**SOX Walkthrough Deliverables and Timelines**

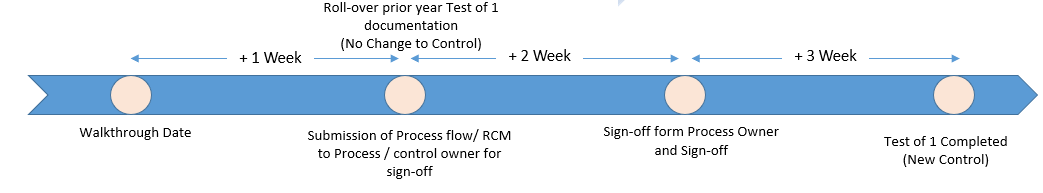
**Overall Audit Practice Guidance**

The purpose of this document is to summarize the SOX walkthrough documentation expected to be submitted to Management and PwC, and the related timelines. During the SOX walkthrough process all BU teams are expected to prepare process flow templates and update RCM, utilizing the attached templates. At the completion of each walkthrough meeting the expected deliverables are: 1) Completion of BPA Test of Design Screens, 2) Process Flow (using attached template) and 3) Risk and Control Matrix (“RCM”) (using attached template).

Once the process flow and RCM covering a process/sub-process have been completed it is expected that the BU teams will communicate these to Management who is expected to provide feedback and approve the documentation. Once we have received Management's approval it is expected that the BU teams will submit the process flow and RCM to the PWC Sox teams.

If the respective controls have not significantly changed since prior year, the SOX teams are expected to rollover the prior year documentation. However, if the control procedures have changed the SOX teams are expected to upload new documentation into BPA. Documentation should be sufficient to evidence our full understanding of the control process and to evidence design effectiveness. The SOX teams should document the Test of One (“WTO”), consistent with the test of operating effectiveness documentation, including our typical testing attributes, tick marks, test procedures etc. This level of documentation will reduce our testing and documentation during our test of operating effectiveness.

Below is a summary of the expected timelines related to documentation requirements:



