UNT System

IT Change Management Standard

Purpose

The IT Change Management Standard provides direction for a managed IT change environment that brings value to the UNT World through activities supporting the following goals:

- Establish best practices for managing changes to information resources.
- Ensure that changes are prioritized and scheduled to be in in alignment with business needs while ensuring service continuity.
- Minimize the impact and disruption of a change to IT services and business units.
- Reduce risks associated with change implementation.
- Ensure that stakeholders receive relevant and timely communication about changes.
- Maintain segregation of duties associated with changes.
- Maintain consistency throughout the life cycle of technology as changes are made.
- Foster a culture that embraces change management practices and ensure compliance with change management policies and standards.
- Ensure that changes create business value as qualified and quantified by customers by conducting performance and risk evaluation of changes that impact service availability.

Scope

The IT Change Management Standard acts the basis for change management practices. Change management activities include the planning, review, testing, approval, communication, implementation, evaluation, and documentation of changes. Standards noted in this document as well as those that are established to supplement these standards must align with the UNT System Information Security Handbook (Handbook). The Handbook is based on requirements of Texas Administrative Code 202 and the State of Texas Department of Information Resources Security Control Standards Catalog. Change management controls are found in the following sections of the Security Control Standards Catalog:

CM-1 Configuration Management Policy and Procedure
CM-2 Baseline Configuration
CM-3 Configuration Change Control
CM-4 Security Impact Analysis
CM-5 Access Restrictions for Change
CM-6 Configuration Settings
SA-10 Developer Configuration Management

UNT SYSTEM

Change Management Terminology

Accountable (A). In a RACI responsibility assignment model, the Accountable role is assigned to the individual that is the owner of change activities and ultimately answers for all tasks, decisions, and completion of change management work.

Change. A Change is the addition, modification or removal of software, hardware, communications equipment, applications, environmental control systems, networks, data, or systems. The scope of a change may include maintenance and changes to information resources, configuration items, processes, and documentation. A change may be standard, normal or an emergency change.

Change Advisory Board (CAB). A Change Advisory Board is a group of representatives of service groups that support the authorization, assessment, prioritization, scheduling, approval, communication, and post implementation review of changes. A CAB includes representatives from IT teams that have responsibility for supporting changes to information technology or may include representatives that are impacted by changes made to information technology. Representatives may also include service providers, representatives of business units, or representatives of the emergency change advisory board.

Change Initiator. Change Initiators are individuals responsible for submitting a request for a change. A change initiator may be a customer, IT representative or an individual acting on behalf of a business unit.

Change Management. Change Management is the formal process for making changes to IT services. Change management activities include the planning, evaluation, review, approval, communication, implementation, and documentation of changes.

Change Manager. A Change Manager is the individual responsible for guiding the application and adherence to the change management policy and standards. The person who takes on this role will be responsible for facilitating CAB meetings and may also have responsibility for ensuring that changes adhere to change management standards.

Consulted (C). In a RACI responsibility assignment model, the Consulted role is assigned to the individual or individuals that are consulted prior to a final decision or action. The individual(s) act as subject matter experts and their opinions are sought in regard to activities or aspects of a change.

Customer. A Customer is representative of a business unit that receives an IT service.
Data. Data is information that is stored or produced in a structured or unstructured format (e.g., electronic file, email, etc.). Data may be used to calculate, analyze, or in planning.

Emergency Change. An Emergency Change is a change that must be implemented as soon as possible to address an issue that may impact service levels or may significantly increase risks to an IT service if not implemented. Emergency changes may be needed to resolve a major incident, to preserve data, or to implement a critical security patch.

Emergency Change Advisory Board (ECAB). An Emergency Change Advisory Board is an emergency CAB created to handle a particular emergency change. Representatives of the ECAB includes CAB members and individuals that hold expertise needed to assist with reviewing, resolving, or making the emergency change.

Hardware. Hardware includes physical components of an information resource, such as computers, printers, communications equipment and other types of information resources.

Impact. Impact is an estimate of a potential loss associated with an identified risk.

