Template for SUM: e-Framework editorial work

Manage Subscription Workflows

The library wishes to inform the decision-making processes underlying the subscription and platform lifecycle relating to journals and to e-resources more broadly. In order to do this the library team gathers and shares intelligence and evaluation data at key stages.

The University of Huddersfield has analysed a number of workflows and defined a series of checklists. These checklists define the data that is required for a given workflow (or Task within a workflow). Checklists can be reused across workflows, so whilst a checklist may have been conceived as part of a task on one workflow, the checklist (or some elements of it), may be of use in other workflows.

Collection of data for workflows is problematic, and is repeated by many institutions across the sector. It is proposed that an above campus service (a knowledge base) be set up to store this checklist data. Further the data held by this service would be shared to all other institutions, leading to a massive de-duplication of effort and large saving in resources.

An additional benefit is that if this data is represented in a machine readable format, it will be possible for institutional workflow engines to be able to process it.

Problem description

Many of the tasks that Libraries are called upon to perform are essentially workflow based. These workflows pertain to most (perhaps all) of the activities that the library undertakes. For example, if a journal subscription is to be cancelled, there will be a workflow, consisting of tasks which will need to be undertaken.

Difficulties arise when the workflow (or task) requires "data" for some reason (the exact semantics of the "data" are irrelevant at this time; data required for a task in a workflow varies depending upon the task). Collection of the data can be difficult – typically it will need to be assembled from diverse sources, including the previous experience of the library staff, and is often unreliable. Furthermore the data required is often not readily available from the expected parties in the supply chain (e.g. publishers).

Across the sector, there is anecdotal evidence that institutions are repeating this work; collecting similar and identical data for similar tasks in similar workflows. This is resource intensive across the sector, and is a wasteful duplication of effort.

Goal

Template for SUM: e-Framework editorial work

It is proposed that an above campus service be created which will allow libraries to share the data pertaining to checklists. Each institution can define the checklists that apply to their tasks and workflows. The checklist itself would be a lightweight data object, consisting of a number of "questions". An instance of a checklist (with "answers") would then be linked to a specific key entity.

For example, an institution could define a checklist to address the selection of a new e-journal. Questions on the checklist could include "is a trial available?", "what is the cancellation policy?" and/or "is the e-journal peer reviewed?" Once the checklist is defined, when the institution then has to select a new e-journal, the answers to the questions on the checklist are recorded against the particular candidate e-journals.

As institutions complete the data for a given checklist, that data can then be posted to an above campus shared service. This service makes the checklist data available to users, saving a vast amount of time. This would reduce the duplication of effort across the sector as a whole, for which the resource savings alone are considerable.

Additionally, it can be postulated that publishers and agents will benefit from not needing to answer the same question for several different institutions, leading to reductions in support costs.

Use case (Business Process Modelling)

Actors:
The actors include everyone that is involved in the data collection process, either by seeking out the data which answers a question, or by providing the data required to answer a question.
Library staff:
  * Responsible for e-journal subscription management.
  * Required to collect checklist data and perform tasks as determined by the workflow.
  * Liaise with faculty members and external suppliers.
  * Required to make workflow decisions.
Faculty Members:
  * Making requests on the library – typically initiators of workflows relating to e-journal subscriptions.
  * May be required to provide further information to the library as determined by the library workflow.
Publishers & Agents:
  * Make resources available to the library via a legal and/or commercial agreement.

Template for SUM: e-Framework editorial work

- Provide information of a legal and/or commercial nature to the library staff.

Shared Service Support Team
- Provide verification for critical data such as license terms (e.g. Use in VLE).

Business Objects:
Authorisation / Authentication Data – this is the data that is used at an above campus level to determine which institutions have access to which other institutions' checklist data. Additionally, this data allows individuals to use the shared service (either to read or contribute).

Checklist – this is a set of questions that are required to be an answered to complete a task in a workflow. Checklists can be reused between tasks in different workflows. Note that in the strictest sense, a checklist will contain simple instructions (e.g. "send data to librarian: [ ]"). For the purposes of the shared service, checklists should only consist of intelligence gathering instructions (collecting data for the purposes of retention or sharing with others). Thus, "list cancellation policy" would be the sort of data to include in a checklist business object; "send copy to vice chancellor" would not be.

Checklist Data – this is the answers to the questions posed by a particular checklist, as applied to a specific key entity. For example, the checklist for evaluating a new e-journal might include "is a trial available?" and "is the journal peer reviewed?" The checklist data for "the journal of Genocide Studies" might be "is a trial available: no" and "is the journal peer reviewed: yes". Naturally checklists for other tasks and relating or relating to other key entities will have different questions, and thus generate different checklist data.

