BT Managed Web Application Firewall Security Service
Annex to the BT Managed Security Schedule

Contents

APPLICATION OF THIS ANNEX 2
A note on 'you' 2
WORDS DEFINED IN THE GENERAL TERMS 2
Part A – The BT Managed Web Application Firewall Security Service 2
1 Service Summary 2
2 Standard Service Components 2
3 Service Options 3
4 Service Management Boundary 3
5 Associated Services and Third Parties 4
6 Specific Terms and Conditions 4
7 Monitoring and management 6
8 Continuous improvement 10
9 IP Addresses and Domain Names 13
Part B – Service Delivery and Management 14
10 BT's Obligations 14
11 Your Obligations 14
Part C – Service Levels 18
12 Service Availability 18
13 Resiliency Restoration 19
14 Requests for Service Credits 19
Part D – Defined Terms 20
15 Defined Terms 20

APPLICATION OF THIS ANNEX

This BT Managed Web Application Firewall Security Service Annex (the "**Annex**") sets out the additional terms that will apply where BT provides you with the BT Managed Web Application Firewall Security Service. The terms of this Annex apply in addition to the terms set out in:

(a) the Schedule; and
(b) the General Terms.

A NOTE ON 'YOU'

'You' and 'your' mean the Customer.

WORDS DEFINED IN THE GENERAL TERMS

Words that are capitalised but have not been defined in this Annex have the meanings given to them in the General Terms or the Schedule.

Part A – The BT Managed Web Application Firewall Security Service

1 SERVICE SUMMARY

1.1 BT will provide you with a web application firewall service that provides a dedicated security control capability to filter, monitor and block traffic to and from a web application which is comprised of:

1.1.1 the Standard Service Components; and

1.1.2 any of the Service Options that are selected by you as set out in any applicable Order,

up to the point of the Service Management Boundary as set out in Paragraph 4 (the "**BT Managed Web Application Firewall Security Service**").

2 STANDARD SERVICE COMPONENTS

BT will provide you with all of the following standard service components ("**Standard Service Components**") in accordance with the details set out in any applicable Order:

2.1 **Security Appliances:**

2.1.1 You will select a Security Appliance in conjunction with BT, details of which will be set out in the Order.

2.1.2 BT will provide, install and commission the Security Appliance, including any hardware and Software, licensing and support agreements for the Security Appliance and will arrange for any on-Site support and remote service management. BT will provide Out of Band Access and switches, if required.

2.1.3 **High Availability (dual appliance) Solutions:**

(a) BT will configure a pair of Security Appliances on a single Site to give increased resilience against failure.
(b) This Standard Service Component may require additional switches to be included as part of the solution which will be provided by BT.
(c) BT will configure the Security Appliances as "**Active Passive**" (one Security Appliance handles the load under normal conditions, with failover to a secondary Security Appliance in the event of the primary Security Appliance failing).

2.1.4 **Monitoring:**

(a) BT will:

(i) monitor traffic passing through your Security Appliance for attacks, in accordance with the applicable signature files;
(ii) implement the agreed configuration setting, as defined by the supplier of the Software. BT will also maintain a subscription to the necessary Signature Updates, and arrange for these to be applied following issue by the supplier; and
(iii) not be responsible for evaluating these signatures beforehand.

(b) BT will advise you how the Security Appliance that you have selected operates with regard to alerting or specific reporting.
(c) If BT agrees a request from you to alter the parameters for applying new signatures in "**block**" mode, to give a greater or lower sensitivity to attacks, you accept responsibility for the increased risk of false positives (blocks to legitimate traffic) or the increased risk of attacks being missed.

2.1.5 **Security Event Reporting:**

(a) BT will:

(i) provide reporting facilities, via the Security Portal, which allows analysis of security-related events; and

(ii) not pro-actively view your reports and events for Security Incidents.

(b) If this Standard Service Component is delivered via a shared reporting platform, BT will configure the platform such that you are only provided with access to your reports. This may mean that some of the platform's functionality is restricted to preserve the confidentiality of all customers using that platform.

(c) Data can be analysed for reporting purposes over a rolling 30 day period.

2.1.6 **SSL/TLS Inspection:**

(a) BT will intercept and decrypt SSL Encrypted Traffic in order to carry out inspection in accordance with the CSP. Once the traffic has been inspected, it will be re-encrypted and relayed to its original destination (if permitted by the CSP).

(b) BT will not intercept and decrypt SSL Encrypted Traffic for every category of web content due to a high possibility of issues with associated applications with certain websites e.g. some websites may not permit decryption.

(c) If you do not allow traffic to be decrypted, BT cannot inspect it.

3 SERVICE OPTIONS

3.1 BT will provide you with any of the following options ("**Service Options**") as set out in any applicable Order and in accordance with the details as set out in that Order:

3.1.1 **Ad Hoc Professional Service:**

(a) BT will provide ad hoc technical support, chargeable per day, as set out in the Order.

(b) Professional Services are delivered remotely unless otherwise set out in the Order.

3.1.2 **Eagle-I Enhanced Firewall Service**

BT shall provide you with the Eagle-I Enhanced Firewall Service, subject to the requirements set out below.

(a) Existing Blocklist Enhancement

(i) Subject to BT confirming that your Security Appliance is suitable for use with the Eagle-I Enhanced Firewall Service, BT will use its Eagle-I Platform to identify any unique malicious IPs and/or URLs to supplement your Security Appliance's existing blocklist of malicious IPs and/or URLs ("**Indicators of Compromise**" or "**IOCs**".)

(ii) Upon confirming the suitability of your Security Appliance, BT will add new IOCs to the BT Blocklist for consumption by your Security Appliance ("**Existing Blocklist Enhancement**".)

(b) Automated IOC Blocking

(i) Subject to BT confirming the technical feasibility of applying Automated IOC Blocking to your Security Appliance, as part of its remote service management of your Security Appliance, BT shall automatically implement changes to your Security Appliance so that it will block IOCs propagated from the BT Blocklist ("**Automated IOC Blocking**").

(ii) For the avoidance of doubt, when the Eagle-I Enhanced Firewall service is specified, subject to the requirements of technical feasibility (as outlined above at Paragraph 3.1.15(b)(i)), BT shall implement Automated IOC Blocking. By specifying the Eagle-I Enhanced Firewall Service, you hereby consent to BT implementing Automated IOC Blocking in respect of your Security Appliance.

(iii) BT shall not be responsible for any wider impact of any Automated IOC Blocking, including but not limited to any impact from the Automated IOC Blocking on Customer Equipment, or on your wider Network.

3.2 The BT Managed Web Application Firewall Security Service may not be available in all locations and Service Levels may vary depending on Site location.

4 SERVICE MANAGEMENT BOUNDARY

4.1 BT will provide and manage the BT Managed Web Application Firewall Security Service as set out in Parts A, B and C of this Annex and as set out in the Order up to:

4.1.1 the Internet/WAN side: the cable connecting to the BT provided switch;

4.1.2 the web server side: the Ethernet port on the Security Appliance; or

4.1.3 the analogue exchange line: the cable connecting BT's provided modem to the PSTN socket,

("**Service Management Boundary**").

4.2 BT will have no responsibility for the BT Managed Web Application Firewall Security Service outside the Service Management Boundary, including:

4.2.1 issues on Users' machines, free downloadable vendor software not provided by BT, or your servers (e.g. operating system, coding languages and security settings);

4.2.2 end to end network connectivity (e.g. your network or Internet connectivity); or

4.2.3 identity source management.

4.3 BT does not make any representations, whether express or implied, about whether the BT Managed Web Application Firewall Security Service will operate in combination with any Customer Equipment or other equipment and software.

4.4 BT cannot guarantee that the BT Managed Web Application Firewall Security Service will operate without Incident or interruption or to intercept or disarm all malware.

4.5 BT does not make any representations or warranties, whether express or implied, as to any outcomes of Automated IOC Blocking undertaken as part of the Eagle-I Enhanced Firewall Service Option, including but not limited to any reduction in security incidents or to the threat impact on any Customer Equipment or your wider Network.

