IT RISK MANAGEMENT
DRIVERS, CHALLENGES AND ENABLERS FOR AUSTRALIAN ORGANISATIONS

Paras Shah
David Roche
Anthony Rodrigues
Paras Shah
Principal Author and the Whitepaper Project Manager

Paras Shah is Founder and Principal Consultant at Vital Interacts, a professional services firm focused on offering IT Governance, Risk Management, Information Security and Business Process Improvement services.

Paras has over fourteen years’ experience in business and technology. Paras started his career as a Chartered Accountant and ventured into the field of Information Technology as Auditor in 2001. Thereafter pursued a blend of consulting, audit, advisory, business development and training roles.

Paras is a Certified Trainer and Certification Assessor for Management Systems Certifications including ISO27001, ISO20000, and ISO9001. He has trained over 250 IT and Security professionals for IT Certification Trainings across Australia, Asia South, Middle East and India. Paras is also CISA, CGEIT and CRISC certified.

Some of his recent involvements include:
- ISACA Framework Committee Member (2012-2013).
- Member of Standards Australia’s Quality Management Committee ‘QR-008’.

Contact: +61 420 978 258 | paras@vitalinteracts.com.au

David Roche
Co-author and ISACA Sydney Chapter President

David is an independent consultant at Governance Architects, specialising in strategy, business architecture, investment prioritisation and IT governance. Over 22 years, he has solved business problems and delivered value to corporate strategy, portfolio management, IT and risk management functions. His clients include Australian and NZ banks, wealth managers, government and not-for-profit organisations.

His risk management experience includes risk profiling, key risk indicators, assessing organisational risk culture and the capability of enterprise risk management.

David is also President of ISACA Sydney Chapter. He developed the business strategy and in his spare time, leads its execution. Twice a year he trains ISACA members on IT governance practices in preparation for doing ISACA’s IT Governance certification exam CGEIT. David is CRISC certified and has passed ISACA’s CISM and CGEIT certification exams.

Contact: +61 488 221 888 | david@govern.net.au

Anthony Rodrigues
Co-author and ISACA Melbourne Chapter Director

Anthony has over 20 years’ experience in the banking and finance industry having worked for Bank of America in his last role as Vice President specialising in Internal Audit, Operational Risk, IT Security SOX Compliance and has had wide ranging responsibilities for Risk Management across 13 countries in the Asia & Australia region.

Anthony currently works at LUCRF Super, Australia’s first industry fund, as an Internal Auditor. Prior to joining LUCRF Super, he has worked with NAB, ANZ and KPMG.

Anthony’s professional certifications include CISM, CRISC, Certified Fraud Examiner (CFE) and Provisional ISMS & QMS Auditor.

Anthony is also Certifications Director of ISACA Melbourne Chapter.

Contact: +61 434 527 708 | anthony.rodrigues@isaca-melbourne.org
Contents

About this Whitepaper 2
Executive summary 3
Key findings 4
Participant profile 6
Main Drivers 7
Key Challenges 8
Enablers
  • Strategic 9
  • Architecture 11
  • Delivery and Value 13
How ISACA can help 14
Acknowledgements 16

Reservation of Rights

© 2013, ISACA Sydney Chapter and ISACA Melbourne Chapter. All rights reserved.

No part of this publication may be used, copied, reproduced, modified, distributed, displayed, stored in a retrieval system or transmitted in any form by any means (electronic, mechanical, photocopying, recording or otherwise) without the prior written authorisation of ISACA. Reproduction and use of all or portions of this publication are permitted solely for academic, internal and non-commercial use and for consulting/advisory engagements, and must include full attribution of the material’s source. No other right or permission is granted with respect to this work.

Disclaimer

This publication has been written in general terms and therefore cannot be relied on to cover specific situations; application of the principles set out will depend upon the particular circumstances involved and we recommend that you obtain professional advice before acting or refraining from acting on any of the contents of this publication. ISACA accepts no duty of care or liability for any loss occasioned to any person acting or refraining from action as a result of any material in this publication.
Purpose
ISACA Sydney Chapter and ISACA Melbourne Chapter initiated a joint project to prepare this whitepaper to:

- understand IT risk management drivers and challenges faced by Australian organisations;
- describe enablers of IT risk management;
- provide awareness of ISACA frameworks, such as COBIT 5, Risk IT and Val IT; and
- assess the recognition of ISACA’s IT risk management (CRISC) and IT governance (CGEIT) certifications, that support individuals and their employers to govern and manage IT risks.

Readers will be interested in this whitepaper if they are looking to improve their organisation’s ability to proactively identify, assess and manage IT risks to an acceptable level.

Please note that this whitepaper does not intend to cover:

- the maturity of IT risk management activities performed by Australian organisations; or
- identification or ranking of operational IT risks, such as Cloud risk, BYOD risk, Service Desk risk or key IT personnel risk.

Approach taken
The information used in the development of this whitepaper was gathered at the end of 2012 using a survey questionnaire followed by a set of structured interviews with industry practitioners.

At each stage in this project, the approach and results were reviewed by seven expert reviewers. The expert reviewers are all senior IT risk practitioners (Heads of IT risk or similar).

IT risks
The definition of ‘IT Risk’ becomes important at this stage. There is a common misperception in the industry that IT risks only include security-related IT risks.

