MANAGED VULNERABILITY ASSESSMENT SERVICE

SERVICE DESCRIPTION SD103

DOCUMENT CONTROL

Version	Completed by	Date
2.0	Theo Jarvis	01 November 2023
2.1	Theo Jarvis	05 November 2024
2.2	Theo Jarvis	30 July 2025

The version history has been recorded and archived and is available upon request should these be required.

PREPARED BY

Name	Job title
Theo Jarvis	Service Development Programme Manager

CONTENTS

1. SERVICE OVERVIEW

All bold and capitalised terms used throughout this Service Description are described in the Glossary and definition of terms

1.1 SERVICE SUMMARY

The Managed Vulnerability Assessment Service is provided directly by Softcat. The Service provides Customers with easy-to-understand dashboards, including simple risk scores for their internal and external vulnerabilities and the severity of these vulnerabilities.

The Service is a network and agent scanning solution for identifying vulnerabilities that does not include remediation activity itself. Whilst Softcat can Support Customers to implement their Get-Well plan through technology, Professional Services, and advisory services, these would form a separate project and would be chargeable as additional work. Customers of the Cyber Assessment Service should contact their Account Manager and/or Service Manager with any queries.

This Service is delivered in four (4) phases listed below. More details of these phases are described within Section 2.2 of this document.

- Design, planning and readiness.
- Implementation, configuration and enablement.
- Documentation and coordination.
- Monitoring and Support.

The Service comprises:

- 24x7x365 access to log Support Cases **("Softcat Support")**
- Deployment and on-going Support of the Tenable Platform **("Tenable Platform")**
- A Vulnerability scan of assets on an agreed frequency **("Vulnerability Assessment")**
- Executive and technical dashboards and feedback on recommended actions **("Assessment Dashboard")**
- Configuration of supported integrations with the Platform **("Integrations")**
- Access to an individual scanning tenant, and threat intelligence portal. **("Threat Intelligence")**
- Creation of the configuration settings for the Agent set up **("Agent Set Up")**
- A point of contact and escalation **("Service Delivery Associate")**

Together, the above comprise the "Managed Vulnerability Assessment Service", referred to as the "Service" within this document.

The Service is delivered in accordance with the following ISO standards:

- ISO 20000
- ISO 27001
- ISO 9001
- ISO 22301

Unless otherwise stated in the Work Order, and in addition to any terms set out in this Service Description, the following applies to the delivery of the Service set out in this Service Description:

Softcat Terms and Conditions: T&Cs
The Data Processing Agreement: DPA

1.2 SERVICE FEATURE TABLE

Managed Vulnerability Assessment Service [1]	
Softcat Support	
Log Support Cases 24x7x365 [2]	✓
Online Support portal to track and log calls	✓
Up to ten (10) authorised contacts	✓
P1 response Service Level	✓
Tenable Platform	
Deployment and configuration of the Platform	✓
Technical Support of the Platform	✓
Create up to twelve (12) users [3]	✓
Create up to eight (8) access groups [3]	✓
Vulnerability Assessment	
Create up to twelve (12) discovery scans for predetermined subnets [3]	✓
Create up to sixteen (16) Windows and/or Linux credentialed scans for predetermined subnets [3]	✓
Create four (4) CIS ("Centre for Internet Security") compliance scans based upon four (4) benchmarks [3]	✓
Schedule and carry out Vulnerability assessments	✓
Network Scanning of external and/or internal networks	✓
Agent scanning for more in-depth internal scans	✓
Monthly assessments	✓
Assessment Dashboard [4]	
Optional consultancy review of scan data and dashboards	✓
Recommended next steps	✓
Creation of up to sixteen (16) dashboard views [3]	✓
Create up to twelve (12) tags [3]	✓
Create up to sixteen (16) saved searches [3]	✓
Integrations	
Up to three (3) out of the box integrations included as part of deployment [3]	✓
Additional integrations [5]	Optional [5]
Threat Intelligence	
Risk-based Vulnerability management dashboards	✓

Agent Set Up [6]	
Setting up of Agents	✓
Service Delivery Associate	
Contact and escalation	✓

[1] For the Managed Vulnerability Assessment Service, the Service is priced according to the total number of internal and external assets scanned, which will be confirmed on the Work Order.

