Bluecube

Service Descriptions

What we do & how we do it

Dated: 20/06/2023
Version: 3.1
Security: Commercial-in-Confidence

Contents

Version Control

This document is electronically version controlled (with each change being tracked automatically). The list of changes below represents significant document releases that are communicated to all Bluecube clients. Changes are listed in reverse chronological order.

Version	Date	Changes	Author
3.0	22/09/2022	Rebrand of document	
2.0	27/06/2022	Re-grouping of the services to reflect the new delivery structure (addition of dedicated SOC teams) as well as the addition of new Security Services.	RG
1.0	15/03/2022	Concatenation of all Service Description Documents to create a single 'Service Description' document following internal review and approval.	RG
DRAFT	02/12/2021	Concatenation of all Service Description Documents to create a single 'Service Description' document for internal Bluecube distribution.	LC

Introduction

These Service Descriptions are the supporting information to contractual agreements. They are grouped into four sections: Support, Security, Infrastructure and Logistics.

Each Service Description provides further details of Bluecube's standard service offerings. Not every client of Bluecube will receive every service detailed within this document; specific details of which services are being delivered to a client can be found within the agreed contract.

These service descriptions ('Service Description') are entered into by the client ('Client') and Bluecube Technology Solutions ('Supplier') as Identified within the Client contract. By purchasing these Services, the Client agrees to be bound by the terms and conditions associated with that service in addition to the contract Terms.

Bluecube also offer bespoke and discrete services that are not detailed within this document.

These service description Terms and conditions, where at conflict, are superseded by any specific contractual agreement Terms.

Each Service Description contains a link to Bluecube's internal processes that relate to the delivery of each service. These links are for internal Bluecube reference only and will not work for Clients or any other external parties (this is by design).

SECTION ONE
SUPPORT SERVICES

Services to provide support
and engagement to our clients.

1. Client Engagement

WHAT	
Name	**Client Engagement**
Overview	The provision of a named contact within Bluecube to provide a point of contact, over and above the delivery function. The purpose of this engagement is to build and hold a relationship between Bluecube and our clients. The Client Engagement Manager (CEM) will handle any requests from the client. This can include the escalation of tickets, procurement activities, general advice and guidance as well as the delivery of strategic guidance and advice (normally delivered through strategy days).
HOW	
Prerequisites	Subscription to an ongoing service from Bluecube
Procedures	Each Bluecube client will be provided with a named CEM. Contact with the CEM can be made through email or phone. Regular, structured, Service Reviews will be scheduled between the CEM and the client and the CEM will also (in conjunction with the client) maintain a Technology Road Map. All procurement activities will be managed by the CEM.
Knowledge base	Bluecube Compass
WHEN	
Service hours	Normal UK working hours. Monday to Friday, 08:30 to 17:30, excluding UK bank holidays.
TERMS & SLA	
Service Levels	-
Exclusions	-
Billing	N/A - every client of Bluecube benefits from a CEM. The charges are included within the ongoing monthly service charges.
Client Responsibilities	To engage with their CEM to share feedback, views and future plans.

2. Monthly Reporting

WHAT	
Name	**Monthly Reporting**
Overview	The provision of metrics monthly, typically used to monitor and track service quality and delivery in respect of Service Desk performance.
HOW	
Prerequisites	24x7 Service Desk
Procedures	All reporting is delivered using PowerBI. Bluecube delivers a unified report for all of its syndicated service clients. Bespoke reports can be created on request (and for an additional fee). The report data is updated on a daily basis and made available to our clients monthly.
Knowledge base	Bluecube Compass
WHEN	
Service hours	This is a reporting service that is conducted every month as part of your security or service desk service.
TERMS & SLA	
Service Levels	-
Exclusions	-
Billing	Integrated as part of the per user charge for applicable services typically 24x7 service desk. The creation of bespoke reports will be subject to a one-off charge (NB. Bespoke reports will require maintenance which will be subject to an additional fee).
Client Responsibilities	-

3. 24x7 Service Desk

WHAT	
Name	**24x7 Service Desk**
Overview	Our Service Desk service involves the logging, assessment, and prioritisation of incoming tickets with process driven resolution of tickets where appropriate. Tickets that cannot be resolved using the defined processes will be escalated to our 2nd Line Engineering teams (within the Service Desk). Tickets that cannot be resolved within the Service Desk team will be escalated to specific teams (this will typically be internal Bluecube teams, however it can also be to Client's internal teams or to external third parties). This description refers to the provision of a syndicated service.
HOW	
Prerequisites	None
Procedures	An in-house developed system (Lighthouse) is used to manage all interactions of a technical nature with our clients and their users (typically requests for assistance or support). Each item that we work on is referred to as a ticket. There are three ways in which a client can log a ticket on the Bluecube Service Desk; • By sending an email to **help@bluecube.tech** • By calling the client specific **service desk number** • Through the on-line portal at **www.bluecube.tech** Each ticket will be triaged as a particular type: Incident, Request or Change, and the type of the ticket, linked with the impact and urgency, will define the Service Levels to which the ticket will be prioritised (please see SLA details below). If the Service Desk are unable to resolve the ticket, then it will be escalated to third line, field engineering and/or Problem engineering teams to resolve; these are typically internal Bluecube teams if the client is subscribed to these services, however it can also be to Client's internal teams or to external third parties. Our engineers may initiate Remote Support for servers without any input required from the client. This type of access is typically instigated for major issues or for system maintenance tasks. When delivering support to individuals, remote support will typically be instigated via a phone call. In the event that the engineer is unable to talk the user through to resolution, a remote-control session will be established to the user's device. All remote-control sessions are made via secure connections (using SSL data encryption). During a remote-control session, the end user (client) has complete control over the session and can terminate the remote session at any time. All remote support sessions are recorded with detailed logs of session activity. In addition to this, all phone calls in and out of Bluecube are also recorded which combine with the remote control audit logs and Lighthouse to provide a full audit trail of all activity with our clients.
Knowledge base	Bluecube Compass
WHEN	
Service hours	24 hours a day, 365 days a year. Although it should be noted outside of key operational hours (Monday to Friday, 08:30 to 17:30) 3rd line engineers are operating on an on-call basis only. Escalation to a 3rd line engineer can be instigated by the Service Desk for high priority issues.

TERMS & SLA	
Service Levels	The service levels to which we work are detailed below. Although the Service Desk operates 24x7x365 we measure our Service levels within our primary UK operational hours which are Monday to Friday, 08:30 to 17:30, excluding public holidays. Incidents An Incident is recorded when something is not working as it should be, for example a PC, laptop, printer or an application, etc. is not performing as expected. There are differing priorities that can be assigned to an Incident, each with varying response and target resolution times. We assign a priority based on the impact and urgency of the incident. **Priority** / **Response Time** / **Target Resolution** 1-Major / 15 minutes / 2 hours 2 - High / 30 minutes / 4 hours 3 - Medium / 45 minutes / 12 hours 4 - Low / 60 minutes / 24 hours 5 – As time permits / 120 minutes / 64 hours Requests A Request is recorded when we are being asked to do or change something for an individual. Good examples of a request would be a new user creation, expansion of disk space, help to use an application or system or the setup of a new printer. **Priority** / **Response Time** / **Target Resolution** All / 60 minutes / 24 hours Changes A Change is a request for an installation, move, addition or change to core infrastructure or something that will (or has the potential to) impact the entire organisation. A good example of a Change would be changes to a Firewall. Due to the nature of changes, we do not have defined target resolution times because they require planning and Client liaison to minimise any potential disruption. **Priority** / **Response Time** / **Target Resolution** All / 120 minutes / N/A Response Times and Target Resolution We have an internal objective to respond to any ticket within 15 minutes, however Bluecube has a contractual commitment to attempt to reach the individual who has raised a ticket within the stated Response Time for a particular ticket type and priority. In the event that the individual is not available, we will continue to attempt to contact them. Each contact attempt (be it via a phone call or email) will be recorded within Lighthouse. The Service Level 'Clock' will start once we have made contact with the individual who has raised the ticket. There may be times during the lifetime of a ticket when we are unable to conduct any work

	on it. A good example of this will be when a client is not available due to other commitments or if we are waiting on a third party to assist. During these times a ticket may be placed on hold. The time that a ticket is on hold will be taken into account and deducted from any Service Level calculations, as will any non-UK working hours (Bluecube's working hours for SLA calculations is Monday to Friday, 08:30 to 17:30, excluding bank holidays). Once we believe that a ticket has been resolved we will attempt to contact the individual who has raised the ticket to verify that they are happy with the resolution. If we are unable to reach them we will email them asking them to contact us and place the ticket on hold for 24 hours before trying again. If we are unable to reach them for a second time we will mark the ticket as Resolved and send an email to the individual explaining why we believe the ticket is resolved. If the Service Desk are unable to resolve the ticket then it will be escalated to third line, field engineering and/or Technical Specialists to resolve; these are typically internal Bluecube teams if the client is subscribed to these enhanced support services, however it can also be to Client's internal teams or to external third parties. The SLA measurement for these type of tickets move with the ticket to the resolving party.
Exclusions	Only Users registered in lighthouse will be able to log a support ticket.
Billing	This service is billed based on the number of users in your organisation. Every user within your organisation will need a Lighthouse Account as only users with a Lighthouse account can receive support and services from Bluecube. Users can be easily added and removed by using the user management tools within Lighthouse.
Client Responsibilities	Clients are expected to maintain a real and accurate list of their users via the Lighthouse portal. Lighthouse allows you to see all users that exist within your organisation at any one time. It is the Client's responsibility to ensure that Lighthouse is correct at all times. Please note that it is possible to have multiple user types, which will potentially attract different charges and varying services. These will be detailed in the contract if they exist. Once the monthly billing has been processed and the invoice issued on the 1st of each month then no corrections, or credits, will be made.

