RESERVE BANK OF NEW ZEALAND
TE PŪTEA MATUA

Innovation and Risk Management: Insights from Executive Management at Statistics New Zealand and the Reserve Bank of New Zealand

An address delivered to the New Zealand Institute of Chartered Accountants in Wellington

On 24 June 2014

By Geoff Bascand, Deputy Governor and Head of Operations and Steve Gordon, Head of Risk Assessment and Assurance

2 The Terrace, PO Box 2498, Wellington 6140, New Zealand
Telephone 64 4 472 2029 Online at www.rbnz.govt.nz

"A ship in harbor is safe, but that is not what ships are built for" (John A. Shedd, Salt from My Attic (1928)).

Introduction and rationale for risk management

Effective risk management provides an environment for calculated risk taking and innovation. Good risk management contributes to institutional success. To be effective it requires strong leadership and organisation-wide ownership. Talking about risks and communicating plans to mitigate them is a leadership responsibility and an important part of a successful risk management framework. In this address, we will share our insights and experiences from Statistics New Zealand and the Reserve Bank of New Zealand to facilitate discussion about effective approaches to risk management while enabling innovation and institutional progress.

In 2003-2005, Statistics New Zealand set about modernising the collection of Household Labour Force Survey (HLFS) interview data through computer assisted (face-to-face and telephone) interviewing. It was not a success.

A review of the project by John Smyrk in 2005 stated[1]:

- "threats to the project were not identified";
- programs of pre-emptive and contingency actions were not assembled;
- "things kept going wrong" for which there was no allowance in the plan.

As a result, statistical outputs were hard to interpret and the statistical series and the organisation suffered reputational damage. Operating costs rose rather than declined as expected.

They say one learns better from mistakes than victories. As the euphemism goes: there were lots of learnings about risk (and project) management from the project!

---

[1] J. Smyrk, "Enhancing business projects in Statistics New Zealand:
learning from the HLFS-CAI initiative, A Report on a Review of HLFS-CAI", September 2005.

The HLFS estimates employment and unemployment and is one of Statistics New Zealand's highest priority economic data series. It is a costly collection, both in financial terms and in the burden imposed upon survey participants. Like other household surveys, it had been collected in the same manner for over 20 years. The incentives for change were considerable. A much expanded social survey programme was being introduced and there was a strong desire to modernise survey collection methods to reduce costs, speed processing, and introduce innovation. Rewards were in prospect but risks were not adequately anticipated or managed.

Innovation is critical to strong business performance as organisations seek to enhance product and service offerings, lift efficiency, upgrade technologies and increase their resilience and adaptability.

Without innovation, organisations wither and customers and business owners suffer. Becoming ideas constrained is fatal, but there are risks in innovating. As Machiavelli said centuries ago, "Never was anything great achieved without danger." Risk and reward are inextricably intertwined. Leaving the boat safe in its harbour will not yield progress.

Good risk management is imperative for managing successful change. It involves anticipating and diminishing threats; protecting sources of value; and enabling value-creating risks to be taken in a calculated way, with reduced likelihood of failure or loss[2]. Done well, it enables an organisation to seize opportunities to create and protect value for all its stakeholders.

Good risk management enables an organisation to move forward, because the downside risks of change are contained, and risk management provides a forward-looking orientation. It allows organisations to focus their competencies on value creating activity. Done well, it informs strategy, investment prioritisation and business decision-making. It drives organisational direction and positioning.

[2] Risks can be positive or negative. Almost exclusively in this paper, we focus on negative risks, reducing loss. Often there is an intent of managing possible eventualities to a more neutral position where upside and downside risks are 'balanced' and we shall address this approach. Positive risks are commonly treated as windfall gains. More sophisticated approaches are applied in some business circumstances, e.g. financial markets, which we largely ignore for the purposes of this general exposition.

A second key benefit is that it reduces the likelihood and costs of adverse events that may damage organisational reputation, financial or business viability, and distract the organisation from achieving its goals. Novopay, and ACC's privacy breaches, are familiar examples where the organisational and societal costs of risk management failures have been considerable.

Good risk management fosters both adaptability and resilience, two crucial aspects of enduring organisational performance.

Types of risk

Generally, three categories of risks are identified: strategic, operational and project risks.

