Quick Guide: Managing ICT Risk for Business

This Quick Guide is one of a series of information products aimed at helping small to medium sized enterprises identify and manage risks when assessing, buying and implementing new IT products.

The Discipline of Risk Management

Risk management is an increasingly important element of corporate governance and is closely associated with the pursuit of improved business performance, innovation and productivity. The identification, analysis, acceptance and mitigation of risk is essential to the process of buying and implementing new IT products.

By identifying potential risks in advance of undertaking a business activity or business decision, management can determine the likelihood and potential impact of the risks identified, as well as strategies to avert or minimise the threats that each risk poses.

Many companies may already have a standing Risk Committee, comprising employees, managers and/or board members, as appropriate. Typically such a committee would be chaired by the operations manager, a senior executive or a board member, and would regularly meet to review and assess a company's risk exposures and risk treatment activities.

General Risk Management Methodologies

Two useful methodologies for managing risks are the 'Risk Register' and the 'Risk Matrix'. The Risk Register is a list of all risks that have been identified, their significance (i.e. whether the risk is likely and how severe its impact will be if it occurs) and whether there is a way of mitigating (reducing) the impact.

The headings in a typical Risk Register look something like this:

Risk Number	Risk Description	Likelihood of Occurring (Lo/Med/Hi)	Impact if it Occurs (Lo/Med/Hi)	Agreed Risk Mitigation Treatment	Residual Risk Rating (Lo/Med/Hi)	Risk Owner
e.g. R01	**Corruption of customer data**	**Med**	**Hi**	**Full back up of customer records, always reconcile before new**	**Lo**	**Sales Manager to sign off before going live.**

Often a company will maintain a general risk register for all of its activities and periodically report to senior managers and board members on the status of these risks. If a company is undertaking a new initiative or project, it will typically create a risk register specifically focused on this new initiative.

The important discipline with the risk register is that there is a designated person who is responsible for maintaining it and that there is a regular risk review process during which all active risks are reviewed, to ensure that all risks are being monitored and treated.

The Risk Matrix is a visual tool that is very useful for highlighting the key risks confronting any project or business. There are a variety of sophisticated visual presentations, but all employ the same basic concepts. For a small and medium business, the following type of presentation will often be sufficient:

Risk Matrix – Residual Risks Following Risk Treatment

Business Impact if Risk Occurs	High	R06 *	R12	
	Medium	R02, R09	R10, R11	
	Low	R01, R04, R13, R14, R15, R16, R17, R18, R19, R120, R21, R22, R23	R03, R05, R07	R08
		Low	Medium	High
		Likelihood of Risk Occurring		

Legend:

- Low Risk
- Medium Risk
- High Risk

* The codes R01, R02 etc. above refer to risk numbers in the relevant Risk Register

When using risk management methodologies as illustrated above, it is important to ensure the status of risks is regularly monitored by management and that all risks in the Medium to High (orange to red coloured) categories are managed intensively to minimise the business risk they pose if risk mitigation action is not taken.

For a more in depth explanation of the broader discipline of risk management, refer to the *Australian Standard AS/NZS ISO 31000:2009 Risk Management – Principles and Guidelines*.

ICT Risks

ICT risks are an increasingly important part of corporate risk management, because they include such threats as business interruption, disaster recovery, business and information security, data back-up and protection, software licence compliance, ICT outsourcing and cloud services, and employee and contractor internet and social media use. However, one of the most important and far-reaching areas of ICT risk relates to how new or improved IT products are evaluated, purchased and implemented within a business. This is because new or changed IT systems can have game-changing impacts on a business, potentially affecting many areas.

If well thought through, these changes can be extremely positive, creating major business improvements. But careful planning and project management are required, otherwise a new IT system can have major, negative impacts; extending well beyond employees, to customers and suppliers and, ultimately, the viability of the business itself.

The Major Types of IT Risk for Business

In recent years, a variety of industry surveys of IT risk for business have been conducted across many firms in many industries in a large number of countries. From these types of survey, it is possible to identify four Common themes of IT risks for businesses:

1. Risks caused by falling behind

Firms failing to leverage readily available technology to improve business performance, access to markets and competitive position, with the result that they lose ground against competitors and new market entrants.

2. Risks caused by buying without sufficient care:

Firms making IT choices that do not fit with their other IT systems (or those of key customers or suppliers), that do not produce the benefits expected and take much longer to implement, or which create unexpected new costs.

3. Risks caused by failing to establish and maintain organisational commitment:

Firms failing to ensure adequate preparatory training and buy-in by staff, not ensuring strong project alignment and commitment from senior management, and failing to ensure project timelines and new system cut-overs occur as planned. All of which can lead to projects failing to realise anticipated benefits and where legacy systems often continue to run in parallel.

4. Risks caused by missing the opportunity to innovate:

Firms not being sufficiently strategic in their IT choices. This is perhaps the greatest risk and can be a consequence of any of the three foregoing risks. Because the opportunity costs of failing to maximise the potential transformative effects of new IT products and solutions can stifle innovation and best-in-class performance.

