

State of Kansas
Department of Administration
DISC

Change Control Process Guide

Version 3
Jan-11

TABLE OF CONTENTS

1. ABOUT THIS DOCUMENT.....	3
2. OBJECTIVE.....	4
PROCESS OBJECTIVES	4
PROCESS GOALS	4
STRATEGY	5
3. SCOPE.....	6
ORGANIZATIONAL SCOPE	6
TYPES OF COMPONENTS.....	6
SPECIAL ACTIVITIES	6
4. CONCEPTS AND DEFINITIONS.....	8
CHANGE	8
MAINTENANCE	8
PRODUCTION	8
RISK	8
IMPACT.....	9
IMPACT AND RISK	9
PROJECT-ORIENTED PERSPECTIVE	10
5. CHANGE CLASSIFICATION METHODOLOGY.....	11
OVERVIEW	11
CHANGE CATEGORIES.....	11
IMPACT AND RISK LEVELS	14
IMPACT AND RISK FACTORS	14
<i>Risk Factors</i>	15
<i>Impact variables</i>	16
ASSESSING IMPACT AND RISK	17
LEAD TIME AND CHANGE APPROVAL REQUIREMENTS	19
<i>Lead Time Requirements</i>	19
<i>Change Approval Requirements</i>	19
6. ROLES AND RESPONSIBILITIES.....	21
CHANGE CONTROL PROCESS OWNER.....	21
CHANGE REQUESTER.....	21
DATA CENTER CHANGE COORDINATOR.....	22
CHANGE REVIEW TEAM	22
<i>DISC Deputy Directors</i>	23
SUMMARY OF ROLES AND RESPONSIBILITIES	23
7. PROCESS FLOW.....	25
PHASE 1: NOTIFICATION	25
PHASE 2: REVIEW	26
PHASE 3: SCHEDULING	26
PHASE 4: FINAL APPROVAL	26
<i>Decision appeal</i>	27
PHASE 5: IMPLEMENTATION.....	28
PHASE 6: FOLLOW-UP	28
8. NON-STANDARD CHANGES	29
EMERGENCY CHANGES	29
EXCEPTION CHANGES	30

9. APPLICATIONS DEVELOPMENT STANDARDS AND PROCEDURES.....31

POLICY FOR SHARP AND SMART SYSTEM CHANGE MANAGEMENT.....31

STEERING COMMITTEE31

APPLICATION SOFTWARE CHANGE CATEGORIES.....32

POLICY FOR KIRMS SYSTEM CHANGE MANAGEMENT33

KIRMS MANAGERS GROUP34

CHANGE IMPLEMENTATION.....34

10. REPORTING.....35

11. ADDENDUM 136

1. About this document

Change control, as described in this document, is a **process discipline** established to ensure the achievement of the Information Technology Management Plan Goals and Objectives. The disciplines described in this document are to be followed by the Department of Administration, Division of Information Systems and Communications (DISC) and its business partners as they provide data center, network and application support services.

As a process discipline, change control is comprised of an overall process **architecture** that is realized through a variety of supporting **sub-processes** and standardized **procedures**.

This document formally defines the process structure that achieves the stated Change control process objective, outlining a standardized and repeatable methodology that assures continuous improvement in process effectiveness over time.

When changes are made, consideration must be given to the Disaster Recovery Plan.

2. Objective

Change control is an on-going process designed to *safeguard the production service delivery environment against changes that:*

- *are potentially disruptive, or*
- *carry unacceptable levels of service level risk*

Through the Change control process, the *implementation of changes affecting the production environment is centrally controlled, encompassing change planning, communication, scheduling, approval, monitoring, verification, measurement, and reporting.*

Process objectives

DISC is committed to delivering information services of exceptional quality, and the Change control process has been implemented to assure *DISC consistently meets--and surpasses--the service expectations of its customers.*

Process goals

The broad process objective is realized through constant focus on the supporting process goals outlined in the table below.

Change Control Process Goals	
1. SERVICE LEVEL EXCELLENCE	<i>Changes introduced do not interfere with the achievement of explicit or implicit service level commitments to business partners and customers</i>
2. HIGH AVAILABILITY	<i>Unavoidable change-related service disruptions are kept to an absolute minimum</i>
3. STRATEGIC SUPPORT	<i>Changes must conform to stated business and technical plans and strategies</i>
4. EFFICIENCY	<i>Changes are processed promptly, efficiently, and in a non-bureaucratic manner, appropriately blending formality with effectiveness.</i>
5. COMMUNICATION, COORDINATION	<i>Changes are communicated to all affected parties, internal and external to DISC, in a timely and informative manner</i>

6. PARTNERSHIP

All stakeholders, internal and external to DISC, provide informed consent prior to proceeding with change implementation

7. CONTROL

Changes are implemented in accordance with scheduled implementation dates and installation windows or as agreed to by customers.

8. RELIABILITY

Changes are implemented in an orderly and consistent way using established (and repeatable) methods and procedures

9. CONTINUOUS IMPROVEMENT

Change activities are measured, correlated to the problem management process, and reported. Experience gained is incorporated into change policies and practices, creating a "learning" organization.

Strategy

The change process is based upon a strategy of **engagement** that encourages DISC and its customers **to cooperatively manage risk** as changes are introduced into a dynamic and complex service environment. Process mechanisms allow DISC and its partners to:

- **collaboratively assess the overall level of "readiness"** to proceed with the implementation of a production change, and
- **make mutually informed decisions regarding acceptance of, and responsibility for, all change risks**, confident that *prior to implementation*, all necessary and reasonable preparatory actions have been taken to mitigate those risks, and that, *following implementation*, prompt and appropriate action will be taken in response should any change-related service incident materialize.

3. Scope

Any change affecting any component of the DISC production service environment falls within the scope of the Change control process. In addition, *certain types of special activities and processing events* are within the scope of the process.

"In scope" as well as "out of scope" changes and activities are discussed later in this section.

Organizational scope

The Change control process and supporting procedures apply to all employees of DISC.