**Additional guidance – Information Technology**

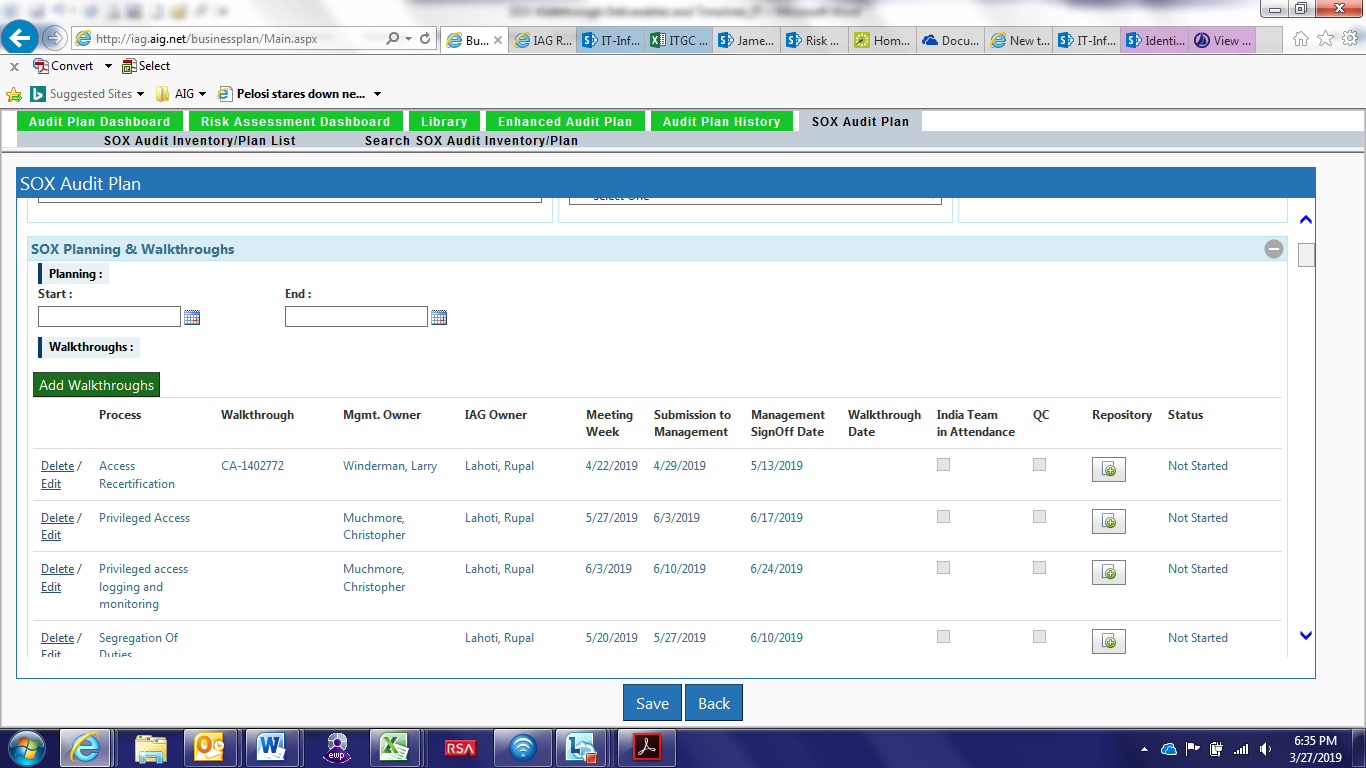
**Walkthroughs Execution**

ITGC Walkthrough schedule and timeline is being uploaded into BPA and will be found within each individual SOX plan record. Walkthroughs are created at the organizational hierarchy/process/sub-process level. Since there may be multiple walkthroughs performed for each sub-process, control assessment ID(s) will be entered into the free form Walkthrough field to demonstrate the corresponding control(s).

**Action**: Prior to the walkthroughs, ensure that:

* Prior year’s documentation of the control (e.g. process flows) is translated into the new Audit format and shared with the client
* Documentation is reviewed with the client and updated, as needed, in preparation for the walkthrough
* Clients are clear on the walkthrough agenda and expectations and are prepared to **lead** the walkthrough and demonstrate an example of one
* Draft agenda is shared with PwC ahead of time and any feedback incorporated. Final walkthrough agenda should address AIG and PwC topics
* For controls that were consolidated (e.g. job schedule changes, version control, separation of environments) because the risk was considered to be covered in other existing controls, leverage the walkthroughs to confirm that existing controls fully cover the related risk for these areas. Where it doesn’t, a separate control would need to be created. For example, if it’s determined that job scheduling changes do not follow a standard change management process in a particular environment, a separate control should be created. Please also ensure that test steps are updated appropriately to capture testing/sampling of these controls.

**Action**: As the walkthroughs are scheduled, BPA should be updated to reflect the actual Walkthrough Date; in addition, Status field should be updated to reflect the progress of the walkthrough scheduling and documentation.



Walkthrough – free form field that will be used to capture control assessment ID covered by a given walkthrough

Mgmt Owner – IT process owner

IAG Owner – IT SOX Lead

Meeting Week - the end date of the time range for completing the walkthrough.

Submission to management (auto calculated) - target date for providing WT documentation to management for confirmation, one week after the Meeting Week.

Management sign off (auto calculated) - target date for receiving confirmation/sign off on the WT documentation, two weeks after Submission to Management.

Walkthrough date – actual date of the walkthrough

Repository – used to attach process flow documentation

Status - progress of WT scheduling and documentation. Options include: not started, meeting scheduled, in progress, management sign off, completed. Completed indicates management sign off has been obtained.

**Walkthrough – Minimum Documentation Requirements**

|  |  |  |
| --- | --- | --- |
| **Documentation** | **Completion Guidance** | **Documented Where** |
| Meeting invitation and attendees | A pdf of the walkthrough meeting invitation showing AIG and PwC participants as well as the walkthrough agenda should be included as part of the walkthrough documentation. | Walkthrough repository |
| Process Flows (minimum requirement) | Process flows have to be completed in the format provided by the Audit Practices (refer to the attachment). Existing process flows provided by management can be leveraged, where applicable, but should be further updated to align with the audit template requirements.  In addition, since multiple controls may be covered in the same process flow, please indicate the relevant Control Assessment ID(s) on the process flow cover page. | Walkthrough repository |
| Risk and Control Matrix  (minimum requirement) | Risk and Control matrix summarizes risks and key controls, which will then form the basis for operating effectiveness testing. Any control design gaps identified during the walkthroughs should be documented in the RCM.  While the attached Excel template is not a required deliverable in itself, it includes the sub-set of fields that will be required to be populated in BPA to capture walkthrough results and design testing. These fields can either be updated directly in BPA OR captured in the Excel template and uploaded into BPA centrally. | Control Screen  Control Leadsheet – Test of Design tab |
| Narratives | A high level control narrative should be captured in the “Control Activity performed by Control Owner” field (column M of the walkthrough template). Based on the complexity of the control, additional, more granular narrative documents may be completed and attached as part of the overall walkthrough documentation. | Control Leadsheet – Test of Design tab |
| Test of One  (required) | Test of One should be completed during the walkthroughs, by observing demonstration of the end to end control execution for one example. The test of one can count towards the overall operating effectiveness testing. | Control Leadsheet - Test of Operating Effectiveness tab |

