Example Best Practice Analysis

CLIENT: ...
N: ...
T: ...
E: ...

Date: ...

Site Configuration

Here you can see a technical overview of your current site infrastructure.

Components	Description
Infrastructure Type	Microsoft 365 Cloud Managed
Firewall Appliance	Sophos XGS 116w
Primary Connectivity	VDSL Supplied by BT
Telephony Provider	Unknown
Backup Power Supply (UPS)	Yes / No
Primary Email Solution	Microsoft 365 Exchange Online
Primary File Access	Microsoft 365 SharePoint
Wireless Solution	Ubiquiti Cloud Managed Access Points
Device Management	Microsoft Intune for Laptops
Backup Solution	Amazon AWS / Datto Backupify
Antivirus Solution	Sophos Central Intercept X Essentials
MDR Solution	Sophos MDR Complete
Laptop Encryption	Sophos Central Device Encryption
MFA	Enabled for Microsoft 365

Current Tech Stack

- MS365 Exchange Online
- MS365 SharePoint Online
- MS365 OneDrive
- Microsoft Teams
- Microsoft 365 EntraID / Azure AD
- Microsoft 365 Intune
- Ubiquiti Managed Wi-Fi
- Sophos Intercept X Essentials
- Sophos Device Encryption Management
- Datto Backupify
- Exclaimer Signature Management

Best Practice Analysis

The first steps to piecing together your IT roadmap is starting with a full site survey and IT audit. Firstly, we will conduct a full site survey of your IT hardware, software and services including a consultation with you and your staff. We detail your existing IT infrastructure and discuss any additional requirements and ongoing/outstanding problems. Our engineers will then install our highly-secure remote management and monitoring tools.

Once we have collated all your information, your dedicated account manager will contact you to arrange your Best Practice Analysis. This is a detailed document providing information on security, compliance and continuity specific to your charity. We also detail any upcoming renewals or out-of-date solutions, as well as information on forthcoming technologies and services that may benefit your organisation.

Your Audit Includes

- Business Continuity
- Physical Infrastructure
- Device Security
- Infrastructure Security
- User Security
- Productivity

Rating Breakdown: Business Continuity

Business continuity refers to the comprehensive strategies and practices put in place to ensure the uninterrupted operation of an organisation's information technology systems and services, even in the face of unforeseen events or disasters.

Best Practice Recommendations	Status
Cloud Based Email Solution	✓
Cloud Based File Share Solution	✓
Cloud Based User Management	✓
Cloud Based Device Management	Q
Cloud Backup Solution	Q
Third Party Vendor Support	✓
Failover Connectivity	–
Failover Network Hardware	×
Backup User Devices	×
Disaster Recovery Simulation	×
Rating:	Good

Key: ✓ In Place × Not in Place – Not Applicable / Possible Q Upcoming Project

Rating Scale: Unsatisfactory | Needs Improvement | Acceptable | Good | Excellent

Best Practice Recommendations

As part of our review, we have identified some key areas within your IT infrastructure that do not meet best practice guidelines. These are detailed below for your review in order of priority.

	Description / Resolution
High Priority	**No Centralised Management of Devices** Laptops, desktops and mobile device security policies and updates are not centrally managed.
	Resolution: Deploy Microsoft Intune With Intune, we can efficiently control and secure devices, ensuring consistent policies and updates across the board. It grants the ability to remotely deploy software and updates, bolstering cybersecurity measures by enforcing updates, access controls, and threat management.
High Priority	**No External Backup for Microsoft 365 Environment** Qlic does not currently backup your Microsoft 365 environment and will not be able to recover a corrupted mailbox, restore missing email or SharePoint files/folders within the Microsoft 365 environment in the event of a disaster recovery scenario.
	Resolution: Implement Microsoft 365 Cloud to Cloud backups, providing unlimited storage and one year retention, ensuring that all critical data stored within Microsoft 365 is securely backed-up to a third party outside of the Microsoft 365 framework.
High Priority	**No Cloud-Based File Sharing Solution** The organisation currently lacks a cloud-based system to share and access files. This causes delays, poor collaboration, and difficulty working remotely or managing document versions.
	Resolution: Implement SharePoint Online To resolve the issue, the organization will implement **SharePoint Online** as its cloud-based file sharing solution. SharePoint provides a secure platform for storing, accessing, and collaborating on documents from any location. It supports real-time editing, version control, and role-based access, ensuring that teams can work efficiently and securely. Integration with Microsoft 365 tools like Teams and Outlook further enhances productivity. The next steps include setting up SharePoint sites, migrating existing files, and providing staff training to ensure smooth adoption and proper use.

Best Practice Recommendations

As part of our review, we have identified some key areas within your IT infrastructure that do not meet best practice guidelines. These are detailed below for your review in order of priority.

	Description / Resolution
High Priority	**Issue: No Centralised User Management** The organisation currently lacks a centralised system for managing user identities, with individual user accounts being created and managed separately across devices and services. This leads to inconsistent access control, security risks, and increased administrative overhead. It also makes it difficult to onboard and offboard staff efficiently and securely, particularly in remote or hybrid working environments.
	Resolution: Deploy Microsoft Entra ID We recommend implementing Microsoft Entra ID as a cloud-based identity and access management solution. This will provide a secure, scalable platform for centralising user accounts, applying consistent access policies, and enabling secure login to Microsoft 365 and other cloud services. It will also streamline user onboarding, simplify password management, and support modern security practices such as multifactor authentication.