Types of components

The following general types of components, when deployed in support of the DISC production service environment, are subject to the change control process:

- *Application software*
- *Database*
- *System hardware*
- *System software*
- *Network hardware*
- *Network software*
- *Security*
- *Facilities*
- *Operating procedures*

Note that "in-scope" components are not limited to those service elements that a customer is able to perceive directly. Quality service delivery requires that attention be focused on a broad array of "internal" components (including procedures) that support production service delivery activity.

Special activities

Special activities that **require production resource alterations or scheduling consideration** also fall within the scope of change control. Formal application testing events—e.g., application stress, performance, or acceptance testing—need to be coordinated through the change process, as do authorized product demonstrations conducted in connection with marketing efforts.

In addition, ***exceptional production processing events***—for example, special year end processing or predictable fluctuations in transaction volumes attributable to normal business cycle events—need to be communicated and coordinated via the change control process.

4. Concepts and definitions

Precise nomenclature is critical to constructing a solid process foundation. If key words or concepts are unclear, personnel with dissimilar process or organization backgrounds are almost certain to interpret the same statement or passage in different ways, and process effectiveness may be compromised as a result.

To mitigate the risk of misunderstanding, this document:

- **employs terminology believed to be common to the information technology industry**
- **defines terms explicitly** to eliminate ambiguity, where necessary
- **uses context** to reinforce intended meanings

Change

Generally, any intentional event that alters the production environment is viewed as a change.

For purposes of this process, a change is even more specifically defined as **“the introduction or modification of any component in the production environment.”**

Maintenance

The term "maintenance" describes a specific subset of changes performed:

- to eliminate potential sources of service interruption by means of a "preventive service" program, or
- to adjust (or repair) components that are operating outside of recommended specifications

Routine maintenance changes typically follow well-established and well-practiced procedures and often merit very little change control focus beyond basic scheduling.

Production

The term **“production”** (a.k.a. **“live environment”**) refers to the human and technological means through which DISC services—*subject to explicit or implied service level commitments*—are delivered to its customers.

Risk

The term “risk” is generally regarded as an “exposure to loss.” In the context of Change Control, risk is defined as **“the potential threat a given change may pose to**

the stability of the production environment.” (By “stability,” we mean a state in which services are delivered consistent with established commitments, without degradation or unplanned/unscheduled interruption.)

It is a fundamental precept of change control that some degree of ***risk is inherent in any change.*** Furthermore, because component relationships and dependencies can be quite sensitive, the level of risk often increases dramatically as the volume of change increases. Indeed, industry research has demonstrated that the vast majority of production incidents are the direct result of recently installed changes.

Risk is a relative term, operating along a continuum that extends from very low to very high. It is often useful to think of risk as a ***probability indicator that reflects “the overall likelihood of encountering a failure during, or as a consequence of, a production change implementation.”***

Mitigating and ***managing this risk is the fundamental challenge*** in change control.

Impact

For purposes of change control, “impact” refers to the ***“overall visibility of a change”*** or ***“the relative importance that a stakeholder attaches to the timely and successful implementation of a given change.”***

As is the case with risk, impact is a relative term that functions along a continuum extending from very low to very high.

For DISC, impact is most effectively expressed in terms of disruption to service: ***What is the consequence to customers of a disruption in service caused by a given change not being implemented on schedule or failing after implementation?***

Procedures must address: Who is affected, business impact, who to notify, how they are to be notified, the logging requirement and reporting

Of course, other variables may enter into the impact equation, depending upon specific circumstances. They could include such things as financial and health impacts.

Impact and risk

Together, ***“impact and risk”*** provide change control participants a rather simple but effective conceptual framework for thinking about change. Viewed in combination, the terms “impact” and “risk” allow DISC to balance the likelihood of change failure against the potential consequences of that failure (or delay).

When expressed quantitatively, impact and risk offer a concise measure of a given change’s relative significance. Such a measure is then used to determine the level of change control attention that should be devoted to a particular change.

Project-oriented perspective

While, in the strictest sense, a change takes place at the level of an individual component, **as a practical matter, only rarely does a change occur in isolation.** There are two basic reasons why such is the case:

- **Project complexity:** Delivery of new or enhanced service often involves the carefully timed and coordinated migration of multiple inter-related components. A project affecting only a single component is the exception—not the rule.
- **Environment dynamics:** The dynamic nature of the production service environment often requires that multiple, independent project-related changes be introduced simultaneously. Consequently, even the simplest project needs to be considered in the larger context of changes to the entire environment

The effect of such complexity on the administration of the change process is considerable. If a change request involve alterations to multiple inter-related components—and these same components are also being altered by a second change request that must be completed at the same time—change risks can escalate rapidly.

A standard point of view is needed to allow process participants to manage this complexity. To balance both efficiency and effectiveness, the process adopts a **project-oriented perspective**, approaching implementation planning in terms of:

- **Individual project viability** (keeping in mind that any given project may involve modification to multiple components)
- **Multiple-project compatibility** (in terms of ability to be implemented simultaneously within the available production change window and then successfully coexist with all other production components)

This is **not** intended to suggest that change control is not also vitally concerned with individual tasks. On the contrary, it is recognized that the successful completion of each implementation task is critical to success; however, viewing a task in the context of the larger project offers the most meaningful way to assess “readiness” from a change control perspective.

5. Change Classification Methodology

Overview

To facilitate the systematic handling of a wide variety of changes in a complex environment, change control relies upon a classification scheme. Under this scheme, each **change is analyzed and classified according to:**

- **Nature or type of change**
 - **Degree of Complexity**
 - **Number of components affected**
 - **Scope of control, DISC versus Service Provider**

- **Associated impact and risk level**
 - **Number of customers potentially affected**
 - **Nature of work potentially interrupted**
 - **Likely duration of potential outage**

Together, these two indicators:

- **establish most of the basic process requirements** to be satisfied in connection with a given change, and
- **form the foundation for most process-related reporting**

In this section, we:

- **explain the classification scheme** in greater detail
- **describe the general criteria used in the classification process**
- **outline the general process requirements** associated with specific indicator values

Change categories

Broad categories of change components were presented in the earlier discussion of process scope.

