**Configuration Status Accounting**

Configuration Status Accounting and Reporting keeps track of the following CI status changes:

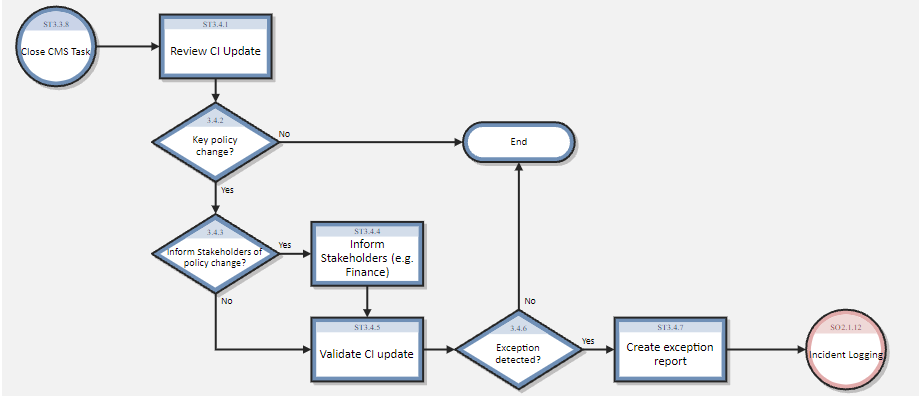
• New item received

• Reporting the implementation, the new item

• Check specific tests

• Identify exceptions

• Unauthorized CIs or CI version changes



|  |  |  |  |
| --- | --- | --- | --- |
| Process ID | Procedure or Decision | Description | Role |
| ST 3.4.1 | Review CI update | Modifications to the key attributes of the CI are recorded in the historical record and verified. The following points are evaluated:   * State of change * Version number * Implementation date   Verification date   * Description of possible incidents * Critical CI changes are logged with entries by Reason, Date, and Person Who Logs Status Change. | Configuration Auditor |
| ST 3.4.2 | Key policy change? | Determine if the policy needs to be reviewed or validated. It must be clearly contained as the new item may affect and the benefits it brings as well as the method of application. | Configuration Auditor |
| ST 3.4.3 | Inform stakeholders of policy change? | The purpose for which it should be reassessed must be informed, as well as recommendations on how to improve or restructure the process.  Verify that the event should be reported. If not, go to ST 3.4.5. If so, continue to ST 3.4.4. | Configuration Auditor |
| ST 3.4.4 | Inform stakeholders | Specific changes must be reported to the stakeholders. These include:   * Project manager * Customer * Tester * Financial director * Political Accessor * Programmers   It should be noted that they should be advised that what role they will take in the new change and what responsibilities correspond to them. | Configuration Auditor |
| ST 3.4.5 | Validate CI update | Confirm that all relevant status data documented in the CI is complete and correct, according to Configuration Management policies derived from agreements, relevant legislation, and standards.  Ensure that the status change or version update is a result of an authorized change.  It is important that at this point there is a concise documentation that follows a format, that provides methods for revisions and adding new changes. | Configuration Auditor |
| ST 3.4.6 | Exception detected? | If the CI update or CI details are not correct or complete according to the configuration policies it will be necessary to raise an exception.  It is important that in order to avoid an exception, the document specifies; who, what, when, why and how. This in order to facilitate control over changes. | Configuration Auditor |
| ST 3.4.7 | Create exception report | A report will be created that includes the incident in detail mentioned to the parties involved, the reason for the incident, possible recommendations and the date.  The report should answer the following questions:  What needs to change?  who requests the change?  when was it requested?  What areas does the change affect or include?  What other aspects of the system are involved? | Configuration Auditor |