Service Management Schedule - PLUS

Section A – Summary

1. SUMMARY

1.1 This document sets out the service management functions that will be performed for the Service and as further set out in the Order.

1.2 BT will provide a managed service including a service desk, proactive monitoring, management, and maintenance of the Services.

1.3 For the purposes of this Schedule, the "Services" refer to those services identified as falling within the scope of the BT Service Management Boundary.

1.4 BT will provide and maintain a set of operational service management processes that enable the management of the services.

1.5 Some day-to-day operational procedures will be set out in the Customer Handbook, which will be referred to frequently within this Schedule but will be provided as a separate document to Customer.

1.6 Termination Charges for the managed service element set out in this Service Management PLUS Schedule are not applicable, however, the Order will contain the Termination Charges which may apply to each product that forms part of the Service.

1.7 In the event of any conflict, the terms set out in this Service Management PLUS Schedule will prevail over any service management terms set out in the respective service schedules.

Section B – The Service

2. SERVICE GOVERNANCE

2.1 Monthly Service and Operational Review

2.1.1 The monthly Service and Operational Review Board will cover technical and operational aspects of the Service including incidents, problems, and changes.

2.1.2 The service manager will host a specific service management monthly conference call, unless otherwise agreed between BT and Customer.

2.2 Quarterly Executive Review Board

2.2.1 The Executive Review Board will review and report on the overall delivery of the Services on a quarterly basis. The Executive Review Board will focus on the mid/longer term service delivery aspects and will serve as the platform for reporting on technical review and innovation, upcoming new service offerings and upgrades/ improvements to the existing Services.

2.2.2 The business manager will host a specific service management quarterly conference call, supported by the service manager and technical design authority (TDA), or as otherwise agreed between BT and Customer.

2.3 Bi-Annual Strategic Review Board

2.3.1 The Strategic Review Board will be responsible for overseeing the success of the overall relationship, focusing on the needs and expectations of Customer's business.

2.3.2 The business manager will host a strategic review of the services bi-annually via a conference call unless otherwise agreed between BT and Customer.

2.4 Customer Handbook

2.4.1 The Customer Handbook is a document agreed with Customer and prepared by BT during service transition. The Customer Handbook will include:

(a) the high-level Service scope specific to Customer;

(b) administrative and operational procedures for interaction between Customer and BT for the provision of the Services;

(c) communication methods;

(d) incident escalation procedures;

(e) contact details for key personnel;

(f) any defined planned maintenance schedule; and

(g) Major Incident procedures.

2.5 Language

2.5.1 All communications, whether spoken or written, will be in the English language, unless otherwise agreed. Note that other language capabilities are available as an upgraded service option (if chosen, this will be shown on the Order).

2.6 Hours of Service and Communication Methods

2.6.1 Hours of operation for most functions are 09:00 – 17:30, Monday to Friday, UK hours (excluding local bank holidays), except for the Service Desk and incident management which are available 24x7.

2.6.2 For all functions, there are several methods available for Customer to communicate with BT.

2.6.3 Details of key contacts and how to contact for all service functions will be provided in the Customer Handbook.

3. SERVICE DESK

3.1 Scope of Service Desk

3.1.1 The service desk performs the following functions:

(a) incident management;

(b) problem management;

(c) monitoring and event management; and

(d) change enablement.

3.1.2 The service desk also works closely with the configuration management team to ensure the reliability of the service.

3.1.3 The service desk:

(a) acts as a single point of contact for incidents, escalations and queries relating to the Services;

(b) is available 24 hours a day, 7 days a week to receive incidents and escalations; and

(c) is responsible for the management and resolution of all incidents, problems, and changes throughout their lifecycle.

3.1.4 BT will deploy standard systems and tools to support the services.

3.1.5 Customer will be supported from a shared-desk environment and will not receive a dedicated team of service desk staff, unless selected as an upgraded service option.

3.2 Location of Service Desk

3.2.1 The service desk will be located in one of BT's global hubs. If BT needs to relocate the assigned service desk, BT will formally request this change in writing and manage the move through the change enablement process. Customer cannot unreasonably withhold or delay its consent.

3.2.2 BT will not permanently locate any personnel at any Customer site.

4.   INCIDENT MANAGEMENT

4.1   Scope and Obligations

4.1.1   Incident management involves diagnosing and resolving incidents so that services can be restored to normal business operations as quickly as possible.

4.1.2   BT will:

(a)   only progress incidents that are within BT's Service Management Boundary;

(b)   take responsibility for coordinating and managing each incident from the time the incident is created within BT's incident management system, through to its resolution or reassignment to Customer, as applicable;

(c)   provide incident management using a professional, multi-skilled team from the assigned global hub;

(d)   assign the incident to a service reliability engineer with the relevant skills to resolve the incident at first contact wherever reasonably possible; and

(e)   progress incidents in line with the contracted service levels and the contracted hours of service.

4.2   Incident Creation

4.2.1   Incidents will be identified in one of two ways, either:

(a)   proactively detected by BT's monitoring systems; or

(b)   reactively reported by Customer to BT (whether via the Customer's own service desk or via a third party/service partner service desk) using the contact methods set out in the Customer Handbook.

4.2.2   All incidents are recorded on BT's standard incident management system. Once created, a system generated message is sent to Customer providing a unique reference number and priority level.

4.3   Incident Response and Keeping the Customer Informed

4.3.1   Throughout the lifecycle of the incident, BT will keep Customer informed at regular intervals and whenever there is a significant update. Updates will be via eBond/API or the BT My Account Portal.

4.3.2   The incident clock starts when the incident is recorded in the BT incident management system. Response time is measured from the time an incident record is created until Customer has been informed that the incident has been received and is being worked on.

4.3.3   When BT is waiting for further information or input from Customer, or when the incident falls outside of the contracted hours of service, the incident clock will be suspended. It will be restarted once input has been received or when the service is back within the contracted hours of service. During any suspension time, there will be no status updates and any affected SLAs are disapplied.

4.4   Prioritisation

4.4.1   Priority levels are based on impact (the severity of the situation) and urgency (how important and business critical the site or service is to Customer). Customer's core sites and core business functions (where a total outage would cause material business impact) will receive a higher urgency level than sites hosting non-essential business functions (where a slower response to a total outage would not cause material business impact).

4.4.2   Customer's core sites are set out in the Order. Core business functions should never be hosted at sites with no resiliency, to reduce the risk of those core functions being unavailable. If core sites need to change during the lifetime of the Services, Customer will inform BT in writing (which may require an uplifting in the resiliency at the site, if necessary, via the service request process).

4.4.3   Incident priority levels are assigned as follows:

(a) P1 – one or more core sites or services are completely unavailable, or one or more core business functions are completely unable to be performed. For user-based services (e.g. MS Teams), this would typically be all users;

(b) P2 - material impact to business e.g. a partially interrupted or impaired service which cannot be mitigated, or core business functions can be performed but in a reduced capacity. This priority level would also apply for the loss of a non-core site or service;

(c) P3 - medium impact to business, e.g. a site or service experiencing intermittent or localised interruption or impairment. This might be an issue where a large percentage of a business is functioning normally, such as the site is suffering slow response, but users are able to work, a small number of users at a site have total loss of service but the majority are functioning normally, or perhaps one element of service is unavailable, such as access to voicemail. A P3 incident would also be raised for a resilient site where either the primary or resilient path is unavailable;

(d) P4 - typically very minor or no business impact, such as a single user or very small number of users having minor issues, but core business functions can be carried on as normal.

4.5 Downgrading of Priority Levels

4.5.1 If an incident is found to have been caused by a Customer power related issue, Customer induced (i.e. caused by an issue within the Customer's own scope of responsibility), or planned maintenance work, the priority level will be downgraded. In each of these cases, the Customer will be informed, with reasons, prior to downgrading the priority level to P4. These types of incidents will also be excluded from any availability SLA measurements.

4.6 Escalation

4.6.1 BT will automatically escalate incidents if they hit certain trigger thresholds during the incident management process. However, BT acknowledges that there may be times when the Customer may want to escalate an incident itself. In this case, the Customer will need to follow the escalation process defined in the Customer Handbook.

4.6.2 BT operates a 5-level incident escalation model:

(a) level 0: BT service desk;

(b) level 1: service desk shift leader;

(c) level 2: service desk duty manager;

(d) level 3: service desk operations manager;

(e) level 4: service desk director / global escalation manager;

(f) level 5: VP, service assurance / head of global escalation management.

4.6.3 The key principles of escalation are as follows:

(a) escalations will only be handled for active service-impacting incidents (priority 1-3);

(b) to escalate, Customer should always contact the BT service desk (Level 0) to perform escalations. The BT service desk will then escalate to the right level within BT to ensure appropriate action is taken; and

(c) incidents related to matters beyond BT's reasonable control cannot be escalated (e.g. force majeure incidents). These types of incidents will also be excluded from any availability SLA measurements.

4.7 Incident Investigation and Diagnosis

4.7.1 BT will carry out necessary diagnostics to identify the cause of the incident and devise a plan to resolve it. BT will engage with Customer's service desk if further information is required to assist the diagnosis and resolution of the incident.

4.8   Restoration and Closure

4.8.1   BT will restore service by addressing the root cause of the incident or providing an acceptable workaround agreed with Customer.

4.8.2   When a potential solution has been identified, BT will test it, apply it and document it in the BT incident management system.

4.8.3   Where possible, BT will resolve incidents remotely. Where this is not possible, the BT service desk will engage with resolver groups and third-party suppliers, as required, and co-ordinate the resolution of the incident.

4.8.4   If an engineer is required to attend site, Customer will be required to provide reasonable access so that BT can remedy the incident. If the site is not accessible 24/7, the engineer will attend on-site the following business day and the incident ticket clock will be suspended during the hours in which site access is not available.

4.8.5   When BT determines that the incident is resolved, the ticket will be marked as resolved and Customer will be informed. BT will verify with Customer to make sure that Customer is reasonably satisfied that the incident is resolved before BT closes the incident ticket. If the incident is still not resolved for any objective reason, BT may carry out further diagnostics until the incident is remedied. Note that availability SLA downtime is measured until the timepoint when the ticket is marked as resolved by BT. Where reasonably appropriate, BT will continue to measure availability SLA downtime until resolution is confirmed. If BT is unable to reach Customer to confirm incident resolution, BT will attempt to contact Customer three times in total, at regular intervals, before automatically closing the incident ticket.

