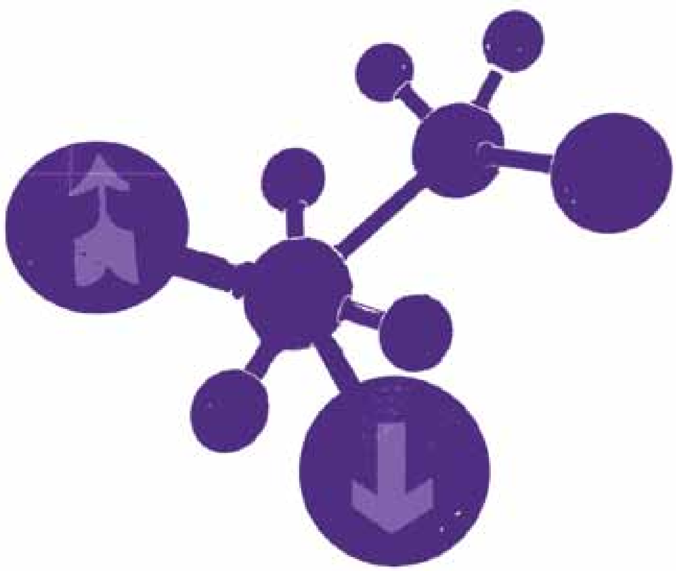
17: High-impact, low-likelihood risk management

Q: Now we'd like to know about your organisation's approach to very-high-impact, low-likelihood risks. Are high-impact, low-likelihood risks monitored and reported, and if so, how frequently?



xv: High-impact, low-likelihood risk management by sector

		Public sector	Private sector	Not for profit sector
Continuously	Monitor	23%	20%	15%
	Report	8%	11%	8%
Monthly/2 monthly	Monitor	24%	22%	15%
	Report	30%	22%	25%
Quarterly	Monitor	32%	30%	39%
	Report	39%	31%	25%
Twice a year	Monitor	7%	8%	15%
	Report	9%	15%	8%
Sub–totals for six months	Monitor	**86%**	**80%**	**84%**
	Report	**86%**	**79%**	**66%**
Annually	Monitor	5%	2%	0%
	Report	4%	6%	0%
Other	Monitor	4%	2%	0%
	Report	0%	2%	8%
Not done	Monitor	5%	16%	15%
	Report	10%	14%	25%



Across all sectors there is a consistent pattern of monitoring very-high-impact, very-low-likelihood risks on a more regular basis than these risks are reported. This pattern holds until the twice yearly (6 monthly) category by which point 86% of public sector organisations and 80% of private sector organisations have both monitored and reported very-high-impact, very-low-likelihood risks.

Between 10% and 25% of all organisations (depending on the sector), do not report very-high-impact, very-low-likelihood risks, with approximately 10% of all organisations not monitoring such risks.

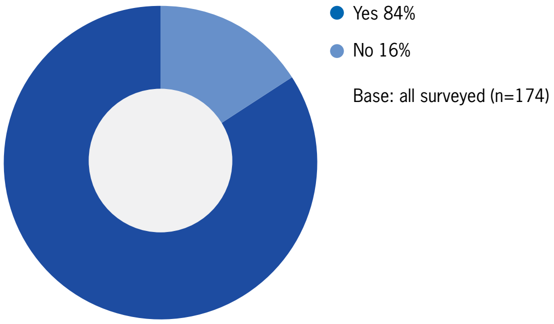
Incident/event analysis

The majority of organisations analyse incidents or events to assist in the analysis of risk – about eight out of ten. The risk management segment 'starting out' uses event analysis more, at about nine out of ten.

Both the boards and senior management of organisations who analyse events value risk management significantly more highly than those that don't. The same is true for organisations' overall risk management rating (how well or poorly they feel their organisation manages risk).

18: Event analysis in risk management

Q: Do you analyse incidents or events to assist in the analysis of risk for your organisation?



xvi: Event analysis in risk management by sector

Sector	Yes	No
Public	84%	16%
Private	87%	13%
Not for profit	79%	21%

Risk reporting

Many risks are reported to senior management monthly and boards quarterly

Risk reporting goes to the highest level of organisations, with the CEO as the first port-of-call. This is particularly evident in the public sector.