5 ASSOCIATED SERVICES AND THIRD PARTIES

5.1 You will have the following services in place prior to the BT Managed Web Application Firewall Security Service being delivered. You will ensure that these services meet the minimum technical requirements that BT may specify:

5.1.1 Internet connectivity;

5.1.2 WAN connectivity;

5.1.3 PSTN direct exchange line, to enable Out of Band Access management;

5.1.4 LAN/DMZ connectivity and associated infrastructure; and

5.1.5 broader IT environment, including authentication services, server/client platforms, Security Incident and event management (SIEM) solutions,

(each an "**Enabling Service**").

5.2 If BT provides you with any services other than the BT Managed Web Application Firewall Security Service (including any Enabling Service) this Annex will not apply to those services and those services will be governed by their separate terms and conditions.

6 SPECIFIC TERMS AND CONDITIONS

6.1 **EULA**

6.1.1 BT will only provide the BT Managed Web Application Firewall Security Service if you have entered into an end user licence agreement with the Supplier of the Security Appliance in the form set out at https://www.fortinet.com/content/dam/fortinet/assets/legal/EULA.pdf, as may be amended or supplemented from time to time by the Supplier ("**EULA**").

6.1.2 You will observe and comply with the EULA for all or any use of the applicable Software.

6.1.3 In addition to what it says in Clause 15 of the General Terms, if you do not comply with the EULA, BT may restrict or suspend the BT Managed Web Application Firewall Security Service upon reasonable Notice, and:

(a) you will continue to pay the Charges for the BT Managed Web Application Firewall Security Service until the end of the Minimum Period of Service; and

(b) BT may charge a re-installation fee to re-start the BT Managed Web Application Firewall Security Service.

6.1.4 You will enter into the EULA for your own benefit and the rights, obligations, acknowledgements, undertakings, warranties and indemnities granted in accordance with the EULA are between you and the supplier and you will deal with the supplier with respect to any loss or damage suffered by either of you as such loss or damage will not be enforceable against BT.

6.1.5 Where the EULA is presented in a 'click to accept' function and you require BT to configure or install Software on your behalf, BT will do so as your agent and bind you to the EULA.

6.2 **Amendments to the BT Managed Security Service Schedule**

6.2.1 The wording in Paragraph 3 (**Initial Setup**) of the Schedule is deleted and replaced with the following:

BT will facilitate the setup and delivery of the Associated Services that are set out in the Order and that are included as part of the BT Managed Security Service.

3.1 **Foundation**

3.1.1 BT will keep you informed throughout the delivery process.

3.1.2 BT will provide standard policies that reflect good practice.

3.1.3 Not used.

3.1.4 You may request changes to your CSPs after the Service Start Date in accordance with Paragraph 6.3.

3.1.5 You are responsible for defining your ongoing CSP(s) beyond that set out in the policies selected by you after the Service Start Date.

3.1.6 BT may provide you with Professional Services at an additional Charge, at your request, to assist you in the creation of your CSP(s). The responsibility for the CSP(s) will remain with you.

3.1.7 BT will co-ordinate the delivery of the Associated Services.

3.1.8 BT will install the BT Equipment and the Purchased Equipment for the Associated Services, if applicable.

3.1.9 BT will commission the Associated Services remotely in accordance with the policy selected by you and in accordance with Paragraph 10.2.

3.1.10 You may request that BT, at an additional Charge:

(a) appoints a named BT Project Manager to be your single point of contact during the Initial Setup. The BT Project Manager will undertake any activity remotely and will not visit your Site; or

(b) provides a named BT Project Manager who will be available to attend meetings at your Site depending on your location for the duration of the Initial Setup.

3.2 **Foundation Plus**

3.2.1 BT will appoint a named BT Project Manager to be your single point of contact during the Initial Setup. The BT Project Manager will undertake any activity remotely and will not visit your Site.

3.2.2 BT will provide a customisable security policy to use as your CSP.

3.2.3 You may request that BT provides a named BT Project Manager who will be available to attend meetings at your Site depending on your location for the duration of the Initial Setup at an additional Charge.

3.3 **Premium**

BT will provide a named BT Project Manager who will be available to attend meetings at your Site depending on your location for the duration of the Initial Setup.

6.2.2 The wording in Paragraph 4 (**Controlled Deployment**) of the Schedule is deleted and replaced with the following:

BT will work with you during the Controlled Deployment CSP Optimisation Period.

4.1 Foundation, Foundation Plus and Premium

4.1.1 The Security Appliance will monitor logs for a period of seven days at the end of the Initial Setup.

4.1.2 After the period set out in Paragraph 4.1.1, BT will enable blocking of traffic that the Supplier knows to be bad.

4.1.3 After blocking has been enabled, BT will switch the Security Appliance to learning mode, monitor traffic for behaviour patterns and propose additional types of traffic that could be blocked or cause issues. This will continue for a period of seven days or until sufficient data has been gathered.

4.1.4 After the period set out in Paragraph 4.1.3, BT will agree with you additional traffic to be blocked and enable this for a period of time that will be advised to you by BT.

4.1.6 BT will notify you of the date of completion of the Controlled Deployment CSP Optimisation.

4.1.7 If you require to implement blocking after the end of the Controlled Deployment CSP Optimisation Period, BT will enable such blocking at an additional Charge.

4.1.8 If you have requested changes to the CSP(s) after the Controlled Deployment CSP Optimisation Period, BT will direct you to the CSP change management facility on the Security Portal set out in Paragraph 6.3. If

BT is aware that, or you advise BT that, you are unable to access the Security Portal, BT will direct you to the appropriate BT Personnel to review your request.

6.2.3 Paragraph 5 (**Monitoring and Management**) of the Schedule will not apply and Paragraph 7 (Monitoring and Management) of this Annex will apply in its place.

6.2.4 Paragraph 6 (**Continuous Improvement**) of the Schedule will not apply and Paragraph 8 (Continuous Improvement) of this Annex will apply in its place.

6.2.5 The wording in Paragraph 10.3 (**BT's Obligations During Operation**) of the Schedule will not apply and Paragraph 11.2 of this Annex will apply in its place.

6.2.6 Paragraph 11.2 (**Controlled Deployment CSP Optimisation)** of the Schedule will not apply.

6.2.7 The definition "**Controlled Deployment CSP Optimisation**" in the Schedule is deleted and replaced with the following:

"**Controlled Deployment CSP Optimisation**" means the process as set out in Paragraph 4.

6.2.8 The definition "**Controlled Deployment CSP Optimisation Period**" in the Schedule is deleted and replaced with the following:

"**Controlled Deployment CSP Optimisation Period**" means the periods of time as set out in Paragraph 4.

6.2.9 Paragraph 14 (**CSP Change Request Delivery Time Targets**) of the Schedule will not apply.

7 MONITORING AND MANAGEMENT

The Monitoring and Management will commence on the Service Start Date.

7.1 Security Threat Intelligence

7.1.1 Foundation

(a) BT will provide you with general threat intelligence bulletins and reports in English through the Security Portal. This could include:

(i) daily threat advisories: these provide a view of the latest headline security events, actors, targets, operations and campaigns, vulnerabilities and suspicious IP Addresses;

(ii) global threat summaries: these provide a wide angle and high-level view of the significant events and attacks that have occurred globally and across all industries;

(iii) monthly executive level briefing: these provide a CISO level view of the threat landscape focussing on events impacting global organisations from a strategic perspective; and

(iv) global critical bulletins: these provide a technical assessment of significant global security events such as WannaCry so that a more detailed understanding can be obtained.

7.2 Manage Service Incidents

BT will act as a single point of contact for resolution of Incidents related to the BT Managed Web Application Firewall Security Service.

7.2.1 Foundation

(a) You will notify all Incidents to the Service Desk via the Security Portal or directly to the Service Desk if agreed by BT.

(b) All communications with the Service Desk will be in English.