While by no means offering an exhaustive list, the table below expands upon these component types, providing general examples that help illustrate classification structure

<i>Classification of Changes by Category</i>	
APPLICATION SOFTWARE	
USER-ORIENTED APPLICATIONS <i>(e.g., STARS, SHARP, Budget, DofA WEB page)</i>	<ul style="list-style-type: none"> ➤ Develop or install new application program modules ➤ Develop or Enhance existing Web sites (e.g., expand functionality, access additional data sources) ➤ Maintain existing Applications and Web site (e.g., change referenced file name in response to change implemented by information sharing partner, or improve usability)
OPERATIONAL SUPPORT UTILITIES	<ul style="list-style-type: none"> ➤ Deploy or Modify internally developed operational procedures ➤ Deploy new support utility
DATABASE	
<i>(e.g., Oracle, DB2, SQL Server)</i>	<ul style="list-style-type: none"> ➤ Migrate Application to new Ver/Rel of database software ➤ Add, modify, delete fields, entity relationships ➤ Performance tuning
SYSTEM	
HARDWARE	<ul style="list-style-type: none"> ➤ Install, modify/upgrade, or de-install physical enterprise level hardware devices such as servers (application, data base, WEB), storage devices (tape and disk), printers, cables
SOFTWARE <i>(e.g., OS390, Solaris, NT, Oracle, DB2)</i>	<ul style="list-style-type: none"> ➤ Install, upgrade, modify or de-install third-party software products that support <i>customer application</i>. Includes operating systems, database products, and application development tools. ➤ Activation of new system software feature/function ➤ System tuning
NETWORK	
HARDWARE	<ul style="list-style-type: none"> ➤ Install, upgrade, modify, de-install or other <i>physical</i> change to enterprise communications hardware such as hubs, router, switches, firewall, and fiber cables.
SOFTWARE <i>(NOS, FTP, etc)</i>	<ul style="list-style-type: none"> ➤ Install, upgrade, modify or de-install third-party software products that support the communications environment ➤ Other changes to logical network environment ➤ Performance tuning
SECURITY	
SYSTEM	<ul style="list-style-type: none"> ➤ Logical (software) changes to system access, capabilities
NETWORK	<ul style="list-style-type: none"> ➤ Logical (software) changes to firewall and other network security devices
APPLICATION	<ul style="list-style-type: none"> ➤ Define or delete users ➤ Modify user access rights
FACILITIES	
OFFICE	<ul style="list-style-type: none"> ➤ Individual office setup or relocation ➤ Changes to physical security
ELECTRICAL	<ul style="list-style-type: none"> ➤ Installation or testing of UPS systems ➤ Re-wiring or reconfiguring electrical subsystem ➤ Improvements to office power distribution
OPERATING PROCEDURES	

APPLICATION CONTROL	<ul style="list-style-type: none"> ➤ Monitoring and reporting application processing results ➤ Changes to processing schedule (i.e. JobTrac and Unicenter)
SYSTEM MONITORING, SUPPORT	<ul style="list-style-type: none"> ➤ Monitoring the status of system, network, and/or applications ➤ Troubleshooting system and/or network problems ➤ Performing system backups
SOFTWARE DISTRIBUTION	<ul style="list-style-type: none"> ➤ Application software migration / promotion ➤ Distributing application software

Ideally, these change categories should correspond quite closely to the problem classification scheme defined under the problem management process.

Reason for Change

Within the KIRMS Change Management Module there are a list of reasons for any change to take place. The table below describes and defines those reasons.

<i>Change Reasons</i>	
<i>Reason</i>	<i>Definition</i>
Break Fix	Repair broken component NOT causing outage
Customer Request	Customer requested this change
Maintenance	Preventative service to eliminate potential sources of service interruption
New Install	Add new component
Outage	Repair broken component causing an outage
Patch/Hot Fix	Software patch/firmware
Recovery	
Vendor Request	Vendor requested change

Impact and risk levels

To establish a common basis for comparing the relative exposure arising from a wide variety of changes, the change control process employs a standardized classification scheme that provides four discrete levels of impact and risk:

- **CRITICAL**
- **HIGH**
- **MEDIUM**
- **LOW**

Level assignment is central to the entire change control process: once a determination as to appropriate level has been made, implementation lead time, general management approval parameters, presentation requirements, and the like are basically established.

Impact and risk factors

If risk is defined as “the overall likelihood of encountering a failure during, or as a consequence of, a production change implementation,” what sorts of factors tend to increase the level of change risk?

While the specific elements are too numerous to list here—and inevitably vary depending upon the specific type of change under consideration—some useful generalizations can be made about factors that tend to contribute to overall risk. A partial list of these variables is offered in the table on the next page.

Risk Factors

<i>Factors Associated with Increased Change Risk</i>	
<i>PROJECT RISK</i>	
<ul style="list-style-type: none"> ➤ Large project team and/or large number of different organizations actively involved ➤ Inadequate breadth of participation ➤ Frequent turnover of key project team members ➤ Level of testing not commensurate with magnitude of change ➤ Delivery timeframe compressed significantly ➤ Insufficient user training ➤ Inadequate user and/or technical documentation ➤ Absence of communication with users 	
<i>TECHNICAL RISK</i>	
<ul style="list-style-type: none"> ➤ Use of new or unfamiliar technology ➤ Design complexity, with large number of components modified ➤ Complex, poorly-understood component relationships or dependencies ➤ Significant change to underlying application architectural foundation ➤ Outside influence, such as an unexpected software version change ➤ Human Error ➤ Shortage of key skill sets 	
<i>OPERATIONAL RISK</i>	
<ul style="list-style-type: none"> ➤ Number of other “unrelated” changes scheduled for implementation during the same window ➤ Extent to which change is exceptional (i.e., not routine or proven “repeatable”) ➤ Complexity of implementation script, including “tightness” of tasks, window, margin for error ➤ Insufficient post-implementation verification ➤ Absence of client communication ➤ Support complexity ➤ Insufficient system or network capacity to handle anticipated workload ➤ Inadequate understanding of performance and capacity implications ➤ Unclear support arrangements ➤ No disaster recovery provisions ➤ Poorly defined or documented operational procedures 	

If change impact refers to the “overall visibility of a change” or “the relative importance that a stakeholder attaches to the timely and successful implementation of a given change,” what factors are associated with an increasing level of change impact?

