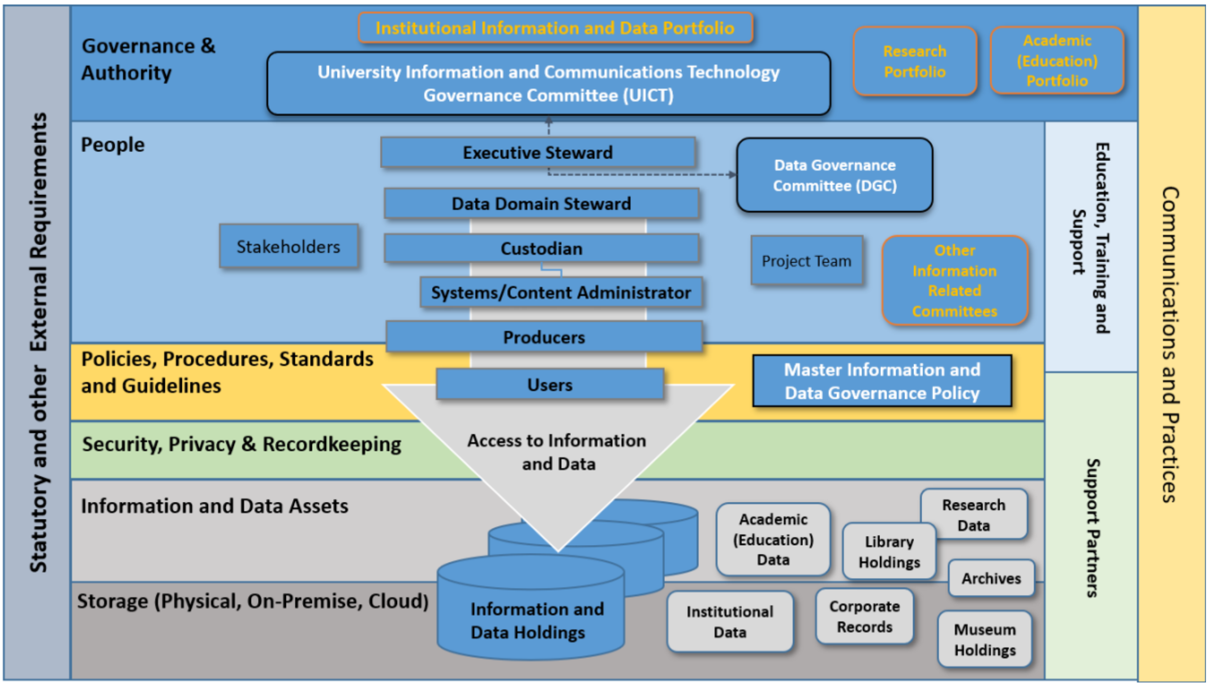
Tips on privacy, record keeping and systems for system business owners and stewards

Background

The University is an education-intensive research institute, originally established by an Act of the Commonwealth Parliament in 1946. The *Australian National University Act 1991* is our primary legislation. As a commonwealth body the University is governed under the *Public Governance, Performance & Accountability Act 2013* and other commonwealth legislation including the *Privacy Act 1988* and *Archives Act 1983*.

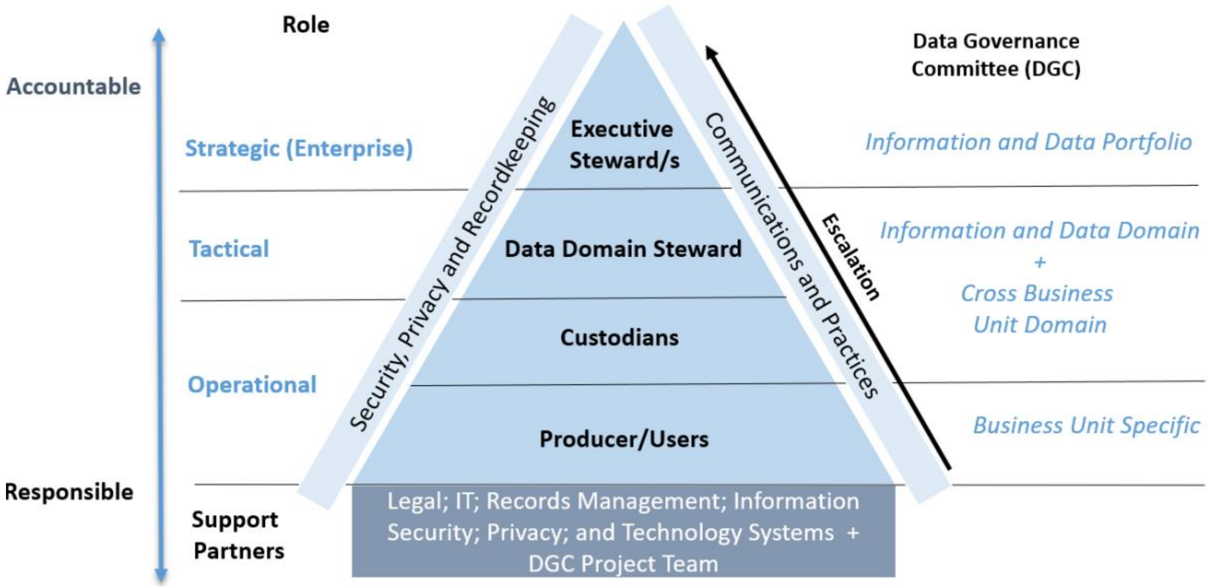
The University's Data Governance principles and framework have recently been developed. Drafts were provided to Service Division Directors and General Managers earlier this year and the principles have been endorsed by the University's ICT Committee.