(c) The Service Desk that will action the Incident notifications is available 24x7x365 and is staffed by security trained professionals.

(d) BT will give you a Ticket.

(e) BT will assess the Incident in accordance with the criteria set out in the table below:

Priority	Description
P1	Serious impact and Incident cannot be circumvented, typically where the Associated Service is completely down / unavailable; for example: your Site is isolated or there is a complete loss of service to a Site or critical business functions are prevented from operating.
P2	Large impact on a portion of the Associated Service and cannot be circumvented, causes significant loss of the BT Managed Web Application Firewall Security Service, but the impacted business function is not halted; for example: there is a complete loss of primary link and the BT backup link

Priority	Description
	(if provided) is invoked or business functions are disrupted but not prevented from operating.
P3	Small impact on the BT Managed Web Application Firewall Security Service or where a single User or component is affected and it causes some impact to your business; for example: there is an intermittent or occasional disturbance which does not have a major impact on the BT Managed Web Application Firewall Security Service or where a temporary work around has been provided.
P4	Incident minor or intermittent impact to a non-operational element of the BT Managed Web Application Firewall Security Service; for example: a temporary failure of reporting or billing.
P5	Incident has no direct impact on the BT Managed Web Application Firewall Security Service. Records normally kept for Incidents are used for information purposes. Example: to track upgrades, to obtain a Reason for Outage report, for planned outages or for enquiries as well as customer provoked Incidents.

(f) BT will review the status of the Incident and amend the priority level assigned initially if necessary.

(g) BT will maintain back-up configurations to allow the BT Managed Web Application Firewall Security Service to be restored fully following the swap out of a Security Appliance.

(h) BT will keep you informed throughout the course of the Incident resolution at regular intervals by posting updates on the Security Portal or via e-mails to the Customer Contact in accordance with Paragraph 12 (Service Targets Incident Management) of the Schedule.

(i) BT will inform you when it believes the Incident is cleared and will close the Ticket when:

(i) you confirm that the Incident is cleared within 24 hours after having been informed; or

(ii) BT has attempted unsuccessfully to contact you, in the way agreed between both of us in relation to the Incident, and you have not responded within 24 hours following BT's attempt to contact you.

(j) If you confirm that the Incident is not cleared within 24 hours after having been informed, the Ticket will remain open, and BT will continue to work to resolve the Incident.

(k) Where BT becomes aware of an Incident, Paragraphs 7.2.1(d) to 7.2.1(j) will apply.

(l) In the event of a failure of a Security Appliance, you will permit BT or BT's agents at BT's discretion to remove and replace faulty components or to remove the faulty Security Appliance in its entirety and exchange it with a functioning replacement, where applicable. BT will use reasonable endeavours to ensure any data on the recovered appliance or component is rendered unreadable prior to disposal or recycling.

7.2.2 **Foundation Plus**

You will notify all Incidents to the Service Desk directly or via the Security Portal.

7.2.3 **Premium**

You will agree with BT whether you report Incidents to the Service Desk directly or via the Security Portal or to the Security Operations Centre.

7.3 **Proactive Monitoring**

BT will monitor the performance of the BT Managed Web Application Firewall Security Service against parameters that BT deems appropriate depending on the nature of the BT Managed Web Application Firewall Security Service.

7.3.1 **Foundation**

(a) BT will monitor the performance of the BT Managed Web Application Firewall Security Service at intervals set by BT and, where possible, provide advance warning to you through the Security Portal of impending issues that may affect the BT Managed Web Application Firewall Security Service and that BT identifies as a result of the monitoring. BT may not identify all impending issues.

(b) You are responsible for resolving the issues that BT provides you advance warning of in Paragraph 7.3.1(a).

(c) BT will check that the BT Managed Web Application Firewall Security Service is operating correctly by:

(i) polling the Security Appliance to check it is powered on and has network connectivity. If the Security Appliance is not powered on or does not have network connectivity, the SOC will investigate and either take appropriate action or recommend action that you require to take;

(ii) Security Appliance status test: BT will test at regular intervals at BT's discretion as follows:

i. Resource status: conduct one test per Resource per Security Appliance such as CPU and RAM;

ii. physical status: conduct one test per physical attribute per Security Appliance such as temperature, where applicable to the Security Appliance;

iii. compare test results against standard vendor thresholds and notify any variances to the SOC. The SOC will investigate and either take appropriate action or recommend action that you are required to take; and

iv. BT Managed Web Application Firewall Security Service access monitoring: generate alerts in near real time for unauthorised access attempts.

(d) You will ensure that you or third parties, as required, configure routing/permissions on platforms or the BT Managed Web Application Firewall Security Service to allow BT to carry out the monitoring or management. Failure to do so could impact implementation plans or BT's ability to update Software and signature on the Security Appliance(s).

7.3.2 **Foundation Plus**

(a) Both of us will agree a process for BT to contact you when it identifies an issue that impacts the BT Managed Web Application Firewall Security Service.

(b) In addition to the checks carried out by BT in accordance with Paragraph 7.3.1(c), BT will check that the BT Managed Web Application Firewall Security Service is operating correctly by monitoring the applications under the BT Managed Web Application Firewall Security Service against parameters set by BT.

7.3.3 **Premium**

(a) In addition to the checks carried out in Paragraphs 7.3.1(c) and 7.3.2(b), BT will check that the BT Managed Web Application Firewall Security Service is operating correctly by:

(i) password management including checking age and complexity of passwords, along with checking password hashes against known leaked password hash databases; and

(ii) certificate expiry monitoring. You are responsible for updating certificates.

7.4 Signature Updates

BT will identify and implement Signature Updates on BT Managed Web Application Firewall Security Service.

7.4.1 Signature Updates will be managed by BT's supplier.

7.4.2 **Foundation, Foundation Plus and Premium**

(a) You consent to BT applying the Signature Updates automatically.

(b) BT will apply the Signature Update at a time convenient to BT.

(c) If BT is aware that your BT Managed Web Application Firewall Security Service will have downtime or that the Signature Update will cause an impact on the BT Managed Web Application Firewall Security Service, both of us will agree an appropriate time within Business Hours for the Signature Update to be applied.

(d) BT will, where possible, identify and apply an automated method for applying Signature Updates unless this may impact the BT Managed Web Application Firewall Security Service.

(e) If BT requires to apply a Signature Update manually, both of us will agree an appropriate time within Business Hours for the Signature Update to be applied.

(f) If you request that the Signature Update is applied outside Business Hours, BT may invoice you for an additional Charge.

(g) You will request or authorise BT to reverse the Signature Update if it causes an Incident in the BT Managed Web Application Firewall Security Service.

(h) BT is not able to simulate your environment to test the impact of automatically applying a Signature Update.

7.5 Log Capture

7.5.1 BT will implement a logging capability on the BT Managed Web Application Firewall Security Service.

7.5.2 A minimum log set, at BT's discretion, will be captured and stored to enable BT to offer effective management of the BT Managed Web Application Firewall Security Service and the captured logs will be made available to you if you request access to the logs in accordance with Paragraph 7.5. BT will advise you how the captured logs will be made available to you.

7.5.3 **Foundation**

(a) BT will store the Audit and Alert Logs within an appropriate secure BT environment outside of your environment on a rolling 13 month basis where appropriate.

(b) BT will store the Operational Logs within an appropriate secure BT environment outside of your environment on a rolling one month basis where appropriate.

(c) BT will make available the previous 60 days' Audit and Alert Logs to you on your request. If you require access to the Audit and Alert Logs outside of the previous 60 days, BT will make them available to you at an additional Charge.

(d) BT will make available the previous 30 days' Operational Logs to you on your request.

(e) BT will use reasonable endeavours to transmit and store the logs securely.

(f) BT will store the logs in their raw state or compress them if appropriate.

(g) You will confirm your specific logging requirements at the time of placing the Order. BT may raise a Charge for any of your specific requirements that BT deems are non-standard.

