Interim Report:
Risk Management Maturity in Large Australian Superannuation Funds

Elizabeth Sheedy, Denise Jepsen

Associate Professor Elizabeth Sheedy is a specialist in financial risk management based at the Macquarie Applied Finance Centre.

Associate Professor Denise Jepsen is an organisational psychologist in the Faculty of Business and Economics at Macquarie University.

This research has been conducted with financial sponsorship from EMC Corporation, the parent company of RSA Security LLC, a provider of systems for governance, risk and compliance i.e. RSA Archer® Suite of products.

We gratefully acknowledge advisory support from the following organisations: Australian Securities and Investment Commission, Financial Services Council, Mercer Australia and RSA Archer. Survey administration/reporting was conducted with the assistance of Voice Project. Research assistant Lina Tong provided statistical analysis of survey data.

The research would not have been possible without the many industry participants who gave up their time and expertise for interviews. The four organisations that allowed us survey access have also played a vital role. While they must remain nameless, their generous contribution for the good of the industry is deeply appreciated.

No individual or organisation had any right of review with regard to this publication, except (where relevant) to ensure that they could not be identified.

This version: April 2018

Summary:

Given the immense importance of the superannuation sector for all Australians, the objective of this study is to investigate risk management maturity in the superannuation sector and identify areas for further improvement. The study focusses on large superannuation funds (i.e. those with assets under management in excess of $10 billion) and coincides with the fifth anniversary of the implementation of the prudential standards for risk management in July 2013.

1. Building on previous research from the safety field, and with input from our panel of subject matter experts, we have developed a 5 level model of risk management maturity.

2. The majority of subject-matter experts interviewed believe that Level 1 would be appropriate and desirable for the sector given the importance of managing retirement savings. While rapidly evolving, most large Australian superannuation funds, have not yet met this risk maturity standard. This is true despite the laudable focus of the industry on member outcomes.

   A majority of experts believes that most large funds are currently at Level 3, some at Levels 2 and 4, with few if any at Level 1. In other words, many large funds are still working to realise effective risk management systems and frameworks. At this level the focus is on ensuring that risk management systems are well resourced and functioning efficiently (people, IT systems, processes, reporting lines, remuneration and performance measurement); risk management is built into the governance framework; the board takes responsibility for risk management and ensures that the risk appetite is consistent with strategy. This is not surprising given the relatively short time since prudential standards for risk were introduced.

   A minority of experts had a more positive perception of risk management maturity in the sector, perceiving a number of funds to be at Levels 1 and 2 already.

3. We also developed a list of attributes of organisations with risk management maturity. These attributes should be seen as requirements over and above the implementation of effective risk management systems (Level 3). At Level 1 an organisation should have all, while at Level 2 an organisation should have some of the following attributes:
    i. *Commitment to continuous improvement of the risk management framework*. This attribute could also be thought of as 'chronic unease' regarding risk. An example might be participation in benchmarking with firms, both peer and outside the sector, in order to learn and improve. New risk management initiatives are well supported by all managers. The incident reporting system is comprehensive (i.e. captures all risk events) and this information is analysed and used for organisational learning. The risk management system is regularly audited and follow-up is timely and thorough.
    ii. *Everyone has accountability for risk management*. All staff in the organisation have a role to play in the risk management process and they take that role seriously i.e. thoughtful engagement as opposed to 'mere compliance'. Risk management is not just something for the risk experts.
    iii. *Risk management viewed as an enabler*. Risk management is seen as adding value to the organisation rather than a drag on performance. This is likely to occur when staff are well-educated regarding risk management and when risk systems are functioning well. In the alternative case, staff will see risk management as simply a regulatory requirement – a hurdle to be cleared but not truly valued.
    iv. *Risk communication is effective*. Staff have regular and useful discussions about risk management. Information about risk flows easily through the organisation to the people who need it for decision-making. For example, staff have a clear understanding of risk appetite as it relates to their role; 'bad news' travels easily to higher levels.
    v. *Right amount of the right risks*. An outcome of maturity is that the organisation is rarely surprised by risks that have not been identified and risks affecting the organisation are almost always within tolerances so there are few surprises. Emerging risks are quickly recognised and incorporated into the relevant frameworks. This assumes that risk appetite is consistent with strategy.

4. Interviews with subject-matter experts highlighted challenges for the industry in all of the maturity attributes, thus confirming that risk management maturity has room for improvement.

5. Staff surveys in four large Australian funds confirm the interview findings in relation to risk management maturity. (The sample will extend to five funds in the final report.)
    i. None of the funds we have assessed so far has achieved consistently strong ratings for risk structures, suggesting that there is further work to be done bedding these down.
    ii. The 'structural' area of most concern is performance measurement and remuneration systems. We observed disappointing staff ratings in this category (from 46% to 64% favourable), suggesting that a significant proportion of staff in the funds we assessed perceive that remuneration and performance measurement systems are creating a short-term focus. This is concerning since effective risk management relies on managing for the long-term. In all four

funds we assessed, at least some staff are eligible for annual cash bonuses but systems for deferral and clawback of these bonuses are not widely used.

iii. Many positives were observed, suggesting these funds have made significant progress toward the implementation of a risk management framework. Culture ratings were strong in some dimensions (Proactive, Valued, Manager) with ratings of 90% favourable or higher in most cases. Staff and senior leader ratings of risk governance/structures were also strong with ratings of 80% favourable or higher in most areas.

iv. The weakest culture dimension was Avoidance (the perception that risk events are ignored, downplayed or excused). Weakness on this dimension is likely to reduce the effectiveness of risk communication and thus the ability of the organisation to resolve issues efficiently. Regression analysis has shown that Avoidance is significantly associated with self-reported undesirable risk behaviour such as failure to report risk events, failure to speak up, lack of accountability, unethical behaviour towards members, overconfidence etc.

v. Survey assessments of risk culture suggest significant variation between and within large superannuation funds. Technology teams had the least favourable risk culture scores.

vi. Staff accountability for risk management remains an issue with many still perceiving that risk management is the responsibility of specialists. This suggests that implementation of 'three lines of defence' and other systems to build staff accountability need further work.

vii. The survey assessment of maturity also highlighted that risk management in some funds has too much emphasis on mere compliance (as opposed to thoughtful engagement). Risk managers are also struggling to overcome perceptions that risk management is a drag on performance rather than an enabler for success.

viii. An opportunity for improvement exists in relation to reporting of risk events, with between 10% and 35% of survey respondents admitting to under-reporting.

Following the introduction, Section 1 provides background on risk management in the superannuation sector. Section 2 explains the risk management maturity model while Section 3 reports the results of the interview study. Section 4 reports on the survey study while limitations of the study are described in Section 5.

Introduction and Method

This research aims to build understanding of risk management maturity and related issues in large Australian superannuation funds, those with more than $10 billion in funds under management. The Australian superannuation industry now manages some $2,324 billion in assets (ASFA, 2017), making it one of the largest retirement pools in the world. The industry exists to help Australians save for and live comfortably in retirement, complementing the age pension. This task carries substantial and complex risks. Ensuring the industry is well equipped to manage these risks is of utmost importance.

The study builds on previous research on risk culture in the banking sector conducted from 2013-2016. This mixed methods study incorporates the following elements:

1. *Document analysis*: Evaluation of industry documents (see Section 2)
2. *Expert interviews*: semi-structured interviews with 24 industry experts (see Section 3)
3. *Employee surveys*: census employee surveys of five large Australian superannuation funds (see Section 4). All 21 large superannuation providers (APRA, 2017b) were invited to participate in the research. Surveys have been completed in four of the five self-selected participating superannuation funds. Of the five, three funds are from the 'profit for member' sector, one is a corporate fund and the other is from the retail (for-profit) sector.

To support the project we first established an advisory panel with representation from the Australian Securities and Investments Commission (ASIC), the Financial Services Council (FSC), Mercer Australia, and RSA Archer (a provider of governance, risk and compliance software solutions). We received financial sponsorship for the project from EMC Corporation, parent company of RSA Archer.

The advisory panel provided advice to ensure that we had obtained relevant documents relating to risk management in the industry. The panel also supported our program of interviews with subject-matter experts; in some cases panellists were themselves interview subjects and in other cases they provided introductions to relevant experts for interview. From February 2017 to April 2018 we analysed relevant regulatory documents and cases and interviewed 24 subject-matter experts. The objective was to develop a deep understanding of risk management issues in the superannuation industry by addressing the following questions:

1. How can risk management maturity be defined/assessed?
2. How mature is risk management in large Australian superannuation funds?
3. Reporting and learning from risk events is considered by many to be a crucial attribute of risk management maturity. To what extent is under-reporting occurring and why?

The research was approved by the Macquarie University Human Research Ethics Committee.

1. Background to Risk Management in Superannuation Funds

1.1 Australian Superannuation Industry

The history and structure of the Australian superannuation industry is thoroughly explained in a recent review (ASFA, 2017) by the Association of Superannuation Funds of Australia (ASFA). This document charts the growth of the Australian retirement savings pool and explains the main fund types: Retail funds (for profit and run by large institutions such as banks), industry funds (drawing members from a single industry or state), public Sector funds (sponsored by government primarily for public sector employees), corporate funds (sponsored by one or more employers for the benefit of their own employees) and small funds (including self-managed superannuation funds).

