NSW GOVERNMENT

State Archives & Records

ASSESSING RECORDS, INFORMATION & DATA RISKS

Housekeeping

- **Participants will be muted** - please use '**Chat**' for questions and activities.
- **Session is being recorded**. Will be published on website.

Please note

- Webinar is about the ***general risks*** in managing records, information and data in systems.
- Consult with your **organisation's risk professionals**.

Why a webinar series on *records, information and data risks*?

Increase understanding of records and information risks

+

Risk assessment steps

+

Risk statement formula

=

Enable you to get executive buy-in or support

Through highlighting:
- the various types of risks threatening records, information and data within systems
- strategies/actions

Identifying:
- risk scenario(s)/ event(s)
- causes of risks
- consequences

Effectively articulating and communicating records, information and data risks

Facilitating:
- Business case for records, information and data projects
- Integration of risks into risk governance framework
- Addressing *Standard on records management* requirements

What is RISK ?

Deviation from the expected – be it positive, negative or both – which can address, create or result in opportunities and/or threats

The *effect* of uncertainty on *objectives*

Have different aspects and categories and can be applied at different levels

What are records, information and data risks?

Records, information and data risks are anything that may “affect” or “impact” their characteristics, access to/from, and function of providing evidence or information

Reliability & integrity

- Incomplete
- Inaccurate
- Untrustworthy

Accessibility & retrieval

Unable to:

- locate
- retrieve
- use

Safe custody

- Loss
- Unauthorised/unlawful access
- Unauthorised/unlawful destruction or deletion

Retention

Over and/or under retention

Ownership

Loss of ownership

Risk assessment steps

Step 1

Identify risks

- Scenarios/events
- Potential causes, threats and weaknesses
- Controls in place

Step 2

Assess

- Controls
- Consequences
- Likelihood

Step 3

Decide Treatments

- Accept
- Mitigate
- Transfer
- Avoid

AS/NZS IEC 31010:2020 Risk management – Risk assessment techniques

Link - https://store.standards.org.au/product/as-nzs-iec-31010-2020

Step 1 – Identify risks

Step 1

Identify risks

- Scenarios/events
- Potential causes, threats and weaknesses
- Controls in place

Ask yourself:

"What risk scenario/event might happen? How, when and why?"

- Identify **events**, **causes**, **threats and weaknesses** in your agency's operating environment:
  - Core functions, activities and services
  - Changes – organisational, legal and regulatory, political
  - IT environment
  - Community expectations
- Identify controls already in place for the purpose of determining their effectiveness
- *Records, information and data risks* guidance - https://www.records.nsw.gov.au/recordkeeping/records-information-and-data-risks