Information Resource. Information Resources are the procedures, equipment, and software that are employed, designed, built, operated, and maintained to collect, record, process, store, retrieve, display, and transmit information, and associated personnel including consultants and contractors.

Informed (I). In a RACI responsibility assignment model, the Informed role is assigned to individual that must be informed after a decision or action is taken regarding a change.

Normal change. A normal change is any change that is not a standard change or an emergency change, and may be required to resolve a problem, or to modify underlying infrastructure.

Priority. Priority means the order in which changes should be considered and implemented.

RACI. RACI is an acronym for four key responsibilities: Responsible, Accountable, Consulted, and Informed. It is used to clarify responsibilities in cross-functional or departmental initiatives and describes the participation of various roles in completing change tasks or activities.

Request for Change (RFC). A Request for Change is a formal proposal for a change to be made. An RFC includes details of the proposed change.

Responsible (R). In a RACI responsibility assignment model, the Responsible role is assigned to the individual that completes a change task.

Risk. Risk means the impact of an adverse effect from a change compared with the likelihood of the success of the change.

Segregation of Duties. Segregation of Duties is a control that ensures that separate individuals are responsible for initiating and implementing tasks that involve migrating changes from one

environment to another. Segregation of duties is applied in order to reduce opportunities for the introduction of fraudulent, malicious, unauthorized, or unintentional modifications without detection.

Service. A means of delivering value to customers by facilitating outcomes customers want to achieve without the ownership of specific costs and risks. An IT service is made up from a combination of people, processes and technology.

Service Level Agreement (SLA). A Service Level Agreement is a component of a contract that defines the services and agreements that a service provider will provide to a service user. An SLA establishes a required level or standard for the identified services such as identification of services that will be made available to the service user, service availability times, service recovery times, and other pre-defined expectations.

Software. Software is a set of instructions, data, or programs used to operate and execute specific tasks. Examples include operating systems, utility software (e.g., Computrace, anti-virus, etc.), and business application (e.g., Microsoft Office, Visio, SQL Server, etc.) that run on an information resource.

Standard Change. A Standard Change is a pre-authorized change that is low risk, relatively common, and follows an established procedure or work instruction on a recurring basis.

Guiding Principles of Change Management

Practices and Procedures

Information resources that are critical, mission essential, store or process confidential data, or systems that that require high-availability such as infrastructure systems are subject to change management practices and standards. Low risk systems that are not essential to university operations, do not host or process confidential data, or do not require high-availability may not require full implementation of the requirements of this change standard unless the low risk systems pose a threat to the confidentiality, integrity, or availability of network services or security of operations.

Change management practices and procedures must include documentation of the activities that are associated with making changes, a description of the change, impact assessment; approvals for the change; implementation plans; pre-testing results; post-implementation testing; and a post-implementation review. See Initiating Change Requests (below) for more information.

Planning and Communications

Implementation plans must include pre-testing, communications, schedules, and a back-out plan. Change plans and assessments must be prioritized and scheduled to align with business needs and IT operational schedules to ensure service continuity, minimize the occurrence of conflicting changes, and potential disruption to supported environments.

Communication plans must be established that include notifying customers and service providers about changes prior to implementation and after changes occur.

Backout plans must be established to ensure that services can be restored in the event that the change fails or does not support intended results.

Risk Assessment

Risks to technology, risks to service availability, and risks to business operations must be considered. Answer the questions below and use the chart to determine risks associated with a change.

Likelihood of success:

- Experience – How many times have we successfully done this change before?
- Testing – How extensively has the team tested this change (proved by evidence)?

Impact:

- Criticality – What is the business criticality of the affected service(s)?
- Complexity – How many users will a failure of this change impact? How visible is this change?
- Duration - How long is the service outage?
- Recovery – If the change fails, how long will it take to recover?