More than 90% of funds are now in accumulation schemes where the investment risk is borne by individual members. Such defined contribution superannuation schemes are fundamentally different from investment products such as bank deposits, bonds or defined benefit schemes where the issuing or sponsoring institution makes promises regarding future value. In Australia superannuation funds typically operate as trusts; trustees owe members statutory fiduciary duties as defined in the Superannuation Industry (Supervision) Act 1993.

When the Act (commonly known as the 'SIS Act') came into effect in 1994, it provided an enhanced prudential supervision framework. Most[1] large superannuation funds (retail, industry, corporate and public sector funds) are prudentially supervised by the Australian Prudential Regulation Authority (APRA). From 1 July 2006, all superannuation trustees were required to obtain a Registrable Superannuation Entity (RSE) licence from APRA.

1.2 Risk management regulation

From 1 July 2013, prudential standards relating to risk management (SPS 220, 2013) came into effect for superannuation funds. It applies to all RSE's under the SIS Act. This standard and the accompanying prudential practice guide (SPG 220, 2013) explain APRA's requirements and expectations for risk management in superannuation funds.

The risk management framework is defined as 'the totality of systems, structures, policies, processes and people within an RSE … that identify, assess, manage, mitigate and monitor all internal and external sources of inherent risk that could have a material impact on … business operations or on the interests of beneficiaries' (SPS 220, paragraph 6). The risk management framework is a board responsibility.

[1] Some Public Sector funds are regulated by state or commonwealth government.

Notably, SPS 220 highlights the importance of risk culture for producing good risk management outcomes (paragraphs 4-9). In this regard APRA expects the board to 'demonstrate its commitment to risk management and foster an environment of active engagement and risk management processes and outcomes, and in which the risk management function is influential and respected.'

SPS 220 also provides standards relating to risk appetite[2] (paragraphs 22-34), the risk management function (paragraphs 38-44), controls and mitigation (paragraphs 47-54); monitoring and reporting (paragraphs 55-60), review of the risk management framework including an independent comprehensive review every three years (paragraphs 61-66), audit (paragraphs 67-68), risk management declaration (paragraph 69) and APRA notification requirements (paragraph 70).

The SIS Act stipulates that an RSE licensee must maintain and manage financial resources to cover the operational risk that relates to its business operations. Prudential Standard SPS 114 Operational Risk Financial Requirement (SPS 114) establishes requirements relating to these financial resources. While APRA does not set a minimum capital requirement for superannuation funds per se, the guideline of 0.25 per cent of funds under management has become a de facto standard for soundly run RSE licensees that have implemented a risk management framework. To our knowledge, all large Australian superannuation funds currently resource their operational risk reserve at 0.25 per cent of funds under management.

1.3 Risk Management in Superannuation

In their paper on risk management in superannuation (pension) funds, Kemp and Patel (2012) confirm the relevance of an entity-wide approach to risk management. In other words, the holistic risk management frameworks applied in other financial institutions translate also to superannuation funds.

The fact that superannuation funds are managing risk on behalf of their members, rather than taking risk for their own account, only heightens the need for an effective risk management framework. In other words, the fiduciary nature of the relationship creates a strong duty of care in terms of protecting the interests, and hence the risks, of members. The member focus of superannuation funds, especially profit-for-member funds, is arguably a strength that supports good risk management practices.

Risk management, across all industries, is often misunderstood. It is wrongly viewed as solely a defensive activity with the purpose of reducing risk. But according to international risk management standards (ISO 31000, 2018) the purpose of risk management is the '*creation and protection of value. It improves performance, encourages innovation and supports the achievement of objectives*.' Highlighting the breadth of risk management, the standard states:

> *Managing risk is iterative and assists organizations in setting strategy, achieving objectives and making informed decisions. Managing risk is part of governance and leadership, and is fundamental to how the organization is managed at all levels. It*

[2] The degree of risk an RSE licensee is prepared to accept in pursuit of its strategic objectives.

> *contributes to the improvement of management systems. (ISO 31000, 2018, Introduction)*

Since the primary objective of the Australian superannuation system is to provide income for retirement, then the *purpose of risk management in superannuation is to increase the likelihood that Australians have an acceptable/comfortable income in retirement*. In other words risk management in superannuation is designed to improve the quality of member outcomes.

Analysis conducted by APRA (APRA, 2017a) suggests that in a number of cases superannuation funds are not achieving quality member outcomes. This conclusion is based on the analysis of net returns, cost of insurance cover, administrative and operating expenses, net member benefit outflow ratio etc. The failure to achieve quality member outcomes is likely to be related to risk management deficiencies as indicated below:

> '*Generally, the RSEs that APRA has identified as having concerns in respect of quality member outcomes and future prospects are those RSEs that have performed poorly on an absolute and relative basis on a majority of the quantifiable metrics. In APRA's experience, RSE licensees of these RSEs can also have inadequate strategic and business planning practices, governance and/or risk management frameworks to address the risks arising from poor performance. APRA will review its assessment of RSE licensees and their RSEs regularly*.' (APRA, 2017a)

To achieve quality member outcomes it is necessary to accept a range of risks, notably investment risk. To highlight other examples of appropriate risk-taking, many funds have discovered that to achieve sufficient scale and efficiency for quality member outcomes, it has been necessary to accept and manage the significant risks associated with mergers. In order to achieve efficiencies and enhance service to members it has been necessary to invest in new systems and technology with consequent project risks.

In the regulatory documents risk is defined broadly to include both financial and non-financial risks. Attachment A of SPG 220 thoroughly explains the categories of material risks for superannuation funds. Table 1 below lists the various risks from this document and highlights some of the issues that have arisen in recent years.

Table 1: Risks in the Superannuation Industry

Risk Category (SPG220 Appendix 3)	Recent Issues
1. Strategic and tactical risks are the risks that arise from an RSE licensee's strategic and business plans. Examples may include, but are not limited to, risks: (a) from the development of new products or introduction of new systems and processes; (b) associated with a change of strategic direction, e.g. developing an in-house business function, or a decision to outsource or offshore an existing business function; (c) associated with planned activities such as merger or acquisition; (d) associated with the solvency of the RSE licensee or the risk that the value of the assets of at least one of the RSEs may fall below that required for it to remain a going concern or that an RSE may not be able to provide benefits under the governing rules; and (e) arising from changes to the external business environment, e.g. competitor and market changes.	1. Recent strategic/tactical issues: a) Interviews highlighted that funds regularly launch new products and/or new investment options which may or may not succeed in addressing member needs. New IT systems (including governance, risk and compliance systems) have recently been introduced in many funds participating in the study. Rapid growth was highlighted as a particular source of risk and this is challenging for those funds pursuing a growth strategy. b) A number of large funds have made the decision to either increase or decrease the level of insourcing of investments (Gallagher, Gapes and Warren 2017). Outsourcing is an important feature of the industry not only for investments, but also fund administration. APRA has provided specific prudential standards relating to outsourcing risk (APRA, 2012). c) Industry consolidation has already occurred and is likely to continue. The small scale of many funds creates inefficiencies. (Rice Warner, 2017) d) Numerous changes have occurred and continue to occur e.g. changes to tax arrangements for superannuation, changing regulations, aging population and increasing rates of retirement. See KPMG (2017) for discussion.
2. Governance risks are those risks that threaten the ability of an RSE licensee to make reasonable and impartial business decisions in the best interests of beneficiaries. Governance risks may include, but are not limited to, risks associated with: (a) accountability and transparency of decision making processes; (b) delegations of roles and responsibilities; (c) remuneration arrangements; (d) fitness and propriety; and (e) the management of conflicts of interest.	2. Regulators have expressed concerns about the governance of super funds, especially board selection and renewal. 'We firmly believe that all boards benefit from having some independent directors, to provide access to a wider range of skills and experience and enhance decision-making and constructive challenge.' (APRA, 2017) Interviews with subject matter experts revealed that performance-based remuneration is increasing in the industry. There is potential for this trend to have undesirable consequences if they are poorly designed and staff start to act

	in a more self-interested manner in order to maximise remuneration. Conflicts of interest may arise where (for example) the RSE licensee has an association with a service provider (such as an investment manager or administrator). Although conflicts of interest are arguably far less likely to occur in the profit-for-member sector, an isolated incident is identified in the Royal Commission into Trade Union Governance and Corruption (2015). Here a fund inappropriately released private member information to a related union.
3. Governance risks may also arise in transitional situations where, for example, functions are moved between in-sourced and outsourced arrangements, or when transferring business functions between outsourced service provider; or in situations where essential staff are absent or to be replaced.	See 1b) above.
4. APRA expects an RSE licensee would ordinarily expressly consider agency risk as part of governance risk. Agency risk relates to the possibility that internal or external service providers, subsidiaries, fund promoters, agents and advisors will not act in the best interests of beneficiaries and/or have misaligned incentives for the provision of service to the RSE licensee.	4. Agency risk has been particularly problematic for retail funds with their links to financial advisors. In a significant number of cases advice has been given that is not in the best interests of members. (ASIC, 2018)
5. Operational risk is the risk of loss resulting from inadequate or failed internal processes, people and systems or from external events. This includes legal risks, but excludes strategic and reputational risks. Operational risks are often categorised as the risk of loss from: (a) internal fraud - losses due to acts of a type intended to defraud, misappropriate property or circumvent regulations, the law or company policy (excluding diversity/ discrimination events) which involve at least one internal party; (b) external fraud - losses due to acts of a third party that are of a type intended to defraud, misappropriate property or circumvent the law; (c) employment practices and workplace safety - losses arising from acts that are inconsistent	5. Losses are experienced by super funds in all of these operational categories. Legal/compliance risk is one of the greatest challenges for the superannuation sector. According to PWC (2015) the difficulty of keeping up with constantly changing regulatory expectations and the growing burden of compliance costs are both significant issues. According to our subject-matter experts, many funds have devoted considerable resource in recent years to the management of fraud risk. In relation to (d), it is worth mentioning issues relating to insurance in superannuation e.g.

