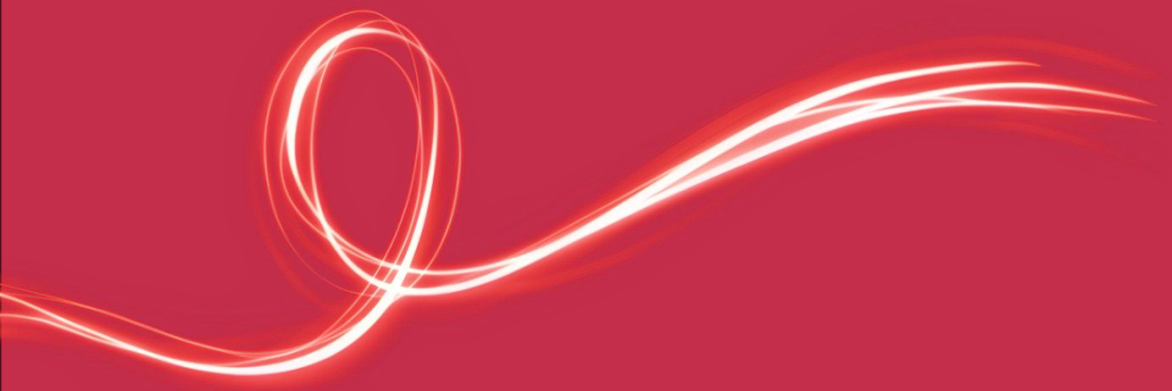
TalkTalk Business

TalkTalk Business SASE

Service Definition



Contents

1. Secure Access Service Edge (SASE) 3
1.1 Backup and restore 4
1.2 Disaster Recovery 4
1.3 Onboarding support 5
1.4 Off-boarding support 7
1.5 Service Constraints 7
1.6 Change Management 8
1.7 Service Levels 8
1.8 After Sales support 13
1.9 Hosting Options 14
1.10 Access to data (upon exit) 15
1.11 Security 15
Version Control 17

1. Secure Access Service Edge (SASE)

Cisco Secure Connect is a cloud-delivered Security Service Edge (SSE) platform designed to protect the modern hybrid workforce. This Cisco Secure Connect service delivers a full Secure Access Service Edge (SASE) solution, combining Cisco SD-WAN connectivity with Cisco Secure Connect SSE security. The combination of Cisco SD-WAN and Secure Connect SSE provides secure, optimised connectivity to both private applications and the internet. By uniting cloud-managed SD-WAN routing with Cisco's cloud-delivered security services, users gain fast, direct, and protected access to all resources without backhauling traffic through a central data centre. This integrated approach improves performance, ensures consistent policy enforcement, and delivers a seamless, secure experience for users wherever they work.

It enables secure, optimised connectivity for hybrid workforces and branch offices, enforcing consistent Zero Trust Network Access (ZTNA), Secure Web Gateway (SWG), DNS-layer security, Firewall-as-a-Service, and unified remote access through Cisco's cloud-delivered platform.

By uniting connectivity and security into a unified SASE approach, the service enforces policy and inspects traffic for any user, site, or application. This model eliminates the need to "backhaul" traffic to a central data centre, which often causes latency and performance issues, instead providing direct, secure access to cloud and internet resources through distributed points of presence (PoPs) located close to users. This architecture improves application performance, user experience, and network efficiency while maintaining consistent Zero Trust security enforcement across all locations.

TalkTalk Business (TTB) can provide both managed and unmanaged Cisco Secure Connect solutions for our customers depending on their existing capability and requirements.

Key service capabilities:

We provide a comprehensive suite of security and connectivity functions managed through a single, unified platform:

- Zero Trust Access: We utilise Cisco Duo to verify user identities and device health, limiting access to the corporate environment to only trusted entities to reduce the attack surface.
- Secure Web Gateway (SWG): Powered by Cisco Umbrella, this uses DNS-layer security and deep inspection to block malware and web threats before a connection is ever established.
- Unified Remote Access: Enables users to securely connect to corporate applications through a single client that supports both traditional VPN and Zero Trust Network Access (ZTNA). This simplifies access for end users, streamlines administration for IT teams, and allows customers to transition smoothly from legacy VPN models to a modern Zero Trust framework without disruption.
- Cloud-Delivered Firewall: Provides Layer-7 protection and IPS to stop threats in the cloud before they reach endpoints.
- Data Loss Prevention (DLP): Offers deep traffic inspection to stop advanced threats and prevent unauthorised data loss.