1. ***Strategic risks*** describe the impact on the business of possible changes in the wider environment, such as political, international, demographic, social, etc., and the dangers of business strategies not being adequately aligned to their operating environment. They also entail risks to the accomplishment of key business goals through loss of focus, inappropriate investment or resourcing, and reputational and communication risks.

   Mitigations of strategic risks tend to be strategic choices and business model approaches; investment prioritisation decisions during planning processes, often resulting in project initiations; and communications and stakeholder management.

Strategic risks are often perennial, yet may be volatile due to changes in the external environment. For example, in the Reserve Bank's case, the risk of monetary policy settings not achieving the inflation goals and the ensuing reputational damage is ever-present, but these risks are accentuated by swings in exogenous factors such as commodity prices, fiscal policy, immigration, or exchange rate movements. Financial stability goals are similarly vulnerable. Threats to financial stability are always present but are usually quiescent until something goes wrong. The global financial crisis (GFC) was an extraordinary escalation of a tail-risk, yet smaller threats may occur intermittently, each of them posing a challenge to the Bank's reputation for managing a sound and dynamic financial system.

In Statistics New Zealand's case, an enduring strategic risk is the loss of confidence in the organisation by failing to deliver timely and accurate statistics. Errors in GDP or the CPI, or substantial unexplained volatility, as has occurred with the HLFS at various times, if persistent, can undermine confidence in the statistics themselves and the organisation more broadly. Consequently, a major component of risk management is the quality assurance framework and associated processes, along with strong project management adapted for 'business as usual' scheduling and delivery.

Other strategic risks may be more contemporary, and related to changes in the business's operating environment. In Statistics New Zealand's case, delivery of a major transformation programme (Statistics 2020 Te Kapehu Whetu) and realisation of the benefits from the investment is critical particularly in the window from financial injection (2011) to major systems and capability change (2017 say). Highly developed programme management and extensive external review processes seek to ensure that benefits are achieved and milestones accomplished.

For the Reserve Bank, the recent introduction of a new macro-prudential policy regime presented significant challenges for the organisation. The adoption of macro-prudential policy in New Zealand drew on international policy insights from the financial cycles that preceded and succeeded the GFC. Governments became more concerned about the financial stability risks associated with credit and asset price cycles and introduced new counter-cyclical 'macro-prudential' policy measures to lean against emerging risks.

A macro-prudential policy framework was agreed between the Reserve Bank and the Minister of Finance in May 2013. New policy frameworks present policy challenges in building understanding of their objectives and operation. Faced with accelerating house price inflation on top of already over-valued house prices, the Bank moved quickly to introduce new policy measures, including new capital requirements against high loan-to-value ratio (LVR) lending and limits on the share of new high LVR lending that banks could undertake.

The challenge confronting the Bank was the risk of not achieving its financial stability outcome goals if it failed to act (with potentially very severe consequences) vis-a-vis the risks to the

Bank's reputation and confidence in its policy-making. There were risks and uncertainties to manage in introducing an important policy innovation that was new for households and banks. A classic risk-reward trade-off – one that required significant evaluation and preparation by senior management.

Several steps were taken to ameliorate possible downside risks. We set the scene for these measures in a number of on-the-record speeches and in remarks at press conferences, and in Monetary Policy Statements and Official Cash Rate statements expressing our concerns with easier lending standards and house price inflation. We consulted with banks and published analyses of the potential impact of the measures, as well as comparisons with regimes in other countries. Following their introduction, we provided assessments of the impact, rationale and objectives in further speeches, media interviews, and in the November 2013 and May 2014 Financial Stability Reports.

The introduction of LVR restrictions has attracted commentary from different quarters. In some commentators' eyes, there has been a blurring of financial stability and monetary policy objectives, with some analytical debate about the merits of the policy. Others have questioned the Bank's operational policy design and its distributional impacts. Some have credited the Bank with policy innovation and the willingness to act before a crisis eventuates. To date, the impacts have been broadly in line with the Bank's expectations. House price inflation is moderating, along with the risks to financial stability (FSR, May 2014).

2. ***Operational risks*** relate to the achievement of business plans and 'business as usual' results. They entail risks of failure to business operating systems, quality or service failures, integrity and conduct risks, security, operator error, incident or business continuity threats, etc.