ISACA’s Risk IT Framework defines IT Risk as

“the business risk associated with the use, ownership, operation, involvement, influence and adoption of IT within an enterprise”

The Risk IT Framework covers all IT-related risks, including:

- Not achieving enough value from IT
- Late project delivery
- Compliance issues
- Misalignment with business objectives
- Obsolete or inflexible IT architecture
- IT service delivery problems
- IT skills shortage

The Whitepaper development team has leveraged ISACA’s Risk IT Framework, Principles and definitions throughout the project. (more details about the Framework on page 16).
To attain strategic, program and operational objectives, most organisations rely on the right IT services to be delivered at the right time. This is only possible if IT risks have been identified and mitigated to an acceptable level.

This whitepaper has been written to help organisations protect, enable and optimise their value chain, through an effective IT risk management capability. This document identifies the key drivers and challenges of IT risk management. It also outlines what enablers are available to solve these challenges.

In late 2012, an ISACA-led survey was taken across Australia by 111 business and IT professionals. Structured interviews were then conducted with senior executives and IT risk practitioners to validate the findings.

Based on this data, we recommend organisations assess the status of their IT risk management capability.

To address the above questions, readers can refer to ISACA’s COBIT 5 and Risk IT Frameworks, which articulate critical components in the form of enablers.

We hope you enjoy your read, and welcome all comments and questions to: paras@vitalinteracts.com.au
Business drivers for IT risk management

When asked to select three main drivers for organisations to manage IT risks, “External compliance requirement” topped the chart scoring more than 65%. “Enabling business value and achievement of objectives” topped the rank for non-Banking and Financial Services organisations and ranked third overall.

The majority of Australian organisations have a fair way to go before leveraging their IT risk management function to “Optimise business value (~15%)”

IT risk management activities are generally perceived by business stakeholders either as a compliance burden, whether external and/or internal (~89%), or an IT overhead cost (e.g. more than 23% participants identified “Major IT-related failure event,” as one of the main drivers.)

IT risk management activities not viewed as contributing to business value creation

There was consistent opinion across industry responses, as IT risk practitioners expressed, that IT executives were not effective in communicating the role of IT risk management as a critical decision support tool for organisations to enable and optimise business value.

Board and Senior Executives’ awareness about the governance of IT risk, as well as their appetite to invest in IT risk management activities ranked third among the potential improvement opportunities.

Lack of commitment from senior management is one of the main challenges faced by non- Banking and Financial Services organisations.

Siloed approach to Enterprise and IT risk management

The organisations with an effective risk culture and tone at the top tend to have better alignment with the enterprise risk management framework as well as dedicated IT risk management function.

More than half of the participants believed that one of the top three challenges of Australian organisations today was that there was a “Siloed approach to risk management,” i.e. IT risk framework is inconsistent or separated from their enterprise risk management (ERM) framework.

This observation was further supported in the survey results as the majority of participants selected IT risk management and enterprise risk management (ERM) alignment and integration as their most important improvement initiative.
A view that the Security team is managing IT Risks

For a large number of Australian organisations (~40%), there is a belief that ‘the Security team is managing IT Risk.’

Over 26% of participants stated that their IT risk management programs focused too much on IT security risks rather than considering all IT-related risks.

We found that Information Security Functions (~30%) were most likely to have responsibility for developing IT risk management processes. This probability rises to 38% for non-Banking and Financial Services organisations.

Improvement opportunities

Practitioners stated that in order for IT risk management to be successful, it was imperative to drive the awareness and need of IT risk management across business and IT.

Extending IT risk management program beyond its traditional focus and ensuring that it is effectively integrated into the organisation’s business and enterprise risk management processes emerge as the highest priority improvement opportunities for survey respondents.

‘Developing and implementing an IT risk management framework’ ranked second overall and was on top for non-Banking and Financial Services organisations.

Many of small (250-1000) to medium (1001-5000) sized Banking and Financial Services organisations have preferred ISO/IEC 27001 or 27005 (Information Security Management standard) over ISO/IEC 31000 (Risk management standard, previously AS/NZS 4360).

Most organisations are using informal and reactive initiatives to improve their IT risk management capabilities.
For the survey, the participants were asked to identify themselves either as ‘Practitioner’ or ‘Consultant.’ Their inputs were captured using two separate sections in the survey.

**Participant by risk management role**
The survey meets its objective of achieving a balanced view from practitioners as they represented IT, Audit, Security, Risk, Compliance and Governance team across industry sectors.

Please note that senior and executive practitioners are not categorised separately, e.g. Head of IT or CIO are included as ‘IT team members’.

<table>
<thead>
<tr>
<th>Role</th>
<th>%</th>
</tr>
</thead>
<tbody>
<tr>
<td>IT team member</td>
<td>19%</td>
</tr>
<tr>
<td>Audit team member</td>
<td>14%</td>
</tr>
<tr>
<td>IT Security team member</td>
<td>14%</td>
</tr>
<tr>
<td>Risk or IT risk team member</td>
<td>10%</td>
</tr>
<tr>
<td>Compliance team member</td>
<td>5%</td>
</tr>
<tr>
<td>Risk and Security team member</td>
<td>4%</td>
</tr>
<tr>
<td>Governance team member</td>
<td>3%</td>
</tr>
<tr>
<td>Others</td>
<td>4%</td>
</tr>
<tr>
<td>Consultants</td>
<td>28%</td>
</tr>
</tbody>
</table>

**Participant by sector and organisation size**
With sizable representation from ‘Banking and Financial Services,’ ‘Energy and utilities’ and ‘Government and Defence’ sectors in our survey, we have provided industry specific information and insights wherever possible in this Whitepaper.
Compliance remains a significant priority for IT risk management functions and organisations more widely. This holds true whether requirements are forced by external regulatory bodies or internal policies. Enabling and protecting business value are key drivers which may lead to organisational acceptance and future growth of IT risk management practices.

