IT Service Ownership Standard

The purpose of this standard is to establish a common definition of IT Service Ownership and Service Owner responsibilities.

The standard is a foundational component for effective IT management and governance supporting:

- Clear accountability, roles and responsibilities for IT service and system management
- Consistency and quality of IT service delivery across UNSW
- Risk reduction for services and systems critical to UNSW operations

The standard applies to:

- All IT/technology services and systems at UNSW irrespective of which department service ownership resides

Version	Approved by	Approval date	Effective date	Next full review
1.0	Christine Burns	11/12/24	01/01/25	01/02/26
Accountabilities				
Responsible Officer		Mark Griffith, Director Customer Service Delivery		
Contact Officer		Cheri Watts, Head of Service Management Office		
Supporting Information				
Relevant University-wide Policy		n/a		
Supporting Documents		Service Management Processes Cyber policy and standards Application Software Maintenance Standard		
Superseded Documents		n/a		

1. High-level roles

Business Owners	Business Owners are accountable for the business capability being supported by the system/technology. They own the business outcomes delivered by the system. The Business Owner plays a strategic role defining the vision and communicating with key stakeholders. They work closely with the Service Owner, who is responsible for developing a roadmap that aligns with the vision.
Business Operations Owner	The Business Operations Owner provides support to end-users of the service and undertakes the day-to-day business responsibilities on behalf of the Business Owner. This role differs from that of the Service Owner and (technical) Delivery Owner whose focus is the support and maintenance of the underlying service technology.
Service Owner	The service owner is accountable for the end-to-end management of a specific IT service. They are responsible for service lifecycle management and roadmap. The service owner's accountability for a specific service is independent of where the underpinning technology components, services, or competencies reside.
Delivery Owner	The operational owner of day-to-day support and maintenance of the system.
Subject Matter Experts (SMEs)	Subject Matter Experts can be technical or business experts in the service, system and/or the processes it supports.

This standard focuses primarily on the **Service Owner** role.

2. Service management practices

Service practice	Description	Further information
Change and release management	Change Management is a set of processes and procedures that provide a systematic approach for managing changes to IT systems, services, and infrastructure to minimise business disruption. Release management refers to the process of planning, designing, scheduling, testing, deploying, and controlling software releases.	Change Management (SMO website)
Cyber security and regulatory compliance	Ensure ongoing cyber security policy and standards compliance. Cyber Security Risk Management Framework includes obligations across many control domains.	Cyber Security Policy and Standards
Financial, Budget and resource management	Reviews service budgets and expenditure plans to ensure financial health; manages all costs and resources required to deliver and manage the service. Financial management and vendor management are closely aligned.	
Information and Data Governance	Ensure data and information management in compliance with UNSW Data Governance Policies and Standards	Information Governance Policies and Standards
Incident Management	An incident is an unplanned interruption or reduction in the quality of an IT service. Incident management is the process responsible for managing the lifecycle of all incidents. Incident management ensures that normal service operation is restored as quickly as possible and the business impact is	Incident Management (SMO website)

