DOMINE DIRIGE NOS

CITY OF LONDON

Future IT Network Strategy

October 2023

Contents

1) Executive summary

This document is intended to provide a strategic vision of the future of the City of London and City of London Police (CoL/P) network delivery. It is a high-level plan to achieve multiple goals for a high-performance, world-class environment for CoL/P for the next 10 years.

As a strategy, it does not focus on the low-level detailing of every single use case for a network or the technical implementation, nor does it attempt to provide a detailed timeline for implementation and scheduling. Both outputs will come from the next phases including business analysis and requirements gathering, technical designs in HLD/LLD format and detailed project planning.

The objective is to ensure a centralised set of objectives and key pillars on which to make future decisions on network services across the estate ensuring a common delivery method and reduced ongoing management costs.

The scope encompasses both LAN and WAN services including (but not limited to) on premise cabled networking, Wi-Fi, Internet provision, VPN's and cloud connectivity.

Delivering the new network across Col/P will provide a blueprint to evolve over time, extending to include other networks within the Col/P estate, such as Barbican, schools, public areas, and City Bridge Foundation.

This strategy is written as an overarching organisation vision and roadmap for a holistic and common approach for networking across the City of London and its institutions.

This approach to a common blueprint (or set or blueprints defined by use cases) is intended to provide a future proof platform with longevity for modern technology but also a simplified network approach which will increase resilience and reduce ongoing management costs.

The final section of this document outlines key recommendations and decisions on which to base future network decisions and procurements.

2) Introduction

As technology advances, so does the need for a more robust and efficient network infrastructure.

It is worth pausing to think back just 4 short years ago when members, officers, staff and police officers were using outdated technology that failed to work at the most critical of times on the street, during Committee Meetings and across our offices and police stations.

- The Lenovo laptops ran Windows 7, were slow to boot up, took days to build and were well past end of life.
- Police officers relied on Panasonic Toughbook's which were clunky, made every day more difficult for the officers and did not work well in the field.
- The vast majority of officers did not have mobile smartphones with biometric logins for data entry and retrieval in seconds rather than hours.
- Officers and members mobile devices were not managed, and our data was spread across many disparate devices which presented a large risk to the organisation.
- The Corporation and City of London Police's network relied on a hybrid mix of aging hardware, including firewalls, which were not up to the job for mass migration of data to cloud, or for people working from home.
- The server estate contained a large amount of legacy operating systems and technical data all hosted in an expensive third-party datacentre and presenting huge cyber security risk to the organisation.
- There was no capability to make a video call.
- The force internet was incredibly slow being provided by a 20Mbps provision on the PSN for Policing network.
- There was no national Security Operations Centre (SOC) monitoring the entire estate.

Fast forward to 2023 and all the above have been addressed. From starting to look at a refreshed estate in 2019 and having to accelerate this in 2020 due to the Covid Pandemic, the organisation's change programme included new laptops and smartphones, a migration to the Exchange Online, SharePoint, OneDrive and a full datacentre exit with a 'lift and shift' to Azure cloud hosting and connection into the National Management Centre and delivery of the national Policing blueprints.

The City of London Corporation & Police are unrecognisable from just four short years ago in terms of technology adoption and digital transformation.

CoL has shown how forward thinking an authority can be around cloud adoption and delivery.

CoLP has evolved faster and further than any of the 43 forces in the UK.

The level of technology change during this period has exceeded everything else in the previous decade, however it has not been plain-sailing – there have been significant deviations and challenges along the way due to the environment the organisation was operating within, be it financial, operational or outside factors.

Because of this, our network has had to evolve around legacy solutions, contracts, and the demands of the organisation meaning it is now a 'patchwork quilt' of technology and contracts across multiple telecommunication providers (telcos) and vendors. The CoL/P network needs a 'reset' using standardised technology and an improved service wrapper whilst still retaining carrier diversity for redundancy.

Technology advancement stands still for no person or organisation and to that end, CoL/P need to address the next wave of transformation that will support the Corporation & Future Police Estate and their demands of an IT network.

As officers and staff increase their digital demand and adopt and mature their usage of the technology provided, this further increases the demands on the CoL/P Local and Wide Area Networks (the IT Network).