4.8.6   BT keeps a record of all incidents, including the cause of the incident and what action has been taken to resolve.

4.9   How to Report an Incident

4.9.1   Customer may raise incidents with BT 24 hours a day, 7 days a week via:

(a)   an API integrated with Customer's toolset, if available. This will be the primary and preferred method;

(b)   an E-bond integrated with Customer's toolset, if available. This is the preferred method if the API solution isn't available;

(c)   telephone – the number for the BT service desk can be found in the Customer Handbook. Telephone contact should only be used to report incidents in emergency situations; and

(d)   the BT My Account Portal.

4.9.2   Details of all these contact methods are set out in the Customer Handbook.

4.10   Major Incidents

4.10.1   Identify Major Incident

(a)   If an incident is categorised as "major" (i.e. highest-impact, highest-urgency), then the Major Incident Management ("**MIM**") procedure applies. A major incident includes where a large number of Sites, geographies and Users are impacted, and the Customer is deprived of one or more crucial Services ("**Major Incident**"). A P1 incident would not normally be classified as a Major Incident, however, a Major Incident will always be associated with a P1 incident ticket.

(b)   BT may also use the term Major Service Outage where a Major Incident has been identified. A Major Service Outage is used to describe an event or threat that spans multiple customers or BT lines of business and follows the MIM procedure described in this Section 4.10.

4.10.2   Engage Major Incident Management

(a)   On identification of a Major Incident, the BT service desk will notify the dedicated Major Incident Management function to seek support. To ensure the Major Incident Management function

can properly assess the incident, the BT service desk provides a standard set of key information. In the event that demand for Major Incident resources is higher than can be effectively handled by the Major Incident managers on duty, BT will prioritise the Major Incidents using the following criteria:

(i) safety of life issue;

(ii) actual business impact to the Customer; and

(iii) possible BT/Customer brand damage.

(b) The Major Incident function will always validate a Major Incident to be certain that it meets Major Incident criteria. This is done to ensure that the full focus remains on genuine Major Incidents.

4.10.3 Initiate and Conduct Communication

(a) The Major Incident function will provide status updates on any Major Incident which has an impact on the Customer's Service. Updates will go to the Customer and other key stakeholders, including senior management within BT. Notifications will be sent at key points throughout the life of the incident. As a minimum, this will be at the point that the incident is declared as a Major Incident, at resolution and at closure. The notifications will be issued in a standard format and will include detail of the current impact of the incident, current situation, and next steps.

(b) Where required, BT will also attend bridge calls with the Customer to ensure incident progression. The BT service manager will normally represent BT in such cases.

(c) Up-to-date contact details are maintained to ensure communication is sent to the correct Customer contacts.

(d) The Major Incident function will also maintain a log of relevant facts and a timeline for the Major Incident. This information may be used for post-incident review purposes and to identify any lessons learned or improvement actions.

4.10.4 Establish and Conduct Technical Bridge

(a) Once engaged, a Major Incident manager will participate in ongoing technical bridge calls throughout the Major Incident lifecycle. The Major Incident manager is the single point of contact representing BT in the technical bridge for the duration of the incident, responsible for leading and driving the actions needed to resolve the incident.

(b) The Major Incident function works in collaboration with the service desk, duty managers, operations managers, and client services, ensuring that appropriately skilled experts are invited to the bridge as required.

4.10.5 Resolve Major Incident

(a) All necessary technical resources will be allocated to enable a rapid resolution of the Major Incident and the Major Incident manager will drive and lead the activities required to resolve the incident. When BT has identified a potential resolution, it will be tested, applied, and checked for successful restoration.

(b) Actions taken will be documented in the incident case record. The change enablement function may be involved to manage any emergency changes required to implement a fix or work-around.

4.10.6 Confirm Closure

(a) Once the issue is resolved, BT will check with Customer to confirm impact is mitigated before closing the incident. If it is not resolved, BT will carry out further diagnostics until the incident is fixed.

(b) If the service is restored by a workaround, the Major Incident is demoted to a regular incident and then follows the standard incident management process.

4.10.7   Review Major Incident

(a)   Following closure of a Major Incident, BT conducts a comprehensive internal review. This will look at the timeline of the incident, activities undertaken, root cause and any lessons learned. Any follow up activities required will be captured to ensure progression. A problem record is raised if further work is required to establish the root cause and identify a permanent fix (in cases where the incident has been resolved by a workaround).

5.   PROBLEM MANAGEMENT

5.1   Primary Objective

5.1.1   BT manages problem tickets using a standard toolset to prevent incidents from occurring, eliminate recurring incidents and minimise the impact of incidents that cannot be prevented. A problem is characterised as the cause of one or more incidents. The effective management of problems is essential to reduce and mitigate the risk of new or recurrent service interruptions or degradation.

5.2   Scope and Obligations

5.2.1   All assets falling within the Service Management Boundary are included within the problem management function.

5.2.2   ITIL best practice processes are followed by BT to manage problems throughout their lifecycle. Problem tickets are managed using BT's standard toolset.

5.2.3   BT will:

(a)   identify problems both reactively and proactively as described in paragraph 5.3 below;

(b)   classify problem tickets in order to address the most significant problems first;

(c)   carry out detailed investigations to understand the root cause of the problem;

(d)   keep Customer informed of progress;

(e)   where further activity is required, deliver a documented action plan; and

(f)   define and implement measures to avoid the recurrence of problems.

5.3   Problem Creation

5.3.1   BT will identify problems both reactively and proactively:

(a)   reactively in response to a P1 incident that has already occurred and where the root cause is unknown; and

(b)   proactively when trend analysis highlights potential service issues. Trending information may come from a review of incidents, or from data provided by other service management functions (e.g. event, change, availability or capacity management). When assessing trends, a problem ticket is raised if trend analysis has identified three or more repeat occurrences on the same device or service, within a three-month period.

5.4   Root Cause Analysis

5.4.1   BT will carry out detailed investigations to understand the root cause of a problem. Once the root cause is established, BT records a "known error" in its centralised knowledge management system and notes details of any work-around. This helps BT's service team when resolving any related incidents which might occur prior to a fix being made available for the underlying problem. By doing this, the impact to Customer's services during the period where a permanent solution is being pursued is minimised.

5.4.2   BT will keep Customer informed of progress during this phase with a root cause analysis (RCA) report for any problem that has been raised for a P1 incident. BT aims to provide this within 10 days of the problem occurring. In addition, where further activity is required, BT will aim to deliver a documented action plan within a further 10 days of delivery of the RCA report.

5.4.3 Once the root cause is known, investigations will continue until BT has found a permanent fix for the problem.

5.5 Resolution and Closure

5.5.1 Where problem resolution requires a change to the Service, BT will manage this change through appropriate change governance. This will depend on the specific details of the change required. For example, a change requiring an amendment to Configuration Items (CIs) will go through BT's change enablement function. Whereas a change relating to a vulnerability issue will go through BT's vulnerability management function. Regardless of the type of change required, BT's focus is on making sure that the proposed solution fully remedies the identified problem and that the fix is carried out in a controlled manner which minimises the risk to Customer.

5.5.2 Once a resolution has been implemented, BT will carry out a period of monitoring to confirm that the problem has been eliminated. At this point, BT will close the problem ticket and associated known error.

5.5.3 In some cases, it may not be appropriate for a solution to a problem to be implemented and BT will discuss options with Customer. To ensure that an informed decision is reached, the following considerations will be considered:

(a) the impact and risk of not implementing a permanent solution;

(b) the cost effectiveness of implementing a permanent solution;

(c) the resources required to implement a permanent solution;

(d) the timing of implementation and the impact on the Service; and

(e) whether a workaround is more viable and equally effective in dealing with the problem.

5.5.4 Where a decision is made not to implement a solution (e.g. due to cost, equipment which is end-of-service life or a known vendor bug), BT will record a status of "unresolved" in BT's known error database. In these circumstances a related risk will be raised and shared.

5.5.5 When a permanent solution is not implemented because Customer instructs BT to not fix the problem, any resulting incidents which cause SLA breaches will be excluded from SLA reporting and service credit payments.

6. MONITORING AND EVENT MANAGEMENT

6.1 Primary Objective

6.1.1 The purpose of monitoring and event management is to detect any changes in the operational status of the Services and to take action in order to reduce incidents, maximising service availability and reliability, and to identify issues before they cause any service disruption.

6.2 Scope and Obligations

6.2.1 BT utilises industry-leading systems and tools to provide a 360° view of assets with monitoring capability within the Service Management Boundary. Services are monitored 24 x 7, and action is taken when changes in operational status is detected.

6.3 Monitoring

6.3.1 Standard alert thresholds will be established for assets with monitoring capability within the Service Management Boundary.

6.3.2 When a change of operational status is detected, an alert is generated, categorised, time stamped and, where appropriate, an incident is auto-generated in BT's management tools.

6.3.3 Examples of changes in operational status include:

(a) breaches of thresholds;

(b) unexpected changes;

(c) service degradation;

(d) patterns of symptoms (which could lead to potential issues); and

(e) when failures have occurred.

6.4 Event Management

6.4.1 When an alert results in an incident ticket, it becomes the responsibility of the service desk to own the incident through to resolution following the process defined in this Schedule. Incidents will be progressed in line with contracted service levels. When a problem ticket is generated, it is progressed in accordance with the process outlined in this Schedule.

6.4.2 All alerts are analysed for patterns and hot-spots and event trend reports are created to support the problem management function and to enable BT to refine event thresholds.

6.4.3 When areas which have the potential to impair the performance of the Services are identified, BT will use all reasonable endeavours to act before they impact Customer, thereby maintaining the quality of the Service. Actions are taken via problem management, change enablement and in discussion with Customer.

6.4.4 Events are closed once an incident or problem ticket has been created or, where no further action is needed, the event will automatically clear itself. In all cases, the events remain stored in the event database, allowing for correlation if there are repeat alerts.

7. CONFIGURATION MANAGEMENT

7.1 Primary Objective

7.1.1 The purpose of configuration management is to maintain and improve the components of the service and maintain accurate configuration information on the current and planned state of the infrastructure providing the service.

7.2 Scope

7.2.1 BT will:

(a) maintain an accurate Configuration Management Database (CMDB) for all assets within the Service Management Boundary;

(b) deploy auto-discovery tools to aid maintenance of an accurate, up-to-date inventory;

(c) archive configuration files for all managed Configuration Items (Cis) and restore the configuration in the event of a failure;

(d) store information on the configuration of Customer's devices to enable BT to define and control the components and to support other ITIL functions;

(e) seek formal approvals for all releases and changes into controlled environments; and

(f) manage CIs using the standard BT strategic toolset from asset discovery, configuration identification, control, verification, and audit until decommission.