Review and approval

For documentation rolling over from the prior year – Test of Design tab, including supporting documentation, has to be completed and reviewed one week after the Walkthrough date

For a new or changed control – Test of Design tab, including supporting documentation, has to be completed and reviewed one week after Management sign off date.

**Action**: After walkthrough is completed, ensure that:

* Process flow, narrative, and RCM documentation is updated and submitted to management for review
* Management feedback is incorporated and final sign off obtained on the documents
* BPA is updated to reflect any changes to the control descriptions, test steps, application linkages, IT dependent controls, etc.
* After management sign off, final documentation is submitted to PwC

**Action**: Before testing commences, ensure all of the in-scope applications, controls, and test procedures have been aligned with PwC.

**IT Dependent Controls**

In addition to conducting ITGC walkthroughs, IT SOX auditors will participate in the Business walkthroughs to identify IT dependent controls (e.g. automated controls, interfaces, key reports). Each IT SOX lead should work with their business counterparts to identify business walkthroughs relevant for IT participation. In the instances when IT SOX auditor is not able to attend due to scheduling conflicts or timing constraints, the following probing questions should be leveraged by the Business auditors to identify IT dependent controls. Subsequent follow up meetings may need to be scheduled to obtain a deep dive of the identified controls.

Business walkthrough probing questions –



**Automation**

Walkthroughs should be leveraged to confirm existing or identify new opportunities for automated control testing. Please leverage the attached automation use case inventory for a view of the existing automation pipeline.



For the automation use cases where development is complete (3 use cases), testing can be performed centrally under Infrastructure Services.  Business Units can refer to the testing as interdependency.  In addition, Infrastructure Services and other Business Units specific plans that are not covered by the central automation or requiring a manual assessment will continue to be executed separately.  The team can reach out to Jared Henderson and Carlo Malacon to coordinate obtaining test results.

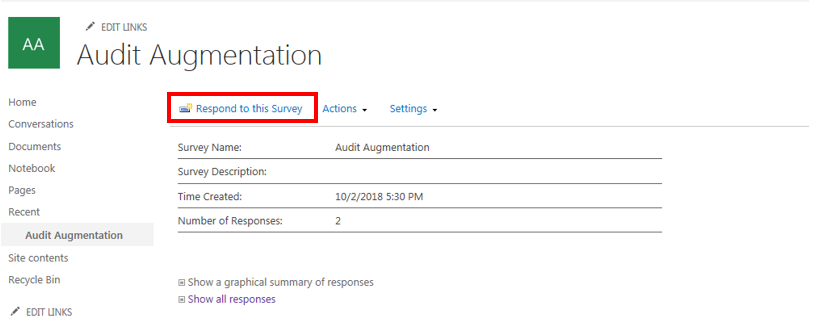
* If PwC relies on management testing of these controls, the automation solution needs to be vetted with PwC prior to leveraging in testing.
* If PwC doesn’t rely on management testing of the control, automation solution can be used for initial testing.

The other automation solutions in the pipeline will be considered for phase 2 testing, if developed and vetted by PwC by the end of July.

For any controls identified as potential new automation candidates during the walkthroughs, consider:

* *Data availability* – are we able to get data on a regular basis in an automated way (e.g. a system feed, FTP, automated email, etc.)?
* *Process is well defined and repeatable* – is process clearly defined and can be assessed objectively based on the defined thresholds, requirements, workflows, etc.?

