Australian Government
Australian Taxation Office

Information System Risk Assessment (ISRA) tool manual

30 October 2019

How to use the ISRA tool to self-assess the overall integrity of your information system, internal controls and reduce determined risks

Contents

Contents **2**

About this manual **4**

Preparing to use the ISRA tool **4**

Requirements 4

Setting up the tool 4

Completing ISRA 5

Reviewing the ISRA report and results 6

Unit 1: Systems inventory assessment **7**

Instructions 7

System questions 8

Unit 2: Systems interfaces assessment **21**

Instructions 21

Interfaces 22

Unit 3: Customisation assessment **26**

Instructions 26

Customisations 27

Extent 27

Maturity 28

Ownership 29

Documentation 30

Unit 4: IT projects assessment **31**

Instructions 31

Projects 32

Costs 33

Process changes 33

Project team 34

Technology changes 35

Management methodology 36

Stakeholder engagement 37

Post implementation review (PIR) 38

Unit 5: IT governance assessment **39**

General background on control questions 40

Instructions 40

Governance 41

Alignment 41
Staffing 42
Responsibilities 43
Outsourcing 44
Application development and support methodology (ADSM) 45
Logical assets 46
Cloud assets 47
Physical assets 48
Business continuity planning (BCP) 49
Disaster Recovery Planning (DRP) 50
Risk mitigation **51**
Systems inventory 51
System interfaces 54
Customisations 55
Projects 56
Governance 58

About this manual

The instructions in this manual will help you use the Information System Risk Assessment (ISRA) tool to self-asses your IT system and determine what you can do to reduce any risks you find. These risks are based on five risk areas or auditable units detailed below.

In this manual:

- Unit 1**:** Systems inventory assessment
- Unit 2: Interfaces inventory assessment
- Unit 3: Customisations inventory assessment
- Unit 4: IT projects and methodologies assessment
- Unit 5: IT governance assessment
- Risk mitigation

The standard questions were developed internally by us using the references listed below:

- Information Systems Audit and Control Association (ISACA), IS Standards, Guidelines and Procedures for Auditing and Control Professionals, as of 1 March 2010.
- IT Governance Institute (ITGI), COBIT Control Practices, Guidance to achieve Control Objectives for Successful IT Governance, 3rd Edition, 2012.
- IT Governance Institute (ITGI), IT Control Objectives for Sarbanes-Oxley, The Role of IT in the Design and Implementation of Internal Control Over Financial Reporting, 2nd Edition, September 2006.
- IT Governance Institute (ITGI), CobiT 5., Framework, Control Objectives, Management Guidelines and Maturity Models, 2007.

Preparing to use the ISRA tool

Requirements

This tool runs on a Microsoft Access database. A link to access the tool can be securely downloaded here, or you can also view the accessible version on our ato.gov.au website here.

To use the tool effectively you must have Microsoft Access and Microsoft Word available on the computer or device you are downloading the file to.

Setting up the tool

Follow the below steps to download and the ISRA tool database:

1. Click on this link to download a copy of the ISRA tool access database
2. Select save to save the tool
3. A Macro Single step box will pop up – click X in right hand corner
4. Select Enable Content from the yellow ribbon bar
5. Make this a trusted document pop up by selecting yes.

The ISRA database is now ready for you to use.

To start using the tool follow the below steps:

1. Navigate to the home tab
2. Click on the reset database button on the home tab
3. Enter your Australian Business Number (ABN) and entity name
4. Normally you would tick each of the five auditable units to be completed. If you have made a decision to conduct a partial ISRA, you may tick only those units to be assessed
5. Save the database.

The tool is a standalone tool and is not connected to any ATO systems, which means we do not access your data in your ISRA tool database.

We will also not be able to access to a copy of your ISRA report, your responses or supporting evidence until such time as you voluntarily submit them to us.

Completing ISRA

To complete the ISRA you will need to work through each auditable unit. Each unit contains a number of questions and each question may have to be answered separately for each system, interface, customisation or project.

As you answer each question, record the evidence that supports your answer in the 'comments box'.

There will be further detailed instructions for each auditable unit in the guidelines in the tool.

Depending on the number of systems and complexity of your IT architecture the ISRA can take 2-6 hours to complete.

Who should fill out and use this tool

A person completing this tool should have a good working knowledge of:

- tax governance
- financial controls
- information systems
- business processes.

If understanding of all the above sits across different positions, it may be advisable to arrange a meeting, or to complete the ISRA with people who have responsibilities over the different areas to ensure a more accurate result.

An ISRA should generally be completed by either an experienced business representative with long term business and system knowledge or an Advisor.

Where the ISRA has been completed by an independent advisor we will generally accept the outcome of the tool assessment, subject to the supporting evidence being provided to us.

Where concerns are identified about the integrity of the output of the assessment, we may conduct an ATO generated ISRA assessment and request supporting evidence as required.

Reviewing the ISRA report and results

Once you have completed the ISRA you can preview the report, which will show you the risk rating for each question and auditable unit.

What to do if you have medium or high risk ratings

A medium or high risk rating is only an indicator of a risk. It should be used as part of your decision making process to assess if you need to address the risks raised by the ISRA based on your knowledge of your business and systems. Generally the focus should be on the level of control and governance you have put in place to address the risk. For guidance on how to mitigate the risk identified please refer to the 'Risk Mitigation' section of this manual.

Where the risk ratings are medium or high, you may consider engaging with your tax agent, independent advisor or us. You would discuss options regarding the risks identified, and establish a plan to mitigate the risks.

Evidence

The evidence you have based your responses on is to be recorded in the 'Comments box' within the tool and the document name recorded in the 'Documentary Evidence box'. Recording this evidence is important and will assist if we ask you to provide copies of the evidence to us for an ATO engagement meeting.

Saving the Report

You can save the answers to the questions, comments and evidence you relied on by navigating to the report function. The report function will collate all the responses, evidence and comments and provide an overall rating based on your answers.

You can save the report in PDF or Word format by selecting the 'Save to PDF' or 'Save to Word' functions from the report tab.

Voluntarily submitting your ISRA to the us

If you want to submit your ISRA to us, you can send the completed ISRA tool report and supporting evidence to us by contacting the case officer you have been engaging with.

Disclaimer

We are committed to providing you with guidance you can rely on, so we make every effort to ensure the Information Systems Risk Assessment Tool is correct.

If you act in accordance with your professional standards and follow our guidance and it turns out to be incorrect or misleading, and you fail to comply with the law as a result, we must still apply the law correctly. However, we will take the fact that you followed our guidance into account when deciding what action, if any, we should take.

If you make an honest mistake in using the Information Systems Risk Assessment Tool and you fail to comply with the law as a result, we will take the reason for the mistake into account in deciding what action to take.

We regularly revise the Information Systems Risk Assessment Tool to take account of any changes to the law, so make sure that you have the latest version of the Information Systems Risk Assessment Tool.

The Australian Taxation Office:

- provides the Information Risk Assessment Tool to take account of any changes to the law, so make sure that you have the latest version of the Information Risk Assessment Tool

- gives no express or implied warranties (and to the full extent permitted by law excludes all statutory warranties) in relation to Information Risk Assessment Tool (including as to its performance or fitness for a particular purpose)

- will not be liable in any way for any loss or damage (including special, indirect or consequential) arising from, or in connection with, Information Risk Assessment Tool or its use or performance.

Unit 1: Systems inventory assessment

The main purpose of obtaining an inventory of IT systems is to assess the size and complexity of your IT environment. The inventory will also reflect on your business processes and information/data flows that will help in later steps of the assessment.

Instructions

Progress bar

There is a progress bar on the 'summary tab' which progressively auto populates to show the percentage of the auditable unit that has been completed.

The report will not populate with a rating if less than 100% has been completed.

Identify the information systems

First identify the information systems to be included in the scope of the ISRA review if you have many information systems within your organisation. Depending on the function of the system it may not be necessary to assess all systems using the ISRA tool.

However, the scope of the ISRA needs to include all the IT systems, controls, processes, procedures and software relevant to tax and super regulatory compliance.

This will include source data, accounting data, financial data, compliance and regulatory reporting data.

Assess each system

Each of the systems you identify will be assessed separately.

The steps below are repeated separately for each identified system.

Setting up the system

In the ISRA tool, select the 'systems tab' at the top level and the 'overview tab' at the second level. Create an entry in this table for each system, including:

- the name of the system
- the version
- the business function it performs
- the entities within your business which use this system
- the name of the contact responsible for information about this system.

Select the 'questions tab' to see the short titles for the 12 questions. Selecting a question title on the left of the ISRA screen shows the possible answers in the main body of the ISRA screen.

You need to answer these questions for each of the systems you have identified. To do this select the system from the 'commercial name' drop down menu.

Answering the questions

There are 12 questions you need to answer separately for each information system. The questions are listed in the section below, under the short titles corresponding to the question titles in the ISRA tool screen. Select a question below for more detailed guidelines.

For each system and for each question in the ISRA tool select the question below to see the detailed guideline notes.

In the ISRA tool, under the systems and questions tabs:

- check the correct system name is selected in the 'commercial name box' above the answers
- select the abbreviated question title on the left of the screen
- follow the detailed question guideline to record the evidence you have to support your answer to this question, using the 'comment box'
- select the answer that best represents your system.

System questions

- Nature of application support
- System support
- User base
- Auditing software
- Database
- Software delivery methods
- Software defined infrastructure
- Prior audit findings
- Maturity of application
- Data reconciliation
- Documentation
- Criticality

Nature of application package

Q1. What is the nature of the information system used by the business to record, store and report tax and superannuation obligations?

Background

Information systems can be divided into two broad categories:

- cloud off the shelf (OTS) products that are vendor developed and vendor maintained
- custom bespoke developed.

Off-the-shelf refers to those systems that can be purchased over the counter at various commercial distributors and can be installed within a short period of time and requires minimal configuration. This can be either installed on-premises or a cloud version.

Cloud custom bespoke refers to internet-based distributed, stored and maintained systems.

Both custom cloud and OTS cloud products are vendor developed and likely vendor maintained.

For the purpose of assessing this ISRA key variable, cloud-based OTS packages are treated the same way as larger, vendor developed and implemented Enterprise Resource Planning systems (ERPs) such as SAP, Oracle Financials, JD Edwards, PeopleSoft.

This is because all of these systems are developed by specialist vendors and offer standard functionality to automate a variety of commonly accepted best practice business processes

Why we are asking this question

There are different risks depending on how your system was developed and how it is maintained. For example, a bespoke system developed recently in-house for a single implementation may not be as thoroughly tested as a general purpose system developed by a large software company that has been implemented many times over a long period.