4. 3rd Line Support

WHAT	
Name	**3rd Line Support**
Overview	Our 3rd Line Support involves the investigation and resolution of tickets that have been escalated from the Service Desk (this will typically be an internal Bluecube Service Desk team; however it can also be from internal client teams). This is a syndicated service but can be provided as a dedicated service if required.
HOW	
Prerequisites	None
Procedures	An in-house developed system (Lighthouse) is used to manage all interactions of a technical nature with our clients and their users (typically requests for assistance or support). Each item that we work on is referred to as a ticket. For escalations from an internal Bluecube Service Desk, a ticket will be re-assigned to the 3rd Line Team. This will create a seamless flow from ticket creation through to resolution. For escalations from internal client teams a ticket must be logged within Lighthouse. There are three ways in which a client can log a ticket on the Bluecube Service Desk; • By sending an email to **help@bluecube.tech** • By calling the client specific **service desk number** • Through the on-line portal at **www.bluecube.tech** Our engineers may initiate Remote Support for servers without any input required from the client. When delivering support to individuals, remote support will typically be instigated via a phone call. In the event that the engineer is unable to talk the user through to resolution, a remote-control session will be established to the user's device. All remote-control sessions are made via secure connections (using SSL data encryption). During a remote-control session, the end user (client) has complete control over the session and can terminate the remote session at any time. All remote support sessions are recorded with detailed logs of session activity. In addition to this, all phone calls in and out of Bluecube are also recorded which combine with the remote-control audit logs and Lighthouse to provide a full audit trail of all activity with our clients.
Knowledge base	Bluecube Compass
WHEN	
Service hours	24 hours a day, 365 days a year.
TERMS & SLA	
Service Levels	Please refer to the Service Levels as detailed in '24x7 Service Desk' as they apply to this service also.
Exclusions	Only Users registered in Lighthouse will be able to log a support ticket.
Billing	This service is billed based on the number of users in your organisation. Every user within your organisation will need a Lighthouse Account as only users with a Lighthouse account can receive support and services from Bluecube. Users can be easily added and removed by using the user management tools within Lighthouse.

	When a user is added in Lighthouse, a ticket is automatically generated for Bluecube engineers to create their user account within your organisations systems. Likewise when a user is removed, a request will be automatically generated to remove the user from your systems. The Lighthouse portal is the only way that users can be added and removed from your systems; this process is designed to ensure that Lighthouse is a true reflection of your organisations users. Each new user will also receive a welcome call to talk them through our service, ensure that they have access to Lighthouse and that their IT is working for them from the outset. (All welcome calls are exempt from any SLA).
Client Responsibilities	Clients are expected to maintain a real and accurate list of their users via the Lighthouse support portal. Lighthouse allows you to see all users that exist within your organisation at any time. It is the Client's responsibility to ensure that Lighthouse is always correct. Please note that it is possible to have multiple user types, which will potentially attract different charges and varying services and these will be detailed in the contractual documentation if they exist Once the monthly billing has been processed and the invoice issued on the 1st of each month then no corrections, or credits, will be made.

5. Field Engineering

WHAT	
Name	**Field Engineering**
Overview	Field Engineering (sometimes referred to as on-site support) involves the dispatch of a Bluecube engineer to a client site for the investigation of a ticket with a view to working with the Bluecube office based engineering teams to progress the ticket towards resolution. This is a syndicated service.
HOW	
Prerequisites	'24x7 Service Desk' and/or '3rd Line Support'.
Procedures	Field Engineering can only be engaged though the escalation of an existing Lighthouse ticket. Any tickets requiring Field Engineering will be re-assigned to the Field Engineering Team. This will create a seamless flow from ticket creation through to resolution. Full-time second and third-line engineers deliver Field Engineering, sometimes referred to as on-site support. Bluecube will dispatch an engineer on-site when a ticket (irrespective of its priority) cannot be resolved remotely in a timely or effective manner. The decision to dispatch an engineer resides with Bluecube.
Knowledge base	Bluecube Compass
WHEN	
Service hours	Normal UK working hours. Monday to Friday, 08:30 to 17:30, excluding UK bank holidays.
TERMS & SLA	
Service Levels	Please refer to the Service Levels as detailed in '24x7 Service Desk' as they apply to this service also.
Exclusions	Only Users registered in Lighthouse will be able to log a support ticket. Locations not included within the contract; typically, Field Engineering will only be delivered to the head office of an organisation, unless explicitly stated within the contract.
Billing	This service is billed based on the number of users in your organisation and is typically included in the per user charge for '24x7 Service Desk' and/or '3rd Line Support'. For any Field Visits required that fall outside the scope of support (e.g. projects) these will be charged for on a day rate basis and will typically be included within the scope of a fixed-price project.
Client Responsibilities	Provision of any relevant site or health and safety training. Any site-specific guidance that will be required by our visiting engineer. Provision of any required health and safety equipment or guidance provided in advance relating to any required equipment.

6. Dedicated Resource

WHAT	
Name	**Dedicated Resource**
Overview	The provision of dedicated resource to deliver a stand-alone service for a client, or to supplement other services, to deliver a bespoke or boutique service.
HOW	
Prerequisites	None
Procedures	Bluecube will provide the agreed resources to the client. The skill, availability and number of resources will be defined in the contract, or an appendix to the contract.
Knowledge base	Bluecube Compass
WHEN	
Service hours	As agreed within the client agreement.
TERMS & SLA	
Service Levels	As agreed within the client agreement.
Exclusions	As agreed within the client agreement.
Billing	As agreed within the client agreement; typically, this is delivered for a fixed monthly fee.
Client Responsibilities	To be defined as part of the solution required.

7. User Account Management (UAM)

<table>
<tr><td colspan="2">WHAT</td></tr>
<tr><td>Name</td><td>User Account Management (UAM)</td></tr>
<tr><td>Overview</td><td>The creation of ‘user accounts’ for people when they join a client and the deactivation of their accounts when they leave a client.</td></tr>
<tr><td colspan="2">HOW</td></tr>
<tr><td>Prerequisites</td><td>24x7 Service Desk</td></tr>
<tr><td>Procedures</td><td>When a user is added in Lighthouse a ticket is automatically generated for Bluecube engineers to create their user account within your organisations IT systems. Likewise when a user is removed a request will be automatically generated to remove the user from your systems.

Bluecube will create and store a defined process for the creation and deactivation of users. Where possible Bluecube will use automation to streamline this process (not all UAM processes will be able to be automated).

Any change to the agreed UAM processes could be subject to formal Change Control and testing depending on the nature of the change and if it falls under formal change request processes.

The Lighthouse portal is the only way that users can be added and removed from your systems; this process is designed to ensure that Lighthouse is a true reflection of your organisations users. Each new user will also receive a welcome call to talk them through our service, ensure that they have access to Lighthouse and that their IT is working for them from the outset. (All welcome calls are exempt from any SLA).</td></tr>
<tr><td>Knowledge base</td><td>Bluecube Compass</td></tr>
<tr><td colspan="2">WHEN</td></tr>
<tr><td>Service hours</td><td>As agreed within the client agreement.</td></tr>
<tr><td colspan="2">TERMS & SLA</td></tr>
<tr><td>Service Levels</td><td>A UAM is defined as a Request and is therefore subject to the following SLA. Although we would recommend that as much notice as possible of a new starter is provided.

<table><tr><th>Priority</th><th>Response Time</th><th>Target Resolution</th></tr><tr><td>All</td><td>60 minutes</td><td>24 hours</td></tr></table>
For any UAM processes that refer to or rely on third parties we reserve the right to remove our SLA obligation. UAM Processes are related to the creation of the user’s system accounts and are not inclusive of the supply or delivery of any hardware.</td></tr>
<tr><td>Exclusions</td><td>Anything detailed outside of the agreed UAM processes.</td></tr>
<tr><td>Billing</td><td>This service is typically included in the per user charge for ‘24x7 Service Desk’ and/or ‘3rd Line Support’.</td></tr>
<tr><td>Client Responsibilities</td><td>To inform Bluecube of any changes to the UAM processes and to work with us through formal Change Control and testing.</td></tr>
</table>

8. Contract Review Meeting

WHAT	
Name	**Contract Review Meeting**
Overview	This is a scheduled review of specific services being provided within a service delivery contract with a view to assessing the performance of the relevant services against the outcomes defined within the service description. If further action is deemed necessary during the review, then stated outcomes for performance must be defined as part of the process and timeframes are to be established to the achievement of these metrics. The review is to be arranged via the client engagement manager.
HOW	
Prerequisites	Subscription to a relevant ongoing service from Bluecube
Procedures	Each Bluecube client will be provided with a named CEM. Contact with the CEM can be made through email or phone. The CEM will take ownership of arranging the session and minuting the actions and next steps. The output will be a series of objectives and a timeframe. The output could also be the establishment of a service improvement programme (SIP).
Knowledge base	Bluecube Compass
WHEN	
Service hours	Normal UK working hours. Monday to Friday, 08:30 to 17:30, excluding UK bank holidays.
TERMS & SLA	
Service Levels	-
Exclusions	-
Billing	N/A
Client Responsibilities	To ensure clarity around actions and to engage in the process productively.

9. Service Improvement Plan (SIP)

WHAT	
Name	**Service Imrpovement Plan (SIP)**
Overview	Bluecube define a SIP as a formal and documented set of objectives taken as output from a contract review meeting. Each output will be related to a Bluecube Service Description and the SIP will detail any metrics or actions required to improve or meet agreed service level agreements. A timeframe will be established with which to achieve the metrics set out within the SIP and at the end of the timeframe a review will be held to assess the impact of the SIP.
HOW	
Prerequisites	Subscription to a relevant ongoing service from Bluecube and following a Contract Review meeting.
Procedures	Each Bluecube client will be provided with a named CEM. Contact with the CEM can be made through email or phone. The CEM will take ownership of arranging the session and minuting the actions and next steps. The output will be a series of objectives and a timeframe. The output could also be the establishment of a service improvement programme (SIP).
Knowledge base	Bluecube Compass
WHEN	
Service hours	Normal UK working hours. Monday to Friday, 08:30 to 17:30, excluding UK bank holidays.
TERMS & SLA	
Service Levels	-
Exclusions	-
Billing	N/A
Client Responsibilities	To ensure clarity around actions and to engage in the process productively.

SECTION TWO
SECURITY SERVICES

Services to secure our clients data and systems.