(h) If requested by you and subject to an additional Charge, logs may be sent to and stored in a repository on your Site or third party premises based on a design that is agreed by both of us and:

(i) BT will not be responsible for the logs while they are sent to or stored in such a repository;

(ii) the other provisions of Paragraph 7.5 will not apply to logs sent to or stored in such a repository;

(iii) you will take any action necessary in a timely manner to enable the logs to be routed to the repository as agreed with BT; and

(iv) you will ensure that you or the nominated third party use reasonable endeavours to secure the repository appropriately.

7.5.4 **Foundation Plus**

(a) BT will make available the previous 120 days' Audit and Alert Logs to you on your request. If you require access to the logs outside of the previous 120 days, BT will make them available to you at an additional Charge.

(b) BT will make logs available to:

(i) your, or third party technologies, where appropriate as agreed with you; or

(ii) to other services BT is providing to you that do not form part of the Contract where appropriate as agreed with you.

7.5.5 **Premium**

(a) BT will make available Audit and Alert Logs to you on your request for a rolling 13 month period.

7.6 **Licensing and Vendor Support Agreement Management**

BT will ensure that all software licences and required vendor support agreements are placed and renewed for the term of the Contract for the Associated Services on your behalf.

7.6.1 **Foundation, Foundation Plus and Premium**

(a) BT will provide, implement and deploy appropriate licences and required vendor support agreements for the Associated Services on your behalf.

(b) BT is responsible for ensuring software licences and any required vendor support agreements are renewed for the term of the Contract.

(c) Unless you give BT Notice of an intention to terminate in accordance with Paragraph 9.1 (Minimum Period of Service and Renewal Periods) of the Schedule, BT will renew the software licence or required support agreement for a period of 12 months or as agreed by both of us or for any other period that is appropriate to the nature of the applicable software licence or vendor support agreement.

(d) If you cancel or terminate the software licence or vendor support agreement during the contract term or renewal period of the software licence or vendor support agreements, you will pay any costs that are incurred by BT including any charges reasonably incurred by BT from a supplier as a result of the cancellation or termination. If you have paid the charges or fees for the software licence or vendor support agreement in advance, you may not be entitled to a refund of the charges for the remaining months of the contract term or renewal period.

(e) BT will validate that you have ordered the correct number of licences either direct from the vendor or through BT to serve your requirements for the BT Managed Web Application Firewall Security Service in accordance with terms of the software licences and vendor support agreements and information provided by you and:

(i) if BT determines that you have not ordered sufficient licences either direct from the vendor or through BT for BT Managed Web Application Firewall Security Service, BT will notify you and you will seek to rectify the situation within 30 days of the date of notification;

(ii) if the situation is not resolved within this time, BT may suspend the BT Managed Web Application Firewall Security Service and subsequently terminate the BT Managed Web Application Firewall Security Service in accordance with Clause 18 of the General Terms; and

(iii) BT is not liable for unknown breaches of the software licences and vendor support agreements where BT is acting on information provided by you.

(f) You will confirm to BT any change in the number of Users or Security Appliances requiring licences as part of the BT Managed Web Application Firewall Security Service.

7.7 Reporting

7.7.1 Foundation, Foundation Plus and Premium

(a) BT will provide you with an inventory of the BT Managed Web Application Firewall Security Service and reporting for the BT Managed Security Service and the BT Managed Web Application Firewall Security Service via the Security Portal in accordance with this Paragraph 7.7 including:

(i) a dashboard tailored to the BT Managed Web Application Firewall Security Service; and

(ii) inventory information BT deems appropriate.

(b) BT will provide reports with details and at a frequency as it deems appropriate on:

(i) usage and capacity management of the BT Managed Web Application Firewall Security Service; and

(ii) end of life and end of service of Security Appliances, firmware and operating systems.

8 CONTINUOUS IMPROVEMENT

8.1 Reviews

8.1.1 Foundation

(a) The Security Optimisation Manager will work with your Customer Contact regularly during the provision of the BT Managed Web Application Firewall Security Service to carry out reviews as follows:

(i) a BT Managed Security Service and BT Managed Web Application Firewall Security Service review focussing on the performance of the BT Managed Security Service and the BT Managed Web Application Firewall Security Service;

(ii) a BT Managed Security Service and BT Managed Web Application Firewall Security Service review of recent security events;

(iii) a review of the reports set out on the Security Portal; or

(iv) an end of life review on an ongoing basis. The Security Optimisation Manager will review the details set out on the Security Portal summarising the Security Appliances, applications and software that are managed by BT on your behalf as part of the BT Managed Web Application Firewall Security Service that will go end of life within the following six months. The report will include Security Appliances, applications and software advised to you previously that are past end of life and that require immediate action by you.

(b) If requested by you and if agreed to by BT, both of us may hold a conference call to discuss the report.

(c) If BT has agreed to participate in a conference call you will ensure that the reports set out on the Security Portal will be reviewed by your suitably qualified personnel who are participating in the conference call prior to the conference call taking place. You will ensure that your suitably qualified personnel will have the authority to authorise changes to the configuration of the BT Managed Web Application Firewall Security Service.

(d) You will take appropriate action to address issues as recommended by the Security Optimisation Manager:

(i) in respect of the BT Managed Security Service or BT Managed Web Application Firewall Security Service including implementing security improvements as agreed with the Security Optimisation Manager or as advised by the Security Optimisation Manager as your responsibility; and

(ii) in respect of the end of life review or as set out in the end of life review report.

8.1.2 **Foundation Plus**

(a) The Security Optimisation Manager will work with your Customer Contact regularly during the provision of the BT Managed Web Application Firewall Security Service to carry out reviews as follows:

(i) a BT Managed Security Service and BT Managed Web Application Firewall Security Service review focussing on the performance of the BT Managed Security Service and Associated Services against Service Levels and Service Targets and capacity management of the BT Managed Web Application Firewall Security Service;

(ii) a BT Managed Security Service and BT Managed Web Application Firewall Security Service review of recent security events;

(iii) a review of the reports set out on the Security Portal;

(iv) a review of your CSP(s) focussing on the effectiveness of the rules applied to the CSP(s) and the need to fine tune or amend the rules of your CSP(s); or

(v) an end of life review as set out in Paragraph 8.1.1(a)(iv).

(b) In addition to taking the action set out in Paragraph 8.1.1(d), you will ensure that your relevant personnel are authorised to instruct BT to initiate the appropriate change requests in accordance with the CSP Change Management Process to address issues in respect of fine tuning or amending your CSP(s) as discussed with the Security Optimisation Manager

8.1.3 **Premium**

(a) The Security Optimisation Manager will work with your Customer Contact regularly during the provision of the BT Managed Web Application Firewall Security Service to carry out reviews as follows:

(i) a BT Managed Security Service and BT Managed Web Application Firewall Security Service review every month focussing on the performance of the BT Managed Security Service and BT Managed Web Application Firewall Security Service against Service Levels and Service Targets and capacity management of the BT Managed Web Application Firewall Security Service;

(ii) a BT Managed Security Service and BT Managed Web Application Firewall Security Service review of recent security events;

(iii) a review of the reports set out on the Security Portal;

(iv) a review of your CSP(s) focussing on the effectiveness of the rules applied to the CSP(s) and the need to fine tune or amend the rules of your CSP(s); or

(v) an end of life review as set out in Paragraph 8.1.1(a)(iv).

8.1.4 The allotted time for the Security Optimisation Manager included in the Charges will vary depending on the Graded Service Tier you select and will be agreed by both of us. You may request additional assistance from the Security Optimisation Manager at an additional Charge.

8.2 **Vulnerability Management and Patching of Security Appliances**

8.2.1 BT will rank all Patch updates as priority ranking in accordance with the CVSS:

CVSS Score	Graded Service Tier
5.0 – 6.9	Premium
7.0 – 8.9	Foundation Plus and Premium
9.0 – 10	Foundation, Foundation Plus and Premium

8.2.2 Vulnerability Management and Patching of Security Appliances will only be available while the Security Appliance is supported by the vendor.