Vendor developed and maintained OTS products are generally rated as low risk. However this risk may rise as the product ages and is no longer supported by the vendor.

Custom or bespoke developed systems are considered more risky and therefore rated as medium or high (depending on the circumstances) as they are developed to a specific company's requirements, and are generally not subject to the scrutiny or testing of a broad user-base.

Evidence you need to support your answer

Where applicable, in the 'comment box' at the bottom of the ISRA screen for this question enter:

- details of the system vendor
- the developer and maintainer of the system
- where there is joint responsibility, describe the responsibilities and relationships.

Possible answers

You have ten options to choose from:

- OTS cloud product or vendor developed and vendor maintained
- custom built by vendor and maintained by vendor
- vendor developed and in-house maintained
- vendor developed and not maintained/end of life cycle
- jointly developed and vendor maintained
- jointly developed and in-house maintained
- in-house developed and maintained
- mitigated
- awaiting response
- n/a.

Selecting your answer

Select the answer that most closely represents the nature of your system.

For each question where ‘mitigated’ is selected you must clearly outline the reason why in the ‘comments box’.

System support

Q2. How is the system supported?

Background

System support or maintenance refers to the provision of assistance in matters related to information technology products. This may include functions such as computer hardware, software installation, configuration and troubleshooting, among other IT related services.

The key to assessing the risk is to determine how quickly or easily both software related issues and hardware or network problems are resolved within the organisation, reducing the risk of incorrect reporting, treatment or revenue leakage.

There are a variety of factors which may influence this variable including (but not limited to):

- the physical location of the support provider
- experience of technical ability of the support staff
- escalation process
- timeliness of issue resolution
- levels 1-3 support structures
- prioritisation of issues.

Why we are asking this question

Ineffective support arrangements could impact the availability and accuracy of your information systems which could affect the accuracy and completeness of your tax and super reporting and lodgement activities.

Evidence you need to support your answer

In the ‘comment box’ at the bottom of the ISRA screen for this question, enter a description of the support structure and what happens when issues occur.

If you have service level agreements with external providers and or internal service level agreements, record the names of those documents in the ‘comment box’.

Possible answers

You have six options to choose from:

- in-house support
- external support
- mixture of in-house and external support
- no support or ineffective support
- awaiting response
- n/a.

Selecting your answer

Select the answer that most closely represents your support arrangements.

User base

Q3. What percentage of staff have administrator authorisation to make changes to the critical master data code etc. in this information system?

Background

This question is about the number of people who are able to change master files, tables and parameters in the system, such as supplier and customer files, tax code files, formulas, backend data codes etc. It does not include normal end users of the system who have no ability to change or set up data. The number is expressed as a percentage of the workforce.

Why we are asking this question

When a higher percentage of staff are able to make changes to critical data in the system there is a higher risk of the system's integrity being compromised. This risk can be mitigated with tighter controls and a higher level of governance appropriate to the number of staff with this function.

Evidence you need to support your answer

In the 'comment box' at the bottom of the ISRA screen for this question, enter the number of staff who are able to change critical data in the system and the number in the total workforce.

Possible answers

You have seven options to choose from:

- up to 20% of staff
- between 20% and 40% of staff
- between 40% and 60% of staff
- between 60% and 80% of staff
- between 80% and 100% of staff
- awaiting response
- n/a.

Selecting your answer

Select the answer that most closely represents your staff's use of the system.

Auditing software

Q4. Is the audit functionality turned on so you can monitor access, date and time of transactions?

Background

The aim of database and software auditing is to proactively monitor end-user and administrator access and activity in an ongoing manner for early detection of breaches, including hacking by an external party.

Audit trails enable auditors to identify the origins of a specific transaction – whether it may be an end user or another system – and the timing of that transaction.

Top-end databases such as Oracle and other large ERP systems such as SAP and Oracle Financials have in-built auditing capabilities that log all system changes and details of the user that made the change, including date and time.

Auditing changes in both your organisation's database and software is the most proactive way to ensure that any abnormal transactions are caught early and addressed promptly.

Why we are asking this question

The risk of unauthorised or inappropriate access to information systems is reduced when auditing software is installed, is being used and the results are monitored.

Having auditing software installed, in use and being monitored reduces the risk that unauthorised or inappropriate use will occur or go undetected. Unauthorised access could expose you to material or reputational damage and potentially risk breaching privacy obligations.

Evidence you need to support your answer

If your system has an auditing capability, enter details of its use in the 'comment box' at the bottom of the ISRA screen for this question, including:

- whether it is turned on
- whether it can be manually turned off, and if so, by whom
- whether it generates regular or exception audit reports
- how frequently the reports from the system are monitored, and by whom are they monitored.

If you have auditing software turned on and you have an example of a monitoring report, record the name of the report in the 'comment box'.

Possible answers

You have five options to choose from:

- auditing software is always turned on
- auditing software is always turned off
- the system does not have auditing software capability
- awaiting response
- n/a.

Selecting your answer

Select the answer that most closely represents your use of auditing software.

Database

Q5. What type of database does this information system use?

Background

Computer data storage consists of computer components and recording media used to retain digital data. It is a core function and fundamental component of computers. A database is an organised collection of data.

Some databases offer more inherent security, integrity and performance features than others. Databases, such as cloud databases, that are run on and accessed via the internet belong to this category and are assigned a low risk as the use of databases of this type eliminates lengthy implementations, behind-the-scene updates and allows for better scalability.

However it is recognised that stronger controls and governance is required to support data bases of this nature due to the increased risk of data breaches and hacking. Commonly used relational databases (such as Oracle, Sybase, IBM, CA, MySQL and MS SQL server) also are low risk.

Microsoft Excel and Access are considered more risky as databases due to the greater likelihood of data corruption and their inefficiency when dealing with larger volumes of data.

Flat files are the most at risk, as they have no internal structure of their own (ie there is no file definition as such) as their structure is defined within the logic of the software program that generates them.

Why we are asking this question

The integrity of an information system is fundamentally linked to the integrity of the database that stores data. Your ability to meet your reporting and lodgement activities could be compromised if critical data is lost or corrupted or not available when required.

Evidence you need to support your answer

In the 'comment box' at the bottom of the ISRA screen for this question, enter details of the type of database used by your system and where it is located.

Possible answers

You have seven options to choose from:

- Cloud
- Relational Database Management System (RDBMS)
- Microsoft (MS) Access
- spreadsheet (eg Excel)
- flat file
- awaiting response
- n/a.

Selecting your answer

Select the answer that most closely represents a description of your system's database.

Software delivery methods

Q6. How is your software delivered to the end user?

Background

The delivery method refers to the way that applications or software get to your eventual users within your organisation. This could be via:

- externally supplied, maintained and deployed (usually internet cloud-based). This is low risk as it is generally automated
- internally provided, maintained and updated (usually on a non-cloud platform)

- mix of external and in-house.

Why we are asking this question

The concern is whether the regular updates or patches made available by the vendor are being loaded in a timely fashion to keep the systems and or platforms up-to-date.

Internally managing the complexity of maintaining and testing deployments potentially increases the risks that critical updates are not being made, such as excise rates, PAYGW tax rates.

Evidence you need to support your answer

In the ‘comment box’ at the bottom of the ISRA screen for this question, describe the software delivery method for this system.

If you have service level agreements with external providers and or internal service level agreements record the names of those documents in the ‘comment box’. The service level agreement would be expected to include:

- how updates are delivered
- how upgrades are managed
- how it is determined when to apply an upgrade
- what authorisations and approvals are required to apply an upgrade
- how you ensure tax and superannuation changes are applied when required
- what testing and approval is included in the upgrade process.

If your software delivery method is managed either wholly or partially in-house and the details above are not covered in a service level agreement, include those details in the ‘comment box’.

If you have taken steps to mitigate the risks inherent with a mixed external and in-house support structure, describe the mitigation steps you have taken in the ‘comment box’.

Possible answers

You have six options to choose from:

- externally supplied and maintained
- in-house developed, delivered and maintained
- mixture of both external and in-house
- mitigated – mixture of both external and in-house
- awaiting response
- n/a.

Selecting your answer

Select the answer that most closely describes the software delivery method for this system.

For each question where ‘mitigated’ is selected you must clearly outline the reason why in the ‘comments box’.

Software defined infrastructure

Q7. Who develops and maintains your software defined infrastructure?

Background

The software defined infrastructure question is concerned with where the software is hosted and how it is managed. Infrastructure components include:

- computer hardware platforms
- operating system platforms
- enterprise and other software applications
- data management and storage
- networking and telecommunications platforms
- internet platforms
- consulting and system integration services.

Why we are asking this question

The overall integrity of your infrastructure is critical to the information system providing the functions it is designed to perform. It is also important to be able to support your changing business requirements by being scalable and providing resource balancing and redundancy.

The risks from deficiencies in the infrastructure are likely to be reduced where you have clear ownership and accountability for the infrastructure.

Evidence you need to support your answer

In the 'comment box' at the bottom of the ISRA screen for this question, enter a description of the management of the components of the infrastructure, particularly those components that are not covered by other questions in this auditable unit.

If you have service level agreements with external providers or agreements with internal service providers record the names of those documents in the 'comment box'.

If you have taken steps to mitigate the risks inherent with mixed external and in-house software defined infrastructure, describe the mitigation steps you have taken in the 'comment box'.

Possible answers

You have six options to choose from:

- externally owned, provided and maintained
- in-house developed, provided and maintained
- mixture of both external and in-house
- mitigated – mixture of both external and in-house
- awaiting response
- n/a.

Selecting your answer

Select the answer that most closely represents the nature of your software defined infrastructure.

For each question where ‘mitigated’ is selected you must clearly outline the reason why in the ‘comments box’.

Prior audit findings

Q8. Has this system or systems recently been audited by the ATO or your external and internal auditors?

Background

Information system (IS) audits or reviews are generally conducted within your business either by an internal audit function or an external party. Prior IS audit findings may indicate risks to the information system or the absence of IS audits may in itself indicate a risk. This question seeks to:

- establish whether your systems are regularly audited by an external party
- determine whether you have an internal review process to examine the systems
- determine whether these audits or reviews have identified issues and whether the identified issues have been rectified.

Why we are asking this question

Prior IS audits are likely to have investigated certain risk areas more closely than an ISRA review. Therefore the findings from prior IS audits are relevant to the ISRA process of assessing risk.

Any systems or IT management issues detected during a past IS audit may still be relevant irrespective of whether these issues were later resolved.

The frequency of IS audits is also relevant. If you carry out regular proactive IS audits or reviews your own systems, this would represent a lower risk than if you don’t.