with employment, health or safety laws or agreements, from payment of personal injury claims or from diversity/discrimination events; (d) clients, products and business practices - losses arising from an unintentional or negligent failure to meet a professional obligation to specific clients, including fiduciary and suitability requirements, or from the nature or design of a product; (e) damage to physical assets - losses arising from loss or damage to physical assets from natural disaster or other events; (f) business disruption and systems failure – losses arising from disruption of business or system failures; and (g) execution, delivery and process management – losses arising from failed transaction processing, process management, relations with trade counterparties and vendors. This category includes administration errors and unit pricing errors.	over-insurance of young members (Rice Warner, 2017a). In relation to (f), APRA has provided specific prudential standards relating to ensuring business continuity (APRA, 2012a). In relation to (g) it is worth highlighting project risks. Interviews revealed that many funds are pursuing complex projects to exploit digital technology. These projects have considerable risks with potential for cost blow-outs and delays.
6. Investment governance risk is the risk that threatens the ability of an RSE licensee to manage its investments to adequately protect the interests, and meet the reasonable expectations, of beneficiaries. Investment governance risks may include, but are not limited to, weaknesses in: (a) the investment governance framework; (b) delegations and decision-making processes; (c) the selection, retention, monitoring and reporting of investments; and (d) management of the services provided by investment managers, advisors and other third-party service providers.	6. Investment governance risk is a major area of focus for superannuation funds. Subject-matter experts highlighted the extensive due diligence that many funds apply in relation to external fund managers. The most common potential problem is that funds can underperform their investment benchmarks and/or member expectations due to poor investment choices. Investments is a highly technical area, creating challenges for directors who are less skilled in the quantitative disciplines. The Trio Capital case affected a number of superannuation funds that suffered losses due to fraud in a managed investment scheme. (Commonwealth of Australia, 2013)
7. Liquidity risk is the risk of inability to meet obligations as and when they fall due without incurring unacceptable losses.	7. Interviews highlighted that liquidity risk will become an increasing focus as more people retire and wish to withdraw funds. It is particularly problematic for funds holding significant illiquid assets such as unlisted property and private equity. See Gribble and Helenius (2011) for a discussion of liquidity issues during and following the global financial crisis.

8. Insurance risk is the risk of making insured benefits available to beneficiaries including where an RSE licensee self-insures benefits to members.	8. Some issues have emerged recently regarding insurance claims and complaints handling (ASIC, 2017a).

When a superannuation fund experiences losses due to one of the risks in Table 1, the losses may be experienced in a variety of ways. For example losses may result in:

- Higher operating costs, resulting in lower net returns to the member;
- Insurance claims, resulting in higher premiums and hence higher operating costs;
- Withdrawals from administrative and operational risk reserves, thus reducing the level of reserves available for future needs and potentially inflating the necessary level of reserves, and;
- Diminished investment returns.

The often discussed issue of member disengagement (Financial Services Council, 2017) means members are often unaware of losses due to poor risk management, even when those losses are disclosed in member communications. Even if they are aware of losses, lack of understanding may mean that members do not always make the connection between loss events and poor risk management practices.

2. Risk Management Maturity Defined

To assess risk management maturity in Australian superannuation funds it is first necessary to define what is meant by this concept. Again we approached this issue by examining relevant documents. Table 2 lists the documents we analysed.

Table 2: Analysis of Documents (Safety and Risk Management Maturity)[3]

Reference	Comment
Westrum, 1996	Original 3 step safety maturity model: pathological (lack of safety is entrenched), bureaucratic (focus on compliance with safety rules and procedures) and generative (safety fully integrated into decisions).
Reason, 1997	Took the 3 step model of Westrum to 5 steps including Reactive (only focuses on safety after an incident) and Proactive (taking active, anticipatory steps to minimise accidents).
Hillson, 1997	Characteristics of maturity: proactive approach to risk management; leaders committed to risk management and lead by example; processes regularly refreshed and updated; regular external training; state-of-the-art tools and methods; risk-based reporting and decision-making; learning from experience is embedded; focus on opportunity management (upside risk); all staff are risk aware.
Hudson, 2001	See especially evolutionary model of safety culture from oil and gas industry. At the 'generative' level: information is sought (not hidden); messengers are trained (not shot); responsibilities are shared (not shirked); failure causes enquiry (not cover up); new ideas are welcomed (not crushed).
Parker, Lawrie and Hudson, 2006	Provides more detailed understanding of the 5 levels of safety culture (see Reason, 1997; Hudson, 2001). Emphasises importance of reporting. At low levels many incidents go unreported but at higher levels information is relatively complete and incident reports/investigations are used to improve processes.
Macgillivray, Sharp, Strutt, Hamilton and Pollard, 2007	Describes five maturity levels. Level 5, the optimised organisation, is characterised by flexibility and attention to human behaviour. Focus is on continuous learning and innovation to optimise risk management.
ISO 31000, 2009	Annex A gives attributes of high performance (mature) risk management organisations: continual improvement, staff accept full accountability for risks,

[3] We acknowledge the valuable assistance of Rosalie Degabriele who assisted us by identifying a number of these documents.

	risk management built into all decisions, continual communication about risk, risk integrated into governance structures.
Chartered Secretaries of Australia, 2010	Findings from a survey of governance and risk professionals. Identified a gap in 'forward-looking, strategic level of risk management'. Also noted that risk management often seen as defensive rather than as an enabler for value creation.
Institute of Internal Auditors, 2013	'The Risk and Insurance Management Society Risk Maturity Model for ERM measures organizations on their adoption of enterprise risk management (ERM) best practices from the most widely used risk management standards' e.g. ISO31000, COSO, SOLVENCY II. Attributes: adoption of ERM approach, ERM process management, risk appetite management, root cause discipline, uncovering risks, performance management, resilience and sustainability.
Farrell and Gallagher, 2015	This study applies the Risk and Insurance Management Society Risk Maturity Model, which scores firms on a five-point maturity scale. The authors document a positive association between maturity (by this measure) and higher firm value.

Risk management maturity has not been investigated in the academic literature but it is likely to be related to safety maturity. Occupational safety risk is an example of a particular risk type with potentially massive human cost. With such high stakes it is not surprising that researchers have been investigating the issue for some years. In many hazardous workplaces there is a natural tension between workplace safety and production/profit. That is, managing safety well often results in higher costs and slower rates of production. An obvious parallel exists in financial institutions where a tension exists between effective risk management and short-term profits[4]. Many lessons from the field of safety, including the importance of firm culture for achieving good outcomes, have translated well to the field of risk management more broadly. It seems reasonable to assume that a safety maturity model will have relevance for risk management maturity, so for this reason we analyse documents relating to safety maturity as well as risk management maturity.

The 5-step model of safety maturity (Reason, 1997; Hudson, 2001; Parker, Lawrie and Hudson, 2006) is an obvious starting point. Substituting terminology that is less safety specific, we produced the following:

[4] As noted previously, for 'profit-for-member' superannuation funds, a tension exists between risk management and other objectives such as cost reduction, increasing fund size and increasing investment returns.

Figure 1: Risk Management Maturity (adapted from Parker, Lawrie and Hudson, 2006)

Many organisations start at Level 5 where risk is not on the agenda at all but rather the focus is elsewhere (growth, profits etc). Early risk management initiatives are reactive (Level 4) – attention is given to risk only when something goes wrong or the regulator requires it. Often a major problem, scandal or loss can be the catalyst for implementing a risk management program. Level 3, calculative, is where many organisations experience challenges. The task of establishing effective systems and framework is considerable. Here the focus is on ensuring risk management systems are well resourced and functioning efficiently (people, IT systems, processes, reporting lines, performance/remuneration systems). Risk management is also built into the governance framework; the board takes responsibility for risk management and risk appetite is consistent with strategy.

The higher levels of risk management maturity go beyond simply having these effective systems and the organisation becomes more proactive in its approach to risk. The organisation is now on the front foot. Levels 2 (Proactive) and 1 (Generative) are associated with attitudes and perceptions throughout the organisation that support risk management. In other words, risk management is embedded into the organisational culture – our way of doing business (Kemp and Patel, 2012). Risk management is no longer regulator-driven but self-generated. Based on the literature from Table 3 we also developed a list of key attributes of organisations with risk management maturity. At Level 2 an organisation might have some of these attributes whereas at Level 1 the fund should have all of the following:

- *Commitment to continuous improvement* of the risk management framework. This could also be thought of as 'chronic unease' regarding risk. An example of this might be participation in benchmarking with both peer firms and firms from outside the industry in order to learn and improve. The incident reporting system is comprehensive (i.e. captures all risk events) and this information is analysed and used

for organisational learning. The risk management system is regularly audited and follow-up is timely/thorough.