   Operational risks are managed and mitigated through measures such as process design, process controls, policies and discretion limits, back-up and redundancy measures, quality assurance processes and review/feedback cycles, alignment of skills and resources with requirements, and investment in research and development and capital equipment.

Mitigations operate on both likelihood and impact. For example, payroll authorities and process controls are often designed so as to minimise the possibility of error or fraud, and limit the financial impact if such an eventuality occurs. Many business continuity measures are focused on reducing impact (for example back-up procedures for disaster recovery, as they have no influence on event probability), whereas others, such as electing higher standards, may reduce vulnerabilities.

Among their enormous social and economic impacts, the Christchurch earthquakes were a tragic wake-up call in respect of disaster recovery/business continuity planning (BCP) for many organisations. Statistics New Zealand was hit very hard in business terms by the three major quakes. The February quake severely damaged the main Christchurch office building and the separate census building. The quake of February 22, 2011 occurred 14 days before census day. After 48 hours assessing whether we could continue the five-yearly population and dwelling census, or usefully run it excluding Christchurch, we decided it was infeasible and I recommended that the government cancel it. $72 million spent, 7500 people employed and then let go (and paid out). As a result of cancelling the census, a number of other national post-censal social surveys also needed to be abandoned, specifically the Maori Social survey and the Disability Survey.

Other economic and population statistical releases were delayed, and business was severely disrupted for subsequent weeks. In the week following the February quake, IT staff retrieved back-up tapes of data processed in January and February from the server room, which had been scheduled for transfer to Auckland. We operated tape back-up in Christchurch, after having rejected proposals for network (WAN-based) back-up from that site[3] due to cost and budget restrictions and an assessed lower-risk profile in Christchurch. The back-up data was important for timely release of GDP data on March 23.

Notwithstanding very extensive risk planning and control in the census programme, the organisation was unable to continue the census programme at that time. Some unforeseen risks eventuate. Their impact can sometimes be mitigated by management actions but sometimes organisations just have to trust their resilience.

[3] It was operating between Wellington and Auckland, but not between Christchurch and Auckland.

About four weeks after the February quake, Statistics New Zealand's IT Group introduced remote access computing for staff. Initially, access was enabled through webmail that provided limited access to non-secure corporate tools. Subsequently, fully access to secure internal databases and statistical software was introduced. When the severe after-shock struck in June, all 240 Christchurch staff had such a facility and 'normal' work resumed quickly.

Remote computing had been considered in Statistics New Zealand for many years but had been assigned as low priority due to security concerns and limited demand given our office-based working norms. When the imperative arose, it was a quick and successful initiative. Sometimes innovation flows from risks that have already materialised.

Reinforcing this point, when the census was re-run in March 2013, Statistics New Zealand sought to avail itself with the benefits of cloud computing, using Infrastructure as a Service for database management. The potential security and loss of control risks from third-party storage with cloud computing were a concern, but from a full systems-perspective, the marginal risks and costs were assessed to be lower than those entailed in Statistics NZ replicating the security environment and having to provide its own disaster recovery arrangements. Risk perceptions and the ability to manage them were definitely influenced by the experiences of 2011.

The Reserve Bank sets very high standards for business continuity, and has strengthened these further in recent years, reflecting the importance of the 24/7 hours availability of the payments system and the need to maintain domestic liquidity and foreign exchange dealing operations.

We have experienced several incidents that spurred further risk assessment and mitigation measures. On the evening of 24 April 2012, several banks experienced difficulties in processing retail payments (i.e. exchanging and settling payments between banks' retail customers such as merchants, government departments etc.). Some payments missed being included in the end-of-day processing and banks had to post them late, in some cases as late as the afternoon of the April 25. As a result, some bank customers who accessed their accounts on the morning of ANZAC day found that expected transactions had not been completed.

The issue was triggered by a technical problem with the international financial communications network (SWIFT) and affected participants in the new Settlement Before Interchange (SBI) arrangements that had recently been implemented. These allow banks and other parties to exchange files of payment instructions and send settlement instructions to the Reserve Bank's Exchange Settlement Account System (ESAS). ESAS operated normally, but because of the fault in the messaging system payments instructions were delayed or failed. The incident was the most significant disruption to the processing of retail payments for many years and the effects were felt by bank customers nationwide.