When both of the above criteria are met, the control would be considered a candidate for automation. A new portal is being developed to submit new automation ideas. In the meantime, leverage the below survey link to capture new automation ideas. Please [**Click Here**](https://share.connect.aig/teams/AuditAugmentation/Lists/Audit%20Augmentation/overview.aspx) to access the survey on SharePoint and select **Respond to this Survey** near the upper-left corner (see below screenshot).



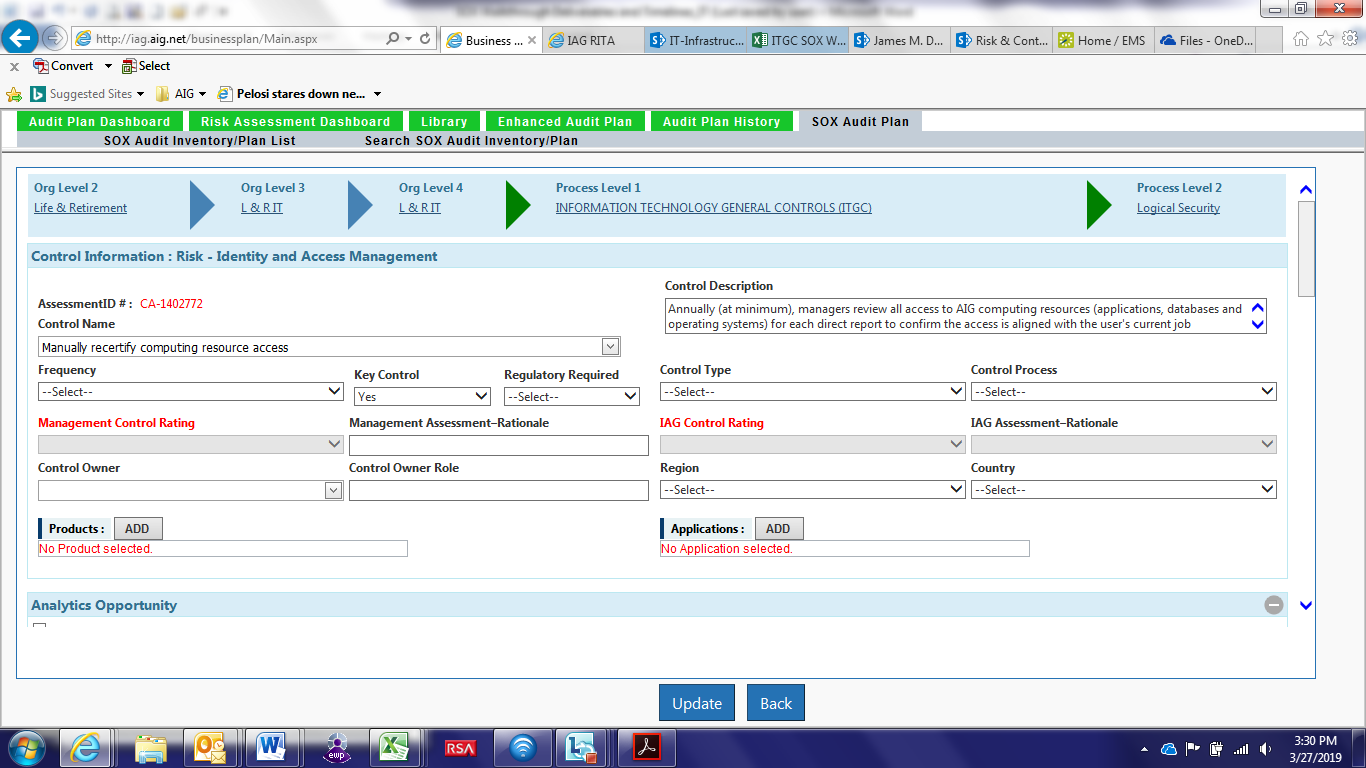
Note: there is a pending BPA enhancement request to align test steps to the automation use cases in BPA.

**BPA Updates – Control Screen**

Updated control descriptions and application linkages captured during the rationalization effort will be uploaded into BPA. Any subsequent changes to the controls identified as a result of the walkthroughs should be made directly in BPA.

*Control Updates*

From the audit plan record, click on the Control hyperlink to navigate to the Control Screen. Please refer to the descriptions of the key fields to the right. Note that descriptions are provided for select fields that have been newly added or may need to be updated as a result of the walkthroughs.