- *Everyone has accountability* for risk management. All staff in the organisation have a role to play in the risk management process and they take that role seriously i.e. thoughtful engagement as opposed to 'mere compliance'. Risk management is not just something for the risk experts.
- *Risk management viewed as an enabler.* Risk management is seen as adding value to the organisation rather than a drag on performance. This is likely to occur when staff are well-educated and experienced regarding risk management and when risk systems are functioning well. In the alternative case, staff will see risk management as simply a regulatory requirement – a hurdle to be cleared but not truly valued.
- *Risk communication is effective*. Staff have regular and useful discussions about risk management. Information about risk flows easily through the organisation to the people who need it for decision-making. For example, staff have a clear understanding of risk appetite as it relates to their role; 'bad news' travels easily to higher levels.
- *Right amount of the right risks.* An outcome of maturity is that the organisation is rarely surprised by risks that have not been identified and the risks affecting the organisation are almost always within tolerances i.e. few surprises. Emerging risks are quickly recognised and incorporated into the relevant frameworks. Risk appetite is consistent with strategy.

3. Expert Perceptions of Sector-Wide Risk Management Maturity

We conducted a series of semi-structured subject-matter interviews with 24 experts from the field to discuss their perceptions of risk management maturity among large Australian superannuation funds. The experts represented the following perspectives:

- 12 senior risk professionals (RPs) mostly currently Chief Risk Officers or equivalent in large[5] superannuation funds, and many had experience from outside of superannuation,
- 6 trustee directors (TDs) on the board committee with responsibility for risk management, either Chair or member of the Audit, Risk and Compliance Committee,
- 1 senior representative of an organisation that researches and rates super funds (Ratings),
- 1 regulator (Reg), and
- 4 consultants with extensive expertise in risk management/governance in the superannuation sector (Consultants).

The experts were interviewed on the basis of confidentiality i.e. neither they nor the organisations they represent would be identified in research publications. The interviews were conducted with approvals under Macquarie University's Human Subject Ethics Committee.

We applied a deductive research approach. That is, both the maturity model and the list of attributes described in Section 2 were presented to the subject-matter experts for comment. In the semi-structured interviews we asked a series of questions including: What does risk management maturity mean to you? Do you feel this model adequately captures the issues as you see them? How mature is risk management in your fund (if applicable)? How mature are large Australian funds generally? Of the risk management attributes, which are most challenging for superannuation funds? What impediments exist to risk management maturity; what are the competing priorities?

3.1 Feedback on the model

We received unanimously positive feedback on the proposed model. There was no significant disagreement regarding the attributes of risk management maturity although some minor modifications were made during the interview process.

[5] One of the risk professionals represented a medium-sized superannuation fund.

3.2 Maturity ratings for large super funds

During interviews, the majority of subject-matter experts expressed the opinion that risk management maturity in large superannuation funds often lags that of banks. This viewpoint was supported by the fact that a number of the senior risk professionals we met had been recruited from risk roles in banking due to their experience in that sector. The reflections of risk professionals with cross-sectoral experience were telling:

> *Super funds are behind the banks by about 5-10 years (RP).*
>
> *Maturity in super funds is growing but definitely lags banks and I'm happy to be quoted on that (RP).*

We specifically asked whether any large funds have reached Level 1 (Generative) at the top of the maturity ladder. While three interviewees felt that a number had reached this point[6], the majority opinion was that no Australian super fund has yet reach this point, but some have reached Level 2 (Proactive). The majority opinion from our experts is that most large Australian funds sit at Level 3 (Calculative). In other words they are still focused on embedding risk systems and frameworks. Further evidence to support this conclusion is found in the following sections of the report which examine the various attributes of risk management maturity.

It is important to note that the industry has a well-established focus on meeting the needs of members, especially in the 'profit-for-member' sector. Numerous interviewees commented favourably on this characteristic and contrasted it with attitudes elsewhere in financial services. While the member-driven ethos is consistent with and even supportive of a risk focus, it does not necessarily guarantee risk management maturity as we have defined it.

All experts agreed there is a range of risk management maturity both within and between funds. A number of experts suggested that within funds, maturity was greater in investment teams. As a generalisation, larger funds tend to have greater maturity than small; this is because smaller funds tend to struggle with resourcing of the risk function. Some expressed the opinion that size is not a perfect predictor of risk management maturity in super funds.

Why the difference between banks and large super funds? It is likely that different regulatory requirements are a causal factor. In Australia the larger banks have all obtained approval from APRA to use the Advanced Measurement Approach for both Operational Risk and

[6] For example two interviewees from the same consulting firm shared their views of large super funds as follows: 'The leaders are very engaged in risk management and have a good understanding of strategic risks. They are doing a good job of managing outsourcing risks. Three lines of defence has been well embraced. Issues that come up are dealt with appropriately i.e. there is good learning from risk events. These days risk management is typically built into performance indicators i.e. the appraisal process. Boards are being more active and this is showing up in turnover of senior executives. In many cases a separate Risk Committee has been created and a CRO role has been created (often on the Exec Committee). The funds we have close dealings with are making concerted efforts to embed a risk culture.'

Credit risk. These approvals were obtained in the mid-2000's to prepare for the introduction of the Basel II Capital framework and, given the scale and complexity of operations, required a substantial investment in risk management frameworks to manage, measure and monitor risk. Significant firm resources (systems and people) were allocated to risk management, signalling the value placed on risk management.

The requirement to develop capital models that were risk sensitive brought considerable analytical rigour to bear on risk management. Despite the imperfections of the risk models that have become apparent (PWC, 2015), their introduction meant that many risks became more obvious and therefore a focus for management. For the first time managers had a clear incentive to reduce risk to minimise the requirement for expensive equity capital.

The global crisis that emerged in 2007 brought even more scrutiny of risk management practices in Australian banks. While Australian banks had a 'good crisis' relative to those in most other countries, it was nevertheless a time of heightened risk management focus due to higher funding costs, increasing impaired assets, need for capital raising and the need for more conservative liquidity management (for example, see RBA, 2009). From late 2009 consultations began regarding enhancements to the Basel II framework (i.e. Basel III) to strengthen regulatory capital, risk management and supervision requirements (see APRA, 2009). In the years following the crisis the focus on and resourcing of risk management in banks continued to grow (Economist Intelligence Unit, 2010).

In the case of superannuation funds, most implemented a risk framework at the time the new regulations came into effect in mid-2013. International risk management standards (ISO 31000, 2018) argue that risk management is an iterative process. By definition, there has not been sufficient time for these frameworks to mature and become fully effective.

3.3 What level of maturity is appropriate in superannuation funds?

All but one of the experts we interviewed believes that Level 1 is desirable for the sector, having regard for the importance and complexity of the task of managing retirement savings. Reaching Level 1 does not guarantee quality member outcomes but increases the likelihood of achieving this objective.

3.4 Attributes of maturity

Experts provided insights in relation to each of the attributes.

3.4.1 Effective Systems and Frameworks

This maturity attribute relates most closely to Level 3 in the risk maturity model. Most experts said that systems and frameworks are still under development in the superannuation sector. Adequate resourcing of systems and frameworks is improving but remains an issue for many large funds as the following quotes highlight:

> *Governance Risk and Compliance (GRC) systems in the sector are typically very basic. It's essential that systems and frameworks adapt to reflect growth in funds under management and changes in the business model e.g. insourcing investments, mergers. (Consultant)*
>
> *Large and very large funds are investing substantially in cutting-edge GRC systems. There have been a number of implementation issues as systems and new processes are*

bedded down and risk professionals get more familiar with how the GRC tools work in practice. In a number of cases, there also seems to have been a gap between what some of the systems are able to deliver in practice vs. the expectations formed during the glitzy sales process. (Consultant)

In my fund, risk frameworks and systems are still being established. We were using spreadsheets to run our risk and control assessments until recently. (RP)

Many funds are still getting risk frameworks set up and are still very reliant on consultants for advice on how to do this. (RP)

The industry has a significant challenge to reduce operational costs and become more efficient. In some cases this is leading to insufficient investment in risk systems. (Ratings)

Lack of investment in proper systems is typically cost-related, highlighting the tension that may exist between risk management and an excessive cost focus. One of the challenges for risk professionals is to make the business case for investment in risk systems in an environment where capital requirements are not risk sensitive. In other words there is no benefit in terms of capital reduction for funds that invest more in risk infrastructure.

Staffing of the risk function was also considered a challenge by the experts as lack of expertise can hamper the effectiveness of the entire risk framework. Many highlighted the shortage of high calibre risk professionals in the sector, with many coming from compliance roles and failing to sufficiently adapt[7].

Many super funds are recruiting risk experts from the banking sector because risk management expertise is scarce in superannuation (Ratings, Consultant).