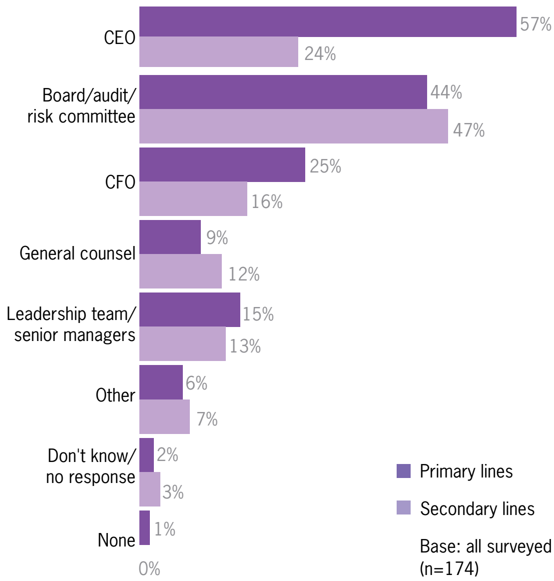
The CEO and the board are the most common primary reporting lines, followed by the CFO for one in four. An organisation's board is equally likely to be either the primary or secondary reporting at around two out of five. Boards are by far the most common secondary reporting line.

Organisations tend to have one or two primary reporting lines and most have one secondary reporting line.

As reflected in the table below, in the public and not for profit sectors the CEO is the most common primary reporting line, with the private sector more evenly split between the CEO and the board.

19: Primary and secondary risk management reporting lines

Q: What are your risk group's primary reporting lines? And your secondary reporting lines?



Base: all surveyed (n=174)

xvii: Primary and secondary risk management reporting lines by sector

	Public sector		Private sector		Not for profit sector	
	Primary	Secondary	Primary	Secondary	Primary	Secondary
CEO	60%	27%	51%	24%	71%	25%
Board/audit/risk committee	42%	51%	45%	48%	50%	68%
CFO	28%	22%	25%	13%	7%	17%
General counsel	8%	13%	11%	14%	0%	8%
Leadership team/senior managers	16%	16%	8%	4%	0%	0%
Other	7%	9%	5%	6%	7%	8%
Don't know/no response	1%	1%	3%	6%	7%	0%
None	1%	0%	0%	0%	0%	0%

Base: all surveyed (n=174)

What is reported?

Analysis of what is reported to the core interest groups of the board, senior management and divisional or line management shows us the following:

xviii: Risks reported and reporting lines

Public sector			
Type of risk	Board/governance	Senior management	Divisional line management
Strategic risks	81%	63%	15%
Top/largest risks	88%	60%	24%
New risks	67%	70%	41%
Operational risks	43%	76%	48%
Project risk	44%	69%	42%
Divisional /business unit risk	27%	76%	45%
Risk remediation	75%	86%	57%

Private sector			
Type of risk	Board/governance	Senior management	Divisional line management
Strategic risks	82%	49%	15%
Top/largest risks	79%	61%	22%
New risks	62%	74%	34%
Operational risks	54%	67%	39%
Project risk	49%	68%	38%
Divisional /business unit risk	39%	74%	43%
Risk remediation	68%	71%	33%

Not for profit sector			
Type of risk	Board/governance	Senior management	Divisional line management
Strategic risks	86%	50%	7%
Top/largest risks	79%	57%	7%
New risks	77%	62%	23%
Operational risks	69%	54%	23%
Project risk	31%	62%	23%
Divisional /business unit risk	50%	83%	25%
Risk remediation	85%	62%	23%

We can dig deeper into how different kinds of risk are reported to different people in an organisation. The board and senior management are very likely to have some type of risk reported to them (nine in ten do), while half of the organisations report some form of risk to divisional/line management.

An organisation's board or governance body is most likely to receive reports of strategic and the most significant risks (about three-quarters of organisations do so). Senior management is most likely to have new risks, operational risks, divisional/business unit risks, and project risks reported to them (about six in ten organisations have each of these reporting lines).