7.3 Configuration Management Planning

7.3.1 BT will produce a configuration management plan which sets out the approach BT will take to control, verify, and maintain accurate CIs. The plan will also detail which parts of Customer's IT infrastructure will need a CI record, along with:

(a) attributes / relationships that will be recorded;

(b) items BT will manage under the change enablement process; and

(c) roles, responsibilities and process activities, procedures, and relationships with other ITIL practices.

7.3.2 Planning activities cater for the introduction of new configuration management requirements and ensures that only required data is handled, and redundant CIs are archived or purged.

7.3.3 The configuration management plan will be agreed with Customer and will be used to manage Customer's CIs. The plan will be reviewed annually, and any necessary updates (including new service types) will then be added.

7.4 Identify Configuration Types and Items

7.4.1 Through configuration identification, BT will gather information on CIs that will support configuration management objectives (as defined in the configuration management plan). This is a one-off activity that takes place at service commencement. A configuration baseline is made before the deployment of a release into the live environment.

7.4.2 CIs are uniquely identified and are recorded in the CMDB.

7.5 Maintain and Control CIs

7.5.1 The information recorded for each CI will ensure effective control and will include:

(a) a description of the CI and its attributes;

(b) the relationship between the CI and other CIs;

(c) the relationship between the CI and other service components, e.g. software and licenses.

(d) the status of the CI;

(e) the IOS version;

(f) the physical location; and

(g) any SLAs associated with the CI (if appropriate).

7.5.2 Only authorised / identifiable CIs under BT's change enablement will be accepted and recorded from the point of receipt to decommissioning. No CI will be added, modified, replaced, or removed without the appropriate controlling documentation e.g. approved request for change.

7.5.3 BT will archive configuration files and restore the configuration if there is a network failure. Archive files will be prepared each week and the last three configurations for each device will be stored. Customer may request the restoration of configuration files for any other reason provided that the total number of restorations made in any operational year, starting on the service commencement date, does not exceed a sum equivalent to three restorations per device per operational year.

7.5.4 BT manages the CMDB to maintain reliability and accuracy, including control of update access.

7.5.5 Note that CIs may exist within the CMDB that are not under BT's management. BT is not responsible for the proactive monitoring, maintenance or accuracy of the data held for these CIs. Should Customer need the information to be updated, Customer must raise a service request which will be managed via the change enablement process.

7.6 Audit, Configuration and Data Quality

7.6.1 BT will audit CIs under BT's management on a monthly basis to ensure both the inventory and the configuration are accurate and that the CMDB remains reconciled with:

(a) content associated with orders (service requests) held in BT's service delivery systems;

(b) data in BT's configuration management and monitoring tools (so that BT can manage the device and predict / resolve issues before they become service affecting); and

(c) the correct operating system (OS) and firmware versions.

7.6.2 BT uses auto-discovery tools (with manual activity when required) to discover and audit devices, and to allow reconciliation with the data held in the CMDB. Audits significantly contribute to the reliability of the service as they bring a high level of inventory accuracy.

7.6.3 Corrective action is taken where discrepancies are identified by the audit. This is performed automatically via the auto-discovery tool or, where necessary, manually.

8. CHANGE ENABLEMENT

8.1 Primary Objective

8.1.1 The purpose of change enablement is to minimise the risks associated with operational changes (additions, modifications, or removals) to ensure that the service remains reliable and functioning at a high operational level.

8.2 Scope

8.2.1 All assets within the Service Management Boundary are included within the change enablement function.

8.2.2 Change detail will be communicated effectively and disruptions avoided. If impact to the Service is expected, BT (or BT's suppliers) will schedule work outside of business hours to avoid impact to Customer's business functions (unless they are approved to be carried out during business hours or necessary emergency changes which need urgent action to mitigate a bigger risk).

8.2.3 BT will:

(a) test change plans (wherever possible) and have back-out plans;

(b) validate and approve changes, including implementation timelines;

(c) carry out changes during the agreed change window. If impact to service is expected, work will be carried out outside of business hours to mitigate the impact;

(d) wherever reasonably possible, seek approval from Customer before commencing any emergency changes which need to be carried out straight away;

(e) carry out changes to agreed specifications (i.e. no fall back to the original status should be required);

(f) not back out or roll back changes whenever possible;

(g) aim to carry out changes without causing incidents; and

(h) progress changes in line with the contracted service levels and contracted hours of service.

8.3 Review and Assess Change

8.3.1 All changes are reviewed and, where applicable, the configuration item detail in the CMDB is checked. If more detail is needed to evaluate the change, BT will contact the change initiator.

8.3.2 A change assessment is conducted to properly understand the implications of the change looking at factors such as risk, benefit, impact, resources required to deliver, and testing requirements.

8.3.3 BT will undertake change scheduling, looking for potential conflicts, assessing the level of risk and considering whether a change should be scheduled out of hours. Scheduling is performed in a way that will cause minimal disruption to the Service.

8.3.4 For emergency changes, BT will assess and implement the change in the fastest practicable timeframe to mitigate any greater risk to the services. Wherever reasonably possible, BT will attempt to gain Customer's approval in advance. Where an emergency change is implemented outside of contracted hours, the change record will be raised retrospectively.

8.4 Authorise (Approve) Change

8.4.1 The approval stage is crucial to ensuring the success of the change. Prior to seeking any formal approval from Customer, BT will verify that the change has been properly prepared for and conduct an internal validation to confirm this.

8.4.2 BT will send Customer details of normal changes, via email, to provide input as required and to provide approval. BT will record the outcome in the work log, to meet audit compliance requirements. For emergency changes, wherever reasonably possible, BT will seek approval prior to change implementation.

8.4.3 The updated forward schedule of change (FSC) is made visible to Customer and other relevant stakeholders following approval for change deployment.

8.4.4 If there are any issues regarding scheduling during the authorisation phase, BT will investigate and re-schedule if needed.

8.4.5 In addition to normal and emergency changes, BT also manages standard records only, and planned network changes. All change types are explained as follows:

(a) normal changes - this means all changes that need formal approval, scheduling and authorisation to implement. They are generally complex operational changes which may be part of wider project management activity or underpin a complex service request;

(b) standard changes - these are pre-approved as they are simple and repeatable activities with minimal risk and impact. The risk, impact and urgency levels are generally set to low by default;

(c) emergency changes - these are changes that are expedited due to a service breakdown and will be implemented against a P1/P2 incident only;

(d) records only changes - these are pre-approved changes, which are raised with the sole intention of updating or adding CI data within the (CMDB). Risk, impact and urgency levels are set to low; and

(e) planned engineering works (PEW) - these are changes that BT, or BT's suppliers, are planning and scheduling which may impact the Services. They are planned in advance, providing a 360° holistic view to global service desks and customers with a forward schedule or calendar of change from BT.

8.4.6 Where required, BT will review these categories with Customer and amend / update if appropriate.

8.5 Implement Change

8.5.1 Where practicable, BT will minimise risk by undertaking the build and test of the change deployment in a non-production scenario. Doing it this way means that any timed activities are proven and tested. BT then uses this information to shape implementation plans, which will also include any back-out arrangements that may be needed if the change is unsuccessful.

8.5.2 Prior to implementation, BT will seek final authorisation from Customer for the change to proceed. BT will then co-ordinate the implementation of the change, ensuring that all resources are aligned, and all risks are mitigated. When the change is completed, BT will record the outcome in consultation with the implementation team.

8.5.3 In relation to incidents and problems, BT's multi-skilled, multidisciplinary teams will work collaboratively to quickly identify, understand, and implement any changes that are needed to proactively resolve issues identified. In some cases, this may mean that a change may be able to be implemented before there is any noticeable impact to service.

8.6 Close Change Record

8.6.1 BT will carry out testing to confirm the change has been successful, and then close the change record.

8.6.2 If for any reason the change is not successfully implemented, BT will record the findings of any associated review, including any reasons for agreeing to cancel or back-out the change.

9. SERVICE RELATIONSHIP MANAGEMENT

9.1 Primary Objective

9.1.1 The service manager manages the service relationship with Customer and acts as Customer's primary contact for all service matters (issues, complaints, or queries) which will be dealt with in a timely and structured way. The engagement with Customer centres around commitments, meetings, reports and promoting a healthy operational service relationship with key stakeholders in the Customer business.

9.2 Scope and Obligations

9.2.1 BT will provide a named service manager to work closely with Customer, who will be responsible for the following:

(a) provide a Customer Handbook;

(b) prepare and host monthly service review meetings (via MS Teams meeting or phone);

(c) provide monthly reporting covering service performance, trends and recommendations;

(d) provide service level management (see Section 10);

(e) own service improvement plans (see Section 11);

(f) drive continual improvement;

(g) schedule regular conversations and pulse calls;

(h) work with Customer to understand service strategy, key requirements and priorities; and

(i) provide service escalation management when required.

9.3 Building the Key Documentation

9.3.1 **Customer Handbook**: provides the Customer with information about the products, services, and interactions with BT during the lifecycle of the contract – see Section 2.4 for more details.

9.3.2 **Service Improvement Plan (SIP)**: documenting actions needed to overcome poor service performance, perception, or issues. The service manager will capture actions and oversee and report on progress on a regular basis. See Section 11 for more details.

9.3.3 **Performance Reporting**: a monthly report covering the key aspects of service – see Section 10.4 for more details.

9.3.4 **Data and Trend Analysis**: building on the data used to produce the monthly reports to create a picture of Customer's evolving service requirements. This data will enable a degree of prediction for future demand and help the service manager make recommendations for improvements.

9.3.5 **Change Management Tracker**: a simple document detailing changes expected in the next reporting period and beyond plus details of any changes that have failed implementation in the current reporting period. A commentary for each change will be captured and can be used to highlight issues. This information may be presented with the support of a change manager or project manager. It will be reviewed regularly with Customer at service review meetings.

9.3.6 **Planned Engineering Work Notifications**: the service manager will maintain this list.

9.3.7 **Risk Register**: the service manager will maintain a register of known risks pertinent to Customer's service.

9.3.8 **Key Contacts**: the service manager will maintain a list of key customer contacts and key change authorisers.

9.4 Service Review Meetings

9.4.1 Service review meetings occur once a month. Ahead of the meeting, the service manager will gather the key information and issue minutes of the previous meeting ahead of the review.