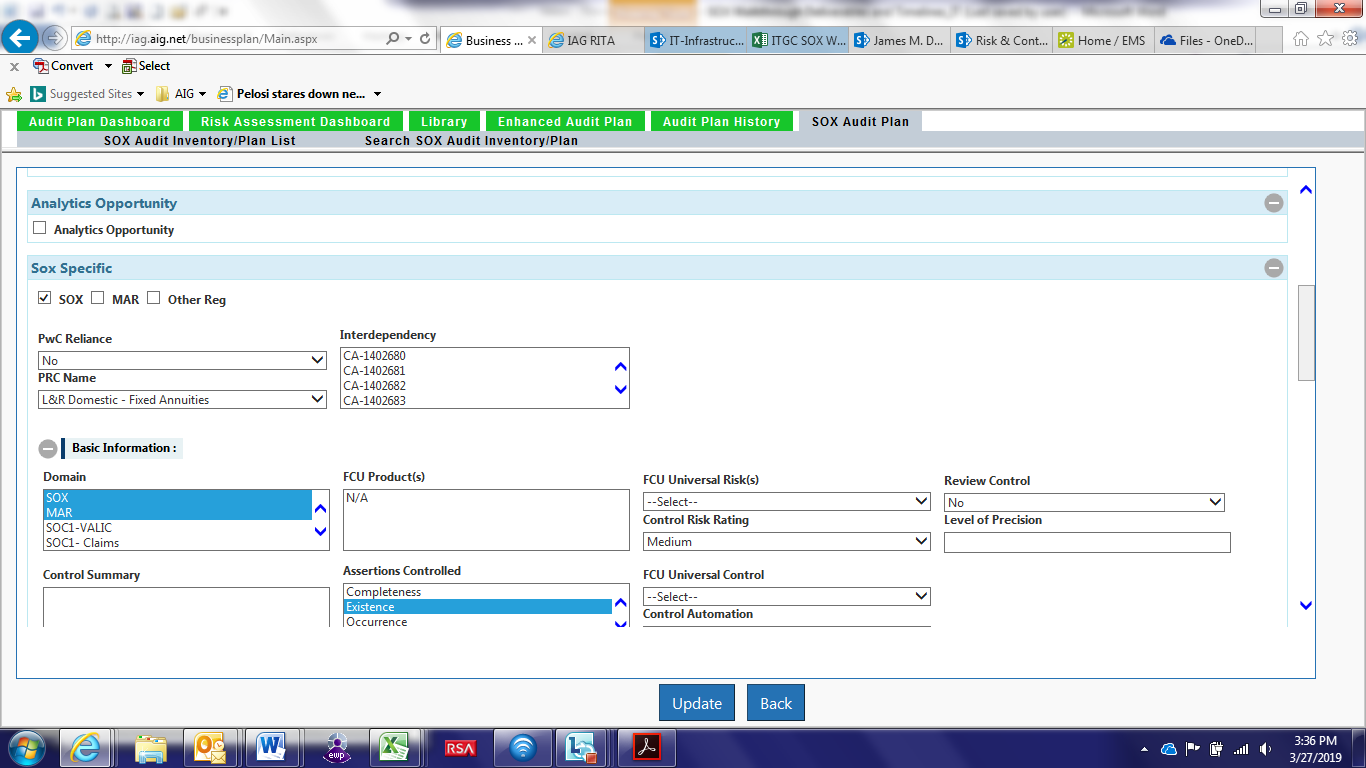
Control Name – equivalent to the Control Summary field in Archer. Reflects brief overview of the control

Control Description – detailed description of the control, as implemented in a given environment. While generic wording may have been used initially, it is expected to be customized, as needed, to reflect the actual control implementation.

Key Control\* – denotes if this is a key control. While non-key controls are still retained in BPA, they are not visible in the plan records.

Applications\* – applications covered by a given control. Multi-select value is available.