8.2.3 All communications in respect of Vulnerability Management and Patching of Security Appliances will be through the Security Portal.

8.2.4 **Foundation**

(a) BT may not assess the configuration or contextual exposure of any Security Appliances to the Vulnerability.

(b) You will assess the suitability for deployment of the Patches that BT advises are available to address notified Vulnerabilities within your specific environment and for any post-implementation testing.

(c) BT may implement Patches with a High CVSS score or a Medium CVSS score, on your request, at an additional Charge.

(d) BT will implement a Patch for a Vulnerability with a Critical CVSS score, subject to your agreement and also agreeing an implementation time slot with you.

(e) BT will provide a secure mechanism on the Security Portal for you to confirm your agreement to BT implementing a Patch that BT has recommended.

(f) BT will specify an implementation window for BT to implement the Patches which will be typically a weekly six hour window outside of Business Hours for the Site where the Security Appliance is situated.

(g) BT will apply the Patch in the specified implementation window and confirm to you via the Security Portal when the Patch has been implemented.

(h) BT will roll the Patch back upon your request in the event that you detect undesirable side-effects. Any activity by BT required to resolve issues resulting from the implementation of a Patch is not covered by the Vulnerability Management and Patching and BT will invoice you for reasonable additional Charges.

(i) If you do not consent to accept and implement a Patch within 14 days of notification by BT of a recommended Patch, or if you request that an installed Patch is reversed out due to your specific undesirable side-effects, BT will be under no further obligation to provide further Vulnerability Management and Patching in respect of that Patch and will not have any liability for potential exposure should a threat subsequently exploit that related Vulnerability.

8.2.5 **Foundation Plus**

(a) BT will implement a Patch for a Vulnerability with a Critical CVSS score and a High CVSS score and latest stable variant of the vendor's general availability code, subject to your agreement and agreeing an implementation time slot with you.

(b) BT may implement Patches with a Medium CVSS score, on your request, at an additional Charge.

8.2.6 **Premium**

(a) BT will implement a Patch for a Vulnerability with a Critical CVSS score, a High CVSS score and a Medium CVSS score and latest stable variant of the vendor's general availability code, subject to your agreement and agreeing an implementation time slot with you.

8.3 **CSP Change Management Process**

8.3.1 BT will implement changes to the CSP(s) in response to your request subject to the following process:

(a) the authorised Customer Contact will submit requests to change the CSP(s) through the Security Portal, providing sufficient detail and clear instructions as to any changes required. If BT is aware that, or you advise BT that, you are unable to access the Security Portal, BT will direct you to the appropriate BT Personnel to review your request;

(b) all changes will be processed in accordance with Clause 31 (Service Amendment) of the General Terms;

(c) any change you request requiring physical changes to the BT Managed Web Application Firewall Security Service including Security Appliance upgrades or LAN re-arrangements, additional hardware or licences will also proceed in accordance with Clause 31 (Service Amendment) of the General Terms;

(d) BT may provide you with Professional Services at an additional Charge, at your request, to assist you in writing your change request;

(e) BT will communicate the status of change requests via e-mail to the Customer Contact requesting the change;

(f) you will not, and ensure that Users with access to the Security Portal do not, submit any unauthorised changes;

(g) you are deemed to have approved all changes to the CSP(s) that you submit to BT;

(h) you are responsible for the impact of BT implementing the changes and BT is not liable for any consequences arising from the impact of the implementation of the changes;

(i) BT will not be liable for any consequence arising from:

(i) your misspecification of your security requirements in the CSP(s); or

(ii) unforeseen consequences of a correctly specified and correctly implemented CSP(s);

(j) there is no Target Implementation Time for Complex Changes; and

(k) the Customer Handbook will set out the changes that can be requested along with a classification of complexity.

8.3.2 **Foundation, Foundation Plus and Premium**

(a) The authorised Customer Contact may submit requests to modify the CSP(s) either through the Security Portal or direct to the Security Optimisation Manager.

9 IP ADDRESSES AND DOMAIN NAMES

9.1 Except for IP Addresses expressly registered in your name, all IP Addresses and Domain Names made available with the BT Managed Web Application Firewall Security Service will at all times remain BT's property or the property of BT's suppliers and are non-transferable.

9.2 All of your rights to use such IP Addresses or Domain Names will cease on termination or expiration of the BT Managed Web Application Firewall Security Service.

9.3 BT cannot ensure that any requested Domain Name is available from or approved for use by the applicable Regional Internet Registry and BT has no liability for any failure in the Domain Name registration, transfer or renewal process.

9.4 You will not use IP Addresses that you do not own or that are incorrectly specified and you will be responsible for the use of IP Addresses within your network. BT may apply additional Charges for dealing with changes or Incidents that occur as a result of incorrect / illegal IP Addressing schemes.

9.5 You warrant that you are the owner of, or are authorised by the owner of, the trade mark or name that you wish to use as a Domain Name, and that such Domain Name will not infringe the rights of any person in a corresponding trade mark or name.

9.6 You will pay all fees associated with registration and maintenance of your Domain Name, and will reimburse BT for any and all fees that BT pays to any applicable Regional Internet Registry, and thereafter pay such fees directly to the applicable Regional Internet Registry.

10 REGULATORY COMPLIANCE

10.1 The BT Managed Web Application Firewall Security Service may not be able to meet all regulatory compliance requirements and therefore may not be a suitable service for your purposes. It is your responsibility to meet all applicable regulatory compliance requirements e.g. Payment Card Industry Data Security Standards and ensure that the BT Managed Web Application Firewall Security Service is suitable for your purposes.

10.2 BT is not responsible for any impact resulting from non-compliance to regulations.

Part B – Service Delivery and Management

11 BT'S OBLIGATIONS

11.1 **Service Delivery**

Before the Service Start Date and, where applicable, throughout the provision of the BT Managed Web Application Firewall Security Service, BT will provide you with the Site Planning Guide.

11.2 **During Operation**

On and from the Service Start Date, BT:

11.2.1 will maintain and will use reasonable endeavours to provide uninterrupted access to all pre-agreed and authorised Customer Contacts to the Security Portal but BT does not guarantee that the Security Portal will be available at all times or will be fault free;

11.2.2 may carry out Maintenance from time to time and will use reasonable endeavours to inform you at least five Business Days before any Planned Maintenance on the BT Managed Web Application Firewall Security Service however, BT may inform you with less notice than normal where Maintenance is required in an emergency;

11.2.3 may, in the event of a security breach affecting the BT Managed Security Service or the BT Managed Web Application Firewall Security Service, require you to change any or all of your passwords;

11.2.4 will provide 24x7x365 on-Site maintenance response where this is available locally, where applicable. BT will advise you where this level of cover is not available and what level of on-Site support will be available;

11.2.5 may install additional BT Equipment on your Site, for the purpose of monitoring and management of the BT Managed Web Application Firewall Security Service;

11.2.6 will use secure protocols or provide a secure management link to connect to the Security Appliance via the Internet or other agreed network connection, in order to monitor the BT Managed Web Application Firewall Security Service proactively and to assist in Incident diagnosis;

11.2.7 will provide an Out of Band Access link that connects directly to the Security Appliance(s), via a modem provided by BT and a PSTN direct exchange line provided by you to allow further remote management and diagnostics capability;

11.2.8 will notify you if BT anticipates that your hardware or software will become End of Life and will no longer be supported by the BT Managed Web Application Firewall Security Service. BT will recommend to you to replace or upgrade the applicable hardware or software at an appropriate time. BT will notify you of any changes to the Charges if the relevant hardware or software is BT Owned and will discuss with you the costs of upgrade if the relevant hardware or Software is Customer Equipment;

11.2.9 will, in relation to certificates required to enable traffic to be decrypted and encrypted:

(a) monitor certificate expiry;
(b) notify you of a certificate expiry at least 30 days before the expiry of the certificate;
(c) on request by you, generate a certificate signing request for completion by you;
(d) back-up the private key; and
(e) upload the certificate on the Security Appliance when the certificate is received from you; and

11.2.10 where the Eagle-I Enhanced Firewall Service Option is specified, BT will implement any changes as part of Automated IOC Blocking as quickly as is technically practicable.