Best Practice Recommendations

As part of our review, we have identified some key areas within your IT infrastructure that do not meet best practice guidelines. These are detailed below for your review in order of priority.

	Description / Resolution
Medium Priority	**Failover Network Hardware** The absence of failover hardware poses a critical risk in the event of network hardware failure. Without backup systems in place, the network could become non-functional until replacements are procured and installed, potentially causing several days of downtime.
	Resolution: Store a Cold Spare Network Switch & Router. Please note that a cold spare router would not automatically update. Therefore, the deployment of this type of failover will inevitably take longer than an automated High Availability system.
Medium Priority	**Backup User Devices** The organisation doesn't currently hold any spare devices should there be a fault with any existing user device that may require it to be sent away for repair.
	We highly recommend maintaining around 10% of the total number of staff devices as spare devices. This percentage ensures that there are enough backup laptops to cover unexpected failures or repairs without significantly impacting operations.
Medium Priority	**No centralised device monitoring is currently in place.** Currently there isn't a system in position to oversee or manage all devices from a single location. This absence implies that each device likely operates independently without a unified way to track or manage them together.
	As an alternative to Microsoft Intune, that does not require Windows Professional, consider deployment of Datto Remote Monitoring & Management software across all devices. This would allow for centralised monitoring of device performance and unification of services such as software deployment and security policy.

Best Practice Recommendations

As part of our review, we have identified some key areas within your IT infrastructure that do not meet best practice guidelines. These are detailed below for your review in order of priority.

	Description / Resolution
Medium Priority	**Disaster Recovery Simulation & Testing** Currently there is no external Disaster Recovery Simulation or testing to ensure backups can be recovered
	Resolution: Implement Disaster Recovery Simulation & Testing Service Consider procuring annual disaster simulation testing of your organisational data to ensure a proven, planned recovery method is in place should a disaster occur.
Medium Priority	**Failover Connectivity** Currently there is no failover connectivity in place for the office. If the internet connection were to fail Microsoft 365, Email, SharePoint and OneDrive would not be accessible.
	Resolution: Implement Automated Backup Internet Connection This is essential for uninterrupted service delivery and ensures continual operations during internet outages.

Rating Breakdown: Physical Infrastructure

IT physical infrastructure refers to the physical components and facilities including server rooms, network equipment, cabling infrastructure etc.

Ensuring the reliability, scalability of IT physical infrastructure is crucial for operational resilience.

Best Practice Recommendations	Status
1Gbps Switching Equipment	✓
Structured Cabling	✓
Uninterruptable Power Supply	✓
Locked Data Cabinet	✓
Tidy & Labelled Data Cabinet	✓
Using Managed Printer Service	×
Centrally Managed Wireless Network	–
Full High Speed Wireless Coverage	×
Core Infrastructure has Vendor Warranty	×
Rating:	Good

Key: ✓ In Place × Not in Place – Not Applicable / Possible Q Upcoming Project

Rating Scale: Unsatisfactory | Needs Improvement | Acceptable | Good | Excellent

Best Practice Recommendations

As part of our review, we have identified some key areas within your IT infrastructure that do not meet best practice guidelines. These are detailed below for your review in order of priority.

	Description / Resolution
Medium Priority	**Basic Wi-Fi Provision** At present, the wi-fi network within the building is provisioned by a basic router, which may not be providing sufficient coverage or capacity.
	Resolution: Consider replacing the non-enterprise equipment with an enterprise grade Wi-Fi solution to allow for enhanced management, security, speed and roaming functionality. We recommend Ubiquiti Wi-Fi solutions as they have proven to perform excellently in our experience.
Medium Priority	**Data Cabinet Organisation** Data cabinet is disjointed, difficult to navigate and there is no cable management in place. In the event of a hardware fault, diagnosis and remedy could be slow and difficult.
	Resolution: Completely re-configure / replace the existing cabinet with dedicated cable management, colour coded cables and easily identified and labelled hardware.
Low Priority	**No Uninterruptable Power Supply or Surge Protection Installed** There are currently no backup power supplies (UPS) or mechanisms in place to protect against power surges. Without these safeguards, devices might be vulnerable to sudden power interruptions or fluctuations, potentially risking damage or data loss during power disruptions or surges.
	Resolution: Consider installation of a UPS battery backup or surge protector for critical network infrastructure.

Best Practice Recommendations

As part of our review, we have identified some key areas within your IT infrastructure that do not meet best practice guidelines. These are detailed below for your review in order of priority.

	Description / Resolution
Low Priority	**No Serviced Printer Arrangement with Qlic** There isn't an established service or maintenance plan in place with Qlic for the organisations printers. Without a serviced printer arrangement, there might not be regular maintenance, repairs, or support for the printers, which could lead to potential issues or disruptions in their functionality.
	Resolution: Please note that Qlic provides competitive serviced printer/copier leasing agreements. If you are able to provide a recent summary of printer spend, we would be happy to speak to our suppliers to see if we can reduce print costs and improve functionality.
Low Priority	**100Mbps Switch** There is a secondary 100Mbps switch in place being used by a few staff. This switch is below the minimum recommended speed, which will be severely impacting network performance.
	Resolution: Replace low-spec switches with Gigabit Switches to improve network speed and reliability.
Low Priority	**Core Infrastructure has Vendor Warranty** The core infrastructure components should be covered under a vendor warranty. This includes critical systems such as servers, storage, and networking equipment, ensuring that any hardware failures or issues can be addressed and resolved by the vendor.
	Resolution: Maintain an up-to-date record of warranty details for all core infrastructure components. Regularly review and renew warranties before expiration to ensure continuous coverage. Establish a protocol for contacting the vendor for support and service claims in the event of hardware malfunctions.