This incident was complex due to the multiplicity of parties involved, some unclear (at the time) responsibilities, and communication between parties proving problematic. New, untested contingency arrangements were used reluctantly by banks. In the end those arrangements proved crucial, allowing the SWIFT system to be by-passed, and payments to be completed through NZClear. Since that event, the industry has accepted greater accountability for the collective responsibility to address issues and communicate effectively between the parties. As a result, subsequent incidents have been resolved more effectively.

The Bank's own payments system disaster recovery operations have been strengthened in recent years. In February 2011, the Bank established an office in Auckland as a full back-up to its payments and financial markets operations. There is fail-over capability to Auckland should Wellington's operations be disrupted, and vice versa. Hardware, database and software back-ups exist for the most critical systems. The Bank's BCP programme is extensive and regularly tested.

The Reserve Bank, whilst perhaps better known for its monetary policy responsibilities, is a bank. It operates financial, lending and investment functions that are similar in a number of respects to those of commercial banks. And it holds and disburses cash, lots of it, albeit almost entirely to intermediaries rather than the public directly. Some $9 billion of payments flow through the interbank settlement and payments systems (ESAS/NZClear) each day. Security risks are a very serious matter for the Bank. Recently, we extensively upgraded the security arrangements around our cash processing and storage functions.

IT security is an ongoing challenge. IT security risks arise through malware (viruses etc); cyber attacks (hacking and denial of service attacks) targeting external-facing publicly available services or exploiting vulnerabilities in our infrastructure; loss of data through mobile devices; insider breaches of privileges or authorities; and staff introducing vulnerabilities through exploitable physical or social media.

The Bank has a dedicated security function and the IT security framework (that is currently being updated) provides an integrated, organisation-wide program for managing information security risks. Extensive control measures are in place, including technology-based mitigations and non-technical mitigations revolving around IT security policies, training, and incident management procedures.

Systematic external and internal security monitoring and testing arrangements are in place. They reveal extraordinary numbers of potential threats. Suspicious events triggering alerts number around 500 million per month.   These comprise a mix of non-standard but permissible events and adverse events. The security and network control task is to distinguish these and exclude the adverse anomalies, while enabling the acceptable abnormal.

Operational risks, be they security, business continuity or service delivery, are most effectively managed through a risk management approach that is integrated into the business and culture of the organisation. Total quality management (TQM) is well recognised as everyone's job, and the same is true of other operational risk management practices.

3. ***Project risks*** are sometimes treated as a subset of operational risks and are linked to the achievement of project outcomes. They relate to benefits not being achieved, perhaps because of delivery failure, key assumptions not being met, scope being poorly defined, delays in project completion, cost escalation, disruption from extraneous events etc.

   Typical risk controls for projects include: the establishment of a project risk register with risks identified, evaluated and controls determined, project planning, resourcing, and monitoring mechanisms, and governance arrangements.

Risks often eventuate during change processes because existing processes were not fully understood and the number of unknowns is allowed to be greater than it should through inadequate planning, trialling and risk management.

The Bank recently upgraded its treasury system (Findur) that captures financial trading activity, and produces financial performance reports among other functions. What was expected to be a relatively simple and quick upgrade process took around 11 months and incurred substantial frustration and cost – directly in terms of additional resources and indirectly through deferment of other scheduled developments. Risks unfolded that were not anticipated. With the benefit of hindsight, initial project planning, testing work and collaboration with the vendor were inadequate, and risk mitigations were not well enough established in advance. The project has now been completed with very satisfactory business outcomes, but better risk management and planning could have yielded better outcomes at lower cost.

It need not be like this. The (population and dwellings) census is arguably New Zealand's biggest project in any one year, involving over 7000 employees, every New Zealander, and a budget of approximately $100 million. Notwithstanding the cancellation in 2011 due to the Christchurch earthquake, the census – which is four years in the planning and involves six weeks of collection and analysis for around a year - has been conducted successfully, on schedule, within (or close to) budget, and achieved its objectives, for over 100 years.