11.3 **The End of the Service**

On termination of the BT Managed Web Application Firewall Security Service by either of us BT:

11.3.1 will terminate any rights of access to the relevant Security Portal and relevant Software and stop providing all other elements of the BT Managed Web Application Firewall Security Service; and

11.3.2 will, where requested in writing prior to the termination of this Contract, delete configuration information from the Security Appliances.

12 YOUR OBLIGATIONS

12.1 **Service Delivery**

Before the Service Start Date and, where applicable, throughout the provision of the BT Managed Web Application Firewall Security Service by BT, you will:

12.1.1 complete any preparation activities that BT may request to enable you to receive the BT Managed Web Application Firewall Security Service promptly and in accordance with any reasonable timescales, including, any account names and passwords necessary to install and commission the BT Managed Web Application Firewall Security Service on BT Equipment or Customer Equipment;

12.1.2 ensure that the LAN protocols and applications you use will be compatible with the BT Managed Web Application Firewall Security Service;

12.1.3 if an Out of Band Access modem is not included as part of the BT Managed Web Application Firewall Security Service, agree an appropriate alternative with BT to allow for fault diagnosis and base configuration, allowing BT to establish in-band control of the Security Appliance, at the time of installation and following a failure of the Security Appliance;

12.1.4 ensure that your MPLS/Internet access circuit bandwidth is sufficient to meet your requirements and the requirement for in-band management access from BT;

12.1.5 manage, and provide BT with accurate details of your internal IP Address design;

12.1.6 register any required Internet domain names using legitimate addresses which are public, registered and routed to your Site;

12.1.7 modify your network routing to ensure appropriate traffic is directed to the Security Appliance. You acknowledge that switches provided as part of the BT Managed Web Application Firewall Security Service only provide direct physical connectivity between Security Appliances and are not intended to support any network routing functionality;

12.1.8 obtain and provide in-life support for any Software running on your Security Appliances;

12.1.9 where necessary, provide and manage physical or virtual servers on your Site to a specification that BT agrees to run any Software that BT provides;

12.1.10 if BT has agreed to provide all or part of the BT Managed Web Application Firewall Security Service using Customer Equipment, ensure that the Customer Equipment is working correctly. If it is discovered to be faulty before the Service Start Date:

(a) you will be responsible for resolving any faults;
(b) BT will raise Charges to cover additional Site visits; and
(c) agreed installation dates or Customer Committed Date may no longer apply;

12.1.11 ensure that your network and all applications conform to relevant industry standards and provide written confirmation to BT upon reasonable request;

12.1.12 be responsible for ensuring compliance with Applicable Law, including obtaining (if required) local import and User licenses and the written authority from all respective authorities, particularly for countries where the use and import of encryption Software and devices may be restricted by Applicable Law, or the export and re-export of the encryption Software or devices may be subject to the United States of America export control law, not act to misuse the BT Managed Web Application Firewall Security Service as provided by BT to contravene or circumvent these laws. BT may treat any contravention of these laws as a material breach and:

(a) suspend the BT Managed Web Application Firewall Security Service and BT may refuse to restore BT Managed Web Application Firewall Security Service until BT receives an acceptable assurance from you that there will be no further contravention; or
(b) terminate the BT Managed Web Application Firewall Security Service upon Notice in accordance with Clause 25 of the General Terms;

12.1.13 comply with the Site Planning Guide;

12.1.14 work with BT to fine tune the BT Managed Web Application Firewall Security Service;

12.1.15 adhere to local encryption regulations;

12.1.16 provide public IP Addresses to BT for the integration of the BT Managed Web Application Firewall Security Service;

12.1.17 test the BT Managed Web Application Firewall Security Service during Initial Setup;

12.1.18 tune the BT Managed Web Application Firewall Security Service and enable blocking during Controlled Deployment; and

12.1.19 in relation to certificates required to enable traffic to be decrypted and encrypted:

(a) choose the appropriate certificate, select the certificate authority and manage the process of obtaining the certificate;

(b) ensure your certification method has a valid Trust Chain for any certificates provided by the Security Appliance;

(c) renew certificates using the certificate signing requests with the certificate authority;

(d) verify identity of the organisation with the certificate authority for certificate renewal;

(e) download the new certificate and send this to BT in a timely manner to enable BT to complete process before expiry of the old certificate;

(f) pay the cost of certificate renewal direct to the certificate authority;

(g) request that BT uploads the certificate onto the Security Appliance in a timely manner to enable BT to complete the process before expiry of the old certificate; and

(h) notify BT of any certificate revocation.

12.2 **Service Operation**

On and from the Service Start Date, you:

12.2.1 will provide suitably qualified personnel to carry out reviews with the Security Optimisation Manager;

12.2.2 will ensure that all Software provided is used solely for operation of the BT Managed Web Application Firewall Security Service;

12.2.3 will comply with the provisions of any Software licences provided with or as part of the BT Managed Web Application Firewall Security Service;

12.2.4 will allow BT downtime to upgrade the Software on the Web Application Firewall at minimum intervals of six months. If you do not allow BT to upgrade the Software after a total of three attempts or more then this could result in the Security Appliance and the IT environment the BT Managed Web Application Firewall Security Service is protecting will be more vulnerable to attacks;

12.2.5 will agree to upgrade or replace your hardware or software if it becomes End of Life in accordance with BT's recommendation set out in Paragraph 11.2.8. If you do not replace or upgrade in accordance with BT's recommendation, BT will not be liable for any faults or errors when your hardware or software becomes out of support, and BT will only be able to provide you with a limited BT Managed Web Application Firewall Security Service;

12.2.6 will request, if applicable, up to five login/password combinations for access to a Customer Portal for use by you or your agents. You may assign one login combination to BT's personnel. You are responsible for your agents' use of these IDs; and

12.2.7 agree that:

(a) BT will not be liable for failure to supply or delay in supplying the BT Managed Web Application Firewall Security Service if another supplier delays or refuses the supply of an electronic communications service to BT and no alternative service is available at reasonable cost;

(b) BT will provide the BT Managed Web Application Firewall Security Service to you on an "**as is**" and "**as available**" basis. BT does not guarantee that the BT Managed Web Application Firewall Security Service:

(i) will be performed error-free or uninterrupted or that BT will correct all errors in the BT Managed Web Application Firewall Security Service;

(ii) will operate in combination with your content or applications or with any other software, hardware, systems or data;

(iii) including any products, information or other material you obtain under or in connection with this Contract, will meet your requirements; and

(iv) will detect or block all malicious threats;

(c) BT will not be liable in the event that Software updates from the supplier used to identify and control your network traffic (including malware signatures, URL categories or application definitions) contain errors or omissions, beyond making appropriate corrections (where reasonably possible) as soon as reasonably practical;

(d) you will own all right, title and interest in and to all of your information and will have sole responsibility for the legality, reliability, integrity, accuracy and quality of any of your information; and

(e) you will be responsible for results obtained from the use of the BT Managed Web Application Firewall Security Service, and for conclusions drawn from such use. BT will have no liability for any damage

caused by errors or omissions in any information, instructions or scripts provided to BT by you in connection with the BT Managed Web Application Firewall Security Service, or any actions taken by BT at your direction.

12.3 **The End of the Service**

On termination of the BT Managed Web Application Firewall Security Service by either one of us, or expiry you will:

12.3.1 if requested by BT, provide BT with all reasonable assistance necessary to remove BT Equipment from the Sites;

12.3.2 if requested by BT, disconnect any Customer Equipment from BT Equipment located at the Sites;

12.3.3 if requested by BT, not dispose of or use BT Equipment, other than in accordance with BT's written instructions or authorisation;

12.3.4 if requested by BT, arrange for any BT Equipment, including Software, located at the Site(s) to be returned to BT;

12.3.5 be liable for any reasonable costs of recovery that BT incurs in recovering the BT Equipment; and

12.3.6 arrange for relevant certificates to be re-issued.