Analysis of what is reported shows reporting of strategic risks and the top or largest risks to be fairly consistent across all three sectors for the board, senior management and divisional management.

In the public and private sectors, under half of divisional management receive reporting on their operational risks, falling to only a quarter for the not for profit sector. Three quarters of senior management (across all three sectors) receive reporting on divisional/business unit risks, but again under 50% of divisional management receive this reporting. This does not appear to be consistent with the "communicate", "monitor" and review" expectations of ISO 31000.

Given that projects, by their nature, should be strategic to the organisation and the sobering statistics around project success rates, it is surprising that under half of all boards and less than 70% of senior management receive any form of reporting on project risk. Conversely, it is pleasing to see a high proportion of senior management and boards receiving risk remediation reporting.

Risk is most commonly reported monthly, although quarterly and continuously is also common practice, depending on the kind of risk and to whom it is reported.

Senior management deal with risks more frequently than boards or governing bodies. Senior management also deal with the more significant risks, new risks, strategic risks, and divisional or business unit risks on a continuous and monthly basis. Boards and governing bodies deal with significant risks, strategic risks, new risks, and divisional or business risks on a quarterly basis.

When organisations take action to remediate controls or mitigate risks, the status of these actions is reported in much the same way. Senior management and board/governing bodies are equally likely to be reported to (about seven out of ten organisations do each). Divisional/line management are less likely to be involved (mentioned by around two out of five).

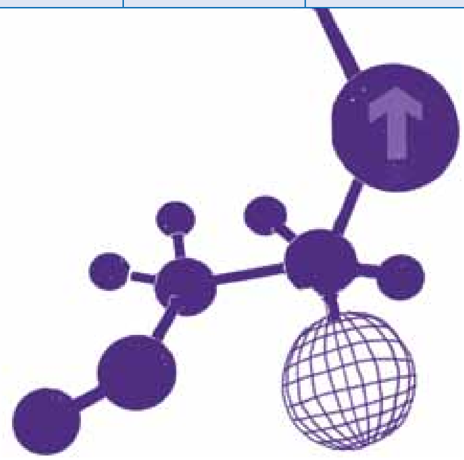
xix: Risks reported by perceived value

Comparison of risk reporting to senior management and board, and perceived value of risk management by senior management and board.

Public sector		
Risk type reported	Senior management high value (4 or 5)	Board high value (4 or 5)
Strategic risks	58%	91%
Operational risks	53%	91%
Project risks	51%	94%
Top/largest risks	57%	90%
New risks	61%	94%
Divisional risks	61%	90%
Risk remediation	64%	93%

Not for profit sector		
Risk type reported	Senior management high value (4 or 5)	Board high value (4 or 5)
Strategic risks	43%	83%
Operational risks	29%	78%
Project risks	50%	75%
Top/largest risks	50%	82%
New risks	50%	80%
Divisional risks	40%	100%
Risk remediation	50%	82%

Private sector		
Risk type reported	Senior management high value (4 or 5)	Board high value (4 or 5)
Strategic risks	88%	88%
Operational risks	69%	92%
Project risks	74%	94%
Top/largest risks	81%	87%
New risks	73%	89%
Divisional risks	71%	92%
Risk remediation	73%	85%



Linking the perceived value rating of senior management and boards to what is reported gives us some insight into what board reporting is valued, or at least what reporting is received by senior management and boards who value risk. On the assumption that senior management and boards have the ability to change what is reported, this analysis should be a reasonable proxy for the risk reporting these two key groups value.

The consistent pattern is that boards value all risk reporting more than senior management, reflecting that boards value risk management more than senior management.

There is an interesting trend for boards who value risk management to receive reporting on operational, project and divisional risks. Significantly lower level risk information than valued by senior management and potentially reflective of the hands-on nature of management compared with the oversight role of the board.

In the public sector, senior management who value risk management are more likely to want reporting on new and divisional risks as well as risk remediation. They are less likely to value reporting on operational risks and project risks. Public sector boards are more likely to value reporting on project and new risks as well as risk remediation but less likely to value reporting on the top or largest risks and divisional risks.

