-->

Change Enablement Standard

Last Modified on 05/18/2026 2:59 pm EDT

For more details about the Information Security Office, **please visit our website**!

1. Introduction

The Wharton Change Enablement Standard outlines the activities, decisions, and outputs required for submitting and approving changes to Information Technology (IT) systems and services within the Wharton environment. The change enablement process ensures that all modifications are completed through a structured and transparent workflow, allowing for sufficient review, approval, and secure implementation of changes.

This Standard describes the workflow for planning, submitting, approving, implementing, and reviewing changes to production and disaster recovery environments.

Wharton departments and centers are responsible for managing their own change enablement process, documentation, etc. A department or center may elect to participate in Wharton Computing's change enablement process. If a department chooses to establish their own process, that process should be documented and available for audit/review by ISO. All Wharton groups must align with this Standard.

1.1 Standard Owner

Wharton ISO is accountable for the development and maintenance of this Standard, in alignment with University and Wharton policies.

Process owners for authorized change bodies are responsible for implementing change enablement for their services.

1.2 Purpose

The purpose of this Standard is to ensure that all Requests for Change (RFCs) are reviewed and approved in a consistent and risk-aware manner, minimizing the impact of change-related incidents on the secure operation of Wharton's IT systems and services.

The process fosters:

- Transparency among stakeholders.
- Review and approval by subject matter experts (SMEs) and governance bodies (CABs).
- Secure and reliable implementation.
- Oversight via a Change Advisory Board(s).

1.3 Scope

This Standard applies to all changes (additions to, modifications of, or removals from a service) introduced into

Production and Disaster Recovery environments for Wharton-managed services. It includes employees, contractors, and third-party providers who implement or support changes in these environments.

Service Requests (e.g., individual user account adjustments) are managed under the separate Request Management process and are not covered by this Standard unless explicitly designated as a change.

1.4 Compliance

This Standard complies with University and Wharton information security requirements and industry best practices (e.g. ITIL Change Enablement, NIST SP 800-128). All stakeholders must adhere to this Standard when submitting or approving changes.

1.5 Key Roles & Responsibilities

Role	Responsibilities
Change Requester	Initiates and prepares a Request for Change (RFC) in an Enterprise Service Management (ESM) system or equivalent documentation repository. Provides required documentation and classification inputs.
Change Owner	Owns the RFC from submission through closure. Ensures implementation, documentation, testing, communication, and post-implementation review are completed.
Technical/SME Review Team	Reviews RFCs for technical feasibility, risks, and impacts. Approves or rejects changes within assigned authority.
Change Advisory Board (CAB)	Comprised of service/system SMEs and stakeholder representatives. Reviews and votes to approve or reject Medium and Large changes, as well as Emergency and Confidential changes. Regular meeting cadence is required.
Emergency-CAB (E-CAB)	Designated CAB representatives authorized to review and approve emergency changes on a 24x7 basis. Verbal approval is sufficient for immediate implementation.
Wharton Computing ISO	Informed of and/or reviews confidential changes and determines security handling requirements. Advises on risk/impact as needed. Maintains this Standard.
Change Calendar Administrator	Ensures approved changes are recorded in ESM system and reflected on a Change Calendar.

2. Change Classifications

Changes are classified to ensure appropriate review and approval paths. Any change process should include lead times to facilitate appropriate review.

2.1 Normal Changes

Normal changes are automatically classified as **Small, Moderate, or Large** based on responses to a standardized risk/impact questionnaire within the ESM system ticketing system.

Risk / Impact	Low	Moderate	High
Low	Small	Moderate	Moderate
Moderate	Moderate	Moderate	Large
High	Moderate	Large	Large

- **Small Change:** Low overall risk/impact. Requires SME review only.
- **Moderate Change:** Moderate risk/impact. Requires SME review and CAB approval.
- **Large Change:** High risk/impact. Requires SME review, CAB approval, and representation at the next CAB meeting.

2.2 Standard (Pre-Approved) Changes

Routine, low-risk activities that are pre-approved and listed in Wharton Computing's Standard Change Catalog.

- No lead time required; no additional CAB review.
- Must use the designated ESM system template for tracking and calendar visibility.
- The CAB reviews and updates the catalog regularly.
- Items that repeatedly fail may be removed from the catalog and reclassified as normal changes.

2.3 Emergency Changes

Required to resolve or prevent a **Sev-1 incident** (critical service outage, major security breach, or imminent high-impact issue).

- Require explicit **E-CAB approval** (verbal approval acceptable).
- Must be documented in ESM system after implementation.
- Reviewed retrospectively at the next CAB meeting.
- Must reference the associated Sev-1 incident number where applicable.

2.4 Confidential Changes

Certain sensitive changes may require confidentiality.

- Must notify and get approval by Wharton's Information Security Office (ISO) to implement a confidential change.
- Documentation is securely stored by ISO, with only necessary details shared with CAB.
- Workflow for confidential changes is being incorporated into ESM system.

3. Severity Definitions

Wharton aligns with University definitions for service severity (Sev-1 through Sev-4) and critical components.

- **Sev-1**: Critical outage or imminent risk, no workaround, requires emergency change.
- **Sev-2:** Significant performance or partial outage, workarounds exist.
- **Sev-3:** Low or minimal impact, non-critical systems affected.
- **Sev-4:** No significant impact, non-critical systems affected.

Critical components are defined by the University as servers or applications whose compromise could cause significant harm (legal, reputational, operational, or confidentiality-related).

4. Compliance & Enforcement

All implemented changes must comply with this Standard. Non-compliance, including unauthorized changes, will be subject to review by Wharton ISO, with corrective actions as required.