9.4.2 The service manager will endeavour to provide updates on all outstanding actions and activities. Additionally, copies of the most recent monthly reports, trends, and other pertinent issues (such as Major Incidents) will be available ahead of the meeting.

9.4.3 The service review meetings are used to assess how the service is performing against contractual targets, measures, and customer expectations, as well as to take action if expectations and performance are falling short. These meetings are also a forum for understanding Customer's evolving business needs and aligning service support to fulfil the requirements.

9.4.4 A typical service review meeting will review the service performance for the period, performance against SLAs, capture up and coming changes, address problems and capture future activities. Where performance is failing to achieve contractual standards, these meetings will also be used to build a Service Improvement Plan and will measure achievements against this plan in subsequent meetings.

9.4.5 Relevant BT personnel may occasionally attend the meetings to discuss specific topics - the service manager will organise attendance where required.

9.4.6 The service manager will chair the meeting and issue minutes and actions following the meeting.

10. SERVICE LEVEL MANAGEMENT

10.1 Primary Objective

10.1.1 Service level management capability is designed to ensure that the Services are delivered to a high level and that performance meets the contractual commitments made to Customer. Service level management proactively monitors performance against Customer's SLAs to identify potential (jeopardy) or actual SLA breaches, collects evidence to support investigations of confirmed breach(es), identifies remedial actions, and reports on SLA performance.

10.2 Scope and Obligations

10.2.1 BT will:

(a) monitor performance against SLAs and implement remedial actions to prevent SLA breaches or avoid recurrence of breaches;

(b) where appropriate, instigate service improvement initiatives;

(c) report on SLA performance on a monthly basis, providing a report to be used at the monthly service review meeting; and

(d) review the SLAs annually to ensure they remain suitable throughout the lifetime of the contract and drive the expected performance.

10.3 Monitor Ongoing Service Performance and Address Breaches

10.3.1 BT will monitor SLA performance to identify potential or actual breaches, against the contractual SLAs, across all ITIL functions and Services which have SLAs associated with them.

10.3.2 When an actual or potential SLA breach is identified, BT will collect evidence to understand the breach and help identify any remedial action required to prevent a future breach or mitigate the impact of the breach.

10.3.3 When remedial action is required, BT will work to develop a solution, implement the agreed solution and monitor its success in addressing the breach. Solutions will vary; for example, they could be quick tactical amendments to ways of working, or more significant pieces of work where progress needs to be tracked over a period of time. Where appropriate, BT will record a service improvement initiative in a service improvement plan and solution delivery will be managed under continuous service improvement. Progress will be reviewed with Customer regularly.

10.4 Create Performance Review Pack

10.4.1 BT will collect performance data for input into the monthly performance report, evidencing the performance against the contracted SLAs. Data may come from a variety of functional areas, such as incident management, problem management, configuration management, change enablement, capacity management, commercial, project and / or technical service teams.

10.4.2 The data will be reviewed and verified before creating the monthly performance report, which will typically include performance against both SLAs and key measures, progress against outstanding issues, action updates, information relating to improvement initiatives and risks, "good news" stories and any other performance related information relevant to the contract. This performance summary is produced and supplied on a monthly basis, prior to the service review.

10.5 Review SLAs During Contract Lifetime

10.5.1 During the lifetime of the contract, to ensure the SLAs are measuring performance to Customer's reasonable satisfaction, BT will carry out periodic reviews of the SLAs, identifying any changes needed to remove redundant SLAs, potentially add new SLAs, or revise existing SLAs. Any identified suggestions for changes will be discussed and agreed with Customer and, where required, the BT commercial team and any necessary contractual amendments will be made via the contract change process.

11. CONTINUAL IMPROVEMENT

11.1 Primary Objective

11.1.1 There are two distinct parts to the continual improvement function. Firstly, it is designed to ensure that the contracted Services are delivered at a high level of quality and ensure any shortfalls are addressed. Secondly, it is to ensure BT's understands Customer's changing business needs and can make recommendations for improvements during the lifetime of the contract.

11.1.2 This capability proactively identifies and ensures delivery of improvement initiatives to BT's practices, processes, products, relationships, resources, or any other area where there is an opportunity for a service improvement to be made.

11.1.3 Ongoing improvement is focused on understanding Customer's business vision, goals, and objectives, and how well BT's services are aligned. By establishing where improvements can be made, effective plans are created and actions taken to ensure timely delivery, with regular reviews and tracking of progress.

11.2 Scope

11.2.1 BT will:

(a) put in place improvement initiatives where any contractual commitments are not being met;

(b) proactively identify improvement opportunities which will enhance the Services delivered;

(c) work with Customer to gather insight into Customer's changing business needs and make recommendations for service improvements to meet those changing needs;

(d) manage delivery of improvements, addressing deficiencies in a reliable, structured and consistent way;

(e) assess improvement initiatives to verify alignment with Customer's business vision, goals and objectives prior to progressing those initiatives;

(f) conduct a cost/benefit analysis to make sure delivery of improvement initiatives are worthwhile;

(g) prioritise delivery of improvement initiatives to ensure benefit is delivered in the most effective and efficient way;

(h) record and track improvement initiatives within a service improvement plan;

(i) regularly review progress of initiatives to ensure good progression;

(j) following delivery of an improvement, assess whether the anticipated benefits were achieved;

(k) the SRM will be responsible for ensuring the continual improvement capability functions effectively; and

(l) where any suggested improvement initiatives require a contract change, this will be discussed and agreed with Customer and the BT commercial team before any amendments are made via the contract change process. Some changes may result in additional costs.

12. SERVICE REPORTING

12.1 Primary Objective

12.1.1 Monthly reporting aims to provide Customer with easily understandable information to demonstrate current performance of Customer's services and help plan for the future.

12.2 Scope

12.2.1 BT will:

(a) create a monthly reporting pack detailing the overall performance of your services ahead of the monthly service review;

(b) provide information on exceptional items requiring focus and discussion;

(c) ensure the report is in a format that is easily interpreted; and

(d) provide reporting for each of the service functional areas within Customer's service wrap.

12.2.2 Details of specific report items, which will mirror the service options in the Customer's Order, will be provided within the Customer Handbook.

13. KNOWLEDGE MANAGEMENT

Note: this section only applies if Knowledge Management has been purchased as a feature and is included in the Order.

13.1 Primary Objective

13.1.1 Knowledge management is the process of gathering, analysing, storing, and sharing knowledge that is created within a service organisation. It is the one central process responsible for sharing knowledge to all other ITIL service functions, ensuring BT has access to the latest knowledge for Customer's account, to enable the right decisions throughout the service lifecycle and incident resolution process.

13.2 Scope

13.2.1 BT will:

(a) create a Knowledge Database and provide training to users to ensure usability, ease and searchability to enable quicker problem-solving;

(b) collaborate with the BT support functions to identify knowledge requirements and gaps and create relevant knowledge content to enable BT to deliver the best contracted service to Customer;

(c) use the knowledge management database to react quickly and make informed decisions regarding Customer's service;

(d) work with the problem team to understand any known errors or workarounds and create relevant knowledge articles. Once a permanent solution has been implemented, a new knowledge article will be created in collaboration with BT SMEs and the known error or workaround article will be deleted;

(e) maintain the knowledge database:

(f) new articles will be peer reviewed for quality and technical accuracy;

(g) existing articles will be reviewed at least annually and modified if required; and

(h) obsolete articles will be retired to keep the content current and accurate;

(i) collaborate with other functions, communicate with stakeholders, monitor the KM queue in the KM tool and functional mailbox and manage the KM portal;

(j) hold a quarterly (remote) review with Customer; and

(k) provide a quarterly report to Customer advising of new articles and amendments.

14. SERVICE REQUEST

Note: BT offers some Service Request functionality as part of the managed service package and some additional functionality can be added. This section 14 only applies if the optional Plus level as set out in section 15 (Service Request (Plus)) has not been purchased.

14.1 Primary Objective

14.1.1 A service request is a request to carry out an Add / Remove / Modify to an existing service Configuration Item (CI) as defined in ITIL.

14.2 Request Catalogue

14.2.1 A catalogue will be available through the My Account Portal where Customer can choose pre-priced service requests which are available to Customer for the service.

14.2.2 If Customer wants to make a revision to service which is not offered as an item in the service request catalogue, Customer will need to contact the BT Account Manager or Sales Specialist whose details will be provided in the Customer Handbook.

14.2.3 Where appropriate, a quote will be provided for Customer authorisation prior to an order being raised and the request being delivered.

14.2.4 Where charges apply, the billing process will be initiated in line with the contractual agreement.

14.3 Service Request Definition

14.3.1 Simple service requests (SSRs):

(a) are changes to existing configuration items (CIs) in the service that do not impact the service inventory.

(b) are pre-authorised. From request through to execution, they don't require any additional authorisation.

(c) are not contract-impacting. They don't incur any change to ongoing charges other than the charge for the SSR itself.

(d) don't include any hardware or site visits.

14.3.2 Pre-defined - a standardised Complex Service Request where submission of the request indicates approval:

(a) catalogue based;

(b) chargeable and have a pre-defined price;

(c) typically associated with hardware and accessories in standard locations (with or without maintenance);

(d) a move, add, change or termination of an existing service which may require a site visit;

(e) no recurring design effort as pre-defined designs are utilised;

(f) no availability/feasibility check required with suppliers;

(g) no need for supplier quote creation; and

(h) no reason a supplier needs a quote to accept an order, as it is an agreed catalogue item with the suppliers.

14.3.3 If Customer wants to make a revision to service which is not offered as an item in the service request catalogue, Customer will need to contact the BT Account Manager or Sales Specialist whose details will be provided in the Customer Handbook.

14.4 Service Request Fulfilment

14.4.1 All requests must be submitted by Customer using the Service Request Catalogue, accessible via the BT My Account Portal (or eBond if available). Customer will ensure only authorised personnel submit requests.

14.4.2 BT's pre-defined process workflow will be applicable for items within the Catalogue and BT will process the requests on the basis that they are pre-authorised.

14.4.3 Automated SSRs will follow an automated validation process before they are fulfilled, without manual intervention, within minutes of their receipt, at which point Customer will receive an auto-closure notification.

14.4.4 Non-automated SSRs and pre-defined complex requests will be manually fulfilled by the request fulfilment teams by following the relevant manual process and Customer will be notified accordingly.