As an organisation, this is a wholly positive outcome – more demand on the network means the technology that sits on top of the network is being exploited – colleagues and visitors within the City are directly benefiting from the investment made by the City of London Corporation. With the evolution of major programmes such as the world first Secure Cities programme, or an entirely new and more powerful Action Fraud and National Fraud Investigation capability or simply higher utilisation of Microsoft 365, Power Platform and SaaS/Cloud solutions this increased demand will continue as the organisation now has an embedded bias for positive change.

Underpinning the whole network is the service management wrapper. Further into this document it lists the various suppliers and brands that are within the CoL/P networks currently and this presents a challenge for service management and hand-off between vendors. It makes fault resolution longer for the support teams who must navigate multiple helpdesks, technology stacks, admin portals and account managers to resolve any faults. An investment in a future network will reduce downtime, improve user experience and could also reduce overall operating costs.

3) Vision

To provide a modern, future proof, secure estate providing 'state of the art sustainable facilities' for policing within the square mile and the force national portfolio

To achieve this vision, City of London Police have identified the following design principles:

- The core estate will remain within (?) the City of London footprint
- Modern estate that is sustainable for the next 30+ years
- A variety of facilities to provide operational resilience
- Value for money to be demonstrated in developing the estate portfolio
- Phased implementation to maintain operational effectiveness
- Adoption of new working practices to be designed in – flexible / agile working / smart initiatives
- Modern, robust and flexible IT infrastructure
- Multi 'use' shared and open plan facilities will be adopted as widely as possible except for specialist facilities (such as Custody, firearms range, Tactical Firearms Group and 'Joint Contact & Control Room' and forensics)
- Operational vehicles securely located and accessible.

The future network strategy for CoL/P should not only deliver on the vision of the police estate in the next 10 years, but also look to deliver on the 3 key themes adopted by the Digital, Information and Technology Service (DITS):

- Brilliant Basics
- Removing Complexity
- Enabling Transformation.

4) Current IT network

a) Wide area network (WAN)

The current City of London network has evolved over many years from a core BT MPLS and with low bandwidth internet breakouts (or PSN for Policing (PSNfP) connection providing the legacy 20Mbps internet provision) to more recently 100Mbps to 1Gbps internet breakout carrying nearly all outbound traffic from all sites.

The City of London has very little flexibility in this provision and is entirely dependent on BT to provision circuits which can often delay accommodation moves or the introduction of new sites (such as a new school or office building).

Due to this inflexibility, we are also limited to the technology that can be deployed for hard to reach sites or those with low network infrastructure in the ground.

Most sites are entirely dependent on the Guildhall or Bishopsgate/New Street to provide firewall security and internet access which presents a suboptimal experience for today's users and demands.

b) Local area network (LAN)

The City's current LAN provision has evolved over many years and is managed by ROC Technologies. The LAN can be considered the 'in building network' which includes physical network points, Wi-Fi, access and core switching. Depending on the service contract, the LAN could also include the next generation firewall provision.

The City of London operates HPE Aruba technology across the estate and a large proportion of the hardware will become unsupported in the next two years.

Our Wi-Fi access points are considered outdated and the majority offer Wi-Fi 5 or below technology. The current Wi-Fi standard, which offers much greater throughput and density, run Wi-Fi 6e with Wi-Fi 7 being released in early 2024. A proportion of our access points are end of life and will require replacement in early 2024.

Most of the in-building physical infrastructure is connected by aging copper or fibre cabling with a maximum throughput of 1Gbps. These limits are a combination of cable types, optics and constraints on the hardware.

c) Supplier & technology list

The organisation currently utilises the following network 'stack':

Telcos

- BT
- Vodafone
- Virgin Media O2

- Colt

Technology

- Managed/Direct Internet Access (MIA/DIA)
- MPLS
- SD-WAN
- RS1000 secure
- Business Broadband
- Wi-Fi
- 4g/5g
- LECN (SD-WAN)
- Clearpass / MacAuth
- Site to Site VPN
- Point to Site VPN

Vendors

- Fortinet
- Aruba
- Barracuda
- Cisco
- Microsoft

Service management partners

- ROC
- Vodafone
- BT
- Barracuda
- Colt
- Virgin Media o2
- Microsoft
- Agilisys
- Phoenix

The above list is not exhaustive or detailed and is included only to demonstrate the vast landscape and complexity of the current complex network setup.

d) Costs

With complexity, cost and risk is increased.