10.Security Operations Centre (SOC)

WHAT	
Name	**Security Operations Centre (SOC)**
Overview	A dedicated, centralised team of Security Analysts and Engineers whose primary responsibility is monitoring client IT system environments for vulnerabilities, acceptable use/policy violations, unauthorised activity, network intrusions and provides direct support of cyber Incident Response process. The SOC team are also responsible for the delivery and management of all other Security Services that a client receives from Bluecube.
HOW	
Prerequisites	None (the SOC can be delivered as a standalone service)
Procedures	The SOC team leverage the security tools sets of the clients (typically provided by Bluecube as part of a Managed Security Service) in order to provide the following SOC operations; **Monitor Security Posture** Monitoring the client's environment for security conditions, alarms and responding through various technical solution(s). **Initiate & Manage Incident Response** Validating security incidents based on alerts and network monitoring activities. Initiate IR support from vendors, forensic, regulators and other third party sources as required. **Reporting** Run reports to support IT General Controls monitoring and compliance requirements. Run reports to support alarms, incidents and respond to additional data requests. When any action is required an 'Event' ticket will be created in Lighthouse (or a SIEM toolset) to track all activities in relation to an Event. The SOC team will often work in conjunction with other teams to resolve an issue.
Knowledge base	Bluecube Compass
WHEN	
Service hours	This is an 'always on' service. This means that the solution is designed to be available and operational at all times.
TERMS & SLA	
Service Levels	The target uptime for this service in any given month is 99.5%
Exclusions	Managing or responding to anything that is not deemed to be a Security related alert or any alarms/alerts outside of the scoped, agreed data sources being monitored by the SOC.
Billing	Typically delivered for a flat monthly fee. Occasionally integrated as a per user charge, or per device, (as stated in the contract).
Client Responsibilities	None

11. SentinelOne only SOC

WHAT	
Name	**SentinelOne only SOC**
Overview	A condensed version of the Security Operations Centre that is delivered by a dedicated team of Security Analysts and Engineers whose responsibility is responding to SentinelOne alerts in order to help protect clients against cyberattacks
HOW	
Prerequisites	SentinelOne (End-Point Detection and Response)
Procedures	The SOC team leverage SentinelOne in order to identify unusual, suspicions or malicious activity. When any action is required an 'Event' ticket will be created in Lighthouse to track all activities in relation to an Event. The SOC team will often work in conjunction with other teams to resolve an issue.
Knowledge base	Bluecube Compass
WHEN	
Service hours	This is an 'always on' service. This means that the solution is designed to be available and operational at all times.
TERMS & SLA	
Service Levels	The target uptime for this service in any given month is 99.5%
Exclusions	Any alerts that are not identified by SentinelOne
Billing	Typically delivered for a flat monthly fee. Occasionally integrated as a per user charge, or per device, (as stated in the contract).
Client Responsibilities	To engage with Bluecube to help remedy any alerts. It is possible action many be required by the client in order to mitigate and contain a cyber event.

12. Crisis / Incident Response

WHAT	
Name	**Crisis / Incident Response**
Overview	A dedicated Crisis Response team who will respond to any major incident or crisis (typically, but not exclusively, following a cyberattack). The goal of the team is to reduce the time and disruption suffered by organisations that have fallen victim to a Cyber Incident and recover their systems as quickly as possible.
HOW	
Prerequisites	None
Procedures	A Crisis / Incident Response by its very nature is agile. It requires rapid and dynamic thinking and each engagement is unique. It is for that reason that we have a dedicated Crisis Response team that will lead all engagements to address incident classification, triage, containment, eradication and business recovery activities This dedicated team will be supported by other delivery functions within Bluecube, such as our SOC, NOC and Technical Specialists.
Knowledge base	Bluecube Compass
WHEN	
Service hours	This is an 'always available' service. This means that the service is designed to be available clients at all times.
TERMS & SLA	
Service Levels	N/A
Exclusions	Any specialist third party (external) fees required e.g. Forensics, Data Recovery or new hardware. Provision of the service where a client has chosen *NOT* to adopt or take specific security related advice/recommendations provided by Bluecube (in this scenario the service can still be made available to the client, however a fee for the service will be charged, even if the contract states that it is included).
Billing	Typically delivered for an agreed one-off fee or provided as an integrated service for those client taking the Security Operations Centre (SOC) service. The associated Service Contract will confirm if this service is included (if it is there are no additional fees for the utilisation of this service).
Client Responsibilities	To ensure availability of key personnel including stakeholders to discuss (and approve) any necessary, or recommended, actions

13. External Attack Surface Management (EASM)

WHAT	
Name	**External Attack Surface Management (EASM)**
Overview	External Attack Surface Management (EASM) is a cybersecurity discipline that identifies and manages the risks presented by internet-facing assets and systems. EASM refers to the processes and technology necessary to discover external-facing assets and effectively manage the vulnerabilities of those assets.
HOW	
Prerequisites	Security Operations Centre (SOC)
Procedures	The EASM service is initially configured and defined through a consultation and discovery phase with the client. Any vulnerabilities identified through this process will be highlighted to the client (with a view to rectifying). The SOC team will then configure the EASM toolsets to continually monitor the client's internet facing assets and systems for changes and vulnerabilities. When any change is identified an 'Event' ticket will be created in Lighthouse to track all activities in relation to that change (where it be for information only or to address a vulnerability).
Knowledge base	Bluecube Compass
WHEN	
Service hours	This is an 'always on' service. This means that the solution is designed to be available and operational at all times.
TERMS & SLA	
Service Levels	The target uptime for this service in any given month is 99.5%
Exclusions	Any non-internet facing systems
Billing	Integrated as a per user charge, or a one-off consultancy charge for each manual review.
Client Responsibilities	To ensure availability to discuss (and approve) any necessary, or recommended, actions.

14. Intune Policy Management

WHAT	
Name	**Intune Policy Management**
Overview	The manual review of Intune policies in respect of security.
HOW	
Prerequisites	N/A
Procedures	Intune is a 'living' product that is updated by Microsoft on a continual basis. As a result a regular review of the security policies within Intune are required to ensure that a Client's environment is benefiting from the latest available policies within Intune. This is a manual process that is conducted by Bluecube in conjunction with the client.
Knowledge base	Bluecube Compass
WHEN	
Service hours	This is a manual review and reporting service that is conducted every three months as part of your security service.
TERMS & SLA	
Service Levels	The service will be delivered every 6 months.
Exclusions	-
Billing	Integrated as a per user charge, or a one-off consultancy charge for each manual review.
Client Responsibilities	To ensure availability to discuss (and approve) any necessary, or recommended, actions.

15. Anti-Virus Monitoring

WHAT	
Name	**Anti-Virus Monitoring**
Overview	The monitoring of the Client estate to confirm Anti-Virus protection and coverage is in place. To stop known viruses and malware. This includes the provision of reports (on request).
HOW	
Prerequisites	Proactive Monitoring.
Procedures	Proactive monitoring checks all devices at least every 5 minutes to verify that the Anti-Virus is installed and operational. Alert thresholds will be configured to alert when a device is identified that does not have Anti-Virus installed or operational. These alerts result in tickets being generated within Lighthouse for further investigation.
Knowledge base	Bluecube Compass
WHEN	
Service hours	This is an 'always on' service. This means that the solution is designed to be available and operational at all times.
TERMS & SLA	
Service Levels	The target uptime for this service in any given month is 99.5%
Exclusions	Automatic install of monitoring agents outside of a domain or Intune environment.
Billing	Integrated as a per user charge, or per device (as stated in the contract).
Client Responsibilities	Notification of any non-Windows/Linux devices requiring monitoring. Support in installing the agent on standalone machines or workgroups requiring proactive monitoring support.

16. Patch Management (Microsoft)

WHAT	
Name	**Patch Management (Microsoft)**
Overview	The Patch Management service provides automated download and deployment of Microsoft application and Operating System updates to fix known vulnerabilities in Microsoft software. Patching coverage across supported estates can also be reported on.
HOW	
Prerequisites	Proactive Monitoring
Procedures	Our Proactive Monitoring agent is used to deploy and install authorised operating system and Microsoft application updates. Following a standard update schedule designed to provide flexibility and stability of core services. These are customisable upon request and only deal with the provision of Microsoft delivered patches.
Knowledge base	Bluecube Compass
WHEN	
Service hours	Patch Management is scheduled to deploy to an agreed maintenance schedule. The schedule will be agreed with the client on a case-by-case basis, detailing both endpoints and servers. Ensuring that critical security patches are updated on a regular basis and that the underlying infrastructure is updated in the correct sequence and rebooted as required.
TERMS & SLA	
Service Levels	The target uptime for this service in any given month is 99.5%
Exclusions	Any device that does not have the Bluecube Monitoring Agent installed. Any Microsoft application or system that is outside of Microsoft support.
Billing	Integrated as a per user charge, or per device (as stated in the contract).
Client Responsibilities	To approve the maintenance window for patching and server reboots.

17. Patch Management (3rd Party)

WHAT	
Name	**Patch Management (3rd Party)**
Overview	The Patch Management service provides automated download and deployment of selected 3rd party applications updates to fix known vulnerabilities in software.
HOW	
Prerequisites	Proactive Monitoring
Procedures	Our Proactive Monitoring agent is used to deploy and install authorised application updates. Following a standard update schedule designed to provide flexibility and stability of core services. These are customisable upon request.
Knowledge base	Bluecube Compass
WHEN	
Service hours	Patch Management is scheduled to deploy to an agreed maintenance schedule. The schedule will be agreed with the client on a case-by-case basis.
TERMS & SLA	
Service Levels	The target uptime for this service in any given month is 99.5%
Exclusions	Any device that does not have the Bluecube Monitoring Agent installed. Any software package that does not make patch repositories available to the patching tool. Any software application that is not under manufacturer or vendor support.
Billing	Integrated as a per user charge, or per device (as stated in the contract).
Client Responsibilities	Any bespoke requirements that fall outside of the Bluecube default patch management policy.

