Australian National University

Standard: Enterprise systems management

Purpose

This standard provides a framework for the governance and management of enterprise systems and defines the roles and responsibilities of Information Technology Services (ITS) and other business areas within ANU. The purpose of this standard is to ensure the security, availability, and integrity of enterprise systems.

Definitions

Definitions of additional terms used in this document are provided in the overarching policy, Information technology security.

Business continuity: the capability of the organisation to continue delivery of products or services at acceptable predefined levels following a disruptive incident. The emphasis in business continuity is on business operations.

Business re-engineering: changes that improve the cohesiveness between enterprise systems and University business processes.

Business Solutions Group: an individual or group that supports tier 1 and/or tier 2 systems.

Configuration: changes to an application via pre-set choices.

Customisation: changes to the application via coding and integrating this with the system. Includes data integration between two or more systems.

Disaster Recovery: both preparation for the recovery of an Enterprise System after major failure, as well as the actual process of recovering should a failure occur. This includes ensuring the right processes, policies and procedures, as well as software, hardware are in place and people are on hand and trained. The emphasis in disaster recovery is on technology.

Enterprise Architecture: defines the technological structure and operation of an organisation for the purpose of determining how it can most effectively achieve its current and future objectives.

Information Technology Team: as not all ANU systems are managed by ITS, this is a more generic term.

ITIL: Information Technology Infrastructure Library. A set of detailed practices for IT service management that focuses on aligning IT services with the needs of business.

Major change: a major change involves a significant amount of preparation, planning and work with complex situations or major expenses (see the Change Management Module Manual for further details).

Minor change: A minor change is a change, where there is minimal risk and impact (see the Change Management Module Manual for further details).

Mobile compatible: A website that is viewable on a smartphone or tablet, but is not optimised for mobile viewing (i.e. 'mobile friendly').

Mobile responsive: the layout and/or content responds or adapts to the size of screen they are presented on.

Operating Level Agreement: an agreement between areas that are providing a service together, describing how they will achieve the joint level of service.

Recovery Point Objective (RPO): amount of acceptable data loss.

Recovery Time Objective (RTO): time to restoration after a disaster recovery event is declared.

Service Level Agreement (SLA): an agreement between ITS and another area to which ITS is providing services.

System support: Day-to-day monitoring, maintenance and back end technical support of the system application and infrastructure.

Technology uplift: changes that improve technology platforms to ensure the stability of business processes. The majority of technical uplifts will also require business re-engineering.

Standard

1. Enterprise systems are business critical software applications that have broad institutional impact, support campus-wide administrative and academic functions, and address key University needs.

2. Governance and management arrangements for enterprise systems are required to give the University confidence that:

   a. enterprise system functionality is aligned to business requirements and strategy;

   b. operational responsibility and authority are clearly assigned;

   c. effective planning processes are in place;

   d. system support and architecture documentation is complete and comprehensive;

   e. system risks have been identified and are being managed;

f. systems are current and fully supported by a vendor;

g. systems are responsive, available, robust, and secure;

h. system security and data breaches are managed appropriately; and

i. system performance is monitored.

Enterprise systems tiers

3. Enterprise systems are divided into three tiers; Tier 1, Tier 2, and Tier 3. Whether those systems are hosted off-site or run on-site, the following classifications are still applicable, although the approach as to how the recommendations are applied may vary.

Tier 1

4. A Tier 1 enterprise system is a University-wide system that supports the core business of the University – research, teaching, and/or learning – with data critical to the University as a whole. A system is considered to be Tier 1 if the University would suffer a critical loss if the system were to be unavailable for two days.

5. Tier 1 systems are the authoritative source of information for the University and data can be used to assist ANU to meet statutory requirements.

6. All Tier 1 systems are endorsed by the University Information and Communications Technology Governance Committee (UICT). A business unit may request that UICT consider a system to be Tier 1 by presenting a business case detailing what it would take to move an application and its supporting infrastructure to Tier 1, including funding to provide the appropriate level of support.

7. A Tier 1 system requires:

a. a Business Solutions Group (BSG) to manage the system lifecycle and prioritise work in alignment with University requirements;

b. full-time support staff;

c. full redundancy, in separate data centres - “warm” standby that can fail-over to disaster recovery with some human input, or fully active-active where no human intervention is required;

d. development, test, production, and disaster recovery environments;

e. load testing, to establish the peak load capacity for the purpose of major system upgrades;

f. a Disaster Recovery (DR) plan including contacts, required Recovery Point Objective (RPO) and Recovery Time Objective (RTO);

g. management of data including defined back up, archiving, and retention levels; and

h. up to date and comprehensive documentation.