Costs are increased due to more human effort, more time to provision new additions on the network or to troubleshoot issues and increased hardware costs to bring new services or sites online. Our current network is inflexible to the demands of a wide range of sites and worker styles.

Risk is increased as the end-to-end provision is not fully understood and documentation from vendors has become outdated and inaccurate over time. "This disparate approach allows elements of the NCSC anti-patterns (Security architecture anti-patterns - NCSC.GOV.UK) to manifest in distinct sections of the network.

In the last 7 years CoL/P have undertaken two network programmes – Network Transformation Programme and Secure Zone Programme. Both programmes of work were scoped to deliver the change requirements of the organisation and ***achieved their goals at that point time.***

It is important to note that this strategy focuses on the future network and not what was delivered within those programmes of work with the goal of ensuring any network decisions made now are fit for purpose for the vision of the organisation for the future.

The current high-level costs for the City's network are as follows:

ITEM	5 YEAR COST
BT MPLS WAN	£3,572,656.60
ROC MANAGED SERVICE	£4,363,024
HARDWARE	£3,521,580 (anticipated based on qty and pricing from XMA)
TOTAL	**£11,457,260.60**

e) Scale

The City of London network scale is vast. Our network currently includes approximately:

- 120 City of London Corporation Sites
- 17 City of London Police Sites
- 100 Secure City CCTV Sites
- Total: 237 sites (approx.)

This presents a complex network refresh programme and will dictate a phased set of works which will include LAN services as the first component to be refreshed due to contractual milestones with incumbent suppliers. Thereafter the WAN elements will be swapped out and the incumbent supplier solution reduced over time as we move onto the new platform.

5) Future IT network

a) SASE

Secure Access Service Edge (SASE) is the recommended strategic direction for the City of London’s future IT network, offering a modern and comprehensive approach to networking and security. SASE represents a paradigm shift in IT infrastructure for several compelling reasons.

First and foremost, SASE combines network and security services into a unified cloud-based architecture. This consolidation simplifies the network, reducing complexity and operational costs. It replaces the traditional hub-and-spoke network model with a more agile, user-centric approach, optimizing performance and ensuring fast, secure access for remote and on-premise users.

SASE also aligns with the evolving nature of work. With an increasing number of remote and mobile employees, the traditional network perimeter is no longer effective. SASE's zero-trust security model verifies the identity and security posture of every user and device, providing a granular, context-based access control system that adapts to the dynamic needs of your organization.

Furthermore, SASE leverages the power of the cloud, making it highly scalable and adaptable to an organization's growth. This eliminates the need for large upfront investments in infrastructure and allows for a more pay-as-you-go, cost-effective model.

> *Our SMT concluded that, unanimously, all network hardware vendors and managed service providers believe SASE is the future of enterprise networks and are investing heavily in its future development.*

SASE will deliver what has eluded most enterprises in the last 5 to 10 years providing services to:

ANY USER

from

ANYWHERE

using

ANY DEVICE

via

ANY CONNECTION

to

ANY APPLICATION

all

WITHOUT FRICTION

SASE will deliver the foundations for 'Brilliant Basics' and allow the City to provide a truly world class user experience to colleagues and visitors alike

b) What is SASE?

SASE is a culmination of 5 distinct network and security offerings that have existed in the market for several years to varying levels of maturity. A SASE platform comprises of:

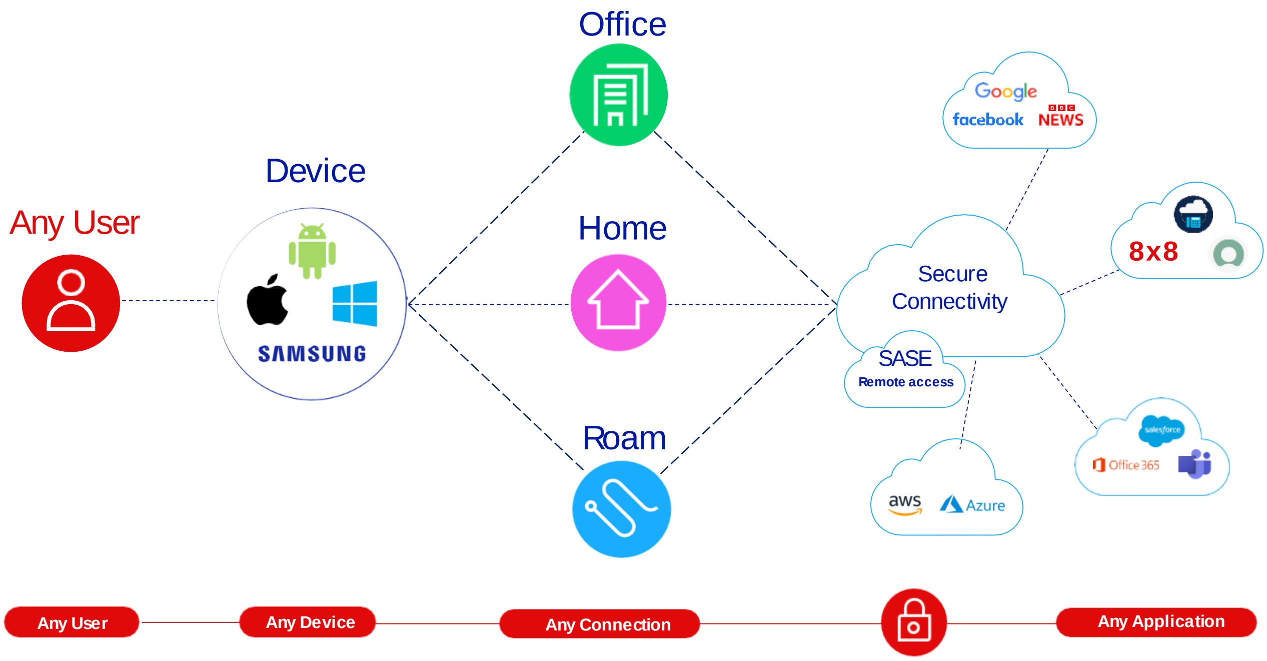
- Zero Trust Network Access (ZTNA)
- ZTNA is a security model that assumes no trust within a network i.e. no device or user on a network can communicate to any other without explicit permission therefore reducing cyber threats
- Software Defined Wide Area Networks (SD-WAN)
- SD-WAN is a technology that optimizes and manages network traffic across geographically dispersed locations using software, enhancing performance, and reducing costs.
- Secure Web Gateways (SWG)
- SWG is a cybersecurity solution that filters and monitors web traffic, ensuring safe and compliant internet access for organizations, protecting against online threats and data breaches.
- Firewall-as-a-Service (FWaaS)
- FWaaS is a cloud-based security solution that provides protective barriers for networks and applications, ensuring data and traffic remain secure from unauthorized access and cyber threats.
- Cloud Access Security Broker (CASB)
- CASB is a cybersecurity tool that helps organizations safeguard their data when using cloud applications by enforcing security policies and monitoring user activity.

Until recently there has never been an easy (and in certain cases even technically possible) way to bring them all together into a holistic platform for management, insights and billing. It has never been possible to have a 'single pane of glass' to our network with many point products that work in isolation.

By 2024 at least 40% of enterprises will have explicit strategies to adopt SASE, up from less than 1% at year-end 2018.

A SASE architecture identifies users and devices, applies policy-based security, and delivers secure access to the appropriate application or data. This approach allows organisations to apply secure access no matter where their users, applications or devices are located. (*Gartner)

c) SASE diagram



d) WAN

The City of London aims to simplify the networking across buildings, cloud and remote workers and the future WAN technology will be based on SD-WAN solutions. SD-WAN can run over any 'raw' internet underlay including internet from enterprise suppliers, business broadband, home broadband, 4g/5g or satellite.

SD-WAN comes in many variants from many different vendors but can be categorised into deployment types which are summarised below.

- **On-Premises SD-WAN:** This type of solution is installed on-site, either as hardware or software and allows the organisation to manage its own WAN locally by way of a hardware-based SD-WAN orchestrator. By way of an example this can be provided by hardware suppliers such as Fortinet and Cisco.