[2] Requests are acted upon within contracted coverage hours, as confirmed in the Work Order.

[3] The parameters stated are applicable to the initial onboarding activity; additions can be handled in life of the Service and will be handled where applicable through a request.

[4] The Consultant will agree the delivery method (by phone or in person) and attendees with the Customer prior to its delivery. For some services all reports are delivered by phone; a list of such services is available on request.

[5] "Optional" and "Optional Add-On" means a chargeable extra. Where a chargeable extra is chosen by a Customer, this is confirmed on the Work Order.

[6] Sensors include Nessus Agents, Nessus Scanners and Nessus Network Monitor.

2. SERVICE DETAIL

2.1 SOFTCAT SUPPORT

Authorised Customer Contacts have access to Softcat Support around the clock and on any day of the year ("24x7x365")[1].

Customer Contacts should raise a Case primarily via the Support portal, where the Case type will be assessed, defined and communicated and the priority level will be agreed with the Customer. Where Service Levels apply to the management of a Case, these will be confirmed on the Work Order. For any Case which the Customer believes to be urgent, the Customer Contact must report to Softcat by telephone.

[1] Requests are acted upon within contracted coverage hours, as confirmed in the Work Order.

2.2 TENABLE PLATFORM

Softcat will deploy and configure the Tenable Platform as part of a remote engagement. The Service will then go on to include technical Support for the Tenable Platform.

Softcat will determine the scope of the Customer's implementation, based on network specifics and visibility goals. From this a list of pre-requisites will be identified to create a schedule of the engagement.

Softcat will install and configure the Tenable solution in the Customer's environment for the included number of assets, while aligning with best practices. This will be completed as a remote engagement.

Additional integrations can be set up as Optional add-ons; the current list of available integrations can be found via the Tenable documentation site

This Service comprises four (4) core phases detailed below.

2.2.1 DESIGN, PLANNING AND READINESS

- **Design and planning** - Softcat will perform a design and architecture workshop with the Customer to agree on a solution design according to Tenable's best practice and recommendations.
- **Readiness exercise** – Softcat will review and validate the solution design, prerequisites and specifications before implementation and enablement commences.

2.2.2 IMPLEMENTATION, CONFIGURATION AND ENABLEMENT

- **Install sensors and configure** - sensors will be installed and configured based on the Customer's requirements and will be implemented following Tenable's best practices.
- **Validate operational capabilities** – the Platform will be validated end-to-end for scanning and other operational capabilities.
- **Enablement** – Softcat will provide an enablement session guiding the Customer through Tenable's best practices for Vulnerability management.

2.2.3 DOCUMENTATION AND COORDINATION

- **Deliverable documents** -Softcat will provide documentation of the Customer's specific Tenable product configuration after installation for future reference, including design and architecture workshop deliverables.

- **Coordination** - Softcat will provide ongoing project coordination and updates throughout the project.

2.2.4 MONITORING & SUPPORT

- **Scan success** – Softcat will monitor the Platform for the success of scans and where required Softcat will work with the Customer to remediate issues preventing a scan from completing.
- **Support** - Softcat will handle the ongoing creation or modification of scans as requested by the Customer, while providing ongoing Support of the deployed Platform through Softcat's experienced security operations team.

2.2.5 PLATFORM ROLES

The following table outlines the pre-defined user roles available in the Tenable Platform. As part of the onboarding and deployment of the Platform the Customer can request up to twelve (12) users to be created; the table below highlights the role names available. A detailed breakdown of the roles and the associated permissions per area of the Platform can be found here: Tenable-Provided Role Privileges (Tenable.io).

