TAHO
Tasmanian Archive + Heritage Office

Information Management Advice 60 - Part 4
Identifying information risks that impact- high risk business

High risk business areas in each agency should be priorities for information management activity, in order to identify and mitigate any information-related risks these business areas might face. This advice defines common and specific information risks; articulates strategies for identifying areas of business which face information risk; and provides mitigation strategies and case studies for dealing with information risk.

1. Defining information risks

Information risks are related to, but distinct from, technology risks. Information risks are those risks which relate to the inherent characteristics and value of information. The threat and impact of information risks are significantly increasing. Common information risks that could be occurring in high risk business areas include:

- information that cannot be generated in a useable form
- information that cannot be maintained in a useable form
- information that is incomplete
- information that is meaningless
- information that cannot be trusted
- information that cannot be authenticated
- information that is inaccessible
- information that does not survive for as long as it is needed by the business area
- information that is overwhelming, unmanaged, and inhibits rather than enables business process.

Information risks can hamper government business and accountability, particularly when these risks occur within high risk areas of business operations.

Information risks are different to the risks that are assessed and mitigated in business continuity planning processes. Business continuity planning builds processes to ensure that agencies are able to re-establish themselves as quickly and comprehensively as possible after a disaster. Separate processes need to be established to identify and mitigate information risks in high risk areas of business.

2. Identifying high risk areas of business

Areas in your Agency that perform core, strategic, highly accountable or high value business operations are likely to be classed as high risk business. Because these areas are likely to be performing key aspects of government business, it is critical that good information exists to account for and support these operations, in both the short and long term.

Other areas of high risk business that need to be identified and assessed are areas undergoing significant transition. In these areas, it is possible that traditional processes are changing, new technologies and services are being adopted and information itself is changing or disappearing, potentially placing your business at risk. To identify high risk areas of business in your Agency you can:

- identify areas that perform core, strategic, highly accountable or high value business operations
- use your Agency's corporate risk register to flag existing areas of identified corporate risk
- look at business areas that are adopting a lot of new technologies and services
- focus on business areas under transition
- focus on areas adopting BYOD (bring your own device) approaches
- talk to managers and staff about any information-related concerns they may have in their specific business areas.

After identifying areas of high business risk, you should then identify what information is required to support these business areas.

3. Know what information is needed to support high risk business processes

To know what information is needed to support your business, you can:

- talk to staff – what information do staff working in high risk business areas say that they need to support their business? Is this information readily available to them? Can they readily find, understand, access and use all the information they need to do their job in both the short and medium term?
- look at the authorised retention and disposal schedules that apply to this business area for an indication of the type of information required to support this business
- look at legislation and standards that apply to the high risk business area, as legislation and standards are often very specific in terms of the records you need to keep and the information that these records need to contain
- look at quality controls or procedure statements that say what records need to be created from specific processes. Are these records being created? For example, if the internal business procedures for case management say that 'a record must be kept of each action in a case in the Case Management System, including the date of the action and who approved it', does your case management system actually do this?
- understand corporate accountability controls and reporting requirements. Is the information required to support these available, meaningful and useable in these business areas?
- understand business needs for information dissemination and sharing. Are these possible in high risk business areas?
- identify the information needed to support clients, projects and cases in the short and medium term. Is this information accessible, useable and accountable for the periods of time required to support these business needs?
- examine the data, metrics and analysis that is required to account for the performance and operation of certain business operations. Can this be gathered, sustained and shared by the business in the short to medium term?

These and other consultative mechanisms will help to identify what your business area's specific information needs are.

4. Know the technology used to support high risk business areas

Understanding business operating environments is critical to understanding and developing strategies to mitigate information risk. This involves understanding whether your high risk business areas are using:

- cloud-based service offerings
- BYOD
- social media
- collaborative environments such as SharePoint, wikis, Google Docs or Office 365
- complex datasets as the basis for decision making
- systems including legacy applications
- large uncontrolled network environments
- personal storage networks
- diverse applications to perform different aspects of their operations
- backup systems as information storage environments.

Knowing the environments where high risk business is performed will help you to plan and implement strategies to mitigate your specific information risks.