The overall model is:


Statutory and other External Requirements
Governance & Authority
Institutional Information and Data Portfolio
University Information and Communications Technology Governance Committee (UICT)
Research Portfolio
Academic (Education) Portfolio
People
Executive Steward
Data Governance Committee (DGC)
Data Domain Steward
Stakeholders
Custodian
Project Team
Other Information Related Committees
Systems/Content Administrator
Producers
Policies, Procedures, Standards and Guidelines
Users
Master Information and Data Governance Policy
Security, Privacy & Recordkeeping
Access to Information and Data
Information and Data Assets
Academic (Education) Data
Library Holdings
Research Data
Archives
Storage (Physical, On-Premise, Cloud)
Information and Data Holdings
Institutional Data
Corporate Records
Museum Holdings
Education, Training and Support
Support Partners
Communications and Practices

Data responsibility

The model includes a range of authorities for data responsibility, as opposed to the past ANU approach of System owners, including the following levels:


Role
Accountable
Strategic (Enterprise)
Tactical
Operational
Responsible
Support Partners
Security, Privacy and Recordkeeping
Executive Steward/s
Data Domain Steward
Custodians
Producer/Users
Legal; IT; Records Management; Information Security; Privacy; and Technology Systems + DGC Project Team
Communications and Practices
Escalation
Data Governance Committee (DGC)
Information and Data Portfolio
Information and Data Domain + Cross Business Unit Domain
Business Unit Specific

Records responsibility

Under the University's Records management and archives policy, records may be managed in enterprise systems or in the Electronic Records Management System (ERMS).

The University's storage and management of records must comply with the Archives Act. Records disposal is covered by the Administrative Functions Disposal Authority and ANU-specific authorities for Student Progress and Services, Research, and Teaching and Learning records (PDF, 3.45 MB). The authorities apply to paper and electronic records and data.

The University Records team provides support and training in use of the ERMS and general advice on records creation, management and disposal.

Tips

There are a number of areas where business owners, custodians and data domain stewards should consider reviewing their systems to ensure legislative compliance and good practice.

1. **Systems should only contain information that is required for the purpose that they serve.** The University may have collected information in excess of that required in the past. It is timely to review information to ensure that personal information that is not required is both not collected and removed from systems. If you wish to collect additional information consent for collection should be a standard business practice.

2. **Systems data should be reviewed to ensure only appropriate data is included in the system.** Free text fields may have been used to record information that should be in another system, such as the ERMS. Reviewing free text data and ensuring the information is stored in the appropriate system will enable better management of information.

3. **Systems should have planned and implemented data management strategies to ensure data/information is removed when it is no longer required and securely disposed of.** It is not necessary to retain everything forever. When systems are established a key aspect is data management planning to ensure that retention requirements are built in so that data can be removed when it is no longer legally required. Business areas may not have reviewed

systems to ensure that the disposal process is consistent with the disposal authorities and legal requirements. Review systems to ensure that application of the requirements is timely and will lead to better practice.

4. **Staff training and manuals should be up-to-date and reflect current legislative requirements.** Privacy training is offered online. An up-to-date full new module was delivered for implementation last December after detailed alpha and beta testing with a broad range of University areas. It will be available through PULSE shortly. Training programs and manuals should be reviewed regularly to ensure they are up-to-date. Training sessions will be scheduled and feedback on specific areas will be important to ensure they meet needs. Note that the resources available to provide face-to-face training are limited, noting that session will be run by an external provider after the PULSE module is online.

5. **Information and Data Classification Standard**. The forthcoming standard, which includes the **Infrastructure Security Classification Standard**, needs to be reviewed to ensure that issues identified are addressed. Note that that responsibility for the data held within the system lies with the system owner and it sets out other user responsibilities.

6. **Master Data Model Standard**. The standard will be supported by a master data management tool owned by PPM which removes duplicates, standardises data (mass maintaining) and incorporates rules to eliminate incorrect data from entering the system in order to create an authoritative source of master data. When implemented all business systems must be assessment and recorded in the PPM tool.

7. **Storing Data for Reporting Purposes.** Data is often stored in Enterprise Systems to facilitate reporting and analysis. Sometimes this data has no operational purpose beyond reporting and is either duplicated or stored for that reason alone. Data should not be stored in operational systems beyond the regulatory disposal periods in order to facilitate trend based reporting. It is possible to store de-identified trend data in the University's data warehouse to support these activities. The Data Warehouse is also a more appropriate place to join data across systems to support reporting, avoiding unnecessary further duplication. Contact the Insight Team to discuss this further.

8. **Privacy Impact statements** should be prepared for systems with personal information and are progressively being developed. The Guideline is online here https://policies.anu.edu.au/ppl/document/ANUP_019407.

Roxanne Missingham
ANU Privacy Officer and Chief Scholarly Information Officer
9 June 2019