- **Cloud-Managed SD-WAN:** This type of solution is hosted in the cloud and maintained by a third-party provider in the cloud. It offers a simplified deployment process and requires little to no on-site maintenance. Cloud-managed SD-WAN is a popular choice to manage by local teams whilst removing a lot of the management overhead of the SD-WAN orchestration hosting and configuration. By way of an example, this can be provided by a solution such as Meraki.

- **DIY SD-WAN**: This type of solution is designed for organizations that want to build their SD-WAN infrastructure in-house. It requires a high level of technical expertise and resources. By way of an example, this could be built using open-source technologies that build the underlying VPN's such as OpenStack and Ansible.

- **Managed SD-WAN**: This type of solution is managed by a third-party provider that offers network monitoring, troubleshooting, and support services. Managed SD-WAN is a popular choice for organizations that want to outsource their network management to an experienced provider. The added benefit of this solution is that CoL/P own the SD-WAN solution (which could be any of the above options) but it is managed by a 3rd party. Should contracts come to an end or the vendor/customer relationship breaks down, a new managed service partner could be introduced without replacing the network. The risk to be aware of with this solution is the introduction of a large telco providing the solution that is baked into a proprietary solution owned by them.

The SD-WAN solution we select as part of the SASE platform should be a managed SD-WAN delivered with SASE on a cloud platform.

e) Internet

The internet forms the foundation of the City's future network. Legacy networks are stitched together from a combination of MPLS networks, point to point VPN's and physical hardware firewalls within a building that often become a single point of failure. These firewalls provide the 'pop' out onto the internet for on premise and remote workers. They are also the ingress point for remote workers to access corporate systems. Sites were often connected by private fibre (sometimes called dark fibre) which is expensive and inflexible.

Modern networks are built upon the concept of 'everything over the internet' and this is what will allow simplification of the City's network and to reduce costs.

f) LAN & Wi-Fi

The usage profiles of modern office buildings differ significantly from those of offices five or more years ago. Fixed desks and data points per employee, along with fixed phones and named locations, are a thing of the past. The pandemic has forced the adoption of video calling at scale, and nearly all office workers are now familiar with this technology and expect it to work flawlessly in order to do their daily work.

Moreover, working patterns have changed on an individual and team level. The focus is now on work being something you do, rather than necessarily somewhere you go. A wholesale shift to an agile working format is mandatory, where employees can hot-desk anywhere in any corporate building, along with using public Wi-Fi in lounges, coffee shops, on the train, and at home, as agile working and a modern working environment is now an expectation of the workforce.

There is an opportunity with the adoption of this future network strategy for CoL/P to become a leader in this vision and be more sustainable. Future CoL/P buildings don't need to have fixed data points to every desk or as miles of structured cabling and vast amounts of networking equipment that generate heat and consume power. Most CoL/P buildings will be fitted with a core network and **high-density Wi-Fi** covering the main building and exterior with only well-defined and specific areas being cabled with copper or fibre connectivity inside the building.

The LAN and Wi-Fi provision should **baseline at Wi-Fi 7** which is due to come to market in 2024 meaning CoL/P will be an early adopter of the very latest Wi-Fi standards. This should vastly improve connectivity from any building to the services users require.

Wi-Fi 7 is poised to redefine the technological landscape, promising an unprecedented leap in connectivity and speed. With its potential to deliver blazing fast speeds of up to 30 Gbps, Wi-Fi 7 will revolutionize the way we interact with the digital world. Its enhanced efficiency and reduced latency will pave the way for seamless integration of advanced technologies like augmented reality (AR), virtual reality (VR), and the Internet of Things (IoT). The improved spectrum utilization and increased bandwidth efficiency will enable smoother data transmission, fostering a more interconnected and dynamic digital ecosystem. Moreover, the heightened security features, including the latest encryption standards, will ensure robust protection against cyber threats, solidifying its position as the cornerstone of secure communication networks.

To ensure we maximise the network performance of all buildings, every core site will have a ***full Ekahau Wi-Fi survey*** which is regarded as the 'gold standard' of Wi-Fi reporting.

Ongoing, the future operator of the network will be required to maintain a solution that continuously monitors and reports on network throughput at each segment of the network.