5. Determine whether necessary business information is being impacted by information risk

Once you have an understanding of the information that your high risk business areas need and the technological environments where the business is performed, you can then determine whether the information required to support business is:

- still being generated in a useable form, and still being maintained in a useable form
- now incomplete and therefore not meeting business needs
- losing its meaning and can no longer be used to meet business needs
- being impaired and now cannot be trusted
- unable to be authenticated and is therefore unreliable for business or client needs
- inaccessible and cannot be found and used
- not surviving for as long as it is needed by the business area

6. Examples of Emerging Business issues and possible risk mitigation strategies

With the transitions that are occurring in business environments, many issues can impact on business information. Here are some of the problems which may be occurring in your agency and the possible solutions to them.

Changes to government services

Problem: Evolving business and service environments do not support information accountability requirements

Example:

- Outsourcing of government business process without proper consideration of the recordkeeping accountability built into the outsourcing contract.

- Outsourcing of government business without staff in the business area understanding their changing role in ensuring the service provider is accountable, and transitioning their role from one of direct service provision to policy development, performance review and accountability checks of the service provider
- Procurement of business service from cloud hosted service providers

Mitigation:

- understand where high risk/high value business in your organisation needs to be supported by strong accountability management
- define where metadata that tracks actions, responsibilities, outcomes and accountabilities must be deployed and supported through system transition and maintenance
- ensure accountability requirements can be applied and sustained in cloud service arrangements if high risk/high value business processes move to cloud environments

Problem: Increased use of social media, applications, BYOD, email and other diverse business platforms create an inability to track, use and share consolidated client, project or process information, leading to incomplete and untrustworthy information

Example:

- Implementation of BYOD, social media, Whole of Government (WoG) email, specific services provided in the cloud.

Mitigation:

- understand the information that is required for effective service delivery and know the diverse environments where this information is located
- understand the impacts to business and information flows when business delivery or client service mechanisms are changed, such as when community engagement or consultation exercises move to social media channels and away from more traditional business pathways
- implement tools or utilise workflows to consolidate all business information required for informed decision making or effective client management, and to minimise service duplication
- monitor the adoption of new systems, services, applications and processes to identify and manage changes that will impact on business information

Problem: Incomplete or partial data migrations do not carry all necessary business information from one system to another, and result in information that is no longer be trusted for client service or business arrangements

Example:

- System refresh projects do not migrate all data

Mitigation:

- prior to migration, comprehensively understand the high-value information that is required to support and account for ongoing business operations
- ensure that sufficient metadata for the integrity, understanding and accountability of that information is built into migration arrangements
- build these high-value information and metadata needs into procurement processes to ensure that new systems can bring in exported information and sustain the information needed by business operations

- if migration is not possible, fully assess, understand and accept the business and accountability impacts of not migrating legacy information to new operational environments by documenting them in risk assessments and alerting management

Problem: Cloud services do not sustain or export all necessary business information, leading to incomplete and untrustworthy business information

Example:

- Migration from agency systems to purchased business specific service in the cloud where only current data is migrated

Mitigation:

- ensure functionality for information portability, including metadata is built into contractual arrangements or that alternative arrangements are identified where the agency purchase consumer applications in the cloud where this is possible
- ensure the right to withdraw information, including metadata, is built into contractual arrangements
- if the service has limited data export functionality, ensure that it can export the information and metadata to support the integrity, understanding and accountability of high value information
- understand any standard data purge arrangements that may be applied by the service provider
- identify when high risk/high value business information is moving to the cloud and identify the accountability safeguards that are necessary to ensure this information can be trusted and accessible for as long as it is required by your business operations

Problem: Staff use a variety of uncontrolled business and data storage environments that result in limited information accessibility, no consolidated view of a project or client, and information that cannot be trusted for client service or business arrangements

Example:

- Agency has no policy and process for the management and control of information storage. Various storage environments exist, network drives, SharePoint, records systems, legacy systems, and service provided in the cloud.

Mitigation:

- foster a good corporate understanding of the information required to support high risk/high value business processes
- ensure staff understand the processes and systems needed to create and manage comprehensive and accurate business information
- do not allow isolated data silos to proliferate
- ensure staff share and use clear metadata to identify definitive versions of reports and other business information, by defining records naming conventions and identifying minimum metadata requirement mapping these requirements to each of the storage solutions

Uncontrolled IM environments

Problem: Volumes of uncontrolled data overwhelm storage environments and result in inaccessible data lost within the 'noise'

Example:

- Agency has no policy and process for the management and control of information storage. Various storage environments exist, network drives, SharePoint, records systems, legacy systems, and service provided in the cloud.
- Agency does not have an active record disposal program.