Evidence you need to support your answer

In the ‘comment box’ at the bottom of the ISRA screen for this question, list recent IS audits, both internal and external, and summarise the findings from those IS audits and the actions taken to resolve issues raised.

If you have IS audit report and management response documents, record the names of those documents in the ’comment box’.

If you have taken steps to mitigate the risks identified in an IS audit, describe the mitigation steps you have taken in the ‘comment box’.

Possible answers

You have nine options to choose from:

- recent audit with no weaknesses
- recent audit with minor weaknesses
- recent audit with some weaknesses
- mitigated – recent audit with some weaknesses
- recent audit with many weaknesses
- mitigated - recent audit with many weaknesses
- no recent audit
- mitigated – no prior audit

- awaiting response
- n/a.

Selecting your answer

Select the answer that most closely represents your history of recent audits.

For each question where ‘mitigated’ is selected you must clearly outline the reason why in the ‘comments box’.

Maturity of application

Q9. How old is your system and how long has this information system was in place?

Background

The length of time that an application is in production may play a factor in how stable the application is. An application that has been around for a greater length of time is usually more firmly bedded down and better integrated.

A newly implemented system may take several months to bed down teething issues and longer for procedures and support networks to be established. As the application ages however, the risk may rise again as the software approaches obsolescence and is no longer supported by a vendor.

Why we are asking this question

Recording the maturity of your information system will show the inherent risk if the system is still at a stage where there could be teething issues with the system itself or the processes around it.

Evidence you need to support your answer

In the ‘comment box’ at the bottom of the ISRA screen for this question, record the history of the implementation of your system.

If it has been recently implemented, show the implementation schedule and highlight the critical activities that are still outstanding. If a replacement or major upgrade is planned for the system, give details of the planned replacement and the schedule.

If you have taken steps to mitigate the risks inherent with system less than four years old, describe the mitigation steps you have taken in the ’comment box’.

If your system is ten years or older provide details of how the risk of obsolescence is being managed by the vendor and whether there is continued vendor support provided.

Possible answers

You have eleven options to choose from:

- over 10 years - supported and maintained
- over 10 years - not supported or maintained
- between 7-10 years
- between 4-6 years
- mitigated 4-6 years
- between 1-3 years
- mitigated – 1-3 years

- less than 1 year
- mitigated <1year
- awaiting response
- n/a.

Selecting your answer

Select the answer that most closely represents the maturity of your system.

For each question where ‘mitigated’ is selected you must clearly outline the reason why in the ‘comments box’.

Data reconciliation

Q10. How is data reconciliation and exception reporting handled?

Background

This question is about the use of data audit log files and automated data reconciliation with exception reporting. Systems with these capabilities offer a higher level of security and assurance on the quality of the data output.

Automated data reconciliation tends to be a feature of integrated systems and may be achieved by running reconciliation reports that compare data from one module with corresponding data from another within the same system.

For example, the accounts payable sub ledger data (ie invoices) should tally to the balance of the accounts payable control account in the general ledger.

The term exception reporting refers to the automated handling of any data integrity or processing error detected either during transaction processing or as a result of running the reconciliation programs the system offers.

Why we are asking this question

Establishing the extent to which use of the system is logged and monitored allows assessment of the risks resulting from inadequate controls over the system’s data, including data entry, data transfer and data storage.

Evidence you need to support your answer

In the ‘comment box’ at the bottom of the ISRA screen for this question, describe the controls over recording data changes, data reconciliations and monitoring for this system. The description may address:

- the process for month end reconciliation
- any automated calculations, coding of transactions or data processing routines programmed into the system
- maintenance and testing of automated features and verification they are working to specifications
- review of system processes – how often and by whom
- exception reporting
- documentation of procedures for error or reconciliation reporting and response to exceptions
- extent of information captured in the systems audit trail
- controls over activating the audit trail

- circumstances under which it may be turned off.
- controls over access to the audit logs

If you have examples of reports and or audit trail logs record the names of those documents in the 'comment box'.

Possible answers

You have seven options to choose from:

- both system generated data reconciliation and exception reporting with full transaction audit trail
- only system generated data reconciliation and exception reporting with no, or only limited, transaction audit trail
- transaction audit trail only with no system generated data reconciliation or exception reporting
- neither system generated data reconciliation and exception reporting nor transaction audit trail
- mitigated – manual process with well governed controls
- awaiting response
- n/a.

Selecting your answer

Select the answer that most closely represents your data reconciliation processes.

Documentation

Q11. What documentation do you have for this information system?

Background

System documentation may include:

- end-user documentation
- system diagrams
- data dictionaries
- program specifications
- test scripts
- process flow diagrams.

To be useful, system documentation must be up-to-date and reflect the latest changes to the system and processes.

Why we are asking this question

Over time the integrity of the system may be compromised if critical documentation does not exist or its currency is not maintained. Examples include code changes not being made visible, interfacing data tables not being changed, etc.

Evidence you need to support your answer

The prime evidence is the actual documentation. In the 'comment box' at the foot of the ISRA screen for this question, enter a description of the documentation you have and record the names of those documents.

Possible answers

You have five options to choose from:

- version controlled specifications and data dictionary and test scripts
- out of date specifications and no test scripts
- no specifications and no test scripts
- awaiting response
- n/a.

Selecting your answer

Select the answer that most closely represents the state of your system documentation.

Criticality

Q12. How critical is this system in the operations of your business?

Background

A system is deemed critical if unavailability results in a significant loss of revenue and goodwill for your organisation. Usually, the systems that you rely on to carry out trading activities will be deemed critical whereas the systems you rely on to perform back office functions such as the production of accounts will be deemed vital or sensitive, depending on the processing complexity and the tolerance to unavailability. The risk is higher if a system is less tolerant to unavailability because of the volume of data processed or the complexity of processing.

Why we are asking this question

The system may have a bearing on your ability to conduct your business, receive revenue and correctly report your tax and super reporting and lodgement activities. The more critical the system the higher the risk. The assessment of this risk for your system helps to weigh the risk relative to your other systems.

Evidence you need to support your answer

In the 'comment box' at the foot of the ISRA screen for this question, describe what would happen if this system was unavailable, including mitigation strategies you may have in place. Refer to any documentation of your mitigation strategies.

Possible answers

You have seven options to choose from:

- non-sensitive - application functions may be interrupted for an extended period of time at little or no cost to your organisation and require little or no catching up when restored
- sensitive - application functions can be performed manually at a tolerable cost and for an extended period of time. However, manual execution is a difficult and laborious process that requires additional staff

- vital – application unavailability will result in some loss of revenue and or goodwill to your organisation. System functions can be performed manually but at great financial and resource costs and therefore for only a brief period of time
- critical - application unavailability will incur significant loss of revenue and goodwill
- mitigated critical - application unavailability will incur significant loss of revenue and goodwill
- awaiting response
- n/a.

Selecting your answer

Select the answer that most closely represents the criticality of this system.

For each question where 'mitigated' is selected you must clearly outline the reason why in the 'comments box'.

Unit 2: Systems interfaces assessment

A program or system interface is a programmatic mechanism enabling two or more separate and independent software systems or components to communicate and exchange data.

Software interfaces adopt a concept of source and destination systems. The source system is the system the data initially comes from and the destination system is the system the interface ultimately aims to take the data to.

A typical automated system interface will usually involve a degree of data transformation and or aggregation from the source system to the destination system following a pre-conceived logic and mapping rules.

This ISRA auditable unit aims to understand the extent of the data manipulation and the complexity of data mapping. For example, is the data converted to a different format to enable the transfer of data with the receiving system.

Instructions

Identify the system interfaces

First identify the system interfaces to be included in the ISRA review. These will be the interfaces to and from the systems you identified in the first auditable unit. They will include interfaces between these systems and may also include interfaces to other systems.

Assess each interface

Each of the interfaces will be assessed separately.

The steps below are repeated separately for each identified interface.

Set up the interface

To set up the ISRA interface:

- select the 'interfaces tab' at the top level and the 'overview tab' at the second level and create an entry in this table for each interface, including:
  - the source system name

  - the target system name
  - the name of any intermediate system
- select the ‘questions tab’ to see the short titles for the four questions. Selecting a question title on the left of the ISRA screen shows the possible answers in the main body of the ISRA screen.
- answer these questions for each of the interfaces you have identified. To do this, select the interface from the ‘source system’ drop down menu.

Answer the questions

There are four questions to be answered separately for each interface. The questions are listed in the following section below, under the short titles corresponding to the question titles in the ISRA tool screen.

For each interface and for each question in the ISRA tool select the question below to see the detailed guideline notes.

In the ISRA tool, under the Interfaces and ‘questions tabs’:

- check the correct interface is selected in the ‘Source system box’ above the answers
- select the abbreviated question title on the left of the screen
- follow the detailed question guideline to record the evidence you have to support your answer to this question, using the checkboxes or the comments box
- select the answer that best represents your system.

Select a question below for more detailed guidelines.

Interfaces

- Complexity
- Method
- Exceptions
- Documentation

Level of Complexity

Q1. How complex is the interfacing between your systems?

Background

The complexity of the interface between two systems is a function of the following factors:

- data mapping between the source system and the destination system based on a single or multiple criteria
- level of data aggregation between the source system and the destination system.

Interface Example: Airline reservation systems

Data from an airline reservation system is at the individual booking level and includes attributes such as passenger names, flight numbers, flight dates, fares, fees, levies and taxes paid.

When this data is transferred to the airline’s accounting system, there will typically be a grand total against

Profit & Loss account for domestic fares, fees and charges codes and taxes paid plus Balance Sheet account codes for the day.

This means that the interface aggregates data following a pre-determined mapping between flight numbers and fare income accounts, fee codes, fee income accounts, charge codes and charge income accounts and tax codes and tax balance sheet accounts.

For the interface program to run correctly, the mapping would have to be updated every time a new flight number, a new fee code, a new charge or a new tax are created in the reservation system. Otherwise, the income would still be raised in the reservation system but it may not appear at all or be incorrectly classified in the accounting system.

Why we are asking this question

A higher level of complexity increases the risk that the interface will not correctly manipulate and map the data moving between the systems.

Evidence you need to support your answer

In the 'comment box' at the bottom of the ISRA screen for this question, describe:

- the data sources
- the manipulation of the data into the target format
- the data mapping process.

Possible answers

You have five options to choose from:

- low complexity - minimal data manipulation/formatting - static data mapping - simple transaction summarisation - few data sources
- medium complexity - intermediate complexity of data manipulation - data mapping based on multiple criteria - several data sources
- high complexity - multiple data sources - complex data manipulation - dynamic data mapping
- awaiting response
- n/a.

