RISK NZ

RiskPost

Issue 15 No. 3 September 2015

Contents

Editorial	Page 3
Chairman’s Corner	Page 4
Why not try your hand at Standards-writing?	Page 5
In-house vs. outsourcing cyber-security: the pros and cons.	Page 6
Self-Insurance 101	Page 10
Cyber security update from the Australian Government	Page 13
Standard and handbooks update	Page 15
RiskNZ news and information	Page 18

RiskNZ gratefully acknowledges
the support of our premier sponsor

JLT

DISCLAIMER

RiskPost is the newsletter of RiskNZ Incorporated. RiskPost welcomes contributions from members of RiskNZ. Any such contributions do not necessarily represent the views of RiskNZ as a whole, although from time to time RiskPost will publish items setting out the views of RiskNZ on a particular topic.

This page is intentionally left blank

Editorial

Miles Crawford

Editor, RiskPost

editor@risknz.org.nz

When this September edition of RiskPost is published, it will most probably not be September anymore, and I will not have upheld my responsibility to ensure RiskPost is published every 2 months. This has happened despite my best efforts and experience in pulling people and information together to make a RiskPost newsletter.

This situation reminds me that unexpected events occur, no matter what amount of thought goes into understanding them or how refined the management may be. And these events occur all the time: just over the last two weeks NZ had a cancelled tsunami warning, Japan beat the Springboks in the Rugby World Cup, and the RiskNZ Development Day changed from a multi-venue seminar to being held only in Wellington.

While unexpected events occur, they don't have to be perceived negatively. As risk practitioners, we understand that it is all about context – by understanding the risk environment, and knowing our capacity for taking and accepting risk – an unexpected event needn't be a setback, but an opportunity for success.

It's what we do about it that matters. In the case of NZ's cancelled tsunami warning, the Ministry of Civil Defence used the opportunity to spread the message that we should not rely only on sirens to keep us safe from tsunamis. In the case of the Springboks, they used the opportunity to rethink how they made on-field decisions and then went on to beat Manu Samoa by 40 points. In the case of RiskNZ Development Day being held only in Wellington, its centralisation means that members have the opportunity to meet with all the speakers on the day, as well as setting a solid foundation for Development Days to grow from in the future.

And what are the opportunities arising from an unexpectedly delayed RiskPost? An editorial topic for starters, but also a stronger working relationship with RiskPost contributors and the RiskNZ Management Board, as well as a sense of confidence in knowing that the show (RiskPost) can go on… regardless.

C'est la vie.

Chairman's Corner

Geraint Bermingham

Chairman, RiskNZ
Improving the knowledge and practice of risk management in New Zealand
chair@risknz.org.nz

"The Times They Are A-Changin'"

Back in the distant past - well 6 months ago, I wrote in the Chair's Piece about the pace of change across the world and suggested the best thing to do with that 2014 risk register was to throw it in the bin and start again! What with the rise of ISIL - or is that ISIS? - and a 50% drop in oil prices among other events, the context has changed so much that the previous risk register should be viewed as history.

Here we are just six months later and all that talk of a 'rock star economy' of just a couple of months ago seems oddly misplaced in light of the debate about the potential for a recession. That new 2015 risk register? I'm not suggesting it is time to throw that one out, but certainly any 6 monthly review or similar should be far more than a chat with each department head followed by a tweak of the previous risk report's text … searching questions need to be asked, alternative futures explored, the unexpected considered. Above all, real debate needs to be prompted. The process must be relevant and meaningful and most importantly, valuable for your organisation.

Have you registered for the Development Day?

This is of a new format RiskNZ event - one that promises to be relevant, current and of great value.

- Relevant as the speakers are active at a national level and so attendees will hear where things are at;
- Current as, unlike the usual large scale conference, this less formal one-day format allows for speakers to speak to the moment; and
- Valuable as, for a fraction of the cost of a full conference or commercial training event - and only one day out of office, you get to network with peers and hear expert speakers covering a range of useful subjects.

The organising team have got some great speakers lined up - and registrations are ramping up - and, in light of requests, there is now a discount for groups. Register here to ensure you are part of it!

And don't forget this is also a chance to network and to share the moment with the recipients of the 2015 Risk Awards!