1.1 Backup and restore

Cisco Secure Connect is a cloud-delivered platform hosted in resilient Cisco data centres with integrated redundancy. All service configuration data (policies, identities, and logs) is automatically backed up within Cisco's infrastructure. Cisco Secure connect implements Backup on Change. The system allows for automatic backups triggered whenever changes are detected, ensuring the latest configuration is saved. This can be restored at any point in time

The managed service element is supported by platforms hosted in Tier 1 data centres or resilient cloud/SaaS environments, ensuring service continuity. Service Now ITSM data is hosted across a redundant pair of European Data Centres.

1.2 Disaster Recovery

Cisco Secure Connect is delivered through Cisco's globally distributed cloud infrastructure designed for high availability and resilience. The service leverages multiple geographically dispersed data centres, redundant service edges, and automated failover mechanisms to minimise downtime and maintain continuous service delivery. Data Centres are located globally which offer 99.999% SLA. This SLA covers availability of core connectivity, security enforcement, and management access functions. Please see https://meraki.cisco.com/en-uk/platform/.

Cisco Secure Connect services operate in the Cisco Umbrella global cloud architecture which is network of data centres located throughout the world interconnected with a high speed, low latency backbone.

The Recovery Time Objective (RTO)

Cisco Secure connect does not specify an explicit maximum downtime duration Recovery Time Objective (RTO) for Cisco Secure Connect. The service availability target is 99.999% uptime per calendar month, implying a maximum allowable downtime of approximately 4.38 minutes per month.

The SLA focuses on service availability and incident management rather than data loss metrics. For related high availability and disaster recovery solutions (e.g., SAP HANA), RPO can range from zero seconds (no data loss) to hours depending on replication and backup strategy, but this is not directly applicable to Cisco Secure Connect.

For the service elements delivered by TTB, we have an established Business Continuity Plan in place certified against ISO 22301 (Business Continuity Management) in 2025. We continue to align our operational preparedness with the requirements of this certification. All resources and systems supporting the managed service are covered by documented Business Continuity and Disaster Recovery plans, which can be invoked as required in the event of a service impacting incident.

Our service model incorporates both UK and Sofia service centres as well as home based teams, providing strong geographical and operational resilience. All teams can

operate fully remotely if required, mitigating risks such as pandemics and major/national power outages.

As part of our ISO 22301 certification, our Business Continuity plans undergo external audit, including verification of our testing schedule. Our annual testing programme covers people, processes, and systems to ensure comprehensive validation of our critical services.

In addition, we maintain alternative working practices to address extreme scenarios, including severe weather events or loss of satellite-based services.

1.3 Onboarding support

TTBD implements a structured onboarding model for all new customers, from SMEs through to major customers, undertaking the following process:

1. The customer order is received by the salesperson, along with a copy of the terms and conditions (signed using DocuSign).

2. All customer orders are verified, and credit checked and, once approved, put into the provisioning work in progress queue (WIP).

3. All orders are built within our Inventory Systems billing system by the Delivery team

4. All updates and communication on installation dates will be provided to the customer via email by the Delivery Team

5. Should a router be requested as part of the solution, TTB will provide engineering resource for onsite installation.

Our service provides comprehensive onboarding and deployment support through a structured end-to-end lifecycle model with defined "Plan, Execute, Operate" phases.

The Plan, Execute, and Operate model represents the end-to-end lifecycle approach used to deliver and manage modern technology environments. This modular framework ensures that our customers have access to the specific expertise needed at every stage of their SASE journey.

1. The Planning Stage

The planning phase focuses on the foundational strategy and architecture of the security solution.

- Expert Strategy & Design: Cisco Certified resources provide specialised expertise to create a tailored strategy and design for Cisco Secure Connect solutions. Cisco Secure Connect is covered by the Security Specialised Certification (CCNP-SEC). Staff working on this service will have attained or work alongside staff who have this specific certification, in addition to their general security expertise.

- Assessment: This stage involves assessing the current environment and "envisioning" the future state to ensure the architecture supports complex policy designs and multi-vendor integrations.

This phase seeks to establish a modern, zero-trust architecture that is specifically aligned with the customer's business needs.

2. **The Execute Stage**

The execution phase is where the planned strategy is turned into a physical reality through procurement, technical implementation and configuration.