Selecting your answer

Select the answer that most closely represents the complexity of your interface.

Method

Q2. How are your systems interfaced?

Background

ISRA distinguishes between three main interface methods:

- system event triggered or automated cyclic batch update. The scheduling of the interface is automated based on a system event such as a time or a status being set
- manually activated batch update. The interface logic is contained in a program but its execution relies on an operator triggering a batch update or a similar system event

- data from the source system manually transposed to the destination system. This interface method relies on human intervention and the correct interpretation of the data between two or more systems.

Why we are asking this question

There are inherent risks with each interface method which are:

- automated scheduling of the interface is considered more reliable and less risky as the running of the interface is not reliant on human intervention
- manual scheduling of an automated interface may be a medium risk because it relies on human intervention, but the data manipulation should be reliable
- a purely manual interface is the riskiest method as it is entirely reliant on the timeliness and consistency of the human intervention.

Evidence you need to support your answer

In the 'comment box' at the bottom of the ISRA screen for this question, describe the processing of your interface, including how the interface is invoked and any human intervention in the operation of the interface.

Possible answers

You have five options to choose from:

- system event triggered or automated cyclic batch update
- manually activated batch update
- Data from source system manually transposed to destination system
- awaiting response
- n/a.

Selecting your answer

Select the answer that most closely represents the method of your interface.

Exceptions

Q3. How do you know if the interfacing and flow of data does not work?

Background

There are a number of techniques your systems may use to monitor the interface for errors and handle exceptions. These include:

- a pre-processing data validation step where the interface data from the source system is validated according to pre-established rules before the actual interface program executes. The main objective to this pre-processing is to ascertain that there is a mapping rule for all the data in the source system
- a post-processing reconciliation step where the data between the source and destination systems is automatically reconciled after the interface program has executed
- system generated exception reporting where an automated report or email systematically reports any interface processing errors (exceptions)
- manual checking and reconciliation.

Why we are asking this question

The risks of data not being accurately passed across the interface are higher when the automated monitoring and exception handling features are not present.

Evidence you need to support your answer

In the 'comment box' at the foot of the ISRA screen for this question, describe the exception handling of your interface, including:

- how you know if errors occur
- whether the systems will continue processing if an interface error occur
- whether there is pre-processing validation or post processing reconciliation
- what happens to correct the situation when an error occurs?

Possible answers

You have five options to choose from:

- good exception processing
  - pre-processing data validation step
  - system generated exception processing & data reconciliation and automated error alert
  - all in or none in record processing
- medium exception processing
  - no pre-processing data validation step
  - system generated record processing reconciliation and no automated error alert, rejected records must be managed by end-users
- low or no exception processing
  - manual reconciliation required, no automated error alert
- awaiting response
- n/a.

Selecting your answer

Select the answer that most closely represents the operation of exception handling in your interface.

Documentation

Q4. Do you have any documentation on the interfacing method and flow of data between your systems?

Background

Documentation is critical to understanding how the data is treated during the transfer between your systems and is a prerequisite for making changes and upgrades to the interface. Documentation may include data and processing specifications, data mapping codes and test scripts.

Why we are asking this question

Without adequate documentation there is a risk changes to the interface will not be properly managed, resulting in inaccuracies in the data crossing the interface.

Evidence you need to support your answer

The prime evidence is the actual documentation. In the 'comment box' at the bottom of the ISRA screen for this question enter a description of the documentation you have and record the names of those documents.

Possible answers

You have five options to choose from:

- comprehensive documentation - version controlled specifications and test scripts available
- average documentation - original specifications available but no test scripts
- poor documentation - no specifications or test scripts available
- awaiting response
- n/a.

Selecting your answer

Select the answer that most closely represents the state of your interface documentation.

Unit 3: Customisation assessment

Customisation occurs where systems are developed or modified to meet your business requirements. The scope of customisations includes software programs, appearance, functionality, business logic, data storage, interfaces, and reports.

The modifications may result in changes in the behaviour of a program, the processing logic of a program, additional data being processed or a combination of these.

Customisation does not normally include customised reports where the changes are only to report on pre-defined fields that are available in the software.

The purpose of this ISRA auditable unit is to assess the level of customisation, the associated risks across all systems and the controls to address these. The higher the customisation, the higher the risk to data integrity as software defects increase proportionately to the number of modifications made to the original software.

Instructions

Identify the customisations

First identify the system customisations to be included in the ISRA review. These will be the customisations made to the systems identified in the first auditable unit.

Assess each customisation

Each customisation will be assessed separately.

The steps below are to be addressed separately for each customisation.

Set up the customisation

To set up the customisation in the ISRA tool:

- select the Customisations tab at the top level and the overview tab at the second level. Create an entry in this table for each changed system or application, including:
  - the name of the changed system/application
  - the nature of the change
- select the questions tab to see the short titles for the four questions. Selecting a question title on the left of the ISRA screen shows the possible answers in the main body of the ISRA screen.
- answer these questions for each of the changed systems or applications you have identified. To do this, select the system or application from the “system changed” drop down menu.

Answer the questions

There are four questions to be answered separately for each changed system or application. The questions are listed in the following section below, under the short titles corresponding to the question titles in the ISRA tool screen. Select a question below for more detailed guidelines.

For each changed system and for each question in the ISRA tool select the question below to see the detailed guideline notes.

In the ISRA tool, under the customisations and questions tabs:

- check the correct changed system name is selected in the ‘system changed box’ above the answers
- select the abbreviated question title on the left of the screen
- follow the detailed question guideline to record the evidence you have to support your answer to this question, using the checkboxes and or the comments box
- select the answer that best represents your customised system.

Customisations

- Extent
- Maturity
- Ownership
- Documentation

Extent

Q1. How extensive are the changes made by this customisation?

Background

A customisation will generally involve changes to a system’s software programs screens and reports. For ISRA the level of system customisation is expressed by the percentage of the number of software programs that have been customised within the system.

The higher the percentage of components that have been changed, the greater the likelihood an error has been introduced into the original system.

Why we are asking this question

The extent of the customisation is one factor in understanding the overall customisation risk. Very extensive customisations may be higher risk depending on the controls that have been in place during the

customisation project to ensure complexities have been thought through in design and there has been thorough testing and stakeholder engagement.

Evidence you need to support your answer

In the 'comment box' at the bottom of the ISRA screen for this question, record the number of programs or components modified in the customisation and the total number of programs or components. You may refer to lists of components.

Possible answers

You have five options to choose from:

- low (from a few to 10% of programs)
- medium (more than 10% but less than 50% of programs)
- high (50% or more of programs)
- awaiting response
- n/a

Selecting your answer

Select the answer that most closely represents the percentage of components customised.

Maturity

Q2. How long has this customisation been in place?

Background

The length of time that a customised system has been in production may play a factor in how stable the system is. A customised system that has been around for a greater length of time is usually more firmly bedded down and better integrated into your business processes.

A newly implemented customisation may take several months to bed down teething issues and longer for procedures and support networks to be established.

However, as the customised system ages there may be developing risks relating to maintenance and support. These risks are likely to be higher when:

- the customisation is not maintained by the system vendor
- there is not good up to date documentation of the customisation specifications
- changes are required for changed business requirements
- changes are required for changes to the supporting infrastructure
- changes are made to other interfaced systems.

Why we are asking this question

The maturity of the customisation is one factor in understanding the overall customisation risk. More recent customisations may be higher risk depending on the controls that have been in place during the customisation project to ensure alignment with business objectives and the level of testing and stakeholder

engagement. Older customisations could have their own risks if good controls have not been maintained over support and documentation.

Evidence you need to support your answer

In the 'comment box' at the bottom of the ISRA screen for this question, record the history of the development and implementation of the customisation. If it has been recently implemented, show the implementation schedule and highlight any critical activities, including testing, that are still outstanding.

Possible answers

You have eight options to choose from:

- over 10 years
- 7-10 years
- 4-6 years
- 1-3 years
- less than 1 year
- awaiting response
- mitigated
- n/a

Selecting your answer

Select the answer that most closely represents the maturity of this customisation.

Ownership

Q3. Who developed and maintains this customisation?

Background

Systems customisation can be developed and maintained by your original system vendor, internal IT staff or a third party.

An internally maintained customisation is likely to be tested by end users who are not solely dedicated to a software verification function like professional software testers within a software vendor.

Customisations done by third parties who are not involved in the ongoing maintenance may also be incompatible with software patches and may have other inherent risks, as neither the vendor nor the in-house staff may be familiar with the specifications of the customisation.

Why we are asking this question

Understanding the ownership history and ongoing responsibilities helps in assessing the risks inherent in customisations to original products.

Evidence you need to support your answer

In the 'comment box' at the bottom of the ISRA screen for this question, record details of who developed the customisation and who is responsible for maintaining the customised changes.

Possible answers

You have seven options to choose from:

- vendor developed and maintained
- vendor developed and in-house maintained
- in-house developed and maintained
- developed by external party (not original vendor) and in-house maintained
- developed by external party (not original vendor) and maintained by contractors
- awaiting response
- n/a.

Selecting your answer

Select the answer that most closely represents the ownership of the customisation.

Documentation

Q4. Do you have any documentation that sets out the specific design of your customisation?

Background

Documentation is critical to understanding what was customised and how the customisation was built.

This understanding is necessary for future changes to the customisation, either to meet your new business requirements or for compatibility with future upgrades to the host system.

Documentation should include test scripts, details of coding, function, interfacing, features, and compatibility with other systems and records of engagement by the end users of the customisation.

Why we asking this question

All systems are likely to require upgrades over time because of changing business requirements or upgrades to the supporting infrastructure. When customised systems are upgraded, there is a risk to the accuracy of the customisation and the level of testing if there are no current and maintained specifications of the customisation or there are no defined test scripts that cover all scenarios.

Evidence you need to support your answer

The prime evidence is the actual documentation. In the 'comment box' at the bottom of the ISRA screen for this question, enter a description of the documentation you have and record the names of those documents in the 'comment box'.

Possible answers

You have five options to choose from:

- version controlled specifications, data dictionary and test scripts
- out of date specifications and no test scripts
- no specifications and no test scripts

- awaiting response
- n/a.

Selecting your answer

Select the answer that most closely represents the state of your customisation documentation.

Unit 4: IT projects assessment

This ISRA auditable unit attempts to establish how stable and mature your IT systems are and the business processes they support. It also looks at the risk management process and the governance and controls your board or management have over the project and how they identify and manage a risk should it arise during the project.