18. Encryption Status

WHAT	
Name	**Encryption Status**
Overview	The monitoring of the Client estate to confirm all devices are encrypted. This includes the provision of reports (on request). To ensure that if a laptop is stolen or lost, all data on it is subject to encryption in order to mitigate unauthorised access.
HOW	
Prerequisites	An encryption solution (typically, but not exclusively, delivered via Intune policies).
Procedures	Our Proactive Monitoring agent is used to confirm the encryption status of all devices. The output is a monthly report to verify the encryption status of the client estate. For any devices that are highlighted as not encrypted a Service Desk ticket will be logged in order to resolve the issue.
Knowledge base	Bluecube Compass
WHEN	
Service hours	This is an 'always on' service. This means that the solution is designed to be available and operational at all times, with reporting issued monthly.
TERMS & SLA	
Service Levels	The target uptime for this service in any given month is 99.5%
Exclusions	Any device that does not have the Bluecube Monitoring Agent installed or that is not enrolled into Intune.
Billing	Integrated as a per user charge.
Client Responsibilities	-

19. Password Enforcement (Monitoring)

WHAT	
Name	**Password Enforcement (Monitoring)**
Overview	The monitoring of the Client user accounts to ensure that passwords meet the complexity requirements as recommended by Microsoft.
HOW	
Prerequisites	Proactive Monitoring
Procedures	Bluecube will deploy toolsets to the client estate that will return a report of all user accounts and their associated attributes, including the password format. This report is then checked on a regular basis and guidance provided to the client accordingly, typically in the form of password policy advice or enforcement.
Knowledge base	Bluecube Compass
WHEN	
Service hours	This is an 'always on' service. This means that the solution is designed to be available and operational at all times.
TERMS & SLA	
Service Levels	The target uptime for this service in any given month is 99.5%
Exclusions	Any device that does not have the Bluecube Monitoring Agent installed or that is not enrolled into Intune.
Billing	Integrated as a per user charge.
Client Responsibilities	-

20. Multi-Factor-Authentication (MFA)

WHAT	
Name	**Multi-Factor-Authentication (MFA)**
Overview	The application of, and monitoring of the Client estate to confirm that all accounts have MFA enforced.
HOW	
Prerequisites	Installation of the proprietary Security Toolset (Poseidon), a platform that supports MFA in a reportable format, for instance Microsoft 365.
Procedures	MFA enforcement checks are carried out monthly, using the Poseidon credential auditing tool and the results provided to the client as part of a monthly security review. MFA enforcement policy will be defined with the client.
Knowledge base	Bluecube Compass
WHEN	
Service hours	This is an 'always on' service. This means that the solution is designed to be available and operational at all times. Reporting on the service is dependent on the Bluecube Security Service and when in place is delivered monthly.
TERMS & SLA	
Service Levels	The target uptime for this service in any given month is 99.5% (NB – MFA once enabled is always on and falls under Microsoft SLAs).
Exclusions	Platforms or systems that do not support MFA.
Billing	Ongoing management and reporting of MFA is integrated as a per user charge within the security service.
Client Responsibilities	To ensure that Lighthouse is kept up to date with all new starters and leavers.

21. Privileged Account Creation

WHAT	
Name	**Privileged Account Creation**
Overview	The monitoring of the Client estate to alert when new privileged (administration) accounts are created. This is to allow verification of all privileged account creation activity.
HOW	
Prerequisites	Installation of the proprietary Security Toolset (Poseidon), a compatible directory-based core IT platform, i.e. Microsoft Azure Active Directory.
Procedures	Checks for Privileged (administrative) accounts are carried out monthly, using the Poseidon credential auditing tool and the results provided to the client as part of a monthly security review. Accounts checked will be based on Active Directory or Azure Active Directory. Google Directory Services can be checked but may be subject to an additional charge.
Knowledge base	Bluecube Compass
WHEN	
Service hours	Auditing of privileged accounts takes place monthly.
TERMS & SLA	
Service Levels	A report will be created, and shared, on a monthly basis.
Exclusions	Technology Platforms that do not provide a centralised directory in a supported format.
Billing	Integrated as a per user charge within the Security Service.
Client Responsibilities	To review the report and take any necessary, or recommended, actions to remove unrequired or suspicious (unknown) accounts; Bluecube can assist with this process if there is an IT Support contract in place (over and above the Managed Security Service).

22. Credential Audit (Account Status)

WHAT	
Name	**Credential Audit (Account Status)**
Overview	The monitoring of the Client estate to provide reports on user account usage and status. This is to ensure that the estate does not have 'stale' or old accounts still active.
HOW	
Prerequisites	Installation of the proprietary Security Toolset (Poseidon), a compatible directory-based core IT platform, i.e. Microsoft Azure Active Directory.
Procedures	Checks for stale accounts are carried out monthly, using the Poseidon credential auditing tool and the results provided to the client as part of a monthly security review. Accounts checked will be based on Active Directory or Azure Active Directory. Google Directory Services can be checked but may be subject to an additional charge.
Knowledge base	Bluecube Compass
WHEN	
Service hours	This is a reporting service, part of the overall Bluecube Security Service and reporting to the client is carried out monthly.
TERMS & SLA	
Service Levels	-
Exclusions	-
Billing	Integrated as a per user charge within the Security Service.
Client Responsibilities	To review the report and take any necessary, or recommended, actions to remove unrequired or suspicious (unknown) accounts; Bluecube can assist with this process if there is an IT Support contract in place (over and above the Managed Security Service).

23. Office 365 Hardening

WHAT	
Name	**Office 365 Hardening**
Overview	Analysing and improving the MS 365 Tenancy Secure Score. Ensuring that your Microsoft Cloud environment is hardened and remains that way; this is an ongoing task as Microsoft are constantly evolving the Office 365 ecosystem and cyber security threats are also ever changing and developing. We recommend that this service is carried out every six months.
HOW	
Prerequisites	A Microsoft 365 based cloud tenancy.
Procedures	Bluecube maintain a best practise approach to ensuring that Microsoft 365 tenancies are configured to an ideal blend of security and operability. Increasing the Secure Score of the target tenancy considerably over the 'out of the box' configuration. Looking at all aspects from Exchange Online right through to endpoint management rules.
Knowledge base	Bluecube Compass
WHEN	
Service hours	This is a manual review and reporting service that is conducted every six months as part of your security service.
TERMS & SLA	
Service Levels	-
Exclusions	-
Billing	Integrated as a per user charge, or a one-off consultancy charge, for each manual review.
Client Responsibilities	To review the report and take any necessary, or recommended, actions; Bluecube can assist with this process if there is an IT Support contract in place (over and above the Managed Security Service).

24. Kerberos Reset

WHAT	
Name	**Kerberos Reset**
Overview	Kerberos is a computer network security protocol that authenticates service requests between two or more trusted hosts. It uses secret-key cryptography and a trusted third party for authenticating client-server applications and verifying users' identities. Kerberos is now the default authorisation technology used by Microsoft Windows. Kerberos is used in Active Directory and is also an alternative authentication system to SSH, POP, and SMTP. The issue (from a security perspective) is that the Kerberos protocol is a target for cybercrime and is often used to create a back door into an environment. In order to mitigate this risk we perform Kerberos resets every six months, and immediately should any suspicious activity be detected.
HOW	
Prerequisites	None
Procedures	TBC
Knowledge base	Bluecube Compass
WHEN	
Service hours	This is a manual review and reporting service that is conducted every six months as part of your security service.
TERMS & SLA	
Service Levels	The service will be delivered every 6 months.
Exclusions	-
Billing	Integrated as a per user charge, or a one off consultancy charge for each manual review.
Client Responsibilities	To review the report and take any necessary, or recommended, actions; Bluecube can assist with this process if there is an IT Support contract in place (over and above the Managed Security Service).

25. SentinelOne (End-Point Detection and Response)

WHAT	
Name	**SentinelOne (End-Point Detection and Response)**
Overview	The provision of SentinelOne Complete software for deployment across the client estate.
HOW	
Prerequisites	None, although a SOC service is required in order for Bluecube to response to alerts.
Procedures	Bluecube will provide SentinelOne Complete and deploy it across all known devices. This is done through leveraging any estate monitoring in place and is typically supplemented through Network Monitoring and the Sentinel Ranger solution in order to capture all devices within the Client network. All installations will be set to 'detect only' mode for an agreed period of time (in order to allow the Artificial Intelligence engine to learn about normal behaviours and to allow any exclusion list to be created by Bluecube). Following this bedding in period (typically a week, although this can vary) SentinelOne will be switched to 'Protect mode' which will provide real-time protection for all devices that SentinelOne is installed on. Any alerts will be responded to by the Bluecube SOC (with all activities being tracked within a Lighthouse ticket).
Knowledge base	Bluecube Compass
WHEN	
Service hours	This is an 'always on' service. This means that the solution is designed to be available and operational at all times.
TERMS & SLA	
Service Levels	The target uptime for this service in any given month is 100% for any device that is operational and powered on.
Exclusions	-
Billing	Integrated as a per user charge, or per device (as stated in the contract), subject to a minimum term commitment of 12-months.
Client Responsibilities	To take any necessary, or recommended, actions.

26. Event Monitoring (Active Directory)

WHAT	
Name	**Event Monitoring (Active Directory)**
Overview	Monitoring for unusual, or suspicious, behaviours and actions across your IT estate (Active Directory) that could indicate an attempted, or live, cyber incident.
HOW	
Prerequisites	Installation of the Bluecube Monitoring Agent
Procedures	The following activities will be checked for every 5 minutes. • Replay Attack; indication of a Kerberos attack. • Audit Policy Change; identification that someone has changed a system audit policy (something malicious actors will do before an attack) and is therefore detection of potential malicious activity. • SID History added to an account; identification that someone has added SID history to an account. Malicious actors commonly alter SID-HISTORY to escalate privileges and impersonate users. • SID History attempt to add to an account failed; identification that someone has tried to add SID history to an account but failed. Malicious actors commonly alter SID-HISTORY to escalate privileges and impersonate users. • Directory Services Restore Mode; identifies an attempt made to change the password of the Directory Services Restore Mode admin password. This is vitally important – if someone is able to enter DSRM they can edit and access the Active Directory database. When we detect these activities – a ticket is logged in our Service Management toolset, Lighthouse, and we respond accordingly, ensuring that all actions and activities are tracked and monitored in a transparent way, so you can see exactly what steps have been taken.
Knowledge base	Bluecube Compass
WHEN	
Service hours	This is an 'always on' service. This means that the solution is designed to be available and operational at all times.
TERMS & SLA	
Service Levels	The target uptime for this service in any given month is 99.5%
Exclusions	-
Billing	Integrated as a per user charge, or a one off consultancy charge for each manual review.
Client Responsibilities	To take any necessary, or recommended, actions.