- Procurement: The service acts as a single source for all necessary hardware, software, and licensing required for the deployment.
- Project Management: Implementations are handled by a proven Project Management Office (PMO) using Prince 2 certified managers. This ensures the project is delivered within designated timescales and against the set budget.
- Deployment & Adoption: Field technicians and certified professionals handle the cost-effective deployment and help the customer "adopt" the new technology into their daily workflows.

This phase provides customers with a rapid and effective deployment and implementation of Cisco Secure Connect within their exiting environments.

3. **The Operate Stage**

Once the system is live, the operate phase focuses on maintenance, peak performance, and continuous improvement.

- Ongoing Management & Support: Customers gain access to specialised expertise for the continuous management of IT infrastructure, including SD-WAN, firewalls, and authentication layers.
- Optimisation: This involves the constant assessment of the active solution to ensure it reaches and remains in a "best practice" state.
- Proactive Maintenance: This stage includes critical patching for security effectiveness and real-time monitoring of systems like DNS Security to protect against attacks.

This phase ensures all systems continue to operate at peak efficiency and new customer requirements are managed in-life, while maintaining robust protection and reliable connectivity.

Our support includes a history of successful implementations across diverse industries, involving complex policy designs and large-scale distributed deployments.

By managing these infrastructure and setup details, we allow your organisation to focus on its core operations while we ensure seamless connectivity and efficient access control from day one.

1.4 Off-boarding support

At the end of a customer's contract, TTB has a cease process in place. After your minimum term, you can end the contract or any connection forming part of a contract by giving 40 days' notice. Any equipment remains the property of TTB and, upon termination of service, should be returned to us as requested. All cease requests must be received by email from the customer with a completed Cease Request Form, this will then create a case within Salesforce.

The Customer Service Team will query the address on the Cease Form to confirm that it matches the address held on our records. Once confirmed the cease process will begin.

The exit plan, developed by the Account Manager with the Customer to ensure a smooth handover, will be provided by email and followed up with a phone call to answer any queries or highlight any missing information. The plan will cover:

- Options for asset acquisition by the customer
- Transfer of service/supply contracts
- Licence terms for IPR
- Data transfer
- TUPE
- Transition and handover planning
- Exit plan review and update

Provided the minimum contract term has expired and payment is up-to-date, no further charges or additional costs will be payable.

1.5 Service Constraints

Any configuration or policy change would undergo the standard change control process, ensuring continual customer engagement at all stages. Any impacts of agreed changes would be communicated with the customer as part of this process.

For all planned notices and maintenance, the customer will be notified 10 business days in advance to allow them to make suitable arrangements. Emergency maintenance is rarely required and is typically not customer-affecting, as it is usually confined to one part of a resilient system. In the event emergency maintenance is required that is likely to be customer affecting, the planning and risk assessment we undertake will include making provision to minimise the impact in terms of scope and duration. Where it is possible, advanced notice will be given.

1.6 Change Management

The service follows ITIL best practices and categorises changes into three specific types.

Standard Change: Common, low-risk, and routine tasks that follow documented procedures and are pre-authorised.

Normal Change: Modifications that are not pre-authorised and must undergo a full assessment, approval, and scheduling process.

Emergency Change: Urgent implementations required to resolve a Major Incident or prevent imminent issues; these bypass some standard procedures but still require documentation and approval.

The customer can customise and configure their service via a catalogue of Standard & Normal service changes that may be requested through a documented change control process. The catalogue is provided to the customer at the start of the service as part of the Statement of Works (SoW) document. Change control tickets are raised via phone or email communication.

Changes are managed through a system of Flex Tokens, which are consumed for each change. The number of Flex Tokens will be based upon your specific environment and service level.

1.7 Service Levels

We can provide customers with unmanaged CISCO Secure Connect without a proactive managed service element. This offering will be relevant for customers who have existing security capability capable of configuring and managing CISCO Secure Connect.

The managed service offerings are structured into four modular tiers, outlined below, designed to accommodate varying levels of organisational maturity and security requirements within a SASE framework.

1. Foundation Essentials

This tier provides unified cloud security for remote users and branch offices connected via SD-WAN. It includes the following features:

- **SWG:** Inspects and filters all web traffic, blocking access to malicious or inappropriate sites and preventing the download of malware. Keeping users safe online, reducing security risks, and ensuring consistent protection for all internet activity regardless of user location.