Rating Breakdown: Device Security

Device security is essential in today's interconnected world, as it encompasses the measures and protocols implemented to protect devices from unauthorised access, data breaches, and malicious attacks.

Best Practice Recommendations	Status
Anti-Virus/Malware Protection	✓
Anti-Ransomware Protection	✓
Internet Content Filtering	✓
Device Encryption	✓
Software Update Management Policies	✓
Mobile Device Management for Smartphones & Tablets	×
Operating System has Vendor Support for up to 12 Months	–
Operating System has Business Functionality	×
MDR or EDR Solution	×
All User Devices Owned by Organisation	?
Enforced MS365 Web Access for BYOD Devices	?
Rating:	Good

Key: ✓ In Place × Not in Place – Not Applicable / Possible Q Upcoming Project

Rating Scale: Unsatisfactory | Needs Improvement | Acceptable | Good | Excellent

Best Practice Recommendations

As part of our review, we have identified some key areas within your IT infrastructure that do not meet best practice guidelines. These are detailed below for your review in order of priority.

	Description / Resolution
High Priority	**No Anti-Virus, Malware or Ransomware Protection** Devices do not have centrally managed, active virus, malware or ransomware protection or active monitoring; leaving device insecure and open to cyber threats.
	Resolution: Deploy Sophos Central Intercept X Essentials Sophos Central Intercept X Essentials is a robust cybersecurity solution designed to protect devices from advanced threats with its comprehensive endpoint protection capabilities. It offers essential features like advanced anti-malware, exploit prevention, ransomware detection and response, helping organisations bolster their defence against evolving cyber threats.
High Priority	**Devices Running Windows Home** Several devices are currently running the Windows Home operating system and cannot be encrypted, domain joined to Azure Active Directory or centrally managed with Microsoft Intune.
	Resolution: Replace or upgrade laptops to Windows Professional, either purchasing licenses through the Windows store, or at a discounted rate from Charity Digital Exchange.
High Priority	**No Managed Laptop Encryption** Laptops do not have local encryption installed or managed. The ICO requires you to demonstrate that a device was appropriately encrypted prior to loss or theft to avoid data breach investigation.
	Resolution: Deploy Sophos Central Device Encryption Implement encryption on all laptops within the organisation to ensure GDPR compliance. Sophos will allow us to manage, support and evidence full disk encryption.

Best Practice Recommendations

As part of our review, we have identified some key areas within your IT infrastructure that do not meet best practice guidelines. These are detailed below for your review in order of priority.

	Description / Resolution
High Priority	**No Automated Software Update Management Policies** Devices are currently standalone, meaning operating system and application updates cannot be centrally managed or enforced. This increases the risk of vulnerabilities due to missed or delayed updates.
	Resolution: Implement Microsoft Intune By implementing Microsoft Intune, we can centrally manage and automate software and security updates across all devices. This ensures all systems stay up-to-date with the latest patches, reducing the risk of cyber threats and improving compliance with security standards.
High Priority	**All User Device NOT Owned by Organisation** When users access organisational systems from personally owned devices, it introduces security risks including lack of device management, unmonitored software, absence of standardised security controls, and higher susceptibility to data breaches.
	Resolution: All devices used to access organisational data and services should be owned and managed by the organisation. This ensures that every device complies with security policies, including encryption, antivirus protection, software update management, and endpoint monitoring. Full control over devices enhances data security, compliance, and operational support across the organisation. Where device ownership is not possible, additional security measures should be applied to BYOD devices, such as blocking the downloading of organisational data.
High Priority	**BYOD Devices Downloading Sensitive Information** When users access organisational data from personal (BYOD) devices, there is an increased risk of sensitive information being downloaded, saved locally, or synced to unmanaged devices. This can lead to data loss, breaches of confidentiality, and non-compliance with data protection standards.
	Resolution: We implement policies within Microsoft 365 to restrict BYOD devices from downloading, syncing, or saving files from OneDrive and SharePoint. Users are instead forced to work securely through the Microsoft 365 web portal, ensuring that organisational data remains within a controlled environment. This approach minimises data leakage risks and strengthens compliance with data protection requirements.

Best Practice Recommendations

As part of our review, we have identified some key areas within your IT infrastructure that do not meet best practice guidelines. These are detailed below for your review in order of priority.