27. Event Monitoring (Office 365 / Azure)

WHAT	
Name	**Event Monitoring (Office 365/Azure)**
Overview	Monitoring for unusual, or suspicious, behaviours and actions across your IT estate (Office 365 and/or Azure) that could indicate an attempted, or live, cyber incident.
HOW	
Prerequisites	Microsoft Cloud Access Security Broker Subscriptions for all users
Procedures	The following activities will be checked for every 5 minutes. • Activity from anonymous IP address; activity from an IP address that has been identified as an anonymous proxy IP address by Microsoft Threat Intelligence or by Bluecube's SOC. These proxies can be used to hide a device's IP address and may be used for malicious activities. • Activity from infrequent country; Activity from a country/region that could indicate malicious activity. We profile your environment and trigger alerts when activity is detected from a location that was not recently or was never visited by any user in the Client organisation. • Activity from suspicious IP addresses; activity from an IP address that has been identified as risky by Microsoft Threat Intelligence or by Bluecube's SOC. These IP addresses were identified as being involved in malicious activities, such as botnet command and control (C&C), and may indicate a compromised account. • Impossible Travel; activity from the same user in different locations within a time period that is shorter than the expected travel time between the two locations. This can indicate a credential breach, however, it's also possible that the user's actual location is masked, for example, by using a VPN. • Misleading OAuth app name; this detection identifies apps with characters, such as foreign letters, that resemble Latin letters. This can indicate an attempt to disguise a malicious app as a known and trusted app so that attackers can deceive users into downloading their malicious app. • Misleading publisher name for an OAuth app; this detection identifies apps with characters, such as foreign letters, that resemble Latin letters. This can indicate an attempt to disguise a malicious app as a known and trusted app so that attackers can deceive users into downloading their malicious app. • Multiple storage deletion activities; activities in a single session indicating that a user performed an unusual number of cloud storage or database deletions from resources such as Azure blobs, AWS S3 buckets, or Cosmos DB when compared to the baseline learned. This can indicate an attempted breach of your organization. • Multiple VM creation activities; activities in a single session indicating that a user performed an unusual number of VM creation actions when compared to the baseline learned. Multiple VM creations on a breached Cloud infrastructure could indicate an attempt to run crypto mining operations from within your organization. • Suspicious creation activity for cloud region; activities indicating that a user performed an unusual resource creation action in an uncommon region when compared to the baseline learned. Resource creation in uncommon cloud regions could indicate an attempt to perform a malicious activity such as crypto mining operations from within your organization. • Activity performed by terminated user; activity performed by a terminated user can indicate that a terminated employee who still has access to corporate resources is trying to perform a malicious activity. • Suspicious change of CloudTrail logging service (AWS users only); activities in a single session indicating that, a user performed suspicious changes to the AWS CloudTrail logging service. This can indicate an attempted breach of your organization. When disabling CloudTrail, operational changes are no longer being logged. An attacker can perform malicious activities while avoiding a CloudTrail audit event, such as modifying an S3 bucket from private to public.

	• Suspicious email deletion activity (by user); activities in a single session indicating that, a user performed suspicious email deletions. This can indicate an attempted breach of your organization, such as attackers attempting to mask operations by deleting emails related to spam activities. • Suspicious inbox manipulation rule; activities indicating that an attacker gained access to a user's inbox and created a suspicious rule. Security Manipulation rules, such as deleting or moving messages, or folders, from a user's inbox may be an attempt to exfiltrate information from your organization. Similarly, they can indicate an attempt to manipulate information that a user sees or to use their inbox to distribute spam, phishing emails, or malware. Cloud App Security profiles your environment and triggers alerts when suspicious inbox manipulation rules are detected on a user's inbox. This may indicate that the user's account is compromised. • Unusual administrative activity (by user); activities indicating that an attacker has compromised a user account and performed administrative actions that are not common for that user. For example, an attacker can try to change a security setting for a user, an operation that is relatively rare for a common user. Cloud App Security creates a baseline based on the user's behaviour and triggers an alert when the unusual behaviour is detected. • Multiple failed login attempts; failed login attempts could indicate an attempt to breach an account. However, failed logins can also be normal behaviour. For example, when a user entered a wrong password by mistake. To achieve accuracy and alert only when there is a strong indication of an attempted breach, Cloud App Security establishes a baseline of login habits for each user in the organization and will only alert when the unusual behaviour is detected. • Unusual addition of credentials to an OAuth app; this detection identifies the suspicious addition of privileged credentials to an OAuth app. This can indicate that an attacker has compromised the app, and is using it for malicious activity. • Suspicious Power BI report sharing; activities indicating that a user shared a Power BI report that may contain sensitive information identified using NLP to analyse the metadata of the report. The report was either shared with an external email address, published to the web, or a snapshot was delivered to an externally subscribed email address. This can indicate an attempted breach of your organization. • Unusual impersonated activity (by user); in some software, there are options to allow other users to impersonate other users. For example, email services allow users to authorize other users to send email on their behalf. This activity is commonly used by attackers to create phishing emails in an attempt to extract information about your organization. Cloud App Security creates a baseline based on the user's behaviour and creates an activity when an unusual impersonation activity is detected. • Suspicious inbox forwarding; activities indicating that an attacker gained access to a user's inbox and created a suspicious rule. Manipulation rules, such as forward all or specific emails to another email account may be an attempt to exfiltrate information from your organization. Cloud App Security profiles your environment and triggers alerts when suspicious inbox manipulation rules are detected on a user's inbox. This may indicate that the user's account is compromised. • Unusual file download (by user); activities indicating that a user performed an unusual number of file downloads from a cloud storage platform when compared to the baseline learned. This can indicate an attempt to gain information about the organization. Cloud App Security creates a baseline based on the user's behaviour and triggers an alert when the unusual behaviour is detected. • Unusual file share activity (by user); activities indicating that a user performed an unusual number of file sharing actions from a cloud storage platform when compared to the baseline learned. This can indicate an attempt to gain information about the organization. Cloud App Security creates a baseline based on the user's behaviour and triggers an alert when the unusual behaviour is detected.

	• Multiple delete VM activities; activities in a single session indicating that a user performed an unusual number of VM deletions when compared to the baseline learned. Multiple VM deletions could indicate an attempt to disrupt or destroy an environment. However, there are many normal scenarios where VMs are deleted. • Ransomware activity; Cloud App Security uses security research expertise, threat intelligence, and learned behavioural patterns to identify ransomware activity. For example, a high rate of file uploads, or file deletions, may represent an encryption process that is common among ransomware operations. • Unusual file deletion activity (by user); activities indicating that a user performed an unusual file deletion activity when compared to the baseline learned. This can indicate ransomware attack. For example, an attacker can encrypt a user's files and delete all the originals, leaving only the encrypted versions that can be used to coerce the victim to pay a ransom. Cloud App Security creates a baseline based on the user's normal behaviour and triggers an alert when the unusual behaviour is detected. When we detect these activities – a ticket is logged in our Service Management toolset, Lighthouse, and we respond accordingly, ensuring that all actions and activities are tracked and monitored in a transparent way, so you can see exactly what steps have been taken.
Knowledge base	Bluecube Compass
WHEN	
Service hours	This is an 'always on' service. This means that the solution is designed to be available and operational at all times.
TERMS & SLA	
Service Levels	The target uptime for this service in any given month is 99.5%
Exclusions	-
Billing	Integrated as a per user charge, or a one off consultancy charge, for each manual review.
Client Responsibilities	To take any necessary, or recommended, actions.

28. GPO Changes

WHAT	
Name	**GPO Changes**
Overview	The monitoring of the Client estate to alert when new GPO's are created or existing ones changed. This is to allow verification of GPO related activity (malicious actors often change GPO's once they have compromised an environment).
HOW	
Prerequisites	Installation of the proprietary Security Toolset (Poseidon)
Procedures	Checks for a known 'safe' state for GPO's. Then, using Poseidon, a daily audit and review of all GPO's are carried out. Any changes are flagged and a ticket will be logged within Lighthouse for review to ensure that it is not malicious activity.
Knowledge base	Bluecube Compass
WHEN	
Service hours	This is an 'always on' service. This means that the solution is designed to be available and operational at all times.
TERMS & SLA	
Service Levels	The target uptime for this service in any given month is 99.5%
Exclusions	-
Billing	Integrated as a per user charge.
Client Responsibilities	To review the report and take any necessary, or recommended, actions to remove unrequired or suspicious (unknown) accounts; Bluecube can assist with this process if there is an IT Support contract in place (over and above the Managed Security Service).

29. Dark Web Monitoring

WHAT	
Name	**Dark Web Monitoring**
Overview	The monitoring of the Dark Web to identify any specific threats by looking for any mention of the Client's domain name and external IP addresses (as these are items of information that are valuable to a malicious actor and are unique and identifiable to an organisation).
HOW	
Prerequisites	None
Procedures	Bluecube will monitor the Dark Web for all Client known IP addresses and domain names. The presence of this information available on the Dark Web would indicate a potential imminent threat in addition to a compromise of credentials of exfiltration of Client data. We will also monitor for 'Typosquatting' which is a type of social engineering attack which targets internet users who incorrectly type a URL into their web browser rather than using a search engine. Typically, it involves tricking users into visiting malicious websites with URLs that are common misspellings of legitimate websites. Anything identified on the Dark Web will result in a Lighthouse ticket being logged and we will notify the client as soon as proactively possible.
Knowledge base	Bluecube Compass
WHEN	
Service hours	This is an 'always on' service. This means that the solution is designed to be available and operational at all times.
TERMS & SLA	
Service Levels	The target uptime for this service in any given month is 99.5%
Exclusions	-
Billing	Integrated as a per user charge, or a stand-alone monthly charge, for the service.
Client Responsibilities	To provide all external IP addresses, domain names and any information that may be requested by Bluecube.