For new buildings and campus buildings, **CoL/P will maintain a wired score** (https://wiredscore.com) so that colleagues and visitors have constant visibility of a world class user experience for connectivity across our estate.

In conclusion, it is vital for CoL/P to adapt to these changing trends and provide a modern and flexible working environment that meets the needs of its employees, both now and in the future. By embracing new technologies and adopting a sustainable approach to network infrastructure, CoL/P can remain competitive and attract top talent in the industry.

g) Site types

To speed up network deployments, and to simplify the network there will be several predefined 'Site Types' which will describe exactly the network topology that should be deployed to that site.

Some locations are essential to maintain a service to employees, workers and visitors to the City, whilst some sites have a much lower criticality and the users on that site could use a business continuity and disaster recovery (BCDR) plan that dictates they simply move to another local site, or work from home.

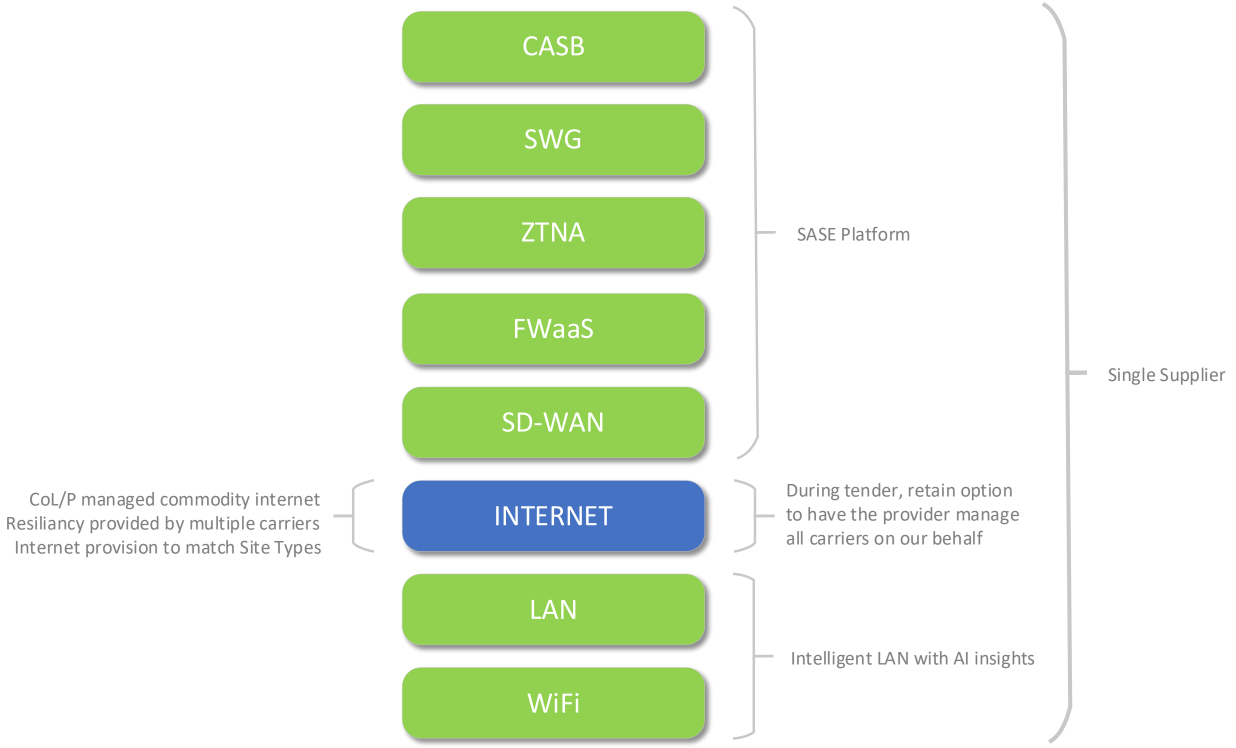
By adhering to a site type list, we can ensure that costs are kept as low as possible, whilst delivering a world class service and giving the flexibility to upgrade the site quickly and at little to no cost.