Having recently joined my organisation from outside the sector, I'm disappointed by the risk management systems and capabilities. There is a lack of risk professionals with sufficient skills/experience and qualifications, although this is somewhat true in all parts of the financial services industry. (RP)

Capable risk teams are not as common as they should be. People have fallen into the profession rather than choosing it. Frameworks are a dime a dozen but a capable risk team is what makes the framework actually work. (TD)

Lots of risk people in super come from compliance background and struggle when issues require judgement. (RP)

No discussion of systems and frameworks can be complete without discussion of the risk governance framework. Under SPS220 large superannuation funds are expected to have a board committee with a risk brief, although this is typically combined with audit and

[7] The differences between risk and compliance are explained more fully in Section 3.6.

compliance. It is clear that in a number of cases funds struggle to find trustee directors with suitable qualifications and experience in risk management. It should be noted that this is a challenge in many industries since risk management is a relatively young profession. As a consequence the pipeline of suitably experienced executives seeking directorships is thin. While director training programs may be of some assistance, a two-day training course is patently no substitute for a lengthy executive career on the front lines of risk management.

> *On our board risk committee the member-nominated directors lack expertise and they are too passive. It's not that they block or oppose risk initiatives – their hearts are in the right place. It's more that they don't have much to contribute to the discussion or to solving problems. (RP)*

> *Some of our directors still don't understand the three lines of defence or the difference between risk and compliance. It's easy to find directors with relevant expertise for audit/compliance but much harder for risk. We have to really push them to be forward looking and proactive. (RP)*

Another crucial issue for the risk governance framework is the status of the most senior risk executive, the Chief Risk Officer. Research suggests that the best governance outcomes are achieved when the Chief Risk Officer has direct access to the board and is also a member of the most senior executive committee (Aebi, Sabato and Schmid, 2012; Magee, Schilling and Sheedy, 2017). In some large superannuation funds the Chief Risk Officer is not on the executive committee. The direct consequence of this is that there is no risk voice in the most senior decision-making forum and the indirect consequence is that the status and authority of risk is downgraded in the organisation.

> *If you report to the CFO it's very difficult to have those honest conversations – the risk function needs to be independent of the finance function. (RP)*

> *In superannuation it's unusual for risk to have a seat at the Executive Committee. This limits the influence of risk. (RP)*

3.4.2 Commitment to continuous improvement of the risk management framework.

This is the first of the attributes associated with advanced levels of risk management maturity. A crucial aspect of a commitment to continuous improvement is the response to risk events. These are treated as an opportunity for learning and to improve the risk framework. In this context the reporting of risk events becomes crucial as the failure to report is a lost opportunity for learning/growth. Many funds are still struggling in this area as a result of structural problems with risk reporting systems. Other possible impediments to reporting of risk events are explored in Section 4.

> *We are making progress in this area but our old system made risk reporting very difficult. To report an issue you had to fill in 19 fields and investigate the cause. Unsurprisingly lots of events were missed – front line staff just didn't have sufficient time and motivation to go to this amount of trouble. The aim is to get as many events into the system as possible. (RP)*

> *I'm not convinced that all risk events/issues are being reported. Experience in my fund in the last year suggests that some important ones are being missed and picked up much later than should be the case. (TD)*

In the last year we've taken on a new system for recording risk events. This took a huge effort but we're starting to see the benefits. We're now starting to get some insightful reports from the data which will be used for root cause analysis, re-engineering processes etc. Risk management improvement is an iterative process. (RP)

Continuous improvement implies that the risk framework does not stand still but evolves over time. The risk management system should be evaluated independently and follow-up should be timely and thorough.

Many people in the industry tend to be driven by regulation rather than being intrinsically committed to risk management. (RP)

In my fund I'm delighted that new risk management initiatives generally get a very good hearing. I gather from my peers that this is not true in all funds. (RP)

Many funds don't want to invest enough in risk management. They are averse to change and very cost-conscious. (Consultant)

Too often I see funds that do the bare minimum to comply with regulations. (Consultant)

I see funds resisting a proper assessment of risk culture which might help to improve things. (Consultant)

3.4.3 Everyone has accountability for risk management.

The three lines of defence model (Kemp and Patel, 2012; Institute of Internal Auditors, 2013; APRA, 2015) is considered by many to be the state-of-the-art for risk governance. Here the business (first line of defence) must take primary responsibility for risk management. Specialist risk/compliance staff (second line of defence) are independent of the business and are expected to provide advice and training as well as objective review and challenge. Finally the third line of defence, internal audit, provides assurance that the risk management framework is operating effectively. All staff therefore play a role in risk management with the majority falling into line 1 – the first line of defence. Risk management is not just something for experts.

Almost all risk experts we interviewed highlighted the challenge of engaging first line staff in risk management.

The biggest challenge we face is keeping risk at the front of peoples' minds when they have big busy jobs. (TD)

Improving front line accountability is a significant issue for the industry (RP)

Three lines of defence is crucial for success since Line 2 can't be everywhere. However I'm not convinced that three lines of defence is really happening and that applies across the whole financial services industry, not just super. (RP)

Many line 1 staff struggle to adopt the risk mindset. It's not their natural style and they generally haven't been taught it in their business studies. (TD)

Part of the challenge is to move beyond 'mere compliance' to 'thoughtful engagement' with risk management. So what is the difference? Differences are apparent on a number of dimensions[8]. First the dimension of authorship – is the focus on regulation or laws (coming from the regulator/government) or going beyond these to consider industry best practice and member needs? Second the dimension of time – is the focus on damage control and remediation schemes (imposed by the regulator) to address past problems or is it forward-looking/pre-emptive/prescient/proactive? The third dimension is attitude – is the focus on 'ticking the boxes' to get the regulators/second line "off our back" and get on with higher priorities? Or is there a genuine desire to produce better member outcomes through improved risk management practices?

> *Around here people are focused on following existing rules rather than questioning whether they make sense. (RP)*
>
> *There's a tendency in the industry to see risk and compliance as the same thing (RP).*
>
> *The industry is so heavily regulated that it is difficult to be proactive. There is a huge amount of work to do in responding to regulators. Documentation obligations are immense. There is a lack of independent, structured thinking and good judgement. (TD)*
>
> *Risk management is not just compliance; it helps the fund to grab opportunities in a considered way (TD).*
>
> *Many funds I'm familiar with still approach risk management from a compliance perspective. This is reflected by the fact that in most funds risk does not have a voice in the most senior executive committee. This makes it difficult to influence key strategic decisions where judgement is required. (RP)*

3.4.4 Risk management viewed as an enabler.

Risk management is seen as adding value to the organisation rather than a drag on performance. Specialist risk managers are not just constraining the business but acting as trusted advisors and problem solvers. This is more likely to occur when risk specialists are experienced, have a good understanding of the business environment and are high in emotional intelligence. This attribute is closely related to 3.4.3 above where risk management is understood as being more than 'mere compliance'.

> *This is probably the toughest to achieve of all the attributes of maturity. (Reg)*
>
> *It's hard to overcome negative views of risk i.e. blocking the business v. enabling the business (RP)*

[8] We acknowledge the contribution of a particular trustee director for a thoughtful contribution in distinguishing between risk management and compliance.

In our fund the marketing staff are frustrated that risk is holding them back – risk is seen as a blocker (RP)

In many funds risk is still seen as an impediment to getting things done. The attitude could be justified as some of the risk/compliance people are excessively cautious (example cited). (Ratings)

We need more risk specialists who can really add value and are not too removed from business operations. (TD)

It's difficult to get sufficient resourcing into risk. I think that's because risk is not seen as an enabler that can help the business. (RP)

In my fund it's still a battle for risk to truly be an enabler. I aim to hire risk people who are approachable, collaborative, solutions focussed. Such people are hard to recruit from outside so we need to develop from within. (RP)

Yes risk is an enabler – you can't drive a fast car without good brakes. But often people don't see the value of risk until they've been involved in a serious risk event – a car crash. (RP)

Good risk management allows you to grab opportunities in a considered way. (TD)

3.4.5 Risk communication is effective.

This attribute implies that staff have regular and useful discussions about risk management. There should be acceptance that any good strategy or process can benefit from some questioning and scrutiny, and there are no sacred cows.

Around here there is not enough questioning/challenge (RP)

For risk maturity you need staff who are willing to push-back and challenge. (Consultant)

We're now providing more 'soft skills' training for line 2 staff to help them challenge line 1 effectively. I've received feedback that their meetings are becoming more productive rather than just information gathering exercises. (RP)

Information about risk flows easily through the organisation to the people who need it for decision-making and in a form that people can use. Risk reports are easily understood with good use of colour and diagrams.

Having good risk reporting is something I look for. (Consultant)

Lots of communication about risk from senior leaders helps to set the tone for openness throughout the organisation. (RP)

Our risk reports are getting much better, but I see value in personal chats with internal auditors and the CRO to find out what people are thinking/observing. This helps to give context to the risk metrics. (TD)

You need to keep reports non-technical otherwise you will quickly lose people. Our reports are continuously changing and this can actually help people to focus on the information. (RP)

Ideally there should be no fear of reporting risk events due to punitive responses. Senior leaders should value staff who come to them with problems early and speak frankly without sugar coating. Too often, however, there is a culture of 'Avoidance' where senior leaders appear unwilling to hear about problems and/or don't seem to accept accountability to do something to address them.