Any major IT project may strain IT and business resources quite significantly to the point where normal reconciliations and controls may be by-passed or not carried out as thoroughly as they normally are to accommodate project deadlines.

Typical IT projects include:

- the upgrade of an existing system
- the implementation of a new system
- the replacement of legacy system
- the implementation of a new module within an existing system
- the change of the configuration of an existing system e.g. changes of financial year, change of chart of accounts etc.

All projects may potentially impact adversely on data integrity because of inherent project activities such as data conversion, business process re-engineering and streamlining.

External events that may trigger the undertaking of such projects may include:

- corporate mergers and acquisitions
- change of legislation
- merger and acquisitions of major IT vendors
- technological advancement.

Instructions

Identify the projects

First identify the IT projects to be included in the ISRA review. These will be the projects that affect the systems you identified in the first auditable unit.

Assess each project

Each of the projects you identify will be assessed separately.

The steps below are repeated separately for each identified project.

Set up the project

To set up the project in the ISRA tool:

- select the ‘projects tab’ at the top level and the ‘overview tab’ at the second level. Create an entry in this table for each project, including:
  - the name of the project
  - the applications affected by the project
  - the project start date
  - the project end date
  - the project budget
- select the questions tab to see the short titles for the seven questions. Selecting a question title on the left of the ISRA screen shows the possible answers in the main body of the ISRA screen
- answer these questions for each project you identified in the step above. To do this, select the project from the ’project name’ drop down menu.

Answer the questions

There are seven questions to be answered separately for each project. The questions are listed in the following section below, under the short titles corresponding to the question titles in the ISRA tool screen. Select a question below for more detailed guidelines.

For each project and for each question in the ISRA tool select the question below to see the detailed guideline notes.

In the ISRA tool, under the projects and questions tabs:

- check that the correct project name is selected in the ‘project name box’ above the answers
- select the abbreviated question title on the left of the screen
- follow the detailed question guideline to record the evidence you have to support your answer to this question, using the checkboxes and or the comments box
- select the answer that best represents your project.

Projects

- Costs
- Process changes
- Project team
- Technology changes
- Management Methodology
- Stakeholder engagement
- Post implementation review (PIR)

Costs

Q1. What is the project cost as a percentage of your administration costs?

Background

Projects create a risk to the stability and accuracy of information systems as their purpose is to change business operations through new systems, replacements, modifications or major upgrades. Larger projects are likely to have more impact on systems, resulting in a higher risk.

To measure the size of a project relative to the systems environment, the project budget as a percentage of the costs of systems administration is a useful indication and is comparable across different types of businesses and scales of projects.

Why we are asking this question

Disruption to normal systems and business operations from project activities could impact on the ability to accurately meet your reporting obligations.

Evidence you need to support your answer

In the 'comment box' at the bottom of the ISRA screen for this question, enter the budget for this project and an estimate of the annual systems administration costs. If the project's duration is more than one year, determine an annual project budget for comparison with the corresponding administration costs year. Calculate the project costs as a percentage of the administration costs.

Possible answers

You have five options to choose from:

- less than 25%
- between 25% and 75%
- greater than 75%
- awaiting response
- n/a.

Selecting your answer

Select the answer that most closely represents the cost of this project as a percentage of administration costs.

Process changes

Q2. Did or will this project require any business process changes?

Background

IT projects may involve a high degree of process changes, for example:

- implementing a new system is likely to automate processes that were previously done manuall

- migrating to a different system is likely to require the end-user to adjust to different processing logic, user interfaces or data.

For this reason, there is likely to be a correlation between the amount of business process changes and the level of risk involved in implementing a new system. The more process changes there are, the higher the risk level and therefore higher level of control and governance is required.

Upgrading from one version of a system to the latest version may be seen as a technical upgrade only, implying you are not changing any of your business processes and will not be (or will be deferring) using the new functionality offered in the new version.

While it is true that a technical upgrade would lower the level of risk involved in the implementation, this kind of upgrade is likely to involve data conversion of all database files which would warrant full user acceptance testing of all modules to ensure that the converted data has come across correctly.

Why we are asking this question

Significant changes to business processes resulting from this project could increase the risk of incorrect use of the system if staff are not supported with trained and the correct use of the system and new functionality. This could affect the accuracy of your systems in conducting your business operations and super and tax reporting.

Evidence you need to support your answer

In the 'comment box' at the foot of the ISRA screen for this question, describe the level of business processing reengineering resulting from this project.

Possible answers

You have six options to choose from:

- no or minimum process reengineering - no or minimal application configuration changes
- moderate process reengineering - moderate application configuration changes
- extensive process reengineering - extensive/fundamental application configuration changes
- mitigated
- awaiting response
- n/a.

Selecting your answer

Select the answer that most closely represents the level of the process changes resulting from this project.

Project team

Q3. What is the make-up of the project team?

Background

This question focuses on the level of experience of your project staff and the permanency of project staff to enable knowledge transfer between project team and eventual systems owners and custodians.

In addition to the obvious risks from using inexperienced project staff, there are additional risks when using external contractors who may not be available to transfer essential knowledge to the system's custodians.

This may create ongoing knowledge gaps, which can cause errors and delays further down the system life cycle when either the configuration must be updated or integration with other modules is needed.

Why we are asking this question

In the short term there is a risk the information systems will not accurately perform their intended functions if they are implemented by inexperienced staff. In the longer term there are risks for later changes and upgrades to the systems if essential knowledge of the systems has not been retained within the organisation.

Evidence you need to support your answer

In the 'comment box' at the bottom of the ISRA screen for this question, describe the experience of the project team and their relationship to your organisation.

Possible answers

You have eight options to choose from:

- dedicated internal staff only – average experience level more than 5 years
- internal staff (mixed level of experience/dedication) and dedicated highly experienced long term IT providers
- dedicated internal staff only - average experience level less than 2 years
- dedicated external consultants only
- non-dedicated internal staff only - average experience level more than 2 years
- mitigated
- awaiting response
- n/a.

Selecting your answer

Select the answer that most closely represents your project team.

Technology changes

Q4. What is the nature of the technology changes introduced by this project?

Background

There is higher inherent risk in changing to technologies that are new, untried, untested or not widely accepted within the industry.

Why we are asking this question

Basing systems critical to your tax reporting obligations on higher risk technologies increases the risk that the systems will not perform their functions reliably and accurately.

Evidence you need to support your answer

In the ‘comment box’ at the bottom of the ISRA screen for this question, describe the technologies used by this project and comment on their industry use and acceptability.

Possible answers

You have six options to choose from:

- tried and widely used
- fairly new but accepted worldwide
- fairly new but not accepted worldwide
- tried and proprietary
- mitigated
- awaiting response
- n/a.

Selecting your answer

Select the answer that most closely represents the status of your technologies.

Management methodology

Q5. What project methodology was applied for the management of this project?

Background

Effective project management is critical to the project delivering on its objectives within the planned budget and schedule. There are a number of approaches to project management and many methodologies. Choosing the right methodology will depend on the objectives, team experiences and fit with the organisation. The methodology groupings include:

- traditional sequential methodologies
- the Project Management Institute (PMI) method of break down into process groups
- the Agile family of methods
- various change management methodologies
- process based methodologies
- others, such as Projects in Controlled Environments (PRINCE) and PRISM.

Why we are asking this question

Without good project management there is the risk that the project will not achieve its objectives or it may miss key schedule milestones or the testing may not be thorough. This may result in the information systems not performing as required or not being available when required.

Evidence you need to support your answer

In the ‘comment box’ at the bottom of the ISRA screen for this question, describe the project management methodology in use.

If you have project plan and schedule documents record the names of those documents in the 'comment box'.

Possible answers

You have five options to choose from:

- proven methodology - documented standards and procedures - clear milestones
- new methodology - uneven documentation - clear milestones
- no/poor methodology - poor documentation - unclear/changing milestones
- mitigated
- awaiting response
- n/a.

Selecting your answer

Select the answer that most closely represents how your project is managed.

Stakeholder engagement

Q6. Who was engaged from the business to provide input into this project?

Background

Both the user community and senior management should remain engaged throughout the project to guarantee buy-in and acceptance.

There will typically be a project sponsor and a project steering committee that will make decisions when issues arise. The project steering committee should meet on a regular basis and minutes of these meetings should be kept.

Why we are asking this question

Without key stakeholder engagement there is a risk the project may not deliver a solution that meets the actual requirements, particularly the requirements of those responsible for reporting business activity and tax obligations. There is also a risk the user community may not be adequately involved, leading to lack of commitment or insufficient familiarity with the system.

Evidence you need to support your answer

In the 'comment box' at the bottom of the ISRA screen for this question, list the evidence you have of stakeholder engagement. This may include meeting minutes, emails, newsletters and training records.

Possible answers

You have six options to choose from:

- senior management and user community engaged
- senior management engaged but user community disengaged
- senior management and user community disengaged

- mitigated
- awaiting response
- n/a

Selecting your answer

Select the answer that most closely represents the stakeholder engagement in the project.

Post implementation review (PIR)

Q7. Have you conducted a post-implementation review on this project?

Background

A post implementation review should be conducted within a few months of a new system being implemented to ensure that corrective action is undertaken when issues have arisen and also to measure and confirm the expected return on investment (ROI).

The main outcome of such a review will normally be captured in a formal report distributed to management and the major project stakeholder groups.

Why we are asking this question

Issues found in the post implementation review could indicate potential risks for the ongoing operation of the system.

Evidence you need to support your answer

In the ‘comment box’ at the bottom of the ISRA screen for this question, describe when and how the post implementation review was conducted and any issues that came out of it.

If you have a report from the post implementation review, record the name of the document in the ‘comment box’.

Possible answers

You have seven options to choose from:

- project ongoing or not started
- conducted - ROI on track - no major issues found
- conducted - ROI compromised - some issues found
- conducted - ROI seriously compromised - many issues found
- review not conducted
- awaiting response
- n/a.

Selecting your answer

Select the answer that most closely represents the status of your post implementation review.

Unit 5: IT governance assessment

The purpose of this ISRA auditable unit is to gauge the adequacy of internal policies, procedures and methodologies that should be consistent with an effective and productive management of the IT function within your organisation.

It is the responsibility of management, executives and the board to ensure good IT governance through organisation structures and process; ensuring the enterprise IT sustains and extends to the organisations strategies and objectives.

IT governance is concerned with two outcomes:

- its delivery of value to the business
- mitigation of IT risks

These two outcomes are enabled by strategic alignment of IT and business and the availability of adequate resources. Management oversight and monitoring of performance is critical in effective IT governance. Implementing good IT governance is almost impossible without engaging an effective governance framework.