As was the case with risk, the specific elements are too numerous to list in detail, but generally, the level of perceived change impact is influenced by the factors listed in the table below.

Impact variables

Variables Associated with Increased Change Impact

- Perceived value of change or upgrade
- Source of change/upgrade request (e.g., Legislative mandate)
- Exposure to significant regulatory penalties or other liability (e.g., Federal requirement)
- Potential for interruption of service
- Introduction of new product or service
- "Real time" access (as opposed to batch)
- Sensitivity due to business cycle considerations (e.g., month end or year end related)
- Large number of users potentially affected by outage, service degradation, or functional deficiencies
- Downstream processing dependencies external to application
- Recent history of less than optimal service to customers
- Unable to implement change within customary change window
- Extended period of time required to complete back out
- Potentially expensive recovery required if results are inaccurate

Assessing impact and risk

A future release of this document will detail the specific criteria, relative weighting, and procedural mechanism for performing a more formal impact and risk assessment. In the meantime, the general indicators presented in the table on the next page, while imprecise, communicate the essence of the classification scheme and can serve as a guide to the assessment process.

<i>Impact Assessment Guidelines</i>		
<i>Impact / Risk Level</i>	<i>Key criteria</i>	<i>Representative examples</i>
<i>4: Critical</i>	Impacts all customers at all locations and is defined as a critical* service or is politically sensitive	Complete Loss of network or mainframe
<i>3: High</i>	Impacts multiple customers at multiple locations and/or impacts a critical service OR is being implemented during production hours OR could be politically sensitive	Swap-out of major Network component Implementation of new mainframe computer New Financial system New release of Top Secret
<i>2: Medium</i>	Impacts multiple customers at a single locations	Upgrade to major DofA application Swap-out of major UNIX server Hardware upgrade that requires more than maintenance window
<i>1: Low</i>	Impacts a single or small number of customers at a single locations and is not a critical service	Moderate programming changes Configuration changes to Hubs and Switches Implement new Ver/Rel of non-critical Operating System component Addition of new KANWIN customer Open Enrollment Process Year End W2 Process

*Critical Change; Defined as any change that has “massive impact” and is highly visible, impacts a significant number of users, a major agency, applications or service, and has no redundancy or alternate path.

NOTE: Agency SLAs may affect the impact level assigned to a change.

<i>Impact Assessment Guidelines</i>	
Risk Category	Considerations: (1 or more of the following)
5 (High)	<ul style="list-style-type: none"> • New technology • Unable to test • Back out up to or greater than two hours • Urgency = Criticality 1 (Immediately) • Impact = Critical
4	<ul style="list-style-type: none"> • Less familiar technology • Unable to test or limited testing • Back out less than two hours • Urgency = Criticality 1 (Immediately) • Impact = High
3 (Medium)	<ul style="list-style-type: none"> • Familiar technology • Tested • Back out up to or less than one hour • Urgency = Criticality 2 (2 - 5 Business Days) • Impact = Medium
2	<ul style="list-style-type: none"> • Familiar Technology • Tested • Back out is less than 30 minutes • Urgency = Criticality 2 (2 - 5 Business Days) • Impact = Medium
1 (Low)	<ul style="list-style-type: none"> • Familiar technology • Tested or does not require testing • Easily and quickly backed out • Urgency = Criticality 3 (General Maintenance) • Impact = Low

Initial assignment of the change level value is the responsibility of the individual requesting implementation of a given change.

The requester must exercise sound judgment in performing the change level assignment task, making certain that any unique circumstances are adequately considered. In view of the criticality of the assessment decision, a change requester should consult his or her manager, or even the change control process owner, if there is significant uncertainty regarding the appropriate value.

Lead time and change approval requirements

The outcome of the impact and risk assessment establishes two critical process requirements: Change lead time and change approvals.

Lead Time Requirements

Associated with each impact and risk level is a ***lead time*** requirement.

Most changes have a preferred implementation target date. Change requestors must allow adequate time to complete the work when establishing implementation target dates.

Lead time describes the ***number of days in advance of a planned implementation that the change requester must notify key stakeholder of their desire to implement a change.*** Change control lead times vary based on the assessment of change impact and risk.

Lead time provides a high-level indicator of the timeframe typically required to effectively plan and execute all appropriate project tasks preparatory to production implementation. When the applicable lead time requirement is not met, experience cautions us that the risks to successful implementation increase. (Risks tend to escalate under such circumstances because, for a variety of business reasons, a great deal of emphasis may be placed on meeting a date commitment, and there may be a real temptation to skip or cut short certain customary--but important--steps like testing, implementation planning, etc.)

Lead time is calculated relative to the planned change implementation date.

Change Approval Requirements

To help ensure appropriate change communication, coordination, and management review have occurred prior to change implementation, the change control process establishes formal change approval requirements.

These approval requirements vary based on change levels that are documented in the following matrix. Note that changes engendering higher levels of impact and risk require commensurately higher levels of management approvals.

Lead Time and Approval Requirements				
Impact / risk level	Lead time	Approvals required	Pre-requisite approvals	CMF Required
High	1 Week	Responsible Bureau's Deputy-Director	Project team	Y
MEDIUM	2 Days	Responsible Bureau's Deputy-Director	Project team	Y
LOW	4 Hours	Bureau Supervisors (or) Functional Lead in the responsible division	None	N

The lead time and approval requirements set forth above are considered minimums: A requester is free to plan additional lead time or request further reviews, all to assure that the installation meets targeted objectives.

