IT Service Continuity Management PinkVERIFY™

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

IT Service Continuity Management PinkVERIFY™

ITSCM	Core Criteria
ITSCM-11-C-001	Does the tool support Business Impact Analysis by employing “what if” scenario techniques to illustrate conditions and impact of a service disruption on the organization, users, and other services?
ITSCM-11-C-002	Does the tool support Business Impact Analysis by enabling a service, system and component to be designated as business critical and include a business recovery priority code, minimum acceptable service level, recovery time requirements and support staff requirements?
ITSCM-11-C-003	Does the tool have the ability to view or sort the list of services by business criticality?
ITSCM-11-C-004	Does the tool have the ability to provide a list of “critical” contacts, back-ups and contact information which are required to deliver associated critical services?
ITSCM-11-C-005	Does the tool have the ability to provide a list of the critical services and / or Vital Business Functions with their associated recovery options?
ITSCM-11-C-006	Does the tool have the ability to display in a graphical format an estimate of the loss of service impact over a defined time period?
ITSCM-11-C-007	Does the tool support risk analysis activities to identify alternative routing and set-up options?
ITSCM-11-C-008	Does the tool have the ability to provide test, forecast and predictive reports?

IT Service Continuity Management PinkVERIFY™

ITSCM	Core Criteria
ITSCM-11-C-009	Does the tool enable resource assignment and notification for the testing and activating of Service Continuity and Disaster Recovery activity workflows?
ITSCM-11-C-010	Does the tool support the development of a detailed recovery workflow for Service Continuity and Disaster Recovery activities?
ITSCM-11-C-011	Does the tool facilitate the development of business rules and workflows to support the distribution of Service Continuity plans and documents to key resources?
ITSCM-11-C-012	Does the tool enable a Service Continuity / Disaster Recovery workflow override of normal workflow activities?
ITSCM-11-C-013	Does the tool enable a Service Continuity / Disaster Recovery hierarchical escalation and notification override of normal hierarchical escalation?
ITSCM-11-C-014	Does the tool facilitate the ability to manage and control changes to Service Continuity documentation such as plans, policies, requirements and procedures?

IT Service Continuity Management PinkVERIFY™

ITSCM	Integration Criteria
ITSCM-11-I-001	Does the tool integrate with Knowledge Management - knowledge databases to support controlled access to criteria to invoke ITSCM plans and to service recovery procedures and scripts? ----------
ITSCM-11-I-002	Does the tool integrate with Service Level Management to track business process / service criticality, time period criticality (e.g. time of day / week / month / year when disruption would be most severe), and service level recovery targets? ----------
ITSCM-11-I-003	Does the tool integrate with Configuration Management Databases (CMDBs) to enable rapid access to Configuration Item attribute details and relationships, which include IT Service Continuity and Recovery requirements? ----------
ITSCM-11-I-004	Does the tool integrate with Configuration Management Systems and CMDBs to enable a structured table or graphical representation of Configuration Items in a current configuration, in a minimum acceptable configuration, and in a disruption impact configuration including customers / users, facilities, services, systems and components? ----------
ITSCM-11-I-005	Does the tool integrate with Change Management to ensure changes to the IT Service Continuity Plan and scheduling of the IT Service Continuity plan tests are under Change Management control? ----------
ITSCM-11-I-006	Does the tool integrate with Incident Management to enable the escalation of incidents to major incident or “disaster / crisis” status? ----------
ITSCM-11-I-007	Does the tool integrate with Availability Management for risk assessment and risk response activities to optimize risk mitigation? ----------

IT Service Continuity Management PinkVERIFY™

ITSCM	Integration Criteria
ITSCM-11-I-008	Does the tool integrate with Capacity Management to identify and enable sufficient resource capacity / requirements? For example: server capacity ----------