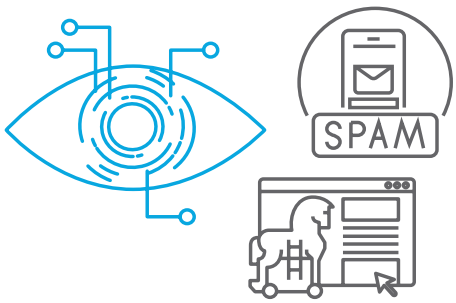
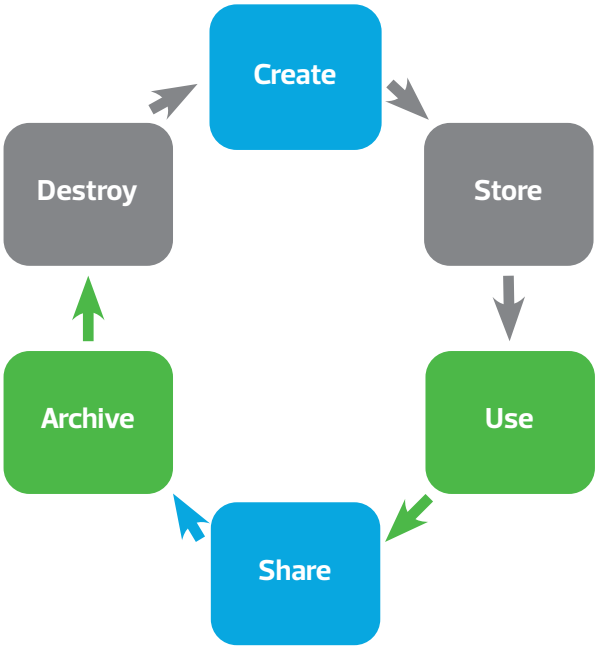
RISK ADVISORY SERVICES
— *Linking Data Lifecycle Management to Data Security*



Aligning a practical and simple data security framework with the data management lifecycle offers numerous benefits. It helps ensure comprehensive protection, consistency, efficiency, compliance, and proactive management of data security risks. To better understand these benefits, let's examine what a data lifecycle looks like.
See below for a visual depiction:



The different stages of the lifecycle are described next

- **Create** – where data is created or captured
- **Store** – data storage for later retrieval and use
- **Use** – where data is used for the purpose it was captured and stored
- **Share** – data being shared internally and with other third parties
- **Archive** – data being stored offline when it is not used regularly
- **Destroy** – data being permanently erased that is no longer required.
- Now let's explore data security controls by the various stages off the data lifecycle.

Create:

- Ensure all data that is captured or created is in line with local privacy laws
- Data capture should be authorised with consent received from the data subject
- All data subjects must be aware of the data being captured and its use
- Data capture devices must be secure from unauthorised access and tampering
- Any locally stored data on the device should be encrypted
- Any data being transferred off the device must be done so securely and any data in transit should be encrypted
- Classify all data when created and apply appropriate data security control sets based on data classification
- Use of data leakage prevention (DLP) technology is recommended to classify and automatically control access to, and transfer of data.

Store

- Do not store data that is not needed
- Any data stored should be encrypted
- Access to all data should be strictly controlled with appropriate authentication and authorisation controls in place
- Access to all data should be logged and reviewed for anomalies
- Large or unexpected transfer of data should be investigated immediately and ideally blocked automatically
- Any unexpected encryption of data should be prevented using automated controls such as endpoint security mechanisms
- DLP technology should be in place to prevent unauthorised access and transfer of data.

RSM

Use

- Use and access to data should be strictly controlled based on data classification
- Access to data should be on a 'need to know basis' only
- Access to data should require authentication, authorisation and logging controls
- Critical data should remain encrypted even when being processed, if feasible
- Never use live data in a test or development environment.

Share

- Data should only be shared with authorised parties
- Relevant provisions of local privacy laws should be adhered to
- Data should not be shared without consent and should not be sent outside of local jurisdiction, if not allowed All data exchange should occur over encrypted channels
- The receiving party must be aware of their obligations to protect the data received.

Archive

- Data should be archived securely and using a medium that is going to be available in future
- All archived data should have security controls implemented based on the data classification
- Appropriate logical and physical security access controls must be in place to protect archived data
- All archived data must be encrypted and encryption keys securely stored for long term use.

Destroy

- Any data no longer needed should be destroyed
- Access to any data being destroyed should be strictly restricted and authorised
- Data destruction should be appropriately supervised to ensure it cannot be stolen and is irretrievably erased
- Regular audits should be performed to verify the control noted above as data destruction can be particularly susceptible to data theft.
- As data becomes more valuable, it becomes more susceptible to theft. Understanding how data is managed in an organisation is critical to understanding how it can be secured. Aligning data security controls to data lifecycle management is a practical and simple way of securing data. Within this paper I have shared a simple framework that I have used before and operationalised, in order to achieve this.

For more information please contact:

Ashwin Pal
Partner, Sydney
T 02 8226 4500
E ashwin.pal@rsm.com.au

Darren Booth
Partner, Melbourne
T 03 9286 8158
E darren.booth@rsm.com.au

Riaan Bronkhorst
Principal, Perth
T 08 92619272
E riaan.bronkhorst@rsm.com.au