Before Australian organisations can optimise business value from their investment in IT, practitioners believe that senior management need to change their strategic thinking to evolve and mature the IT risk management function.

**Protecting business value**

This driver ranks first for ‘Government & Defence’ and in ‘Energy & Utilities’ organisations due to the nature of their organisational objectives.

It was interesting to notice that ‘other commercial organisations’ preferred ‘Protection’ over ‘Enablement’ of business value as the main driver for IT risk management.

**Optimising business value**

Leadership commitment and increased awareness were identified by practitioners as potential improvement opportunities.

Organisations in Australia have remained sluggish to change their strategic thinking and have not leveraged their IT risk management function to play an instrumental role in optimising business value.

**Complying with external and internal requirements**

Compliance may be an easier sell for the IT risk management function as the consequence of non-compliance is high in the form of fines, reputational damage and potential loss of market share.

Even though ‘other commercial organisations’ would benefit more by leveraging IT risk management to ‘Enable’ or ‘Optimise’ business value, neither of these have appeared in their top three drivers.

For Banking and Financial Services organisations, the level of regulation and supervisory requirements has resulted in compliance requirements overshadowing ‘Protection’ and ‘Optimisation’ drivers for IT risk management.
A key challenge facing IT risk professionals in Australia is to establish and reinforce IT risk management as a business enabler to the Board and senior executives. The majority of participants (71%) stated that IT risk management was not viewed as a value-add activity. A potential cause for this challenge, may be too much focus on IT security risk rather than all IT related risks.

Although, external compliance is considered the main driver for IT risk management, it is a double-edged sword. On the one hand, it’s potentially an easier sell for the IT risk management function. However, on the other hand, senior executives may view IT risk management as a compliance burden rather than a value-add activity to optimise business value.

**IT risk management not viewed as adding value**

That survey participants in both ‘Banking and Financial Services’ and in ‘Energy & Utilities’ organisations selecting this as the most important challenge is unusual.

One might assume that business benefits of a well implemented IT risk management program would already be well understood by organisations in these sectors. Apparently this is not the case.

**Immature IT risk management activities**

Immature IT risk management activities also ranked in the top-3 list for both ‘Banking and Financial Services’ as well as ‘Energy & Utilities’ sector organisations.

The interviewees highlighted insufficient coverage of IT risk specific activities in the ERM framework as one of the potential causes.

<table>
<thead>
<tr>
<th>Key challenges</th>
<th>Banking and Financial Services</th>
<th>Government and Defence</th>
<th>Energy &amp; Utilities</th>
<th>Other commercial organisations</th>
<th>Consulting</th>
</tr>
</thead>
<tbody>
<tr>
<td>IT risk management activities not viewed as adding value to meeting business objectives</td>
<td>1</td>
<td>3</td>
<td>1</td>
<td>1</td>
<td>3</td>
</tr>
<tr>
<td>Siloed approach to risk management</td>
<td>2</td>
<td>2</td>
<td>3</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>(IT risk is siloed from enterprise risk management)</td>
<td>3</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td></td>
</tr>
<tr>
<td>Too much focus on IT security risks rather than all IT-related risks</td>
<td>1</td>
<td></td>
<td>3</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Lack of commitment from senior management</td>
<td></td>
<td></td>
<td>3</td>
<td></td>
<td></td>
</tr>
<tr>
<td>A view that the IT team is accountable for IT risk management</td>
<td>3</td>
<td></td>
<td>3</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Siloed approach to risk management**

The existence of siloed risk functions is not uncommon for large organisations, such as large banking or financial services institutions, where the role of IT, centralised risk functions and divisional risk functions may be segregated.

Nevertheless, the majority of survey participants as well as interviewees identified better integration and alignment of Enterprise and IT risk management activities as an important improvement opportunity.

**A view that the Security team is covering IT Risk**

This appears to be a major challenge and one that needs to be addressed by raising business and IT awareness.

This applies to those organisations, especially within the Government sector (~75%), that focus too much on IT security risks rather than all IT-related risks.
Strategic enablers: “Are we doing the right things?”

The success of all programs and projects are reliant on genuine support and sponsorship of the Board and senior management. IT risk management is no exception. We examined the following areas to determine the level of “Leadership commitment” to validate the premise “Are we doing the right things?”

- What is the organisation’s risk culture and tone at the top to manage IT related risks to an acceptable level?
- Has the organisation integrated Enterprise and IT risk management frameworks?
- Is the structure and size of the IT risk management function adequate to attain organisational objectives?

**Organisation’s risk culture and tone at the top**

The Risk IT Framework defines ‘Risk culture’ as the set of shared values and beliefs that governs attitudes towards risk-taking, care and integrity, and determines how openly risks and losses are reported and discussed.