The Bank is introducing new banknotes in 2015, as foreshadowed in the Statement of Intent. While it is early days in the development of the notes, extensive risk planning has been undertaken. The project has been broken into multiple phases, with an actively managed risk register updated regularly, and aligned with the phasing of the project. The first two project phases have been concluded and the risks managed successfully.

Components of risk management

There are a number of core components in any risk management regime. We identify the key elements as follows:

- Risk identification – risk awareness is a valuable trait that is sharpened with practice, but various disciplines are valuable to ensure risks are anticipated effectively. Risk identification is something every employee should do. The risks identified will be influenced by role and perspective. Senior management must focus on identifying strategic risks, while applying their assessment to operational and project risks identified by others.

- Risk assessment – evaluation of likelihood and potential impact. Risks are pervasive but not all risks matter. It is critical to evaluate the significance of risks for the business and for a specific time horizon. Even if unimportant now, they may be significant later. Likelihood can change, as may impact. Risk severity shapes the nature and extent of management action.

- Risk tolerance – what residual risk would be acceptable? Generally, risk cannot be eliminated but can be reduced. Management must decide what level of risk reduction is required and what adverse outcomes might be accepted. Sometimes risk appetite statements may be developed.

- Risk planning and mitigation actions are identified and established to achieve the desired residual risk level. Preventative and remedial actions should be considered. Risks may be prevented or rendered unlikely through various control measures, and impacts alleviated through appropriate plans and actions.

- Risk management is assigned – risks and their management require ownership within the business. When accountability is unclear, risks are less likely to be managed and more likely to materialise. Ownership should be assigned to the role or person who is best placed to manage the risk, acknowledging that impacts may be widespread. Even if the consequence for the organisation would be severe, it is best to allocate and manage the risk in the business area that has greatest scope for risk control.

- Monitoring and review of risks regular risk review is required, to evaluate any changes in the risk or control environment. Likelihood and impact vary as political, social and technological factors evolve, and in response to changes in the business and the mitigations put in place. Incidents occur and provide insight into risk assessment. The monitoring-feedback loop is a critical part of keeping risk management in focus.

- Reporting and escalation procedures – as risk severity changes, incidents occur, and risks materialise into issues, it is important that reporting and escalation processes exist. These enable broader perspectives and judgement to be applied in the evaluation and management of risks. Project governance processes are standard mechanisms for project risks. Supervisory oversight provides a reporting channel for operational risks and the senior leadership group should dedicate time to reviewing strategic risks, but more structured risk reporting processes for material changes in risk should be considered. A risk management committee may be established as one way of reinforcing the review processes.

Enterprise risk management at the Reserve Bank

The Reserve Bank has reviewed its enterprise risk management framework (ERM), and some key insights can be gained from this experience.

The institution has one of the broadest sets of functions amongst its global central bank peers. Amongst others, its activities include responsibility for monetary policy, regulation and supervision of the financial system, currency (cash management) operations, and operations of the payment systems infrastructure. There are considerable risks associated with each of these functions.

At the Reserve Bank we openly acknowledge risk and recognise that an effective enterprise risk management capability is an integral part of successfully running our business.

Our ERM model was developed in-house, following an extensive review of the relevant international standards and research into how other institutions were approaching risk management. It was tailored to meet two critical criteria. Firstly, it had to be the right ‘fit’ relative to the look and feel of the institution. Businesses have unique cultures and values, ways of doing things, and accepted working protocols and ERM solutions need to blend in; otherwise they may not be embraced or effectively used. Secondly, the ERM model had to be capable of covering all broad policy and operational functions within the Bank, and factor in the related external New Zealand level risks. These matters were considered essential to winning the hearts and the minds of stakeholders and embedding the ERM model in the day-to-day operation of the business.

While these criteria may sound fundamental, ERM initiatives do fail due to these considerations being underplayed or bypassed. Some ERM models are abstract and are captured by a risk-by-list mentality that ultimately diminishes their relevance. Others don't take the helicopter view across the broad spectrum of risks and therefore don't pass muster at Board level as truly reflecting an institution's risk profile.

