AI2.10 Application Software Maintenance

Description

Develop a strategy and plan for the maintenance of software applications.

Control Practices

1. Design an effective and efficient process for application software maintenance activities. Prioritise maintenance activities, paying attention to business needs and resource requirements. Ensure that all changes in software comply with the formal change management process, including impact on other systems and infrastructure. Ensure that risk and security requirements and interdependencies are addressed.

2. Monitor all maintenance changes. If appropriate, aggregate maintenance tasks into a single ‘change’ to make management and control easier. Ensure that any major maintenance is categorised and managed as a formal redevelopment.

3. Establish the review and approval of all emergency or any other changes applied without adherence to the formal change process.

4. Ensure that the pattern and volume of maintenance activities are analysed periodically for abnormal trends indicating underlying quality or performance problems.

5. Establish processes to ensure that all maintenance activity is completed successfully and thoroughly. Track maintenance activities to ensure completion. Where necessary, update user systems and operational documentation.

Entity Specific Practices

N/A

Instruction 1st Line of Defence

Read the provided Control Objective description and the Control Objective Practices carefully. Explain which controls are implemented locally to meet the Control Objective and provide evidence. Evidence can be procedure/policy documentations and a random example to prove that the procedure/policy is followed. Determine the level of compliance for this Control Objective based on the rating scale below. If the score is 3 or 4 an improvement action must be taken and recorded in AGRC.

EVIDENCE SUGGESTIONS:

DESIGN:

- Policy or Process document for the maintenance of software applications

IMPLEMENTATION:

- Change management products like (Business) approval for changes, Evidence of testing, Monitoring of status changes.

RATING SCALE:

1. Compliant - Control Objective and all or majority of the Control Objective Practices are satisfactory met

2. Predominantly Compliant - Control Objective is almost met , since most of the relevant Control Objective Practices are met

3. Implementation in progress - The Control Objective or relevant Control Objective Practices are not met and implementation of process/measure/control is in progress

4. Not implemented - The Control Objective is not met since no process/measure/control is in place

5. Not relevant - The Control Objective is not relevant

Ambition level

3: (Defined)

Conclusion

Compliant

Rationale

Control Practices:

1. Design an effective and efficient process for application software maintenance activities. Prioritise maintenance activities, paying attention to business needs and resource requirements. Ensure that all changes in software comply with the formal change management process, including impact on other systems and infrastructure. Ensure that risk and security requirements and interdependencies are addressed.

CP1 – Locally, application software maintenance activities are governed by the guidelines defined in Section C.1 of #1 - IT Change Management Policy.pdf in accordance with #2 - AIM Change Management Policy.pdf. These guidelines outline the steps required for all changes, including:

- A Request for Change (RFC) specifying the change type, change details, and supporting documentation (such as implementation details and a back-out plan). This information is contained on a change ticket opened within the PS'Soft ticketing system – see #3 - PS'Soft Change #15391.JPG for a sample ticket.
- Testing of the change - both developer testing as well as User Acceptance Testing (UAT) to search for problems with the updated system before migration into production servers.
- Approval of the change, which must pass through both the Change Advisory Board (CAB) and Business Change Advisory Board (BCAB) for discussion. These reviews are used to discuss effects of the change on other IT systems, infrastructural security, and business processes. The changes discussed by the CAB and BCAB are documented in the meeting minutes taken during each change review meeting, see #4 - CAB Meeting 08 06 2015.pdf and #5 - BCAB Meeting 07 30 2015.pdf.

A workflow diagram depicting each step in the change management process is shown in section C.3 of #1 - IT Change Management Policy.pdf.

Additionally, a Change Implementation Run Book (CIR) must be completed for each RFC that is submitted, as described in section E1.6 in #1 - IT Change Management Policy.pdf. The Change Requester must complete the CIR security questions which are then reviewed by the Change Manager. These security questions will provide details about the change that a risk rating can be derived from. Based on the risk rating the Change Manager will determine if an additional security/risk review is required.

2. Monitor all maintenance changes. If appropriate, aggregate maintenance tasks into a single 'change' to make management and control easier. Ensure that any major maintenance is categorised and managed as a formal redevelopment.

CP2 - All maintenance changes are monitored and logged as required by the local guidelines, #1 - IT Change Management Policy.pdf. These rules support the global policy given in #2 - AIM Change Management Policy.pdf. An example maintenance change is given in #6 - Maintenance Change.png. CAB meeting minutes for this change can be found in #7 - CAB Meeting 09 17 2015.pdf.

All maintenance changes have a PS'Soft ticket listing information pertinent to the change. This information includes a technological complexity grade of Low, Medium, or High (#8 - 16333 CIR.xlsx). Complex changes are classified as such, and are given thorough testing, as a formal redevelopment would, in order to ensure that the change does not result in a loss of business function. Sample test results for the previously shown change can be seen in #9 - ATIS Test Results.log.

3. Establish the review and approval of all emergency or any other changes applied without adherence to the formal change process.

CP3 – Emergency changes include changes that must be implemented as soon as possible, typically to resolve a major incident or implement a security patch. The procedure for emergency changes is described in Section C.4.1 of #1 - IT Change Management Policy.pdf, in accordance with #2 - AIM Change Management Policy.pdf. This procedure does not require a formal CAB and BCAB review and approval prior to implementing an emergency change, a retroactive approval of the change is required after it has been implemented. The procedure for emergency changed expedites the change process in cases where decisive action is needed. An example emergency change request ticket and its corresponding retroactive approvals are shown in #10 - PS'Soft Change #14959.JPG and #11 - Retroactive approval #14959.msg.

4. Ensure that the pattern and volume of maintenance activities are analysed periodically for abnormal trends indicating underlying quality or performance problems.

CP4 - The pattern and volume of maintenance is recorded weekly at CAB meetings (#4 - CAB Meeting 08 06 2015.pdf). This will allow for prompt discovery of worrying maintenance trends, should they occur. Detailed data is kept logging the number of changes and rollbacks which occur (#12 - Change Data 2015.xlsx). This sheet also includes details on the status of each change discussed. By observing this data for any significant change in the number of rollbacks, abnormal trends indicative of performance problems can be quickly discovered and addressed.

5. Establish processes to ensure that all maintenance activity is completed successfully and thoroughly. Track maintenance activities to ensure completion. Where necessary, update user systems and operational documentation.

CP5 - Maintenance policies are established locally within #13 - IT System Maintenance and Hardening.pdf, and follow global policies listed in #14 - AIM System Hardening Policy.pdf. Section C.5 of the local policy establishes procedures for approving and tracking maintenance processes, including email notifications before and after maintenance, scheduled maintenance windows, and maintenance ticket approval steps. To help ensure that maintenance is completed on-time, regular maintenance is performed during scheduled maintenance windows. These maintenance activity requests are opened and tracked using the PS'Soft ticketing system, to be closed upon successful completion (#15 - PS'Soft Change #16333.PNG). Change status is monitored by quarter in #12 - Change Data 2015.xlsx. If a change is rolled back or cancelled for any reason, detailed information about the change will be recorded within this sheet. User systems will be periodically updated in order to implement maintenance changes, as discussed within #16 - IT Desktop Patch Management Policy.pdf. Operational documentation is updated within the wiki as necessary.