Key Entity – this is a key entity to which checklist data is appropriate. Examples include titles, packages, publishers, platforms and licenses). The shared service does not need extensive data for a key entity; it merely needs a "link entity" to target checklist data at.

Processes:

Create Checklist
On a per task basis:
- Library Staff analyse an existing workflow or task, and determine the basis of checklist from it.
- Simple Instructions are removed from the checklist, but retained as steps in a local workflow.
- Intelligence Gathering Instructions are retained in the checklist.
- The type of key entity(ies) that subsequent checklist data will link to is noted.

Template for SUM: e-Framework editorial work

- Identify the specific questions (intelligence gathering instructions) which may have their data shared.
- Identify the specific questions (intelligence gathering instructions) which are "Critical Data" and require independent verification if shared.
- The completed checklist is uploaded to the central service.

Edit / Delete Checklist
Checklists may change over time. This process allows checklists to be edited or deleted.
- Edit the content of a given checklist; and/or
- Delete the content of a given checklist.

Provide Checklist Data
On a per checklist, per Key Entity basis:
- Select the required checklist.
- Select the required Key Entity.
- Undertake the relevant data capture and verification required to complete the intelligence gathering instructions on a checklist.
- Upload the checklist to the central service.

Edit / Delete Checklist Data
Checklist Data will change over time. This process allows checklist data to be edited or deleted.
- Edit given checklist data; and/or
- Delete checklist data.

Share checklist data
It is assumed that data will be shared as determined by the creation process of the checklist itself. However, institutions may wish to share more or less data; or restrict with whom the data is shared.
- Identify the final set of checklist data fields for sharing.
- Identify the final set of users/ institutions to share with.
- Set the authorisation object on the central service to reflect the determined sharing model.

Read central service data
- Library staff use the checklists and checklist data prepared by themselves and others.
- (Machine Agents use the machine readable checklists and checklist data available from the service; this includes but is not limited to local workflow engines).

Functionality

Create Checklist (Add)

Template for SUM: e-Framework editorial work

The staff need to undertake the work required to produce an intelligence gathering checklist.
An add request needs to be made to the central service. The request contains:
- The checklist business object, as defined in the BPM section.
- An identifier for the checklist.
- An identifier for the type of key entity that the checklist relates to.
- The authentication details of the institution.

Behaviour:
1. The request is validated to ensure that it comes from an actual institution.
2. If the checklist already exists, it is rejected.
3. The checklist business object is added to the data store.

Edit / Delete Checklist (Update, Delete)
An update or delete request needs to be made to the central service. The request contains:
- The checklist business object, as defined in the BPM section.
- The authentication details of the institution.

Behaviour:
1. The request is validated to ensure that it comes from an actual institution.
2. If the checklist already exists, then the stored checklist is either (as appropriate):
    a. Replaced with the new checklist; or
    b. Deleted from the data store
3. Otherwise, the request is rejected.

Provide Checklist Data (Add)
The staff need to undertake the work required to complete a checklist for a specific key entity. By default, data is not shared.
An add request needs to be made to the central service. The request contains:
- The checklist data business object, as defined in the BPM section.
- The authentication details of the institution.
- The key entity that the data is to link to.

Behaviour:
1. The request is validated to ensure that it comes from an actual institution.
2. The key entity is validated to ensure that it exists.
3. If the checklist data already exists, for that institution and key entity, it is rejected.
4. The checklist data business object is added to the data store.

Edit / Delete Checklist Data (Update / Delete)

The staff need to undertake the work required to complete a checklist for a specific key entity

An update or delete request needs to be made to the central service. The request contains:
- The checklist data business object, as defined in the BPM section.
- The authentication details of the institution.

Behaviour:
1. The request is validated to ensure that it comes from an actual institution.
2. If the checklist data already exists, then the stored checklist data is either (as appropriate):
   a. Replaced with the new checklist data; or
   b. Deleted from the data store
3. Otherwise, the request is rejected.

Share Checklist Data (Authorise)
An authorise request is made to the central service. The service responds by updating internal data stores to make the specified data available to the specified user(s).
The authorise request contains:
- The authentication details of the institution.
- Identifiers for the checklist(s) to be shared.
- Identifiers for the checklist datum(a) to be shared.
- Identifiers for the target user(s) to share with.