Mitigation:

- routinely dispose of information that is authorised for destruction
- develop procurement processes that implement systems with the capacity to identify and protect high value information, and apply separate management and authorised disposal processes to information that is authorised for destruction For example, build into the system the capacity to flag certain records types and remove the records/ information from the system using a disposal process. If this is not possible then flag that this information will need to be disposed of during system refresh and migration processes.
- as the costs of uncontrolled data volumes in these environments can quickly become unsustainable, ensure cloud services are established with the capacity to routinely dispose of information that is authorised for destruction, but are concurrently able to maintain information that has an ongoing business use and value. This is unlikely to happen where there are no contractual arrangements in place. Agencies may need to put in place a manual processes with an assigned accountable officer to remove data due for destruction

Problem: Staff use a variety of ad hoc or personal environments for business processes and data storage which results in siloed and inaccessible business information

Example:

- Agency has not policy and process for the management and control of information storage. Use of home drives, personal drives, sticks and portable hard drives is permitted and not controlled by policy, process or IT controls

Mitigation:

- understand where staff are performing high risk/high value business operations and build strong information governance frameworks into these environments to enable good information management to occur for high risk/high value business operations
- foster a good corporate understanding of the information required to support high risk/high value business processes
- develop and deploy change management strategies and training to maintain an organisational culture which values information management
- ensure appropriate policy, process and IT controls exist for the storage of corporate information
- when staff performing high risk/high value business operations leave the organisation, ensure exit processes cover information management issues to ensure appropriate information continuity and accessibility

Problem: Use of backup systems for storage of long term value business information is risking long term information accessibility

Example:

- Agency considers backups systems appropriate for archiving high value, high risk information and do not understand the limitations of this technology in terms of long term accessibility

Mitigation:

- understand that information within backup systems is hard and costly to access and that within a 3-5 year period, will result in information inaccessibility
- ensure backup systems are not used for the storage of long term and high value business information
- understand specific business and organisational needs for information longevity and continuity, and develop more appropriate information storage strategies in these environments
- identify where in your organisation backup systems may be being used as default information management environments, and plan for more appropriate strategies to be put in place

Problem: Business environments and management decisions do not support information access and reuse

Example:

- Systems and services are procured by the agency without an assessment of the system or service capability to manage information for its required retention and governance

Mitigation:

- know the information that is required to support ongoing high risk/high value business in your organisation, and ensure this information is supported and protected
- plan transitions well so that all necessary information components of a case, project or transaction are connected, sustained and supported through system change
- plan transitions well so that information and its supporting metadata can be as robust and unchanged as possible through the transition process
- ensure contracts with service providers enable information to be portable and sustained in useable and accessible formats
- use metadata to enhance accessibility to business information and enable information understanding, authentication and sharing
- document system structures, data dictionaries, core architecture and system rules that are necessary to understand how a system operates and manages business processes. This documentation will be necessary to support system transitions, and to enable meaningful access to and understanding of information generated by the system

Lack of corporate governance over business systems

Problem: Systems are adopted that do not support information retention and longevity

Example:

- No active information governance of systems and service procured by the agency
- Systems and services are procured by the agency without an assessment of the system or service capability to manage information for its required retention and governance period

Mitigation:

- build good information retention capacities into system design, procurement or configuration processes
- in the development of cloud or outsourcing contracts, include requirements concerning the sustainability and portability of information that needs to be kept for long periods of time, or periods beyond the specified contract period including about strategies for extraction/export & return to owner

Problem: Lack of corporate and business awareness of the need to keep some high risk/high value information after its active business use ceases

Example:

- No active information governance of systems and service procured by the agency
- Systems and services are procured by the agency without an assessment of the system or service capability to manage information for its required retention and governance

Mitigation:

- use authorised retention and disposal schedules, legislative mapping and Information Asset Registers to understand the business, client, community and/or legislative drivers that apply to the information in different areas of organisational operations, and the different retention periods that apply to them
- build awareness so that once active business projects or cases close, there is an awareness that the information about these is kept as usable and accessible information for the required periods of time
- understand the diverse systems that are used across the organisation to perform key business operations, and understand that information loss in one of these systems may impair operations or accountabilities in other systems
- ensure that critical information / data sets and their dependencies across the organisation are documented, and that the technology dependencies of these information / datasets are documented
- build awareness of retention requirements into system migration plans so that necessary information can be supported through system transitions