A governance framework must define which decisions have to be made, who is involved in making them, how they are made and what the process is for ensuring that these decisions are carried out in the appropriate manner.

Lack of good controls and governance may result in:

- failure to meet business and user requirements
- systems may not perform as expected
- compromised data or security
- reduced systems availability
- questionable integrity of data
- unclear roles and responsibilities
- loss of revenue
- reputational risk
- inaccurate billing
- insufficient allocation of resources
- control gaps
- costly compensating controls
- inability to satisfy regulatory or compliance requirements
- inability to satisfy audit/assurance requirements.

General background on control questions

Within the ISRA context control refers to the mechanisms by which specific business activities are monitored and directed. Internal controls are the policies, procedures, practices and organisational structures designed to provide reasonable assurance that business objectives will be achieved and undesired events will be prevented or detected and corrected.

A control practice is a key mechanism that supports the achievement of control objectives through responsible use of resources, appropriate management of risk and alignment of IT with business requirements. Control activities are distinct, documented activities dedicated to reduce the risk to the accuracy, completeness, timeliness or consistency in financial reporting. The concern is primarily with access control, change approval and the resolution of incidents of relevant IT systems.

A well designed internal control system will help to ensure financial information and reporting is reliable and free of any material misstatement due to foreseeable risks. The control system ensures objectives are met efficiently and effectively, resources are used appropriately and legal compliance occurs. The risk management process includes determining the priorities of risk, outlining the course of action that needs to take place to avoid the risk and mitigating the impacts of risk.

Within the control system there should be:

- segregation of duties with clear roles and responsibilities – including board, management and staff roles and responsibilities
- data integrity controls – including IT system and application controls that maintain the integrity and security of data
- an IS audit plan outlining the testing of IT controls across the system landscape
- a clearly documented disaster recovery plan – outlining who, when and how systems will be brought back up
- a clearly documented business continuity plan – outlining what staff need to do to mitigate the risk of revenue leakage and reputational risk and keep the business running, including reporting of financial information to meet their compliance obligations.

Specific control questions

Within the ISRA context control refers to the mechanisms by which specific business activities are monitored and directed. Internal controls are the policies, procedures, practices and organisational structures designed to provide reasonable assurance that business objectives will be achieved and undesired events will be prevented or detected and corrected.

Instructions

Set up for the review

- in the ISRA tool, select the governance tab (this unit differs from the other units in that each question is only answered once)
- the answers apply to the overall IT governance of the organisation
- select the questions tab to see the short titles for the ten questions
- selecting a question title on the left of the ISRA screen shows the possible answers in the main body of the ISRA screen.

Answer the questions

There are ten questions to be answered. The questions are listed in the following section below, under the short titles corresponding to the question titles in the ISRA tool screen. Select a question below for more detailed guidelines.

For each question in the ISRA tool:

- select the question below to read the detailed guideline notes.
- in the ISRA access database, under the governance and questions tabs:
- select the abbreviated question title on the left of the screen
- follow the detailed question guideline to record the evidence you have to support your answer to this question, using the checkboxes and or the comments box
- select the answer that best represents your organisation.

Governance

- Alignment
- Staffing
- Responsibilities
- Outsourcing
- Application development and support methodology
- Logical assets
- Cloud assets
- Physical assets
- Business continuity planning
- Disaster recovery planning

Alignment

Q1. How do you know your IT systems will support the future direction of the business?

Background

The IT planning for an organisation must ensure the information systems will have the capability to support the future business strategy. The IT planning process should include a strategic requirement analysis before system or application acquisition. There should be a documented IT roadmap or future work plan setting out the ongoing effective strategic management of IT resources.

Why we are asking this question

Without strong alignment between the business and IT strategies there is a risk the information systems will not accurately support the business activities and reporting of tax obligations.

Evidence you need to support your answer

Evidence of alignment between business and IT could include yearly or multi-year strategy plan documents or IT roadmaps. In the ‘comment box’ at the bottom of the ISRA screen for this question, comment on the alignment between the IT and business strategic plans and the evidence you have.

If you have strategic plan documents record the names of those documents in the ‘comment box’.

If you have taken steps to mitigate the risks inherent with having no documented IT strategy, describe the mitigation steps you have taken in the ‘comment box’.

Possible answers

You have seven options to choose from:

- long and short term IT strategy is documented, published and regularly updated with clear synergy with long and short term business strategy. Regular updates.
- long and short term IT strategy is documented and published with clear synergy with long and short term business strategy. No regular updates.
- no documented IT strategy
- mitigated
- awaiting response
- n/a.

Selecting your answer

Select the answer that most closely represents the alignment between your IT strategy and business strategy.

Staffing

Q2. How long have your IT staff been with the business?

Background

Whilst staff turnover in the IT industry is generally higher than in other sectors, a very high turnover may be an indication of staff dissatisfaction and organisational issues. These could potentially affect the retention of knowledge and expertise within the IT department and may have an effect on business continuity.

The composition of the IT staff is also relevant, as a high reliance on outsourcing or independent contractors could be a risk for the retention of critical knowledge within the organisation.

Why we are asking this question

The ability to effectively maintain critical business systems could be compromised if there is a risk of systems knowledge being lost.

Evidence you need to support your answer

In the ‘comment box’ at the foot of the ISRA screen for this question, describe the composition and experience of your IT staff.

If you have an organisational chart relevant to your response, record the name of the document in the ‘comment box’.

Possible answers

You have six options to choose from:

- mostly employees with low turnover
- mostly employees with medium turnover or mostly long term outsourcing arrangements
- mostly employees with high turnover or mostly contractors selecting your answer
- mitigated
- awaiting response
- n/a.

Selecting your answer

Select the answer that most closely represents the situation with your IT staff composition and turnover.

Responsibilities

Q3. How are IT staff roles and responsibilities managed?

Background

All positions in the organisation chart should have a position description which clearly outlines the expected accountabilities and the qualifications and experience the incumbents should have.

There should be a proper segregation of duties in the IT functions including:

- system accesses are well governed and controlled with appropriate access authorisation matrix
- ensuring the roles that develop and maintain software cannot migrate software to the production environment
- ensuring the roles that grant access to systems cannot update data in those systems.

Why we are asking this question

Without clearly defined responsibilities, appropriate segregation of duties and suitable qualified and experienced staff, there are risks that data could be compromised or systems not properly supported.

Evidence you need to support your answer

In the ‘comment box’ at the bottom of the ISRA screen for this question, comment on the assignment of roles and responsibilities and the segregation of duties.

If you have documents that support your response record the names of the documents in the ‘comment box’.

If you have taken steps to mitigate the risks inherent with roles and responsibilities not being clearly established and documented, describe the mitigation steps you have taken in the ‘comment box’.

Possible answers

You have seven options to choose from:

- transparency & accountability, roles and responsibilities clearly established, documented and up to date; appropriate segregation of duties; accountabilities translated to staff performance and development
- transparency & accountability, roles & responsibilities clearly established and documented. Deficiencies in segregation of duties and/or no clear link to staff performance development agreements
- roles & responsibilities not clearly established or documented
- mitigated – roles & responsibilities not clearly established or documented
- awaiting response
- n/a.

Selecting your answer

Select the answer that most closely represents your allocation of roles and responsibilities.

For each question where 'mitigated' is selected you must clearly outline the reason why in the 'comments box'.

Outsourcing

Q4.To what extent do you outsource IT functions?

Background

Outsourcing is the mechanism that allows organisations to transfer the delivery of services to third parties. Fundamental to outsourcing is accepting that, while service delivery is transferred, accountability remains with the client organisation, which must ensure that the risks are managed and there is continued delivery of value from the service provider.

Outsourcing has become an increasingly standard business practice in IT as it enables economies of scale in system hosting and maintenance. However, it also brings a new set of risks and challenges for organisations. These challenges include the risk of loss of data, ownership and knowledge.

A large number of IT services from the IT help desk to IT operations can be outsourced. Outsourcing in this context is outsourcing IT functions such as data management, hardware, software hosting etc. It does not include system support as this is addressed elsewhere in ISRA.

The need to assure that services provided through outsourcing meet business requirements requires an effective outsource management process.

The internal end-users and administrators knowledge of the inner workings of each outsourced system, and its relationships with other systems, is likely to become more fragmented when more outsourcers are involved within a system landscape.

For this reason, it may be necessary to involve the outsourcer(s) in the ISRA exercise to get a more holistic appreciation of the system landscape, the integration architecture and the data flows.

For all outsourcing arrangements it is important to understand the contract between the organisation and the service provider. It is expected that all outsourcing arrangements have a clearly defined contract that sets out the terms and conditions including:

- what is being outsourced
- how the service will be provided
- who has control over the service being provided
- who has responsibility for the security of the data

- where the data is hosted
- responsibility for the data environment
- terms of the outsourcing including period of contract and cost.

Why we are asking this question

If there is extensive outsourcing, particularly with multiple providers, there are risks the systems or functions will not meet the business and user requirements if the outsourcing is not adequately managed?

Evidence you need to support your answer

In the 'comment box' at the foot of the ISRA screen for this question, describe the extent of outsourcing of your IT systems, including the details of the providers.

If you have service agreement documents that support your response, record the names of the documents in the 'comment box'.

If you have taken steps to mitigate the risks inherent with outsourcing, describe the mitigation steps you have taken in the 'comment box'.

Possible answers

You have six options to choose from:

- 0-30% systems outsourced
- 31-60% systems outsourced
- over 60% systems outsourced
- mitigated
- awaiting response
- n/a.

Selecting your answer

Select the answer that most closely represents the extent of outsourcing in your IT environment.

For each question where 'mitigated' is selected you must clearly outline the reason why in the 'comments box'.

Application development and support methodology (ADSM)

Q5. When developing new applications what methodologies do you apply?

Background

Systems development and maintenance should follow documented and controlled procedures. This question is applicable in ISRA where there is in-house developed software, customisation or vendor developed bespoke software.

Why we are asking this question

Without adherence to a controlled methodology there is a risk that applications developed for critical business functions will fail to deliver systems that perform accurately and reliably and will meet the schedule of business requirements.

Evidence you need to support your answer

In the 'comment box' at the bottom of the ISRA screen for this question, describe your development and support methodology, including the details of the methodology providers if appropriate.

If you have vendor agreement documents that support your response record the names of the documents in the 'comment box'.

Possible answers

You have five options to choose from:

- proven methodology - document standards & procedures - clear milestones
- new methodology - uneven documentation - clear milestones
- no/poor methodology - poor documentation - unclear/changing milestones
- awaiting response
- n/a.