8. Tier 1 systems undergo full failover and failback testing at least once every two years, and within six months of any major change.

Tier 2

9. A Tier 2 system is a non-core University-wide system. The effect of a Tier 2 system's failure on the University is not as critical as a Tier 1 system. Although inconvenienced, the University would be able to function without a Tier 2 system for up to one week.

10. A Tier 2 system will have a lower outage restoration priority than a Tier 1 system in a circumstance in which multiple systems have been impacted by a failure. It will have priority over lower tier systems.

11. There are certain Tier 2 systems that are considered to be Tier 1 at specific times during the year, such as the student admissions system. System requirements and the level of support provided will be determined for each of these systems individually.

12. A Tier 2 system requires:

a. a BSG to manage the system lifecycle and prioritise work in alignment with University requirements;

b. development, test, and production environments;

c. full compliance with standard University architecture;

d. load testing, to establish the peak load capacity for the purpose of major system upgrades;

e. a DR plan including contacts, required RTO and RPO; and

f. data management including defined back up, archiving, and retention levels.

13. A Tier 2 system does not require redundancy infrastructure. If there is no redundancy infrastructure incorporated into the system architecture, recovery time for that system will be slower in the event of a system failure.

14. Tier 2 systems undergo full failover and failback testing at least once every two years, and within six months of any major change. If there is no redundant infrastructure supporting the system then a failover test from system backups must be performed.

Tier 3

15. A Tier 3 system is any system not captured in Tiers 1 or 2.

System owner responsibilities

16. All enterprise systems have a system owner.

17. System owners are responsible for the implementation and operation of their enterprise system, including:

a. ensuring authorised users are advised of all relevant ANU policies and related documents, and are provided with adequate training and support on the use of information infrastructure and security of information assets;

b. the quality of data held in their system;

c. identifying and managing DR plans and business continuity requirements for their system;

d. ensuring that risk management, including risk assessment and mitigation, and change management processes, are undertaken for their system;

e. procedures and processes are in place for the operation and security of the enterprise system, including standard operating procedures and privacy impact assessments; and that such procedures and processes are consistent with current University IT security and privacy policies and procedures;

f. adequate measures are taken to ensure that the application system is protected from unauthorised access by: (1) any utility, operating system or malicious software that is capable of overriding or bypassing application controls and (2) unauthorised users;

g. appropriate steps are taken to ensure the integrity and security of all applications, including that the application does not compromise other systems with which information resources are shared; and

h. that relevant applications and operating systems in each area remain the responsibility of that area.

18. System owners comply with the following:

a. a process for user access to information and application functions is implemented, documented, and reviewed on a regular basis;

b. user administration controls in place including formal procedures and processes for granting, removing, and modifying users

c. formal change control procedures documented and enforced; and a formal document change process, including risk assessment, and impacts of change, implemented

d. audit and monitoring activities logged and recorded; audit and monitoring logs include user activity, exceptions, and events including user ID, date, time, and detail of event.

19. The system owner establishes a BSG for every enterprise system, regardless of tier.

Business Solutions Group responsibilities

20. A BSG may be responsible for multiple enterprise systems within a business area.

21. The BSG will provide operational support for business processes within the business area, including:

a. ongoing business process review;

b. system lifecycle and strategic direction planning;

c. risk planning and mitigation including business continuity planning;

d. proposals to support new and improved functionality;

e. configuration and updates, e.g. modifying the enterprise system without writing new code;

f. helpdesk support;

g. preparation of system/technical change requests;

h. information architecture and data stewardship, relating to the validation and management of data integrity, quality, access, ownership, and usage;

i. non-technical change and communication management;

j. system acceptance testing, user acceptance testing, and quality assurance, including test script preparation;

k. reporting against statutory requirements;

l. role based security;

m. training and implementation; and

n. user documentation.

Information Technology Team responsibilities

22. An Information Technology Team (ITT) supports the function of the BSG. An ITT will either:

a. be established within ITS by the Director. This team may be overseen by an external group or entity at the direction of the Director(ITS) or Chief Operating Officer; or

b. consist of IT technical support staff that are external to ITS. If these groups require support from ITS they will require an Operating Level Agreement (OLA) to define the level of support and responsibility offered between the two teams.

23. The ITT manages:

a. system establishment;

b. system access and security

c. integration;

d. maintenance and upgrades;

e. customisation and development as appropriate;

f. upgrading production and version control;

g. system risk mitigation including disaster recovery (in collaboration with the system owner);

h. third tier support;

i. unit integration and testing;

j. major change and technical life cycle support;

k. performance monitoring; and

l. systems documentation.