{THIS TABLE NEEDS UPDATING POST APPROVAL OF SITE TYPES}

Site Type	Name	Description
A	Datacentre	This site is a critical network location that could be a physical bricks and mortar datacentre or a main hyperscale cloud hosting facility
B	Campus Main Site	This site is considered a main office or HQ type location that has a critical mass of employees working from within it at a single time. It will contain multiple meeting rooms and AV equipment with complex BMS deployments. There will be a requirement for high density Wi Fi across the entire site.
C	Resilient Business Broadband Site	This site has less than 100 employees regularly working from it and there are no complex specialist equipment installs. It is a basic working office where users require high speed internet and access to CoL/P line of business applications. This site will have a mix of employees who must be physically present on site due to their role and also some employees who are able to work flexibly from other locations or home.
D	Non-Resilient Business Broadband Site	This site has less than 50 employees regularly working from it and there are no complex specialist equipment installs. It is a basic working office where users require high speed internet and access to CoL/P line of business applications. All employees utilising this site must be able to transfer to another site or work from home for business continuity should the site fail.

E	Rapid or IoT 4/5g Deployment Site	This site should be used for speed of deployment for new estate or utilised in combination of a D type site to provide resilience. It may also be used for sites that have a small IoT footprint such as sites that require a single BMS connection or for Door Access Controller connections.
F	Satellite Site	
G	CCTV Camera Site	

h) What we will procure



CASB

SWG

ZTNA

FWaaS

SD-WAN

SASE Platform

INTERNET

CoL/P managed commodity internet
Resiliancy provided by multiple carriers
Internet provision to match Site Types

During tender, retain option
to have the provider manage
all carriers on our behalf

LAN

WiFi

Intelligent LAN with AI insights

Single Supplier

6) Procurement & implementation plan

To deliver on the future network vision for CoL/P, DITS will conduct 5 clearly defined and well-planned stages of procurement and implementation.

a) Brilliant basics

Pinning ourselves to the DITS theme of ‘brilliant basics’ all new buildings across CoL/P should plan to be hyper connected.

All future new constructions must provision between 2 and 4 telco carriers. These carriers can be spread across Tier 1 and Alt-Net carriers, but our future sites must always have at least one Tier 1 carrier.

All carriers should be cabled into the basement or other suitable location of the building and converge in a secure comms room or meet-me room.

Where telcos are providing dark fibre, it would be suitable for them to build out a chamber in an adjacent street with the building and have pre-installed ducting allowing the telco connections to be provisioned into the building later without having to drill or dig or complete civils work.

‘Tier 1’ carrier is defined by market share which is listed below (as of April 2023). The recent SMT allowed us to consult with BT, Vodafone, Virgin Media O2 and an Alt-Net called Vorboss. A caveat to the above standard is where the provider of the cabling infrastructure is Openreach, who are a major player and sell cabling to nearly all carriers where they do not have their own fibre infrastructure.

By taking this approach, we ensure all future buildings have as many networking options available to us as possible both now and in the future.

Rank	Company	Market Share
1	BT	30.10%
2	Vodafone	22.50%
3	Virgin Media	14.20%
4	TalkTalk Business	7.30%
5	O2	6.70%
6	Gamma	5.60%
7	Colt Technology Services	4.50%
8	KCOM	2.10%
9	Glide	1.40%
10	DWS	1.30%

b) Let the market talk

The future network strategy will be defined by what we know now, and what we think we know about the future direction of network technology. Without outside consultation, it will also be bound by the skills and knowledge within DITS.

To ensure we counter this intrinsic limitation, our first step will be to conduct a Soft Market Test (SMT) which will allow us to engage in a compliant, non-committal and structured way with the industry and let them tell us about their latest advancements and future vision for the market.

c) Adjust & adapt

Only once we know as much as we can about the technology offerings and services on the market, can we be comfortable with the content of the Future Network Strategy.

This stage will see us review the market offering and adapt our vision and next steps to best fit the needs of the organisation against the commercial offerings available on the market.

A revised draft strategy will be formulated based on the market engagement in this stage.

d) Procure compliantly

When the strategy is finalised, we will launch a formal tender process with support from the Commercial department.