Participant responses indicated that a third of the organisations represented have an effective or very effective risk culture. However, the room for improvement is significant with over 64% participants believed that risk culture at their organisation was either moderately effective or not effective.

The organisations with an effective risk culture and tone at the top tend to have better alignment with the enterprise risk management framework as well as a dedicated IT risk management function.

<table>
<thead>
<tr>
<th>Organisation’s risk culture and tone at the top</th>
<th>Banking and Financial Services</th>
<th>Government and Defence</th>
<th>Energy &amp; Utilities</th>
<th>Other commercial organisations</th>
</tr>
</thead>
<tbody>
<tr>
<td>Very effective</td>
<td>8%</td>
<td></td>
<td></td>
<td>3%</td>
</tr>
<tr>
<td>Effective</td>
<td>48%</td>
<td>38%</td>
<td>13%</td>
<td>23%</td>
</tr>
<tr>
<td>Moderately Effective</td>
<td>40%</td>
<td>50%</td>
<td>87%</td>
<td>50%</td>
</tr>
<tr>
<td>Not effective</td>
<td>4%</td>
<td>12%</td>
<td>4%</td>
<td>24%</td>
</tr>
</tbody>
</table>

**Integration of Enterprise and IT risk management frameworks**

A broad consensus exists among participants that, both business stakeholders as well as Group risk functions, lacked clear understanding of the roles and responsibilities with regards to the IT risk management processes.

The enterprise risk management frameworks lacked a common language, in order to help IT risk related communications amongst business, IT, risk and audit management.
From the perspective of industry maturity and growth, it is encouraging to see a good proportion of organisations with dedicated IT Risk functions.

Organisations with a compliance requirement for an IT risk program and an effective risk culture tend to invest in a dedicated IT risk function. Similarly, large organisations (over 5000 employees) as well as Banking and Financial Services organisations tend to have a dedicated IT risk function.

### Dedicated IT risk management function

<table>
<thead>
<tr>
<th>Dedicated IT risk management Function?</th>
<th>Over 5000</th>
<th>1001 – 5000</th>
<th>251 - 1000</th>
<th>51 – 250</th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>32%</td>
<td>53%</td>
<td>45%</td>
<td>50%</td>
</tr>
<tr>
<td>We are evaluating the need for having a dedicated IT risk management Function</td>
<td>11%</td>
<td>6%</td>
<td>27%</td>
<td>50%</td>
</tr>
<tr>
<td>We are in the process of implementing a dedicated IT risk management Function</td>
<td>8%</td>
<td>12%</td>
<td>18%</td>
<td></td>
</tr>
<tr>
<td>Yes</td>
<td>49%</td>
<td>29%</td>
<td>9%</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Dedicated IT risk management Function?</th>
<th>Banking and Financial Services</th>
<th>Government and Defence</th>
<th>Energy &amp; Utilities</th>
<th>Other commercial organisations</th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>24%</td>
<td>50%</td>
<td>25%</td>
<td>60%</td>
</tr>
<tr>
<td>We are evaluating the need for having a dedicated IT risk management Function</td>
<td>8%</td>
<td>25%</td>
<td>25%</td>
<td>13%</td>
</tr>
<tr>
<td>We are in the process of implementing a dedicated IT risk management Function</td>
<td>4%</td>
<td>38%</td>
<td></td>
<td>10%</td>
</tr>
<tr>
<td>Yes</td>
<td>64%</td>
<td>25%</td>
<td>12%</td>
<td>17%</td>
</tr>
</tbody>
</table>

### Funding

Practitioners from the organisations with a dedicated IT risk function indicated that they received adequate funding and sponsorship from their senior management.

Limited participation and buy-in from business stakeholders and/or board members was of a concern to a small number of these organisations.
Architecture enablers: “Are we doing them the right way?”

An organisation’s success depends on effectively identifying and acquiring capabilities and resources that are important to translate plans into action. These capabilities and resources can be broadly classified as ‘People, Process and Technology.’ For this project, we focused mainly on the following questions to determine an organisation’s ability to manage their IT Risks:

- Who is accountable for IT risk management?
- What reporting hierarchy is appropriate for our organisation?
- What size and organisational structure do we need for IT risk management?
- Has organisation adopted an appropriate framework to support IT risk management processes?

**IT risk management process ownership**

Although there are variations in the structure and reporting lines of organisations, large Banking and Financial Services organisations are likely to have an overall Group risk function and have IT risk as part of it.

Apart from these organisations, most other participants indicated that their organisation preferred delegating the IT risk management process ownership to their Information Security Function over others.

The majority of practitioners and consultants are observing noticeable interest from senior executives and business stakeholders to address IT risk management short-term needs and challenges. However, the senior management’s reaction appears to be reactive and more tactical by assigning their IT security team to manage IT risks.