In the private sector, senior management who value risk management are more likely to value reporting on strategic and the top or largest risks, and less likely to want reporting on operational, divisional and new risks or risk remediation. Private sector boards are more likely to want reporting on operational, project and divisional risks, and less likely to value reporting on risk remediation, the top or largest, strategic and new risks.

In the not for profit sector, senior management who value risk management are more likely to want reporting on strategic and the top or largest risks, and less likely to get reporting on project, the top or largest and new risks as well as risk remediation. They are less likely to value reporting on operational, strategic and divisional risks. Not for profit boards are more likely to want reporting on divisional, strategic and the top or largest risks as well as risk remediation, and less likely to value reporting on project, operational and new risks.

Self assessment

Survey results

Processes

Many organisations adopt a risk management standard such as ISO 31000 or NZS / AS 4360. Which, if any, risk management standard has your organisation adopted?

		Your answer
ISO 31000	47%	
NZS/AS 4360	17%	
Both ISO 31000 and NZS/AS 4360	3%	
COSO	1%	
None	21%	
Don't know	2%	
Other	9%	

Does your organisation use quantitative risk assessment techniques?

		Your answer
Yes	30%	
No	70%	

Does your organisation use key risk indicators (KRIs) to monitor risk?

		Your answer
Yes	61%	
No	39%	

We'd like to know which specific risk management areas your organisation focuses on. For each of these areas please tell me if your organisation has this risk management focus area. You may choose more than one.

		Your answer
Risk management	19%	
Insurance risk	17%	
Audits	16%	
Business continuity planning	15%	
Strategic risk	12%	
Technology risk - IT security	12%	
Project risk - project management	11%	
Financial risk	11%	
Risks/risk assessment	11%	
Review/design framework	7%	
Legal	7%	
Operational risk	6%	
Environmental risk	5%	
Credit risk	5%	
Health and Safety/Safety	5%	
Fraud	5%	
Security	3%	
Property	3%	
Information security	2%	
Clinical risk	2%	
People/personnel	2%	
Foreign currency/exchange	1%	
Compliance	1%	
Market risk	1%	
Other	38%	
None	1%	

External support

Does your organisation ever use external professional advisers in risk management?

		Your answer
Yes - ongoing	54%	
We have in the past, but not anymore	23%	
No, never	17%	
No, but considering using external adviser	6%	

What sort of external professional advisers have you used in risk management?

		Your answer
Chartered Accountancy firms	51%	
Insurance brokers	33%	
Boutique risk management consultants	33%	
Law firms	4%	
Engineering firms	3%	
Other	12%	
None	24%	

For which activities have you used professional external advisers?

		Your answer
Risk management	19%	
Insurance risk	17%	
Audits	16%	
Business continuity planning	15%	
Strategic risk	12%	
Technology risk	12%	
Project risk	11%	
Risk assessment	11%	
Review/design framework	7%	
Legal risks	7%	
Operational risk	6%	
Environmental risk	5%	
Credit risk	5%	
Health and safety	5%	
Fraud	5%	
Other	38%	

Monitoring risk

Does your organisation produce an organisation-wide risk profile?

		Your answer
Yes	76%	
No	24%	

Which, if any, of these does your organisational risk profile cover?

		Your answer
All risks	73%	
Strategic risk	20%	
Operational risk	19%	
Other	6%	

How often is your organisational risk profile updated?

		Your answer
Continuously	19%	
Monthly	13%	
Quarterly	34%	
Twice yearly	13%	
Annually	15%	
Adhoc	1%	
Other	4%	
Don't know	1%	

Organisations sometimes use their risk profile for purposes other than risk management and reporting. Which, if any, of the following purposes does your organisation use the risk profile for?

		Your answer
No other purpose	5%	
Internal audit or assurance planning	82%	
Annual business planning	66%	
Strategic planning	58%	
Other	19%	
Don't know	1%	

Compared with twelve months ago, is your organisation facing either more risks and/or more severe risks, or is it facing fewer risks and/or less severe risks?

		Your answer
More or more severe risks	51%	
No change	39%	
Fewer or less severe risks	7%	
Can't say	3%	

Now we'd like to know about your organisation's approach to very high-impact, low-likelihood risks. Are very high-impact, low-likelihood risks monitored and reported, and if so, how frequently?