24. Privileged access and elevated access accounts can potentially allow access to the entire system, especially if the account provides access to financial, confidential, or otherwise sensitive information or data. Therefore, these accounts need to comply with the *Information technology account management and access procedure*.

Change management

25. All changes to enterprise systems follow the ITS change management process as described in the Change Advisory Board Terms of Reference.

26. Changes to enterprise systems are approved by the BSG and prioritised with the ITT, based on the ITT's capacity and the priority of the change.

27. Minor changes are approved by the system owner or their nominated delegate, and follow business change management and technical change management processes.

28. Minor changes to enterprise systems are to be undertaken with consideration of the capacity of the ITT and the BSG.

29. Major changes to enterprise systems can involve significant preparation, a high level of work complexity, and/or major expenses. A change record is to be submitted to the Change Advisory Board to communicate the change as early as possible, with a minimum of 1 weeks' notice prior to implementation.

Service Improvements

30. Service improvements can include technology uplift and business re-engineering. These may be incorporated into a single project to take advantage of their interdependencies, in which case the Director (ITS) will prepare the proposal.

31. Requests to perform service improvements are to be documented via a project proposal or business case (as appropriate) with endorsement from the Director (ITS) and approval from UICT. These proposals, accompanied by a detailed project plan, are to be submitted to UICT in accordance with procedures on the UICT webpage. In principle approval for funding is sought as early in the planning process as practical from UICT.

32. Technology uplift proposals are based on systems cost and risk to the University of not making the change, and will be prepared by the Director (ITS).

33. Business re-engineering proposals are prepared by the system owner, and are based on:

a. solving pressing problems;

b. ensuring University objectives are met in a timely way;

c. realising potential efficiencies;

d. estimated returns viewed as an 'investment'; and

e. meeting University and IT strategies.

34. A steering committee is required for all service improvements. The committee:

a. ensures that the project plan is closely coordinated to ensure that value-add is achieved;

b. ensures adequate resource management;

c. reviews control changes and recommend additional organisational changes;

d. gives authorisation to proceed with each phase of the project or implementation; and

e. consults as necessary to flag major policy issues and/or conflicting priorities.

Funding management

35. A funding model is established that supports the development and life extension of enterprise systems. Typically:

a. the BSG role is resourced within the recurrent budget of the system owner's Director, based on annualised system support estimates. If the ITT is located with ITS, the Director (ITS) will resource these roles;

b. software licensing and vendor costs (including ongoing vendor maintenance and support costs) are carried by the Director (ITS) for recognised Tier 1 and 2 systems;

c. minor change commitments are carried within BSG and ITT resources based on availability and other commitments;

d. service improvement commitments are carried by projects resourced by the University at the time of commitment to the improvement;

e. platform (back-office) costs such as infrastructure, are carried by the Director (ITS) where the enterprise system is managed within ITS;

f. life-cycle and life-extension analyses is used by the University to provide for future service improvement budgeting where prudent to do so; and

g. if not included as part of major project, education and training costs are carried by the Director (ITS) or the system owner's Director, depending on content (business processes or technical skills etc.).

36. Funding to achieve business transformation is included in the project budget to ensure the investment in technology aligns with the strategic objectives of the University.

Vendor management

37. The initial vendor relationship and contract is established jointly by the system owner with the support of the Director (ITS) or nominated delegates.

38. Vendor payments:

a. initial payment and funding is managed by the system owner with the support of the Director (ITS); and

b. ongoing payments to the vendor is funded via the ITS recurrent budget.

Enterprise architecture

39. ITS is responsible for the ANU Enterprise Architecture (EA) strategy and roadmap. Individual enterprise systems have a roadmap that aligns with this.

40. In conjunction with ITS, the BSG identifies services and capabilities required to deliver both University and local strategies. The BSG and ITS jointly develop the EA vision, including plans and roadmaps to deliver future services that can be achieved within the University's resource constraints. They select opportunities and solutions to cross the gaps between the current and future state.

41. The ITT develops the underpinning technology roadmaps and work with the BSG to implement the EA vision. This may be achieved by the selection and implementation of new enterprise systems, changes to existing enterprise systems, or by leveraging underutilised functionality.

42. All changes to licencing relating to enterprise systems are agreed by the Director (ITS) and the system owner, and follow ANU procurement processes.

43. Existing building block components such as systems, templates, integrations and tools are used to increase agility, improve quality of information and generate potential cost savings wherever possible.