There are some changes to the Production environment for which a formal change notification is not required. These are changes that fall under the category of "routine maintenance". The criteria for such changes are as follows. The change must be one that is performed on a routine basis as part of providing customer service. The risk factor must be considered very low and the process or procedure followed to implement the change is well defined, documented and followed. Individual Bureau supervisors are responsible for defining routine maintenance for their support team and must gain approval from their manager to forgo the official change process.

Routine changes not requiring a formal change notification are listed in Addendum 1 at the end of this document.

6. Roles and Responsibilities

To be effective, the change control process must enlist meaningful participation from a number of individuals, both within DISC and within the customer base.

The most significant process contributors are identified below, with accompanying text that describes respective roles and responsibilities. Clearly, in order to enjoy the benefits of a successful process, these personnel must fully support and actively participate in process activities, and must fulfill their respective process obligations.

A summary of roles and responsibilities is provided in matrix form at the end of this section.

Change Control Process Owner

The DISC Director serves as the overall change control process owner.

As process owner, the DISC Director:

- is responsible for the **process architecture** described in this document
- assures the architecture **integrates appropriately with other service delivery processes** (e.g., problem management)
- **interprets the process document** as well as all other enterprise-wide change-related policies
- presides over or delegates any subsequent efforts to **formally amend process** provisions
- maintains a **central repository of architecture-related documents**, providing access to all process participants
- **coordinates the efforts to certify process compliance**, and monitors the implementation of plans to achieve or restore compliance
- **approves standard change implementation windows; In cooperation with division directors, establishes change "freeze" periods**

Change Requester

The change requester is the individual seeking authorization to implement a specific change. Generally speaking, that is the technician or Programmer/ Analyst making the requested change.

The change requester is responsible for:

- **Initiating the change request**
- performing initial **change impact and risk assessment**
- **providing target dates** for processing the change

- **providing proper lead time** for processing the change consistent with proposed deadlines for the applicable impact and risk assessment category
- **sending the change request to the appropriate DISC deputy director(s)**. The change request must describe the change to a level of detail appropriate for a change of applicable impact and risk.
- **ensuring that the change has been thoroughly tested** based on established guidelines for such changes
- communicating any change in the original change date to application owning program directors and appropriate DISC deputy directors
- **assisting with schedule adjustment necessary because of implementation plan changes.**

Data Center Change Coordinator

The Data Center Change Coordinator role is assigned to the DISC Data Center Manager. The Data Center Change Coordinator is responsible for:

- **creating and maintaining a planning document of changes to the DISC support infrastructure**
- **coordinating activities of maintenance providers, DISC technical support and Bureau of Telecommunications relative to changes in the DISC support infrastructure**
- **chair a weekly coordination meeting of persons making changes to the DISC support infrastructure**
- **coordinating emergency change meetings**

Change Review Team

The Team is empowered to provide **formal implementation approval for changes within its scope of review**. In approving any change, the Team is essentially declaring that, in its collective judgment, the change request is in conformance with standards and there exists the necessary degree of confidence regarding prospects for success.

Of course, **the Team may withhold approval** for any change it believes does not conform to guidelines. In such cases, the Team should explain the basis for its decision so that the requester may address deficiencies and later re-request change approval.

The Team is responsible for resolving conflicts between change requests (e.g., two or more changes may ask to reserve the same dedicated resource for exclusive use during the same time period).

In the event the Team is unable to reach agreement regarding specific change approval, the decision is **escalated to the Director of DISC**.

The Team also sponsors and participates in **post-implementation review** activities associated with changes it has approved, and retains responsibility for following up on exceptions which arise during the implementation of, or as a result of, changes.

In addition, Team members **represent their respective bureaus** in the change process, and are **responsible for enforcing process adherence** within those organizations. Team members also actively **participate in any process amendment effort**.

The Change Review Team is comprised of:

DISC Deputy Directors

The DISC Deputy Directors are viewed as the “owners” of the business relationship between DISC and its customers, and provide the formal and direct interface to that audience.

In the context of change control, the DISC Deputy Directors are recognized as holding the customer/partner "proxy," and are responsible for approving changes on their behalf prior to any implementation action.

Summary of roles and responsibilities

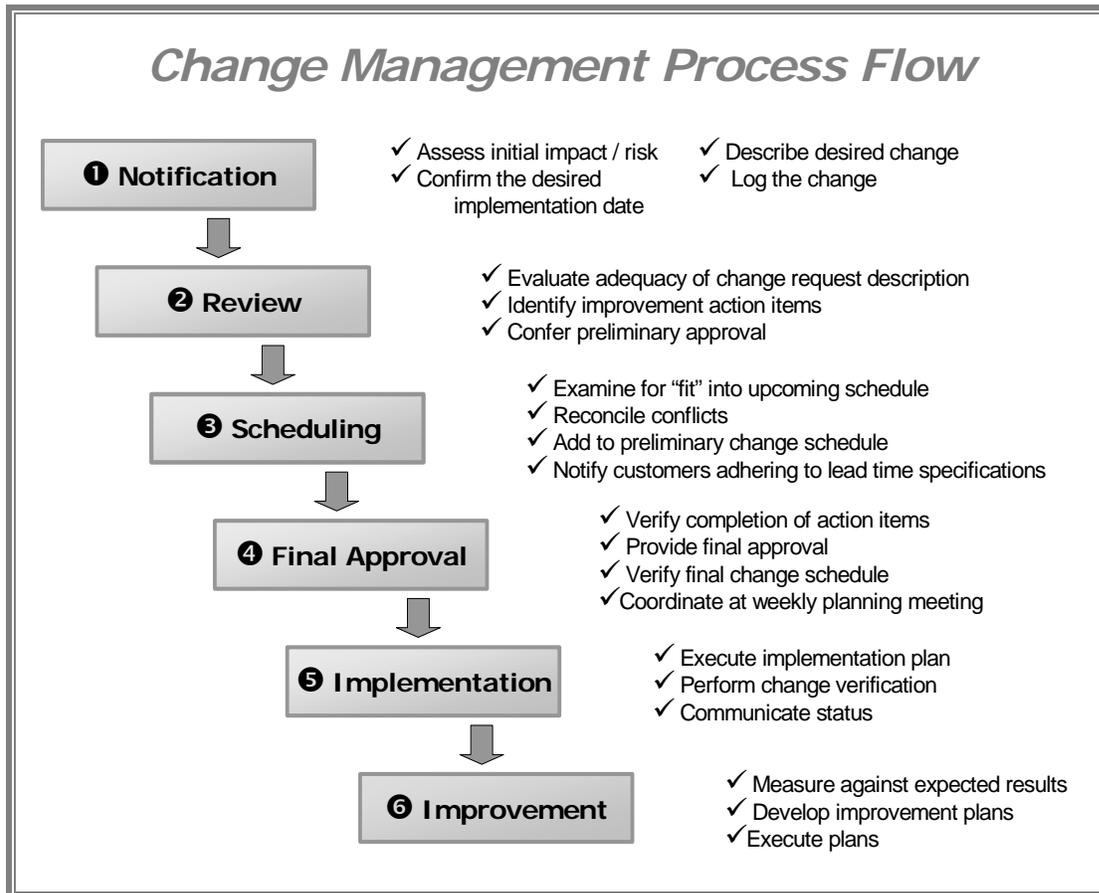
The matrix below recaps the roles and responsibilities of key participants in the change control process.