Whilst on the subject of awards, I can't help but wonder if we should invent an award for the dumbest failure to consider risk. And the winner for 2015 is …..VW!

Why not try your hand at Standards-writing?

Roger Estall

All who have read Roger Estall's reports in RiskPost over several years on standards making at national, Trans-Tasman and International level will understand why he would like to encourage other experienced risk management practitioners to also get involved in what he jokes is 'the black art' of standards-making.

Roger says that standards-making is intellectually stimulating and provides an ongoing learning experience. He has previously described the relevant expertise as follows:

- Subject matter expertise
- Experience of operating in committees – especially where the line of debate can change very rapidly and advocacy of even good ideas (although in English are not necessarily the Queen's or President's English) means creative listening and careful expression are very important.
- Willingness to learn and, on ISO committees, master the rules (known as the ISO Directives) under which committees operate (or are meant to)
- Writing and drafting skills
- Advocacy
- Ability to travel
Note: RiskNZ funds travel to Trans-Tasman meeting subject to an annual limit but SNZ is not in a position to fund travel to ISO meetings,

If you are interested, please contact Roger at: roger_estall@yahoo.com.au

In-house vs. outsourcing cyber-security: the pros and cons.

Tom Walton,

Sales and Marketing Director for Network Box Australasia

Tom is a passionate communicator and cyber-security specialist on a mission to assist New Zealand businesses better understand and manage their cyber risk. Currently, Tom is the Sales and Marketing Director for Network Box, a Managed Security Services Provider who protect New Zealand and Australian business from both inbound internet based threats and outbound data leakage, loss or theft. Having recently presented to the New Zealand Risk Society on cyber governance best practice, Tom has been asked to further the discussion regarding an organisation's next steps to reduce their cyber-security business risk.

Introduction

Cyber-security is a complex and challenging subject and presents a substantial business risk to organisations today. Effective cyber-security management requires comprehensive monitoring of systems and networks and the right processes and procedures to protect and defend against cyber-attack.

Unless you are an IT security company, your organisation may not possess the expertise, time and resources required to effectively manage cyber-risk. It's a rapidly changing specialist area, and why would you want to spend all your time managing cyber-security risk when you have a business to run?

The key question to consider is: what risks are you better able to manage by outsourcing your cyber-security to a Managed Security Services Provider (MSSP)?

Prior to engaging a MSSP, a thorough assessment of your organisation is required to establish:

- the critical network functions that require protection;
- the damage to the organisation if these critical functions were to fail or be unavailable;
- the level of service required and if this includes support outside of standard business hours; and
- any specific technical or network requirements that must be addressed.

Evaluation of a MSSP's within the following categories will identify the risks involved and an organisation's ability to successfully manage them.

Outsourcing cyber-security: the pros

Direct costs

The security hardware and software required to combat today's cyber-threats are costly and require considerable up-front financial investment. With stretched budgets and return on investment top of most Financial Officers' minds, outsourcing security can have significant financial benefits over a comparative in-house solution.

When engaging with a MSSP, the cost of the service is explicit and agreed upon upfront. This reduces budgeting and profit and loss risks through standardised annual billing.

Two financing options typically present themselves. Purchasing specialist hardware from the MSSP allows an organisation to finance the project as a capital expense. The MSSP is contracted to monitor and manage network systems for an agreed length of time and the organisation retains ownership of the hardware.

Alternatively, leasing the hardware from the MSSP provides the ability to finance as an operational expense. The hardware remains the property of the MSSP and is leased to the organisation for the duration of the contract. Both options must be given consideration and it ultimately comes down to which financing option works best for the organisation.

In-direct costs

With a MSSP there are no additional or in-direct costs to the service.

A similar level of monitoring and protection delivered in-house requires the employment of a dedicated IT security team. In addition to staff and ongoing training costs, in-direct costs incurred through the operation and maintenance of an in-house solution include office space, power, network connectivity, and rack space.

Predictable service

With most MSSPs, the client enters into a Service Level Agreement for a set duration of time. This agreement details issue response times, prioritisation levels, hours of support, and service uptime.

As the service is managed via a formal contractual agreement it provides clarity as to the level of service expected of and delivered by the MSSP. This provides a mechanism to ensure effective management and accountability of an organisation's cyber-security and lessens the risk of not receiving an expected level of service.