	Description / Resolution
High Priority	**No Mobile Device Management for Smartphones & Tablets** Smartphones and tablets are not centrally managed, exposing the organisation to risks such as unsecured configurations, unmanaged apps, and potential data loss if devices are lost or compromised.
	Resolution: By using Microsoft Intune to manage mobile devices, we can enforce security policies, control app access, and remotely wipe data when needed. This reduces security risks and ensures mobile devices comply with organisational standards.
Medium Priority	**No Managed Detection & Response.** Anti-Virus, email protection and network permitter firewall do not have centralised monitoring to detect and act on suspicious user, device and network activity.
	Resolution: Implement Sophos MDR. Unlike traditional cyber defence solutions, MDR makes it easier for organisations to respond to cyber threats in a structured and rapid manner using a combination of AI and human-led threat hunting, providing more visibility into user activity, system vulnerabilities, and emerging threats with 24/7 monitoring and response!
Medium Priority	**No Content Filtering** Workstations have no Web Content Filtering to protect staff from inappropriate websites.
	Resolution: Upgrade to Sophos Intercept X Advanced (or if not currently using Sophos, install DNSFilter on a network or per device) for safe, secure and responsible internet traffic management for all staff devices.
Medium Priority	**Devices Not Compatible with Windows 11** Windows 10 will be outside of extended support in October 2025 and devices will no longer receive critical security updates.
	Resolution: Replace Hardware Consider a refresh of workstations below minimum specification to bring them in line with Windows 11 Professional.

Rating Breakdown: Infrastructure Security

IT infrastructure security refers to the configuration & protection of an organisation's underlying technology systems, networks, and resources from potential threats, vulnerabilities, and unauthorised access.

Best Practice Recommendations	Status
Infrastructure Management	✓
Device Management Policies Meet Cyber Essentials Guidelines	✓
Dedicated Network Perimeter Firewall	✓
Firewall Licensed & Vendor Supported	✓
Server Operating System has Vendor Support	✓
Remote Access Configured Securely	✓
Remote Access Brute Force Protection	–
Line of Business Software Has Vendor Support	–
Microsoft 365 Security Baseline Policies Applied	×
Cyber Essentials Accredited	–
Rating:	Good

Key: ✓ In Place × Not in Place – Not Applicable / Possible Q Upcoming Project

Rating Scale: Unsatisfactory | Needs Improvement | Acceptable | Good | Excellent

Best Practice Recommendations

As part of our review, we have identified some key areas within your IT infrastructure that do not meet best practice guidelines. These are detailed below for your review in order of priority.

	Description / Resolution
High Priority	**Device Management Policies Do Not Meet Cyber Essentials Guidelines** Staff are currently using personal (BYOD) devices that are not enrolled in any centralised management system. As a result, there is no ability to enforce critical security policies such as device encryption, password complexity, or operating system updates. This creates significant security and compliance risks, particularly around data protection and cyber threat exposure.
	Resolution: Deploy Microsoft Intune & Entra ID (Azure AD) To address this, we recommend using Conditional Access policies in Microsoft Entra ID to restrict access to Microsoft 365 services unless devices meet defined criteria. Additionally, deploy Intune App Protection Policies to enforce security controls (e.g. preventing downloads, copy/paste restrictions, requiring PIN or biometric access) on corporate apps like Outlook, Teams, and OneDrive — even on personal devices. This ensures organisational data is protected without needing to fully manage the personal device, aligning with Cyber Essentials requirements in BYOD scenarios.
Medium Priority	**Dedicated Network Perimeter Firewall** The office does not currently benefit from the protection a stateful firewall will provide.
	Resolution: Install Sophos XGS Stateful Firewall Upgrading to a stateful Sophos XGS firewall from the current basic router firewall would significantly enhance your cybersecurity posture. The Sophos XGS provides advanced threat protection with deep packet inspection, application control, and intrusion prevention capabilities, offering granular control over network traffic. This means better defence against sophisticated cyber threats, ensurin safeguard sensitive data and maintain operational continuity.
Medium Priority	**Line of Business Software Has Vendor Support** Line of Business Software with Vendor Support refers to specialised applications provided with direct support from the software vendor.
	Resolution: Having vendor support for Line of Business Software ensures expert guidance and quick resolution of any issues, enhancing software reliability and performance.

Best Practice Recommendations

As part of our review, we have identified some key areas within your IT infrastructure that do not meet best practice guidelines. These are detailed below for your review in order of priority.

	Description / Resolution
High Priority	**Microsoft 365 Baseline Policies Applied** Several non-standard security policies within your Microsoft 365 environment, recommended by Microsoft, are recommended for safeguarding your systems. These policies are designed to establish a strong security framework, covering aspects such as data protection, access controls, and threat detection.
	Resolution: Our proposal is to implement a series of technical enhancements aimed to significantly bolster the security measures within your Microsoft 365 environment. These improvements include the adoption of multi-factor authentication, geo-location blocking, integration of advanced threat protection, and conducting a thorough security audit. Each measure not only enhances your overall security framework but also adheres to Microsoft best practices, essential for protecting sensitive information. Through these enhancements, we can help ensure that your organisation's data is well-protected against unauthorised access and potential breaches.
Medium Priority	**Cyber Essentials** Cyber Essentials is a government-backed, industry-supported scheme to help organisations protect themselves against common online threats. It provides a clear set of guidelines and security practices that, when implemented, can prevent cyber attacks.
	Resolution: By achieving Cyber Essentials certification, your organisation can demonstrate its commitment to cyber security. Certification assures customers and stakeholders of the organisation's proactive stance on mitigating cyber risks.

Rating Breakdown: User Security

User security encompasses the implementation of measures and practices to protect users and their digital assets from various security risks and threats.

