



UNIVERSITY OF  
TECHNOLOGY SYDNEY

# Risk and Records at UTS

# U t S

THINK.CHANGE.DO



## Records Management Program

- > University Records, Governance Support Unit, Registrar, DVC (Corporate Services)
  - 6½ dedicated f/t positions
- > Devolved system
  - 2 campuses (city campus over several blocks)
  - 7 Faculties & 41 Units, totaling over 200 business units
  - Approx 974 academic / 1434 support staff (2010 head count).



## Records Management Program



- > Approach
  - Systems implemented across all areas....AND...
  - High risk business activities and high risk areas targeted
- > Roles and responsibilities
  - Primary Records Contact in each Faculty/Unit
  - Records Contacts in every business unit to facilitate recordkeeping activities



## Imbedding Risk in the Records Management Program

- > Risk Management Framework and Disaster Recovery Plan
- > Inc traditional Counter Disaster Plan and incorporates risk related programs as part of prevention strategies, inc:
  - Records Management Program
  - Vital Records Program
  - Repository and Archive Management Program
  - Destruction Program
  - Digital Recordkeeping



## Imbedding Risk in the Records Management Program

- > Audit and Risk Committee's Audit Schedule
  - 2009 Records Audit undertaken
  - Key outcome was restructure of assessment program
- > History of Assessment Program
  - 2001-2005 [resourced - all business units visited annually]
  - 2006 [all business units undertook self-assessment]
  - 2007 to 2009 [only 10% high risk areas visited]



## Imbedding Risk in the Records Management Program

- > New Records Assessment Program (c. late 2010) \*  
—
  - Resourced
  - Risk focused schedule of assessment
  - Self assessment and risk assessment activities
  - Liaison and monitoring of completion and results
  - Planning and review



## Assessment Program

- > Self-Assessment Schedule
  - Triennial schedule based on their risk and our resources
    - Yearly: areas maintaining central collections of high risk records critical to operations
    - Bi-annual: other considered medium-high risk, but not centralised
    - Triennial: remaining areas

## Assessment Program – Stage 1: Self-Assessment Process

### > Self-Assessment Tool

\*  
—

Responsibilities / delegations (inc. list contacts and training)	Storage of records (inc. assessment & approval)
Planning (inc. id business activities & records)	Security / confidentiality
Creation of official files	Digital recordkeeping systems (inc. assessment / approval)
Filing documents	Archiving and Destruction
Managing physical files	Risk mgt / disaster prevention



## Assessment Program – Stage 1: Self-Assessment Process

### > Records Storage Risk Assessment Tool

\*  
—

Environmental conditions
Fire / water
Location of storage areas
Method of storage

## Assessment Program – Stage 2: Planning

### > Records Management Plan

\*  
—

Communication plan
Routine recordkeeping
New projects arising from Self-Assessment
New projects arising from Records Storage Risk Assessment
New projects arising from planning restructures / office moves
New projects arising from legal / policy changes

No such thing as set and forget...it doesn't end here...

- > UTS Planning & Improvement Framework's Quality Cycle
- > Review outcomes of the assessment program
- > Review tools
- > Review schedule
- > Monitor review of Records Management Plans
- > Incorporate common / high risk issues into training program to mitigate against risk of ongoing systemic issues



## New element - Digital Recordkeeping

- > Identification of systems
  - Liaised with ITD
  - Cover requirements in communication and training
  - Included in self-assessment process
- > Existing systems
  - Digital Recordkeeping Identification Tool
    - Identify whether system supports “high risk” activity
    - Identify whether records are created and where held

\*

## New element - Digital Recordkeeping

- > Existing and New systems
  - Digital Recordkeeping Assessment Tool \*  
—
    - Recordkeeping functionality
    - Metadata requirements
    - Metadata map
  - Action Plan - priorities and decisions based on
    - Resources
    - Existing level of system compliance
    - Nature of the records