Facilities

Security Operations Centres (SOC's) are specialist, purpose built and security hardened facilities housing state of the art security infrastructure. MSSPs invest heavily in these facilities and it is unlikely that an in-house IT security team will have access to the same level of technology and support.

Staff and expertise

The specialist training MSSP security personnel regularly receive increases their competency in delivering effective cyber-security protection. This is comparative to the risk involved in relying on the more generalist skills of an in-house IT team, to whom cyber-security may not be the top priority.

When a close working relationship is established, the MSSP security staff become an extension of an organisation's in-house IT team, complementing and strengthening the IT function of the organisation. By outsourcing cyber-security, internal IT resources can be utilised on more critical business initiatives.

The experience and expertise gained through addressing many different cyber-security incidents every day across many devices and a variety of clients ensures MSSPs are able to deal with incidents in a timely manner. A MSSP's access to threat intelligence and additional resources, often unavailable to individual organisations, aids the diagnosis and resolution of client issues.

Security updates

MSSPs work very closely with the manufacturers of the security technology with some even developing their own specialist technologies. Many MSSPs have their own security research functions where they are actively seeking out emerging threats and threat trends. This often provides advanced intelligence and security updates, which are passed on to clients.

Round the clock support and monitoring

A MSSP is able to provide 24x7 round-the-clock monitoring and protection of their clients' networks. The same level of protection from an in-house solution would require either dedicated staff for continuous monitoring or system down-time.

Compliance

As part of the service, many MSSPs are able to analyse and log security incidents. All logs are stored off-site in a forensically-sound manner and in compliance with regulatory requirements, removing the need for an organisation to do this.

Outsourcing cyber-security: the cons

The following points highlight potential risk areas that an organisation must be aware of when engaging a MSSP to manage their cyber-security. Careful evaluation of a MSSP is required to ensure their services meet your policy requirements and the risks involved are understood and manageable.

Relinquishing control

An organisation must understand that in employing a MSSP they relinquish control of at least some of their security infrastructure to a third party. The organisation becomes reliant on the MSSP to ensure the security of the information and their network(s).

Although this takes responsibility away from an in-house IT team, it can be beneficial in freeing up in-house IT capabilities. This risk can be successfully managed by ensuring a high level of trust and a good working relationship is established between the MSSP and the in-house IT team.

Data sovereignty

Outsourcing to a MSSP requires all information travelling through an organisation's network to either go off-site or go through the MSSP's appliance in order to be checked and filtered. This raises important questions as to who has sovereignty over the data, in other words, where the data is stored and who is able to see it.

There is the potential that an organisation's data will pass outside their immediate IT infrastructure. As part of the evaluation of a MSSP, and in order to effectively manage this risk, an organisation must clearly understand where their data is stored and monitored from.

Scalability

The resources of a MSSP are shared over all their clients. This poses the risk that they may be unable to provide adequate cyber-protection as your organisation grows. Evaluating the MSSP to confirm it has the ability to scale their solution to meet the needs of your organisation will aid in successfully managing this risk.

Response times

Most MSSPs have very fast response times when it comes to critical security incidents, for example if the system were to go down. Response times for a policy change, however, will depend on the lead-time agreed in your Service Level Agreement and are unlikely to be instant. It is therefore necessary to plan ahead on projects requiring security policy changes or updates.

Administrative access

The MSSP's engineers and security analysts have administrative access to your organisation's systems. It is essential an organisation works with the MSSP to establish exactly whom within the organisation is authorised to request administrative or policy changes from the MSSP.

In conclusion

Although the financial cost savings of outsourcing cyber-security monitoring are apparent, particularly if you are a smaller organisation, there are risks that must be managed when investing in cyber-security.

When considering cyber-security management, either outsourcing or addressing it in-house, an organisation must evaluate their ability to manage the risks involved. If you choose to outsource to a MSSP, an understanding of your organisation's needs and cross referencing these against the MSSP's policies and services will help ensure an effective working relationship. At the end of the day, the MSSP is providing you a service and you must be confident the cyber-security concerns of your organisation are adequately met. The question every organisation must ask themselves is: what will provide the best management of my organisation's cyber-security risk?