<table>
<thead>
<tr>
<th>IT risk management processes development responsibility</th>
<th>Overall</th>
<th>Banking &amp; Financial Services</th>
<th>Government and Defence</th>
<th>Energy &amp; Utilities</th>
<th>Other commercial organisations</th>
</tr>
</thead>
<tbody>
<tr>
<td>Information Security Function (e.g. A Head of IT risk and Information Security)</td>
<td>31%</td>
<td>16%</td>
<td>50%</td>
<td>25%</td>
<td>38%</td>
</tr>
<tr>
<td>Group Risk Function</td>
<td>21%</td>
<td>40%</td>
<td>13%</td>
<td>14%</td>
<td></td>
</tr>
<tr>
<td>Shared responsibility of key IT personnel</td>
<td>17%</td>
<td>4%</td>
<td>13%</td>
<td>25%</td>
<td>28%</td>
</tr>
<tr>
<td>A dedicated Head of IT risk with an IT risk Function</td>
<td>13%</td>
<td>28%</td>
<td>12%</td>
<td>13%</td>
<td>3%</td>
</tr>
<tr>
<td>A dedicated IT risk Manager reporting to Head of IT</td>
<td>7%</td>
<td>4%</td>
<td>25%</td>
<td>12%</td>
<td>7%</td>
</tr>
<tr>
<td>Others</td>
<td>11%</td>
<td>8%</td>
<td>25%</td>
<td>12%</td>
<td>10%</td>
</tr>
</tbody>
</table>

**Reporting hierarchy**

Survey respondents were asked to nominate their organisation’s IT risk management primary and secondary reporting lines. The majority of participants identified the Head of IT or the CIO as reporting manager for the most senior IT risk function by majority of participants.

For most of the Banking and Financial Services organisations, the reporting to manager was from Group / Enterprise risk function. The ‘Head of IT Strategy / Planning’ role was the most noticeable one in the ‘others’ category for reporting line.
Size of IT risk function

We were not able to discern a noticeable relationship between the size of the IT risk function, type of industry and the size of organisation. It appears that there is no right or wrong answer for any organisation. The size of the IT risk function will depend on a number of factors including immediate needs and focus of an organisation.

The practitioners at the organisations with a dedicated IT risk function were mostly comfortable with the number and mix (interval vs. external) of staff operating in their IT risk management function.

<table>
<thead>
<tr>
<th>Size of IT risk function team</th>
<th>Overall</th>
<th>Banking and Financial Services</th>
<th>Government and Defence</th>
<th>Energy &amp; Utilities</th>
<th>Other commercial organisations</th>
</tr>
</thead>
<tbody>
<tr>
<td>over 10</td>
<td>31%</td>
<td>41%</td>
<td>40%</td>
<td></td>
<td>26%</td>
</tr>
<tr>
<td>5 to 10</td>
<td>14%</td>
<td>18%</td>
<td>20%</td>
<td></td>
<td>11%</td>
</tr>
<tr>
<td>2 to 5</td>
<td>43%</td>
<td>36%</td>
<td>40%</td>
<td>80%</td>
<td>42%</td>
</tr>
<tr>
<td>1</td>
<td>12%</td>
<td>5%</td>
<td>20%</td>
<td></td>
<td>21%</td>
</tr>
</tbody>
</table>

Frameworks adopted to support IT risk management processes

It appears that, because a number of organisations have delegated IT risk management responsibilities to their Security Function, this has resulted in the widely held view that the Security team is responsible for all IT related risks.

This could be one of the reasons why over 56% of industry survey participants are using ISO/IEC 27001 or 27005 (Information Security Management System standard) as one of the frameworks for their IT risk management function. This challenge becomes more prominent when approximately 44% of these (i.e. 25% of all participants) are using only ISO/IEC 27001 or 27005 to manage their IT risk.

A further trend observed is that many of small (250-1000) to medium (1001-5000) sized Banking and Financial Services organisations have preferred ISO/IEC 27001 or 27005 framework over ISO/IEC 31000 (Risk management standard, previously AS/NZS 4360).

Depending on the development and direction of the risk management practice within organisations the standards and frameworks used as the preferred frame of reference varied.

The interviewees were cautiously positive to explore the role ISACA’s Risk IT Framework can play to enable IT risk functions in facing integration and alignment challenge, citing their inability to influence or provide input to existing enterprise risk management policies and processes.
**Delivery enablers: “Are we getting them done well?”**

ISACA’s Risk IT Framework process model is designed and structured to enable enterprises to apply the six Risk IT Framework principles in practice and to benchmark their performance.

The Risk IT framework’s process model is divided into three domains:

- **Risk Governance,**
- **Risk Evaluation,** and
- **Risk Response**

— with each domain containing three processes.

The framework provides guidance on the key activities within each process, responsibilities for the process, information flows between processes and performance management of each process.

While whitepaper scope did not cover validating the maturity of IT risk management activities performed, we have included this model for your quick reference.

**Value enablers: “Are we getting the benefits?”**

An organisation should establish a clear and shared understanding of the expected benefits from managing IT risks to an acceptable level. This can be achieved by implementing relevant metrics to “Measure and manage IT risk.” We discussed the maturity of existing measurement and improvement activities during one-on-one interviews with practitioners and consultants.

The results were disappointing as very few organisations fared well in the ‘Measure and manage’ IT risk processes. While this can be explained at a high-level by the lower maturity of the IT risk management processes as discussed in the later part of this document, the only observations we can share are:

- Most organisations are using informal and reactive improvement initiatives to improve their IT risk management capabilities and processes.
- Motivated, skilled and experienced IT risk practitioners were the primary enablers for the organisations that fared well.
Traditionally, IT risk management responsibilities have been delegated to technical specialists outside the boardroom, despite falling under the same ‘umbrella’ risk category as other business risks such as credit risk or market risk.