Role name	Description	Available
Tenable.io Vulnerability management user roles		
Basic	Can only manage their user profile, view scan results (including dashboards), and move shared scans to different folders.	✓
Scan operator	Can create and run scans, but may only use existing user-defined scan templates that were created by a standard user or higher. They can create user target groups for use in scans.	✓
Standard	In addition to scan operator privileges, can view user-defined scan templates that were created by a scan manager user or higher.	[7]
Scan manager	In addition to standard user privileges, can configure scan settings and create, configure, use, and delete user-defined scan templates. They can also manage scanners, agents, and exclusions.	[7]
Administrator	Has all permissions and privileges, is responsible for setting up the account, and knows the organisation's architecture. They can create groups to organise different business units and add and manage users on the account.	[7]
Tenable.io web application scanning user roles		
Basic	Can only manage their user profile and view scan results, including dashboards.	✓
Scan operator	Can create and run web application scans, but may only use existing user-defined scan templates that were created by a standard user or higher.	✓
Standard	In addition to scan operator privileges, can view user-defined scan templates that were created by a scan manager user or higher.	[7]
Scan manager	In addition to standard user privileges, can configure scan settings and create, configure, use, and delete user-defined scan templates.	[7]
Administrator	Has all permissions and privileges, is responsible for setting up the account, and knows the organisation's architecture. They can create groups to organise different business units, and add and manage users on the account.	[7]

Tenable.io container security user roles		
Basic	Limited to viewing, searching, and filtering container security data.	✓
Scan operator	Can import, manage, and delete images and image repositories. They can also view policies, but may only use policies set by a scan manager user or higher.	✓
Standard	Can import, manage, and delete images and image repositories. They can also view policies, but may only use policies set by a scan manager user or higher.	[7]
Scan manager	In addition to scan operator privileges, can create, manage, and enforce policies.	[7]
Administrator	Has all permissions and privileges, is responsible for setting up the account, adding and managing users, and configuring connections to registries.	[7]

[7] These roles are reserved for Softcat users providing the Service only.

2.3 VULNERABILITY ASSESSMENT

The Vulnerability Assessment is a scheduled scan of the Customer's environment, where Vulnerabilities are discovered and reported upon.

The Vulnerability Assessment may include both internal and external asset scanning, which can be achieved using Agent-based host scans, appliance-based network scans, or a mixture of the two. The breakdown will be confirmed on the Work Order.

Softcat and the Customer will agree the type of scans and the associated cost, including the number of agreed assets. This will be confirmed on the Work Order [8].

A license is consumed when an asset is assessed for vulnerabilities, using any of the methods described. The asset retains the license for repeated scanning until it has been inactive for ninety (90) days, at which point the license is recovered. Discovery scans may also be carried out to identify all assets on a network; discovery scans do not consume a license.

For Agent-based scanning the Customer will be required to deploy Agents to the identified endpoints within their organisation. The Customer can work with Softcat to adjust the number of Agents or move these licences at any point during the Service.

Scan data is only used for the point-in-time assessment at the agreed scheduled window and is not collected or processed for other purposes. Scan data is retained for fifteen (15) months in the Platform and can be exported in various formats for longer term storage.

The Service includes regularly scheduled scans; the results will be available on the Customer's dashboard, where they can customise reporting. The results will also automatically feed into their organisational intelligence Platform.

The Customer will be able to run as many scans as they wish through their organisational tenant.

Where appropriate, ad-hoc scanning can be initiated outside of already scheduled scans. These scenarios are typically driven through threat intelligence.

[8] For the Managed Vulnerability Assessment Service, the Service is priced according to the total number of internal and external assets scanned, which will be confirmed on the Work Order.

2.4 ASSESSMENT DASHBOARD

Softcat will aggregate the results of the Customer's assessment(s) to produce an executive overview and dashboard of the Customer's security posture. The dashboard will be available to the Customer via the Vulnerability scanning tenant made available to the Customer during onboarding. Softcat will initially create up to sixteen (16) [9] dashboard views using custom widgets or templates.

As part of the creation of the dashboard views, Softcat will initially create up to twelve (12) [9] tags which will help organise assets for dashboards, reporting, viewing and permissions.