Problem: Poor corporate governance inhibits strategic information management

Example:

- Agency does not have an executive approved records management strategy outlining the agency strategic management of records and information

Mitigation:

- promote a broad corporate understanding of the high risk/high value information generated and needed by your organisation
- deploy change management strategies and training to develop an organisational culture which values information management
- develop or procure systems which enable defined management pathways for short and long term value information
- routinely dispose of information that is authorised for destruction
- strategically identify, protect, manage and utilise long term value business information

7. Determine appropriate information risk mitigation strategies

There are many potential strategies you can adopt to mitigate information risk. Key points at which you can mitigate information risk are:

- in the implementation of strong information governance frameworks
- at system specification, design and configuration
- at system transition.

If it is not possible to address information risks at these points, you may be able to undertake remedial actions to mitigate information risk.

Examples of risk mitigation through strong information governance frameworks

- promote a broad corporate understanding of the high risk/high value information generated and needed by your Agency
- communicate specific information management requirements applying to high risk areas of business to staff, management, ICT, contractors
- deploy change management strategies and training to develop an Agency culture which values information management.
- assigning individual (and collective) accountability via Information Governance Framework including appropriate performance management measures

Examples of possible risk mitigation strategies at system specification, design and configuration

- promote information governance by design as a strategy to ensure your information management requirements for high risk business areas are supported in system specification, procurement, design and configuration
- build awareness of information retention requirements into any new system design or development processes
- when cloud offerings are being investigated, ensure corporate information needs are included in all appropriate service assessments and decision making processes

Examples of possible risk mitigation strategies at system transition

- facilitate effective cloud transitions by ensuring services are selected for high risk areas of business that enable data portability, and the application of desired information management processes
- identify where high risk business processes and service delivery are moving to social media environments, and develop information management strategies to help manage, improve and account for these services
- when systems supporting high risk business are migrated, ensure all information that is required to support long term business needs is carried successfully through system transitions
- when systems supporting high risk business are migrated, determine whether any information has been orphaned or made legacy because it was not able to be transitioned to new business environments. If so, determine whether any strategies need to be put in place to ensure the ongoing monitoring and management of this legacy information to ensure its continuing accessibility for as long as business needs to access it, taking into account public access requirements

- when systems supporting high risk business are migrated, ensure all metadata that brings meaning and accountability to business information is migrated and maintained alongside the information it relates to
- if new systems have completely transformed the nature of the information generated to support business, determine whether these new information formats or structures are continuing to meet business needs and whether they can be maintained for as long as the Agency needs to keep and access the information.

Examples of possible remedial actions to mitigate information risk

- if new systems keep only dynamic data and have no capacity for maintaining information in the medium to longer term but a business need exists for this information, develop alternate mechanisms for making and keeping required business information
- if information that is required to support long term business needs has been moved to cloud environments, ensure planning processes are initiated to ensure this information is supported and maintained and re-transitioned if required so that it continues to be available for business use
- where local or cloud-based collaborative tools have been deployed, investigate where high risk/high value information may be being created in these environments and determine whether strategies are necessary to ensure this information can be securely managed and maintained in these environments for as long as it is required
- implement effective record disposal programs to appropriately destroy time-expired business information, and to focus corporate attention on the management of high risk/high value business information

8. Case studies of mitigating information risk and supporting high risk business

Please note, the following scenarios are fictional examples to illustrate possible mitigation strategies and should not be relied on as providing comprehensive advice.

Example: Assessing the information management needs of a high risk business area

Some councils have traditionally provided child care services. To assess information requirements for a high risk area like child care you could start by:

- looking at relevant legislation like Childcare Act 2001 which contains significant recordkeeping requirements, identifying a wide range of records that must be kept about childcare services and specifying how long many of these need to be kept for
- looking at (General Retention and Disposal Schedule) DA 2200, Local Government which in identifies some of the records that should be kept about childcare services
- talking to childcare staff and those who manage the administrative areas of childcare – what information do they want and need in order to do their work effectively and accountably?

