BT Master Services Agreement
Secure Networking Quickstart and Security Assurance Services Annex to the Professional Services Schedule

1 Service Description

BT Security Assurance Services: Secure Networking Quickstart Service (SQNS), (“the Service”), provides the Customer with information to put in place effective network security. The following options are available:

1.1 Level One

1.1.1 Remote Customer Workshop

BT will work with the Customer to identify the key areas of its environment that require Security Assurance Services. The outcome will enable BT to create a high level security assessment strategy taking into account the Customer’s business objectives, asset criticality and long-term security.

The workshop comprises an interactive question and answer session, normally delivered by teleconference unless otherwise agreed, to identify the Customer’s security objectives for the short to medium term. A security effectiveness register is used to quantify the potential risk posed to the Customer. BT may also provide structured questionnaires which the Customer should complete and return no more than one week after the initial teleconference.

BT will review the completed the questionnaires and deliver a written statement of work (“SOW”) with recommendations for a Customer security assessment strategy.

1.1.2 Remote Cyber Security Assessment

This assessment uses a combination of BT developed technology and that of market leading commercial security software providers. BT’s security consultants regularly monitor current threats, the latest hacking tools and exploits, which combined with intelligence gathering helps to identify what blended threats may put the Customer’s business at risk. The report is tailored to the Customer’s technical risk model. The resulting model enables BT to recommend developments to the Customer’s security strategy. Duration is usually 3 (three) days but is subject to the size and complexity of the Customer’s network. The duration will be agreed in advance and be stated on the Order.

The assessment comprises 3 steps:

a) A network mapping and intelligence gathering exercise, that will help to visualise and provide a map of which Customer devices and assets are visible from the Internet. BT’s aim is to identify known and potentially unknown devices on the Customer’s network and assess the network’s segregation to make sure external boundaries are protecting the network adequately and that no internal routes or devices are exposed to the Internet. In addition depending on the engagement BT may also look for information that could help an adversary mount an attack.

b) A Vulnerability Assessment in which BT will use the results from the network mapping exercise to help drive a Vulnerability Assessment of the discovered devices and the Customer’s assets. This will help to identify any critical vulnerabilities in the Customer’s Internet facing system or network. BT will provide an executive summary, and written recommendations that the Customer may consider implementing to improve security.

c) A Risk Modelling exercise in which BT takes information from the previous steps and attempts to model the risks to enable the Customer to visualise its network, verify access policy compliance and routing rules as well as discovering root causes of violations. BT will help the Customer to understand and analyse the business impact of threats, as well as the ability to simulate attacks on the Customer’s network. BT will advise the Customer on remediation alternatives.

BT will deliver a written report outlining the findings and priority areas identified for further action. BT will review the report with the Customer via web conference or face-to-face meeting.

1.2 Level Two. Quick Start Secure Networking Assessment.

The BT Secure Networking Quick Start is made up of a series of Quick Start modules that enable BT to establish an understanding of the Customer’s network security. The Assessment duration is subject to the size and complexity of the Customer’s network, and can vary from approximately 2 (two) to 3 (three) weeks depending on the modules ordered. Level Two modules can be ordered without a Level One assessment if the Customer has an immediate need for any of the work packages. Usually the required modules will be identified from the Level One workshop results. Not all modules are available in all locations.

BT will make an initial assessment of the Customer’s network security, via a Level 1 workshop and the Customer’s completed penetration and/or application testing questionnaires. The security assessment will then be performed using the modules stated on the Order.

On completion of the Modules ordered, BT will present an executive summary and a concise technical report detailing any findings and recommendations for improvement, details of how the Customer’s network security compares to best security practice, list any vulnerabilities found, provide test results, and make recommendations for remedial action.

1.2.1 (Module 1) Network Mapping

This is a network mapping exercise that confirms the Customer’s Internet presence and provides a map of the Customer’s devices which are visible from the Internet. The exercise aims to identify known and potential unknown devices on the Customer’s network and will assess the network’s segregation to make sure external boundaries are protecting the network.

1.2.2 (Module 2) Intelligence Gathering and Blended Attacks

BT will study publicly available information about the Customer to establish any potential threats.