Stakeholder engagement is a major part of our ERM framework at the Bank and spans the Board, Governors, leadership team, and the wider staff population. There has been strong support and tone at the top at the level of the Governors and the Board. Awareness, education, and reporting of results have been important in promoting the importance, power and value of sound enterprise risk management. At the senior management team level we now pass an important litmus test in that every member, whilst often focusing on their own specialist departmental level activities, can articulate in detail the current enterprise risk profile across the institution and the main issues associated with each major project initiative that is linked to a strategic priority.

Effective engagement requires ERM to connect to the day-to-day activities occurring across an institution. This provides the spark that gives substance to risk discussions, and promotes two-way conversation around how risks are being seen, managed, and where necessary treated. This means that risk managers need to have a solid understanding of all parts of the business in the context of strategic, operational and project risks.

Aligned to engagement, the development of capability across the institution is also a major component of the Bank's ERM model. At the outset of our review, we established an ERM Lead community that consists of selected senior staff whom collectively represent every function across the Bank. This community meets regularly and provides a point of contact into every department for the purposes of building up and regularly refreshing the collective risk profile. ERM Leads reach out across their respective departments to discuss risk and this provides ownership, comprehensive coverage, and capability across the entire Bank.

Over time, as new and updated ERM initiatives develop, the ERM Lead community are a key engagement point to disseminate information across the Bank. As a mature and collegial community there are also healthy cross-departmental ERM forums, and these provide a further layer of enterprise level risk focus and robustness.

To summarise, getting the “people” aspect right is critical for successful enterprise risk management. Engage, communicate, teach, explain, and then do it again, and again.

There is of course also a need for sound methodology that allows for effective, repeatable, and consistent assessment and reporting of all risks. This needs to be deployed in the same manner across all functions to provide an enterprise wide ‘apples and apples’ view of respective risks. At the heart of our methodology at the Reserve Bank we have a risk taxonomy, and associated risk likelihood and impact scaling system to classify and measure risk. This serves as a common language and is used to define and assess risks across the Bank’s activities. For example, the Bank’s leadership team can meaningfully discuss and compare a physical banknote risk alongside a monetary policy risk.

Standardised reporting provides a department-level risk profile snapshot and an aggregated whole-of-Bank view. At the whole-of-Bank level a risk trend and treatment summary is compiled and this specifies how every reported risk is being managed. This provides the helicopter view in terms of where resources, spending and focus is being applied to manage specific risks. Importantly, this provides a level of comfort that we are knowledgeable about our risks and can consider opportunities and areas for innovation for the future.

As part of our ERM model, we have given considerable thought to automation and data integration. This has resulted in an ERM data model that incorporates granular risk profiling that is integrated with internal audit issue log information and the Bank’s incident reporting records. In practice, any incident or audit issue arising is mapped to an enterprise risk, and over time a comprehensive view can be formed on how certain risks are manifesting themselves and being managed. Enterprise risks, audit issues, and incidents all use the same risk taxonomy and risk rating system and therefore data can be analysed consistently across these information capture systems. Automation extends to data visualisation of these relationships and this assists in identifying emerging trends and matters for further investigation.

Incident management is a key part of our ERM framework. We call it Proactive Problem Management or PPM in its short form, and see it as a continuous improvement mechanism. While the initial focus is on escalating and risk managing the incident, considerable value is derived from the phase that immediately follows; this being to understand root cause and insights from them. This typically drives various action plans to further strengthen processes and frameworks.

Monthly PPM summary reporting is produced for the Bank's leadership team and discussions between the risk executive and Governors. This promotes discussions at the broader institutional level around matters such as opportunity to innovate and change the way we do things, risk culture and awareness, general robustness of process, and any trends or hot spots for follow-up. Staff are expected, encouraged and thanked for raising incidents in an open and transparent manner.

The final element of the Reserve Bank's ERM framework that brings all of this together is business integration. To obtain this integration, we limit risk profiling to a relatively small set of important risks that align to our objectives and initiatives as outlined in the Bank's Statement of Intent. These risks factor in strategic considerations and related project activity underway across the Bank. The Bank's leadership team regularly review the risk profile, and the Board receive a formal report twice yearly for discussion. In addition, the Bank's senior risk management executive meets weekly with the Governor of the Bank to discuss the risk profile and related matters of significance.