Self-Insurance 101

John Sloan

Sloan Risk Management Services

John Sloan, the principal of Sloan Risk Management Services, has been a member of Risk NZ from its inception.

> **Unless a properly structured internal reserve fund is established 'self-insurance' really means 'non-insurance'**.

In a risk management context, self-insurance is in 'no-man's-land' because:

- It is not risk transfer.
- It is not insurance as such.
- It is internally absorbed.

Insurance is basically where a risk is contractually transferred to an insurer and a premium is paid to reflect that transfer. 'True' self-insurance is where an internal fund is established which consists of the organisation's own contributions either in bulk or made periodically similar to annual insurance premiums.

For any business / industry / commercial enterprise / governmental entity / local authority or major not-for-profits, self-insurance is primarily applied to:

- Totally uninsured risks whether major or minor.
- Claims deductibles (often termed 'excesses') applied by insurers.

Self-insurance is a term normally applied to insurable risks such as fire / business interruption / liability / motor, and not to uninsurable business risks such as reputation, investments or demographic changes. At a higher level self-insurance also enters into risk appetite and retention equations which are invariably applied to all risks whether insurable or not.

This commentary is deliberately restricted to insurable risks.

Total Self-insurance of Insurable Risks

This is where the risks are identified, measured in advance and decisions are made as to whether:

- The risk is too remote to consider insuring.
- Future losses are predicted to be extremely nominal.
- Insurance is not cost effective and is just 'dollar-swapping'.
- The premium submitted by insurers is prohibitive.

Consequently a decision is required to decide:

- Are future losses paid out of current funds?
- Is a ring-fenced self-insurance reserve fund created to accumulate and pay losses?
- Is the risk to be contractually transferred to another party such as a supplier or contractor?
- If a major loss occurred in the future, could funds be borrowed from a bank or other source to fund the loss?

- Could a substantial claims deductible be accepted, self-funded, but commercial insurance arranged for catastrophic losses?

The Main Dangers of Self-Insurance

- **Setting up a self-insurance reserve fund means that it needs to be ring-fenced to avoid being raided for other purposes or even suspended.**
- **The classic danger in self-insurance funds is that in the early stages they are relatively low and could not sustain a catastrophic loss which could wipe out the fund before it builds up a critical mass.**
- **For total self-insurance the risk may not have been annually reviewed and has expanded far beyond the original analysis.**

Claims Deductibles

The simplest example is domestic: for your contents insurance claim you pay the first, say, $250.

The same principle applies to all claims deductibles which recognise:

- Small claims are eliminated which reduce the insurer's liability for pay-outs and their own internal administration costs.
- Deductibles reinforce the need to mitigate losses by the clients.
- Clients can allocate any claims deductibles to business units to reinforce the need to control losses.
- In some cases the deductibles are imposed by all insurance companies with earthquake claim deductibles being the classic example.

If a premium rate is already fine there can be no fat left to cut to provide a discount for a higher deductible which means that the increased deductible is not cost effective.

Do your sums

For claims deductibles for business insurances there is inevitably a break-even point where the discount offered is not worth accepting. The insurers need to have sufficient premium to cover their own catastrophic exposure and often discounts are not attractive for higher deductibles. It is essential for any business to review their past insurance claims and project them forward to estimate what they would have to pay in the future if the higher claims deductible was applied. They should also factor in inflation if they are looking at previous claims paid.

It is also essential for businesses to take claims deductibles into account in their budgets.

Capping Deductibles

Following the Canterbury earthquakes some businesses found that they had to absorb 3 separate deductibles for each of the earthquakes, particularly where the same building was damaged.

With some earthquake claims deductibles being, say, 5% of the total sum insured on a property and any business interruption, the total amount can be substantial. However, it is possible that, in some cases, insurers may agree to put an upper limit on the deductible to reduce the potential exposure for a major earthquake.

Another technique is to have an agreement that the company will only accept, say, 2 or 3 deductibles during an insurance year when the amount is then reduced to a much lower figure to prevent an unexpected run of major deductibles during one year.