- **DNS Security:** Provides protection at the earliest stage of a network connection, when a user or device attempts to reach a domain; identifying and blocking connections to malicious and suspicious domains before the session even starts. This prevents users from accessing harmful sites or command-and-control servers, stopping threats before they can take hold.

- **Cloud-Delivered Firewall:** Provides advanced Layer-7 inspection and centralised control over all internet-bound traffic. Simplifies management, can remove the need for on-premises firewall appliances, and ensures uniform protection and visibility for distributed and hybrid environments.

Ideal for: Customers taking their first step into SASE by simplifying and centralising internet access and security.

2. Foundation Advantage

This tier builds upon the Essentials foundation by adding deeper traffic inspection and advanced protection capabilities. It includes the features of Foundation Essentials, plus:

- **Advanced Threat Prevention:** Includes Layer-7 Firewall and Intrusion Prevention Systems (IPS) that detect and block cyber threats in real time. Analysing traffic at the application level to identify and stop malicious activity before it reaches users or systems. Provides additional proactive protection against advanced attacks to tackle threats before they can take hold.

- **Data Loss Prevention (DLP):** Monitors and controls the movement of sensitive information across email, web, and cloud applications. It automatically detects and prevents unauthorised sharing or transfer of confidential data. Protects against accidental or intentional data leaks, safeguards sensitive information, and supports compliance with data protection regulations such as GDPR.

Ideal for: Customers with specific compliance needs that require advanced tools to stop sophisticated threats.

3. Complete Essentials

This tier shifts focus toward modernising how users access internal resources by introducing ZTNA. It includes the features of Foundation Essentials, plus:

- **ZTNA:** Provides secure, policy-based access to private applications, serving as a modern alternative to traditional VPNs. Every user and device is authenticated, authorised, and continuously verified before access is granted to ensure that connections are based on identity and context rather than network location. ZTNA also enforces the principle of least privilege, only providing users with access to the specific applications they need. Enhances security by reducing the attack surface and limiting the scope of lateral movement within the network, whilst improving user experience through faster, more direct connections to applications.

Ideal for: Hybrid workforces that need to secure remote access to private applications without the performance lag of older methods.

4. Complete Advantage

A comprehensive tier, delivering a full SASE solution from a single platform. Which includes all the features of the Complete Essentials tier, plus:

- **Maximum Advanced Threat Protection**: Integrates the highest level of security features which include: Layer-7 Firewall, IPS, and DLP into a single, comprehensive service. These features work together to inspect, detect, and stop both known and emerging threats while preventing the unauthorised movement of sensitive information across a customer's network. Provides the highest level of defence against sophisticated cyber threats and data breaches. This ensures critical business data remains secure, user activity is fully protected, and customers maintain compliance with security and privacy standards.

- **Unified Fabric:** Combines Cisco SD-WAN connectivity with Zero Trust Network Access (ZTNA) to create a single, integrated network and security architecture. This allows users to securely connect to private and cloud applications through the most efficient network path, while security policies are enforced consistently across all sites and remote users. Delivers simplified management, improved performance, and consistent protection for all users and locations.

Ideal for: Customers with a mature SASE strategy looking to unify their entire security and networking stack for peak protection and performance.

Performance

SLA Alignment: The contracted Service Level Agreement (SLA) is used to determine the exact coverage and activity level for a customer. Furthermore, all target response and resolution times are strictly subject to the customer's contractual service hours.

Incident Prioritisation Definitions

Urgency	**Impact**			
	Widespread Entire Customer network is affected (more than 75% of individuals, sites or devices)	**Large** Multiple Sites are affected (between 50% and 75% of End Users, Sites or End User devices)	**Localised** Single Site, room or multiple End Users are affected (between 25% and 50% of End Users, Sites or devices)	**Individualised** A single user or group is affected (less than 25% of End Users, Sites or devices)
High	Priority 1	Priority 1	Priority 2	Priority 2

Primary business function of Customer is stopped with no redundancy or backup, immediate financial impact				

Medium Primary business function of Customer is severely degraded or supported by backup or redundant system, probably significant financial impact	Priority 1	Priority 2	Priority 2	Priority 3
Low Non-critical business function is stopped or severely degraded, possible financial impact.	Priority 2	Priority 3	Priority 3	Priority 3

Response Time by Incident Priority

Priority	Definition	Target Response Time
Priority 1	A complete, unplanned outage or interruption to a business-critical IT service, without an available workaround solution. This will impact the entire user base or a significant subset of users.	15 minutes
Priority 2	A degradation to the performance and availability of a business-critical IT service for the entire user base or a significant subset of users.	15 minutes
Priority 3	A failure of or disruption to service (this can include but is not limited to, business-critical systems) for a single user. All other business users would not be impacted by the identified issue meaning the impact on the wider business is minimal.	1 hour
Priority 4	This priority would indicate a request for a new service/function. While this may be impacting a specific user's ability to perform their role, it would not have an impact on the wider audience.	24 hours

Reporting Responsibilities: The TTB Service Delivery Team will provide the customer with a standard monthly summary report, documenting the network's health, changes and availability.