Part C – Service Levels

13 SERVICE AVAILABILITY

13.1 **Availability Service Level**

13.1.1 From the Service Start Date, BT will provide the BT Managed Web Application Firewall Security Service with a target availability corresponding to the agreed SLA Category for the BT Managed Web Application Firewall Security Service as set out in the table in Paragraph 13.2.2 below (the "**Availability Service Level**").

13.1.2 You may request Availability Service Credits for Qualifying Incidents at either:

(a) the Standard Availability Service Credit Rate, as set out in Paragraph 13.3.5; or

(b) as applicable, the Elevated Availability Service Credit Rate, as set out in Paragraph 13.3.6.

13.2 **SLA Categories**

13.2.1 The SLA Categories depend on a number of factors, including:

(a) any applications you deploy and any CSP you implement;

(b) the broader network and server environment including any resilient elements; and

(c) the physical location of the Security Appliances and availability of on-Site field support.

13.2.2 The following table sets out the Availability Annual Targets, the Maximum Annual Availability Downtime, the Maximum Monthly Availability Downtime, the Standard Availability Service Credit Rate, the Elevated Availability Service Credit Rate and the Service Credit Interval for each SLA Category:

SLA Category	Availability Annual Target	Maximum Annual Availability Downtime	Maximum Monthly Availability Downtime	Standard Availability Service Credit Rate	Elevated Availability Service Credit Rate	Service Credit Interval
Cat A++	≥ 99.999%	5 minutes	0 minutes	4%	8%	5 min
Cat A+	≥ 99.99%	1 hour	0 minutes	4%	8%	15 min
Cat A1	≥ 99.97%	3 hours	0 minutes	4%	8%	1 hour
Cat A	≥ 99.95%	4 hours	0 minutes	4%	8%	1 hour
Cat B	≥ 99.90%	8 hours	1 hour	4%	8%	1 hour
Cat C	≥ 99.85%	13 hours	3 hours	4%	4%	1 hour
Cat D	≥ 99.80%	17 hours	5 hours	4%	4%	1 hour
Cat E	≥ 99.70%	26 hours	7 hours	4%	4%	1 hour
Cat F	≥ 99.50%	43 hours	9 hours	4%	4%	1 hour
Cat G	≥ 99.00%	87 hours	11 hours	4%	4%	1 hour
Cat H	≥ 98.00%	175 hours	13 hours	4%	4%	1 hour
Cat I	≥ 97.00%	262 hours	15 hours	4%	4%	1 hour

13.3 **Availability Service Credits**

13.3.1 If a Qualifying Incident occurs, BT will measure and record the Availability Downtime for the Site starting from when you report or BT gives you notice of a Qualifying Incident, and ending when BT closes the Incident in accordance with Paragraph 5.2.1(i) of the Schedule.

13.3.2 BT will measure the Availability Downtime in units of full minutes during the Local Contracted Business Hours for Access Line Incidents, and during the Contracted Maintenance Hours for BT Equipment Incidents. Where the BT Managed Firewall Service is connected to a third party network, the Availability Service Level will not apply.

13.3.3 Following the measurement taken in accordance with Paragraph 13.3.1 and Paragraph 13.3.2, BT will calculate the cumulative Availability Downtime for the calendar month(s) in which the Qualifying Incident occurred (the "**Cumulative Monthly Availability Downtime**") and for the previous 12 consecutive calendar months (the "**Cumulative Annual Availability Downtime**").

13.3.4 In the event a Site has been installed for less than 12 consecutive months, BT will apply an assumed Cumulative Annual Availability Downtime for the previous 12 consecutive months for that Site or Circuit using the Availability Downtime data recorded to date.

13.3.5 If the Cumulative Monthly Availability Downtime of the Site exceeds the Maximum Monthly Availability Downtime, you may request Availability Service Credits at the Standard Availability Service Credit Rate for each stated Service Credit Interval above the Maximum Monthly Availability Downtime.

13.3.6 If the Cumulative Annual Availability Downtime of the Site or Circuit exceeds the Maximum Annual Availability Downtime, you may request Availability Service Credits for all further Qualifying Incidents at the Elevated Availability Service Credit Rate for each started Service Credit Interval above the Maximum Annual Availability Downtime up to and until the Cumulative Annual Availability Downtime by BT Managed Web Application Firewall Security Service is less than the Maximum Annual Availability Downtime.

13.3.7 Availability Service Credits are available up to a maximum amount equal to 100 per cent of the monthly Recurring Charges.

14 RESILIENCY RESTORATION

14.1 **Resiliency Restoration Service Level**

Where you have purchased a Resilient Service and experience loss of BT Managed Web Application Firewall Security Service on any Resilient Component (which does not amount to a Severity Level 1 Incident), BT aims to restore the BT Managed Web Application Firewall Security Service to the affected Resilient Components within one Business Day of you reporting the Incident, or BT detecting the Incident, ("**Resiliency Restoration Service Level**"). The Resiliency Restoration Service Level will not apply where there is a Qualifying Incident (in which case, the Availability Service Level will apply, in accordance with Paragraph 13.1).

14.2 **Resiliency Restoration Service Credits**

14.2.1 If the affected Resilient Components are not restored within one Business Day, you may request a Resilience Restoration Service Credit for each commenced hour in excess of the Resiliency Restoration Service Level.

14.2.2 This Service Credit only applies where the Resilient Component is covered by an on-Site maintenance agreement of next Business Day or shorter.

15 REQUESTS FOR SERVICE CREDITS

15.1 You may request applicable Service Credits within 28 days of the end of the calendar month in which an Incident occurred by providing details of the reason for the claim. Any failure by you to submit a request in accordance with this Paragraph 15.1 will constitute a waiver of any claim for Service Credits for that calendar month.

15.2 Upon receipt of a valid request for Service Credits in accordance with Paragraph 15.1;

15.2.1 BT will issue you with the applicable Service Credits by deducting those Service Credits from your invoice within two billing cycles of the request being received; and

15.2.2 following termination of the Contract where no further invoices are due to be issued by BT, BT will pay you the Service Credits in a reasonable period of time.

15.3 Service Credits for all Service Levels will be aggregated and are available up to a maximum amount equal to 100 per cent of the monthly Recurring Charge for the affected BT Managed Web Application Firewall Security Service after any discount has been applied.

15.4 Service Credits due to you under this Annex will be calculated on the Recurring Charges after any discount has been applied.

15.5 All Service Levels and Service Credits will be calculated in accordance with information recorded by, or on behalf of, BT.

15.6 The Service Levels under this Annex will not apply:

15.6.1 in the event that Clause 8 of the General Terms applies;

15.6.2 during any trial period of the BT Managed Web Application Firewall Security Service;

15.6.3 to failures due to any Force Majeure Event;

15.6.4 if you cause a delay or do not provide any requested information in accordance with any reasonable timescales BT tells you about;

15.6.5 if your hardware or software becomes End of Life and BT has notified you of this in accordance with Paragraph 11.2.8 and you choose not to replace or upgrade the applicable hardware or software; or

15.6.6 to any Incident not reported in accordance with Paragraph 5.2 of the Schedule.