Summary of Roles and Responsibilities	
Role / Position	Responsibilities
<p>Process Owner</p> <p><i>DISC Director</i></p>	<ul style="list-style-type: none"> ➤ defining process architecture ➤ integrating the process with other service delivery processes ➤ interpreting the process document ➤ amending the process ➤ providing a central repository of architecture-related documents ➤ certifying process compliance ➤ approving standard change implementation windows; establishing change "freeze" periods
<p>Change Requester</p>	<ul style="list-style-type: none"> ➤ initiating the change request ➤ performing impact and risk assessment ➤ providing target dates

	<ul style="list-style-type: none"> ➤ recording the change in the DISC change log ➤ providing proper lead time ➤ communicating the change request to appropriate DISC deputy director. ➤ ensuring the change is thoroughly tested ➤ securing change approvals
<p>Change Review Team DISC Deputy Directors,</p>	<ul style="list-style-type: none"> ➤ managing change review process ➤ providing formal implementation approval, including approval of non-standard / exception changes, critical/high impact changes, high risk changes and other changes deemed necessary by approving supervisor ➤ performing post-implementation review and follow-up
<p>Data Center Change Coordinator Data Center Manager</p>	<ul style="list-style-type: none"> ➤ create and maintain planning document of changes ➤ coordinate activities of all persons making changes to data center ➤ chair weekly coordination meetings ➤ coordinate emergency change meetings

7. Process Flow

The figure below provides an overview of the basic six-phase path applicable to a "typical" change. Supporting detail is provided in text which follows.



Phase 1: Notification

In this phase, the change requester declares his or her intention to pursue implementation of a change. As examples, a technician may file a Change Management Action Form (CMA Form) or a customer may initiate a work request.

The CMA Form/work request provides basic information about the change, such as:

- description of the change
- impact and risk assessment results
- target implementation date
- Implementation Plan

Phase 2: Review

The first level of approval comes from the requestor's supervisor. Together, they will review the details relevant to the change and agree to move forward.

In the meeting with his/her supervisor, the change requester should be prepared to discuss pertinent information about the change, such as:

- ***reason / justification for change***
- ***technical / operational impact***
- ***test plans / results***
- ***communication plan, internal and external***
- ***documentation requirements, user and technical***
- ***implementation plan, including timeframes and verification plan***
- ***back-out and recovery plan***

Depending upon the results of the meeting, the change may receive *preliminary approval (conditioned upon completion of activities already planned)*, *tentative approval (pending completion of action items explicitly assigned by the supervisor, or denial of implementation authorization)*.

Changes denied preliminary approval either return to Phase 1 or are abandoned.

Phase 3: Scheduling

Changes that receive preliminary or tentative approval in Phase 2 are placed on the preliminary change schedule. All changes to the DISC data center must be posted on the change calendar, TSSYTIME. This is accomplished by completing the on-line CMA form. This process also routes the CMA form to the management and supervision team at DISC so everyone is aware of the impending change.

Notification of impending changes must also be sent to all potentially affected DISC customers. The length of time this notice must be sent out prior to the change must comply with the standards set forth earlier in this document.

Phase 4: Final approval

For all changes done outside the Sunday Maintenance window, final approval is granted by the Bureau Director. The Change Review Team's approval is assumed based on routing a CMA form describing the change and receiving no negative feedback.

All data center changes, be they hardware, or system software, planned for the Sunday maintenance window are discussed and coordinated at a weekly data center change coordination meeting. In cases where the change involves system software or data center hardware, the change requestor is required to attend this meeting.

If all special action items identified in the review step are complete, and there are no conflicting change requests, the Data Center Change Coordinator adjusts and finalizes the weekend schedule.

The final schedule of changes to occur in the weekend maintenance window is then presented to the Change Review Team who grant final approval.

Decision appeal

Where he or she believes special circumstances warrant reconsideration, a change requester may appeal an "unfavorable" approval decision by initiating management escalation, following the path defined in the following table.

Management escalation following the path defined below is also appropriate should the team attending the weekly coordination meeting find itself at an impasse when attempting to resolve scheduling conflicts.

<i>Change Approval Escalation Path</i>			
<i>Escalation initiator</i>	<i>Level 1 contact</i>	<i>Level 2 contact</i>	<i>Level 3 contact</i>
Change requester (Functional)	Division Directors	DofA Program Directors	Secretary of Administration
Change requester (Technical)	Deputy Directors	Change Review Team	DISC Director

Phase 5: Implementation

In accordance with the final change schedule, the change requester (or project team associate) executes all tasks required to implement the change, and performs post-implementation verification.