> *Both under-reporting and over-reporting can occur, but the latter is not really a bad thing if you handle it well. When we introduced a new system we got a massive uplift in the number of reported events but many were not material. This created an opportunity to communicate with staff about the kind of risk events we want to record and why. It helped staff to better understand what we're trying to achieve. (RP)*
>
> *We see discussion and learning from risk events as crucial. (Consultant)*
>
> *Staff are less likely to raise issues if leaders appear not to be listening or fail to respond appropriately. (TD)*

3.4.6 Right amount of the right risks.

Risk appetite has been set in a manner that is realistic given business strategy. It is important to note that high risk appetite can be appropriate in some areas, such as liquidity risk and investment risk for a fund with young membership. Having a high risk appetite is consistent with risk management maturity provided the risks are understood, rewards for risk-taking are acceptable and controls and mitigants are in place.

Having set risk appetite sensibly, the organisation is rarely surprised by risks that have not been identified such as emerging risks. Risks affecting the organisation should usually be within tolerances so there are few surprises. We note that some surprises are inevitable due to the nature of emerging risks and 'black swan events'[9]. A number of interviewees highlighted the difficulty of avoiding surprises in areas such as cyber-security which are evolving very rapidly.

> *Boards are trying very hard at this – I rate our efforts at around 6 or 7 out of 10. In the last 6 months we've had some meaningful discussions at board level about risk appetite in areas like product development/innovation. Previously this issue had not been well considered. To do risk appetite well you need to be very clear on your business strategy i.e. are you an innovator or more of a follower? (TD)*

[9] Prior to exploring Australia, Europeans believed all swans were white. Much as we say 'pigs will fly', they used the black swan as a way of describing something impossible. Their assumption that black swans did not exist was founded on empiricism or experience, but it turned out that they had not observed a large enough sample. On reaching Australia, Europeans discovered that black swans did indeed exist. The black swan problem in risk management refers to the possibility that a risk event will occur which is entirely unpredictable based on past experience.

When I joined my fund the risk appetite was quite unrealistic in a number of areas e.g. zero appetite for regulatory breaches. We had to make our risk appetite more consistent with the business environment where some regulatory breaches are unintentional. (RP)

More work is needed in the area of setting risk appetite; we're currently showing too many exceedances. It's an iterative process for us. (TD)

Few funds are doing appetite/tolerance reporting well (Consultant).

Proactive identification of emerging risks is challenging in many funds, and this is true in other industries as well (RP).

In my fund I'm starting to see appetite mean something and be used for decision making. For example in the last year we have refused to appoint certain fund managers without an internal audit function due to concerns about governance risk. We're doing more operational due diligence to assess the processes of vendors. (RP)

4. Employee Perceptions of Risk Management Maturity

Considering the list of attributes identified in Section 2, few[10] higher-order attributes of risk management maturity can be objectively measured; almost all are cultural and hence a matter of perception. Given that perceptions are all-important, it is likely that surveys and interviews will play a role in any assessment of risk management maturity. While interviews can be useful in some situations, they can be a costly and inefficient means of gathering information. In the context of the three lines of defence model, the perceptions of all staff are relevant and necessary for any assessment of risk culture. Surveys provide an efficient mechanism for canvassing opinion throughout a large organisation. Finally, and depending on the methods employed[11], surveys can offer anonymity which is a crucial condition for eliciting candid opinions of staff.

Staff in four large superannuation funds were surveyed anonymously between July 2017 and February 2018. Each employee was sent a link to the online survey which took around 20 minutes to complete. Response rates varied from 50% to 79% and we received a total of 1,018 responses. A different but related survey was sent to the senior leaders in each organisation (the trustee directors and the most senior executive committee). From this group we gathered 55 survey responses.

4.1 Effective Risk Structures

As noted in Section 2, establishing effective systems and frameworks is a pre-condition for risk management maturity. At Level 3, the focus is on ensuring that risk management systems are well resourced and functioning efficiently (people, IT systems, processes, reporting lines, performance/remuneration systems).

The Senior Leaders' survey allowed the research team to better understand risk governance structures. Almost unanimously, senior leaders reported favourably on the operation of the board (and the relevant risk committee), the CEO and the CRO with regard to risk governance. In two funds, however, survey results identified some concerns about the amount of time available to the board to discuss risk implications of decisions.

The survey assessed employee perceptions of the structures and frameworks relating to risk management. We used 21 survey items to create four factors or dimensions. As shown in Table 3, the outcomes varied according to the organisation. While scores for Risk Knowledge

[10] *Right Amount of the Right Risks* is one that may in future lend itself to objective measurement, provided that risk systems accurately capture losses that exceed appetite/tolerance. But it may take many years to gather sufficient data to be statistically confident that losses outside of tolerance are the result of bad management as opposed to bad luck. The effectiveness of Systems and frameworks can be reviewed by auditors/consultants but as noted in Section 2, to achieve higher levels of risk management maturity requires much more than effective systems/frameworks.

[11] Many organisations conduct 'invitational' surveys where every staff member receives a unique link to assist with the tracking of responses. Staff do not perceive such surveys to be anonymous and therefore they are unlikely to elicit candid responses.

and Risk Training were generally strong, staff ratings of Risk Managers were a little weaker. Perhaps the biggest surprise of the survey was the staff perception of performance measurement and remuneration. Here the range was from 46% to 64% favourable, suggesting that a significant proportion of staff in superannuation funds perceive that remuneration and performance measurement systems are creating a short-term focus. This is quite concerning since effective risk management relies on managing for the long-term. Regression analysis shows that less favourable scores in this category are associated with less desirable risk behaviour (non-compliance, lack of accountability, under-reporting of risk events, failure to speak up).

Table 3 Structures/Frameworks relating to Risk Management

Four Dimensions	**Proportion of Favourable* Factor Scores in Superannuation Funds**			
	Fund A	Fund B	Fund C	Fund D
Performance and Remuneration: Perceptions that performance measurement and reward systems encourage a focus on risk management. e.g. 'Remunerations systems encourage employees to focus on short-term rewards' (Reversed)	64%	46%	58%	52%
Risk Managers: Perceptions of the efficacy of those staff with additional risk responsibilities. e.g. 'The risk managers have been integral to our business unit's performance'	93%	76%	87%	88%
Risk Knowledge: Perceptions of the risk management knowledge and expertise within the organisation. e.g. 'My colleagues have sufficient knowledge about risk to perform their jobs well.'	96%	96%	96%	95%
Risk Training: Perceptions of the quality and applicability of staff training relating to risk. e.g. 'Our risk training program is effective.'	97%	88%	95%	96%

**We define favourable in this context as a factor score of 4 or greater. Factor scores are the average of individual item scores in that category (using a six-point scale where negatively worded items have been reversed where appropriate).*

In the funds we have assessed, some or all staff are eligible for a variable short-term reward program. Typically such staff are assessed across a range of measures; a balanced scorecard is used to determine the reward. For example, the scorecard might include manager ratings of risk and compliance behaviour. While balanced scorecard systems are commonly used in the financial services sector to determine variable rewards, there is currently no clear research evidence to support this. It is possible that staff focus on the more objective financial measures rather than those with a subjective element. Such programs also suffer from the fact

that compliance is never perfectly monitored. In other words, violations of policy often go undetected. In the four organisations we assessed there appeared to be no system for deferral and clawback of bonuses, other than in relation to Investments staff in one organisation.

4.2 Risk Culture

The Macquarie University Risk Culture Scale (MURCS) is a four-factor survey instrument developed for assessing risk culture in financial institutions and has been validated for use in superannuation funds (Sheedy and Jepsen, 2018). It consists of 18 survey items.

In our model, the higher maturity Levels 1 and 2 are linked to cultural attributes. We hypothesise that the MURCS should capture certain aspects of risk management maturity. Table 4 maps the maturity attributes of Section 2 with the risk culture factors under the MURCS. This mapping is based on an assessment of face validity by the research team. The mapping suggests a considerable degree of prima facie overlap between the two constructs.

Table 4 Mapping Maturity Attributes to Risk Culture

Risk Management Maturity (Higher order attributes)	Related Risk Culture Factor(s)
Commitment to continuous improvement	Proactive e.g. 'For us, analysing risk events (including a near miss) is very useful'
Everyone has accountability	Proactive e.g. 'Staff are encouraged to identify potential risks' Manager e.g. 'When it comes to managing risk, my manager is an excellent role model of desirable behaviour
Risk management viewed as an enabler	Valued e.g. 'The value of risk management has been embraced throughout the organisation'
Right amount of the right risks	Not Applicable
Risk communication is effective	(lack of) Avoidance e.g. 'Senior leaders don't want to hear bad news'

Table 5 presents the organisation-wide factor scores reported in the four employee surveys conducted to date. The fact that many scores are over 90% favourable suggests, prima facie, that all four funds have made significant progress in implementing a risk culture. In the cases indicated with asterisks, the culture scores are significantly higher than the average scores achieved by large banks in Australia and Canada in the previous research project (Sheedy and Griffin, 2017). While superannuation funds introduced formal risk management programs

later than banks, they have the advantage of smaller staff numbers[12]. This may simplify the task of inculcating risk culture.