Best Practice Recommendations	Status
Password Complexity Enforced on Devices	✗
Password Complexity Enforced on Email	✗
Password Management Software	✗
Dark Web Monitoring of Passwords	✗
Advanced Email Anti-Virus & Spam Protection	✗
Multi-Factor Authentication Enforced for Email	✓
Geo-Location Blocking Enforced for Email	–
Phishing Awareness Training Performed Regularly	✗
Phishing Simulation Performed Regularly	✗
Rating:	Good

Key: ✓ In Place ✗ Not in Place – Not Applicable / Possible Q Upcoming Project

Rating Scale: Unsatisfactory | Needs Improvement | Acceptable | Good | Excellent

Best Practice Recommendations

As part of our review, we have identified some key areas within your IT infrastructure that do not meet best practice guidelines. These are detailed below for your review in order of priority.

	Description / Resolution
High Priority	**Multi-Factor Authentication (MFA) Not Enforced for MS365** Currently, users are able to access their MS365 accounts with just a single password. This exposes the organisation to high-risk threats such as phishing attacks and credential theft, especially given the widespread availability of breached credentials on the dark web.
	Resolution: Enforce Multi-Factor Authentication (MFA) Enforce across all email accounts using Microsoft Entra ID (formerly Azure AD). MFA significantly strengthens login security by requiring a second factor (e.g. SMS code, authenticator app, or biometrics), dramatically reducing the risk of unauthorised access — even if credentials are compromised.
High Priority	**No Geo-Location Blocking for MS365 Access** With an ever-increasing dependence on electronic communication, it's vital to maintain a high level of security. At present, your Microsoft 365 environment is accessible from any location in the world.
	Resolution: Implement Conditional Access policies Implement Conditional Access for Office 365. Conditional access can will prevent any unauthorised access by enforcing the use of MFA for ALL users and sending the end user a verification code each time they try to login from a new device or location, it can also be used to define specific conditions in which a user is able to access Microsoft 365, such as user geo location, device, network, user group membership, and more.
High Priority	**No Advanced Email Anti-Virus & Spam Protection** The email environment lacks intelligent scanning for malware, phishing attempts, and malicious links, making it easier for threats to reach end users and increasing the likelihood of successful attacks.
	Resolution: License & Deploy Defender for Microsoft 365 Deploy Microsoft Defender for Office 365 or an equivalent email protection solution. This provides real-time scanning of incoming and outgoing emails, phishing and malware protection, URL/link checking, and detailed reporting — all critical to reducing user risk and email-based threats.

Best Practice Recommendations

As part of our review, we have identified some key areas within your IT infrastructure that do not meet best practice guidelines. These are detailed below for your review in order of priority.

	Description / Resolution
High Priority	**Weak or Unenforced Device Passwords** Personal devices used by staff do not follow any enforced password policies, making them susceptible to unauthorised access and local data compromise.
High Priority	**Resolution: Enforce Password Policy via App Protection** Use Microsoft Intune App Protection Policies to require strong passwords and device-level security for access to M365 apps. This helps ensure that even on personal devices, organisational data is protected behind proper authentication standards.
High Priority	**Strong Password Complexity Not Enforced on Email or Devices** There are currently basic or no requirements in place for strong passwords, which could pose a security risk. It's important to ensure that devices have password policies in place to protect against unauthorised access.
High Priority	**Resolution: Deploy Microsoft Azure Active Directory & Intune,** Utilise Microsoft Intune and Azure Active directory to ensure password complexity within Microsoft 365. Define specific password policies, including length and complexity requirements, and then apply these policies to relevant user groups or the entire organisation. This helps enhance security by enforcing stronger password practices across devices and accounts.
Medium Priority	**No Password Management Solution** Users are likely reusing passwords or storing them insecurely on personal devices. This creates risk across multiple platforms, especially when credentials are reused across work and personal accounts.
Medium Priority	**Resolution: Roll Out a Cloud-Based Password Manager** Introduce an enterprise password management tool like Keeper or LastPass. These tools store strong, unique credentials securely and work across personal devices without requiring device ownership or control.

Best Practice Recommendations

As part of our review, we have identified some key areas within your IT infrastructure that do not meet best practice guidelines. These are detailed below for your review in order of priority.

	Description / Resolution
Medium Priority	**No Dark Web Monitoring for Leaked Credentials** There is currently no way to detect if organisational email addresses or passwords have been leaked or sold online. This is particularly dangerous in BYOD environments where personal and work usage can overlap.
Medium Priority	**Resolution: Enable Credential Leak Monitoring** Use dark web monitoring tools often incorporated within password management tools to get alerts when organisational credentials appear in known breaches. This enables early action to reset passwords and secure accounts before damage is done.
Medium Priority	**No Cybersecurity Training for Users** Staff using personal devices have not received formal training on identifying phishing attempts, risky links, or cyber hygiene. This is a critical oversight as user behavior is often the weakest security link.
Medium Priority	**Resolution: Launch Regular Phishing Awareness Training** Run monthly phishing and security awareness training via platforms like ProofPoint. This arms staff with practical knowledge and improves their ability to recognise and report suspicious activity.

Rating Breakdown: Productivity

Productivity encompasses the efficient and effective use of technology tools and systems to enhance individual and team performance.