Step 2 – Assess

Step 2

Assess

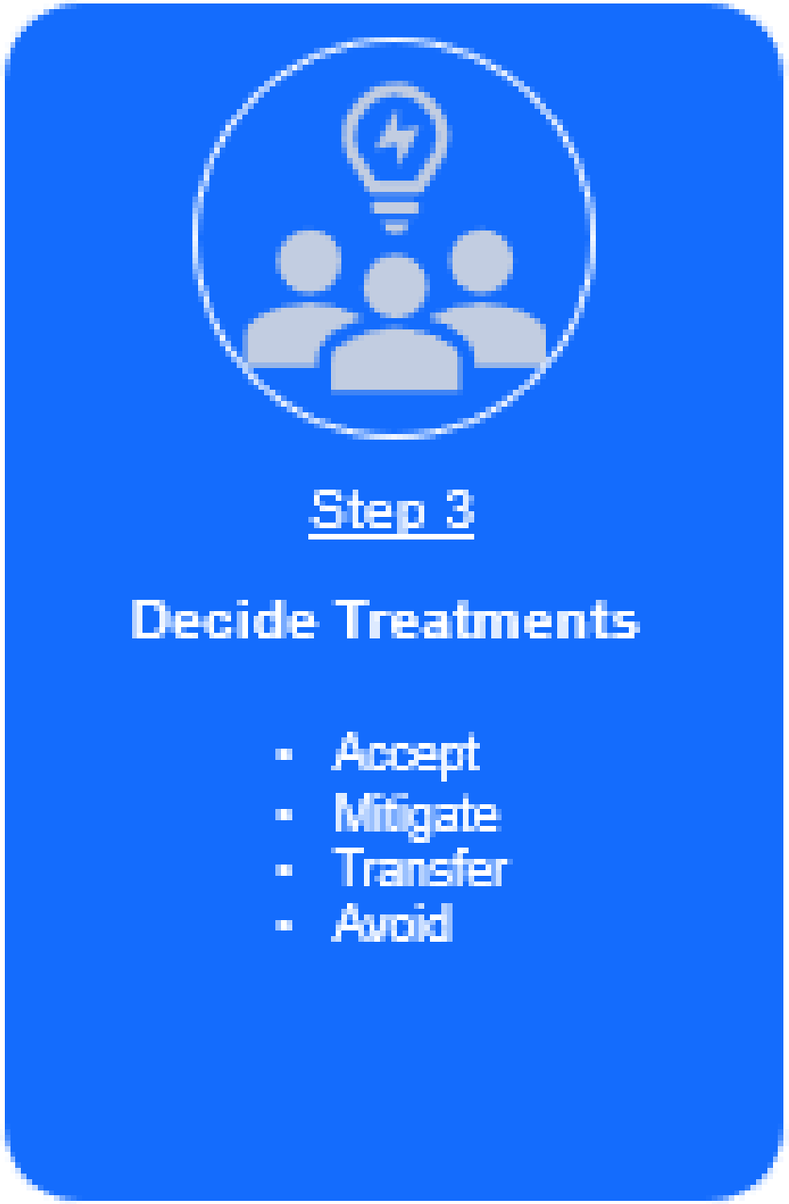
- Controls
- Consequences
- Likelihood

Ask yourself:

1. ***What controls are in place and are they operating as intended?***
2. ***"What is the likelihood that the risk will occur?"***
3. ***"What are the consequences or impact on the records, information and/or data if this risk scenario/event occurs?"***

- Assessing the **likelihood** of identified risks occurring and quantifying what their **consequences** or impact may be if they were to.
- Quantifying the risk will help you frame it in terms of the tangible business impact on records information and data.
- Risks should be assessed in line with your organisation's risks management framework.

Step 3 – Decide

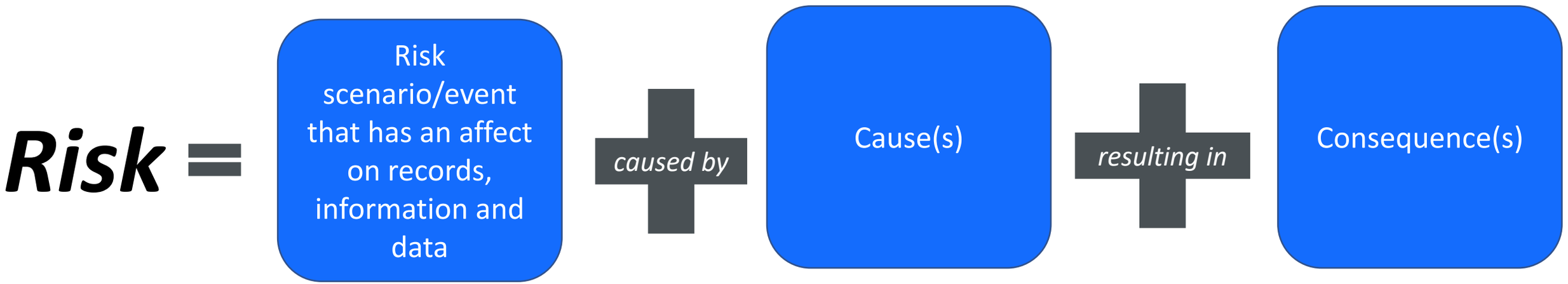


Ask yourself:

"How should we manage these risks?"