Self-Insurance on a Grand Scale

The hundreds of unresolved earthquake claims in Canterbury involving hundreds of millions of dollars are self-insured until settled. Whether a claim is for thousands or millions of dollars, the same hard-nosed questions arise especially: "why? Who arranged the insurance? Did we have the full information on actual insurance coverage, sums insured, valuations, deductibles, policy limits and exclusions? Who is at fault? Are the insurers justified in their response? Who can we sue? And, who is going to finally pay?"

Cyber security update from the Australian Government

Sue Trezise,

Sue-lutions Ltd.

Sue Trezise is an independent risk advisor providing specialist assistance to government, businesses and community organisations. Her cross-sector experience and pragmatic approach help boards, CEOs and managers embed risk thinking to improve strategic decision making and business performance. An experienced facilitator, Sue assists communication between technical experts and non-technical stakeholders and makes managing risk practical and effective.

The Australian Cyber Security Centre (ACSC) has published its 2015 Cyber Threat report. The following notes attempt to summarise the content as a follow-up to the RiskNZ Cyber Security lunchtime seminar. While the report focuses on the Australian environment, our proximity and the globalised nature of internet connectedness means the information is equally pertinent for us.

The report identifies a range of cyber adversaries (individuals or organisations that conduct cyber espionage, crime or attack) operating for different purposes:

- Foreign state-sponsored adversaries seeking economic, foreign policy, defence or security information for strategic advantage
- Criminals who exploit or access systems for financial gain
- Hacktivits causing disruption (denial of service, web defacement) and vandalism (electronic graffiti)

Significant system compromises cause economic harm, damage reputations and undermine international and domestic confidence in network security. Cyber adversaries target both industry and government networks to acquire desired information. This may be by direct attack or through a secondary target of connected networks that are easier to compromise.

Cybercrime refers to criminal acts involving use of computers or other ICT or targeting computers or other ICT. Examples include unauthorised access to, modification or impairment of data, online fraud and identity theft.

The impacts of cybercrime include:

- Financial losses from fraud
- Cost of immediate response
- System remediation costs
- Damage to personal identity and reputation
- Loss of business or employment opportunities
- Emotional and psychological harm to individuals

Common techniques to gain unauthorised access to a computer include:

- Spear phishing - using a carefully crafted email to entice a user to click on a link or open an attachment. Such emails may incorporate misappropriated business names and counterfeiting of legitimate brands which brings harm to the affected companies (and associated costs to remedy) at the same time

- Remote Access Tools (RAT) - allow someone to access a computer from a remote location
- Watering-hole - a compromised legitimate website frequented by the intended target
  In many cases the owner of the compromised website may not be aware until the site is blacklisted by a security organisation. A blacklisted website can experience a significant drop in traffic and therefore revenue

Other forms cyber intrusions include:

- Ransomware - encrypts files so they cannot be accessed until a ransom has been paid
- Malware such as ZeroAccess - causes infected computers to generate 'clicks' on advertising to receive commissions from the advertising companies
- Denial of Service - preventing legitimate access to online services (typically a website) by consuming the amount of available bandwidth or processing capacity of the computer hosting the online service

Strategies to Mitigate Targeted Cyber Intrusions is a key publication by The Australian Signals Directorate (ASD). The list of strategies is informed by ASD's experience in operational cyber security. The covering information notes that while no single strategy can prevent malicious activity, at least 85% of cyber intrusions responded to by the ASD would have been mitigated by implementing the Top 4 mitigation strategies as a package.

The Top 4 mitigation strategies are:

1. **Application whitelisting** of permitted/trusted programmes, to prevent execution of malicious or unapproved programmes including .DLL files, scripts and installers.
2. **Patch applications**** e.g. Java, PDF viewer, Flash, webs browsers and Microsoft Office.
3. **Patch operating system vulnerabilities****
4. **Restrict administrative privileges** to operating systems and applications based on user duties. Such users should use a separate unprivileged account for email and web browsing

**Patch/mitigate systems with "extreme risk" vulnerabilities within two days. Use the latest version of applications/operating systems.