Best Practice Recommendations	Status
Anywhere Access to Files & Folders	✓
Anywhere Access to Line of Business Applications	✓
User Hardware Standards Above Recommended Specifications	✓
Server and/or Remote Server Performance Adequate	✓
Data Structure / Layout follows Best Practice Guidelines	✓
21" or Larger High-Definition Monitors	✓
Docking Stations for Laptops	–
Email Signature Management	✗
Formal IT Training for Staff	✗
Use of AI Productivity Tools	Possible
Rating:	Good

Key: ✓ In Place ✗ Not in Place – Not Applicable / Possible Q Upcoming Project

Rating Scale: Unsatisfactory | Needs Improvement | Acceptable | Good | Excellent

Best Practice Recommendations

As part of our review, we have identified some key areas within your IT infrastructure that do not meet best practice guidelines. These are detailed below for your review in order of priority.

	Description / Resolution
High Priority	**Data Structure - SharePoint Layout Does Not Follow Best Practice** Please see the following comments from our engineers. • **Unused Default Site:** Missing central updates and communication hub. • **Limited Use of Pages / Subsites:** Fragmented content, hindering collaboration. • **Team Sites Using Default Doc. Library:** Limits customisation and scalability. • **Complex Security Setup:** Harder management, potential vulnerabilities. • **Teams Connected Sites**: File permissions are not managed by unique groups. • **Using Classic Team Sites:** Reduced functionality, missing collaboration tools, productivity boosters.
	Resolution: SharePoint Restructure Our recommended solution is to completely rebuild the current SharePoint site to ensure it is setup for long term use and to best practice recommendations. Currently all your SharePoint data resides within the default document libraries, we do not recommend this as best practice from a user experience, GDPR and security perspective. We would migration this into a new modern SharePoint Communications Site and splitting into multiple correctly designed document libraries, which has the following benefits: 1. Fewer sync errors due to naturally reducing the path lengths. 2. Fewer sync cycles due to reducing the how often each library needs syncing. 3. Users only sync the document libraries they need. 4. Security can be applied at the document library level for easier management. 5. Easier user navigation. 6. Custom views can be applied to each document library. 7. Custom meta tags can be applied to each document library.

Best Practice Recommendations

As part of our review, we have identified some key areas within your IT infrastructure that do not meet best practice guidelines. These are detailed below for your review in order of priority.

	Description / Resolution
Medium Priority	**Workstations Below Minimum Recommend Specification** As highlighted within the hardware lifecycle attachment, some of the devices currently in use fall short of our minimum recommended specification and may be impeding user productivity.
Medium Priority	**Resolution: Consider Upgrading or Replacing Hardware** Consider a refresh of workstations below minimum specification to bring them in line with recommended Windows Professional, Intel Core i5 (8th Generation or newer), 16GB RAM and Solid-state hard drives.
Low Priority	**Docking Stations & Monitors for Laptops** The organisation does not appear to have procured docking stations or external monitors for user laptops.
Low Priority	**Resolution: Purchase Hybrid Docking Stations & Monitors** Research shows that docking stations and larger and ideally dual monitors, improve user productivity significantly. Docking stations and monitors for laptops simplify work setups by centralising connections to multiple devices. They streamline transitions from mobile to workstation use, ensuring quick access to peripherals and boosting productivity without cable clutter.
Low Priority	**No Email Signature Management** The organisation does not have centralised management of users' email signatures.
Low Priority	Exclaimer for Microsoft 365 offers centralised signature management for all users, allowing you to create multiple signatures from the Exclaimer portal and automatically roll out to all users. Exclaimer also enforces the managed signature to the users email from any device, so replying from your smartphone still applies the appropriate corporate signature to all emails.

Best Practice Recommendations

As part of our review, we have identified some key areas within your IT infrastructure that do not meet best practice guidelines. These are detailed below for your review in order of priority.

	Description / Resolution
Low Priority	**No Formal IT Training for Staff** The organisation does not currently have a formal IT training function available to staff to assist with training in productivity tools, cyber security awareness and upcoming technologies.
	Qlic has partnered with Bigger Brains Training to provide an innovative training platform for your users. This collaboration aims to enhance the skills and knowledge of your staff through a comprehensive suite of online courses and training modules. Bigger Brains covers a wide range of training categories, including **Microsoft & Google Productivity Tools**, **Business Skills**, **Cybersecurity**, **Project Management**, **Communication**, and **Diversity and Inclusion**. By leveraging Bigger Brains' expertise in e-learning, Qlic NFP ensures clients have access to high-quality, flexible, and engaging educational resources, empowering them to achieve their organizational goals more effectively.

Best Practice Recommendations

As part of our review, we have identified some key areas within your IT infrastructure that do not meet best practice guidelines. These are detailed below for your review in order of priority.