IT risk is not just a technical issue. While IT subject matter experts help to understand and manage aspects of IT risk, business management is the most important stakeholder. Business managers determine what IT needs to do to support their business; they set the targets for IT and are accountable for managing the associated risks.

**The Risk IT Framework**

To prioritise and manage IT risk, senior executives need a frame of reference and a clear understanding of the IT function and IT risk. ISACA’s Risk IT framework provides a set of guiding principles and processes to help organisations identify, govern and effectively manage IT risk.

The connection to business is founded in the six principles on which the Risk IT Framework is built. These principles are based on commonly accepted Enterprise risk management principles, which have been applied to the domain of IT.

**Benchmarking maturity against the Risk IT principles**

Practitioners as well as consultants were asked to provide their opinion on how well organisations are performing against the Risk IT Framework principles.

**Practitioners’ view on their organisation’s performance against the Risk IT Framework principles**

<table>
<thead>
<tr>
<th>ISACA’s Risk IT Framework Principles</th>
<th>Poorly</th>
<th>Somewhat</th>
<th>Good</th>
<th>Very well</th>
</tr>
</thead>
<tbody>
<tr>
<td>Always connect to business objectives</td>
<td>8%</td>
<td>43%</td>
<td>41%</td>
<td>8%</td>
</tr>
<tr>
<td>Align the management of IT-related business risk with overall ERM</td>
<td>7%</td>
<td>48%</td>
<td>34%</td>
<td>11%</td>
</tr>
<tr>
<td>Balance the costs and benefits of managing risk</td>
<td>15%</td>
<td>43%</td>
<td>39%</td>
<td>3%</td>
</tr>
<tr>
<td>Promote fair and open communication of IT risk</td>
<td>16%</td>
<td>34%</td>
<td>36%</td>
<td>13%</td>
</tr>
<tr>
<td>Establish the right tone from the top while defining and enforcing personal accountability for operating within acceptable and well-defined tolerance levels</td>
<td>15%</td>
<td>41%</td>
<td>36%</td>
<td>8%</td>
</tr>
<tr>
<td>Are a continuous process and part of daily activity</td>
<td>13%</td>
<td>51%</td>
<td>33%</td>
<td>3%</td>
</tr>
</tbody>
</table>

The predominant response from practitioners of “somewhat” reflects the lower maturity of the IT risk management activities in organisations.

**Consultants’ view on how their clients are performing against the Risk IT Framework principles**

<table>
<thead>
<tr>
<th>ISACA’s Risk IT Framework Principles</th>
<th>Poorly</th>
<th>Somewhat</th>
<th>Good</th>
<th>Very well</th>
</tr>
</thead>
<tbody>
<tr>
<td>Always connect to business objectives</td>
<td>8%</td>
<td>64%</td>
<td>28%</td>
<td></td>
</tr>
<tr>
<td>Align the management of IT-related business risk with overall ERM</td>
<td>20%</td>
<td>60%</td>
<td>20%</td>
<td></td>
</tr>
<tr>
<td>Balance the costs and benefits of managing risk</td>
<td>12%</td>
<td>56%</td>
<td>32%</td>
<td></td>
</tr>
<tr>
<td>Promote fair and open communication of IT risk</td>
<td>8%</td>
<td>48%</td>
<td>32%</td>
<td>12%</td>
</tr>
<tr>
<td>Establish the right tone from the top while defining and enforcing personal accountability for operating within acceptable and well-defined tolerance levels</td>
<td>12%</td>
<td>60%</td>
<td>20%</td>
<td>8%</td>
</tr>
<tr>
<td>Are a continuous process and part of daily activity</td>
<td>20%</td>
<td>64%</td>
<td>12%</td>
<td>4%</td>
</tr>
</tbody>
</table>

Though more conservative, the predominant response of “somewhat” from consultants reaffirms the lower maturity of Australian organisations to meet their IT risk management objectives.

However, it was encouraging to note that both practitioners and consultants agreed about growing trend of organisations promoting fair and open communication of IT risk.
ISACA’s CRISC and CGEIT certifications

Certified in Risk and Information Systems Control (CRISC)

CRISC is the only certification that prepares and enables IT professionals for the unique challenges of IT and enterprise risk management, and positions them to become strategic partners to the enterprise.

The CRISC designation focuses on:
- Risk identification, assessment and evaluation
- Risk response
- Risk monitoring
- IS control design and implementation
- IS control monitoring and maintenance

Why Employers should hire CRISCs

CRISCs bring additional professionalism to any organisation by demonstrating a quantifiable standard of knowledge, pursuing continuing education, and adhering to a standard of ethical conduct established by ISACA. CRISC employees:
- Build greater understanding about the impact of IT risk and how it relates to the overall organisation
- Assure development of more effective plans to mitigate risk
- Establish a common perspective and language about IT risk that can set the standard for the enterprise.

ISACA draws on a global network of leading professionals to develop its certification programs. With access to experts around the world, ISACA is defining how IT risk is managed in current and future business environments.

Certified in the Governance of Enterprise IT (CGEIT)

CGEIT recognises a wide range of professionals for their knowledge and application of enterprise IT governance principles and practices.