\*refer to Appendix for scope change process

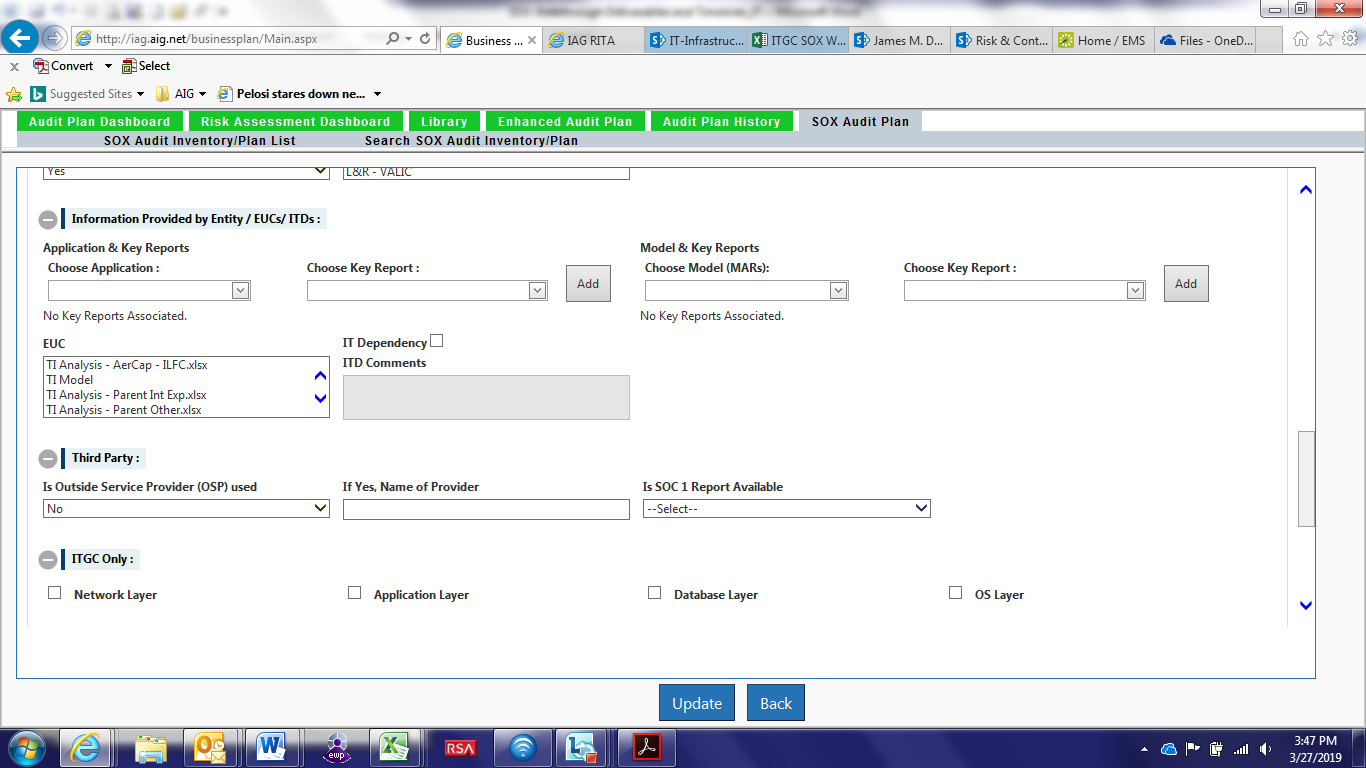


Analytics Opportunity – should be checked if the control is a candidate for automated testing

SOX Specific - Checkboxes are used to indicate if the control is in scope for SOX, MAR and/or other regulatory requirements.

PRC Name – PRC name is inherited from Archer

Interdependency – if testing for this control is performed by a different Business Unit, leverage the “interdependency” field to select the corresponding Control Assessment ID(s) under which testing is performed.



Application & Key Reports – select application and corresponding key report

IT Dependency – will be leveraged to capture interfaces (field is under development in BPA)

Third Party – indicate if the control relies on the Third Party Service Provider. If yes, populate the name of the provider and indicate if SOC1 report is available.

ITGC Only – indicate if the control applies to the network (Active Directory), application, database, and/or OS layer. Additional detail about the selected environment (e.g. AD domain, Database type and server, etc.) will be provided at the test plan level.

