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 We also detail any upcoming renewals or out-of-date solutions, as well as information on forthcoming technologies and services that may benefit your organisation.

Click Here to Download our Example Best Practice Analysis

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 / No
Primary Email Solution	Microsoft 365 Exchange Online
Primary File Access	Microsoft 365 SharePoint
Wireless Solution	Ubiquiti Cloud Managed Wireless Access Points
Device Management	Microsoft Intune for Laptops Windows Server for Desktops
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

- 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 annual IT review, 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.

	Initial Rating	Proposed Rating
Business Continuity	Very Good	Excellent
Physical Infrastructure	Good	Excellent
Device Security	Good	Excellent
Infrastructure Security	Good	Excellent
User Security	Excellent	Excellent
Productivity	Very 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	Q
Cloud Backup Solution	Q
Third Party Vendor Support	✓
Failover Connectivity	–
Failover Hardware	×
Remote Management & Monitoring Tools	×
Cyber Essentials Accreditation	×
Rating:	Good

Key: ✓ In Place × Not in Place – Not Applicable 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	**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 LFJL 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.
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.

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.

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	×
Rating:	Good

Key: ✓ In Place × Not in Place – Not Applicable 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.
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.
Low Priority	**No Serviced Printer Arrangement** There isn't an established service or maintenance plan in place for the 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.

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:	Good

Key: ✓ In Place × Not in Place – Not Applicable 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** LFJL devices are currently standalone, and updates cannot be centrally managed or enforced.
	Resolution: Deploy Microsoft Intune – See Issue 1

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	–
Rating:	Good

Key: ✓ In Place × Not in Place – Not Applicable 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** LFJL 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 LFJL 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 that LFJL can safeguard sensitive data and maintain operational continuity.

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	✓
Advanced Email Anti-Virus & Spam Protection	✓
Multi-Factor Authentication Enforced for Email	✓
Multi-Factor Authentication Enforced for Remote Access	–
Geo-Location Blocking on Email & Cloud Platforms	×
Phishing Awareness Training Performed Regularly	×
Phishing Simulation Performed Regularly	×
Rating:	Good

Key: ✓ In Place × Not in Place – Not Applicable 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, See Issue 1. 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.

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	**Phishing Simulation & Training** The organisation does not currently conduct regular phishing training or email attack simulations to upskill staff on cyber security.
	Resolution: Deploy ProofPoint Simulation Phishing simulation and training software is recommended to improve an organisation's cybersecurity by educating employees on how to identify and respond to phishing attacks. By training employees to be more vigilant and aware of potential threats, organizations can reduce the risk of successful phishing attacks and better protect sensitive data and systems.

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	×
Rating:	Good

Key: ✓ In Place × Not in Place – Not Applicable 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	**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 Subsite Use**: Fragmented content, hindering collaboration. • **Default Library Restriction:** Limits customisation and scalability. • **Complex Security Setup:** Harder management, potential vulnerabilities. • **Minimal 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. In migrating your data, we will be working with yourselves to ensure the correct level of access-based user permissions are in place, safeguarding your critical data and making sure users are only able to view and access the files and folders they are permitted to. Users will be able to share documents whilst benefiting from centrally controlled security policies for files, folders and email. We will configure these services to work seamlessly with your current equipment and any new devices going forward. Our aim is to keep the existing user experience intact, with limited change or disruption.

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 at the beginning of the document, several 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 Although we understand it may not be viable to replace these devices all at once. Please consider a refresh of workstations below minimum specification to bring them in line with recommended Windows Professional, Intel Core i5, 16GB RAM and Solid-state hard drives. If not for everyone, then perhaps for the core/power users that are currently experiencing issues with device performance.
Low Priority	**Docking Stations for Laptops** The organisation does not appear to have procured docking stations for the laptops.
	Resolution: Purchase Hybrid Docking Stations Docking stations 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.

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
- Intel Core i5 7th Gen or Lesser: Recommended replace
- 6GB 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.

Qlic

@QlicIT

@QlicIT

@Qlic IT for Business

ENQUIRIES 0203 904 3464

QlicIT.com