Part D – Defined Terms

16 DEFINED TERMS

In addition to the defined terms in the General Terms and the Schedule, capitalised terms in this Annex will have the following meanings (and in the case of conflict between these defined terms and the defined terms in the General Terms or the Schedule, these defined terms will take precedence for the purposes of this Annex):

"**Access Line**" means a Circuit connecting the Site(s) to the BT Network.
"**Active Passive**" has the meaning given in Paragraph 2.1.3(c).
"**Automated IOC Blocking**" has the meaning given in Paragraph 3.1.2(b)(i)
"**Availability**" means the period of time when the BT Managed Web Application Firewall Security Service is functioning.
"**Availability Downtime**" means the period of time during which a Qualifying Incident exists as measured by BT in accordance with Paragraph 13.3.1.
"**Availability Service Credit**" means the Service Credit calculated at the Standard Availability Service Credit Rate or at the Elevated Availability Service Credit Rate as applicable.
"**BT Blocklist**" means any IOCs which BT has identified using its Eagle-I Platform.
"**Availability Service Level**" has the meaning given in Paragraph 13.1.1.
"**BT Managed Web Application Firewall Security Service**" has the meaning given in Paragraph 1.1.
"**Circuit**" means any line, conductor, or other conduit between two terminals by which information is transmitted.
"**Contracted Maintenance Hours**" means the times during which BT will provide maintenance for BT Equipment, which will be Business Hours unless specified otherwise in the Order.
"**Cumulative Annual Availability Downtime**" has the meaning given in Paragraph 13.3.3.
"**Cumulative Monthly Availability Downtime**" has the meaning given in Paragraph 13.3.3.
"**Customer Portal**" means one or more webpages made available to you by BT to provide for one or more specific functions in relation to the BT Managed Web Application Firewall Security Service.
"**DMZ**" means de-militarised zone.
"**Domain Name**" means a readable name on an Internet page that is linked to a numeric IP Address.
"**Eagle-I Enhanced Firewall Service**" means the Service Option specified at Paragraph 3.1.2.
"**Eagle-I Platform**" means the solution through which BT shall identify IOCs .
"**Elevated Availability Service Credit Rate**" means the applicable rate as set out in the table at Paragraph 13.2.2 for the relevant SLA Category.
"**Enabling Service**" has the meaning given in Paragraph 5.1.
"**End of Life**" means any hardware or software that is no longer supported by the manufacturer, vendor or supplier and is incapable of cost-effective upgrade or update to a supported version. BT can only provide limited support if your hardware or software reaches this stage.
"**Existing Blocklist Enhancement**" has the meaning given in Paragraph 3.1.2(a)(ii).
"**Ethernet**" means a family of computer networking technologies for LANs.
"**EULA**" has the meaning given in Paragraph 6.1.
"**IOCs**" or "**Indicators of Compromise**" has the meaning given in Paragraph 3.1.2(a)(i).
"**Local Contracted Business Hours**" means the times during which maintenance of any Access Line is provided, which will be Business Hours unless specified otherwise in the Order.
"**Maximum Annual Availability Downtime**" has the meaning given in the table at Paragraph 13.2.2 for the relevant SLA Category.
"**Maximum Monthly Availability Downtime**" has the meaning given in the table at Paragraph 13.2.2 for the relevant SLA Category.
"**Multi-Protocol Label Switching**" or "**MPLS**" means Multi-Protocol Label Switching, a private, global IP-based VPN service based on industry standards that provides the Customer with any-to-any connectivity and differentiated performance levels, prioritisation of delay and non-delay sensitive traffic as well as voice and multi-media applications, all on a single network.
"**Out of Band Access**" means access used for initial configuration and for in-life management where the primary means of access to the Security Appliance has failed or to help resolve failure of the Security Appliance.
"**Payment Card Industry Data Security Standards**" or "**PCI DSS**" means a set of policies and procedures, issued by the PCI Security Standards Council LLC (as may be adopted by local regulators) and intended to optimise the security of credit and debit card transactions and protect cardholders against misuse of their personal information.
"**PSTN**" means Public Switched Telephone Network, which is the concentration of the world's public circuit switched telephone networks.

"**Qualifying Incident**" means a Severity 1 Level Incident, except where any of the following events have occurred:

(a) the BT Managed Web Application Firewall Security Service has been modified or altered in any way by you, or by BT in accordance with your instructions;
(b) Maintenance;
(c) you have performed any network configurations that BT did not approve;
(d) an Incident has been reported and BT cannot confirm that an Incident exists after performing tests;
(e) you requested BT to test the BT Managed Web Application Firewall Security Service at a time when no Incident has been detected or reported; or
(f) the Incident has arisen as a result of you changing your CSP.

"**Regional Internet Registry**" means an organization that manages the allocation and registration of Internet number resources within a particular region of the world. Internet number resources include IP Addresses and autonomous system (AS) numbers.

"**Resiliency Restoration Service Credit**" means one per cent of the total monthly Recurring Charges for the Resilient Service up to a maximum amount equal to 100 per cent of the monthly Recurring Charges.

"**Resiliency Restoration Service Level**" has the meaning given in Paragraph 14.1.

"**Resilient Component**" means, with respect to a Resilient Service, any of the Access Lines, BT Equipment or Customer Equipment.

"**Resilient Service**" means a BT Managed Web Application Firewall Security Service or part of a BT Managed Web Application Firewall Security Service, as set out in the Order that is designed to have high availability and without single points of failure, such that if one component fails the BT Managed Web Application Firewall Security Service is still available.

"**Schedule**" means the BT Managed Security Service Schedule to the General Terms.

"**Security Appliance**" means the BT Equipment used to apply the CSP.

"**Security Incident**" means a single unwanted or unexpected security event, or series of events, consisting of the actual or potential (attempt underway) exploitation of an existing vulnerability, and that has a significant probability of compromising business operations and threatening information security.

"**Service Credit**" means each of the Availability Service Credit and the Resiliency Restoration Service Credit.

"**Service Credit Interval**" means as set out in the table at Paragraph 13.2.2 for the relevant SLA Category.

"**Service Level**" means each of the Availability Service Level and the Resiliency Restoration Service Level.

"**Service Management Boundary**" has the meaning given in Paragraph 4.1.

"**Service Options**" has the meaning given in Paragraph 3.1.

"**Severity Level 1 Incident**" means an Incident that cannot be circumvented and that constitutes a complete loss of service at the Site or Circuit and in respect of a Resilient Service, excluding any loss of service of a Resilient Component where you still have access to the BT Managed Web Application Firewall Security Service through the other back-up Resilient Component.

"**Site Planning Guide**" means a guide provided by BT to you detailing the hardware specification, including environmental, physical and electrical details of any BT Equipment provided to you with the BT Managed Web Application Firewall Security Service.

"**SLA Category**" means the category, as set out in the Order which, in accordance with the table set out at Paragraph 13.2.2, specifies the following in relation to the BT Managed Web Application Firewall Security Service, Site or Circuit:

(a) Availability Annual Target;
(b) Maximum Annual Availability Downtime;
(c) Maximum Monthly Availability Downtime;
(d) Standard Availability Service Credit Rate;
(e) Elevated Availability Service Credit Rate; and
(f) Service Credit Interval.

"**SSL**" means secure sockets layer.

"**SSL Encrypted Traffic**" means encrypted traffic transferred via the following protocols that BT will support for SSL/TLS Inspection:

(a) HTTPS;
(b) SMTPS;
(c) POP3S;
(d) IMPAS; and
(e) FTPS.

"**SSL/TLS Inspection**" means the Service Option as set out in Paragraph 2.1.6.
"**Standard Availability Service Credit Rate**" means the applicable rate as set out in the table at Paragraph 13.2.2 for the relevant SLA Category.
"**Standard Service Components**" has the meaning given in Paragraph 2.
"**Supplier**" means Fortinet Inc, 899 Kifer Road, Sunnyvale, CA USA or Fortinet Singapore Pvt Ltd, Beach Road, #20-01, The Concourse, Singapore 199555, as applicable.
"**Trust Chain**" means where the browser platform checks whether or not the root certificate authority is explicitly trusted by the browser platform.
"**Uniform Resource Locator**" or "**URL**" means a character string that points to a resource on an intranet or the Internet.
"**VPN**" means a virtual private network with the use of encryption to provide a communications network that appears private to your Users while being provided over network infrastructure that is shared with other customers. Unless otherwise agreed in writing, your communications over your VPN are restricted to those Sites belonging to your VPN.
"**Wide Area Network**" or "**WAN**" means the infrastructure that enables the transmission of data between Sites.