Risk Calculation

		Adverse Impact (Risk)			
Likelihood of Success		VERY HIGH IMPACT • Critical service • Majority of users impacted • service outage exceeds SLA • recovery time exceeds SLA	HIGH IMPACT • Critical service • > 50 users impacted • service outage exceeds SLA • recovery time exceeds SLA	MODERATE IMPACT • Non-critical service • < 50 users impacted • service outage within SLA • recovery time within SLA	LOW IMPACT • Non-critical service • < 10 users impacted • no service outage • no recovery time required
	LOW LIKELIHOOD • Previously unsuccessful or no experience • Untested	VERY HIGH RISK	HIGH RISK	MODERATE RISK	LOW RISK
	MODERATE LIKELIHOOD • Previously successful after issues • Unit tested	HIGH RISK	MODERATE RISK	MODERATE RISK	LOW RISK
	HIGH LIKELIHOOD • Previously successful Unit tested, quality assured and UA tested	MODERATE RISK	LOW RISK	LOW RISK	LOW RISK

Setting Priorities for Change

Changes must be prioritized based on impact to the business and the urgency of the change in order to reduce potential disruption to supported environments. Using the conditions identified in the Priority Matrix below, determine the impact and urgency of the change (high, medium, or low).

Priority Matrix

Impact	Urgency: High	Urgency: Medium	Urgency: Low
	• Incident rapidly increasing in scope • Time sensitive work impacted • Several VIP users impacted • Confidential data potentially exposed	• Incident scope increasing over time • VIP user impacted	• Incident scope not increasing or increasing slowly • Any work impacted is not time sensitive
High • Critical Service is affected • Confidential data breached • Large number of users affected • High financial impact • Impact to reputation is great • Life-safety concerns	-1-	-2-	-3-
Medium • Moderate number of users affected • Moderate financial impact • Reputation of the institution could be moderately affected	-2-	-3-	-4-
Low • Very few users impacted • Low financial impact • Little to no impact to reputation	-3-	-4-	-5-

Priority 1 ratings are critical and must be implemented immediately in order to mitigate critical risk to the organization. The ECAB may be convened to address this priority.

Priority 2 ratings have high priority and must be scheduled and implemented soon. The ECAB may be convened to address this priority.

Priority 3 ratings have moderate priority and may be considered a normal or standard change.

Priority 4 ratings have low priority, low risk and result in a low impact to the organization. There is no urgency in mitigating risk, though the change should be implemented.

Priority 5 ratings have low priority, low risk, and a limited number of users are impacted. There is no urgency in mitigating risk and the work is not time sensitive.

Responsibilities for Changes

Roles and responsibilities for Individuals that are responsible for supporting changes are outlined in the RACI Chart below. These individuals must be identified and made aware of their roles and responsibilities.

RACI Chart

	Responsible Positions / Activities	IT Leadership	Requestor \ Initiator	Change Manager	Change Advisory Board / Change Review Team	Emergency CAB / Emergency Change Team	Development/ Implementation Team	Development/Implementation on Team Lead/Supervisor	Customer / End Users
Change Management	**Initiate Request / Submit RFC**		R	A	I				I
	Filter requests / Allocate Initial Priority	A	I	R	I				
	Change Assessment / Planning		R	A	R		C/I		
	Change Approval			R/A	R	R			
	Coordinate Change Implementation*			A			R		C/I
	Approve Change Implementation*				I			R/A	
	Change Evaluation and Closure		C	R/A			C		C
	Communication Plan		R/I	A	R		R		I
	Emergency Change Handling		R	R/A		R	R		C/I

Approving Changes

Changes must be communicated to stakeholders that include the work that is to be done, expected outcomes, and must be approved prior to submission to the change advisory board or IT group that is responsible for reviewing or approving the change. Communications, expected outcomes, and approvals must be documented and retained in change records.