Within the dashboard and reporting section of the portal Customers will have the ability to select pre-defined searches for common reporting queries for easy access to data. Softcat will initially create up to sixteen (16) [9] searches.

Optionally, a review workshop will be held with the Customer covering:

- High level summary of findings
- Any assets that did not scan during the scheduled scan window
- Get-Well recommendations

Softcat will contact the Customer for a follow-up call to allow the Customer to ask questions and to suggest recommended next steps. If the Customer would like Softcat to provide assistance in remediation, a quote will be provided for the identified technology and/or services relating to this.

[9] The parameters stated are applicable to the initial onboarding activity; additions can be handled in life of the Service and will be handled where applicable through a request.

2.5 INTEGRATIONS

Up to three (3) out-of-the-box ("OOTB") integrations from the following list can be included as part of the initial deployment and are Supported within the Service:

- SAML – SAML 2.0 configurations only.
- Cloud Connectors:
    - Amazon Web Services - https://docs.tenable.com/integrations/AWS/Content/Welcome.htm
    - Azure - https://docs.tenable.com/integrations/Microsoft/Azure/Content/welcome.htm
    - Google Cloud Platform - https://docs.tenable.com/integrations/GCP/Content/AuditGCPio.htm
- ServiceNow - Configuration Management Database ("CMDB") - https://docs.tenable.com/integrations/ServiceNow/Content/Welcome.htm

All other third party integrations are the responsibility of the Customer.

Further out of the box integrations can be included as an Optional Add-on. Where optional extras and or optional add-ons are chosen by a Customer, this is confirmed on the Work Order.

2.6 THREAT INTELLIGENCE

The Customer will have their own risk-based Vulnerability management dashboards which will provide contextualised information by assessing the risk associated with technical vulnerabilities – known as "CVE" (common vulnerabilities and exposures) that an organisation has on its internet-facing infrastructure, and contextualising this with bespoke threat intelligence at an organisational and industry level.

Periodic reports are not provided from the Vulnerability management dashboard, instead, the information in the dashboard is continually updated which can be accessed at any time by the Customer.

The Service will use intelligence reports on how any CVE is being exploited by hackers, together with intelligence on the severity of its exploitation, to prioritise which CVEs are currently the most important to focus on.

The Threat Intelligence Platform will also deploy machine learning which predicts which CVEs are likely to be exploited in the future, so that Customers can stop cyber risk before it happens.

2.7 AGENT SET UP

The Customer is responsible for deploying Agents, where these are used, in accordance with the type of scanning confirmed in the Work Order.

Agents are best deployed to user endpoints (desktops, laptops) and especially devices which may be portable or reside outside the corporate network. Agents may also be deployed to servers; however, these should be monitored for performance impact during scan windows. While this risk is low, there may be an impact on highly utilised assets.

Where required, the Customer may request assistance with Agent set up by contacting their Account Manager for a Professional Services quote: this is available as a chargeable option.

To keep the Agents up to date, software updates are performed automatically by the Agent as and when needed.

2.8 SERVICE DELIVERY ASSOCIATE

The Service Delivery Management team is a point of contact and escalation for any services detailed within the Work Order. The Service Delivery Management Team is available during standard UK Working Hours.

A named Service Delivery Manager, service report and service reviews are available for an additional charge. Customers can request this by contacting their Softcat Account Manager. This will then be detailed in the Work Order.

3. SERVICE LEVELS

3.1 SOFTCAT SUPPORT

Softcat offers a response metric, which is Softcat's commitment to raise a Case within a given time from when the request is made to Softcat Support.

In the table below, the Service Level target is the percentage of requests responded to within the response Metric, for example: 95% of Cases logged as a P1 are responded to within fifteen (15) minutes.