	Description / Resolution
	Docking Stations & Monitors for Laptops The organisation does not appear to have procured docking stations or external monitors for user laptops.
i	**Resolution: Purchase Hybrid Docking Stations & Monitors** Research shows that docking stations and larger and ideally dual monitors, improve user productivity significantly. Docking stations and monitors for laptops simplify work setups by centralising connections to multiple devices. They streamline transitions from mobile to workstation use, ensuring quick access to peripherals and boosting productivity without cable clutter.
	Use of AI Productivity Tools AI is a profound tool to help boost staff and workplace productivity.
i	AI boosts workplace productivity by automating routine tasks and enabling rapid data analysis. It enhances decision-making, personalises employee experiences, and aids in predictive maintenance, while also reducing errors and fostering continuous learning. Watch our Microsoft Copilot demo here.
	Video Conferencing Solution A video conferencing solution enables real-time virtual meetings, enhancing communication, collaboration, and productivity while reducing travel costs.
i	Video conferencing solutions enhance productivity by reducing travel time, streamlining communication for quick decision-making, and enabling efficient remote work. It supports flexible scheduling across time zones and integrate with other digital tools to streamline workflows, helping employees stay focused, reduce downtime, and increase overall efficiency.

Rating Breakdown: Telecoms

Productivity encompasses the efficient and effective use of technology tools and systems to enhance individual and team performance.

Best Practice Recommendations	Status
Cloud Telephony Solution	✓
Telephony Redundancy In-Place	✓
Call Recording with at least 90 Days Retention	✓
Voice Encryption, Call Analytics and Fraud Detection	✓
CRM Integrated with Phone System	✓
Competitive Mobile Tariff	✓
International Roaming Included	–
High Speed Broadband Connectivity	✘
Rating:	Good

Key: ✓ In Place × Not in Place – Not Applicable / Possible Q Upcoming Project

Rating Scale: Unsatisfactory | Needs Improvement | Acceptable | Good | Excellent

Best Practice Recommendations

As part of our review, we have identified some key areas within your IT infrastructure that do not meet best practice guidelines. These are detailed below for your review in order of priority.

	Description / Resolution
Medium Priority	**Broadband Speeds are Insufficient** Broadband connectivity is outdated and cannot handle modern business demands.
Medium Priority	**Resolution: Implement Dedicated High Speed Internet Connectivity** Migrate to FTTP, FTTC or a Dedicated Leased Line to take advantage of faster and more stable internet options.
Low Priority	**No CRM Integrated with Phone System** The telephony system does not integrate with the CRM (such as Sage, SalesForce etc), leading to missed opportunities for streamlined workflows.
Low Priority	**Resolution: Enable CRM Integration** Enable CRM integration with a cloud telephony platform to log calls automatically, improve customer interaction history, and simplify call workflows.
Low Priority	**No International Roaming Tariff** High costs associated with international roaming can impact budgets significantly.
Low Priority	**Resolution: Implement Voice & Data Roaming Package** Implement cost-effective roaming packages or use VoIP services through mobile apps like Teams or Zoom over Wi-Fi/4G.
Low Priority	**Call Recording Insufficient** Organisation is unable to record calls or the current product is not fit for purpose, potentially violating compliance requirements in regulated industries.
Low Priority	**Resolution: Implement Complaint Call Recording** Implement call recording with secure storage and role-based access on a cloud telephony platform to meet compliance standards like GDPR or industry-specific requirements.

Best Practice Recommendations

As part of our review, we have identified some key areas within your IT infrastructure that do not meet best practice guidelines. These are detailed below for your review in order of priority.

	Description / Resolution
High Priority	**On-Premise Telephony Solution** Organisation does not have a modern cloud telephony system to ensure seamless communication during outages or remote work
	Resolution: Implement Cloud Telephony Implement a cloud telephony system (e.g., Microsoft Teams Phone, 8x8, Gamma etc) that provides failover, call routing, and remote access for business continuity.
High Priority	**No Telephony Redundancy in Place** No telephony redundancy exists, meaning downtime during broadband failure affects incoming and outgoing calls.
	Resolution: Implement Failover Configuration Introduce a failover setup with a 4G/5G, ADSL, FTTC backup connectivity to ensure continuity of voice services during broadband outages. Migrate to a cloud telephony solution with softphone capabilities.
High Priority	**No Voice Encryption, Call Analytics and Fraud Detection** Current telephony system lacks encryption, and there is no mechanism to monitor telephony usage for unusual patterns, leading to potential fraud risks.
	Resolution: Deploy Comprehensive Telephony Solution Deploy a cloud telephony platform with built-in encryption, fraud detection, call analytics, and reporting to monitor and prevent misuse.
Medium Priority	**Broadband Speeds are Insufficient** Broadband connectivity is outdated and cannot handle modern business demands.
	Resolution: Implement Dedicated High Speed Internet Connectivity Migrate to FTTP, FTTC or a Dedicated Leased Line to take advantage of faster and more stable internet options.

Hardware Audit

We have taken the opportunity to audit your existing hardware and highlight lifecycle dates for each device.

How Do We Work Out The Lifecycle?

- Desktops: Recommended 5-year lifecycle
- Laptops: Recommended 3-year lifecycle
- Windows 7/8 Pro: Out of extended support January 2020
- Windows 10: End of support October 2025
- Intel Core i5 8th Gen or Lesser: Recommended replace
- 8GB Ram or Less: Recommended replace / upgrade

Attached with this proposal document is a device report in Excel format taken from our ScreenConnect remote support software, which includes our recommendations for upgrading/replacing any devices which do not meet the above device specifications for Operating System, RAM or Processor.

Our recommendations are based on providing a good experience for staff who will be using your current platform as well as the additional resources needed for video calling solutions such as Teams or Zoom.