	minimized. Including Major Incident Management and Post Incident Reviews.	
Maintain record of the service offering (CI) record in CMDB	Configuration Management Database (CMDB): The database in the organisation's ITSM tool, which at UNSW is *'CA Service Desk (CASD)'*, that holds information about the service including service name (CI), description, service role assignments, incident and support assignment groups. All incidents, requests and changes will be logged against this entry in the CMDB for service delivery.	Service Management Office Toolset
Preventative Maintenance	The planning and execution of proactive ongoing preventative maintenance required to keep the technology components current (within support and recommended security versions)	Application Software Maintenance Standard
Risk management	Identification, assessment and control of technical risks.	UNSW Risk Management
Security Patching	Timely application of relevant updates or fixes to software systems to address known vulnerabilities or security weaknesses.	
Service continuity and Disaster Recovery	A collection of back-up and recovery procedures to be followed in the event of a disaster or damaging event that affects UNSW IT services. A full test of the Disaster Recovery Plan is required to be performed annually for tier 4&5 critical systems. Includes completion of a Business Impact Assessment which determines technical service continuity requirements.	Service Continuity and Disaster Recovery - Service Management Office website
Service support model (Service Management Pack)	Service support model is captured in the Service Management Pack (SMP) which defines the key service attributes including service criticality, service level agreements, roles and support processes and groups responsible for the various technical parts of the service.	Service Management Pack - Service Management Office website
Service lifecycle management and roadmap	Creation of the service lifecycle roadmap that aligns with the vision of the Business Owner. The roadmap defines the activities of the service from launch through service improvement to service sunset.	
Service monitoring, alerting and reporting	Service monitoring is the process of monitoring service performance, availability, and end-user experience to ensure it is functioning properly. Includes both automated technical monitoring as well as manual service performance and compliance against SLAs.	
Solution Design and Technical Documentation	Solution architecture capturing the design of the application and its integrations. Technical and technical support documentation typically contained in Confluence (aimed at technical support staff not end-users)	Architecture Governance
User access management	Responsible for the process by which users are added and removed. Responsible for technical / privileged access management.	
Vendor and contract management	Ongoing supplier management and governance for IT service providers. Vendor management and financial management are closely aligned.	

3. Service practices mapped to business criticality

All IT Services have a criticality rating which is determined through a Business Impact Assessment as part of Service Continuity planning.

The following mapping of service dimensions to service criticality is a guide to advise which responsibilities apply to which services.

M	Mandatory	O	Optional

Service Practices (Service Owner = A/AR)	**Core**	**Mission Critical**	**Business Critical**	**Business Important**	**Non-Critical**
Change and release management	M	M	M	M	O
Cyber security compliance	M	M	M	M	M
Financial, budget and resource management	M	M	M	M	M
Incident Management	M	M	M	M	M
Maintain service offering (CI) in CMDB	M	M	M	M	M
Preventative Maintenance	M	M	M	O	O
Risk management	M	M	M	O	O
Security Patching	M	M	M	M	M
Service Continuity and Disaster Recovery	M	M	O	O	O
Service Lifecycle and roadmap	M	M	M	O	O
Service Support Model	M	M	M	M	O
Service monitoring, alerting and reporting	M	M	M	O	O
Solution design and technical documentation	M	M	M	O	O
User access management	M	M	M	M	M
Vendor and contract management	M	M	M	O	O

4. Responsibilities across roles

4.1. High-level RACI

Service dimension	Business Owner	Business Operations Owner	Service Owner	Delivery Owner
Change and release management	I	C	A	R
Cyber and regulatory compliance	A	R	R	R
End user support, documentation and training	I	AR	I	C
Financial, budget and resource management	C	C	AR	C
Incident Management	I	C	A	R
Information and Data Governance	A	R	R	I
Maintain service offering (CI) record in CMDB	I	C	A	R
Preventative Maintenance	I	C	A	R
Risk management	A	R	R	R
Security Patching	I	C	A	R
Service Continuity and Disaster Recovery	C	C	A	R
Service Lifecycle and roadmap	C	C	AR	I
Service monitoring, alerting and reporting	I	I	A	R
Service Support Model (Service Management Pack)	C	C	AR	I
Solution Design & Technical Documentation	I	C	A	R
User access management	A	R	R	I
Vendor and contract management	C	C	AR	C