30. Enhanced Dark Web Monitoring

WHAT	
Name	**Enhanced Dark Web Monitoring**
Overview	The monitoring of the Dark Web to identify any specific threats by looking for any mention of the Client's domain name, external IP addresses, individual email addresses or keywords (such as brand & VIP details) in addition to hidden / known identifiers.
HOW	
Prerequisites	None
Procedures	Bluecube will monitor the Dark Web for all Client known IP addresses, domain names and specific email addresses (typically of prominent staff). The search can be expanded to include key words for a client Brand and also VIP's information and details. This is especially important if the Client has employees who have a high profile. The presence of this information available on the Dark Web would indicate a potential imminent threat in addition to a compromise of credentials of exfiltration of Client data. Bluecube will monitor for 'Typosquatting' which is a type of social engineering attack which targets internet users who incorrectly type a URL into their web browser rather than using a search engine. Typically, it involves tricking users into visiting malicious websites with URLs that are common misspellings of legitimate websites. Bluecube will provide the Client with a unique identifier. This is typically a unique phrase/code that can be placed (hidden) in documents and data. Bluecube will then search the Dark Web for the presence of this unique identifier. Any presence of this unique identifier would indicate a potential data exfiltration situation. Anything identified on the Dark Web will result in a Lighthouse ticket being logged and we will notify the client as soon as proactively possible.
Knowledge base	Bluecube Compass
WHEN	
Service hours	This is an 'always on' service. This means that the solution is designed to be available and operational at all times.
TERMS & SLA	
Service Levels	The target uptime for this service in any given month is 99.5%
Exclusions	-
Billing	Integrated as a per user charge, or a stand-alone monthly charge, for the service.
Client Responsibilities	To provide all external IP addresses, domain names and any information that may be requested by Bluecube.

31. Simulated Phishing Attacks

WHAT	
Name	**Simulated Phishing Attacks**
Overview	The provision of the tooling and configuration to allow for the simulation of a real phishing threat, delivered to the client directly. The purpose of which is to both understand end user behaviours and / or deliver targeted training.
HOW	
Prerequisites	None
Procedures	A phishing attack will be built based on client requirements. All campaigns tend to differ. The result is a 'fake phishing attack' delivered by Bluecube. The output of this exercise is a report that will identify any users that engaged with the email and clicked on links. This will allow for greater awareness of these attacks and will also highlight individuals who would benefit from further training / awareness.
Knowledge base	Bluecube Compass
WHEN	
Service hours	08:30 – 17:30 excluding weekends and bank holidays
TERMS & SLA	
Service Levels	-
Exclusions	-
Billing	Integrated as a per user charge with campaigns quoted for separately, based on requirements.
Client Responsibilities	-

32. SecOps Intelligence

WHAT	
Name	**SecOps Intelligence**
Overview	SecOps Intelligence is all about empowering the SOC function with the most up-to-date intelligence and insights. Our SecOps intelligence service enables our SOC function to make faster, confident decisions based on external intelligence automatically correlated with your internal threat data in real time.
HOW	
Prerequisites	SOC Service
Procedures	In order to deliver the most effective service, we combine sophisticated machine and human analysis to fuse open source, dark web, and technical sources with original research. This approach automatically creates outcomes that can be consumed by analysts easily and integrated with security systems to support three primary uses cases for security operations and incident response: • Alert Triage: Confidently Prioritise and Resolve Alerts • Threat Detection: Correlate our intelligence with your data to detect previously undetected threats • Threat Prevention: Block Threats with high confidence for less operational disruption
Knowledge base	Bluecube Compass
WHEN	
Service hours	This is an 'always on' service. This means that the solution is designed to be available and operational at all times.
TERMS & SLA	
Service Levels	The target uptime for this service in any given month is 99.5%
Exclusions	-
Billing	Typically integrated within the SOC charges.
Client Responsibilities	None

33. Threat Intelligence

WHAT	
Name	**Threat Intelligence**
Overview	Threat Intelligence is all about empowering the SOC function with the most up-to-date intelligence and insights when hunting for threats or monitoring emerging attack methods on the dark web. We ensure that our analysts are not manually collecting, analysing, and sharing the vast amount of (possibly static) intelligence we need to deliver an effective service.
HOW	
Prerequisites	SOC Service
Procedures	We collect our threat intelligence from the greatest breadth of sources available. We eliminate the mundane manual research and deliver real intelligence in real time to our analysts who are protecting you. This delivers you (and us) a comprehensive view of your threat landscape and helps with the following use cases: • **Advanced threat research and reporting**: access to our entire cyber repository and threat intelligence, including finished reporting, in one central location with centralised reporting and search capabilities. • **Advanced detection and validation**: we simplify threat detection and response workflows with pre-built threat hunting packages. • **Dark Web Investigation**: visibility into the threat landscape to identify relevant threats before impact with highly customizable dark and closed web search capabilities. • **Monitoring for threats to your tech stack**: we will receive automatic notification of new or trending vulnerabilities affecting the specific technology that you use.
Knowledge base	Bluecube Compass
WHEN	
Service hours	This is an 'always on' service. This means that the solution is designed to be available and operational at all times.
TERMS & SLA	
Service Levels	The target uptime for this service in any given month is 99.5%
Exclusions	-
Billing	Typically integrated within the SOC charges.
Client Responsibilities	None

34. Brand Intelligence

WHAT	
Name	**Brand Intelligence**
Overview	Typosquat websites, leaked data, and command-and-control attacks are a few ways threat actors may attack your brand - all orchestrated outside of your security perimeter, leaving organisations blindsided. Our Brand Intelligence solution proides actionable, up-to-the-minute analytical insights to proactively defend against new and emerging threats to your brand, products, employees, executives, and customers.
HOW	
Prerequisites	SOC Service
Procedures	We check all of our data sources on a daily basis for to mitigate against the following threats: • **Domain abuse detection**: We detect typosquat websites as they are registered and as they are actually weaponised. Our analysis provides context about the severity of a typosquat or copycat domain. We also provide recommended actions and takedown services within the alert so you can act immediately. • **Data and credential leakage monitoring**: We scour the internet - including paste sites like GitHub and closed underground forums - to look for data leaks. • **Brand attack mitigation**: We look for any malicious mentions of your brand across all of our sources, including closed channels on messaging platforms like Telegram and Discord. • **Brand impersonation detection**: We look for unauthorized use of your brand images so you can protect your brand from reputational damage from phishing campaigns impersonating your brand. • **Digital asset monitoring**: We notify you if your company's domain(s) or IP address(es) have an elevated risk score so you can investigate and secure your network. • **Executive impersonation detection**: We detect imposter profiles on professional networking sites like LinkedIn so you can protect your executives and company from reputational damage that may come from threat actors impersonating your executives to engage with your customers, partners, etc • **Industry threat monitoring**: We look for threats targeting your industry and companies you've identified as peers so you can identify emerging threats and take necessary preventative measures.
Knowledge base	Bluecube Compass
WHEN	
Service hours	This is an 'always on' service. This means that the solution is designed to be available and operational at all times.
TERMS & SLA	
Service Levels	The target uptime for this service in any given month is 99.5%
Exclusions	-
Billing	Typically integrated within the SOC charges.
Client Responsibilities	None

35. Vulnerability Intelligence

WHAT	
Name	**Vulnerability Intelligence**
Overview	Vulnerability Intelligence is about priritising vulnarbilities, ensuring that time and effort is invested into the vulnerabilities that actually matter. Keeping on top of the volume of vulnerabilities that need to be patched can be overwhelming; over 20,000 are issued each year. Thousands of those are rated as critical that were supposed to be patched immediately. However, only 5.5% of vulnerabilities are ever actually exploited. Real-time Security Intelligence avoids wasting time and resources, money and effort on vulnerabilities that are very low risk. Vulnerability Intellligence allows us (and you) to focus attention on the vulnerabilities that actually matter.
HOW	
Prerequisites	None
Procedures	We score vulnerability risk in real-time, based on active exploitation and the availability of exploit kits, making it easy to understand which vulnerabilities to prioritise. Allowing a greater reduction in risk. We also constantly monitoring for new vulnerabilities. On average, we find them 11 days before they are published in the national vulnerability database. That means faster, more informed action on newly emerging, high-risk vulnerabilities.
Knowledge base	Bluecube Compass
WHEN	
Service hours	08:30 – 17:30 excluding weekends and bank holidays
TERMS & SLA	
Service Levels	-
Exclusions	-
Billing	Integrated as a per user charge with campaigns quoted for separately, based on requirements.
Client Responsibilities	-

36. Attack Surface Intelligence (ASI)

WHAT	
Name	**Attack Surface Intelligence (ASI)**
Overview	Attack Surface Intelligence allows us to see all of your internet facing digital assets (this is the same attack surface that malicious attackers can see). In order to provide a comprehensivce security service it is important to have a full understanding of the external attack surface as you cannot defend what you cannot see.
HOW	
Prerequisites	None
Procedures	There are two processes that combine to deliver ASI; • **Continuous scanning of the internet**: This is to identify all internet (public) facing assets to identify any potential blind spots. We discover previously unknown shadow IT and out of policy assets. • **Persistent view of the attack surface landscape**: we understand your footprint (we share it with you) and therefore we can protect you. With this knowledge we can accelerate vulnerability scanning and incident response (and prioritise assets that may be vulnerable to threats or exploits).
Knowledge base	Bluecube Compass
WHEN	
Service hours	08:30 – 17:30 excluding weekends and bank holidays
TERMS & SLA	
Service Levels	-
Exclusions	-
Billing	Integrated as a per user charge with campaigns quoted for separately, based on requirements.
Client Responsibilities	-

SECTION THREE
INFRASTRUCTURE SERVICES

Services to deliver resilient infrastructure to our clients.

37. Network Operations Centre (NOC)

WHAT	
Name	**Network Operations Centre (NOC)**
Overview	A dedicated team of IT engineers responsible for monitoring infrastructure health and capacity on a clients' environment and in relation to key services (such as Managed Backup). They make decisions and adjustments to ensure optimal network performance and organisational productivity.
HOW	
Prerequisites	Proactive Monitoring and/or Network Monitoring
Procedures	The NOC team leverage the tooling made available through Proactive Monitoring and Network Monitoring to allow them to assess the health of a client's environment. When any action is required an 'Event' ticket will be created in Lighthouse to track all activities in relation to an Event. The NOC team will often work in conjunction with other teams to resolve an issue.
Knowledge base	Bluecube Compass
WHEN	
Service hours	This is an 'always on' service. This means that the solution is designed to be available and operational at all times.
TERMS & SLA	
Service Levels	The target uptime for this service in any given month is 99.5%
Exclusions	Managing or responding to Security Alerts.
Billing	Integrated as a per user charge, or per device, (as stated in the contract).
Client Responsibilities	To ensure availability to discuss (and approve) any necessary, or recommended, actions.