All businesses need to be constantly alert to the potential transformative effects of IT and to adopt systematic processes for evaluating, selecting, buying and implementing IT in just the same way that they would approach any other major, long-term business decision.

Identifying and Managing Risks during the IT Product/Service Assessment Stage

You should start by asking the following four questions:

1. Do we have a clear idea of our requirements?
2. How have others solved this requirement and what problems have they encountered?
3. Has our initial market research identified solutions with the potential to meet our requirements?
4. Do we have enough information to compare the costs and benefits of potential solutions?

One of the best start-points in establishing a sound risk management approach towards IT projects is to review the problem that you are trying to solve or the requirements that you have identified.

Often you will need to visit trade shows, conduct internet searches of available solutions and make enquiries of vendors and other businesses with which you interact or of industry associations of which you are a member.

The objective is to gain as much understanding of what is available in the market- place and how closely these offerings match your particular requirements.

For some businesses, these initial enquiries may be undertaken by one of the owners themselves, in the first instance, or this may be a project that can be allocated to a suitable member of the management team.

Either way, it is important, that this early process also involves consultation within the business – especially those whose work area will potentially be affected. Obtaining input to requirements and ensuring the regular review of preliminary findings is a key element in ensuring alignment and buy-in, as well as ensuring that important considerations are not overlooked.

Depending on the size of the business and the extent of the ICT solution under evaluation, a project team may need to be constituted and specialised external expertise may need to be bought in to augment the process.

Once this early 'scoping' phase of your potential IT purchase is complete it is important, as part of the process of establishing the 'business case', to analyse the findings and the risks that have been identified.

Tips:

Try listing out potential risks under the following headings:

Requirement Risks: e.g. are the requirements documented and agreed by internal stakeholders?

Technology Risks: e.g. have the options available and relevant IT trends been adequately researched/validated?

Project Management Risks: e.g. is there sufficient capacity to finance and manage the kind of changes envisaged?

Project Scheduling Risks: e.g. are there any internal or external factors that impact on when the IT solution can be implemented, and will the changes need to occur in stages?

Project Governance Risks: e.g. Are there clear arrangements in place governing accountability for consultation, sign offs and decision-making?

Identifying and Managing Risks during the Procurement Phase

Once a business has taken a decision to proceed beyond evaluating possible solutions, the serious commitments (and potential risks) commence. It is therefore important to have a clear idea about how ICT procurement works and how to minimise the commercial and business risks involved.

ICT procurement typically involves four components:

- Hardware (such as a computer server or other equipment);
- Software (such as a new customer relationship management system or accounting system);
- Implementation services (such as the setting to work of the new hardware, the setting up of the new software, migration of existing data to the new system and staff training); and
- Ongoing support.

Some ICT procurements will involve only one of these categories, but for most ICT procurements all four elements need to be considered collectively. A common procurement risk occurs when a business attempts to purchase these components separately and inadvertently become responsible for system integration.

Larger businesses will have one or more existing ICT personnel, who can advise on some aspects of procurement, but they will also be busy managing existing IT activities and may not have the time or expertise to manage a significant ICT procurement process.

An important first step is therefore determining whether a business has the in-house capacity to manage ICT procurement, or whether specialist assistance will be required. If specialist assistance is required, the business should consult with their other advisors (such as their accountants and/or lawyers) as well as their industry association, before making a decision on who to engage.

If using an external advisor, ask for references from other clients who had similar needs and make sure you check with those clients about their experience, before making an appointment. In terms of the risks and risk mitigation strategies that a business should consider when commencing the procurement phase, the following issues are very common potential problems that can be averted if care is taken at the outset.

It is important to avoid committing to a single vendor until all of these questions can be answered:

General Procurement Risks

E.g. how will you decide on a vendor – will you seek quotations? Will you provide vendors with a briefing and an information package? Do you have a draft contract? Have you considered how you will structure payments to ensure that you have control over the vendor's performance? Will you use your legal or accounting firm to assist with managing elements of the procurement process? What process will you follow to determine a preferred vendor?

Vendor-related Risks

E.g. Before selecting a preferred vendor, have you checked whether the short-listed vendors have a reputation for successfully meeting requirements similar to yours? Have you spoken with (and even visited) some of the short-listed vendors' reference sites? Do the vendors have the capacity to be on site and/or respond to calls for assistance when you need them at your location(s)?

Are you sure that you understand the structure of each short-listed vendor's pricing and ongoing support terms. (For example, some vendors will require you to pay an annual software licence fee and if you fail to do so, the software will be deactivated and some cloud service providers may not allow you to transfer your data if you change vendors.)

Do each of the short-listed vendors have a detailed implementation schedule and have you walked through it with them to make sure that you agree with their approach and that you can meet any obligations that you have to provide resources, etc.?

Have you ensured that the key internal stakeholders have had an opportunity to understand and agree to the preferred vendor's proposal and to meet the vendor and visit or speak to reference sites, if appropriate?

Have you conducted a web search on the short-listed vendors to determine if there are any customer complaints posted on discussion boards and so forth?