44. The BSG provides solution architecture, in conjunction with the ITT, for each new system or change to existing architecture, including DR architecture.

45. Where possible all enterprise applications are mobile responsive, in particular in the case of student-facing systems.

46. All other enterprise applications are mobile compatible and configured in alignment with the *Information technology security policy*.

Enterprise system responsibilities

47. The responsibilities between the BSG and ITT are defined below. Agreement through Service Level Agreements (SLAs) and OLAs is established where responsibilities vary from the service catalogue, or more system specific information is required. System responsibilities include:

Responsibility	BSG	ITT
Day-to-day operations		
Systems monitoring		X
Production scheduling		X
Database administration and tuning		X
Helpdesk services (Levels 1 and 2 ITIL support)	X	
Level 3 ITIL support		X
Migration between development, testing and production environments		X
Application of patches and fixes		X
Testing and quality control	X	
User documentation/version control	X	

System documentation/version control		X
System support – primary support to keep the system running		X
Security		
Update role-based security (profiles)	X	
Update and maintenance of access controls (mechanism for access)		X
Application specific security		X
Intrusion and breach monitoring and prevention		X
Minor change		
Specification of change requests and transmission using service management system	X	
Applying configuration changes	X	
Customisation: Coding and application of change requests		X
Version control		X
Testing and acceptance of changes	X	
Migration of approved changes to production		X
Technical change management		X
Major change		
Preparation of proposals and associated business cases to support major functional change	X	
Preparation of proposals and associated business cases to support major technical change		X
Managing the technical installation and upgrade projects including		X

establishing the project and project team and undertaking technical and load testing		
Managing the functional installation and upgrade projects including establishing the project and project team and undertaking UAT testing	X	
Managing staff in business area	X	
Managing technical staff		X
Managing business communications and business change	X	
Managing technical communications and technical change		X
Life-cycle management		
Managing technical life of system from purchase to retirement or decommissioning		X
Managing functional life of system from purchase to retirement or decommissioning	X	
Reporting		
Reporting against performance measures i.e. up time		X
Reporting against functional audit recommendations/reviews	X	
Reporting against technical audit recommendations/reviews		X
Reporting against statutory requirements	X	
Reporting against business metrics	X	
Standard support hours		
Student and staff support provided during agreed hours i.e. 9:00am to 5:00pm Monday to Friday	X	
System support provided during agreed hours i.e. 9:00am to 5:00pm Monday to Friday		X

Provision of after-hours help desk support (seldom offered and requires discussion)	X	X
Provision of after-hours technical support		X
Risk		
Identify risks and plan for risk mitigation	X	X
Knowledge management		
Keeping current with sector knowledge ie. application functional knowledge and its fit for purpose status	X	
Keeping current with technology knowledge		X
Keeping current with technical roadmaps		X
Keeping current with vendor roadmaps	X	X
Strategy and planning		
Sets service strategic direction	X	
Sets technology strategic direction in conjunction with Enterprise Architect including 3 year portfolio and system planning		X
Determines priority of changes in conjunction of resourcing bandwidth	X	
Determines bandwidth of resources to manage changes	X	X
Enterprise architecture		
Minor changes to enterprise architecture	X	
Development, updating and storage of enterprise architecture strategy and roadmaps	X	
Development of technology roadmaps		X

Document information

Title	Enterprise systems management
Document Type	Standard
Document Number	ANUP_000738
Version	11
Purpose	This standard provides a framework for the governance and management of enterprise systems and defines the roles and responsibilities of Information Technology Services (ITS) and other business areas within ANU. These are required to ensure the security, availability, and integrity of enterprise systems.
Audience	Staff, Students, Alumni, Affiliates
Category	Administrative
Topic	Information Technology
Subtopic	Security
Effective Date	2 Apr 2019
Review Date	5 Apr 2024
Responsible Officer	Director, Information Technology Services (director.its@anu.edu.au)
Approved By	Vice-Chancellor (eo.vc@anu.edu.au)
Contact Area	Information Technology Services (policies.its@anu.edu.au)
Authority	AS ISO/IEC 27002:2015 Australian National University Act 1991 Australian Government Protective Security Policy Framework Public Governance, Performance and Accountability Act 2013 Public Governance, Performance and Accountability Rule 2014 Australian Government Department of Finance and Deregulation Finance Circular No. 2009/08 Crimes Act 1914 (Cth) Privacy Act 1988 Telecommunications Act 1997 Telecommunications Regulations 2001
	1504249905

Information Infrastructure and Services Rule 2020
Information Infrastructure and Services Order 2020

Printed On 3 Jul 2022