4.2. Responsibility descriptions

Practice	Business Owner	Business Operations Owner	Service Owner	Delivery Owner
Change and release management	Approves service outages	Responsible for supporting system changes: providing business resources for UAT and communicating across business stakeholders	Accountable for compliance of change and release management to IT Standards	Responsible for managing changes to the system and controlled release management
Cyber and regulatory compliance	Accountable for managing cyber security risk	Supports the Business Owner in identifying and mitigating Cyber Security Risk	Supports the Business Owner in identifying and mitigating Cyber Security Risk and Responsible for managing the application of cyber security technical controls	Supports the Business Owner in identifying and mitigating Cyber Security Risk and Responsible for applying cyber security technical controls
End user support, documentation and training		Accountable and responsible for end user support and production and maintenance of end user training and documentation		Supports Business Operations where necessary
Financial, budget and resource management	Accountable for ensuring the service has the resources required and advocating for resources where necessary including major change projects	Management of business resources who contribute to delivering the service	Management of costs, payment of invoices, budgets and forecasting; Management of technical resources and resource allocation to delivering the service	May have delegated responsibility for managing resources contributing to delivering the service (for example, technical developers)
Incident Management		Support the Service and Delivery Owner to resolve incidents where necessary	Accountable for managing service incidents within Service Level Agreements, approving Post Incident Reviews (PIR) and ensuring PIR findings are actioned	Responsible for organising response and resolution to service incidents within Service Level Agreements; Responsible for managing major incidents and undertaking Post

				Incident Reviews (PIRs)
Information and Data Governance	Accountable for compliance with UNSW Data Governance Policies and Standards	Ensures that data is managed responsibly and in compliance with UNSW Data Governance Policies and Standards	Ensures that data is managed responsibly and in compliance with UNSW Data Governance Policies and Standards	Ensures that data is managed responsibly and in compliance with UNSW Data Governance Policies and Standards
Maintain service offering record in IT Service Management database			Accountable for service record quality and currency in the IT service management system	Responsible for maintaining the service record in the IT service management system
Preventative Maintenance	Approves service outages if necessary	Supports system maintenance including providing business resources for UAT and communicating across business stakeholders	Accountable for the planning and execution of preventative maintenance	Responsible for Preventative Maintenance Plans and ongoing execution of the plan including technology stack patching
Risk management	Accountable for the identification and assessment of service risks and associated action plans	Responsible for the identification and assessment of service risks and associated action plans	Responsible for the identification and assessment of service risks and associated action plans	Responsible for the identification and assessment of service risks and associated actions
Security Patching	Approves service outages if necessary	Supports the Service Owner where necessary in the application of critical patches	Accountable for the assessment of critical security patches and determining appropriate application timeline	Responsible for the application of relevant updates or fixes to software systems to address security vulnerabilities
Service Continuity and Disaster Recovery	Accountable for Business Continuity Plan	Responsible for Business Continuity Plan	Accountable for Disaster Recovery planning and testing for Critical Systems	Responsible for Disaster Recovery planning and annual testing for Critical Systems
Service Lifecycle and roadmap	Provides business strategy and requirements	Provides business requirements	Accountable and Responsible for the service lifecycle roadmap. The roadmap defines the activities of the	Supports the service lifecycle key milestones

			service from launch through service improvement to service sunset.	
Service monitoring, alerting and reporting			Accountable for designing and implementing appropriate service monitoring for performance and availability.	Responsible for implementing and operating service monitoring. Responsible for managing response to service monitoring events.
Service Support Model (Service Management Pack)			Accountable for production and sign-off of Service Management Pack (SMP)	Responsible for Service Management Pack (SMP); Ensures SMP is reviewed annually
Solution Design & Technical Documentation			Accountable for key technical documentation being produced and maintained: as a minimum high-level solution architecture and high-level integration documentation	Responsible for key technical documentation being produced and maintained: as a minimum high-level solution architecture and high-level integration documentation
User access management	Accountable for appropriate user access and annual user access reviews ensuring the principal of least privilege	Responsible for appropriate user access and annual user access reviews ensuring the principal of least privilege	Responsible for the process by which users are added and removed. Responsible for technical / privileged access	Responsible for managing privileged access – adding, removing and reviewing privileged access users
Vendor and contract management	Provides business strategy and requirements	Provides business requirements	Accountable and responsible for vendor and contract management of any suppliers in the delivery of the service, for example, software licensing, support or technical development.	Supports the Service Owner with reporting on vendor performance.

Revision History				
Version	**Approved by**	**Approval date**	**Effective date**	**Modifications**
1.0	Christine Burns, CIO	11/12/2024	01/01/2025	First Draft, Author: Sally Anderson, Directors, StARS IT