1.2.3 (Module 3) Web Application Testing

This testing identifies and investigates the prioritisation of vulnerabilities found in thin client (web browser) and thick client (java) applications, including front end and back end systems. Activities range from injections to cross site scripting to decompiling code and HTML proxy manipulation. Tests are performed with in-depth application scanning tools and thorough manual checks.

1.2.4 (Module 4) Penetration Testing

Penetration testing is similar to the vulnerability assessment in Level One. In this module BT will explore in greater depth and exploit the vulnerabilities to gain access to the Customer’s system.

1.2.5 (Module 5) Firewall Rulebase Assessment

This identifies areas of weakness, such as insecure protocols, poor change control and inefficient rule order.

1.2.6 (Module 6) Email Application Assessment

BT will provide a time limited assessment of the Customer’s email traffic to determine the levels of viruses, SPAM, and general content control issues within the Customer’s email.

1.2.7 (Module 7) Voice & VOIP Audit

BT will provide a security assessment and a real-time audit of the Customer’s VOIP applications. The scope will be agreed before testing starts.

1.2.8 (Module 8) Secure Code Review

BT will undertake a secure code review of the Customer's applications, which together with Penetration and Application testing ensures that deployed applications can undergo an extra level of security evaluation. This ensures that web applications have the level of assurance required to handle financial and personal information.

1.2.9 (Module 9) Database Security Testing

BT will undertake Penetration testing of key Database assets to ensure that the risk posture is understood and ensure that confidentiality, integrity and availability is in line with the Customer's organisational policy.

1.2.10 (Module 10) Wireless Enterprise Audit

BT will evaluate the Customer's existing wireless network security and identify weaknesses and vulnerabilities specific to the wireless infrastructure. BT will recommend technical and procedural changes that may increase wireless infrastructure security.

1.2.11 (Module 11) Mobile Worker Assessment

BT will take a risk based approach in reviewing the security of remote access into the Customer's network infrastructure. Remote access and VPN testing will be performed. BT will attempt to breach a mobile worker's laptop and its access controls to see if Customer data can be accessed. In addition mobile application testing can be ordered for a range of mobile devices.

2 Minimum Period of Service

2.1 The Minimum Period of Service for the Level One Quick Start Customer Workshop is one (1) day, unless stated otherwise on the Order.

2.2 The Minimum Period of Service for the Level One Quick Start Secure Technical Risk Assessment is three (3) days, unless stated otherwise on the Order.

2.3 The Minimum Period of Service for the Level Two Quick Start Secure Network Assessment is two weeks, unless stated otherwise on the Order.

2.4 If the scope and/or duration of the Level Two Modules ordered extend beyond the boundary of standard Level Two services then BT will work with the Customer to redefine the scope of the Service and will provide a quote for the revised scope.

2.5 If the Customer orders repeat health checks (penetration testing and web application testing) over a twelve (12) Month period the Minimum Period of Service for each test will three (3) days, and the average quarterly review takes two to three weeks, depending on the size and complexity of the network.

3 BT's Responsibilities

BT shall perform the Service in a professional manner commensurate with good practice for work of this nature.

4 The Customer's Responsibilities

4.1 The Customer will provide BT with all the information reasonably required by BT otherwise BT may not be able to provide the Service. This will include, but not be limited to, information on the Customer's network configuration and security policies such as up-to-date network diagrams, security policy documents, electronic or paper copy of the current firewall rule base, and IP address information of firewall(s), connecting infrastructure, and servers.

4.2 The Customer will provide BT with the name(s) of the individual(s) ("Customer Contact") and all requisite contact details. The Customer Contact will be available during Business Hours and be responsible for providing assistance and information as needed by BT.

4.3 In jurisdictions where an employer is legally required to make such disclosure to its employees, it is the Customer's responsibility to:

(i) inform its employees and Users that as part of the Service being deployed by BT, the usage of any targeted applications by the Customer's employees and/or Users may be monitored and reported to the Customer by BT; and

(ii) ensure that the Customer's employees and Users have consented or will be deemed to have consented to such monitoring and reporting, if such consent is legally required, and

BT shall not be liable for any failure of the Customer to comply with this paragraph 4.3 and the Customer shall indemnify BT from and hold BT harmless against any claims or actions brought by its employees or Users against BT arising out of the delivery of Services by BT in accordance with the terms hereof.