Behaviour:
1. The request is validated to ensure that it comes from an actual institution.
2. The authorisation data is updated to permit the specified users access to the data as specified in the request.

Read Checklist Data (Search, Read)
A search request is made to the central service. The service responds by returning the checklist data that is pertinent to the specified key entity and checklist.
The search request contains:
- The authentication details of the institution.
- The identifier of the checklist and/or key entity to search against (the query).

Behaviour:
1. The request is validated to ensure that it comes from an actual institution.
2. The search for the checklist data is undertaking, subject to the authorisation of the requester (i.e. only shared or owned data can be searched).

3. The search results are returned to the requester.

Service arrangement

Add (Checklist)

Description: this function needs to validate that a request to create a new checklist has come from a real institution. If so, and if a checklist with this identifier, for this type of key entity does not exist, it is created on the system.

Orchestration:

- Call Authenticate
- Call Add

Service Name: Authenticate

Actions:

- The central data service needs to satisfy itself that the request received has come from a bona fide institution. The model is silent on how this is achieved. It is suggested that institutions are given simple usernames and passwords in a user accounts database.
- If the request fails authentication, the request should be rejected.

Service Name: Add

Target Data Source: Checklist Database

Target Business Object: Checklist

Actions:

- If the checklist already exists in the checklist database, then this request should be rejected.
- Put the checklist into the checklist database; do not modify the values of the checklist.

Update / Delete (Checklist)

Description: this function needs to validate that a request to update or delete a checklist has come from a real institution. If so, and if the checklist exists on the system, it is updated or deleted as appropriate. If the request is valid but the checklist does not exist, then the request is rejected.

Orchestration:

- Call Authenticate
- Call Update; or
- Call Delete

Service Name: Authenticate

Actions:

- The central data service needs to satisfy itself that the request received has come from a bona fide institution. The model is silent on how this is achieved. It is suggested that institutions

       are given simple usernames and passwords in a user accounts database.
* If the request fails authentication, the request should be rejected.

Service Name: Update
Target Data Source: Checklist Database
Target Business Object: Checklist
Actions:
* If this checklist does not exist in the checklist database, then this request should be rejected; otherwise
* Modify the values of the stored checklist.

Service Name: Delete
Target Data Source: Checklist Database
Target Business Object: Checklist
Actions:
* If this checklist does not exist in the checklist database, then this request should be rejected; otherwise
* Delete the stored checklist.

Add (Checklist Data)
Description: this function needs to validate that a request to create new checklist data has come from a real institution. If so, and if checklist data with this identifier, for this key entity does not exist, it is created on the system.
Orchestration:
* Call Authenticate
* Call Add
Service Name: Authenticate
Actions:
* The central data service needs to satisfy itself that the request received has come from a bona fide institution. The model is silent on how this is achieved. It is suggested that institutions are given simple usernames and passwords in a user accounts database.
* If the request fails authentication, the request should be rejected.

Service Name: Add
Target Data Source: Checklist Data Database
Target Business Object: Checklist Data
Actions:
* If the checklist data already exists in the checklist data database, for this key entity, then this request should be rejected.

- Put the checklist into data the checklist data database; do not modify the values of the checklist.

Update / Delete (Checklist Data)
Description: this function needs to validate that a request to update or delete checklist data has come from a real institution. If so, and if the checklist data exists on the system, it is updated or deleted as appropriate. If the request is valid but the checklist data does not exist, then the request is rejected.
Orchestration:
- Call Authenticate
- Call Update; or
- Call Delete
Service Name: Authenticate
Actions:
- The central data service needs to satisfy itself that the request received has come from a bona fide institution. The model is silent on how this is achieved. It is suggested that institutions are given simple usernames and passwords in a user accounts database.
- If the request fails authentication, the request should be rejected.

Service Name: Update
Target Data Source: Checklist Data Database
Target Business Object: Checklist Data
Actions:
- If this checklist data does not exist in the checklist data database, then this request should be rejected; otherwise
- Modify the values of the stored checklist data.

Service Name: Delete
Target Data Source: Checklist Data Database
Target Business Object: Checklist Data
Actions:
- If this checklist data does not exist in the checklist data database, then this request should be rejected; otherwise
- Delete the stored checklist data.

Authorise
Description: this function maintains the sharing permissions for checklist data, By default, checklist data is not shared, unless the owner of the data explicitly gives permission. Even then, only the fields in the checklist that are marked as being sharable are shared. Critical Data fields are only shared once verification has been received.
Orchestration:

Template for SUM: e-Framework editorial work

- Call Authenticate
- Call Authorise
- Call Validate

Service Name: Authenticate
Actions:
- The central data service needs to satisfy itself that the request received has come from a bona fide institution. The model is silent on how this is achieved. It is suggested that institutions are given simple usernames and passwords in a user accounts database.