Selecting your answer

Select the answer that most closely represents the nature of your methodology.

Logical assets

Q6. How do you monitor and manage access and security of your logical assets?

Background

A documented access policy and procedure is required to ensure appropriate access to your systems and data repositories. System passwords should be strong and users should be prompted to change their passwords regularly.

Biometric devices offer the added security of authentication (which aims to ascertain that users are who they say they are) in addition to the usual authorisation process that simply checks that the user logging in has adequate security access to perform a particular function within the system.

Terminated employees should have their system access revoked in a timely manner after they have left the company.

Why we are asking this question

If access to your information systems is not adequately controlled there is a risk inadvertent or malicious access could prevent the systems meeting their business objectives and reporting obligations.

Evidence you need to support your answer

In the comment box at the foot of the ISRA screen for this question, outline your logical access controls.

If you have documents that support your response record the names of the documents in the comment box. These could be policy and procedure documents, user access mapping lists or monitoring reports.

Possible answers

You have five options to choose from:

- good access control over logical assets - comprehensive access policy, formal user administration procedures enforced, biometric and or strong passwords control access to all systems, administrator and user access to systems is regularly checked, automated monitoring
- medium access control to logical assets - some deficiencies identified in some systems or some circumstances (eg terminated employees)
- poor access control - many deficiencies identified systemic lack of control, inadequate or absence of access control procedures awaiting response
- n/a.

Selecting your answer

Select the answer that most closely represents the status of your logical access controls.

Cloud assets

Q7. How do you manage access and use of your cloud assets?

Background

A documented access policy and procedure is required to ensure appropriate access to all cloud systems and or data repositories. Cloud access passwords should be strong and users should be prompted to change their passwords regularly.

Terminated employees should have their system access revoked in a timely manner after they have left the company.

Why we are asking this question

If access to your cloud based systems and data is not adequately controlled there is a risk inadvertent or malicious access could prevent the systems meeting their business objectives and reporting obligations.

Evidence you need to support your answer

In the ‘comment box’ at the foot of the ISRA screen for this question, outline your cloud access controls. Include a description of the formal user access administration procedures and how they are enforced.

If you have documents that support your response record the names of the documents in the ‘comment box’. These could be policy and procedure documents, user access mapping lists or monitoring reports.

Possible answers

You have five options to choose from:

- food access control over cloud assets - comprehensive access policy and formal user administration procedures enforced, strong passwords control access to all systems, administrator and user access to systems is regularly checked, automated monitoring

- medium access control over cloud assets - some deficiencies identified in some systems or some circumstances e.g. terminated employees, contractors
- poor cloud control - Many deficiencies identified systemic lack of control, inadequate or absence of access control procedures
- awaiting response
- n/a.

Selecting your answer

Select the answer that most closely represents the status of your cloud access controls.

Physical assets

Q8. How do you manage and monitor access to your physical assets?

Background

Documented policies and procedures are required to ensure appropriate access to your buildings and restricted areas related to your information systems.

Buildings and computer control rooms should be locked or in some way secure and employees should be easily identified.

Why we are asking this question

If access to your physical infrastructure is not adequately controlled there is a risk inappropriate access could result in damage to the infrastructure or bypassing of controls to logical assets.

Evidence you need to support your answer

In the ‘comment box’ at the foot of the ISRA screen for this question, outline your physical access controls.

If you have documents that support your response record the names of the documents in the ‘comment box’. These could be policy and procedure documents, user access mapping lists or monitoring reports.

Possible answers

You have five options to choose from:

- good access control over physical assets - comprehensive facilities access policy and formal access administration procedures, enforced biometric controls and or strong access control to all facilities, access to facilities is regularly checked, automated monitoring
- medium access control over physical assets - some deficiencies identified in some systems or some circumstances eg terminated employees, contractors
- poor access control over physical assets - many deficiencies identified, systemic lack of control, inadequate or absence of access control procedures
- awaiting response
- n/a.

Selecting your answer

Select the answer that most closely represents the status of your physical access controls.

Business continuity planning (BCP)

Q9. Do you have a business continuity plan that sets out what is required to support your operations in the event of a disaster?

Background

A business continuity plan is an enterprise wide group of processes and instructions to ensure the continuation of business processes in the event of an interruption. It provides the plans for the enterprise to recover from minor incidents (eg localized disruptions of business components) to major disruptions (eg fire, natural disasters, extended power failures, equipment or telecommunications failure). The plan is usually owned and managed by the business units and a disaster management or risk prevention function in the enterprise

This question aims to assess the adequacy of business continuity planning (BCP) in case of major business disruptions. BCP involves planning and procedural aspects, encompassing emergency response, crisis communications, business continuity and disaster recovery.

Disaster Recovery Planning (DRP) is the component of BCP that focuses on the continuity of information and communication technology systems that support business functions.

Organisations should have a documented business continuity plan which is available to key staff to access in times of incident to ensure that the business can maintain business activities when there are emergencies or disruptions. The BCP should be tested at regular intervals to ensure it is still adequate for the organisation's circumstances.

Identifying the communication channels that should be adopted in case of emergency is also very important to ensure that staff are aware of who is to give them instructions in case of emergencies when the normal line of commands no longer apply.

The focus of the BCP for the purpose of the ISRA is:

- back-up procedures
- redundancies of back-up systems
- backup data stored in an alternative location to minimise the risk of accidental destruction
- process to capture business information while the systems are unavailable
- process to enter information into the information systems when the systems are restored
- offline servers operating while servers are being restored.

Why we are asking this question

The availability of the information systems may be critical to your ability to continue to meet your business objectives, reporting and regulatory obligations.

Evidence you need to support your answer

In the 'comment box' at the bottom of the ISRA screen for this question, describe the status of your business continuity plan, including test schedules and results.

If you have BCP documents that support your response, record the names of the documents in the 'comment box'.

If you have taken steps to mitigate the risks inherent with an inadequate BCP, describe the mitigation steps you have taken in the 'comment box'.

Possible answers

You have six options to choose from:

- documented BCP, regular BCP training for identified staff, BCP key measures have been tested
- documented BCP but no specific BCP training, BCP key measures have not been tested
- unsound or non-existent BCP
- mitigated
- awaiting response
- n/a.

Selecting your answer

Select the answer that most closely represents the status of your business continuity plan.

For each question where 'mitigated' is selected you must clearly outline the reason why in the 'comments box'.

Disaster Recovery Planning (DRP)

Q10. Do you have a document that sets out what and who is responsible to get your systems back online in the event of a system failure?

Background

This question aims to assess the adequacy of the plans for recovering the IT infrastructure and business data in the case of a disaster. Forming part of the BCP it may include back-up procedures, redundancy of business applications and alternative sites or facilities. The DRP should be tested at regular intervals to ensure that it works as intended and is effective.

Organisations should have a documented disaster recovery plan which identifies the alternative sites and facilities that will be used when the normal facilities become inoperable. Facilities covered are likely to include power generation, computer systems, networks and end user workstations.

Where systems are outsourced, this will refer to the service provider's DRP but must also cover local facilities.

Why we are asking this question

In the case of a disaster affecting your information systems, your disaster recovery plan is likely to be dependent on your ability to recover or switch to alternative systems infrastructure and data.

Evidence you need to support your answer

In the 'comment box' at the foot of the ISRA screen for this question, describe the status of your disaster recovery plan, including test schedules and results.

If you have DRP documents that support your response, record the names of the documents in the 'comment box'.

Possible answers

You have six options to choose from:

- documented DRP, alternate operations sites identified, emergency communication channels identified, redundancy inbuilt in systems and data centres, and regular scheduled backups, regular DRP training/briefing.
- documented DRP but deficiencies identified in some aspects, DRP key measures have never been tested.
- unsound or non-existent DRP
- mitigated
- awaiting response
- n/a.

Selecting your answer

Select the answer that most closely represents the status of your disaster recovery plan.

Risk mitigation

Your answers to the ISRA questions may lead to a high or medium risk rating in some areas. In general this may be due to:

- there are inherent risks because of the nature of your systems, infrastructure or support arrangements eg ISRA results will show a higher risk for outsourced systems than systems managed in-house
- controls are weak or are not being applied diligently and consistently.

Where the risks are inherent there may be little you can do to remove the risk. However, the risks can usually be mitigated with good controls that are applied and monitored. This will not change the ISRA rating, but the rating can be accepted with the understanding of the controls in place.

If controls, or the application of controls, are weak the solution generally is to put stronger controls in place or more rigorously apply the existing controls. This can lead to a lower risk rating in a subsequent ISRA.

The most appropriate risk mitigation strategies will depend on your particular circumstances but for some general guidelines you may look at risk mitigation strategies we have provided for each question.

Systems inventory

Some examples of situations leading to a high or medium systems inventory risk rating could include:

Inherent risks

- in-house or jointly developed systems
- mixed in-house and external support
- high percentage of staff able to change system data
- underlying database system is not robust
- application is new
- system is critical.

Controls weaknesses

- service level agreements not in place or not monitored
- auditing software turned off or not monitored
- weaknesses identified in prior audits
- systems documentation out of date.

Medium or high risk – what you can do to reduce the risk

Nature of application package

You will get a higher risk rating when your staff are responsible for the development and or maintenance of the system. You can reduce the risk by moving to a purely vendor developed and maintained system.

Where this is not possible you need to apply rigour to the testing and documenting of system implementations and changes. You also need a strong support and succession plan to ensure key support personnel are available, skilled and familiar with the system.

System support

The risk rating will be higher where the support arrangements are ineffective or there are mixed responsibilities which could lead to issues with confusion over roles.

With external support, risk can be mitigated by engaging a reputable support provider, establishing strong and well detailed service level agreements and performance monitoring against the agreement to help focus on areas needing improvement.

A service level agreement would be expected to include:

- clearly documented roles and responsibilities
- clearly defined service deliverables
- performance measures and remedies if these measures are not met.
- expectations of service delivery timeframes
- maintenance arrangements and update expectations
- regular governance/incident reporting
- start and end date of the agreement and review and renew arrangements
- key contacts or personnel.

User base

To reduce the risk:

- review the requirements and access matrix for staff to have administrator access authorisation that allows them to change critical data
- remove authorisations where they are not required
- consider a documented authorisation matrix to ensure good governance and oversight is maintained.

Audit software

If an auditing capability is available in your system but not activated, you can reduce the risk by turning it on and regularly monitor the results.

If your system does not have an auditing capability, consider installing standalone auditing software that can perform similar monitoring functions according to user-defined rules.