Table 5 Risk Culture Scores on Four Dimensions

Four Components of Risk Culture	Proportion of Favourable[#] Factor Scores in Superannuation Funds			
	Fund A	Fund B	Fund C	Fund D
Avoidance: Risk issues and policy breaches are ignored, downplayed or excused.	83%**	67%*	78%**	79%**
Proactive: Risk issues and events are proactively identified and addressed	93%*	80%	91%*	91%**
Valued: Risk management is valued within the organisation	94%**	79%	91%**	92%**
Manager: immediate manager is an effective role model for desirable risk management behaviours.	97%*	90%	96%*	96%**

[#]We define favourable in this context as a score of 4 or greater (using a six-point scale and where negatively worded items have been reversed where appropriate).
* Indicates the fund's score is statistically significantly higher than the benchmark of large banks in Australia from the 2014-15 bank study.
** Indicates the fund's score is statistically significantly higher than the benchmarks of large banks in both Australia and Canada from the 2014-15 bank study.

Staff ratings for Manager were the most favourable, suggesting that managers in these large superannuation funds are perceived as effective role models for desirable risk management behaviour.

While Manager scores were statistically similar across the four funds, we observed greater variation across other culture dimensions, especially Valued and Avoidance. This confirms our finding from the interview study that large superannuation funds are not homogeneous with regard to risk management maturity.

[12] Large Australian and Canadian banks have staff numbers in excess of 30,000 whereas the superannuation funds we have assessed all have staff numbers below 1,000.

The least favourable ratings were recorded on the Avoidance dimension, with scores ranging from 67% to 83% favourable across the four organisations. This suggests that more work is needed in the funds focusing on: leadership openness to receiving negative messages, responses to questions about risk, responses to breaches of policy (especially by top performers), and clarity regarding the acceptable level of risk to achieve fund objectives. Our regression analysis has shown that of the four factors, Avoidance culture is the most significantly associated with undesirable risk behaviour such as failure to report risk events, failure to speak up, lack of accountability, overconfidence and unethical treatment of members.

Within three of the four organisations we observed risk culture variation at the business unit level. We coded business units into six categories: administration, financial planning, investments, risk/compliance, technology, and other. In all three the technology teams had risk culture scores significantly below the firm norm. In one organisation the administration team scored significantly lower than the form norm. Investment teams were generally similar to the firm norm but significantly exceeded the firm norm in one organisation.

4.3 Risk Management Maturity

To build understanding of risk management maturity we developed a set of new survey items designed around attributes of the maturity model. The focus here is on issues that may not have been thoroughly canvassed by the MURCS. The new items, based on Section 2 of this paper, are shown in Table 6.

Question 1 highlights the fact that accountability for risk management is confusing for many staff. In one fund only 62% of staff perceived the accountability between business and risk/compliance teams to be clear. More encouragingly, in another fund 83% of staff perceived the accountability to be clear, although even this leaves room for improvement.

Question 6 picks up a similar issue relating to risk accountability. Under the three lines of defence model, risk management is the responsibility of business operations with risk/compliance specialists playing an advisory and oversight role. In the funds we have assessed so far, many staff are still relying on risk/compliance specialists to take primary responsibility for risk. In one fund only 47% of staff agreed that business operations are primarily responsible.

Question 2 captures a different aspect of accountability i.e. the extent to which staff are thoughtfully engaged in risk management as opposed to merely meeting the minimum requirements. We have so far observed scores in the range from 61% favourable to 80% favourable.

Overall we can say that on the attribute of accountability, there is considerable variation across the large superannuation funds. Even in the best case significant room for improvement exists. A similar picture emerges in relation to the other maturity-related survey items.

Table 6: New Survey Items Tested for Risk Management Maturity

	Unfavourable response	Favourable response	Proportion of Staff Responding Favourably in the Organisation			
			Fund A	Fund B	Fund C	Fund D
1. Lines of accountability between the business and risk/compliance teams are:	Confusing…	...Very Clear	81%	62%	76%	83%
2. Risk management in this organisation is characterised by:	Mere compliance …	...Thoughtful engagement	80%	61%	73%	76%
3. Risk management in this organisation is:	Ineffective …	...Very effective	93%	79%	91%	93%
4. Risk management in this organisation:	Meets regulatory requirements and no more…	…Is embraced as the best way to do business	87%	68%	81%	87%
5. Except for risk specialists, staff tend to see risk management as:	A drag on performance…	…An enabler for success	80%	64%	63%	74%
6. Risk management in this organisation is seen as the primary responsibility of:	Risk/Compliance …	...Business operations.	47%	51%	50%	63%
7. In the last year we have been surprised by significant unforeseen outcomes:	Regularly…	...Never	97%	70%	65%	74%

Items are presented on a six-point scale between two opposite poles. In every case a 'Don't Know' option is provided.

The maturity literature highlights the fact that reporting of risk events and addressing them productively is a useful indicator of maturity. Mature organisations value the reporting of risk events because it enables them to accurately track their risk management performance and continually improve. While the large superannuation funds participating in the study all have systems for recording risk events, there remains a possibility that risk events may be under-reported. This would clearly limit the ability of the organisation to learn. We therefore designed two new items to explore the extent to which risk events are being reported, the possible reasons for lack of reporting, and the types of risk events least likely to be reported.

Table 7: Reasons for Under-reporting Risk Events

Sometimes I skip reporting a risk event because:	(Tick any that apply) • I don't want to go through the follow-up interviews and questions • Risk managers lack the expertise to understand/address the issue • I doubt that anything will be done to fix the problem • Work pressure • Our risk system is so cumbersome • I assume somebody else will probably log it • I prefer to focus on solving the issue itself • It might reflect poorly on our business • Reporting might hurt our chances of getting rewards or recognition • The event is not material • I don't know how to report a risk event • I don't think it's part of my role • Other (please explain) • **None of the above, if I was aware of a risk event I would always ensure it had been reported.**

The items are designed to overcome social desirability bias by providing possible justifications for failing to report. By focussing on the justification, we indirectly address the issue of under-reporting. The second item implicitly suggests that some events are more likely than others to be reported, thus also helping to overcome this bias. Both items address the attributes: Commitment to Continuous Improvement and Risk Communication is Effective.

In Table 7 the desirable answer is the last: 'None of the above, if I was aware of a risk event I would always ensure it had been reported.' In the organisations we have surveyed to date we have observed between 65% and 89% of staff selecting this response, suggesting that all have some room to improve. The proportion of respondents admitting to under-reporting are as follows: Fund A (20%); Fund B (35%); Fund C (17%); Fund D (11%)

The popularity of reasons for not reporting varied by organisation. 'I don't know how to report a risk event' was among the top five most important reasons in all four organisations with between 2.9% and 14.5% of staff citing this reason. 'Work pressure' was also a common reason for not reporting, with between 2.2% and 10.2% selecting it.

Table 8: Which Events Are Reported?

How likely is it that the following would be captured in your risk reporting system? ***Slider from Highly Unlikely to Highly Likely (6 point scale)'Don't Know' option included***	**Proportion of Responses in the Organisation who think the event likely to be reported.**
A breakdown in a procedure impacting 30% of members.	80% - 95%
A breakdown in a procedure with no member impact.	56% - 85%
A delay in issuing mandatory member communications beyond legislative timeframes.	74% - 83%
Member complaint resulting in adverse media coverage.	80% - 88%
A delay in project implementation.	80% - 77%
A delay in project implementation caused by failure in the oversight of a third party.	75% - 79%
Miscalculation of a component of a unit price which was identified and rectified prior to any transactions being processed.	69% - 83%
Fraudulent transaction request declined as a result of final approval process.	80% - 91%
Fraudulent death certificate provided by customer as part of claim.	70% - 90%
Customer complaint on social media	70% - 71%
Wrong information sent to one member	69% - 85%
System outage affecting non-customer facing systems	66% - 81%
Staff member accessing member information with no obvious business reason	53% - 66%

5. Limitations of the Study

Like all research, this project has known limitations, including:

1. The four funds assessed to date may not be typical of all large superannuation funds. We have attempted to ameliorate this problem by complementing the survey analysis with an interview study that captures a wider sample of large funds. This suggests that the funds in our sample are typical.
2. The surveys rely on 'reflective self-report' by staff members. Although unlikely to be deliberately distorted, the responses may not truly represent respondents' actual perceptions and behaviour. This risk is addressed, in part, by the review of relevant documents and through interviews. Additional data collection is planned for 2018 to further triangulate or support the results.
3. Social desirability response bias may also influence survey responses. We have used an impression management scale (Hart, et. al., 2015) to control for this. We found that the risk culture scale, risk management maturity items and items related to reporting of risk events are *not significantly prone* to this bias.
4. Causality should not be implied by these cross-sectional results from one point in time. Repeat assessment may allow causality (say between culture and behaviour) to be implied.
5. Despite adequate response rates, interpretation of these results should proceed with some caution. We have not conducted a non-responses analysis to determine whether the results are biased by attracting respondents who favoured particular responses.