If the request fails authentication, the request should be rejected

Service Name: Authorise
Target Data Source: Authorisation Database
Target Business Object: Authorisation Data
Actions:
- Create records as appropriate in the authorisation database to reflect the sharing policy of the checklist data as specified. Critical Data is not made available immediately; rather the validation service is triggered.

Service Name: Validate
Target External System: Alerting (email / SMS/ IM)
Target Data Source: Authorisation Database
Target Business Object: Authorisation Data
Actions:
- Alert the shared service support team (via the external alerting system) that a critical data field is requested to be shared.
- Validation service (accessed by shared service support team) updates the authorisation database to allow access to the critical data.

Search
Description: this function needs to validate that a request to use shared or owned checklist data has come from a real institution. If so, the relevant data matching the query is returned.
Orchestration:
- Call Authentication
- Call Search

Service Name: Authenticate
Actions:
- The central data service needs to satisfy itself that the request received has come from a bona fide institution. The model is silent on how this is achieved. It is suggested that institutions

are given simple usernames and passwords in a user accounts database.
- If the request fails authentication, the request should be rejected.

Service Name: Search
Target Data Source: Checklist Data Database
Target Business Object: Checklist Data
Actions:
- The system locates the data that the requester has access to.
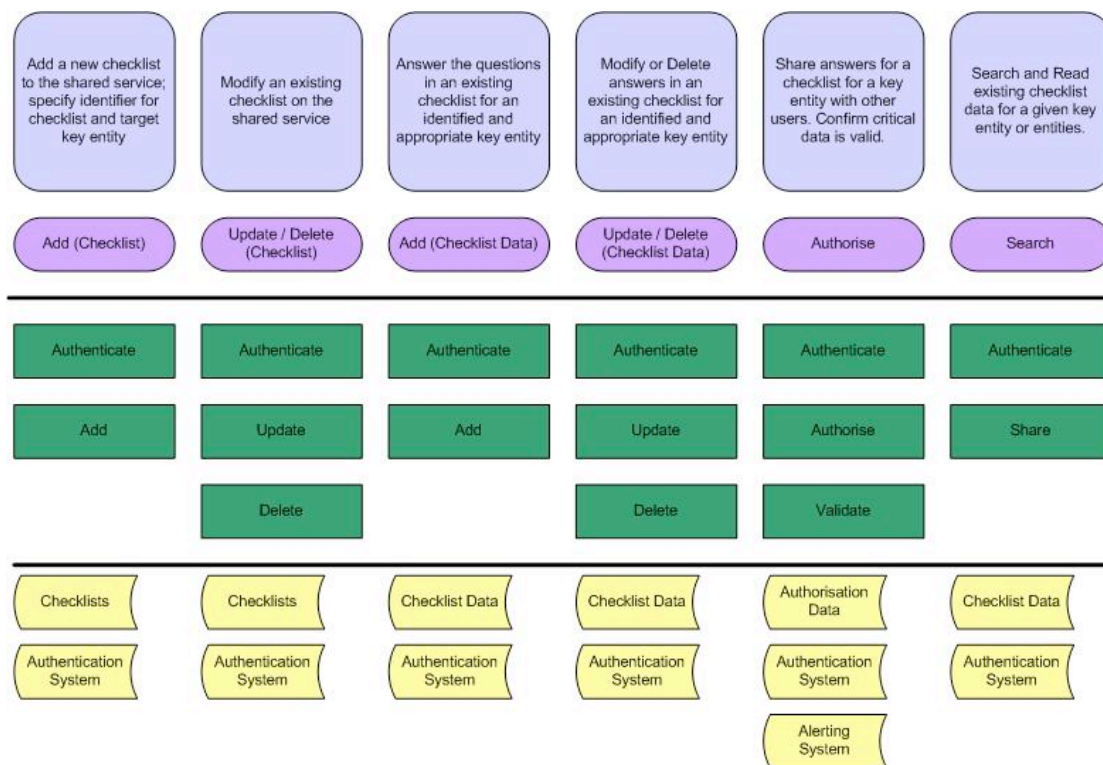- The system returns the checklist data business object that matches the terms specified in the query, subject to sharing permissions.

SUM diagram

Figure 1: Manage Subscription Workflows SUM