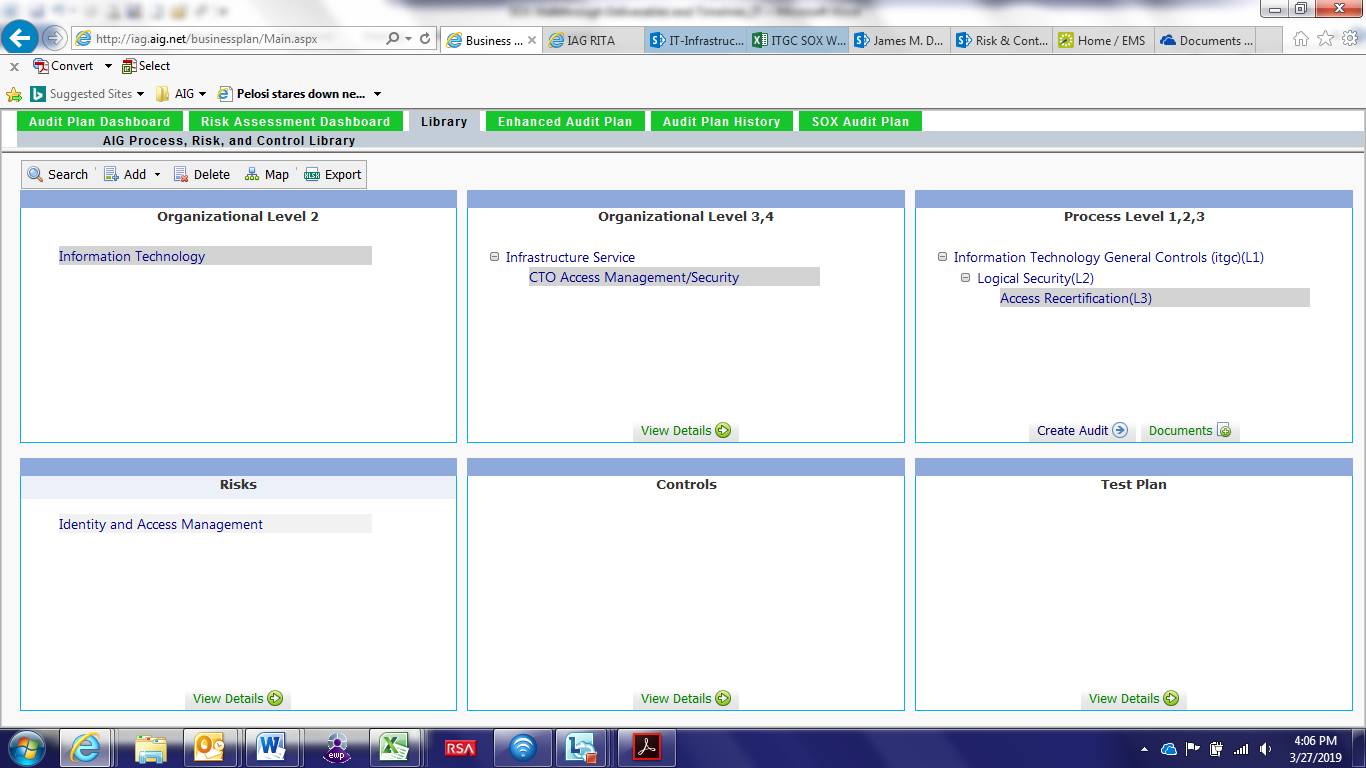
*Adding a New Control*

In order to add a new control, navigate to the Library tab in BPA. As a starting point, click on the appropriate Organizational Level 2 to select the Division. Once Division has been selected, Organizational Level 3, 4 will refresh to allow selection of hierarchy values applicable to a given Division.