As a final step, the change requestor records the status of the implementation in the change log. Change status values are detailed in the table below.

<i>Change Implementation Status</i>	
<i>Status</i>	<i>Applies if:</i>
Successfully Completed	change was implemented according to plan and without incident
Partially Completed	Some, but not all, items on the change were implemented
Completed with problems	an unscheduled outage occurred or unplanned intervention/action was required
Failed	change was attempted, but was subsequently backed out
Aborted	change implementation was not attempted

Phase 6: Follow-up

Each Bureau Director is responsible to confirm that change status data is complete and accurate.

In the next Change Review Team meeting, unsuccessful changes ("implemented with problems" and "backed out") are examined to better understand the reasons for failure. Where procedural improvements are merited, the Team assigns action items and follow-up on progress until completed.

8. *Non-Standard Changes*

From time to time, exceptional circumstances inevitably arise that ***merit relaxation or waiver of selected process steps or requirements***, and the change process makes provisions for managing such exceptions to the standard process flow.

For example, it may be that a change must be implemented immediately to allow restoration of service after an outage has occurred. At some other time, a change that has been progressing normally through the process may need to be implemented sooner than originally anticipated due to external circumstances. It is also possible that the need for a business-critical change, perhaps regulatory in nature, does not become known until there is insufficient time to meet standard implementation lead times.

A change for which there is sufficient business justification to support bypassing certain process requirements falls into one of two general categories:

- ***emergency changes***
- ***exception changes***

Emergency changes

An emergency change is ***implemented on a priority basis to restore committed services, resolve a critical functionality or access problem, or avert an imminent threat to established service levels.***

Because emergency changes often must bypass customary lead time, communication and coordination, testing, and/or scheduling requirements, special procedural steps have been implemented so as to provide an appropriate level of management control.

During regular business hours, the Change Review Team should be alerted in advance to all but low risk change implementations and given the opportunity to examine remedial action.

- ***In an "after hours" situation, support personnel are empowered to take action deemed necessary within customary limits of authority.*** The DISC Deputy Directors should be contacted for assistance whenever support personnel are uncertain about the appropriate course of action.
- ***All emergency changes must be logged*** at the time the change is implemented. In addition, as part of the weekly meeting, the ***Change Review Team conducts a post-implementation review*** of the situation and action taken.

Exception changes

Exception changes tend to occur when unforeseen business circumstances demand an accelerated change implementation, or when a project that has fallen behind schedule encounters a hard and fast delivery deadline.

While exception changes rarely carry the degree of immediate urgency as emergency changes, they nevertheless involve bypassing standard process requirements.

Exception changes cannot be implemented without the explicit approval of the Change Review Team.

The change requester seeking exception approval is responsible for arranging an ad hoc review of the exception change with members of the Change Review Team. As part of this review, the change requester explains the business reasons believed to justify granting exception approval, and the Change Review Team either approves or denies the exception request.

9. Applications Development Standards and Procedures

Policy for SHARP and SMART System Change Management

Change management requirements must be applied whenever changes are made to SHARP or SMART software application and data.

1. All change requests will be entered as a Change Request or DC (Data Correction) in Phire. If a Change Request or Data Correction was initiated by a call to the Help Desk, a reference to the Help Desk ticket number will be included in the Phire Change Request or Data Correction ticket (and vice-versa)
2. All requests will be evaluated by the respective development team to determine if requested change is a required change, an enhancement or data change.
 - A. Required

It is inevitable that certain customizations be made to any packaged software. The following is a list of acceptable reasons for customizing.

 - Maintain compliance where required by law.
 - Maintain compliance with local, state and federal government agencies.
 - Maintenance of the translate table. PeopleSoft delivers numerous code tables and their interpretations in a collection called the translate table. It is assumed that customers will add, change and delete the delivered values as desired.

Packaged changes provided by the software company, for example, Tax Updates or HR Bundles, must have a CMA, Change Management Action, form turned into the DISC Change Review Team before migrating to the production environment.

Steering Committee

The Steering Committee is comprised of Directors, functional, and technical representatives from DofA and KHPA. There is a monthly meeting of this group. Changes that require Steering Committee approval are those significant requests that range in time from one to several months, are defined as CITO projects, or involve changes to the system during a period that is designated as a code freeze. Information will be presented as follows:

- Change Request general description
- List of vanilla objects affected and/or estimate from programming team
- Alternate solutions
- Priority workload

- Long term cost/benefit analysis
- Bring forward analysis

At the time of functional and technical representatives will have the opportunity to present their case. Time will be given for discussion and questions from the Steering Committee members to help with their decision.

Application Software Change Categories

Category	Description
Customizations	Modifications to the delivered application software. These modifications usually change the functioning of the PeopleSoft product
New Development	Creates completely new application objects that provide new or extended features rather than changes to the functioning of the PeopleSoft product. These objects may be attached to the delivered application as hook-on objects invoked from the PeopleSoft application menu.
Patches and Fixes Tax Updates	Include any PeopleSoft delivered or initiated changes other than major PeopleSoft upgrades. Patches and fixes include: <ul style="list-style-type: none"> • Consolidated patches widely delivered on a periodic basis. • Interim patches widely delivered as new errors are identified. • Short-term fixes delivered specifically as a temporary fix to a locally identified problem.
Major Application Upgrades	Moving to a new PeopleSoft Application release. This type of upgrade often involves a major change in functionality.

Policy for KIRMS System Change Management

The change control process outlined in this document must be followed whenever the KIRMS application is modified or customized.

1. Change requests for KIRMS will be submitted to the KIRMS Manager with the appropriate background documentation.
2. All change requests will be evaluated to determine if the requested change is a required change, an enhancement, or a data change with action taken accordingly as outline below:

A. Required Change

The following list describes common situations where modifications could be required:

- If required by law
- If required by a local, state, or federal government agency.
- Packaged changes provided by Compco including updates

Action: Required changes do not require approval by the KIRMS Managers Group. However, these changes will be communicated to the Managers and they will generally participate in scheduling required changes. Approval is required by the Application Development Supervisor. These changes also require the completion of a KIRMS Request and Migration Form.