The Response Service Level for Cases is shown in the table below:

Priority	Description	Service coverage hours	Response metric	Service Level target
Priority 1 (P1)	Business impacted or imminent impact expected within four (4) hours; full Customer Site outage; a business-critical system or Supported Product is not working; Customer cannot perform business critical functions; loss of revenue; risk of severe reputational damage; all End-Users unable to perform business critical roles.	24/7	<15 Minutes	95%
Priority 2 (P2)	Partial Customer Site outage; loss of redundancy; a non-business-critical system or Supported Product is down; Customer experiencing a high degradation in Service; risk to revenue generation; multiple End-Users unable to perform business critical roles.	24/7	<30 Minutes	95%
Priority 3 (P3)	Single End-User issue that prevents them from performing business-critical elements of their role; multiple End-Users affected by an identical issue that does not prevent them from performing their roles; reduction in redundancy for business-critical systems.	Mon-Fri 09:00 -18:00 (ex. bank holidays)	<4 Hours	95%
Priority 4 (P4)	Single user issue that does not prevent them from performing their role or a critical operation; reduction in redundancy for non-business critical systems.	Mon-Fri 09:00 -18:00 (ex. bank holidays)	<4 Hours	95%

Category type	Description	Service coverage hours	Response metric	Service Level target
Request [10]	Request – Working Hours only	M-F 09:00 – 18:00 (ex. Bank Holidays)	<4 Hours	95%

10 Unless specified otherwise, any requests are subject to the above metrics.

4. CUSTOMER RESPONSIBILITIES

4.1 SOFTCAT SUPPORT

a. The Customer should ensure that Customer Contacts are skilled in or knowledgeable of the Customer's Operating Environment, have sufficient access rights, and are of a sufficient proficiency to apply the recommendations that are provided as part of this Service.
b. Prior to Service commencement the customer should provide:
    i. The Customer's admin on Softcat's ticketing platform must maintain at least two (2) Customer Contacts for the purposes of Support and continuity; and
    ii. Any relevant Key Information e.g. models, serials, tenancy, Subscriptions.
c. When raising a Case the Customer Contact should provide, when requested by Softcat:
    i. Valid and applicable serial numbers for the affected Supported Product(s).
    ii. Reasonable visibility of system logs, configuration files and error messages.
    iii. Details of Software versions and configuration.
    iv. A description of the symptoms and other devices or services impacted.
    v. Confirmation of when the issue first occurred and if it has occurred before (where possible provide previous Case references).
    vi. Details of any recent changes or projects implemented prior to the issue being raised.
    vii. Details of all Fixes, configuration amendments and updates already performed to attempt to resolve the issue prior to raising the Case.
    viii. To what extent the issue is affecting operation of the Customer's business.
    ix. The number of End-Users impacted and their location.
    x. Contact details of the Customer Contact.
    xi. Details of any trouble-shooting steps already undertaken
d. Implementation of best practice recommendations advised by Softcat.
e. Direct Support for End-Users. Customers should ensure the Customer's staff are trained to refer all Cases to the Customer Contact in the first instance, and not permit persons other than a Customer Contact to approach Softcat to register Cases.

4.2 TENABLE PLATFORM

a. Ensuring the required Tenable software is downloaded and accessible to Softcat. The downloadable file can be found on the following link:
b. Customer has a valid administrative username and passwords for the software applicable.
c. Network topology diagrams and information to be provided as part of the Platform deployment.
d. Customer SAML ("Security Assertion Markup Language") configuration file (if applicable).
e. Provide relevant access for Softcat to carry out the deployment of the Platform remotely.
f. Ensuring that valid Customer licences for all relevant Tenable software are in place.

4.3 VULNERABILITY ASSESSMENT

4.3.1 AGENT SCANNING

a. In the event of a failing scan or Agent, Softcat are available to advise on possible causes, but the main responsibility is on the Customer to investigate the root cause.

b. Ensure all technical pre-requisites are met for Agent scanning prior to onboarding starting. The technical pre-requisites for Agent scanning are available through the following link: https://www.softcat.com/documents/technical-prereq.pdf
c. The responsibility for the installation, management and removal of an Agent is solely the Customer's responsibility; Softcat can advise and make recommendations where appropriate. It is important to note that until the Agent is removed it will continue to update and report back information.
d. Ensure that agents can communicate to https://cloud.tenable.com using port TCP/443. They are proxy aware and will use the machine's defined proxy if configured.