14.4.5 BT will fulfil all service requests by working with relevant service management teams, BT service lines and third-party vendor(s) (as applicable) in a timely fashion to achieve the expected service level delivery times.

15. SERVICE REQUEST (PLUS)

Note: this section only applies if Plus level Service Request has been purchased as a feature and is included in the Order.

15.1 Primary Objective

15.1.1 A service request is a request from Customer to carry out an add / remove / modify to an existing service. Requests vary in size and complexity – simple service requests (SSRs) and complex service requests (CSRs) - definitions below.

15.2 Scope

15.2.1 Service requests are only applicable to the contracted products and Services. Requests for new services or products will need to go through the new provide process.

15.2.2 BT's service request tooling and systems will be used for service request fulfilment. Customer can interface via the BT My Account Portal or eBond to place service requests and track their progress.

15.2.3 BT will:

(a) provide a service request catalogue applicable to Customer's Services;

(b) fulfil simple and pre-priced requests within the delivery times shown in the catalogue;

(c) work with Customer to ensure understanding of requirements for CSRs and deliver a quote within the timeframe defined in the Customer's Order;

(d) provide a date for delivery and aim to fulfil the request within the committed timeframe;

(e) maintain a status log of all open and closed service requests, which will be reviewed at each service review meeting; and

(f) confirm in writing if BT reasonably believes a request cannot be fulfilled due to the following reasons:

(i) the service request would materially or adversely affect the health and safety of any person;

(ii) the service request would require the service to be performed in a way that infringes any law; or

(iii) the service request is impossible to carry out technically (in this case, BT will provide evidence of why the request is impossible to deliver).

15.3 Service Request Catalogue

15.3.1 A service request catalogue will be available through the BT My Account Portal (or eBond if available). Customer can choose service requests associated with their Services.

15.3.2 If the service request type is pre-priced, the catalogue will show the price. When Customer submits a request of this type, it is considered to be pre-approved and BT is committed to the delivery time shown.

15.3.3 If no price is displayed in the catalogue, BT will consult with Customer to understand the requirements and will then provide a quote, which Customer will need to approve before fulfilment begins.

15.4 SSR Definition

15.4.1 SSRs are:

(a) changes to existing configuration items (CIs) which do not impact the service inventory;

(b) pre-authorised, i.e. from request through to execution, they don't require any additional authorisation;

(c) not contract-impacting, i.e. they do not incur any change to the ongoing charges other than the charge for the SSR itself;

(d) are fulfilled remotely, i.e. they do not include any hardware and do not require a site visit.

15.5 SSR Fulfilment

15.5.1 All SSRs must be submitted by Customer using the service request catalogue, accessible via the BT My Account Portal (or eBond if available). Customer will ensure only authorised personnel submit service requests.

15.5.2 BT's SSR pre-defined process workflow will be applicable for SSR items within the catalogue.

15.5.3 Only SSRs documented in the service request catalogue will be accepted and fulfilled.

15.5.4 BT will process the request on the basis that it is pre-authorised.

15.5.5 Automated SSRs will follow an automated validation process before they are fulfilled, without manual intervention, within minutes of their receipt, at which point Customer will receive an auto-closure notification.

15.5.6 Non-automated SSRs will be manually fulfilled by the request fulfilment teams by following the relevant manual process and Customer will be notified accordingly.

15.5.7 BT will fulfil all SSRs by working with relevant service management teams, BT service lines and third-party vendor(s) (as applicable) in a timely fashion to achieve the expected service level delivery times.

15.6 SSR Billing

15.6.1 SSRs will be defined in units of effort detailed in the service request catalogue and the effort value of each SSR will be defined by the product. Customer will have an allocation of SSRs per annum included in the charges, with details provided in the Order. Any additional SSRs over this allocation will be chargeable in accordance with the effort value set out in the catalogue.

15.7 CSR Definition

15.7.1 CSRs are any type of request which doesn't meet the criteria for an SSR. Depending on their complexity, CSRs may require additional project resource and service introduction. CSRs are not included within the charges and each CSR will be invoiced. There are four categories of CSR (described below) all of which are commercial, billing and inventory impacting:

(a) Pre-defined: a standardised CSR where submission of the request indicates approval:

(i) catalogue based;

(ii) chargeable and has a pre-defined price;

(iii) typically associated with hardware and accessories in standard locations (with or without maintenance);

(iv) an add, remove or modify of an existing Service which may require a site visit;

(v) no recurring design effort as pre-defined designs are utilised;

(vi) no availability/feasibility check required with suppliers;

(vii) no need for supplier quote creation; and

(viii) no reason a supplier needs a quote to accept an order, as it is an agreed catalogue item with the suppliers.

(b) Small CSR:

(i) a request to add, remove or modify a Service for one product, at one site, where a service availability and feasibility check is required;

(ii) utilising predefined designs (according to agreed Site Categories) for standard configuration and maintenance; and

(iii) suppliers may require a specific quote for the item to accept an order.

(c) Medium CSR:

(i) a request to add, remove or modify a Service for multiple products within the same Service at one site or for one product, with requirements outside pre-defined designs. A service availability and feasibility check is required;

(ii) partially fulfilled via utilisation of pre-defined designs (according to agreed site categories) for standard configuration and maintenance, so will require only small design tasks; and

(iii) suppliers require a specific quote for the item(s) to accept an order.

(d) Large CSR:

(i) the most complex type of service request, such as a green field site, multiple products across more than one Service at one site, or for multiple products at multiple sites. A full quote with due diligence, solution design and low-level design will be required;

(ii) can include non-repeatable solutions and third-party solutions;

(iii) will require delivery project management; and

(iv) suppliers will require a specific quote for the item(s) to accept an order.

15.8 CSR - Identify and Qualify Customer Opportunity

15.8.1 The CSR must be raised by authorised Customer personnel, providing at least the minimum information needed to allow BT to proceed, using the service request catalogue. The CSR can be submitted via eBond (if available) or the BT My Account Portal.

15.9 CSR – Categorisation

15.9.1 BT will categorise the CSR to determine the appropriate pathway for it to proceed and review whether technical consultancy is required and whether what is being requested can be delivered. Technical consultancy is provided to support non-standard requests or when requirements are unclear so Customer can provide more definition to enable the request to be actioned.

15.10 CSR – Validation

15.10.1 BT will validate the details provided to ensure that the CSR can proceed and will either accept, resolve or, very rarely, reject the request:

(a) Accept: confirmation that BT can deliver the CSR and agreement to proceed;

(b) Resolve: clarify any missing details or requirements which are not fully understood, or discuss alternatives where the CSR is not viable. Once resolved, the CSR will move to "accept" or "reject" status; or

(c) Reject: BT will terminate the request and provide a reason for rejection (e.g. BT does not have an appropriate solution to meet the requirements).

15.11 CSR - Produce Customer Offer

15.11.1 Where a CSR is accepted, BT will:

(a) identify and assign appropriate operational teams to undertake the required activities for the CSR;

(b) for pre-priced requests - jump to the "Convert Contract to Orders" stage (see paragraph 13.13) as there is no need to provide a proposal;

(c) for unpriced requests - identify if there is a pre-defined solution design to use, revise an existing solution design or design a new solution according to the CSR details. Lower-level configuration details that do not affect the quote or the Bill of Materials (BOM) are not included at this stage;

(d) generate a BOM for the designed solution, obtain quotes from suppliers for the different components and produce a quote for the solution designed to meet the CSR; and

(e) generate a proposal comprising the technical design, resourcing, pricing and assessed risks.

15.11.2 The proposal will be reviewed by Customer and BT will answer any questions or queries. Customer will then approve, modify, or reject the proposal. Depending on the scope of any requested modification, BT may need to undertake another iteration of the whole process, however, if the modification is minor, BT will discuss the modification and reflect any agreed change.

15.12 CSR - Establish and Agree Contract Details

15.12.1 Once Customer has approved the quote, BT will generate a project plan (if necessary, depending on the CSR complexity) for the implementation phase. Where appropriate, the project plan may include a breakdown of the sites impacted, the required activities and milestones to complete the CSR. At this point, if necessary, BT will further develop the design for the solution and share it with Customer.

15.12.2 Meanwhile, BT will be processing the order request and raise it into the Service Delivery teams.

15.12.3 If a contract amendment is needed, BT will follow the contract change process.

15.13 CSR - Convert Contract to Orders

15.13.1 BT will validate the order request(s) and pass to the appropriate order entry teams who will raise the orders for the required components in the appropriate systems.

15.13.2 BT will keep Customer informed of the indicative lead times across each of the order milestones included in the CSR.

15.14 CSR - Fulfil Service Order

15.14.1 BT will deliver the service(s) as per the Order, which could be:

(a) physical delivery e.g. network related, where BT will deliver the access required and/or the Customer Premises Equipment (CPE) to a site(s) including the upload of the service configuration to the CPE; or

(b) virtual delivery e.g. where BT will switch on access to a cloud-based service.

15.14.2 BT will create the configurations scripts and implementation script to be run to activate the service(s).

15.14.3 Where applicable, BT will undertake testing of the service(s) delivered to ensure the solution works as planned and will undertake any corrective action should any issues be identified.

15.14.4 The delivery activities may take place in co-ordination with several instances of the change enablement process, where operational change management of the service(s) is contractually or situationally required.

15.15 CSR - Handover and Close Order

15.15.1 Once BT has completed the delivery and, where applicable, tested the service(s), Customer will be informed that the service is active and ready to be used. Customer will be asked to sign-off to accept the service as delivered.

15.15.2 BT will update the CMDB to ensure that the current state of Customer's estate is reflected in the inventory.

15.15.3 Once all the delivery activities have been completed and the CSR has been fulfilled, it will be closed in the BT system and will be reported on as a completed service request.

15.15.4 The billing process will be initiated in line with the contractual agreement.

16. AVAILABILITY MANAGEMENT

Note: this section only applies if Availability Management has been purchased as a feature and is included in the Order.

16.1 Primary objective

16.1.1 To identify opportunities to optimise the availability of the IT Infrastructure, deliver cost-effective improvements and business benefits, and to make recommendations for improvements to enhance the overall quality of Customer's network.