	Monitored	Reported	Your answer
Not monitored or reported	9%	12%	
Continuously	18%	8%	
Monthly/every 2 months	19%	24%	
Quarterly	27%	31%	
Twice yearly	7%	10%	
Annually	3%	4%	
Other	18%	12%	

Do you analyse incidents or events to assist in the analysis of risk for your organisation?

		Your answer
Yes	84%	
No	16%	

Risk reporting

What are your risk group's primary reporting lines? And your secondary reporting lines?

	Primary	Secondary	Your answer
Board/audit committee	44%	47%	
CEO	57%	24%	
CFO	25%	16%	
General counsel	9%	12%	
Leadership/senior managers	15%	13%	
Other	6%	7%	
None/don't know	3%	3%	

Could you tell us if each of these risks is reported, and if so to whom? You can choose more than one.

	Board/governance body	Senior management	Divisional/line management	Your answer
Strategic risks	76%	52%	13%	
Operational risks	45%	64%	39%	
Project risks	40%	60%	34%	
Top/largest risks	76%	55%	36%	
New risks	56%	60%	31%	
Divisional/Business	29%	64%	36%	

Whenever your organisation takes action to control or mitigate risk, is the status of those actions reported? To whom?

		Your answer
Not reported	3%	
Board / Governance body	67%	
Senior management	71%	
Divisional / Line management	40%	
Other	14%	

We'd like to know if risk management delivers value to your organisation: In your opinion does risk management deliver:

		Your answer
Significant value	56%	
Some value	41%	
No value at all	2%	
Not sure	1%	

On a scale of 1-5 where 1 means risk management is not valued at all, and 5 means risk management is mission critical, to what extent do senior management and the board/audit committee in your organisation value risk management?

	Senior management	The board/audit committee	Your answer
5 - risk management is considered mission critical	26%	44%	
4	37%	43%	
3	27%	10%	
2	9%	2%	
1 - risk management is not valued at all	1%	1%	

Over the past twelve months, have risk management budgets and resources in your organisation generally increased or decreased?

		Your answer
Increased	40%	
No change	54%	
Decreased	6%	

And over the next twelve months, do you expect risk management budgets and resources in your organisation to increase or decrease?

		Your answer
Increase	35%	
No change	58%	
Decrease	7%	

If you could describe your organisation's approach to risk, which, if any, of these words might you use? You can choose as many as you like, or suggest your own.

		Your answer
Reactive	41%	
Proactive	72%	
Comprehensive	51%	
Piecemeal	32%	
Not well-understood	30%	
Well-understood	57%	
Essential	64%	
Nice-to-have	20%	
Formalised	55%	
Less formal	41%	
Others	41%	

On a scale of 1-5 where 1 means very poorly and 5 means very well, how well do you feel your organisation manages risk overall?

		Your answer
1 - very poorly	1%	
2	8%	
3	38%	
4	45%	
5 - very well	8%	

Is your level of risk management right for your organisation, or is it too much or too little?

		Your answer
Too much	2%	
Just right	56%	
Too little	40%	
Not sure	2%	

The survey methodology

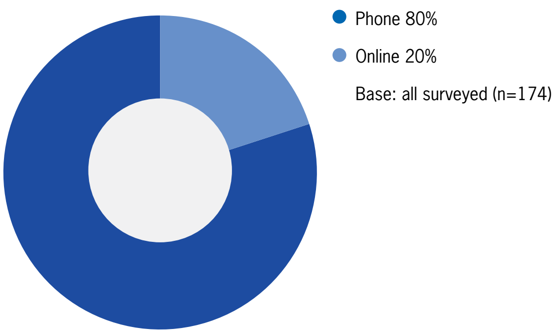
The Grant Thornton business risk survey was commissioned by Grant Thornton New Zealand, an independent member firm of Grant Thornton International, one of the world's leading accounting and consultancy firms providing services globally. We wish to thank the New Zealand Society for Risk Management for their support and involvement in the development of this survey.

Grant Thornton commissioned Ipsos (the world's third largest independent market research company) to conduct the interviews and utilised their research methodologies and analysis tools to prepare the initial data analysis.