Pre-Implementation Testing

Changes must be tested prior to implementation to ensure that the change resulted in desired effect and also to ensure that there is no negative impact to services during implementation. In cases where changes are made by a third-party, obtain relevant information from the third-party about the change including release notes, descriptions of change, and their testing results. Consider the following during testing:

- Where possible, test the change in a non-production environment to ensure that there are no disruptions or adverse impacts to the system or service.
- Collaborate with customers, business unit, and IT personnel as appropriate to verify and validate that the change worked as intended.
- Verify that the change is compatible with other systems and/or software, e.g., browsers, operating systems, mobile devices, and hardware versions as applicable.
- Determine if the change alters the security of the service, e.g., opens ports, allows privileged access, restricts or blocks access, etc..
- Verify that system or application performance is altered or causes a negative impact as a result of the change.
- Verify that the appropriate user roles are able to access the system or service as intended.
- Verify that data are made available to authorized users only and that no vulnerabilities were introduced that would allow unauthorized parties to access, view, or use data.
- Obtain written approval from customer, business unit, and IT personnel as appropriate to proceed with the change prior to implementation.
- Record the results of pre-testing, names of individuals involved, and dates.

Scheduling Changes

Changes must be scheduled such that they are not disruptive and to ensure that occurrence of conflicting changes is minimized.

Initiating Change Requests

Change requests must be submitted to the change advisory board or the applicable IT group that is responsible for reviewing the change prior to implementation. Change requests must be submitted in the manner specified by the change advisory board or IT group. Change requests must include the following documentation:

- Name of Change
- Name of system or application that is affected by the change
- Name of Change Initiator
- Type of Change
- Detailed Description of Change
- Proposed Date and Time of Change (Start and End)
- Stakeholder Names
- Business Justification for Change including significance to business
- Impact to business unit operations
- Approvals from stakeholders to proceed with change
- Priority of Change
- Change Deployment Plan inclusive of expected results
- Resources needed to conduct change
- Risk Assessment results including likelihood of success and impact

- Technical impacts to the primary system that is undergoing the change as well as identification and impact to other systems or services that might be affected by the change, e.g., operating systems, databases, servers, disaster recovery plans, backup requirements, storage requirements, and other supporting infrastructure
- Implementation team member names and responsibilities of each team member (e.g., developer, tester, implementor, approver)
- Documented evidence of segregation of duties maintained between roles, e.g., developer, tester, implementor, and approver
- Security controls that are established to ensure the confidentiality, integrity and availability of data and the information resource undergoing the change
- Pre-Testing Results
- Backout plan
- Communication plan for notifying customers and service providers impacted by the change (send communications prior to change and after change)
- Third Party change information (if change is conducted by third-party):
    - Third Party service level agreement
    - Third Party change management procedures
    - Third Party change results

Change Advisory Board Meetings/Change Review Meetings

The CAB or IT team if no CAB has been established will hold regular scheduled meetings to review, approve, or deny change requests that are submitted. Additional meetings may be called as needed or canceled if no changes are scheduled. Meetings may be conducted in-person or facilitated by technology such as email, teleconference, or videoconference.

The Change Manager or designee is responsible for convening and chairing the change review meetings, and will distribute an RFC docket to change team members prior to the scheduled meetings.

The change review team will review RFCs and take appropriate action. Actions may include approving, denying, postponing, or grouping changes as deemed necessary. The change review team may request additional information from the change initiator.

Emergency Change Advisory Board Meetings/Emergency Change Meetings

An ECAB (or IT emergency change review team if no ECAB has been established) may be held in the event that risk and priority necessitate an emergency change. The Change Manager or designee is responsible for convening an emergency change meeting. Representatives of the change review team and change implementation team that would be responsible for providing information about the emergency, stakeholders (as appropriate), as well as individuals that would be responsible for facilitating the change should be present. Change management procedures must be maintained for emergency changes.

Implementing Changes

The change initiator implements a change in accordance with the implementation plan and during the scheduled time. Failure of an implementation will normally require the change initiator to follow the back-out plan to ensure normal system operations.

Post Implementation Testing and Review

Post implementation testing activities must be conducted and documented in order to determine if the results of the change occurred as expected. In addition, a review of change activities should be conducted to capture lessons learned and potential improvements that can be made for future changes. Post implementation reviews may be conducted in CAB or change review meetings.

References

ITIL v3 2011 edition Service Transition
Texas Department of Information Resources Security Control Standards Catalog
University of North Texas System Information Security Handbook

DOCUMENT VERSION LOG			
Version	Approved By	Date	Description
1	Charlotte Russell, Chief Information Security Officer	8-31-2021	New Standard for IT Change Management