This section of the Schedule identifies the regular reports and management meetings. This will be agreed for each customer with their TTB Account Manager.

Report	Content	Period	Delivered by
Service Report	Performance review, details of previous month, reports on management of Specialist Third Party Suppliers and suggestions for continuous improvement.	Month	At least 5 Working Days before the Service Meeting
Quarterly Report	Performance review, End User satisfaction surveys and proposals for continuous improvement, Managed Service Specific Content	Quarter	At least 10 Working Days before the Quarterly Review Meeting
Annual Report	Performance review, End User satisfaction surveys, proposals for continuous improvement, strategy alignment, financial performance and Managed Service Specific Content	Contract Year	At least 15 Working Days before the Annual Review Meeting

Availability

Cisco Secure Connect has a target availability of 99.999%.

Support hours

Core support availability is 24x7x365; our Operations Centre operates 24x7x365 to manage incidents and events.

The specific hours of service for an individual customer are not universal; they are outlined within the SoW and determined by the specific asset and part codes on the contract schedule.

As part of the service pre-requisite, we work with the customer to define the specific service hours for each offering, this must be captured in the SoW.

TalkTalk Business Responsibilities

- Incident Review / Analysis
- Service Level Performance
- Problem Management Review / Analysis
- Change Management Review / Analysis
- Availability Review / Analysis
- Flex Token/ Change Summary
  Event Summary
  Service Improvement Reporting

Customer Responsibilities: Depending on the upfront scoping process the customer may choose how much responsibility they take on.

Output: Standard Monthly Summary Report

1.8 After Sales support

Incidents and support requests can be raised by telephone on 0845 456 6541 or 0845 310 3444. Our team aims to diagnose faults within 30 minutes. Support requests which are less time sensitive can also be raised by emailing tsc@talktalkbusiness.co.uk. Requests can also be made via our customer portal: https://extra.mytalktalkbusiness.co.uk where customers can log in and submit a 'call log'.

Technical requirements

Certain requirements must be fulfilled by the customer prior to provision of the TTB service. Failure to do so may result in delays to the provision of the service, limit our ability to provide the service and diminish service performance.

- Identify a SPOC to engage throughout the Service Transition period
- Provide the reasonably requested inventory and topology information by the dates agreed between TTB and customer
- Provide all relevant address and contact details of all sites within the scope
- Provide access levels for their internal IT team
- Perform tasks specified as customer's responsibility by the date specified

Outage and maintenance management

Cisco Secure Connect operates with a SaaS model and falls within the Shared Responsibility model of Cloud Compute and is covered by SLA.

For all planned notices and maintenance, the customer will be notified 10 business days in advance. Regarding all unplanned disruption or major failures, all TTB staff will receive email notification internally, informing them of the exact nature of the disruption and the details of the known failure. At this stage it will be the responsibility of the Assurance Desk to inform all affected customers via email and/or text message within 30 minutes of the fault being logged . Updates will be provided by the Assurance desk and Account Manager on a regular basis (every four hours) until fault restoration. For all Major Service Outages (MSOs) a full RFO report will be provided as part of the communication.

Reverting to a normal service in the event of a failure of MSO will follow a procedure whereby all necessary testing is completed within the Assurance and Technical Engineering teams. These teams will initially follow up through direct contact with named representatives within the customer's organisation. All relevant checks will be completed by both parties to ensure all services and deliverables are working correctly prior to any buyer sign-off.

1.9 Hosting Options

TTB currently has multiple Datacentre facilities, notably Corsham and Milton Keynes. We also have Data Centre space in 2 facilities - Virtus 2 in Hayes, and Virtus 5 in Stockley Park, both in west London.