The survey used two methodologies. Respondents from the Grant Thornton database were contacted and interviewed by telephone. An email invitation to an online version of the interview was sent to the members of the New Zealand Society for Risk Management. A note was included in the interview introduction to avoid anyone completing the interview twice if they appeared on both databases.

The majority of interviews (eight out of ten) were completed by telephone.

20: Contact method

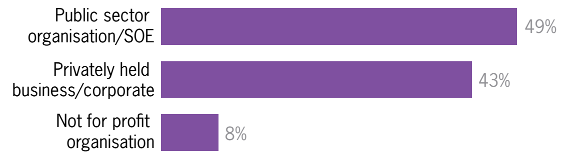


Base: all surveyed (n=174)

About the survey participants

We completed interviews with privately held, corporate, public sector and not for profit organisations.

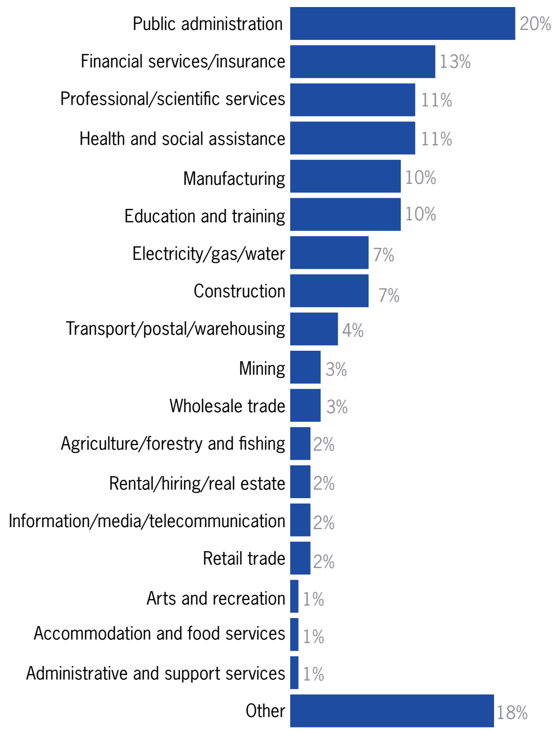
21: Business type



Base: all surveyed (n=174)

22: Industry sector

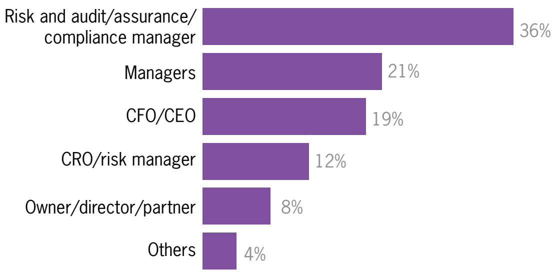
Q: Which industry sector does your organisation operate in? You can choose more than one.



Base: all surveyed (n=174)

The roles of the people we talked to varied from organisation to organisation. About one in two is directly involved in risk management, audit, assurance or compliance. About one in ten has a job which is dedicated to risk management.

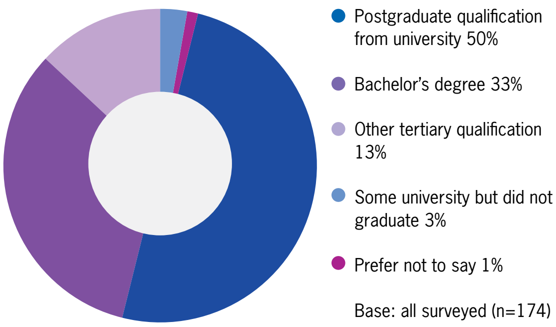
23: Job title
Q: What is your job title?



Base: all surveyed (n=174)

The people within the organisations we talked to were highly educated, with about half having a postgraduate qualification. Almost all had a tertiary qualification.

24: Highest level of education
Q: Which of these best describes the highest level of formal education you have achieved so far?



Base: all surveyed (n=174)

The questionnaire

The interview script was prepared by Ipsos based on Grant Thornton's questionnaire. The questionnaire was reviewed by representatives of the New Zealand Society for Risk Management to ensure the appropriate language and topics were covered. A range of questions were included on five topic areas:

- Attitudes towards risk
- Processes
- External support
- Monitoring risk
- Risk reporting

Some minor differences between the telephone and online versions of the questionnaire were introduced to accommodate the interview medium.