References:

ACSC *2015 Threat Report* https://acsc.gov.au/publications/ACSC_Threat_Report_2015.pdf

ASD *Strategies to Mitigate Targeted Cyber Intrusion* http://asd.gov.au/infosec/mitigationstrategies.htm

Standard and handbooks update

Roger Estall

Roger was the first Chairman of the Society and represents it on the trans-Tasman joint standards committee for risk management known as OB-007. He also represents New Zealand on ISO Technical Committee TC 262 which is responsible for ISO risk management standards. He was one of the authors of ISO 31000 and has been a principal author of many related SNZ/SA standards and handbooks

Revision of ISO 31000:2009

In my last report, I outlined the change in direction by the relevant ISO Technical Committee (TC 262) for the revision of ISO 31000:2009. The revision plan has shifted from development of a 'Limited Revision' with no technical changes, to carrying out a full, or unlimited, revision.

After a hiccup in the administrative arrangements, a draft of the Draft Statement (DS) was eventually issued by TC 262 to all member National Standards Bodies for comment. Although the DS itself is quite tightly worded it also includes a detailed 'Explanatory Note' to assist in understanding its rationale – including why it isn't intended to become a 'management system standard'.

It was decided that both the purpose statement (reproduced below) and the DS would be expressed in plain language without the use of defined expressions – such as 'risk'. This was thought necessary because many of the defined expressions also have other meanings – for example, there are apparently 40 different meanings for the word 'risk' in ISO Standards alone. There are also statutory definitions (in a variety of jurisdictions), common law meanings and everyday meanings.

Purpose statement for ISO 31000:20XX

This International Standard updates the advice in ISO 31000:2009 (which concerns 'risk management') in order to better assist organizations to achieve their ultimate purposes. It does this by-

i) *providing universally applicable guidance for recognizing and responding to uncertainty relevant to those ultimate purposes –*
   - *as a part of decision making wherever it occurs within the organization (irrespective of the type of activity), and*
   - *if changes inside or outside the organization create new uncertainties about earlier decisions*

ii) *assisting organizations to adopt a "risk based approach" where required by a management systems standard or other documents using this expression*

iii) *enabling the guidance in this International Standard to be used in other standards concerned with more specific areas of decision making involving uncertainty*

.

One of the issues that the Task Group identified as hindering the application of the existing standard is that 'risk management' is substantially presented as a theoretical construct which end users are then encouraged to 'integrate' into what they do. In other words, it is presented as a (very desirable) 'bolt on' or 'add in'. At the same time, somewhat confusingly but quite correctly, the existing standard says that all organisations already manage risk – at least with some degree of success.

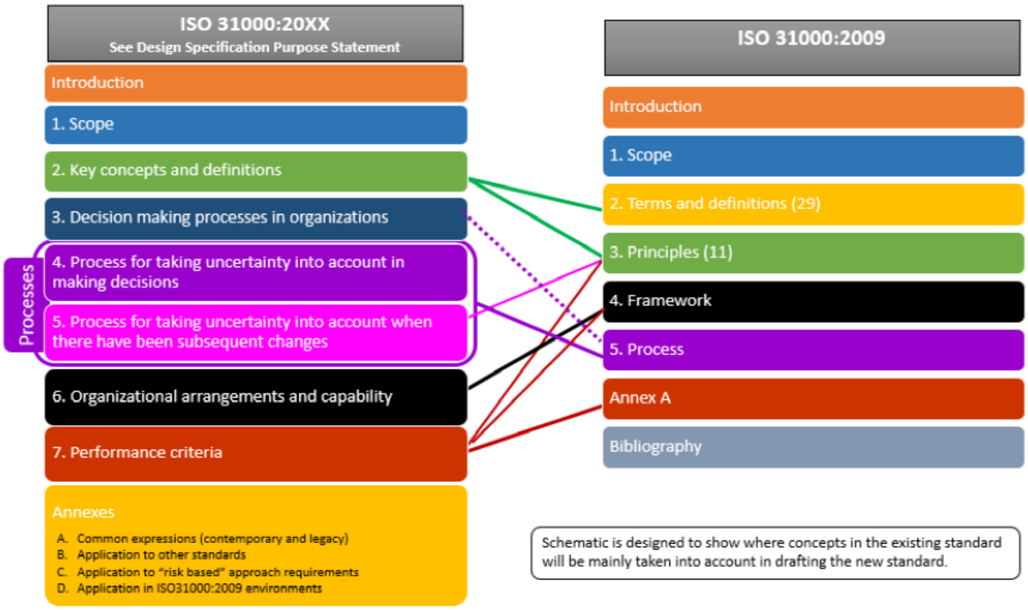
The DS acknowledges that the way organisations of every type pursue their objectives is by making decisions. It recognises that decision-making inevitably involves taking account of uncertainties – something that can be challenging to do well, and yet can strongly affect the outcome of decisions.