38. Proactive Monitoring

WHAT	
Name	**Proactive Monitoring**
Overview	Proactive Monitoring is defined as the automation of the remote monitoring of systems across endpoints and servers, (Servers, PCs, laptops, etc). The intended outcome of the service is to provide both pro-active maintenance, alerting and activity in relation to either real or predicted problems across the client estate.
HOW	
Prerequisites	N/A
Procedures	A monitoring agent is installed on each supported device. Each agent then reports back to Bluecube's monitoring platform. The monitoring platform will then alert either the security operations team or the operations team accordingly. Each device will then have a set of checks and thresholds against which the monitoring result is checked. If the result breaches a threshold, a ticket is automatically created within Lighthouse for investigation. Devices will be added and removed automatically by our monitoring platform. Devices that have not checked in for more than 30 days will be removed. Devices will be added through Group Policy, Intune, or by using a probe that scans the network for new devices each day.
Knowledge base	Bluecube Compass
WHEN	
Service hours	This is an 'always on' service. This means that the solution is designed to be available and operational at all times.
TERMS & SLA	
Service Levels	The target uptime for this service in any given month is 99.5%
Exclusions	Automatic install of monitoring agents outside of a domain or Intune environment.
Billing	Integrated as a per user charge, or per device, (as stated in the contract).
Client Responsibilities	Notification of any non-Windows/Linux devices requiring monitoring. Support in installing the agent on standalone machines or workgroups requiring proactive monitoring support.

39. Network Monitoring

WHAT	
Name	**Network Monitoring**
Overview	Advanced proactive network monitoring to provide visibility of the entire network in order to provide insights into network performance and security. Provides a graphical representation of the clients network and can alert on changes.
HOW	
Prerequisites	-
Procedures	At least one collector is installed onto a node/device that can see all of the clients networks. The ranges for each network are required to support the installation. The collector then runs an audit of the network. Credentials for the domain and SNMP traps will be required in order to capture all of the available details of the environment. As soon as it's deployed, monitoring of the network begins with pre-configured alerts aligned with industry best practices and ranging from informational to emergency. These alerts will be configured to deliver the desired monitoring outcome. The solution constantly monitors and polls the network (topology, config history, device performance) in order to provide a real-time look at the network for troubleshooting, analysis, planning, and reporting. Clients can be provided with their own login to the monitoring portal, if required.
Knowledge base	Bluecube Compass
WHEN	
Service hours	This is an 'always on' service. This means that the solution is designed to be available and operational at all times.
TERMS & SLA	
Service Levels	The target uptime for this service in any given month is 99.5%
Exclusions	-
Billing	Integrated as a per user charge, or per device (as stated in the contract).
Client Responsibilities	To provide the network ranges and inform Bluecube of any additional networks that have not been configured by Bluecube.

40. Infrastructure as a Service (IaaS)

WHAT	
Name	**Infrastructure as a Service (IaaS)**
Overview	Infrastructure as a Service (IaaS), often referred to as Cloud Computing, is the supply of computing power, processing capability and storage as a service.
HOW	
Prerequisites	-
Procedures	The IaaS platform is delivered from large infrastructure that is wholly owned by Bluecube. The compute layer is delivered from a cluster of servers and storage modules, referred to as a SAN. A virtualisation layer sits over the cluster and SAN to create a platform that allows us to allocate resources and storage to individual virtual servers on the platform. Due to the nature of IaaS the resources allocated to a virtual server can be changed with ease; disk drives can be expanded without any downtime, memory and processor allocation can be increased within minutes; removing the need to worry about upgrade routes, capacities, hardware warranty and other concerns normally associated with hardware ownership. Our IaaS solutions are designed to allow for ease of access; all you need is an internet connection. All of your data and applications will be hosted and run from our secure Data Centre environment, giving you unrivalled security and flexibility.
Knowledge base	Bluecube Compass
WHEN	
Service hours	Infrastructure as a Service is an 'always on' service. This means that the solution is designed to be available and operational at all times.
TERMS & SLA	
Service Levels	The target uptime for Infrastructure as a Service in any given month is 99.95%
Exclusions	-
Billing	Infrastructure as a Service will attract an initial set-up fee; this fee is based on the complexity of your environment. The monthly service charge is based on the compute and storage resources allocated to the Client solution. These will be detailed within your services contract. Any variation will be agreed on a case-by-case basis.
Client Responsibilities	-

41. Disaster Recovery

WHAT	
Name	**Disaster Recovery**
Overview	Disaster Recovery is defined as the restoration of your key IT systems onto the Microsoft Azure platform to a known time frame (referred to as a Recovery Time Objective) and a known maximum window of data loss (referred to as a Recovery Point Objective).
HOW	
Prerequisites	In order to deliver the service a client must be subscribed to Microsoft Azure through Bluecube. In order to provide access to the Disaster Recovery environment it will be necessary for you to have a Remote Desktop Server or a network link into Azure to provide access.
Procedures	In order to calculate the Recovery Time Objective and Recovery Point Objectives we conduct a full Disaster Recovery test. We use the results of this test to confirm the timings and service levels that you can expect. These are formally communicated as part of a documented Disaster Recovery plan. Disaster recovery is invoked by logging of a service request via the Service Desk.
Knowledge base	Bluecube Compass
WHEN	
Service hours	Disaster Recovery is an 'always on' service. This means that the solution is designed to be available and operational at all times. Please note that invocation of Disaster Recovery can only be requested during normal working hours (Monday to Friday, 08:30 – 17:30, excluding Bank Holidays) due to the requirement to have 3rd line engineers available throughout the process. Outside of normal UK working hours we will make a best endeavours attempt to invoke a Disaster Recovery plan, however this will be subject to senior engineer availability.
TERMS & SLA	
Service Levels	Recovery Time Objective – Subject to specific contract, agreed and defined as part of the testing process. Recovery Point Objective – Subject to specific contract, agreed and defined as part of the testing process. An annual test is provided as part of the service (additional tests can be conducted for an additional charge).
Exclusions	Any servers / systems not included in the Disaster Recovery solution.
Billing	The Disaster Recovery service will attract an initial set-up fee; this fee is based on the complexity of your environment. The monthly service charge is based on the amount of reservation of computing power and storage within Microsoft Azure. Typically the charge for Disaster Recovery will be included within the IaaS charges made by Bluecube. However, the cost for ongoing Azure charges should Disaster Recovery be invoked (other than for testing) are not included and will be passed onto the client..
Client Responsibilities	Client's must provide written notice of any infrastructure changes not carried out by Bluecube.

42. Managed Backup

WHAT	
Name	**Managed Backup**
Overview	Managed Backup is the secure off-site backup of data to our UK based backup facility. The Data is stored in encrypted format (at a minimum of 128 bit AES encryption) with an encryption key that is known only on the device from which the backup originated. The encrypted data is transmitted via an SSL based secure connection between the device and the Bluecube backup server. The service is built on a modular basis so that storage capacity can be added without hindering the availability of the backup service. The backup servers are resilient with data storage platforms built using RAID technologies.
HOW	
Prerequisites	The service agent must be installed onto compatible servers or endpoints.
Procedures	By default, Bluecube will backup every known server in its entirety (this includes the System Drive, System State and Data Drives). This approach allows the restoration of individual files and folders as well as a full Server restore. Our standard data retention period is 90 days. We can alter the backup selections and change retention periods on request. In the event that a backup does not complete two successful Sequential backups then a ticket will automatically be logged in Lighthouse to the Bluecube Service Desk for resolution of the issue. We also monitor our backup platform and individual client backups on a daily basis (Monday to Friday) and will engage in the resolution of any issues.
Knowledge base	Bluecube Compass
WHEN	
Service hours	Managed Backup is an 'always on' service. This means that the solution is designed to be available and operational at all times; allowing backups to be run at any time.
TERMS & SLA	
Service Levels	The target uptime for this service in any given month is 99.95%
Exclusions	Any data outside of the agreed retention period. Any servers that are excluded from the backup selection (at the request of the client). In the event that there is no connectivity or internet outages managed backup will not be able to complete. Any such failures will be handled following the standard support processes.
Billing	The Managed Backup Service is charged on a per Gigabyte (GB) basis, based on the amount of data that is selected for backup. An audit of the selected backup data is conducted every day and is viewable from within Lighthouse. On the 1st of each month this figure will be used to calculate the monthly charges. Our pricing for our Data Backup Service is reviewed annually on 1st January. Any proposed changes to our pricing structure will be communicated to clients well ahead of any changes to the fee structure.
Client Responsibilities	Client's must provide written notice of any infrastructure changes not carried out by Bluecube.

43. Office 365 Backup

WHAT	
Name	**Office 365 Backup**
Overview	Managed Backup is the secure off-site backup of data to our UK based backup facility. The Data is stored in encrypted format (at a minimum of 128 bit AES encryption) with an encryption key that is known only on the device from which the backup originated. The encrypted data is transmitted via an SSL based secure connection between the device and the Bluecube backup server. The service is built on a modular basis so that storage capacity can be added without hindering the availability of the backup service. The backup servers are resilient with data storage platforms built using RAID technologies.
HOW	
Prerequisites	The service agent must be installed onto compatible servers or endpoints.
Procedures	By default, Bluecube will backup every known server in its entirety (this includes the System Drive, System State and Data Drives). This approach allows the restoration of individual files and folders as well as a full Server restore. Our standard data retention period is 90 days. We can alter the backup selections and change retention periods on request. In the event that a backup does not complete two successful Sequential backups then a ticket will automatically be logged in Lighthouse to the Bluecube Service Desk for resolution of the issue. We also monitor our backup platform and individual client backups on a daily basis (Monday to Friday) and will engage in the resolution of any issues.
Knowledge base	Bluecube Compass
WHEN	
Service hours	Managed Backup is an 'always on' service. This means that the solution is designed to be available and operational at all times; allowing backups to be run at any time.
TERMS & SLA	
Service Levels	The target uptime for this service in any given month is 99.95%
Exclusions	Any data outside of the agreed retention period. Any servers that are excluded from the backup selection (at the request of the client). In the event that there is no connectivity or internet outages managed backup will not be able to complete. Any such failures will be handled following the standard support processes.
Billing	The Managed Backup Service is charged on a per Gigabyte (GB) basis, based on the amount of data that is selected for backup. An audit of the selected backup data is conducted every day and is viewable from within Lighthouse. On the 1st of each month this figure will be used to calculate the monthly charges. Our pricing for our Data Backup Service is reviewed annually on 1st January. Any proposed changes to our pricing structure will be communicated to clients well ahead of any changes to the fee structure.
Client Responsibilities	Client's must provide written notice of any infrastructure changes not carried out by Bluecube.

