Incident Management PinkVERIFY™

INCIDENT	General Criteria
IM-11-G-001	Does the tool use ITIL 2011 Edition process terms and align to ITIL 2011 Edition workflows and process integrations? --
IM-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? --
IM-11-G-003	Does the tool support designating fields as mandatory? --
IM-11-G-004	Does the tool provide out-of-the-box reports and facilitate flexible (ad hoc) report generation? --
IM-11-G-005	Does the tool facilitate the production of management reports from historical records? --
IM-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 --
IM-11-G-007	Does the tool automate notification and escalation to keep IT and users informed of potential issues or progress? --
IM-11-G-008	Does the tool provide facilities within the tool database for archiving closed records? --

Incident Management PinkVERIFY™

INCIDENT	Core Criteria
IM-11-C-001	Does the tool facilitate the opening of Incident Records via various methods? For example: manually via Service Desk agent, user, or automated via email, system alert --
IM-11-C-002	Does the tool automatically create a distinct and unique identifier and number for each Incident Record? --
IM-11-C-003	Does the tool automate the date and time of the incident registration or logging, and all updates throughout the lifecycle of the Incident Record? --
IM-11-C-004	Does the Incident Record have a field or fields to capture contact information of the person reporting an incident and preferred method for notification? ---
IM-11-C-005	Does the Incident Record have a field or fields to identify the reporting source of the incident? For example: person, department, organization, location, monitoring tool (event) --
IM-11-C-006	Does the Incident Record have a field or fields to distinguish Incidents from Service Requests? For example: user requesting a password reset or a new keyboard as self-service request --
IM-11-C-007	Does the tool have a tiered categorization structure allowing the identification of an incident with a service (e.g. payroll) as well as system and component? --
IM-11-C-008	Does the Incident Record have distinct impact, urgency and priority fields, with associated factors which can be defined by an authorized user? --

INCIDENT	Core Criteria
IM-11-C-009	Does the tool have the ability to automate the calculation of priority based on defined impact and urgency factors? --
IM-11-C-010	Does the Incident Record have field or fields to designate the assignment of the Incident Record to an individual or support group? --
IM-11-C-011	Does the tool have the ability to notify and functionally escalate (assign) an incident to an individual or support group based on pre-defined parameters, thresholds or manual override conditions? For example: category (component at fault), response and resolution service levels --
IM-11-C-012	Does the tool have the ability to notify and hierarchically escalate an incident to an individual or group based on pre-defined parameters, thresholds or manual override conditions? For example: response and resolution service levels in jeopardy of breaching --
IM-11-C-013	Does the Incident Record have a field or fields for the input of the incident description and symptoms? --
IM-11-C-014	Does the Incident Record have a field or fields for the input of text by date and time for the incident investigation and diagnosis activities and resolution? --
IM-11-C-015	Does the tool automate the rapid recording, classification and linking of incidents for multiple related incidents? For example: using templates or cloning or copying of an incident that is already open, using a parent-child record relationship --

INCIDENT	Core Criteria
IM-11-C-016	Does the Incident Record have a status field to monitor and track the lifecycle statuses of an incident from detection / reporting through response / assignment to resolution and closure? For example: opened, assigned, resolved, closed --
IM-11-C-017	Does the tool have defined incident resolution and closure statuses, and automated date and time stamps? For example: Resolved, Closed --
IM-11-C-018	Does the Incident Record have a field or fields to record with date and time the incident category information at closure? For example: identifying the repaired component --
IM-11-C-019	Does the tool facilitate gathering customer feedback and / or rating of IT support and service? For example: sending customer satisfaction surveys or feedback request emails after the closing of an incident record --
IM-11-C-020	Does the tool record priority changes with system time stamp, user ID, and action taken for forensic inspection? --
IM-11-C-021	Does the tool accommodate authorized manual priority overrides? --
IM-11-C-022	Does the tool require selection of a justification for manually overriding priority? --
IM-11-C-023	Does the tool facilitate the establishment and application of Incident Models for specific situations? (Example a specific mix of category, service, and CI type) --

Incident Management PinkVERIFY™

INCIDENT	Core Criteria
IM-11-C-024	Does the tool support chronological task sequences and dependencies in Incident Models? --
IM-11-C-025	Are Incident logs in the tool protected from alteration after-the-fact? --
IM-11-C-026	Does the tool limit create and update access to specific data elements by role? --
IM-11-C-027	Do all authorized tool users have read access to all Incident information? --
IM-11-C-028	Does the tool allow authorized users to determine the order in which Incidents were acted on and by whom? --
IM-11-C-029	Does the tool log all Incident actions taken and by whom? --

Incident Management PinkVERIFY™

INCIDENT	Integration Criteria
IM-11-I-001	Does the tool integrate with Knowledge Management - knowledge databases to support incident investigation (e.g. through scripting), diagnosis and resolution (e.g. work-around, temporary fix, routine incident fix)? --
IM-11-I-002	Does the tool integrate with Problem Management to enable the rapid opening of a Problem Record from Incident Management, and to enable the creation and maintenance of the linked relationships between the Incident and associated Problem / Known Error Record(s)? --
IM-11-I-003	Does the tool integrate with Request Fulfillment to enable rapid opening of a Service Request Record from an Incident Record; and to enable the creation and maintenance of the linked relationships between the Incident Record(s) and associated Service Request Record(s)? --
IM-11-I-004	Does the tool integrate with Configuration Management Databases (CMDBs) to enable rapid access to Configuration Item attribute details and relationships, and to enable the creation and maintenance of the linked relationships between the Incident Record(s) and associated Configuration Record(s)? --
IM-11-I-005	Does the tool integrate with Configuration Management Systems or CMDBs to enable the Service Desk to identify, investigate and diagnose incidents? --
IM-11-I-006	Does the tool integrate with Change Management to enable the rapid opening of a Request for Change Record (RFC) from an Incident Record; and to enable the creation and maintenance of the linked relationships between the Incident Record(s) and associated RFCs? --
IM-11-I-007	Does the tool enable the creation and maintenance of "caused by" linked relationships between Incident Record(s) and associated RFCs? For example: recording incidents which are caused by changes --
IM-11-I-008	Does the tool integrate with Service Level Management to monitor and track incident response time and resolution time based on priority and / or service levels? --