ISACA’s IT governance certification tests the ability and judgement of individuals in:
- Aligning business strategy, capabilities and investment priorities
- Bridging the gap between business and IT
- Continuously tracking and improving performance
- Optimising the use and allocation of resources
- Proactively managing risks to an acceptable level

Why Employers should hire CGEITs

When an enterprise employs a CGEIT, they ensure good governance, which provides for an environment of no or few “surprises” and the ability to have an agile response to any that arise. The employee has the knowledge and experience necessary to support and advance the IT governance of an enterprise.

The enterprise’s IT and business systems operate with greater efficiencies and optimum effectiveness resulting in greater trust in, and value from, information systems.

CGEIT demonstrates proven expertise. Boards and executive management expect IT to deliver business value. IT governance is a key component of enterprise governance and success. A CGEIT designation demonstrates that you have proven experience and knowledge in the governance of enterprise IT.

References

- www.isaca.org/riskit
- The Risk-IT Brochure by ISACA

ISACA has recently won the 2013 Best Professional Certification Award from SC Magazine for the Certified in Risk and Information Systems Control (CRISC) credential.

“SC Magazine is proud to recognize ISACA as a leader in the information security industry,” said Illena Armstrong, vice president of editorial, SC Magazine.
# Acknowledgements

This Whitepaper is the result of collective efforts of the Expert Reviewers and Development Team. This entire team participated generously offering their talent and expertise. Their participation and insight is truly appreciated. We would also like to thank our funding sponsor, Transpire, for their contribution.

Special thanks to all survey participants and interviewees who offered their time, talent and expertise. Their invaluable opinions and support was vital for the success of this Whitepaper project.

## Expert Reviewers for this Whitepaper project

<table>
<thead>
<tr>
<th>Name</th>
<th>Role</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>Babu Srinivas</td>
<td>CISO, SP AusNet</td>
<td>Babu has more than 17 years’ experience in Information Security and Information Technology. He has worked with and helped develop solutions for various commercial organisations such as nationalised &amp; private banks, pharmaceutical companies, BPOs, and Software EOU’s. Over the past 7 years he has been CISO at SP AusNet, Australia, providing information security leadership and strategic direction. He and his team provide expert advice, governance, assurance and security solutions for advanced technologies.</td>
</tr>
<tr>
<td>Chander Vohra</td>
<td>Assistant Commissioner, Australian Taxation Office</td>
<td>Chander has more than 30 years’ experience in various areas of IT and is currently working with Australian Taxation Office as Assistant Commissioner for Trusted Access and is responsible for IT and Information Security. Chander is an active member of ISACA’s Melbourne Chapter. He is an I-RAP assessor, holds ISACA’s CISA, CISM, CRISC and CGEIT certifications and is an alumni of the prestigious Indian Institute of Technology.</td>
</tr>
<tr>
<td>Christoph Strizik</td>
<td>Head of IT Risk, Origin Energy</td>
<td>Christoph is the Head of IT Risk and Information Security Management for Origin Energy where he is responsible for governance and strategy for IT Risk, including Compliance and Assurance, IT Service Continuity, and Information Security. Prior to his appointment to this position, he served in senior leadership and consulting roles for large corporations in Australia and Europe, primarily in financial services and the energy industry.</td>
</tr>
<tr>
<td>Gladys Rouissi</td>
<td>Srn Financial Risk Governance Manager, ANZ Global Wealth and Private Banking</td>
<td>Gladys is a risk and assurance professional with over 17 years’ experience primarily in the Banking and Financial Services industry, as well as in State Government. Over the past six years Gladys has participated in a number of ISACA initiatives including the ISACA IT Risk Taskforce (Chicago) for the development and review of the Risk IT Framework. She is currently a member of the COBIT 5 for Risk Taskforce established to review and implement this new framework. Gladys also served as President of the ISACA Sydney Chapter and held various roles on the Sydney Chapter Board for over 10 years.</td>
</tr>
<tr>
<td>Lambros Lambropoulos</td>
<td>IS Audit Leader, Audit Office of NSW</td>
<td>Lambros Lambropoulos is an IS Audit Leader with the Audit Office of NSW. He has extensive external and internal IS audit experience in project/transformation delivery (project auditing), and IT Risk and IT and Security Governance. On a yearly basis Lambros manages a client base of 45 large entities in the public sector. Lambros is also a current Board member of the Sydney Chapter.</td>
</tr>
<tr>
<td>Mitra Minai</td>
<td>Head of Technology Governance, ANZ Bank</td>
<td>Mitra has over 14 years of experience in Technology, Information Security and Business Operations risk and control management across private and public industry sectors within Europe, Asia and Australia. She has designed and implemented Business and IT strategies, governance structures and operational and compliance frameworks. She has managed large scale programs and project with focus on risk identification and management and compliance with local and international regulatory requirements. Mitra works at ANZ Bank in Technology Governance and is the current ISACA Melbourne Chapter President.</td>
</tr>
<tr>
<td>Stephen Smith</td>
<td>Managing Partner, Transpire</td>
<td>Stephen Smith has extensive global IT management experience with particular expertise in Strategy, Planning, Enterprise Architecture, Risk and Governance. Stephen has gained this experience in his roles as Head of Technology for NAB Asia, Head of Strategy, Planning and Finance for NAB Services (Europe), as Head of Global Channel Strategy for the NAB Group, as Chief Architect for Westpac and as G.M. Strategy and Architecture for RailCorp.</td>
</tr>
</tbody>
</table>
ISACA is an international not-for-profit, member based professional association. It comprises 100,000 members globally across 200 chapters. ISACA develops and maintains frameworks, provides certifications and professional development.