44. Office 365 & Azure (Microsoft Cloud)

WHAT	
Name	**Office 365 & Azure (Microsoft Cloud)**
Overview	The provision of Azure & Office 365 (Microsoft Cloud) products / subscriptions / licenses
HOW	
Prerequisites	-
Procedures	As a Tier 1 Microsoft Cloud Solution Provider (CSP) Bluecube is able to procure Microsoft Cloud products/subscriptions/licenses from Microsoft for our clients. The term and pricing of the products/subscriptions/licenses will be detailed in the contract or an addendum to the contract. Clients will also be able to view and manage their Microsoft Cloud subscriptions through the Bluecube portal; Cloudhouse.
Knowledge base	Bluecube Compass
WHEN	
Service hours	The software is deployed and is available for the lifetime of the agreement between Bluecube and the Client. Each subscription will have a minimum commitment of one calendar month, although this may also be 12 or 36 months. Please refer to the contract or contract addendum for specifics.
TERMS & SLA	
Service Levels	N/A as this is a service delivered by Microsoft and is outside of Bluecube's control.
Exclusions	-
Billing	Billing is based on usage and is calculated each month. Each subscription / license is charged on a monthly basis and the charge for each type of subscription will vary, all of which are available on Microsoft's public website or through the Bluecube portal; Cloudhouse.
Client Responsibilities	Where flexible month-by-month subscriptions are being utilised to check that the correct volume of license are allocated each month prior to the billing run.

45. Managed Wireless Network

WHAT	
Name	**Managed Wireless Network**
Overview	Our Managed Wireless Network service is the provision of a fully managed wireless network that delivers a very powerful meshed network that delivers better wireless performance and a single network across multiple sites and locations, as well as providing the ability for guest networks and wireless access control.
HOW	
Prerequisites	A compatible, supported wireless network management vendor
Procedures	Wireless Access Points are deployed in each location that requires wireless access (these can be indoor and outdoor locations). The Access Points report back to Bluecube's wireless management platform (which is geographically redundant), which provides the configuration information for each Access Point. All wireless network configurations are centralised and managed by Bluecube. The Access Points constantly monitor the other wireless activity and change their settings to ensure that the network signal is strong and unimpeded by other wireless signals in the vicinity. The Access Points work independently, meaning that operation continues even if the connection to the wireless management platform is lost.
Knowledge base	Bluecube Compass
WHEN	
Service hours	Our Managed Wireless Network is an 'always on' service. This means that the solution is designed to be available and operational at all times.
TERMS & SLA	
Service Levels	The target uptime for the Wireless management platform in any given month is 99.5%. Please note that the management platform is not required for normal operation of the on-premise wireless network .
Exclusions	–
Billing	The Managed Wireless Network will attract an initial set-up fee; this fee is based on the complexity of your environment. A monthly or annual service charge will be made based on the number of Wireless Access Points that are deployed.
Client Responsibilities	To advice of any changes to the working environment that could influence/impact the performance, range of individual Access Points or meshed Wi-Fi solutions. For example - electrical or structural changes, installation of new copiers, appliances (microwave) emitting interference (EMC), unmanaged/rogue Wireless Access points

46. Internet Connectivity

WHAT	
Name	**Internet Connectivity**
Overview	The Internet Connectivity service provides your internet connectivity, including converged data and voice traffic.
HOW	
Prerequisites	-
Procedures	Bluecube partners with multiple tier-1 Internet Service Providers (ISPs). We can offer a range of connectivity solutions from leased line, fibre circuits through to satellite connections.
Knowledge base	Bluecube Compass
WHEN	
Service hours	The Internet connectivity service is an 'always on' service. This means that the solution is designed to be available and operational at all times.
TERMS & SLA	
Service Levels	The terms and SLA vary for each type of circuit (DSL, Fibre) and agreement. Any SLA and minimum term commitment will be communicated during the ordering process.
Exclusions	-
Billing	As detailed within the contract or associated addendum.
Client Responsibilities	Once installed, Client premise equipment cannot be modified, removed, or tampered with in any way and must remain in the state and location that it was originally installed. Any proposed changes to contracted services must be discussed with Bluecube.

47. Mobile Phone Provision

WHAT	
Name	**Mobile Phone Provision**
Overview	The provision of mobile phones, SIM cards and mobile phone contracts.
HOW	
Prerequisites	-
Procedures	Bluecube partners with EE to deliver mobile phones and associated contracts to our clients.
Knowledge base	Bluecube Compass
WHEN	
Service hours	Mobile provision is an 'always on' service. This means that the solution is designed to be available and operational at all times. Queries & requests are handled by the Bluecube Service Desk.
TERMS & SLA	
Service Levels	N/A - this service is delivered by EE and as such their SLA's for mobile provision apply to this service.
Exclusions	-
Billing	As detailed within the contract or associated addendum.
Client Responsibilities	Once installed, Client premise equipment cannot be modified, removed, or tampered with in any way and must remain in the state and location that it was originally installed. Any proposed changes to contracted services must be discussed with Bluecube.

SECTION FOUR
LOGISTICS SERVICES

Services to manage stock, builds
and logistics for our clients

48. Stock Management

WHAT	
Name	**Stock Management**
Overview	The purpose of Stock Management (as defined within a Stock Control Agreement) is for Bluecube to maintain a stock of laptops (and other agreed devices) for clients ensuring that they are able to be efficiently distributed to staff as required.
HOW	
Prerequisites	-
Procedures	A Stock Control Agreement will define the levels and types of IT equipment that Bluecube will hold on behalf of a client and the conditions and rules of distribution of that equipment. Bluecube will ensure that the stock levels will be maintained and that hardware is distributed as agreed. When any of the minimum stock levels are met, Bluecube will order the necessary quantity of laptops to replenish the stock to the maximum levels. Typically (but not always) the Stock Control Agreement provides Bluecube with the authority to order the required stock items to maintain stock levels. It is accepted that the maximum stock levels may be exceeded from time to time when hardware is returned to Bluecube when staff members leave. Any purchase requests for items not detailed within the Stock Control Agreement will need to be approved on a case-by-case basis. Bluecube may also provide additional storage for miscellaneous items. The provision of this facility will be detailed within the Stock Control Agreement.
Knowledge base	Bluecube Compass
WHEN	
Service hours	This is a manual procurement service that is based on daily reporting. It is operated within normal UK working hours.
TERMS & SLA	
Service Levels	As defined within the Stock Control Agreement.
Exclusions	_
Billing	Bluecube will issue an invoice for all stock purchases as and when the purchases are made. All courier / distribution charges will be passed onto the client at cost. Invoices in relation to any additional miscellaneous storage charges will be issued monthly.
Client Responsibilities	To inform Bluecube of any desired changes to the Stock Control Agreement.

49. Device Builds

WHAT	
Name	**Device Builds**
Overview	The build of devices for clients when they procure new end user devices (laptops, PCs, iPads, phones, etc).
HOW	
Prerequisites	-
Procedures	Bluecube will create a defined process for the build of devices. Where possible, Bluecube will use automation (imaging, scripting or Intune) to streamline this process (not all PC Builds processes will be able to be fully automated). Any change to the agreed Build processes are subject to formal Change Control and testing. Typically a device build will be triggered through a UAM (creation) process or Stock Control Agreement.
Knowledge base	Bluecube Compass
WHEN	
Service hours	This is a manual procurement service that is based on daily reporting. It is operated within normal UK working hours.
TERMS & SLA	
Service Levels	As defined within the Stock Control Agreement.
Exclusions	–
Billing	When devices are purchased through Bluecube, the build charge will typically be incorporated into the purchase price. When devices are not purchased through Bluecube a cost per device will be charged.
Client Responsibilities	To inform Bluecube of any desired changes to the build processes.

50. Asset Management (Basic)

WHAT	
Name	**Asset Management (Basic)**
Overview	The addition of hardware into the Bluecube Asset Management system in order to track the lifetime of hardware, when it was built and who it was distributed to.
HOW	
Prerequisites	-
Procedures	Each client device that is handled by Bluecube (such as procurement, or the return of a device to us for repair or to be placed into stock) will have an Asset Tag applied to it. A corresponding record will be created within our Asset Management system, using the Asset Tag as the unique identifier. Against this record we will record the following information; • Asset type (e.g. laptop) • Make • Model • Serial Number • Condition (New, used) • Location • Warranty dates (where available/appropriate) • WEEE disposal records (where appropriate) The location will be tracked through Bluecube (Goods In, Secure Storage, PC Build Area, Quality Control, Goods Out) and when it is issued to a client ('Issued to Client'). Bluecube can issue a report based on the above information at anytime.
Knowledge base	Bluecube Compass
WHEN	
Service hours	This is a manual service that is operated within normal UK working hours.
TERMS & SLA	
Service Levels	All client hardware that Bluecube handle will be subject to this process.
Exclusions	Any hardware that has not been to Bluecube.
Billing	Integrated as a per user charge.
Client Responsibilities	-

51. Asset Management (Enhanced)

WHAT	
Name	**Asset Management (Enhanced)**
Overview	The addition of hardware (including existing equipment) into the Bluecube Asset Management system in order to track the lifetime of hardware, when it was built and who is the current owner (user) of the equipment.
HOW	
Prerequisites	-
Procedures	Typically an initial audit of all hardware allocated to each person is conducted. This is a manual activity that is supported by automated tasks and discovery software. Allocated devices are then matched to individuals and are audited and tracked. Asset tags will be applied to equipment to provide a unique identifier (often there is a gap between asset identification and the application of an Asset tag; during this time the Serial Number will be used as the unique identifier). Typically the Asset Register will then be audited every 6 months to ensure compliance. This will be a combination of manual activities alongside the information provided from our monitoring platforms.
Knowledge base	Bluecube Compass
WHEN	
Service hours	This is a manual service that is operated within normal UK working hours.
TERMS & SLA	
Service Levels	All client hardware that Bluecube handle will be subject to this process.
Exclusions	-
Billing	The set-up of the service is subject to a one-off project charge. Following this, there will be a monthly per device or per user charge as specified within the contract.
Client Responsibilities	-