16.2 Scope

16.2.1 BT will:

(a) monitor the infrastructure components that underpin the services;

(b) provide availability reporting to make sure that agreed levels of availability, reliability and maintainability are measured, reported, monitored on an ongoing basis and can be clearly evidenced;

(c) where product tooling allows, self-service availability data will be provided through the BT My Account Portal, giving a view of near real-time information about the operational status of device availability;

(d) provide root cause analysis on failures and produce recommendations to address any shortfalls in availability, resolve issues and optimise the performance of the IT infrastructure;

(e) categorise services per-site and per-device and, with customer support, maintain a list of critical business devices;

(f) review availability and discuss reports, recommendations, and exceptions at monthly service reviews. Where necessary, to support the BT Customer Success Manager, an availability professional will attend the meetings virtually;

(g) make recommendations for the use of new technology to improve performance, efficiency or effectiveness of the availability process; and

(h) perform regular reviews of the availability management process and procedures to ensure that all are subjected to continuous improvement and remain fit for purpose.

16.3 Collect Availability Data

16.3.1 Network components will be added to the availability reporting platform to enable the systems to poll the network devices for availability related data. Proactive monitoring will be put in place for contracted Services, with thresholds set and alerts in place and acted upon if thresholds are breached.

16.4 Produce Availability Reports

16.4.1 A monthly quality of service report will be available via the BT My Account Portal containing the following:

(a) network/service availability for the previous month; and

(b) overall service availability summary for the rolling 12-month period, including a graphical representation with target and actual availability of Customer's network (expressed as a percentage) for that rolling 12-month period.

16.5 Investigate Availability Issues

16.5.1 The availability management team will proactively investigate availability issues by analysing incident data. Trend analysis will be provided to identify current and potential availability issues which may have caused incidents. When required, the availability management team will work with the problem management team to perform root cause analysis on failures.

16.6 Make Recommendations

16.6.1 Following the analysis of availability issues, recommendations or potential service improvement initiatives will be identified for consideration at scheduled service reviews.

16.6.2 Availability concerns or recommendations will be discussed at monthly service reviews covering the following areas:

(a) review current availability issues;

(b) agree actions and owners to address issues; and

(c) recommend availability changes to optimise or improve the network performance where appropriate.

16.6.3 When necessary, an availability professional from the availability management team will attend the service review meeting via telephone or an online meeting.

17. CAPACITY MANAGEMENT

Note: this section only applies if Capacity Management has been purchased as a feature and is included in the Order.

17.1 Primary Objective

17.1.1 To ensure the capacity of the Service meets Customer's business needs, in a timely and cost-effective manner. This means providing optimum capacity at the agreed grade-of-service for current and future business requirements, proactively highlighting early warning of any capacity and performance issues when threats or exceptions are identified and providing timely capacity recommendations.

17.2 Scope

17.2.1 BT will:

17.2.2 provide optimum capacity at the agreed grade-of-service for current and future business requirements;

(a) proactively raise early warnings for any capacity and performance issues when threats or exceptions are identified;

(b) provide timely capacity recommendations;

(c) provide a monthly report which details a standard set of performance metrics;

(d) provide a self-service capacity data option through the BT My Account Portal;

(e) investigate, analyse and process capacity exceptions that have been identified through monthly monitoring and provide recommendations to resolve them;

(f) hold a monthly capacity review meeting - to discuss reports, recommendations and exceptions; and

(g) tune systems to achieve optimum use of all hardware, network, and TCP application resources. The capacity team will make recommendations for tuning based on advice from subject matter experts for each service.

17.3 Monitor Service Capacity

17.3.1 Data and voice network components will be added to the capacity reporting platform enabling polling of the network devices for capacity related data.

17.3.2 To support effective capacity management, the capacity and performance management team will ensure performance monitoring is in place for all contracted services, thresholds are set, and alerts are in place and acted upon if thresholds are breached.

17.4 Model and Analyse Capacity

17.4.1 Data collected for each managed service element (key performance metrics e.g. device, interface, storage etc.) will be used to baseline traffic usage. As part of normal service operation, investigation into shortfalls regarding capacity and performance will be required. Exception thresholds will then be pre-defined and configured. Breaches to these thresholds will then be flagged with exception analysis like heat maps, utilisation graphs and, where appropriate, top talkers.

17.4.2 Identified capacity exceptions will be investigated and progressed in collaboration with the event, incident and problem management functions and discussed at the capacity review meetings.

17.4.3 As part of proactive capacity management, data gathered on the performance and capacity of the services, components and resources will be used in trending and modelling to forecast future capacity levels.

17.5 Produce Capacity Report

17.5.1 The following reports will be available via the BT My Account Portal each month:

(a) monthly report detailing utilisation and exceptions to threshold, including capacity analysis and recommendations for changes to optimise the solution made by the capacity management team and the technical design team; and

(b) forecast report detailing the future capacity requirements for the next 6 months, identifying predicted threshold breaches. This report will help prevent future network capacity incidents.

17.6 Capacity Review Meeting

17.6.1 As the key governance mechanism for capacity management, BT will prepare for and hold monthly capacity review meetings to discuss and agree capacity recommendations.

17.6.2 Inputs for the meetings:

(a) network usage data (obtained directly from systems in this process);

(b) monthly capacity report, with exceptions in case of a capacity threshold breach;

(c) capacity review meeting minutes (previous editions);

(d) capacity-related problem records and risks; and

(e) recommendations for projects to mitigate capacity or performance issues - i.e. where and when to change capacity (in terms of equipment and network service capacity).

17.6.3 Every managed service element that has exceeded its threshold will be discussed. Any actions as a result of discussions will be recorded and assigned an owner for follow-up and recommendations will be made.

17.7 Recommendations

17.7.1 In collaboration with the technical design team, recommendations are likely to be:

(a) upgrade capacity; or

(b) downgrade capacity.

17.7.2 If Customer decides not to upgrade a managed service element (which BT has already recommended for upgrade), this will result in BT adding the issue to the known-exceptions list and a risk being raised for follow-up. To prevent high-utilisation events being triggered in response to a known and accepted issue, BT may choose to suppress these.

17.8 Tune Service Capacity

17.8.1 An upgrade to network capacity is required where breaches to traffic volume thresholds have occurred - either by a predicted step-change, an unexpected step-change, or a long-term growth trend. The tune process is initiated when a step-change in network capacity has been identified and agreed at the capacity review meeting. This is to ensure threshold breaches are resolved or avoided.

17.8.2 Once a capacity recommendation has been agreed, Customer will initiate a request to BT (via the normal service request process) for the change to be costed and carried out. BT's change enablement, project and service teams will then own the change progression and inform the capacity team when changes have been made.

17.9 Resource and Communication

17.9.1 Capacity management is delivered by a shared, operational team providing a service Monday to Friday during UK business hours.

17.9.2 Questions or queries about capacity management matters can be raised directly with the capacity team -contact details will be provided in the Customer Handbook.

18. BUSINESS CONTINUITY AND DISASTER RECOVERY

Note: this section only applies if BCDR has been purchased as a feature and is included in the Order.

18.1 Primary Objective

18.1.1 The Business Continuity and Disaster Recovery (BCDR) capability helps manage risks and ensures that the business (both BT and Customer) can continue in the event of an unplanned service disruption. The function seeks to predict and prevent service disruption wherever possible. Where disruption is unavoidable, the aim is to reduce the duration and impact of the disruptive event, thereby protecting business interests, reputation, brand, and value creating activities. BT delivers this capability to best practice standards, ensuring alignment to ISO 22301.

18.2 Scope

18.2.1 BT will:

(a) develop, maintain and test comprehensive BCDR plans. Such plans are compiled in a number of standard templates that are adapted to the nuances of different parts of BT's organisation. The plans show how the business will continue to operate during an unplanned disruption in service. The BCDR plans will be broad ranging and contain contingencies for IT services, business processes, assets, human resources and business partners/suppliers;

(b) plan for disaster recovery arrangements, including data backup and restore procedures, for all agreed critical products and services. These plans are classified as highly confidential documentation and therefore will not be shared by BT;

(c) plan for continuity arrangements which apply to BT's operations generally. These plans are shared with the Customer in the form of a high-level summary;

(d) review and update BCDR plans periodically to ensure they remain current and valid;

(e) update plans, as required, in response to any material change to the services that are delivered; and

(f) conduct a review of plans following testing or when invoked in response to an unplanned service disruption. Any lessons learned or improvement actions identified will be acted upon and plans updated if appropriate.

18.2.2 Where BT has created a bespoke plan for Customer, BT will ensure that it is updated and re-issued following review with Customer.

18.3 Understand Strategy and Principles

18.3.1 BT's strategic approach is to recognise the causes of disruption, addressing each with an overall objective set that seeks to predict and prevent disruption wherever possible. Where disruption is unavoidable, BT will ensure the organisation has sufficient resources and arrangements to reduce the duration and impact of such disruption.

18.3.2 Overall responsibility of BC strategy lies with BT's Business Continuity Governance Group (BCGG).

18.4 Adhere to BCDR Policy

18.4.1 BT policy guides delivery of the BCDR capability. Policy statements are designed to align with the objectives of ISO22301 and provide a framework for their implementation within BT, defining the roles and responsibilities of BC practitioners and BT people. BCDR policy is reviewed and, where needed, updated on an annual basis.

18.4.2 BT will share the BCM policy with Customer to provide assurance and common understanding.

18.5 Ensure Defined Leadership Roles/Responsibilities

18.5.1 The BCDR capability is delivered across multiple BT customer facing units by a team of personnel. A clearly defined governance structure, with defined accountabilities, ensures consistency of approach. Monitoring of the capability ensures that arrangements remain fit for purpose and are subject to continual improvement.

18.5.2 The incident management strategic forum is responsible for defining strategic goals for pan-BT incident management, operating in parallel with the BCGG. Representatives from within each discipline attend both forums. Similarly, an incident management working group, which exists at an operational level (running in parallel with BT's business continuity operating team), drives implementation of the strategies.

18.6 Understand and Manage Risks

18.6.1 Within BT there is an enterprise-wide risk management process (operational risk framework) built-into all "business as usual" processes, products, and services. Recognised best practice methodologies are followed to assess and manage risks of disruptions to availability, breaches of confidentiality and failures in integrity. As standard, BT conducts annual risk assessments on all critical products and services.

18.7 Establish BCDR Procedures

18.7.1 The BCDR policy drives the definition, creation and upkeep of the multiple related processes and procedures which underpin the BCDR capability. Two core processes in this respect are incident management and IT service continuity management.

18.7.2 To ensure effective ongoing delivery of the customer business continuity plan and the aligned BCDR processes, BT will engage with Customer in ongoing communications as appropriate.

