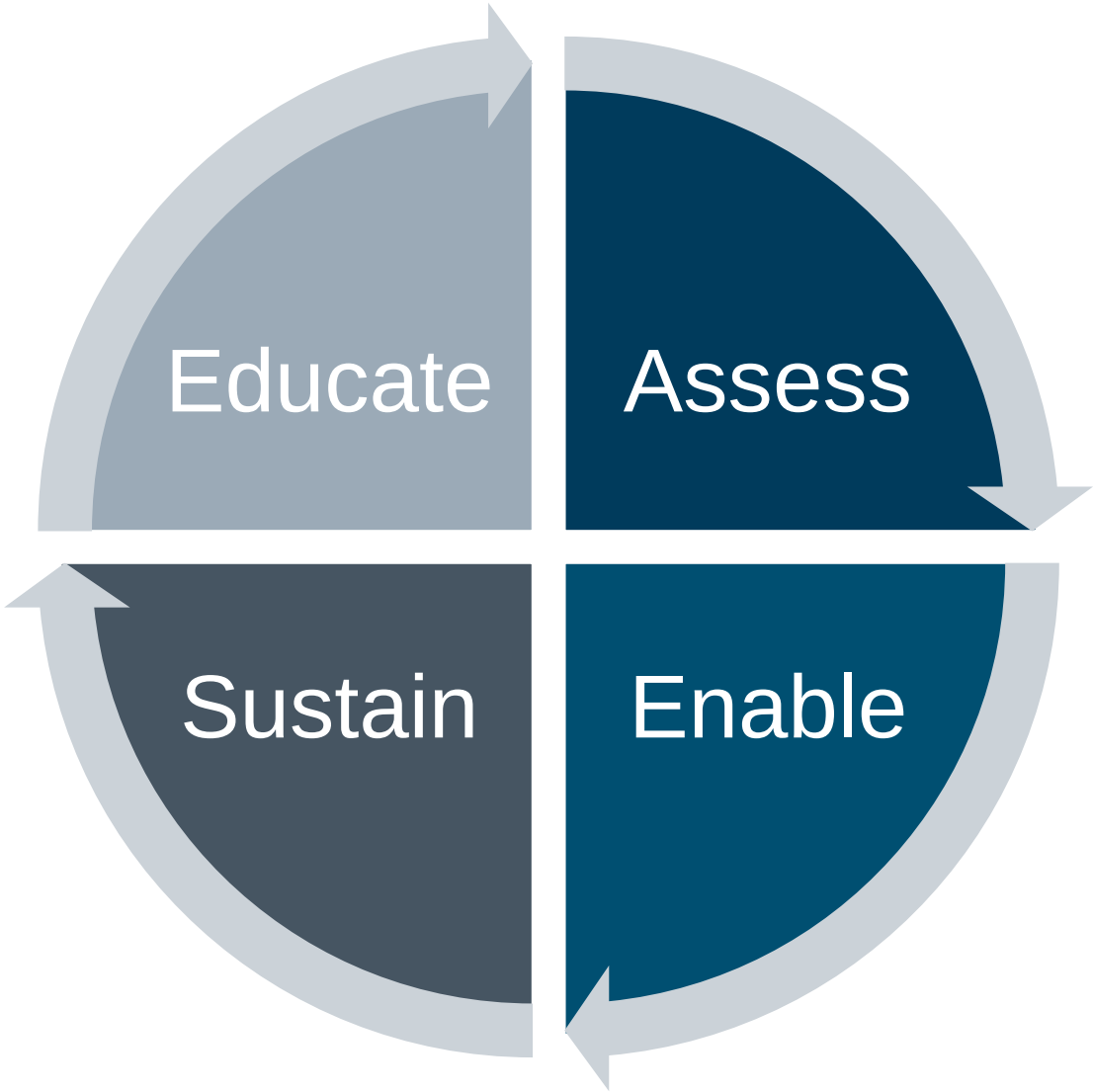


CADMUS CONSULTING
WE GET IT

CADMUS Consulting

Assess

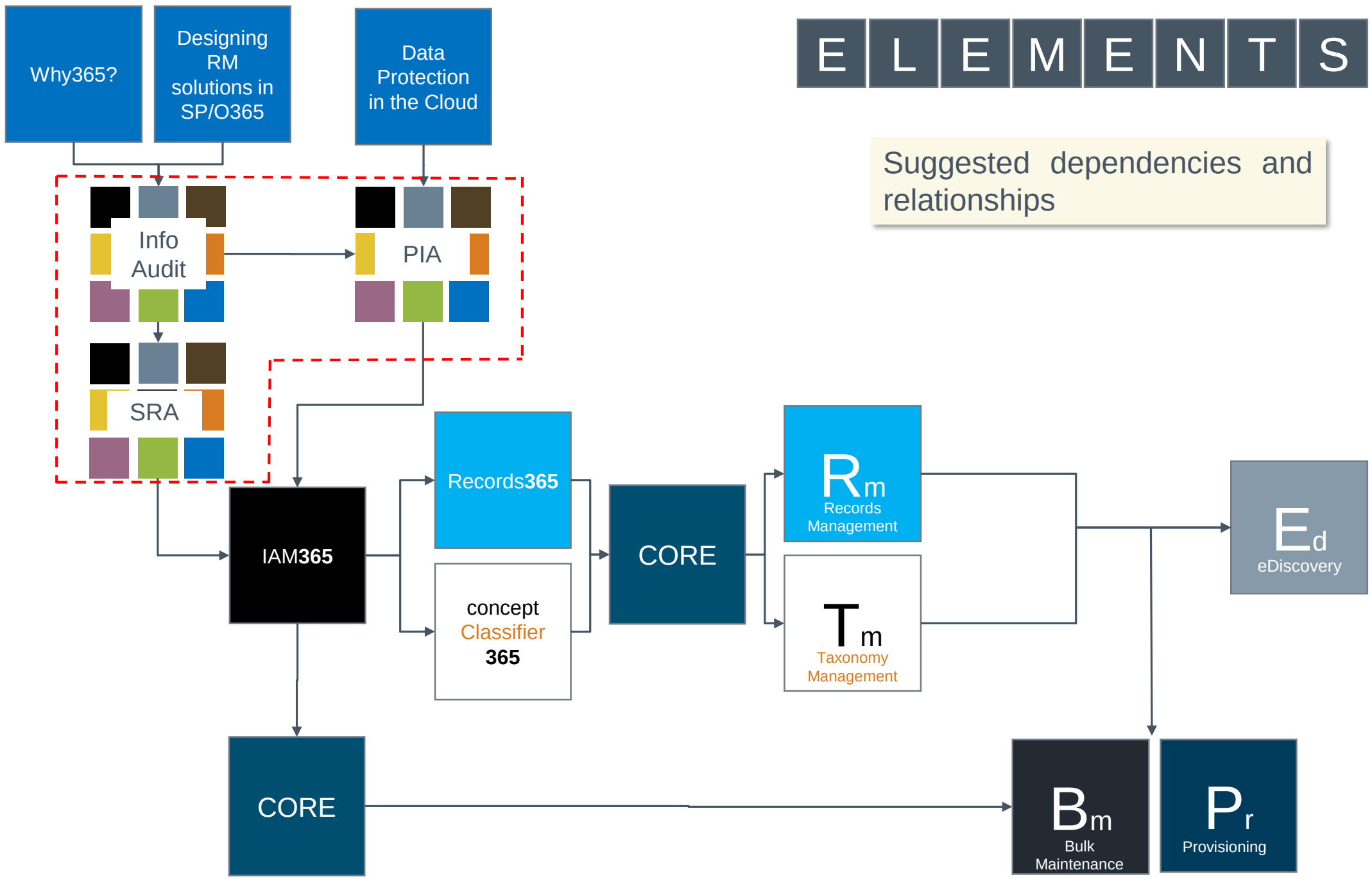
At **CADMUS** Consulting we have developed a framework of assessments that allow you to build a comprehensive understanding of your information landscape. Each assessment can be either self-contained or combined to create an increasingly rich picture.

The approach to the assessments is based on industry best practice relating to information security; specifically, the ISO27K series and the Australian Privacy Principles (APP's).

The Information Audit provides the foundations for your initial or continued journey to the cloud. It identifies your High-Business-Impact information assets, helping you to develop appropriate security, migration, implementation and management strategies.