- The "risk appetite" of your organisation will help you decide whether treatment is required; including prioritising risks for treatment.
- Prioritise high-value and high-risk records, information and data. *Identifying and managing high-value and high-risk records, information and data – https://www.records.nsw.gov.au/recordkeeping/advice/identifying-high-value-and-high-risk-information*
- Treating identified risks:
  - ***Accept*** – the "do nothing strategy".
  - ***Mitigation*** – taking action to either reduce the likelihood of the risk occurring and/or the potential consequences if it does occur.
  - ***Transfer*** – transferring or sharing the risk with another party who is willing to accept the consequences.
  - ***Avoiding the risk*** – selecting an alternative option that is less risky or deciding not to proceed.

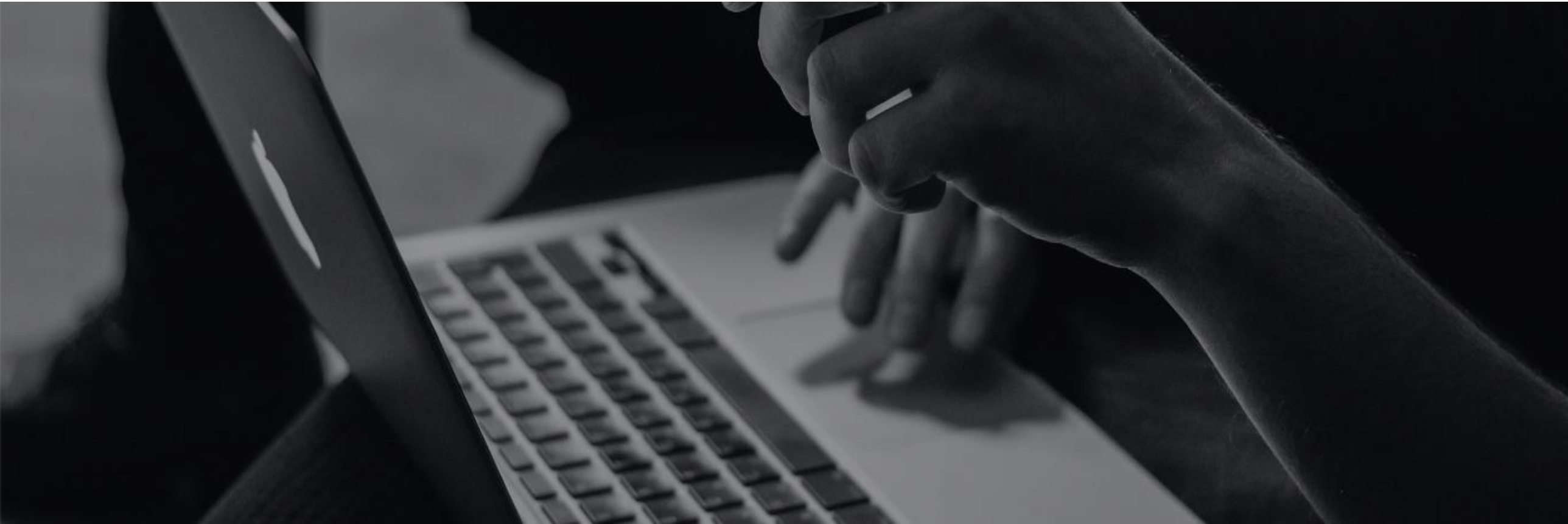
Risk statement formula



Benefits

- Articulating and communicating risks in building a business case to secure executive support
- Enable consistency in how risks are documented within the risk register and information asset register
- Improve maturity in identifying and managing records, information and data risks for reporting on in SARA's new annual monitoring exercise

Risk scenarios



Reliability & integrity

Risk scenario/ event	Cause	Consequences	Treatment (1 = lowest effort → 3 = highest effort)
High-value information missing from a migrated dataset	Post migration quality checking didn't pick up missing information	• System produces inaccurate analysis and reporting • Poor system uptake and benefits not realised • Non-compliance with the *Standard on records management* > breach of *State Records Act*	1. Data entry of missing information 2. Maintain decommissioned system for reference purposes while information is being restored 3. Redo migration activity

<u>Risk statement</u>:

Information missing from a migrated dataset caused by ***inadequate post migration quality checking*** resulting in ***breach of the State Records Act 1998 (NSW)*.**

