**\*. When you redo the workflows, use explicit inter-workflow connectors to join**

**a unique workflow to its shared workflows - much as people do in circuit diagrams**

We're unsure of what exactly you mean by shared workflows. Do you mean alternate flows such as errors? ***Yes. In some cases, the failure options should be common to multiple workflows***.

Also, you mention “common workflow for \_\_\_” multiple times. What do you mean by common workflow? Do you want one massive file that has a million flowcharts on it and possibly even connected? I’d like to see diagrams that communicate. In this regard, avoiding repetition is a best practice.  ***In electrical diagrams, it’s common to make diagrams easier to grasp by***

* ***breaking an involved pathway in, say, the middle;***
* ***ending that pathway with a connector symbol that’s labeled with the name of a “connecting to” symbol that signifies “continued elsewhere” – e.g.,* ⇨**
* ***beginning the pathway’s continuation with a labeled “connecting from” symbol that begins a second pathway – e.g.,* ⇨**

**\*. Also, when the issues raised below are addressed, should we update the requirements**

**document to capture the answers?**

**Now, for the workflows:**

**\*. Generally**

**\*. needed - a common workflow for server anomalies**

***In all of what follows, while the exact reason for an anomaly might not be diagnosable in real-time, the syndrome should be noted, logged, and an action taken – even if it’s “just” a careful error message with a recommended action for a user to take. What that action is, I think, is should be decided on as part of workflow development.***

**-. What should be done/noted if the server is inaccessible?**

**-. possibilities:**

**bad command, command failure**

Can you provide some clarity on what exactly you mean by these?

***Think Warner Vogels, “Everything fails all the time”. Examples:***

* ***The server can’t be contacted for any number of reasons. Examples:***
  + ***the network has partitioned***
  + ***the network dropped the message***
  + ***the host platform has gone off line***
  + ***the CPH-IVT service isn’t operational***
* ***The server rejects the request for any number of reasons. Examples:***
  + ***the request is ill-formed, due to an error in the client’s code***
  + ***a well-formed request is garbled in transmission, due to a network error***
  + ***a well-formed request is rejected, due to an error in the server’s code***
* ***The service cannot complete the request for any number of reasons. Examples:***
  + ***the system is hosted in the cloud and the service has exceeded its allotted budget***
  + ***the database service isn’t operational***
  + ***a well-formed request is rejected, due to an error in the database’s code***
  + ***the database has become corrupted***

**space issues**

We’re assuming the database and application both will be on an ETSU server and that ITS is already monitoring the storage on its servers. If this is the case, perhaps we can communicate with ITS to provide an alert to the CPH admins at a certain storage percent.

***Most likely, this application will be deployed and maintained by CPH personnel rather than by ITS. ITS is stretched thin as it is, thanks to Banner. So, I would expect the system to be deployed***

* ***initially, on a Dept. of Computing server***
* ***then, in the Dept. of Computing AWS cloud***
* ***then, in the CPH cloud – if CPH has a presence in it***
* ***finally, in the AWS cloud***

***I think it will be up to Dara and perhaps a CPH RA to monitor resource usage***

**-. how to recover in midst of a multi-step process?**

We identified these multi-step processes in the CPH-IVT application: Registration, Chart generation, CHR data fetch and upload. In all of these, we believe it is appropriate to completely restart the process.

***I do as well, so long as actions that need to be atomic are handled as transactions***

**-. more careful separate workflow?**

What exactly do you mean by more careful?

***As noted above. Consider what could go wrong in the process and account for responses in the workflow***

**\*. needed - a more precise common workflow for server anomalies**

**-. What should be done/noted if the database is inaccessible?**

**-. possibilities: service inaccessible, bad command, command failure (e.g., space issues)**

**-. how to recover in midst of a multi-step process?**

**-. more careful separate workflow?**

**\*. needed - a common workflow for file system anomalies**

**-. What should be done/noted if the file system is inaccessible?**

**-. possibilities: bad command, command failure (e.g., permission issues, missing files)**

**-. how to recover in midst of a multi-step process?**

**-. more careful separate workflow?**

These seem like repeats of above in a slightly different context, so, see above responses.

***I agree***

**\*. needed - more thought for notifications**

**-. for everywhere where a notification is required, who should be notified?**

This depends on the notification. Data admins should be contacted for e.g., notifications regarding data fetch/upload. Master admins should be alerted for e.g., storage space alerts, service instability.

**-. The master admin(s)?**

**-. The data admin(s)?**

**-. needed - a common workflow for notifications and their anomalies**

We aren’t sure what anomalies could occur with notifications. Being sent to the wrong person, not being sent at all. We aren’t sure how you could even detect those let alone any actions to take regarding them.

* ***For any sort of network-based communication, network inaccessible***
* ***If e-mail is used, e-mail undeliverable (invalid e-mail; e-mail rejected; mailbox full)***
* ***If texting is used, text undeliverable (similar)***
* ***For logging, logging service offline / inaccessible***

**-. For registered users, through the website?**

**-. What happens if the user is logged off when the notification is required -**

**e.g., on an upload from CHR**

Depending on the severity of the notification, emails could be sent.

* ***Agreed. Should be noted in the flows. As a prospective admin, I’d like to know what a system will give me when problems arise.***

**-. Via e-mail?**

**-. What happens if e-mail is unreachable?**

There’s nothing to be done, then.