Hosting network and security infrastructure within a professionally managed data centre delivers significant operational, performance, and resilience advantages. The facility provides:

- highly secure environment, with multi-layered physical access controls and compliance to IL3 security standards, ensuring the integrity and protection of customer equipment.
- Multiple layers of power and network redundancy guarantee continuous service availability, while high-efficiency cooling and power systems achieve a low Power Usage Effectiveness (PUE), reducing environmental impact and operating costs.
- The data centre's Tier 3 design supports scalable, high-availability deployments, enabling customers to expand capacity or integrate additional services without disruption.

Combined, these features ensure that critical systems, operate with maximum reliability, performance, and security within a sustainable infrastructure.

Corsham

The functionality and operation of the TTB Corsham datacentre facility is designed to act as a single point of reference for customers to understand both the facilities provided and how to access/manage their services with TTB. Based in a multi-layered security complex with multiple levels of redundancy at both a power and network level, this facility ensures continuity of service delivery for customers hosting their equipment.

The datacentre combines Tier 3 high-availability with minimum energy usage in the cooling and power system losses, resulting in an annualised power usage effectiveness (PUE) of less than 1.3 within an IL3 security environment. The systems employed ensure that Corsham is highly scalable, ensuring an unusually low PUE is achievable at low IT loads as well as when the facility is at its maximum capacity. This results in a carbon footprint that is nearly half the industry norm, providing customers with additional green credentials.

Milton Keynes

The Milton Keynes Data Centre consists of a purpose-built facility with N+1 redundancy throughout, built with attention focused on high availability. The Data

Centre is secure and available 24x7x365. TTB provides a standard availability of 99.9% on all of the components of its co-location services: power, bandwidth, HVAC and fire suppression. Co-location services can be purchased as a standalone item, or as part of an IPVPN Service. These services may be used to extend service directly into a private MPLS cloud and/or to provide internet breakout.

Cisco Meraki is committed to data protection, privacy, and security and has designed its cloud architecture specifically in a way that enables customers to securely protect their data. Customers can confidently deploy scalable, secure Meraki networks that comply with applicable data protection regulations across the regions in which we operate. Depending on the geographical domain selected during Dashboard creation, data will be distributed across multiple secure data centers in countries as shown in the chart below. The regions that Meraki defines are: North America, South America, Europe, Asia-Pacific, China, Canada and India.

https://documentation.meraki.com/Platform_Management/Product_Information/Privacy%2C_Security%2C_Compliance/Dashboard_Data_Storage_Privacy_and_Security

1.10 Access to data (upon exit)

Data is stored in a secure and resilient N+1 environment and, where applicable, is subject to near real time replication/mirroring across diverse geographic locations. In the event of an incident, including loss or degradation of resilience, the incident will be managed in line with an established procedure to ensure customer SLAs can continue to be supported. Should the customer require access to data upon exit, a plan will be put into place for requesting the data via the customer's Account Manager.

1.11 Security

Should intelligence or alerting indicate any potentially malicious activity, TTB operates a robust security incident management programme, and has deployed industry-leading endpoint protection technology to defend against advanced threats as part of our incident response program. TTB has implemented an Information Security Management System based on industry good practice (NIST CSF, PCI DSS) and is externally working towards being certified to ISO 27001.

Standard security protocols are followed for private network connectivity. The Ethernet Service has no additional security requirements as the security elements lie within the private network. The TTB Security Operations Centre (SOC) facilities are manned 24x7x365, providing a near real-time response to security events with an escalation process to senior management as required. Our 24/7 SOC has extensive monitoring of internal and external security controls, coupled with curated threat intelligence feeds. Incidents are triaged based on risk and impact and playbooks have been developed to focus on containment, eradication, and recovery activities in-line with National Institute of Standards and Technology (NIST) best practices.

TTB conducts security scanning of all infrastructure on a bi-weekly basis. We also conduct weekly threat and vulnerability scanning of all our network assets via InsightVM. Critical/high risk vulnerabilities patches are applied within 14 days. All other updates are applied as soon as possible using a monthly patching cycle. Security updates are assessed and prioritised based on threat level, likelihood of compromise, consequences of compromise, environmental characteristics and regulatory or accreditation-based requirements. TTB gets its information about potential threats from InsightVM for scanning and Altiris Patch Management

Version Control

Document Amendment History Log						
Document Owner	Adam Foden					
Created Date	23-01-26					
Author	Adam Foden					
Next Review Date	23-01-27					
Version Number	**Modified date**	**Amendment history**	**Reviewed by**	**Approved by**	**Approval date**	**Approval evidence**