Qlic

Best Practice Analysis

CLIENT:
NAME:
T:
E:

05/01/2024

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 We also detail any upcoming renewals or out-of-date solutions, as well as information on forthcoming technologies and services that may benefit your organisation.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

Site Configuration

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

Network Requirements	Single Office with Hybrid Working
Infrastructure Type	Microsoft 365 Cloud Managed
Firewall Appliance	Sophos XGS 116w
Primary Connectivity	VDSL Supplied by BT
Backup Power Supply (UPS)	Yes
Primary Email Solution	Microsoft 365 Exchange Online
Primary File Access	Microsoft 365 SharePoint
Wireless Solution	Cloud Managed Wireless Access Points
Device Management	Microsoft Intune for Laptops
Backup Solution	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

- Microsoft Intune - Mobile Device Management
- Azure Active Directory – User Management
- Outlook Desktop & Web Access
- OneNote
- Word
- Excel
- PowerPoint
- Windows Server
- SharePoint – Organisational File Storage
- OneDrive – Personal User File Storage
- Microsoft Teams
- Sophos Endpoint & Intercept X
- Sophos Device Encryption
- Datto Backupify
- Apple Mac OS

Best Practice Recommendations

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	Good	Excellent
Device Security	Acceptable	Excellent
Infrastructure Security	Good	Excellent
User Security	Acceptable	Excellent
Productivity	Good	Excellent
Cyber Essentials	Not Attainable	Attainable

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

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	✓
Cloud Backup Solution	✓
Third Party Vendor Support	✓
Failover Connectivity	–
Failover Hardware	×
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 IT strategy 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 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	**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.
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.

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	×
Managed & Serviced Printer's with Vendor Agreement	✓
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 IT strategy 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 Virgin Hitron 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.

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 Protection	✓
Anti-Malware Protection	✓
Anti-Ransomware Protection	✓
Internet Content Filtering	✓
Device Encryption	×
Software Update Management Policies	✓
Base Operating System has Vendor Support	✓
Base Operating System has Business Functionality	✓
MDR or EDR Solution	×
Rating:	Acceptable

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 IT strategy 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	**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.
High Priority	**No Automated Software Update Management Policies** Devices are currently standalone, and updates cannot be centrally managed or enforced.
	Resolution: Deploy Microsoft Intune – See Issue 1
Medium Priority	**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!

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	–
Cyber Essentials	×
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 IT strategy 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** Devices are currently standalone, and updates and security policies cannot be centrally managed or enforced.
	Resolution: Deploy Microsoft Intune – See Issue 1
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, ensuring you can 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.
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:	Acceptable

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 IT strategy 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	**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.
	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.
High Priority	**Basic Email Protection Only** The current email setup only has basic anti-virus / spam protection.
	Resolution: Implement Microsoft Defender for Office 365 Protect your organisation against sophisticated threats such as phishing and zero-day malware and automatically investigate and remediate attacks by leveraging trillions of signals from the Microsoft Intelligent Security Graph and analysing billions of emails daily.
High Priority	**No Geo Location Blocking within Microsoft 365** 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.
	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.

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	×
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 IT strategy 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.
	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.
	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.
	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 IT strategy 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
ℹ	**Docking Stations & Monitors for Laptops** The organisation does not appear to have procured docking stations or external monitors for user laptops.
	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.
ℹ	**Use of AI Productivity Tools** AI is a profound tool to help boost staff and workplace productivity.
	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.

Qlic

@QlicNFP
@QlicNFP
@Qlic IT for Charities

ENQUIRIES 0203 904 3464

QlicNFP.com

Book your Free IT Consultation