Security and Workflow Strategy

Definition and Overview

The intent of this document is to outline a strategy for the security and workflow configuration efforts necessary to successfully complete the Kuali Finance System (KFS) implementation project. This work includes interaction with functional staff to understand needs for data use, workflows, and access management. Work with technical staff will be needed as well to gain understanding of the security and workflow configuration tools and underlying data structures.

These efforts will be led by the Security/Workflow Lead whose responsibility it will be to understand all aspects of the configuration tools being used for the KFS implementation and to help guide the process of building and implementing manageable security system and associated practices.

This strategy will help to ensure alignment of the project team’s efforts with:

1. The core mission of the University
2. The appropriate units in CIT's Information Systems (IS) division, which will sustain the KFS application once the project is completed

Goals

Security Goals:

- Create and implement a set of processes and standards for managing security within the KFS application
- Ensure that access to data is appropriate for each individual given access
- Ensure that security practices meet audit requirements and are aligned with CIT IT Security Office policies
- Create self-service processes for requesting, approving and granting access to KFS
- Create documentation and procedures for on-going security maintenance in KFS
- Transition ownership of management processes to the IS Configuration Management group after the project is complete
- Work with the CIT IS Enterprise Integration Group (EIG) and Kuali Coeus implementation project teams to ensure that established security management practices and standards are complementary to their efforts and also efforts of other locally built applications that leverage Cynergy

Workflow Goals:

- Create and implement a set of processes and standards for managing workflow configuration changes for the KFS application
- Ensure that workflow configuration practices meet audit requirements and are aligned with CIT IT Security Office policies
- Create documentation and procedures for on-going maintenance of KFS workflow configuration
- Collaborate with CIT IS EIG to design and develop workflow configurations for KFS
- Transition ownership of configuration management processes to the IS Configuration Management group after the project is complete
- Work with CIT IS EIG and the Kuali Coeus implementation project teams to ensure that established workflow management practices and standards are complementary to their efforts and also efforts of other locally built applications that leverage Cynergy

Tools and Deliverables

Tools

There are two tools used to configure security and workflow in KFS - 1. KIM (Kuali Identity Management) for security and workflow responsibilities, 2. KEW (Kuali Enterprise Workflow) for business process workflows. KFS communicates with KIM to determine each user's permissions (access to documents) and workflow responsibilities. In KIM, each user is identified on the KIM Person document. This document identifies the person by a Principal ID and assigns that person to any number of roles. Some roles will be assigned to users while others will be derived or assigned as a result of a data scenario within KFS. For example, Fiscal Officer is a derived role based on an account attribute within KFS.

KIM handles user identification but our intent is that identity data will not be stored in KFS or in KIM, it will be accessed from institutional source identity stores such as PeopleSoft and the Cornell Directory. There may be cases where a data element is required by KFS but not stored in other campus identity data sources. In these cases it will need to be determined where the needed data should be stored, within KFS or in KIM. Integration work needed to tie these systems together to present a single user object in KFS will be done within KIM and developed by the CIT IS Enterprise Integration Group.

KIM also includes group management capabilities. Cornell's current group management tool is the permit server. Other tools including Active Directory and Grouper are being considered for future group management needs at Cornell. Conversations with Identity Management have resulted in an agreement that the KFS implementation will move forward using KIM for group management for the time being while the future group management system is still being determined.
KIM also provides access management capabilities (e.g. Roles, Permissions, etc). KFS will use these features since there are currently no central systems that provide this functionality. KEW will be used to manage all aspects of workflow configuration for KFS.

Deliverables

The Security/Workflow Lead will be working with each of the Module Leads to identify the needed roles. We will determine if delivered roles will be sufficient and identify when custom roles will need to be built. Security/Workflow will build custom roles and configure delivered workflow rules. Modifications to workflow rules will be handled by CIT IS EIG. The deliverable will be a set of roles including all needed permissions and responsibilities for each module as well as a set of workflow configurations.

The Security/Workflow Lead will work with Functional Leads to create an overall Security implementation strategy. We will identify those documents that contain sensitive data and determine how to appropriately limit access. While true row level security is not being considered for KFS at this time, there will be times when a person should only view documents relevant to them. The Security/Workflow Lead will need to understand options and will need to facilitate discussions such as this one.

Create documentation and procedures for on-going Security Maintenance. The Security/Workflow Lead will be creating documentation to be used by whoever will be maintaining security on a day to day basis after implementation. The Lead will work with Functional Staff who will be making decisions about permissions, responsibilities, and role assignments to help them understand how the decisions they make impact the end users.

There will be work to determine which identity fields will be accessed by KIM. The Security/Workflow Lead will work with the other Technical Teams to identify these fields and determine their source. It is important to consider KIM as a potential identity management tool for any number of applications, not just the KFS implementation.

The Security/Workflow Lead will work with the Data Delivery Group to identify reporting roles and distribution mechanism for those roles. KIM will likely be used to assign reporting roles. There is also some analysis to be done to determine the cost of implementing row level security within the data mart. While the initial estimates are to implement with no row level security, there have been requests to estimate cost and feasibility.

Assumptions and Risks

- The base KFS application does not provide sufficient levels of granularity for restricting access through KIM configuration thus requiring KFS modifications
- KEW can be configured to handle all business processes that exist at Cornell University
  KIM can appropriately namespace KFS specific configuration so that it does not impact configurations of Kuali Coeus and other locally built applications that leverage it

Roles and Responsibilities

Security/Workflow Lead:

- Learn and understand KIM and how it will be used in our implementation of KFS
- Learn and understand KEW workflow configurations and how they will be used in our implementation of KFS
- Work with CIT IS EIG to ensure sustainable KIM/KEW configuration patterns are used for KFS that also complement and do not hinder usage of these components by other applications leveraging Cynergy
  - Work with the ID&R team to identify reporting roles and distribution/role assignment mechanism that leverages workflow maintenance
  - Work with functional staff to plan for manageable security/workflow implementation
  - Create processes for identifying access (permissions) and workflow (responsibilities) requirements
  - Work with functional areas and distributed groups to create role specification docs (includes both security access and workflow responsibilities)
  - Create documentation and procedures for on-going security maintenance in KFS
  - Ensure sound audit practices are established for security practice and procedures
  - Work with Data Stewards where necessary to ensure approved data distribution
  - Work with the process analysis module leads to compile the KIM data as defined in the process analysis work (access to system & e-docs, roles, permissions, groups as they relate to the individual KFS modules)
  - Work with tech staff to get the initial KIM dataset loaded
  - Work with the QA lead to fully test KIM functionality

CIT IS EIG:

- Provide ownership support of the Cynergy product which will be used by the Security/Workflow Lead
- Help to train the Security/Workflow Lead on the tools as necessary
- Coordinate with CIT IS Integrated Services, who will support the Cynergy platform and accompanying KFS environments
- Provide guidance and advice on the design and development of processes and standards around security and workflow configurations
- Design and develop any modifications within Cynergy that are necessary for supporting workflow and security configurations, including integrations with other source systems (e.g. KIM and identity information)
- Follow established configuration management procedures