The Summary Risk Assessment is a multi-faceted review of the information assets you own and use.
The assessment seeks to identify any changes in the risk profile of information assets associated with the move from internally managed systems and services to cloud-based services.

The Privacy Impact Assessment is an essential tool in the decision making process related to moving your data to the cloud. It identifies the security and data-privacy considerations related to your content.


Why365?
Designing RM solutions in SP/O365
Data Protection in the Cloud
E L E M E N T S
Suggested dependencies and relationships
Info Audit
PIA
SRA
IAM365
Records365
concept Classifier 365
CORE
Rm Records Management
Tm Taxonomy Management
Ed eDiscovery
CORE
Bm Bulk Maintenance
Pr Provisioning

WHAT

Info Audit

***Information Audit**. A high-level audit and review of your key information assets; covering the core areas essential to good information management: Compliance, Security, Governance, Lifecycle, Usability, Information Architecture and Sustainability*

Co Compliance

- Are important records managed appropriately
- Are you complying with relevant legislation or guidelines e.g. Data Protection, Freedom of Information, ISO 27001
- Can you apply legal holds to content or respond to discovery requests

Se Security

- How is security applied and maintained
- Are the access control models appropriate
- Are they stifling collaboration and re-use
- Do users understand how to secure and “protect” content appropriately
- Is Data Loss Prevention (DLP) important
- Is Digital Rights Management (DRM) important
- Is content accessible outside of your organisation
- How is this controlled
- What “end-points” are being used (Mobile, BYOD, …)

Go Governance

- Who can do what to your assets and why
- Who “Owns” the content and the processes they support
- When and how are changes to assets controlled and communicated
- Are policies in place, up to date, communicated effectively and being monitored

WHAT

Info Audit

***Information Audit**. A high-level audit and review of your key information assets; covering the core areas essential to good information management: Compliance, Security, Governance, Lifecycle, Usability, Information Architecture and Sustainability*

Li
Lifecycle

- When and how does content get deleted
- Is this controlled and or audited

Us
Usability

- Do users understand where to store your assets
- What is the balance between “empowerment” and “control”
- What are the training implications the use and management of you assets
- Are any interfaces intuitive and consistent

Ia
Information Architecture

- Are your assets stored using consistent structures, naming and metadata
- Is there consistency and clarity in how content is stored and classified

Su
Sustainability

- Are the right resources allocated to sustaining any platforms or solutions used to store and manage your assets? Specifically: Security, Auditing, Monitoring, Creation, Lifecycle, Records Management, and Training

W
H
Y

Info Audit

***Information Audit**. A high-level audit and review of your key information assets; covering the core areas essential to good information management: Compliance, Security, Governance, Lifecycle, Usability, Information Architecture and Sustainability*

Understanding what you have, is the key to determining what to do with it

- Acts as a foundation to any information management initiatives
- Pragmatic “risk based approach” allows you to focus on your High-Business-Impact assets first
  - **Controls cost and limits impact on day-to-day business activities**
- Identifies the barriers and opportunities associated with your current use and management of your assets
- Supports: Business continuity, business process improvement / transformations, mergers and acquisitions, organisation restructures, EDRM projects (migrations, upgrades, replacements)