Using these and any other sources you think appropriate, a list of necessary records will start to emerge:

- childcare licenses
- certificates of registration
- emergency plans

- public liability insurance
- records of all registered children including medical records
- records of child attendance and excursions
- records of complaints
- responses to complaints
- reports of complaints to relevant authorities
- probity checks of staff
- records of staff qualifications
- records of staff first aid training
- records of staff attendance
- signed visitor registers
- records of all programs offered by the service
- records of daily timetables
- a developmental record for each child
- a weekly record of the service etc.

To assess whether your processes and systems are supporting these identified information requirements, you should assess whether all the information you have identified is actually being made and kept, and also kept in accordance with business, legal and any appropriate security requirements you have identified.

This means you need to look at business areas and systems and assess whether all the information you need is there and kept in a way that enables it to be used and maintained. It is important to remember that high risk business operations often have long retention requirements, meaning that the records produced in these areas legally often have to be kept for very long period of time. For example, childcare records about children at a childcare service have to be kept until the children reach the age of 25. Part of your assessments would ensure processes, strategies and supports are in place to ensure that your Agency will actually be able to achieve this.

Example: Develop an information risk register

To help ensure information continuity and risk mitigation, you could use a register to identify information risks that need ongoing monitoring or management in specific business environments. For example, you could develop a register to flag:

- certain key information and metadata fields in System X are required to support business process Y and therefore must be maintained through the system's migration
- if, because of the way user permissions are defined, sections of a wiki or SharePoint environment used to manage high risk/high value project information are able to be deleted by project staff, flag that ongoing staff education and user support are necessary to ensure this high value information is not inappropriately deleted from these workspaces
- if certain business information needs to be kept for 10+ years, ensure that this is proactively identified and flagged for any system or service offering or process review associated with this information
- if certain long term value business information has not been migrated to new system environments and is being maintained in a legacy environment, flag that this information needs independent ongoing management and monitoring to ensure its ongoing accessibility
- if a core business system is unable to export data of its transactions, identify that manual workarounds are necessary to provide reporting and other information needed for service delivery and continuity

- if information requirements were not built into contracts with services providers or service offerings and data portability is not guaranteed under the contractual arrangements, identify that alternate strategies for maintaining access to information of long term business value need to be investigated

Example: Information management impacts of BYOD

Agencies are increasingly embracing BYOD (bring your own device) to allow staff flexibility and productivity on their own digital devices. This can present information management challenges if incorrectly implemented. Important agency information may be lost or released with potentially severe impacts, and staff may also be exposed to inconvenience and risk through inadvertent possession of official information on their personal devices.

The following considerations may assist with a well-managed implementation of BYOD:

- examine what staff and business processes are being transitioned to BYOD and what corporate business information needs will need to be managed through these new distributed environments
- assess third party apps that are used in BYOD or for service provision and determine whether all necessary information export, security and management requirements can be enabled in these environments
- if BYOD policies are deployed without supporting information governance frameworks, staff education, strategic planning and risk mitigation strategies are required to ensure high value business information is maintained within corporate environments for as long as needed to support business operations.

Recommended Reading

Managing Information Risk (2014: Guideline 25)

Risk Management - Part 1: Introduction (2014: Advice 60)

Risk Management - Part 2: Applying Risk Management processes (2014: Advice 60)

Risk Management - Part 3: Information Risk Register template (2014: Advice 60)

Further Advice

For more detailed advice, please contact:

Government Information Strategy Unit
Tasmanian Archive and Heritage Office
91 Murray Street
HOBART TASMANIA 7000
Telephone: 03 6165 5581
Email: gisu@education.tas.gov.au

Acknowledgements

- This advice is largely based on *Identifying information risks that might be impacting on high risk business*, State Records NSW, April 2014, and
- *Mitigating common digital information management challenges*, State Records NSW, April 2014

Information Security Classification

This document has been security classified using the Tasmanian Government Information Security classification standard as PUBLIC and will be managed according to the requirements of the Tasmanian Government Information Security Policy.

Document Development History

Build Status

Version	Date	Author	Reason	Sections
1.0	October 2015	Allegra Huxtable	Initial Release	All

Amendments in this Release

Section Title	Section Number	Amendment Summary

Issued: October 2015

Ross Latham
State Archivist