4.3.2 EXTERNAL IP ADDRESSES – NETWORK SCANNING

(i.e. as if an external Threat Actor)

a. Completing all forms and questionnaires that provide Key Information for the Vulnerability Assessment (and/or providing other information that Softcat deems necessary to supply the Service).
b. Configuring scanner access to all external IP/hosts in scope (no privileges required).
c. Ensuring that suitable and maintained internet connectivity is available to enable the scanners to communicate with the host Platform.
d. Signing and returning an "Authority to Test Form" form.

4.3.3 INTERNAL IP ADDRESSES – NETWORK SCANNING

a. Completing all forms and questionnaires that provide Key Information for the Vulnerability Assessment (and/or providing other information that Softcat deems necessary to supply the Service).
b. Ensuring that suitable and maintained internet connectivity is available to enable the scanners to communicate with the host Platform.
c. Signing and returning an "Authority to Test Form" form.
d. Enabling SSH (secure shell) on *.nix systems (e.g. Linux, Mac etc) in scope to permit fully authenticated scanning.
e. Configuring scanner access to all hosts in scope using a domain account with local admin privileges (enforced by group policy or any other appropriate means).
f. Installing the virtual scanning appliance on an appropriate virtualisation Platform (Softcat will provide a link from which the scanner can be downloaded).
g. Ensuring that the Customer's network and systems comply with the relevant specifications provided by Softcat. When required Softcat will contact the Customer if the specifications change from those originally implemented from time to time (where appropriate).
h. Ensure that scanners can communicate to https://cloud.tenable.com using port TCP/443. They can be configured with a proxy server address if required.

Please note: For Customers who consume both internal and external Network Scanning, the merger of both point (b) in external and point (e) in internal is required which becomes the following:

Configuring scanner access to all external IP/hosts in scope (no privileges required) and all hosts in scope using a domain account with local admin privileges (enforced by group policy or any other appropriate means).

5. NOTABLE EXCLUSIONS

5.0 SOFTCAT SUPPORT

At an additional cost the Customer can request project and design work, including Professional Services by contacting their Account Manager for a quote.

5.1 VULNERABILITY ASSESSMENT

a. The Service does not include remediation of security risks or issues identified, or implementation of Get-Well recommendations following the Vulnerability Assessment.
b. Softcat can Support remediation activity, but this would form a separate project and would be chargeable as additional work. Customers of the Cyber Assessment Service should contact their Account Manager and/or Service Manager with any queries.
c. Softcat does not guarantee that the software will be uninterrupted, error-free, or will meet the Customer's requirements.

5.2 INTEGRATIONS

The Service does not include Support for third party integrations - these are the responsibility of the Customer.

5.3 AGENT SETUP

The Customer is responsible for deploying Agents, where these are used, in accordance with the type of scanning confirmed in the Work Order.

6. SERVICE BILLING AND CONTRACT TERM

The billing frequency, and the Initial Term will be agreed with the Customer and confirmed in the Work Order.

Following the acceptance of the Contract, the Onboarding Period will begin. This is the period in which any pre-requisite dependencies for the Service are completed, for example the collation of the Key Information. If there is a requirement for any additional assessment of the Customer's Operating Environment following Softcat's receipt of the Key Information, this will be undertaken during the Onboarding Period.

The Activation Date for the Service will be the day on which the Onboarding Period ends.

Where any Key Information requested by Softcat is outstanding at the Activation Date, Softcat's obligation to deliver the Service shall be subject to reasonable endeavours.

Unless it is stated on the Work Order that the Service will not Auto-Renew[11], or written notice is given by either Party to the other of its intention not to renew the Contract at least ninety (90) Working Days before the expiry of the Initial Term or any subsequent Renewal Term, the Service at the expiry of the Initial Term or any subsequent Renewal Term will be renewed automatically for a further term of twelve (12) months on the same Terms and Conditions as detailed within the Contract.

[11] The state of Auto-Renew will be reflected in the 'service specific section' of the Work Order.