Our membership is made up of: CIOs; IT strategy, governance and portfolio management professionals; Business and IT architects; Auditors and assurance professionals; Business and IT risk managers; Information security professionals and IT professionals. With over 3,500 members, the ISACA Chapters in Oceania include Adelaide, Brisbane, Canberra, Melbourne, New Zealand, Perth, PNG and Sydney.

For more information, please visit [www.isaca.org](http://www.isaca.org)

**Frameworks developed and continually updated by**

<table>
<thead>
<tr>
<th>Framework</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>COBIT 5</td>
<td>A complete, internationally accepted process framework for IT that supports business and IT executives and management in their definition and achievement of business goals and related IT goals by providing a comprehensive IT governance, management, control and assurance model. Available as a complimentary download at <a href="http://www.isaca.org/cobit">www.isaca.org/cobit</a>. COBIT 5 is used by organisations worldwide.</td>
</tr>
<tr>
<td>Val IT</td>
<td>Based on COBIT, now in version 2.0, is a framework with supporting publications that address assumptions, costs, risks and outcomes related to a balanced portfolio of IT-enabled business investments, including guidance to help global organisations maximize the value of IT investments. Val IT is available as a free download at <a href="http://www.isaca.org/valit">www.isaca.org/valit</a>.</td>
</tr>
<tr>
<td>Risk IT</td>
<td>Based on COBIT, is a framework that helps enterprises increase their return on investment by managing risks effectively, rather than trying to eliminate them completely. The Risk IT Framework is available as a free download at <a href="http://www.isaca.org/riskit">www.isaca.org/riskit</a>.</td>
</tr>
<tr>
<td>ITAF</td>
<td>IT Assurance Framework (ITAF) provides guidance on the design, conduct and reporting of IT audit and assurance assignments, and establishes standards that address IT audit and assurance professional roles and responsibilities; a free download at <a href="http://www.isaca.org/itaf">www.isaca.org/itaf</a>.</td>
</tr>
<tr>
<td>BMIS</td>
<td>Business Model for Information Security (BMIS) provides a view of information security program activities within the context the larger enterprise to integrate the disparate security program components into a holistic system of information protection; a free download at <a href="http://www.isaca.org/bmis">www.isaca.org/bmis</a>.</td>
</tr>
</tbody>
</table>

**Globally accepted and recognised ISACA Certifications**

<table>
<thead>
<tr>
<th>Certification</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CISA</td>
<td>A globally respected designation for experienced IS audit, control and security professionals. More than 90,000 have earned the CISA designation since its inception in 1978.</td>
</tr>
<tr>
<td>CISM</td>
<td>A groundbreaking designation for leaders who manage an organisation’s information security. More than 19,000 have earned the CISM designation since it was established in 2002.</td>
</tr>
<tr>
<td>CRISC</td>
<td>CRISC, for IT professionals who have experience with risk identification, assessment and evaluation; risk response; risk monitoring; IS control design and implementation. More than 16,000 professionals have been certified since inception in 2010.</td>
</tr>
<tr>
<td>CGEIT</td>
<td>CGEIT, for professionals who manage, provide advisory and/or assurance services, and/or who otherwise support the governance of an enterprise’s IT. More than 5,400 professionals have earned the CGEIT designation since it was established in 2007.</td>
</tr>
</tbody>
</table>
ISACA Sydney Chapter

ISACA Sydney Chapter was established in 1976 and has over 1,000 members.

Our vision is to enable our members and their employers to gain trust in, and value from, information systems.

To achieve this, we aim to improve the ability of our members to implement ISACA frameworks and pass our certification exams.

Our business activities include: free monthly professional development sessions, regular half day conferences and COBIT 5 framework special interest group sessions. We also provide low cost training courses on our frameworks and certifications.

www.isaca.org/sydney

ISACA Melbourne Chapter

ISACA Melbourne Chapter has over 850 members.

In serving its members, Melbourne Chapter provides free monthly enriching professional development sessions and regular educational review sessions for ISACA Certifications exam candidates. We also offer a wide array of reasonably priced educational seminars and workshops for members.

We ensure our members are abreast of the latest local chapter activities through our periodic Chapter newsletter titled “reView” where articles of professional interest are published along with chapter information and details of our upcoming local Professional Development sessions.

www.isaca-melbourne.org

Transpire

Transpire is an Information Technology Advisory and Project Delivery firm with particular strengths in strategy, sourcing, service delivery and governance.

Transpire combines talented people with proven methods to solve complex business problems and to unearth new opportunities.

Some of Australia’s leading organisations benefit from partnering with Transpire. They get sound advice, projects delivered faster, improved returns and optimised operational efficiency. Moreover, they have confidence their business is in good hands.

Overwhelmingly, clients who choose Transpire value the power of thought. They know with Transpire clever thinking happens. Good ideas flow with Transpire to build better results for you and your organisation.

www.transpire.com.au