18.8 Ensure Inter-lock with Incident Management

18.8.1 Any disruptive event with the potential to require the invocation of continuity plans is designated as a Major Incident and controlled by the MIM team, in conjunction with on-call business continuity specialists and appropriate managers. BT will report disasters (or potential disasters) to Customer immediately upon identification, based on the parameters defined in the BCDR plan.

18.8.2 BT will designate a primary and secondary contact for cases of emergency and disaster to ensure effective communication and invocation of continuity plans.

18.9 Ensure Inter-lock with Crisis Management

18.9.1 A crisis management process, covering all relevant products and services, will be established and the structure of this is shared with Customer. This process will ensure effective communication and escalation channels are known to Customer in the event of a business interruption, providing regular status updates for all service-impacting Major Incidents.

18.10 Exercise and Test BCDR

18.10.1 Business continuity arrangements are tested to validate plans, build confidence and competence. BT has a dedicated team who manage all aspects of business continuity and disaster recovery exercise and testing. BT will ensure all critical products and services are tested on a regular basis.

18.11 Ensure Training / Awareness

18.11.1 BT ensures that business continuity arrangements, including any site-specific arrangements, are properly documented, and understood by stakeholders.

18.11.2 BT ensures that all those employees responsible for carrying out business continuity activities are trained in order that they have a good understanding of the processes and their role.

18.11.3 Documentation is stored and accessed via secure, web-based document libraries, enabling access to those who are authorised.

18.11.4 For each role within the business continuity management system, a set of competencies are defined. Each individual is assessed against the competencies and any resultant gaps are closed with training, job shadowing and other techniques. These records are maintained and regularly reviewed.

18.12 Review BCDR plan

18.12.1 BT BCDR plans are reviewed on a regular basis and in response to significant change in industry practice and ISO22301. End-to-end continuity arrangements are also reviewed following invocation and testing.

18.13 Audit

18.13.1 BT will support Customer's annual supplier audit/assurance programme in regard to BCDR planning.

19. VULNERABILITY MANAGEMENT

Note: this section only applies if Vulnerability Management has been purchased as a feature and is included in the Order.

19.1 Primary Objective

19.1.1 Vulnerability management is the cyclical practice where BT discovers, prioritises, assesses, reports, remediates and verifies software vulnerabilities. The remediation of vulnerabilities is done via patching and configuration changes of security settings. Validating the urgency and impact of each vulnerability, based on various risk factors, ensures a swift response to critical threats. Vulnerability management is an integral part of IT and network security.

19.2 Scope

19.2.1 BT will:

(a) have overall responsibility for managing identified threats and vulnerabilities to software;

(b) use a defined set of criteria to prioritise such vulnerabilities;

(c) monitor supplier/vendor notifications to identify such vulnerabilities;

(d) follow a risk management process for those vulnerabilities not patched on Customer's estate;

(e) deal with such vulnerabilities in a timeframe appropriate to the risk posed;

(f) implement patches following a release and deployment process;

(g) implement all patches/upgrades following a change enablement process;

(h) take appropriate measures to install all new security patches for identified vulnerabilities from vendors/suppliers in a timely manner;

(i) take appropriate measures to ensure patches are installed and software/OS/firmware releases are dealt with as per manufacturer's and BT's recommendations;

(j) implement best practice industry tooling to enable faster detection and exposure of such vulnerabilities to Customer's service;

(k) produce vulnerability reports; and

(l) notify Customer of any end-of-life and end-of-service devices in a timely manner.

19.3 Discover Vulnerabilities

19.3.1 BT will collect and collate details of vulnerabilities notified by manufactures and vendors.

19.3.2 Vulnerabilities are assessed and rated by the notifying party to help assess relative priority from a BT perspective. A four-tier vulnerability rating system is used as follows: low, medium, high, and critical. This rating may be adjusted if further investigation warrants amendment.

19.4 Prioritise and Assess Vulnerabilities

19.4.1 Vulnerabilities are reviewed to filter and identify those which require detailed assessment. Each vulnerability is assessed using a standard set of BT questions and an action level is assigned accordingly:

(a) Priority action: a vulnerability which requires accelerated remediation;

(b) Normal action: a vulnerability where the exploit is imminent or active; or

(c) Drop action: the vulnerability is not progressed as no impact to the Customer.

19.4.2 A Common Vulnerability and Exposure (CVE) report is produced, which informs whether or not the vulnerability impacts Customer's estate.

19.4.3 A detailed risk review is conducted for all vulnerabilities rated as critical or high priority, focusing on reviewing the technical and business aspects of any identified solution or patch. In some cases, lower priority vulnerabilities may require a detailed risk review if deemed necessary by BT.

19.5 Identify Potential Affected Devices

19.5.1 BT uses information in the CVE reports and the vulnerability assessments to identify potentially affected devices, using inventory data from the CMDB.

19.5.2 If identified devices have passed their hardware end-of-vulnerability support date or passed their last date of support they are classed as obsolete and marked as out of scope for patch remediation, as there will be no patch/workaround published by the vendors. In these cases, a risk will be raised. All such devices will be recommended to be refreshed with like-for-like models. This will be captured in the vulnerability report.

19.6 Scan Devices

19.6.1 The potentially affected devices are scanned (using the relevant tools or manually) based on the rules defined for specific vulnerabilities, to identify the actual affected devices.

19.7 Agree Remediation

19.7.1 Consideration is given to potential remediation activities required and the best course of action agreed. Typically, there are two categories of solution / workaround for a given vulnerability:

(a) configuration change or enable/disable of feature; or

(b) patch (OS) upgrade.

19.8 Test Remediation Activity

19.8.1 Where appropriate, testing will be undertaken to ensure the identified workaround or software fix will have the desired effect. Testing also ensures any issues are identified or design changes are fully understood prior to the implementation. Where there is no test environment, BT uses its technical design authority to understand whether the remediation action is compatible with Customer's estate and, therefore, suitable to implement.

19.9 Seek Customer Approval

19.9.1 BT will produce a vulnerability management report, which will detail the proposed remediation plan and will seek approval from Customer for the proposed activity. The process for formal approval will vary depending on the remediation action needed. Where remediation activity requires a formal service change to be raised then approval will be managed via the change enablement process.

19.9.2 In instances where it is believed an identified vulnerability will cause serious impact to BT's infrastructure, remediation will be scheduled and the engagement with Customer will be for information only without seeking Customer's approval.

19.10 Update Risk Register

19.10.1 As appropriate, BT will raise identified risks into the risk register. This would include raising risks for situations where the vulnerability will not be addressed, for example:

(a) where Customer does not approve the fix or wish for BT to remediate;

(b) the workaround/fix is not available for a given vulnerability; or

(c) if the hardware has passed its end of vulnerability support date, or passed its last date of support and has become obsolete.

19.11 Implement Remediation

19.11.1 Once a solution has been agreed with Customer, BT will hand over to the release and deployment function, where the remediation activities to resolve the vulnerable devices will be undertaken. All fixes/patches/upgrades will be performed under the change enablement process.

19.12 Verify Remediation

19.12.1 Once a fix has been applied, post-implementation resilience checks will be conducted and relevant evidence may be shared with Customer and the implementation will be marked as complete.

19.13 Security Consultation

19.13.1 The BT teams involved in day-to-day vulnerability management activities take expert advice from the BT security consultancy service where required. This consultancy provides additional advice on the impact and risk posed by particular vulnerabilities, including advice on remediation activities. In some cases, this consultancy role will communicate with Customer when necessary.

19.14 Performance Metrics and Reporting

19.14.1 A standard monthly report, providing information on a set of vulnerability metrics will be provided. The vulnerability management report will contain:

(a) a list of discovered vulnerabilities – common vulnerability exposure (output from the discover and scanning stage/tool);

(b) an evaluation of vulnerabilities and list of impacted devices – this will explain which vulnerabilities impact Customer's estate (output from scanning and manual assessment);

(c) proposed remediation;

(d) risks and impact - this includes identified vulnerable devices which have passed hardware end-of-vulnerability support date or passed last date of support and are, therefore, obsolete. All such devices will be marked as out of scope for patch remediation;

(e) remediation plan – if known at point of issue; and

(f) implementation details – Including change record information.

20. RELEASE AND DEPLOYMENT

Note: this section only applies if Release and Deployment has been purchased as a feature and is included in the Order.

20.1 Primary Objective

20.1.1 Release and deployment (R&D) management is to plan, schedule and control the build, test, and deployment of recommended software updates into the live environment. The process ensures that the most compatible releases are deployed effectively so that the integrity of hardware, software and service components of the live environment is maintained. A release may involve one or more changes to a service that are all built, tested, and deployed together. Multiple changes may be packaged together to manage dependencies and for the purposes of efficiency.

20.1.2 The main goal is to proactively upgrade the affected operating system (OS) to the recommended version, in a timely manner, in order to avoid security vulnerabilities, non-compatibilities and to minimise risks.

20.1.3 A new release will only be initiated if it reduces the chances of a system failure, a security vulnerability or provides a new feature. Otherwise, the already installed version will remain as is to keep system downtime to a minimum.

20.1.4 R&D tightly integrates with the change enablement, problem management, service configuration management, vulnerability management and lifecycle management functions. BT's R&D process also integrates with BT's third-party vendors and, wherever possible, Customer's R&D process.

20.2 Scope and Obligations

20.2.1 BT will:

(a) produce an R&D plan and use it to consistently drive decisions on release management;

(b) agree the R&D plan with Customer;

(c) ensure all R&D activities conform to the defined release policy;

(d) categorise releases as major, minor or emergency;

(e) build, test and deploy services specified in the BT service design, and ensure Customer can use the BT services as intended;

(f) control release of software into the live environment in a manner that ensures both business continuity and meets the agreed level of availability;

(g) ensure key stakeholder and operational contacts are kept informed of the schedule;

(h) identify releases according to the scheme defined in the release policy;

(i) authorise R&D activity via the change enablement function; and

(j) create a release plan for each release which will include implementation and back-out plans for the approved changes included in a release.

20.3 Define Scope and Plan Content of R&D

20.3.1 Requirements are understood, the scope is defined and agreed, the impact for components and the live environment is determined and plans for building and deploying releases are created.

20.4 Determine Requirements

20.4.1 Various triggers determine the release requirements:

20.4.2 a release upgrade can be requested by Customer, via a CSR e.g. requesting new functionality or updating software which is outdated or approaching end-of-support;

(a) pro-active patch management collation of approved and recommended patches (from Original Equipment Manufacturer (OEM) and BT Portfolio design team) for new functional or maintenance release notifications;

(b) Major Incident root cause analysis - reports from the problem management function identify software which must be updated to fix known bugs.