The recommended action to take for each device has been given on the spreadsheet.

Hardware Audit

We have taken the opportunity to audit your existing hardware and highlight lifecycle dates for each device.

Device Name	Last User	OS	CPU	RAM	Make	Mode
LP001		Windows 10 Home	Intel Core i5-8250U	8	Asus	UX430UAR
LP002		Windows 10 Home	Intel Core i3-1005G1	8	Asus	UX425JA_ UX425JA
LP003		Windows 11 Home	Intel Core i3-1115G4	8	Asus	X515EA_ X1500EA
LP004		Windows 11 Home	Intel Core i3-1115G4	8	Asus	X515EA_ X1500EA
LP005		Windows 11 Home	Intel Core i3-1115G4	8	Asus	X515EA_ X1500EA
WS001		Windows 10 Home	Intel Core i5-1135G7	8	Asus	X515EA_ X1500EA
WS002		Windows 11 Home	Intel Core i5-1135G7	16	Asus	X421EAY_ S413EA
WS003		Windows 11 Pro	Intel Core i5-1235U	16	Lenovo	Think Book 21DH
WS004		Windows 11 Pro	Intel Core i5-1235U	16	Lenovo	Think Book 21DH
WS005		Windows 11 Pro	Intel Core i5-1235U	16	Lenovo	Think Book 21DH
WS006		Mac OS X 14.1	Apple M1	8	Apple	MacBook Air10,1
WS007		Windows 11 Pro	AMD Ryzen 5 7520U	16	Lenovo	Idea 82YU

Recommendation

Replace Soon	Replace Within 12 Months	Replace in 2+ Years

IT Roadmap Summary

We have developed this IT roadmap based on best practice recommendations and our extensive experience working with hundreds of organisations in your sector. By following this structured approach, your organisation will build a much-improved, more robust, and secure IT infrastructure.

Rather than requiring large overhauls or major projects, regular investment in IT through proactive maintenance ensures long-term stability and resilience. This approach minimises disruption, improves user experience, and ultimately benefits both staff and beneficiaries.

Immediate Priorities (0-6 Months)

Device Compatibility with Windows 11 – Upgrade or replace non-compatible devices ahead of Windows 10 end-of-life in October 2025.

Microsoft 365 Baseline Policies – Apply Microsoft's recommended security policies to enhance protection, access controls, and threat detection.

Remove Office 2019 – Uninstall Office 2019 and replace with Microsoft 365 apps.

Deploy Managed Encryption for Laptops – Ensuring encryption reporting can be provided in the event of a lost or stolen device.

Next 12 Months

Disaster Recovery Simulation & Testing – Regular disaster recovery testing ensures that backups can be successfully restored, minimising downtime and operational risk.

Cyber Essentials Compliance – Apply for Cyber Essentials Accreditation to show beneficiaries and governing bodies your commitment to Cyber security.

12-24 Months

Phishing Simulation & Training – Implement regular cybersecurity training and phishing attack simulations.

By following this roadmap, your organisation will strengthen its IT environment, reduce risks and support long-term digital sustainability.

IT Infrastructure Classification

As part of our Best Practice Analysis, we assess key areas of your IT Infrastructure and evaluate each area based on the information we have available and rate this against our recommendations for organisations of a similar size, classification and framework. This is broken down in more detail on the following pages

	Initial Rating	Proposed Rating
Business Continuity	Good	Excellent
Physical Infrastructure	Acceptable	Excellent
Device Security	Good	Excellent
Infrastructure Security	Acceptable	Excellent
User Security	Unsatisfactory	Excellent
Productivity	Needs Improvement	Excellent
Telecoms	Excellent	Excellent
Cyber Essentials	Not Attainable	Attainable

Rating Scale: Unsatisfactory | Needs Improvement | Acceptable | Good | Excellent

Useful Links & Support Information

Did You Know?

We want to make sure you have everything you need to get the most out of working with Qlic IT. Below are some helpful resources and links to support you:

Customer Support Hub

Our Customer Support page is your go-to resource for helpful tools and information, including (but not limited to):

- Useful links to user management forms and self-help articles
- Clear information on our Service Level Agreements (SLAs)
- A helpful IT Glossary to simplify technical terms

Check out our Customer Support page here!

Client Ticket Portal

If you haven't already signed up, our Client Ticket Portal makes it easy to:

•Track the status of existing tickets and view your support history in one place

Need access? Just let us know and we'll get you set up quickly.

We're Telephone-Centric

We understand the value of speaking to a real person, we pride ourselves on being telephone-centric. Call us on: 0203 832 7010 – we're here to help.

Stay Connected - Events & Insights

Click Here to Explore Our Events Page

- Be the first to know about our upcoming webinars, in-person events, and exhibitions where Qlic IT will be speaking or exhibiting.
- Missed a webinar? You can re-watch previous events, including topics such as cyber security, Microsoft 365, cloud solutions, and more.

Click Here to Subscribe to Our Newsletter

Never miss an update, subscribe to the Qlic IT newsletter to receive:

- Invitations to future events
- Monthly IT tips and best practice guidance
- Cyber security updates tailored to charities
- Industry news and software changes that affect your organisation

Qlic

@QlicNFP
@QlicNFP
@Qlic IT for Charities

ENQUIRIES 0203 904 3464

QlicNFP.com