So while the DS does not anticipate that 31000:20XX will be a standard about decision-making per se, the guidance it provides will be constructed around the various decision-making processes that are actually used in organisations.

The DS therefore specifies a somewhat different structure to that of the existing standard as is illustrated in the following graphic, which also, in approximate terms, maps the sections of the new standard across to the sections of the existing.

Again, this structure is not as revolutionary as might seem. For example, the value of including a section that explains the concepts that underpin the standard has already been accepted in the ISO Technical Report (TR 31004) and in our own HB 436:2013 – both of which have the purpose of explaining the existing standard.

General relationship between sections of 31000:20XX and existing standard


ISO 31000:20XX
See Design Specification Purpose Statement
Introduction
1. Scope
2. Key concepts and definitions
3. Decision making processes in organizations
Processes
4. Process for taking uncertainty into account in making decisions
5. Process for taking uncertainty into account when there have been subsequent changes
6. Organizational arrangements and capability
7. Performance criteria
Annexes
A. Common expressions (contemporary and legacy)
B. Application to other standards
C. Application to "risk based" approach requirements
D. Application in ISO31000:2009 environments
ISO 31000:2009
Introduction
1. Scope
2. Terms and definitions (29)
3. Principles (11)
4. Framework
5. Process
Annex A
Bibliography

Schematic is designed to show where concepts in the existing standard will be mainly taken into account in drafting the new standard.

To summarise, the focus and rationale of the DS is really on making the ideas and content of the existing standard more directly relevant to the existing operating practices of every organisation rather than appearing to advocate the adoption of entirely new practices or an artificial construct.

It will also be written in more simple language (for example it won't use the word 'context' in four different ways). The new standard may well end up with some defined words, but the DS requires these to be selected once there has been a plain language draft so that the discussion about content is not confused with the selection or meaning of labels that are attached to particular ideas or – even worse – imagining that knowledge is to be found in the jargon.

In calling for universality of application to all types of organisation and all types of decisions, the DS is creating 'big shoes' to be filled by the drafters. To assist in this regard, the DS incorporates a set of 'representative decisions' for the drafters to use as a test bed against which to test what they write. The representative decisions cover a range of organisation types, a range of decision-makers and a range of decision-types. (The drafters can add additional examples but cannot remove any examples.)

RiskNZ news and information

Management Committee and Officers

The management committee and officers of RiskNZ are:

Chair: Geraint Bermingham **Secretary:** Ross Wells

Executive Officer: Tim Jago **Treasurer:** Tony Yuile

Administration Officer: Rachel Allan

Committee members: Nigel Toms, Brian Potter, Loata Stewart, Hilary Walton, Sally Pulley, Sue-Anne Lee, Sharyn Bramwell

RiskNZ's Website

RiskNZ's website is located at www.risknz.org.nz.

As part of this year's business plan initiatives, our website has been upgraded. Although we have made every endeavour to ensure all aspects of the website are functioning as they should, if you do notice any broken links or other gremlins, please notify the Administration Officer at adminofficer@risknz.org.nz.

The website is your RiskNZ's shop window, and a major risk management information resource, so please take the opportunity to browse the new site. We welcome your feedback on it.

As a financial member of RiskNZ you are entitled to access the members-only section of the website. For this you need a user name and a password. If for any reason you do not have the password or have forgotten it, please contact the Administration Officer.

New Members

RiskNZ welcomes the following new Members. Contact details are included in the Members' section of the Website.