* ***Not necessarily.*** 
  + ***Log the failure message, perhaps marking it specially in the log.*** 
    - ***Not to implement just now or perhaps ever, but consider a utility that ran as a timer job, checked for such messages, and somehow responded***
  + ***Provide for secondary and tertiary places to which to send messages***
    - ***Other e-mails***
    - ***Phone numbers to text***

**\*. needed - a common workflow fo rlogging**

**-. What steps in the process should be logged?**

All committed actions. I.e., do not log a user clicking between options in the UI, but do log the queries associated.

* ***Agreed. Should be noted in the flows.***

**-. What happens if logging fails?**

Email system admin.

* ***Agreed. Should be noted in the flows.***

**\*. System installation workflow**

**-. Need this as well, including (e.g.) establishing initial admin account and password**

**-. Should remote, web-based installation be permitted?**

We’re unsure of what you mean by this question. If CPH uses ETSU servers for this, ITS will handle the installation, right?

***Most likely, no. ITS will almost surely task CPH with maintaining these applications. Automating system installation as best as we can would be important for reinstalling the system at need – e.g., in the event of system migration or server failure***

**-. Contingencies**

**-. Insufficient disk space on server**

**-. Password strength inadequate**

**-. Application installation failure**

**-. Database**

**-. Service initialization failure**

**\*. Uploading data**

**-. Join the two into a single flow**

**-. Use a connector to from the uploading data workflow make the connection clear**

**-. Who should be authorized to upload data?**

**-. Any master admin? (I'd say yes)**

**-. Any data admin? (I'd say yes)**

**-. Contingencies - what happens if**

**-. Server inaccessible**

**-. Database inaccessible**

**-. File system inaccessible**

**-. The data to upload has already been uploaded to the website**

**-. Upload to the host fails partway through workload, due to**

**-. Failure to access the CHR website**

**-. The attempt to transform the content for storage in CPH-IVT fails, due to**

**-. Invalid / corrupt CHR data format?**

**-. The attempt to load the CPH-IVT with data fails**

**-. Notifications**

**-. Who should be notified on an upload?**

**-. How should the process be logged?**

**\*. Registration workflow (users)**

**-. Do we need two registration processes - one for ETSU users and one for external users?**

**-. For internal users, e-number will work as their UID**

**-. If we register external users, do we use their e-mail as their SUID?**

**-. Contingencies**

**-. Server inaccessible**

**-. Database inaccessible**

**-. Invalid attempt to register - specifics**

**-. User name already taken - how is this treated**

**-. Typically, not as forgotten user name**

**-. E-mail for registration already in use?**

**-. Different sites handle this differently**

**-. Invalid user data: e.g.,**

**-. Invalid name**

**-. Check for bogus characters**

**-. Invalid e-mail address**

**-. Disallow e-mail address capture for ETSU users?**

**-. Weak password**

**-. Do we enforce strong password requirements, and, if so, for what roles?**

**-. Notifications**

**-. Who should be notified on an attempt to register?**

**-. How should the process be logged?**

**\*. Read and possibly modify user account data workflow (users)**

**-. Need to allow user to change**

**-. Password**

**-. Possibly e-mail address**

**-. Other personal data?**

**-. Contingencies**

**-. Server inaccessible**

**-. Database inaccessible**

**-. Invalid attempt to register - specifics**

**-. Invalid name?**

**-. Invalid e-mail address?**

**-. Weak password?**

**-. Notifications**

**-. Who should be notified on an attempt to register?**

**-. How should the process be logged?**

**\*. Delete user account workflow (users)**

**-. Contingencies**

**-. Removal of self when self is master administrator**

**-. Notifications**

**-. Who should be notified on an attempt to register?**

**-. How should the process be logged?**

**\*. Add user workflow (master admin)**

**-. Similar but not identical to registration workflow - initiated by master admin**

**-. Contingencies**

**-. Server inaccessible**

**-. Database inaccessible**

**-. The user to add is already in the system**

**-. Notifications**

**-. Who should be notified when a user is added?**

**-. How should the process be logged?**

**\*. Read and possibly modify user account data workflow (master admin)**

**-. Needs to allow modification of any user-related information**

**-. Contingencies**

**-. Server inaccessible**

**-. Database inaccessible**

**-. The user to remove isn't in the system?**

**-. This could happen if two admins are attempting to remove a user at the same time**

**-. Notifications**

**-. Who should be notified when a user is removed?**

**-. How should the process be logged?**

**\*. Remove user workflow (admin)**

**-. Removal of the last user needs to differentiate between**

**-. Removal of the last person whose role is master administrator**

**-. Removal of any other users, since, given the presence of a master admin,**

**any role can be added**

**-. Contingencies - what happens if**

**-. Server inaccessible**

**-. Database inaccessible**

**-. The user to remove isn't in the system?**

**-. This could happen if two admins are attempting to remove a user at the same time**

**-. Notifications**

**-. Who should be notified when a user is removed?**

**-. How should the process be logged?**

**\* View all user account data workflow (master admin)**

**-. Need to specify**

**\* View and possibly update database workflow (master admin)**

**-. Need to specify**

**\* View log workflow (master admin)**

**-. Need to specify**

**\* Create region workflow (master admin, data admin)**

**-. Need to specify**

**\* View and update region workflow (master admin, data admin)**

**-. Need to specify**

**\* Delete region workflow (master admin, data admin)**

**-. Need to specify**

**\* View all regions workflow (master admin)**

**-. Need to specify**

**\*. User login workflow (any)**

**-. Here again, should we require all users to register before using the site?**

**-. Contingencies**

**-. The server is offline?**

**-. Notifications**

**-. Who should be notified when a user attempts to login?**

**-. How should the attempt be logged?**

**\*. Chart creation workflow**

**-. Rename to graph creation workflow**

**-. Contingencies - what happens if**

**-. The server is offline?**