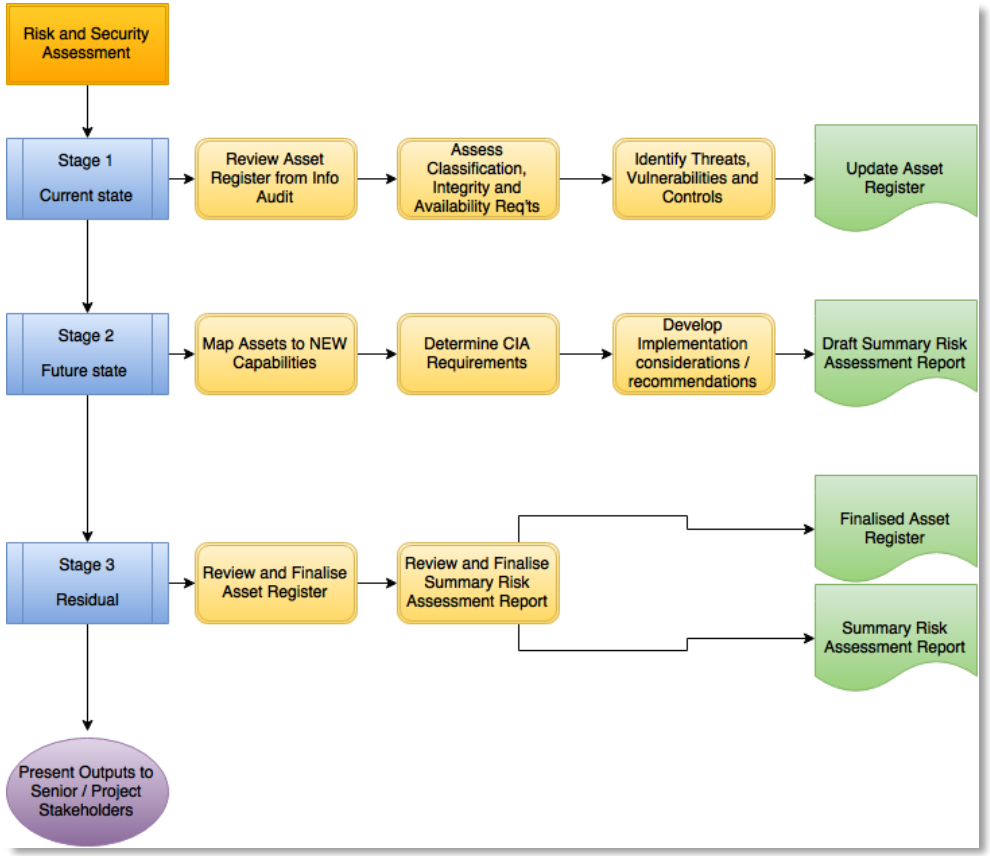
Includes:
A roadmap of recommendations and actions
Presentation of the recommendations to your senior sponsors and decision makers to ensure you are able to move to your desired state in a optimal way.
Comprehensive Information Asset Register for HBI Assets

WHAT

SRA

***Summary Risk Assessment**. Builds on the Information Audit. Analysis of the inherent risk in the way you currently manage your information assets. Projects change in risk profile following a move to the cloud.*

- ✓ Based on ISO27K series and industry best practice
- ✓ Review and assessment of current and future state of HBI assets in relation to key attributes; Confidentiality, Availability, and Integrity (CIA)
- ✓ Identification and assessment of associated Threats, Vulnerabilities and Controls in current and future states
- ✓ Development of risk treatment plan and suggested controls for future state use and management of assets
- ✓ Outline potential benefits that can be achieved by reducing or removing any identified risks



***Summary Risk Assessment**. Builds on the Information Audit. Analysis of the inherent risk in the way you currently manage your information assets. Projects change in risk profile following a move to the cloud.*

W
H
Y

- Reduce risk associated with poor and inappropriate information management
- Provide focus for migration activities
- Ensure funding and resources are appropriately allocated to the right components of any cloud solution
- Demonstrate due diligence and increase trust from employees, customers, and partners
- Supports: Decision making process regarding which content and processes to move to the cloud

Includes:
Specific considerations that should be addressed in the overall design, implementation and ongoing usage of the cloud. This could include modification of processes, creation of, or amendment to, policies, and user education.
Identification of requirement for any new controls.
Identification of any existing controls which can be deprecated or which become redundant.
Recommendations for how any residual risk should be treated / managed.

***Privacy Impact Assessment**. A structured assessment regarding the handling and processing of personally identifiable information in the cloud, in-line with the advice provided by the* Office of the Australian Information Commissioner (OAIC)

WHAT

- ✓ Based on Australian Privacy Principles (APP)
- ✓ 10 Step process - Builds on information audit
  - Validate the need
  - Plan, scope and resource
  - Define and communicate the process
  - Consult stakeholders
  - Map information flows
  - Identify risks
  - Identify solutions
  - Provide recommendations
  - Record outcomes
  - Integrate into project and review

WHY

- ➢ Provide your senior sponsors and decision makers with clear, prioritised, actions and recommendations to ensure that you are able to transition safely to the cloud

CONTACT US

Contact CADMUS Consulting on:

- (08) 9328 1356
- 0475 631 994
- info@cadmusconsulting.com.au
- cadmusconsulting.com.au
- @ConsultCadmus
- cadmus-consulting

CADMUS CONSULTING

WE GET IT