About the Researchers

Associate Professor Elizabeth Sheedy PhD

- Financial risk specialist based at the Department of Applied Finance, Faculty of Business and Economics, Macquarie University.
- Expertise in market risk, enterprise risk management, risk culture and governance
- Has assessed risk culture in 12 financial institutions in Australia, Canada and the UK.
- Finance industry experience with Macquarie Bank, Westpac.
- Editor/Author The Professional Risk Managers' Handbook
- Active in professional associations (PRMIA, RMA)
- Scholarly publications in financial risk management

Associate Professor Denise Jepsen, MOrgPsych, PHCertHE, PhD, FAHRI, MAPS

- Registered psychologist with organizational endorsement based in the Department of Management, Faculty of Business and Economics, Macquarie University
- Teaching undergraduate and postgraduate organizational behavior, human resource management, research methods and design
- Active researcher in evidence-based management, employee attitudes towards workplace, colleagues and workplace relationships, and careers
- Former licensed stockbroker, management consultant
- Former commercial director, employee surveying consultancy
- Ten years elected councilor, Australian Human Resources Institute
- Skills in survey design and construction, project management, data collection, qualitative and quantitative analysis (correlation, regression, structural equation modelling), corporate and feedback reporting.

References

Aebi, V., Sabato, G. and Schmid, M., 2012. Risk management, corporate governance, and bank performance in the financial crisis. *Journal of Banking & Finance*, *36*(12), pp.3213-3226.

APRA (2009) Discussion Paper: Enhancements to the Basel II Framework in Australia. http://www.apra.gov.au/adi/Documents/Discussion-paper-Enhancements-to-Basel-II-Framework-in-Australia-Dec-2009.pdf

APRA (2012) SPS 231 Outsourcing http://www.apra.gov.au/Super/PrudentialFramework/Documents/Final-SPS-231-Outsourcing-November-2012.pdf

APRA (2012a) SPS 232 Business continuity management http://www.apra.gov.au/Super/PrudentialFramework/Documents/Final-SPS-232-BCM-November-2012.pdf

APRA (2013) Prudential Standard SPS 220 Risk Management July 2013 http://www.apra.gov.au/super/prudentialframework/documents/final-sps-220-risk-management-july-2013.pdf

APRA (2013a) Prudential Practice Guide SPG 220 Risk Management July 2013 http://www.apra.gov.au/Super/PrudentialFramework/Documents/Prudential-Practice-Guide-SPG-220-Risk-Management-July-2013.pdf

APRA (2015) Prudential Practice Guide CPG 220 Risk Management January 2015 http://www.apra.gov.au/CrossIndustry/Documents/Prudential-Practice-Guide-CPG-220-Risk-Management-January-2015.pdf

APRA (2016) Information Paper: Risk Culture October 2016 http://www.apra.gov.au/CrossIndustry/Documents/161018-Information-Paper-Risk-Culture.pdf

APRA (2017) APRA's Regulator Radar. A speech made by Helen Rowell to the Conference of Major Superannuation Funds. http://www.apra.gov.au/Speeches/Pages/APRA's-regulatory-radar.aspx

APRA (2017a) Assessing Quality Member Outcomes in the Superannuation Industry. Letter to RSE Licensees. http://www.apra.gov.au/Super/Publications/Documents/Letter_to_RSE_Licensees_assessing_member_outcomes_in_the_superannuation_industry.pdf

APRA (2017b) Annual Fund Level Superannuation Statistics http://www.apra.gov.au/Super/Publications/Pages/superannuation-fund-level-publications.aspx

ASFA (2017) The Australian Superannuation Industry March 2017 file:///D:/Users-Data/mq93500475/Downloads/1703_The_Australian_superannuation_industry%20(2).PDF

ASIC (2017) Regulatory Guide 259 Risk Management Systems of Responsible Entities. March 2017 http://asic.gov.au/regulatory-resources/find-a-document/regulatory-guides/rg-259-risk-management-systems-of-responsible-entities/

ASIC (2017a) Report 529 Member Experience of Superannuation. http://asic.gov.au/regulatory-resources/find-a-document/reports/rep-529-member-experience-of-superannuation/

ASIC (2018) REP 562 Financial advice: Vertically integrated institutions and conflicts of interest. http://asic.gov.au/regulatory-resources/find-a-document/reports/rep-562-financial-advice-vertically-integrated-institutions-and-conflicts-of-interest/

Chartered Secretaries of Australia, 2010. Governance and risk management maturity: indicators and performance

Commonwealth of Australia (2013). Review of the Trio Capital Fraud and Assessment of the Regulatory Framework. https://treasury.gov.au/publication/review-of-the-trio-capital-fraud-and-assessment-of-the-regulatory-framework/

Economist Intelligence Unit (2010) Rebuilding Trust: Next Steps for Risk Management in Financial Services http://graphics.eiu.com/upload/eb/SAS_2010_Rebuilding_trust_WEB.pdf

Farrell, M., & Gallagher, R. (2015). The valuation implications of enterprise risk management maturity. *Journal of Risk and Insurance*, *82*(3), 625-657.

Financial Services Council (2017) Millenials Engagement with Superannuation https://www.fsc.org.au/_entity/annotation/c3740ca0-a471-e711-810a-c4346bc5779c

Financial Stability Board (2014). Guidance on Supervisory Interaction with Financial Institutions on Risk Culture: A Framework for Assessing Risk Culture. April 2014 http://www.fsb.org/wp-content/uploads/140407.pdf

Gallagher, D.R., Gapes, T.M. and Warren, G.J., 2016. In-house asset management in the Australian superannuation industry. *Accounting & Finance*.

Gribble and Hellenius (2011). Managing Liquidity Risk in Superannuation. Presented to the Institute of Actuaries in Australia https://www.actuaries.asn.au/library/events/Conventions/2011/ManagingLiquidity-Paper.pdf

Hart, C. M., Ritchie, T. D., Hepper, E. G., & Gebauer, J. E. (2015). The balanced inventory of desirable responding short form (BIDR-16). *Sage Open*, *5*(4), 2158244015621113.

Hillson, D. 'Towards a Risk Maturity Model' **The International Journal of Project & Business Risk Management** 1(1): 35-45

Hudson, P. 'Safety Management and Safety Culture The Long, Hard and Winding Road' Occupational Health & Safety Management Systems Proceedings of the First National Conference p. 21

Institute of Internal Auditors 2013. The Three Lines of Defense in Effective Risk Management and Control. https://www.iia.org.au/sf_docs/default-source/member-services/thethreelinesofDefenseineffectiveriskmanagementandcontrol_Position_Paper_Jan_2013.pdf?sfvrsn=0

Institute of Internal Auditors, 2013. ERM Program Audit Guide: RIMS Risk Maturity Model & Authors of the RIMS Risk Maturity Model Assessing the Adequacy and Effectiveness of Risk Management

ISO 31000, 2009. Risk Management. See especially Annex A

ISO 31000 (2018) Risk Management Guidelines 2nd edition, www.iso.org

Kemp, M. H. D., & Patel, C. C. (2012). Entity-wide risk management for pension funds. *British Actuarial Journal*, *17*(2), 331-394.

KPMG (2017) Superannuation Insights 2017. https://home.kpmg.com/au/en/home/insights/2017/06/superannuation-insights-2017.html

Macgillivray, Sharp, Strutt, Hamilton and Pollard, 2007, Benchmarking Risk Management Within the International Water Utility Sector. Part I: Design of a Capability Maturity Methodology. **Journal of Risk Research** Vol. 10, No. 1, 85–104

Magee, S., Schilling, C. and Sheedy, E., 2017. RISK GOVERNANCE IN THE INSURANCE SECTOR—DETERMINANTS AND CONSEQUENCES IN AN INTERNATIONAL SAMPLE. *Journal of Risk and Insurance*.

Parker, D., Lawrie, M. and Hudson, P., 2006. A framework for understanding the development of organisational safety culture. **Safety science**, *44*(6), pp.551-562.

PWC (2015). Operational Risk: The end of internal modelling? https://www.pwc.com/gx/en/financial-services/pdf/fs-operational-risk-modelling.pdf

PWC (2017). Risk and Compliance Benchmarking Survey www.pwc.com.au

RBA (2009). Financial Stability Review. March 2009. http://www.rba.gov.au/publications/fsr/2009/mar/aus-fin-sys.html

Rice Warner (2017) Why we need super fund mergers. http://www.ricewarner.com/why-we-need-super-fund-mergers/

Rice Warner (2017a) The role of insurance in superannuation. http://www.ricewarner.com/the-role-of-insurance-in-superannuation/

Reason, J., 1997. Managing the Risks of Organisational Accidents. Ashgate, Aldershot.

Royal Commission into Trade Union Governance and Corruption, 2015. Final Report (Volume 7), December 2015 https://www.tradeunionroyalcommission.gov.au/reports/Pages/Volume-5.aspx

Sheedy, Elizabeth, and Barbara Griffin (2017). "Risk governance, structures, culture, and behavior: A view from the inside." *Corporate Governance: An International Review*. http://onlinelibrary.wiley.com/doi/10.1111/corg.12200/full

Sheedy, Elizabeth A., Barbara Griffin, and Jennifer P. Barbour (2017). "A framework and measure for examining risk climate in financial institutions." *Journal of Business and Psychology* 32.1 101-116. https://link.springer.com/article/10.1007/s10869-015-9424-7

Sheedy, Elizabeth A. and Jepsen, Denise, How to Measure Risk Culture in Australian Superannuation Funds (January 1, 2018). Macquarie University Faculty of Business & Economics Research Paper. Available at SSRN: https://ssrn.com/abstract=3128693

Westrum, R., 1996. Human factors experts beginning to focus on organizational factors in safety. *ICAO journal*, *51*(8), pp.6-8.