In essence, enterprise risk management is highly visible and can be seen in action day-in-day-out across the business. ERM is transparent and inclusive and allows the organisation to make informed decisions. Perhaps most importantly, it has helped instil an organisation-wide risk management culture.

We are very satisfied with the recent refresh of our ERM model. But we know that there will always be more to do to deliver a tailored best practice risk management solution to the institution. With this in mind our current focus is on further refining the articulation of risk appetite and exploring our risk culture as it relates to leadership behaviours and overall staff engagement.

More generally, there is a strong sense that ERM is a powerful tool that can continue to identify opportunity and drive innovation across the Bank. There is a strong sense that by connecting to stakeholders and the business even more we will reap greater rewards in the future.

Insights and reflections on risk management from executive management

With over twenty years of senior executive management experience between us, the authors have witnessed successful and not so successful risk management endeavours. This section summarises our thoughts on the value and critical success factors in organisational risk management.

We are unashamed advocates of risk management: done well, it pays-off. As the Performance Improvement Framework (PIF) "Getting to Great" document[4] attests from its study of public sector agencies (and we see no reason to think it is different for the private sector) "The best performing agencies manage risk, while others tend to avoid it."

In summary:

1 Risks are more likely to eventuate when preparedness is inadequate. This is the story of the HLFS-Computer-Assisted Interviewing development and the Findur upgrade. All too often, we are over-optimistic that things will go well.

2 The adverse consequences when risks eventuate are generally worse when risk management is limited. For example, disaster recovery is a lot easier if measures are in place – even if they prove partial. The census data back-up was not perfect but it was much better than nothing. Reputational damage is lessened if measures exist yet are inadequate compared with the situation where the risks were

[4] SSC, "Core Guide 3: Getting to Great; Lead Reviewer insights from the Performance Improvement Framework", April 2013.

unidentified and uncontrolled, i.e. mitigations were absent. For example, The ACC privacy breaches were accentuated by a lack of privacy management. The payments failure – while it still occurred – would have been much worse without contingency measures in place.

3 Being risk aware and risk prepared (risk smart for short) supports innovation, rather than impeding it, as many fear. In many cases, opportunity and risk are shadows of one another. Both elements must be kept be in focus. When someone identifies an opportunity, we ask what risks exist, so that the gains will not be lost. When risks are raised, we ask what opportunity is there to move forward.

4 Risk management is a whole of organisation task or responsibility. It needs to be demanded and modelled by executive management, owned and applied by business managers, and supported and monitored by a specialist risk management function. Accountability for risks should be assigned but everyone is responsible for risk management. Leadership is crucial in setting the risk/innovation tone and leading the organisational dialogue. An enterprise risk management framework helps instil widespread organisational ownership and builds a risk management culture.

5 Risk management tends to atrophy if one is not careful. Successful risk management tends to undermine its own apparent value. A higher risk appetite can be sustained and greater risks may be taken, or complacency can set in because risks have been successfully, but almost unknowingly, averted. It is important to develop the culture, disciplines, processes, and learning mechanisms that keep risk management fresh, e.g. quasi-incidents can be useful reminders perhaps via BCP exercises, security penetration testing, and external review etc. Risk management committees have a place in maintaining the focus.

6 Engagement and conversations are vital. Risks need to be talked about. This builds awareness and action. Developing a culture in which risks and risk-taking can be discussed, managed and accepted is a key leadership challenge.

While we are not wedded to explicit, whole of organisation, risk appetite statements, the conversations about risk tolerance for particular risks are crucial. It is important to send clear messages to an organisation about whether, why and which risks should be reduced or relaxed a little. Some are below the waterline and must be averted. Others may be above it and permit greater risk taking. Strong, consistent senior leadership is vital.

Often staff or lay observers contend that risk management will tie an organisation up with process and overhead, slowing it and its innovative capacity down. This need not be the case. Motor racing and sail boat racing enthusiasts recognise the finely balanced science and art of incurring increased risk to increase speed, and then set about optimising the trade-off. Recall Sir Peter Blake's famous dictum that the black magic campaign was about doing everything to make "the boat go faster", without making it unstable.

Organisations need to incur risk in order to prosper. We are not there to tie down all the hatches and keep the sails furled. Our goal is not risk avoidance but risk awareness, risk management and, indeed, calculated risk-taking.