System Compatibility Risks

This is a potentially major risk that often only emerges after the procurement decision has been taken. A very good way to avoid this is to have the preferred vendor conduct a small on-site trial to demonstrate how the new system will interface with other business systems.

E.g. will the new system interface neatly with all your existing business systems or will there be a need to upgrade or modify those systems so that they can 'talk' to the new system.

Use this process to identify whether any changes need to be made to network configuration (such as to support more users or to handle multi-site connections), or to adjust on or off-site data storage, back-up or disaster recovery arrangements.

Also use this opportunity to assess the adequacy of business change management plans, such as training needed for users of the new system, opportunities to streamline business processes and retire legacy systems.

This is also a good way to ensure that the vendor fully understands the requirements of the project. It is important that such a trial is undertaken before any final purchase commitment is given. This will generally ensure that the vendor undertakes the pilot at no charge or for a nominal fee and it provides the business with a valuable opportunity for a pre-purchase reality check.

During the past two or three years an increasing range of so-called cloud services has become available. These services are particularly suited to many businesses needs since they essentially outsource many of the traditional hardware and software procurement and maintenance activities to a specialist vendor. For example, many businesses no longer have in-house accounting systems, customer management systems, email systems, switchboards, call centres, secretarial services, and so forth. In the age of the internet, these are all services that can be purchased on a subscription basis and accessed from any location.

In considering IT procurement options, it is becoming increasingly important to also consider whether a cloud service offers a viable alternative to an outright purchase.

Identifying and Managing Risks during the Implementation Phase

If a business conducts its evaluation and procurement phases well, the system implementation phase will be relatively straight-forward. Conversely, deficiencies in evaluation and procurement will surface during implementation and when this does occur, the results can be very painful for all involved.

A successful implementation is based on thorough planning, so it is important to ensure that the staff and the vendor have a well-prepared plan at the commencement of the implementation phase.

This 'Implementation Plan' is often one of the first deliverables for a vendor and can be used as a trigger for their first milestone payment. Important implementation challenges that should be addressed in the implementation plan include:

- Determining the system testing and acceptance regime -

E.g. how will the vendor demonstrate that the system is correctly performing to requirements, before it goes live?

- Depending on the scale of the ICT project, this may entail the initial establishment of a test bed or test environment (on site or at the vendor's premises), so that the new system can be configured and tested without disruption to business as usual activities.

- Determining how much configuration of the new system should be undertaken -

E.g. If an business is upgrading its accounting system, will it bring across its existing chart of accounts, or adopt a new account structure that is designed to make better use of the new system's in-built reporting functionality?

- Planning how (and when) data from existing systems will be migrated to the new system -

E.g. Will all of a firm's customer and vendor data be transferred into the new system, or only customers and vendors from, say, the past two years? If only some data is to be transferred, how will the other data be accessed if required?

Tips:

An ICT system Implementation Plan should determine:

- The system testing and acceptance regime
- How much configuration of the new system should be undertaken
- Planning how and when data from existing systems will be migrated to the new system
- System security requirements
- Training requirements for affected staff
- Board and senior management issues
- Go-live and Cut-over arrangements
- Transitioning to 'Business as Usual' and Benefits Realisation
- System Security requirements -

E.g. Ensuring that any new hardware required is installed (either on site or in a hosted environment) and that associated network and data security operates as required.

- Training for Affected Personnel -

E.g. How much training is required, can it be accommodated 'on the job' or will staff need to be released for training sessions? How will business disruption be minimised? Are staff prepared to undertake additional hours of work/training to minimise disruption?

- Board and Senior Management Issues -

E.g. Are the board and senior management involved in monitoring the project and committed to its implementation? Will there be any impact on the reporting and control processes that they are used to, are they aware of these changes?

- Go-live and Cut-over Arrangements -

E.g. Determining how the business will cut-over to the new system – will it be over a weekend (with sufficient time to roll-back to the old system if there is a problem)? Will there be a staged go-live process, possibly starting at only one site initially and then expanding once the system is known to be

working? Will certain key customers or vendors be advised in advance so that any important processing can be completed before the cut-over commences. Will vendor personnel be required on-site during cut-over to help with any trouble-shooting?

- Transitioning to 'Business as Usual' and Benefits Realisation -

E.g. what is the warranty period for rectification of bugs and deficiencies? How much of the contract value is held back pending final acceptance? Has all training and documentation been delivered? What on-going support arrangements are in place?

Often a major ICT investment is partly based on the realisation of savings, such as reduced running costs of legacy systems, productivity improvements or reduced inventories. It is important to press for the realisation of these benefits and to measure the relevant aspects of business performance before and after.

Risk Management is designed to enable Businesses to Grow, Innovate and Pursue Opportunities

ICT is now one of the major drivers of global productivity and innovation.

Businesses need to invest in IT and leverage its game-changing potential. This is particularly the case for small and medium sized businesses, which make up well over 90% of all Australian businesses.

Successful businesses have systems and management approaches that are designed to do a better job of managing risk than their competitors. The purpose of this guide to managing risks when buying or implementing new IT systems is to help businesses better understand IT risks, so that they can better manage them.

Further information

Visit the business website at business.gov.au.