Segmentation background

Delivering a useful segmentation is both an art and a science. The segmentation groupings derived in this report use a 'blind' computerised process (a programme calculated several natural groupings of our respondents). The programme uses a clustering algorithm which is closest to Proc FastClus and K-means Clustering. It looks at all the responses that interviewees gave and calculates how similar those interviewees are overall, and provides a number of possible solutions. It is then the role of the researcher, who is familiar with the data and what it means, to choose the most useful solution for our needs.

A 'blind' computerised approach does mean that segments are not neat: for example, you won't find that 100% of not for profit respondents fit in a particular segment. We describe the segments talking about how they tend to do X or skew towards people in category Y.

About Grant Thornton

Grant Thornton New Zealand

Grant Thornton New Zealand is a member of Grant Thornton International, one of the world's leading organisations of independently owned and managed accounting and consulting firms. We have approximately 530 offices worldwide providing assurance, tax and advisory services to privately held businesses and public interest entities. We navigate the complexities of dynamic organisations by unlocking their potential for growth and wherever our clients do business, we will deliver valuable advice that makes a difference.

More than 2,600 partners and 31,000 staff provide clients with distinctive, high quality and personalised service in over 100 countries. We have achieved combined global revenues of US$3.8 billion from our member firms for the year ended 30 September 2011.

Grant Thornton New Zealand operates from three locations in Auckland, Wellington and Christchurch with 33 partners and over 250 professional and support staff.

Our infrastructure, expertise and methodology are world class, traits which benefit our local clients. However despite global clout, Grant Thornton New Zealand has not lost sight of its roots and key differentiators – partner/director accessibility and a friendly, personal approach. We work with our clients over the long term to help them to achieve their ambitions and grow their business.

Dedicated business risk team

Grant Thornton New Zealand has a dedicated business risk team working to help organisations like yours get the most out of their risk management strategies. We know the issues you face and we understand your needs. We offer an array of financial, business management and operational services designed to assist you:

Risk management

- Risk management implementation
- Risk management effectiveness
- Project risk management
- Strategic risk assessment
- Specialist risk reviews
- Risk analysis
- Project risk assessments

Internal audit

- Outsourced/co-sourced internal audit
- Internal audit peer reviews
- Control self assessment
- Probity reviews

Internal control effectiveness reviews

- IT audit, advice and process improvement
- IT internal audit
- IT Function effectiveness
- Data management and analysis
- Independent verification and third party reporting
- IT strategy
- DR/BCP - review, advice and facilitation of business continuity and disaster recovery plans.

Why Grant Thornton?

As a member firm of Grant Thornton International, we are able to combine the knowledge and experience of our local marketplace with the technologies, methodologies and specialist resources of a global professional services organisation. We deliver:

- personal attention from all our partners and managers
- services tailored to meet your needs
- business advice resulting in measurable benefits
- technical competency and attention to detail
- realistic goals with solutions that can be implemented
- timely information including alerts, regulatory updates and surveys
- realistic fees
- client satisfaction measurement.

Auckland
L4, Grant Thornton House
152 Fanshawe Street
Auckland 1140
T +64 (0)9 308 2570
F +64 (0)9 309 4892
E info.auckland@nz.gt.com

Doug Blakebrough
M +64 (0)21 243 0563
E doug.blakebrough@nz.gt.com

Wellington
L13, AXA Centre
80 The Terrace
Wellington 6143
T +64 (0)4 474 8500
F +64 (0)4 474 8509
E info.wellington@nz.gt.com

Murray Chandler
M +64 (0)274 899 352
E murray.chandler@nz.gt.com

Hamish Bowen
M +64 (0)274 489 9997
E hamish.bowen@nz.gt.com

Christchurch
L1, The Antarctic Attraction
38 Orchard Road
Christchurch Airport 8053
T +64 (0)3 379 9580
F +64 (0)3 366 3720
E info.christchurch@nz.gt.com

Grant Thornton

www.grantthornton.co.nz