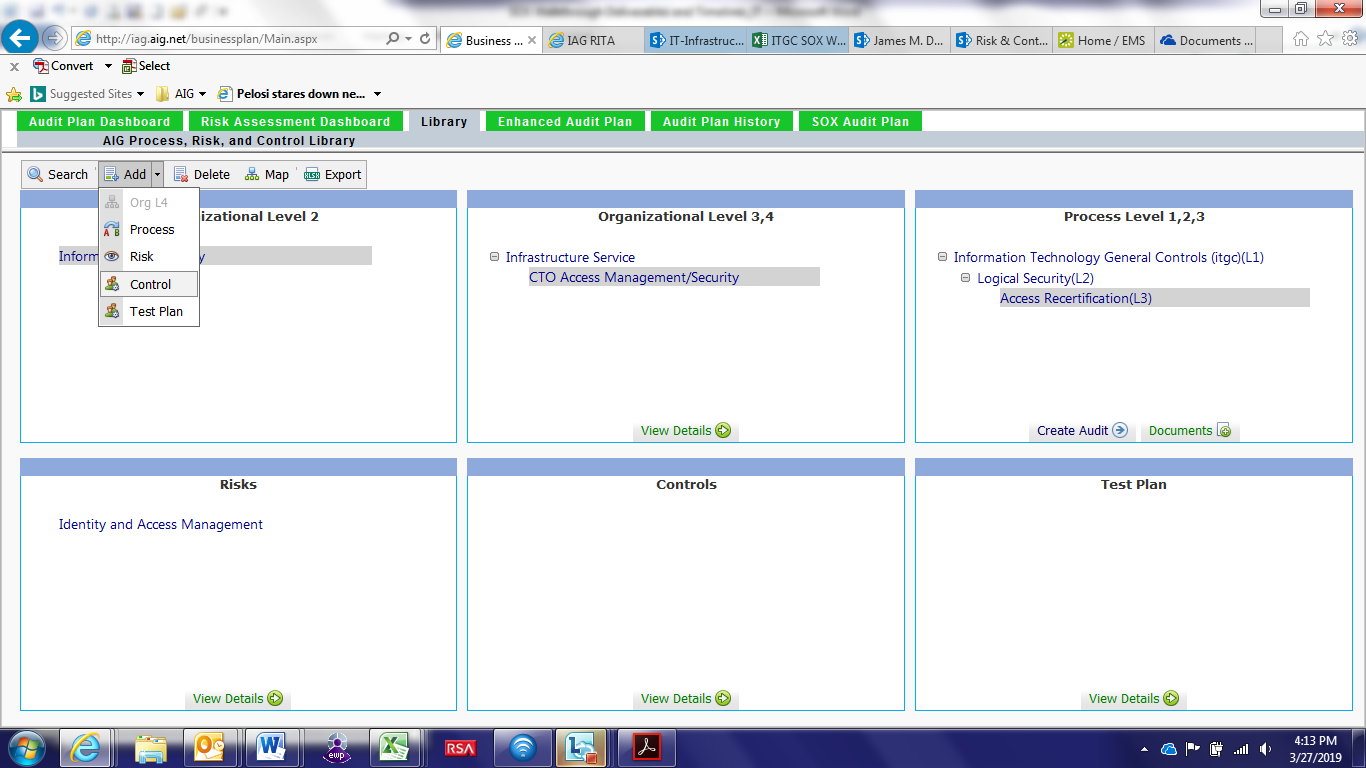
In the Process Level box, select the applicable Process L1, L2, L3 values. For SOX purposes, Level 1 should equal to IT General Controls (ITGC). Level 2 is equivalent to the Process (e.g. Logical Security) and Level 3 is equivalent to the Sub-Process (e.g. access re-certification).

In the Risks box, the available risk values will populate based on the Process selection. Click on the risk that the new control should be mapped to.

The full organizational, process, and risk hierarchy must be selected in the Library tab in order to add new controls.



In order to add a control, in the upper left corner, select “Add” – “Control”



This will allow you to navigate to the new Control screen and populate required information for a new control. When the new control is saved, the control assessment ID will be automatically generated by BPA.

After the control is added, please reach out to Frank to add the new control to the corresponding SOX plan record. Include control assessment ID and SOX plan reference number in your request.

If the control is changed to non-key, please reach out to Frank to remove the non-key control from the corresponding SOX plan record. Include control assessment ID and SOX plan reference number in your request.

Note: Separate guidance will be developed for test plans.

**Appendix 1**

Below guidance should be followed for making scope changes to the applications and controls as a result of the walkthroughs.

|  |  |  |  |
| --- | --- | --- | --- |
| **Type of Change** | **Approve** | **Consult** | **Notify** |
| Application being added to or removed from SOX or other regulatory scope | * Business and IT IAG SOX leads * Business and IT IAG MDs | * PwC | * Business Unit CIO * Business Owner of the application * IAG Transformation and Automation lead |
| Control change from “key” to “non-key”  Control change from “non-key” to “key” | * IT IAG SOX lead | * PwC | * IT IAG MD for a given Business Unit * IAG Transformation and Automation lead |
| Control re-alignment to a different “sub-process” – L3 | * IT IAG SOX lead |  | * IAG Transformation and Automation lead |
| **Strategically, application/scope changes will be submitted and approved via ServiceNow, with supporting documentation maintained in the system.  In the interim, documentation supporting the changes should be retained on the IAG Sharepoint site.** | | | |

**Appendix 2**

Attached is the current schedule of ITGC walkthroughs