Database

If you have a high risk rating it is unlikely you can change the database technology within the current application system. You may have high risk ratings from other ISRA questions and may consider a system replacement or major upgrade to a lower risk overall technology.

Software delivery

The risk is least where you have a strong and well detailed service agreement with a reputable provider to maintain your software. Where this is not possible you can reduce the risk by establishing processes and an authorisation matrix with clearly defined targets and responsibilities, including rigorous testing and approval steps.

Infrastructure

The ISRA tool rates infrastructure as a service (IaaS), which is cloud based, as the lowest risk due to factors such as scalability, resource balancing and redundancy. Cloud infrastructure hosting (public or private) can be scaled as quickly as needed without the organisation having to place strain on internal resources to manage the server acquisitions, implementation and redundancy requirements. This also allows internal IT staff to focus on other initiatives.

If you have a high risk rating, outsourcing to a reputable service provider will reduce the risk where supported with a strong and detailed service level agreement. If this is not feasible the establishment and monitoring of internal service level agreements could help in ensuring the in-house service providers support the infrastructure adequately.

A service level agreement would be expected to include:

- clearly documented roles and responsibilities
- clearly defined service deliverables
- performance measures and remedies if these measures are not met
- expectations of service delivery timeframes
- maintenance arrangements and update expectations
- regular governance incident reporting
- start and end date of the agreement and review and renew arrangements
- key contacts and or personnel.

Prior audit findings

You will have the highest risk rating if you do not have any history of recent audits. This can be addressed by establishing an IS audit program, preferably conducted by a reputable external party.

If your recent IS audits have revealed more than minor weaknesses the auditing body should have provided recommendations for addressing the risks. Implementing those recommendations should reduce the likelihood of significant issues being found in future IS audits.

Maturity of application

The risks inherent in a newly implemented system are mitigated as:

- users become more familiar with the system and its functionality
- processes are developed to support users
- clearly defined roles and responsibilities surrounding the application are created.

Your implementation schedule should address these factors and expedite the progress to a more stable system.

If your system is old you have different risks through potential obsolescence. If the system is externally supported you should be applying provided upgrades and monitoring the vendor's plans for the life of support program.

Older in-house systems require continual monitoring to ensure you maintain the capability to support the system and to ensure upgrades are planned and implemented to maintain currency with changing business and regulatory requirements.

Data reconciliation

You should use the full capabilities of your system for audit trail and data reconciliation, supported by strong monitoring and exception response procedures.

Documentation

If required documentation does not exist and the system was developed and is maintained by the vendor discuss documentation with the Vendor, as they should have documentation available. If there is no vendor developed and maintained documentation then speak to the vendor and ask for it to be developed. Outdated documentation should be upgraded.

If there is significant documentation work to be done for in-house developed and maintained or customised systems a project could be established and monitored to create the documentation.

Procedures should be established to ensure documentation remains current for future changes to the system. Where a large number of documents are required, consider creating a system documentation gatekeeper role to ensure that documentation is updated as the system is changed.

Criticality

Develop strategies for continuing critical business functions when the system is not available. This is covered in more detail in auditable Unit 5 question 9 – business continuity planning. Generally where a system is sensitive or vital it is expected there will be appropriate controls and governance in place to mitigate the risk. This could include a prioritisation matrix, incident reporting and onsite generators for back up.

System interfaces

Some examples of situations leading to a high or medium interfaces risk rating could include:

Inherent risks

- complex interface
- manual intervention required in interface
- automatic exception handling not built into interface.

Controls weaknesses

- poor monitoring of exceptions
- interface documentation out of date or non-existent.

Medium or high risk what you do to reduce the risk

Complexity

If your interface is very complex you will have a high risk rating. Due to the systems' requirements it may not be realistic to simplify the interface but you can concentrate on the management controls and governance over the interface.

Method

Automation of the invoking and operation of the interface will lower the risk rating. Your aim should be to remove any human intervention in its normal operation.

Exceptions

You can reduce the risk of interface errors by building in automated steps to resolve the data after transfer and even do pre-processing validation before the transfer. The validation must be supported by effective reporting and escalation of exceptions and processes to respond to exception situations.

Documentation

Where required documentation does not exist it should be developed and include full details of the interfacing including any data mapping codes. Outdated documentation should be upgraded.

Procedures should be established to ensure documentation remains current for future changes to the system. Consider creating a documentation gatekeeper role to ensure that documentation is updated as the interface is changed.

Customisations

Some examples of situations leading to a high or medium customisations risk rating could include:

Inherent risks

- extensive customisation
- customisation is still new
- customisation was done in-house or by party who does not maintain it.

Controls weaknesses

- maintenance parties do not have good understanding of the customisation
- customisation documentation out of date or non-existent.

Medium or high risk – what you can do to reduce the risk

Extent

Extensive customisation of the system may have been required to meet business needs. Recognising this you should have strong governance and controls over the customisation development and ongoing support of the customised system. This may include:

- developing and monitoring service level agreements if the customisation is maintained by the system vendor or a third party
- maintaining up to date documentation of the customisation specifications
- developing comprehensive test scripts and engaging stakeholders in acceptance testing during development and ongoing maintenance.

Maturity

If the customisation is relatively recent, comprehensive structured testing can reduce the risk that issues have been introduced into the system by the customisation. Development of good documentation will help to manage the stability of the customised system during future upgrades.

Ownership

The risk rating will be higher when the vendor of the system has not developed the customisation and is not responsible for its ongoing maintenance. Without the vendor's clear ownership, emphasis must be placed on strong controls over the general governance of the customisation, including documentation of specifications, thorough testing using defined test scripts and sign off by the business users before implementation.

Documentation

Comprehensive documentation should be developed. It should cover at least what components have been customised, how the customisation was done, any coding requirements and any interface linkages to other systems. The documentation should be updated whenever the customisation is changed or there is a change to systems interfacing with the customisation. Changes to the documentation should be managed with appropriate version control.

Projects

Some examples of situations leading to a high or medium projects risk rating could include:

Inherent risks

- high project cost relative to administration costs
- extensive changes to business processes
- inexperienced staff or staff not dedicated to the project
- new technology or technology not widely used
- poor project methodology.

Controls weaknesses

- methodology not strongly adhered to

- poor documentation
- stakeholders not engaged
- no post implementation review.

Medium or high risk – what you can do to reduce the risk

Costs

If the costs of your project are high it is likely there will be significant changes to your systems, infrastructure or business processes. These changes create the risk of errors or omissions in operations related to your tax liabilities and reporting. You can help to reduce this risk with strong project planning, thorough testing and good controls.

Process changes

The risk to the accurate functioning of your systems is greatest when the project results in significant changes to the business processes that use those systems and the requirements on staff who are involved in the processes. You can help to reduce this risk with strong project planning, thorough process testing, good staff training and controls.

Project team

You can reduce the risks by using experienced and dedicated project staff, supported by external specialists as required. If the team includes externals your project plan should include clearly documented roles and responsibilities to ensure essential systems knowledge is transferred to staff that will be available for future modifications to the systems and processes.

Technology changes

Use of established and widely accepted technologies will reduce the risks inherent in new technologies. If new technologies are used the project plan must include rigorous testing to ensure the technologies are performing as required, and strong controls and governance applied.

Methodology

If you have a high risk rating because you are not using a proven methodology, you could consider enhancing the project with the use of a reputable methodology. One of the most widely accepted project management methodologies for IT systems implementation and or development is PRINCE (Projects in Controlled Environments).

PRINCE is a registered trademark of the Office of Government of Government Commerce (OGC), an independent office of HM Treasury of the United Kingdom.

PRINCE is a process driven project management method which contrasts with reactive or adaptive methods. PRINCE defines 45 separate sub-processes and organises these into eight processes.

Stakeholders

If they are not there already, activities may be included in the project plan and schedule to encourage engagement. These may include stakeholder reviews and sign-offs before further stages of the project may proceed. For end user engagement you may include various publicity and feedback options, such as newsletters, roadshows and forums.

Post implementation review (PIR)

You may conduct a review if you have a high risk rating because a review has not been conducted.

If you have a high risk rating because of issues found in the review you may need to plan, schedule and conduct activities to address the issues.

Governance

Some examples of situations leading to a high or medium governance risk rating could include:

Inherent risks

- reliance on short term or contracted staff
- systems outsourced.

Controls weaknesses

- IT strategy not developed in alignment with business strategy
- roles and responsibilities not clearly established
- poor application development methodology
- poor access controls over logical, cloud or physical assets
- business continuity plan is non-existent, not sound or not tested
- disaster recovery plan is non-existent, not sound or not tested.

Medium or high risk rating - what you can do to reduce the risk

Alignment

A high risk rating indicates you do not have up to date and closely aligned documented strategies for the business and IT. The risk can be reduced by updating or developing the strategies, then ensuring they guide the further development of your information systems.

Staffing

Establishing strong controls and good documentation of systems and work flow processes will assist in retaining knowledge within the IT department, even with changing staff. Measures to retain staff, internal or external, familiar with the systems will also reduce the risks.

Responsibilities

The risks will be reduced if you clearly define staff roles and responsibilities, ensure staff are adequately skilled and experienced for their positions and set up authorisations to ensure appropriate segregations are enforced.

Outsourcing

If you have a high risk rating you are probably using outsourcing for good business reasons; and the level of control and governance would be expected to be higher in recognition of the risk. You can reduce the risks by:

- ensuring strong controls and governance are in place to manage the outsourcing
- ensuring the outsourcing agreements are well managed and monitored

- regularly reviewing the alignment between the services provided and the business needs.

Application development and support methodology (ADSM)

Examples of sound application development include:

- the thorough documentation of all system requirements in a user requirements statement or similar document that will list all the desired system features and rate them in order of importance
- the systematic capture of all features, configuration options and processing logic of the system in a version-controlled system design document.

Examples of sound application maintenance include an established schedule for the migration of patches into production systems and an established workflow for the approval of such patches following appropriate testing.

Logical assets

Strengthening, enforcing and monitoring your logical access controls through on-boarding and off-boarding policies and processes, and regular audits will reduce risks.

Cloud assets

Strengthening, enforcing and monitoring through a strong on-boarding and off-boarding policy and regular audit of your cloud access controls will reduce risks.

Physical assets

Strengthening, enforcing and monitoring through regular audits of your physical access controls will reduce risks.

Business continuity planning (BCP)

The risks from a non-existent or inadequate BCP can be reduced by developing, documenting and testing a strong BCP and training staff in its use.

Disaster recovery planning (DRP)

The risks from a non-existent or inadequate DRP can be reduced by developing, documenting and testing a strong DRP and training staff in its use.

ato.gov.au