Accessibility & retrieval

Risk scenario/ event	Cause	Consequences	Treatment (1 = lowest effort → 2 = highest effort)
Systemic failure to locate information for GIPA requests	Information and data held in disparate systems, including "shadow systems"	• Waste of resources (time, extra staff redirected to assist in locating data/information) • Multiple requests for external reviews lodged with the Information and Privacy Commission (IPC) • Investigation launched by IPC	1. Implementation of policy and procedures identifying the systems information and data are to be captured/managed within 2. Information governance initiatives (e.g. implement e-discovery systems and/or information asset register)

Risk statement:

Systemic failure to locate information for a GIPA request caused by ***information and data held in disparate systems, including "shadow systems"*** resulting in ***the Information and Privacy Commission launching an investigation***.

Safe custody

Risk scenario/ event	Cause	Consequences	Treatment
Loss of digital and hard copy records held by a third-party provider due to a natural disaster	No business continuity and counter disaster/recovery plans in place that cover records	• Impact on service delivery • Scrutiny from the Audit Office in their performance audit report of your agency • Loss of irreplaceable NSW documentary heritage	• Business continuity plan developed for digital records. Continuity planning requirements built into service level agreements • Counter disaster and recovery plans developed for hard copy records, including monitoring and regular disposal • Use RMAT to assess/monitor compliance with the *Standard on storage of physical State records*

Risk statement:

Loss of hard copy and digital records due to a disaster caused by ***no business continuity and counter disaster/recovery plans in place*** resulting in the ***loss of irreplaceable NSW documentary heritage***.

Retention

Risk scenario/ event	Cause	Consequences	Treatment
Destruction of drafts containing significant decisions that are not included in the final version	Ambiguous policy on the retention and disposal of significant drafts, working papers, etc.	• Complaints (e.g. from the public) regarding the information not being available • Scrutiny from the media • Breach of *State Records Act 1998*	• Update policy, procedures and business rules to clearly articulate what can/can't be disposed of under normal administrative practice (NAP) • Awareness sessions and training • Auditing/monitoring compliance initiatives launched

Risk statement:

Destruction of drafts containing significant decisions not contained in the final version caused by ***ambiguous policy*** resulting in ***media scrutiny***.

Bringing it all together

- Reviewing the different types of records, information and data risks:
  - reliability and integrity
  - accessibility and retrieval
  - safe custody
  - retention and
  - ownership

- Using the three-step risk assessment process as a structure in:
  - identifying the potential risk scenarios that may occur and their underlying causes, threats and weaknesses
  - assessing what their consequences – or impact – would be and the likelihood of them occurring
  - deciding how you are going to treat the risks -
    - acceptance
    - mitigation
    - transference
    - avoidance

- Describing risks in the form of risks statements so they can be effectively communicated in your organisation's relevant risk register in facilitating treatment and monitoring

Benefits

- **Articulating and communicating** records, information and data risks in **building a business case to secure executive support**

- Working towards addressing **minimum compliance requirements from the *Standard on records management*** for ensuring records, information and data are:
    - **identifiable, retrievable and accessible for as long as they are required** (3.3)
    - **protected from unauthorised or unlawful access, destruction, loss, deletion or alteration** (3.4)

- **Facilitating consistency** in how the risks are **documented** in your organisation's relevant **risk register** as well as in its **information asset register**. If you do not have an information asset register, or the risks are not high enough to be placed in a risk register, include as part of your unit or team's annual operations plan or as part of "business as usual" practices.

- **Improving maturity** in identifying and managing records, information and data risks which are **reported** on in the new **annual monitoring exercise**

What are your experiences?

Have any anecdotes regarding records, information and data risks? If so, we would like to hear from you.

As part of growing the list of risks in our new guidance titled *Records, information and data risks*, we are after “real world” examples public offices have identified and managed.

Please email your anecdotes to govrec@records.nsw.gov.au.

Recordkeeping Standards and Advice

CONTACT US

Email
govrec@records.nsw.gov.au

Phone
02 9714 3080

Website
www.records.nsw.gov.au/recordkeeping