Individual Members

Pete Branch, Head of Health Safety Environment, Griffins Foods Ltd

Ross Wells, Risk and Assurance Advisor, The Treasury (shifting from Corporate membership)

Balajee Narasimhan, Risk and Compliance Advisor, Te Tumu Paeroa (Maori Trustee)

Philippa Clarke, Risk Manager, healthAlliance

Mark Taulelei, Operational Risk Partner, Kiwibank

Matthew Appleby, Principal Risk Analyst, The Treasury

Neil Beattie, Manager Risk and Assurance, Ministry of Education

Ken Gibb, Associate Director Operational Advisory, Grant Thornton New Zealand Ltd

Aaron Queree, Business Performance Manager, Wellington International Airport Ltd

Debra Branch, National L&OD Manager, Restaurant Brands Ltd

Become a Member

Membership of RiskNZ is open to any person of good character or an organisation engaged in or with an interest in the practice, study, teaching or application of risk management. RiskNZ is keen to attract a wide range of Individual and Corporate members representing all the different aspects of risk management knowledge and practice. This includes those with direct involvement in the field and those with a personal or community interest.

Apply online at http://www.risknz.org.nz/membership/how-to-join/

Social networking – Follow us on	Linked in	https://nz.linkedin.com/groups/RiskNZ-3945531/about
	Find us on Facebook	http://www.facebook.com/pages/The-New-Zealand-Society-for-Risk-Management/178021535579772
	twitter	http://twitter.com/nzrisksociety

Information for Contributors

Next Issue	The next edition will be published in November 2015. RiskNZ strongly encourages all members to contribute items for this newsletter on practices, developments or issues in your particular area of risk management. Contributions for the next issue should be sent to editor@risknz.org.nz and received by 31 October 2015. Members are welcome to submit material for the following sections:
Articles	Articles are welcome at any time; please contact editor@risknz.org.nz if you wish to propose an article.
Developments in risk management and new information sources	Significant new web page content including online articles and major reports available on the web. New publications (including brief descriptions, and where possible website links to further information). This will include new journals in risk management, new books, where they are available, etc.
Activities, services and situations vacant	*RiskPost* provides a membership service for the display of notices and advertisements, if aligned with RiskNZ's objectives. Notices may describe an activity or service, or advertise a risk management vacancy. Notices must not exceed 150 words of plain text, inclusive of all contact and reference details. Pricing and application form for both *RiskPost* and on-line advertising services, are available from: http://www.risksociety.org.nz/advertising

For further details on RiskNZ's submissions and advertising, please contact the Administration Officer: adminofficer@risknz.org.nz,

RiskNZ
PO Box 5890,

Wellington 6145

Links

This section in RiskPost provides our members with useful links to websites and LinkedIn discussion sites. These links hold a lot of information that our members should find useful to enhance their knowledge in Risk Management and related areas. We welcome comment from our members on the usefulness of these links and suggestions for others sites they found useful. Please send feedback or links to editor@risknz.org.nz

Consumer Affairs – Product Safety
http://www.consumeraffairs.govt.nz/for-business/compliance/product-safety

ISO 10377:2013 Consumer Product Safety — Guidelines for suppliers and ISO 10393:2013 Consumer product recall – Guidelines for suppliers.
http://www.iso.org/iso/home/news_index/news_archive/news.htm?refid=Ref1726

Internet sites:

http://globalriskcommunity.com/

http://www.valuebasedmanagement.net/

http://www.knowledgeleader.com/

http://poole.ncsu.edu/erm/

Groups within LinkedIn:

ComplianceX
http://www.linkedin.com/groups?gid=865117

Conference Board of Canada ERM
http://www.linkedin.com/groups?gid=2561072

Enterprise Risk Management
http://www.linkedin.com/groups/Enterprise-Risk-Management-82279?trk=myg_ugrp_ovr

Enterprise Risk Management Association
http://www.linkedin.com/groups?gid=89308&trk=myg_ugrp_ovr

Governance Risk & Compliance
http://www.linkedin.com/groups?gid=95089&trk=myg_ugrp_ovr

ISO 31000 – Risk Management
http://www.linkedin.com/groups/ISO-31000-Risk-Management-1958423?trk=myg_ugrp_ovr

ISO 31000 Risk Management Standard
http://www.linkedin.com/groups/ISO-31000-Risk-Management-Standard-1834592?trk=myg_ugrp_ovr

Research & Benchmarking Risk Appetite Practices
http://www.linkedin.com/groups/Research-Benchmarking-Risk-Appetite-Practices-2401677?trk=myg_ugrp_ovr

Risk Managers

http://www.linkedin.com/groups/Risk-Managers-65207?trk=myg_ugrp_ovr