20.5 Prepare and Review the Release Plan

20.5.1 The release manager will collate recommended patches and functional release versions (from OEM and BT portfolio design team) and share with the TDA to review compatibility against Customer's current estate and determine if the newer software is more suitable. The new software versions will then be captured in the release report under "release versions".

20.5.2 The releases will be categorised as either:

(a) Major - introduces new functionality, including features that may be significant enough to include structural database changes; they may also include bug fixes;

(b) Minor - includes some enhancements, but usually does not require any database changes; they may also include bug fixes; or

(c) Emergency - for known problems which need addressing as soon as possible, i.e. security patches.

20.6 Develop Release Plan and Schedule

20.6.1 After reviewing all information, a release plan will be developed capturing required updates. The plan will include a request for change describing the reason, impact and detailed steps of the change, any associated risks and back out plans, where required.

20.6.2 The release schedule will be updated to provide a quarterly view of planned releases, timelines to be deployed, pre-agreed release windows etc. The schedule is a tabular view in the release report.

20.6.3 The below best practices will be used during the planning of the release cycle:

(a) delay between waves must be long enough to observe deployment success but short enough to minimise risks due to differences in the OS versions of similar communication devices;

(b) release windows will be planned outside of business hours, if possible, to minimise business impact;

(c) every release plan must be approved by Customer before deployment.

20.7 Discuss and Agree Plan

20.7.1 The release manager will share the release plan with Customer and request approval. The plan will highlight the risks and the timeframe in which a decision must be made (plan validity).

20.7.2 Depending on the release category, there may be additional charges for implementation. See section below entitled "Costings for Releases".

20.7.3 If Customer is unable to approve within the timeframe communicated by BT, the release manager will update the release schedule to "hold" status and update the risk register.

20.8 Release Build and Test

20.8.1 Build the Release

(a) The components of the release are bundled into a package for installation. This will be provided by either the OEM or BT portfolio design team.

20.9 Test the Release

20.9.1 Where appropriate, testing is undertaken to ensure the proposed release will have the desired effect, any issues are identified, and design changes are fully understood.

20.9.2 A test environment may be used, based on the environment specifications of the release. If a test environment is not available or feasible then the release will be checked by the TDA to confirm compatibility. BT will propose a proof of concept (POC) of the release on a device or site which has low impact on the business and will be performed out of business hours. The results of the tests/POC will be recorded and analysed to verify the success of the build.

20.10 Deploy Release

20.10.1 Once Customer has given initial approval of the release plan, a formal request for change is raised. The following deployment activities will then be carried out as defined in the release plan:

(a) creation of change record;

(b) securing approval from Customer;

(c) implementation of release;

(d) record incidents, unexpected events, issues or deviations during the change;

(e) remediate / back out release if necessary;

(f) provide early life support as defined in the release plan; and

(g) update the release management report.

20.10.2 In the case of emergency releases, if it would be catastrophic to Customer's live environment to delay deployment while waiting for approval, BT may need to go ahead with deploying the release and seek approval retrospectively.

20.11 Monitor, Review and Close Release

20.11.1 The release manager will monitor the progression of the release deliverables and ensure adherence to governance. The release report will be updated - new IOS version, change implementation schedule, change reference number, successful remediation of the published/reported vulnerability and bugs.

20.11.2 The release manager will share the updated version details with the BT service configuration team to ensure the CMDB is updated to accurately reflect Customer's estate.

20.11.3 Customer will be informed of progress against timelines, release completion and request sign-off with feedback satisfaction regarding the deployment.

20.11.4 A review of the release will include:

(a) feedback on user's satisfaction with the deployment;

(b) review of quality criteria if not met;

(c) check all actions, necessary fixes and changes are complete;

(d) ensure no capability, resource, capacity or performance issues remain at the end of the deployment;

(e) document any problems, known errors and workarounds and confirm they are accepted by Customer, BT and any third-party vendors;

(f) identify issues that impact service operation and support and update the risk register, where necessary.

(g) address risks or agree actions; and

(h) ensure the CMDB reflects all changes (updated by the inventory manager).

20.12 Customer Specific Dependencies

20.12.1 As BT plans and rolls out the releases for the Services, a number of dependencies will need to be discharged by the Customer in a timely manner, as follows:

(a) provide input into the release schedule;

(b) take decisions for obsolete devices and the initiation of refresh planning;

(c) sign-off risks for keeping obsolete devices and devices for which the current OS has passed the end-of-support date;

(d) attend the Customer change advisory board to provide approval of the release activities via the change enablement process;

(e) provide an appropriate point of contact to support emergency releases;

(f) where access to site(s) is required to enable release and deployment activities, assist BT with arranging access and provide an on-site point of contact;

(g) where appropriate, co-operate with BT to undertake any activities which are necessary for the release review.

20.13 Costing for Releases

Release Category	Category Description	Plus Tier Costing
Major	A major release introduces new functionality, including features that may be significant enough to include structural database changes; they may also include bug fixes	Additional cost – CSR raised by Customer
Minor	A minor release includes some enhancements, but usually does not require any database changes; they may also include bug fixes	Included as part of Service, subject to maximum one upgrade per device per year Note: no carry over into the following contract year
Emergency	Security patch/upgrades	Included as part of Service

20.14 Performance Metrics and Reporting

20.14.1 Release Report

(a) A release and deployment management report will be provided monthly, containing:

(i) release schedule;

(ii) risks and impact;

(iii) risk register;

(iv) devices, products, sites, countries, region information;

(v) current and recommended patch details;

(vi) deployment details;

(vii) implementation details – including change record information; and

(viii) release status.

20.14.2 Patch Report

(a) A quarterly patch report will also be provided, containing:

(i) devices/ products details;

(ii) device type information;

(iii) current running OS information; and

(iv) list of BT recommended patches.

21. LIFECYCLE MANAGEMENT

Note: this section only applies if Lifecycle Management has been purchased as a feature and is included in the Order.

21.1 Primary Objective

21.1.1 To manage the lifecycle of the assets that make up your Service throughout the lifetime of your contract. Most Original Equipment Manufacturers (OEMs) give notice (generally 6 months) of when products will be declared end-of-life (EOL) or end-of-support (EOS). BT will gather this data and update the inventory to show the dates the assets will reach EOL or EOS status.

21.2 Scope

21.2.1 Devices supported under this service:

   (a) chassis;

   (b) routers;

   (c) switches;

   (d) wireless controllers;

   (e) access points;

   (f) firewalls.

Power supplies, fans, modules (e.g. SFP) and interfaces are out of scope.

21.2.2 BT will:

   (a) gather data from OEMs;

   (b) update inventory with EOL or EOS dates;

   (c) create recommendations for action needed;

   (d) inform Customer, in good time, that items are expiring and make recommendations so decisions can be made regarding what action to take, i.e. replace the equipment or accept there is a risk to the solution by keeping it;

   (e) inform internal support functions (incident management, problem management and the teams dealing with releases and vulnerabilities);

   (f) add details of expired items to the risk register. These expired items will be excluded from SLA reporting and service credit payments.

21.3 Gather data

21.3.1 Where OEMs supply information for lifecycle management, BT will gather the data. The OEMs publish external EOL notifications approximately 6 months before the end of sale date.

21.4 Update inventory and inform TDA

21.4.1 When EOL or EOS dates become available, the dates will be added to the Lifecycle Management report quarterly and the Customer's inventory will be updated. The lifecycle management report is shared with the contract technical design authority (TDA) and the service manager.

21.5 TDA recommendations

21.5.1 The TDA will impact-assess the expiring devices and make the appropriate recommendations on next steps to replace/upgrade and provide details of suitable products for the replacement.

21.6 Inform customer

21.6.1 The service manager will review all devices approaching EOL or EOS with Customer at monthly service reviews. BT will always advise replacing the devices as soon as possible to prevent risk to the solution. Devices which are EOL are difficult to replace if they become faulty as replacement kit is not always available. Devices which are EOS cannot receive software updates, limiting the opportunity to optimise the services and creating risk of potential security vulnerabilities.

21.7   Replace device or add to risk register

21.7.1   Customer decision will be one of three options:

(a)   upgrade the equipment to newer technology in line with business requirements and technology strategy;

(b)   replace the EOL or EOS kit with a newer version of the same product;

(c)   keep the EOL or EOS kit and accept that there is a risk.

21.7.2   For option 1, BT will provide advice and, where required, support from specialist technical sales teams, on the options for uplifting Customer's solution to new technology, including pricing and timelines.

21.7.3   For option 2, BT will provide costs for a like-for-like replacement.

21.7.4   For both options 1 and 2, BT will ask Customer to place an order in good time so that the solution is not at risk before deployment.

21.7.5   For option 3, once the EOL or EOS dates are reached and the equipment is officially expired, BT will add details to the risk register. At this point, any incidents on the equipment will be managed on a best-efforts basis, and any SLAs and service credits will no longer apply.

21.8   Inform support functions

21.8.1   All the relevant support functions (e.g. incident, problem, change, vulnerability management and the release team) will utilise the data regarding expiring/expired devices from the inventory so that the impact can be managed accordingly.

21.9   Performance metrics and reporting

21.9.1   BT will provide a quarterly report detailing devices which are due to expire within the next 6 to 12 months and recommendations for upgrade/replacement to prevent service issues.

21.9.2   Depending on the products in Customer's solution, the following are some explanations of the dates which will be captured for your products:

(a)   **HW EOL**: Hardware End of Life or Last Date of Support HW: The last date to receive applicable service and support for the product as entitled by active service contracts or by warranty terms and conditions. After this date, all support services for the product are unavailable, and the product becomes obsolete.

(b)   **HW EOVSS**: End of Vulnerability/Security Support HW: The last date that hardware vendor may release a planned maintenance release or scheduled software remedy for a security vulnerability issue.

(c)   **SW EOL**: Software End of Life or Last Date of Support OS SW: The last date to receive applicable service and support for the product as entitled by active service contracts or by warranty terms and conditions. After this date, all support services for the product are unavailable, and the product becomes obsolete.

(d)   **SW EOVSS**: End of Vulnerability/Security Support OS SW: The last date that Cisco Engineering may release bug fixes for Vulnerability or Security issues for. After this date, bug fixes for Vulnerability or Security issues identified in may be provided through later supported software releases. Note that there will be no rebuild releases of provided after this End of Vulnerability/Security Support milestone date.