This procurement will include the provision of (but not limited to):

- MIA/DIA service
- An SD-WAN service
- A LAN support provision
- A WAN support provision
- A SASE solution.

e) Implementation

****THIS SECTION REQUIRES FURTHER INPUT WHEN AN AGREED PROJECT APPROACH IS FINALISED****

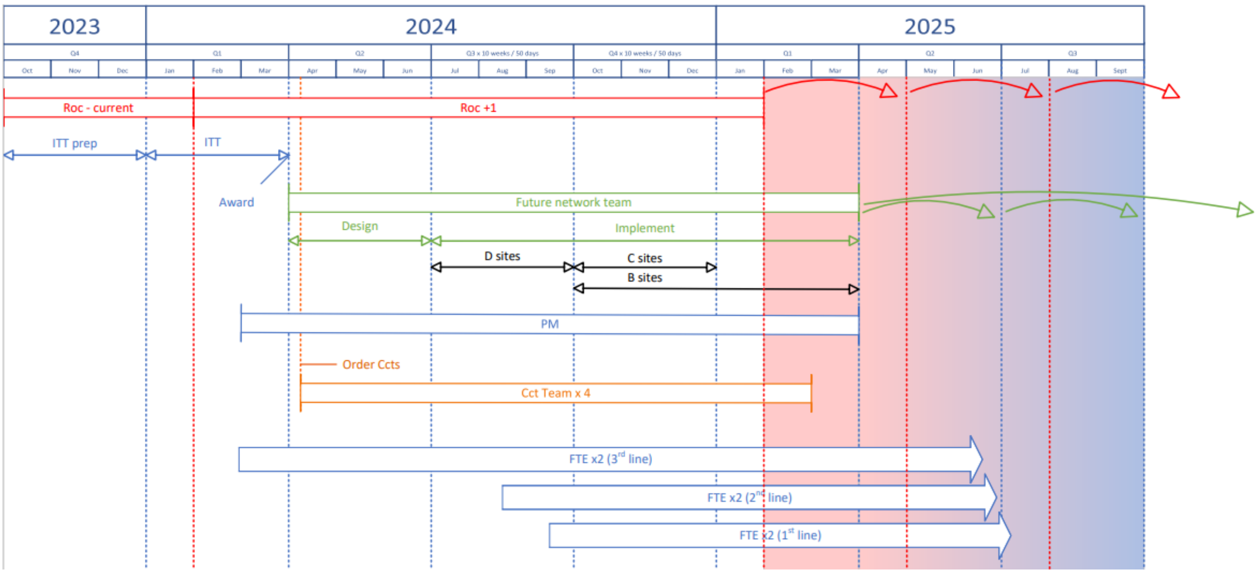
At the point we have a finalised strategy of what our future network provision should be we will need to:

- Recruit
- Design
- Build
- Test
- Deploy

The final approach for implementation has yet to be agreed. Several options are being considered, and the factors at play include:

- The extent to which the incumbent managed network service provider continues to be engaged
- Outsourcing vs insourcing certain roles
- Speed at which the network is refreshed.

The diagram demonstrates one of the options being discussed by the SLT:



7) Summary, recommendations & conclusion

- Ensure structured and compliant engagement with suppliers through to ITT.
- Ensure all technology selected in the future is vendor agnostic.
- Decouple existing network provision and suppliers and allow a period of reset and market evaluation.
- Agree this strategy is to provide a clear direction and roadmap for the future network and it is not a strategy to address existing solutions and vendors.
- Agree that the future network provision is requirements and solution orientated and not vendor constrained.
- Agree incumbent suppliers do not have contract extensions for multiple years until we have a defined procurement plan and thereby locking CoL/P into a sub-optimal technology platform for longer than is needed.
- Agree that this strategy outlines an acceptable future IT network provision for the organisation and that the programme is permitted to move into the detailed requirements gathering and ITT generation.
- The detailed ITT will come to the SLT for review and approval before going to market.

8) Version Control

f) Revision history

VERSION	DATE	AMENDED BY	SUMMARY
0.1		C. Walker	Document created
0.2		C. Walker	Updated to incorporate costs
0.3		C. Walker	Reviewed after comments at programme board
0.4		C. Walker	Feedback added
1.1	04/01/2024	T. Crombie	Minor edits to update wording and remove comments

g) Document approval

VERSION	DATE	APPROVED BY	APPROVAL STATUS (PENDING / APPROVED)
1.0	04/12/2023	Z. Ghauri	Approved