B. Enhancement

Enhancements are defined as the addition or modification of custom functionality or modifying delivered functionality to operate in a manner technically or functionally different from the delivered application or software. These changes also require the completion of a KIRMS Request and Migration Form

Requests which are enhancements will be evaluated to determine:

- If the modification is likely to require DISC programmer maintenance each time the vendor software is upgraded
- The business benefits of the change, particularly in reference to our external customers
- How the enhancement would impact each of the following areas within DISC: BAS, NOC, I/S, P&E and BDAS

All enhancements will be reviewed by the KIRMS Manager and the KIRMS Managers Group

C. Data Changes

Data changes are requested by users to change or fix data that is incorrect in the KIRMS database. These requests should be communicated to the KIRMS Manager with sufficient documentation to

ensure that the correct record is updated. The KIRMS Manager will submit a Production Data Change form to the Applications Development Supervisor after making specific types of data changes as noted below.

- Monthly teletch updates
- Monthly switch id updates for the call conversion
- Monthly billing cycle scripts which create invoice numbers and delete taxes
- Data load projects
- Mass deletes – a Production Data Change Form is required for this type of change
- External user call to the Help Desk to report that they cannot view a work order they entered. This type of change requires a Production Data Change form.

KIRMS Managers Group

The KIRMS Managers Group is comprised of at least one member from each of the following areas within DISC – BAS, NOC, I/S, P&E, along with the BDAS Application Development Supervisor and the KIRMS Manager. The KIRMS Managers Group will be consulted for enhancements to the KIRMS applications / screens, as described above in section B.

The KIRMS Managers Group will consider the interests of both DISC and our external customers when evaluating the impact of modifications to KIRMS, and providing recommendations. The KIRMS Manager will advise the KIRMS Managers Group of the on-going maintenance likely to be required by modifications.

Change Implementation

System protection from unauthorized changes will be accomplished by coordinating with BIS personnel so they can open temporary access to implement authorized changes. Data loads are completed by a member of the KIRMS Development Team, preferably the KIRMS Manager, after coordinating with the BIS Support Staff.

The KIRMS Development Team will communicate the availability of the implemented changes by email to the relevant staff when the changes have been implemented in Production.

10. Reporting

Preparation, distribution, and review of a monthly change control report is necessary for management control and process improvement efforts.

The reporting package will communicate the level of change **activity** during the period and, even more importantly, paint a broad picture of overall process **performance** (effectiveness).

Change reports are prepared by the change coordinators, or designees and distributed to a broad audience within DISC.

MONTHLY CHANGE CONTROL REPORT

Nov 2010

Application Software

User oriented applications

Or Operational Support Utilities

STARS Program DAAPxxx upgraded
SHARP module xxxxxxxx upgraded
Budget

Database Changes

None

System Changes

▪ Hardware

New Tape drives installed
Cables laid and installed for ESS
Upgrade to Solaris 2.6
Upgrade to CA Spool

▪ Software

Network Changes

▪ Hardware

installed new 3270 router

▪ Software

Installed new FTP software

Security Changes

changes to firewall access

Facility Changes

▪ Office

none

Installed new lock on computer lab

▪ Electrical

Tested the motor generators

Operating Procedures

▪ Application Control

Changes to CA-Unicenter

▪ System Monitoring

Installed new network monitor

11. Addendum 1

Routine Changes Not Requiring a Formal Change Notification

BDAS

1. Daily EIS builds and KIRMS migrations
2. Routine Data Warehouse migrations
3. Daily SHARP and SMART change migrations

BIS

1. User/Group Administration
2. Clean up disk (old files, remove unused applications)
3. File copies
4. Service restarts that have no user impact
5. Creating LUNs
6. Add remove tapes from tape pools
7. Build up of new servers
8. Creation of new web sites
9. ACL's in test firewalls
10. Creation of new cluster services
11. DB refresh in test or development
12. Daily migrations for websites
13. Add/removing backup clients
14. File reorgs
15. Electrical or mechanical work in the Data Centers performed by non-DISC personnel
16. Creation of new files, datasets.
17. Security Access – Additions, modifications, deletions.
18. System Outage
19. New Applications Support
20. Telecommunications support
21. Removing unwanted processes (tasks) from system
22. Starting NFS, mounting NFS file systems
23. Preparing and running maintenance scripts, eg. vmstat, iostat log, query system stats, explorer scripts
24. Check patch levels
25. Check application levels
26. Adding printers
27. Cycle software that has no impact/users /etc/hosts corrections, additions, deletions (defines what other systems the servers will talk to)

28. Adding inetd services for application staff

BOCS

1. Server reboots that do not impact users
2. Cluster node changes that do not impact users
3. Day to day firewall access administration
4. Day to day AD routine user administration
5. Day to day routine Exchange administration
6. Creating new virtual servers
7. Migrating servers in Vmware as long as they are within the same datacenter
8. Installing Vmtools on a virtual server

BOT

1. Update of snmp-server commands in routers and switches
2. Update of interface descriptions in routers and switches
3. Update of netflow and IP accounting commands
4. Add/Remove TACACS+
5. Configuring new, unused interfaces in routers and switches
6. A variety of minor commands associated with our configuration standards that have no user impact (e.g. "no service pad" or "service nagle")
7. Configure/modify user access ports for existing VLANS
8. Removal of unused interfaces
9. Update of VLAN names
10. Adding existing VLANS to the svcl groups in the distribution routers for use with load balancers and firewall modules
11. Creating new contexts, interfaces and associated routes nats and rules
12. ACL changes requested by users.
13. Route changes effecting specific hosts/subnet per user request.
14. Failover, when environment is stable
15. Reload of 'standby' firewalls
16. Add/Remove WLAN Access Points

ES

1. Update of IP signatures