4.4 Any Customer data captured by BT in the delivery of the Service will remain the Customer's data and BT will only process this data to the extent necessary to deliver the Service or in accordance with the instructions of the Customer. At all times both Parties will comply with their respective obligations under applicable data protection and privacy legislation.

4.5 **Penetration Testing**

4.5.1 The Customer acknowledges that penetration testing including penetration and unintentional denial of service attacks of the Customer's systems may affect the performance, operation and security of the systems. The Customer confirms that it is solely responsible for the security and integrity of its own equipment and data.

4.5.2 The Customer expressly authorises BT to access its computer systems and networks (and any programs and data held on them) to the extent reasonably required to enable BT to perform the Penetration Testing.

4.5.3 The Customer acknowledges and accepts that BT will use various proprietary penetration testing methods and such other methods as BT may, in its absolute discretion, deem appropriate, in providing the Service, to attempt to gain entry to the Customer's computer systems and networks, which may include replicating methods (whether software-based or not), applications and tools used by computer hackers and the Customer acknowledges and accepts that BT may as a result succeed in gaining access to its computer systems and networks.

4.5.4 The Customer warrants and undertakes to BT that it has the full right, power and authority, and has obtained all necessary third party consents and authorisations, to permit BT to provide Penetration Testing services and that any actions undertaken by BT in providing the Penetration Testing services in accordance with this Annex will not infringe the rights of any third party.

4.5.5 BT reserves the right to stop Penetration Testing if it has reason to suspect that the Customer has failed to obtain any such consents or authorisations. The Customer undertakes to indemnify and hold harmless BT, its directors, officers, employees and agents from and against all costs, claims, demands, expenses and liabilities of whatever nature arising out of or in connection with BT performing the Services in accordance with this Service Annex (save where those costs, claims, demands, expenses and/or liabilities arise as a direct result of BT's negligence) and to accept full responsibility for such liabilities.

4.5.6 Before testing starts the Customer shall make back up copies of all information held on the system to be tested. This information includes, but is not limited to, system data, programs, configuration files, security data (identification, authentication, access control, accounting and audit), source files and operating system configuration parameters. The Customer agrees that it may be necessary for the backups to be restored in order to return the operational system to its original state.

4.5.7 The Customer acknowledges that testing may change information stored on the system. For tests on live services BT will ensure that all tests will be confined to those which have a minimal impact on the system and no key information that could affect the live status of the service will be intentionally changed. Any minor changes made to information should be invisible to the Customer and will only be made if necessary to confirm vulnerabilities with a high level of severity that might exist within the system.

5 Personnel

BT will use security consultants from its global team depending on the assignment and consultant availability, and the Customer acknowledges that BT may perform analysis, including penetration testing remotely, that is from outside the country in which the Customer's Site(s) is located. BT's consultants will follow any specific country legislation around encryption.

6 Charges and Payment Terms

6.1 The Charges for the Service will be as stated on the Order and will become due on delivery of the report(s) detailed above and be payable in accordance with the MSA

6.2 Unless otherwise stated on the Order, Charges for the Service do not include travel expenses. The Customer agrees to pay for all travel expenses incurred by BT for performing the Service. Such expenses include commercial transportation, meals, lodging, parking, tolls and other direct expenses of travel based on actual cost to BT.

6.3 Service Delivery is completed within the Business Hours of the Site. The Customer is liable for any additional charges for Service Delivery outside of Business Hours.

6.4 If the Customer requirements change, and more time is required to provide the Service, BT reserves the right to charge additional Charges for the additional time taken.

7 Termination of Service

Except as provided for in the MSA, if the Customer terminates Service, or if BT terminates Service for breach, before the Minimum Period of Service has expired, then, the Customer agrees to pay the following:

a) All the Charges stated on the Order; and

b) BT's travel expenses incurred prior to termination.

If BT is able to re-allocate to other projects the time of the people who would have provided the Service, BT will make an adjustment (reduction) to the Charges in a) above.

8 Service Levels

There are no Service Levels associated with this Service.

9 Miscellaneous

9.1 BT hereby grants the Customer the right to use any reports, documents or other materials generated by BT hereunder, for its own internal purposes.

9.2 Subject to the Confidentiality provisions of the MSA, nothing in this Service Annex shall operate to prevent BT from making use of know-how acquired, principles learned or developed or experience gained during the performance of its obligations or otherwise in connection with this Service Annex.