7. TERMS AND CONDITIONS

7.1 OVERVIEW OF TERMS AND CONDITIONS

The delivery of the Service to the Customer shall be governed by Softcat's Terms and Conditions and the Work Order. Softcat's Terms and Conditions and the other agreements listed below.

Softcat's Terms and Conditions: https://www.softcat.com/terms-and-conditions-uk/

Capitalised terms in this document shall have the meaning set out here: https://www.softcat.com/documents/glossary-and-definition-of-terms.pdf, unless they are defined in the Terms and Conditions. In the event of any discrepancy or conflict between the Terms and Conditions and this Service Description, this Service Description shall take precedence.

For the purposes of the relevant Work Order and this Service Description, the term "Service" shall be interpreted as an "Annuity Service".

7.2 DATA PROCESSING AGREEMENT

By signing the Work Order, the Customer agrees to the Data Processing Agreement (DPA), available here: https://www.softcat.com/documents/Softcat-Services-DPA2019.pdf

The DPA shall be a separate agreement to the Contract (and no liability shall arise (i) under this Contract in respect of the Processing, or (ii) under the Processing Agreement in respect of the remaining aspects of providing or using the Annuity Services).

7.3 ADDITIONAL TERMS ("CONTRACT ADDENDUM")

These Contract Addendum Additional Terms shall apply to the delivery by Softcat to the Customer of the Service and Softcat's Terms and Conditions shall apply as amended by this Contract Addendum.

7.3.1 VULNERABILITY ASSESSMENT

The Vulnerability Assessment scoring provided by Softcat is based entirely on the information that the Customer provides. Softcat shall not be liable for scoring which is erroneous or incomplete because the Customer has not supplied complete or correct information, including any information which may be relevant, but which may have not been specifically requested by Softcat.

The Customer represents and warrants that it has the appropriate authorisations from the owner of the networks, systems, IP addresses, assets, and/or hardware on which it deploys the Software, or which it targets, scans, monitors, or tests with the Software.

7.3.2 ASSESSMENT DASHBOARD

The Dashboard and Get-Well recommendations provided by Softcat are based entirely on the information that the Customer provides. Softcat shall not be liable for Dashboards or Get-Well recommendations which are erroneous or incomplete because the Customer has not supplied complete or correct information, including any information which may be relevant, but which may have not been specifically requested by Softcat.

The use of the Service or implementation of any Get-Well plan or recommendations does not guarantee, promise, or warrant that the Customer or its systems will be immune to attack or unauthorised access. The reliance that the Customer places on the outcome or use of the Service is solely at the Customer's risk.

The title to and the Intellectual Property Rights in the Service does not pass to the Customer. The Customer is licensed to use the Service in accordance with this Service Description and any EULA applicable to the Service, and by entering into a Contract to use the Annuity Service, the Customer agrees to enter into and comply with the terms of any such EULA(s).

7.4 ISO STANDARDS

The Service is fully compliant with the following ISO standards, ensuring the highest levels of quality, security and continuity:

- **ISO 20000** – Focuses on IT service management, ensuring that service are aligned with business needs and adhere to best practices. By following ISO 20000, the Service guarantees that the IT service management processes are efficient, effective, and continually improving to meet Customer evolving demands.
- **ISO 27001** – Dedicated to information security management systems. It helps organisations protect data and manage security risks systematically. Compliance with ISO 27001 ensures that robust security measures are in place to safeguard sensitive information, mitigate risks and respond promptly to security Incidents.
- **ISO 9001** – Addresses quality management systems. It ensures that the Service consistently meets Customer requirements and strives for continuous improvement. By adhering to ISO 9001, the Service demonstrates commitment to delivering high-quality services that enhance Customer satisfaction and operational excellence.
- **ISO 22301** – For business continuity management systems, helping organisations prepare for a respond to disruptive Incidents. Compliance with ISO 22301 ensures that the Service has comprehensive plans and procedures in place to maintain business operations during unforeseen events, thereby minimising downtime and ensuring service continuity.

SOFTCAT PLC, FIELDHOUSE LANE, MARLOW, BUCKS, SL7 1LW