Service Asset & Configuration Management PinkVERIFY™

SACM	General Criteria
SACM-11-G-001	Does the tool use ITIL 2011 Edition process terms and align to ITIL 2011 Edition workflows and process integrations? ----------
SACM-11-G-002	Does the tool have security controls in place to allow only authorized staff and users to view, open, modify, authorize and close records based on their role? ----------
SACM-11-G-003	Does the tool support designating fields as mandatory? ----------
SACM-11-G-004	Does the tool provide out-of-the-box reports and facilitate flexible (ad hoc) report generation? ----------
SACM-11-G-005	Does the tool facilitate the production of management reports from historical records? ----------
SACM-11-G-006	Does the tool provide an audit trail for record information and updates? For example: IDs of individuals or groups opening, updating and closing records; dates and times of status and activities updates, types of activities ----------
SACM-11-G-007	Does the tool automate notification and escalation to keep IT and users informed of potential issues or progress? ----------
SACM-11-G-008	Does the tool provide facilities within the tool database for archiving/deleting closed records? ----------

Service Asset & Configuration Management PinkVERIFY™

SACM	Core Criteria
SACM-11-C-001	Does the tool facilitate the registration of new Configuration Item (CI) Records? For example: template, Baseline, New CI Records ----------
SACM-11-C-002	Does the tool facilitate the registration and management of an organization's logical, physical and virtual Configuration Items (CIs)? For example, CI Records for services, systems, hardware, software, documents, virtual machines, servers, etc. ----------
SACM-11-C-003	Does the tool have pre-defined CI attributes? For example, serial number, version, and location attribute ----------
SACM-11-C-004	Does the tool facilitate user-definable attribute fields to support different formats? For example: model numbers, documentation references ----------
SACM-11-C-005	Does the tool facilitate the automated validation of CI data through use of data validation and reconciliation techniques? E.g.: Enforcement of standard naming conventions and reconciling federated data sources ----------
SACM-11-C-006	Does the tool have pre-defined and user-definable relationships between CIs? For example, parent/child, peer-to-peer, installed on, runs on ----------
SACM-11-C-007	Does the tool have a field or fields to show current status of the CI? For example: in production, in maintenance, retired ----------
SACM-11-C-008	Does the tool support CI lifecycle status accounting management? For example, designed, ordered, under development, in test, implemented, in production, in repair/maintenance ----------

SACM	Core Criteria
SACM-11-C-009	Does the tool facilitate the recording of CI baselines? For example, reverting to a previous version of CI Configuration in the event that a Change fails ----------
SACM-11-C-010	Does the tool facilitate the verification of the CI Record data with the actual physical environment by either automated or manual means? For example, the use of Systems Management tools to validate real time environment; Service Desk updates ----------
SACM-11-C-011	Does the tool facilitate the linking of CI records to source content residing in the Definitive Media Library? ----------
SACM-11-C-012	Does the tool provide CI inventory, asset and financial type information to facilitate Configuration audits? ----------
SACM-11-C-013	Does the tool maintain a history of CI Records on each configuration item's lifecycle? For example: Records on installation and changes ----------
SACM-11-C-014	Does the tool provide a form of graphic display to show the relationships among CIs? ----------
SACM-11-C-015	Does the tool enable a hierarchical and network structure of CI relationships? ----------
SACM-11-C-016	Does the tool facilitate the automatic identification of CIs related to a given CI? For example: when an incident is reported on a failed CI, related CIs can be identified, or when a change is proposed for a CI, the related CIs can be identified for risk, scope and impact assessment. ----------

SACM	Core Criteria
SACM-11-C-017	Does the tool facilitate the automatic updating of a CI version if any component CI version is changed? ----------
SACM-11-C-018	Does the tool support data federation and reconciliation with other data sources within the Configuration Management System? ----------
SACM-11-C-019	Does the tool facilitate the identification of a CI in development and enable the CI Record to be changed to a live or in production status? For example: one CI Record throughout the lifecycle ----------
SACM-11-C-020	Does the tool provide a procedure and checklist for manual updates to configuration data, and also record the manual updates in a configuration change log in the tool? ----------

Service Asset & Configuration Management PinkVERIFY™

SACM	Integration Criteria
SACM-11-I-001	Does the tool integrate with Incident Management to enable the creation and maintenance of the linked relationships between CI Records and associated Incident Records?
SACM-11-I-002	Does the tool facilitate Incident Management in providing business criticality and impact indicators of failed CIs for classification of Incident Records?
SACM-11-I-003	Does the tool integrate with Problem Management to enable the creation and maintenance of the linked relationships between CI Records and associated Problem Records?
SACM-11-I-004	Does the CMDB facilitate trending (proactive Problem Management) by identifying infrastructure components that are problematic or unstable? For example, reference or links to Problem Records and Change Records, Status Accounting on “in repair” or “maintenance”
SACM-11-I-005	Does the tool integrate with Change Management to enable the creation and maintenance of the linked relationships between CI Records and associated Change Records?
SACM-11-I-006	Does the tool facilitate impact analysis on CIs? For example: for risk assessment and approval of Change requests
SACM-11-I-007	Does the tool facilitate the prevention of changes being made to CI records without authorization via Change Management? For example, CIs which are in a locked status due to month end schedules or controlled attributes which require a change record relationship for update

Service Asset & Configuration Management PinkVERIFY™

SACM	Integration Criteria
SACM-11-I-008	Does the tool facilitate the identification and reporting of unauthorized changes (additions or removals) to the infrastructure? ----------