Tech & Cost Audit:

How our systems & spending stack up

DEMO SITE

Demo UK Limited

Created by:

Jay Ball

Quote ID: Q123456

Date: 06.06.2025

Prepared for:

Demoro Bobero

Please note all prices exclude VAT.

Baseline Plan

Initial Assessment Summary

Audit Score

0 50 80 100

Managed IT

Microsoft Cloud

Network Infrastructure

Cyber Security

Communications

Base Plan S

The results of ea
base plan audit i
using color coded
weighted scoring
were combined an
overall audit score
Individual category
for each audit item a
subsequent pages. Y
IT expense is shown a
has been converted in
monthly expense base
audit score. This helps
playing field when comp

Your customised Audit Report

In the following pages you'll find your customised Audit Report. It contains all of the information gathered from your IT, Cyber & Communications environment into one easy-to-read document.

Upon reading, you will have a much better understanding of your current Technology and what you're spending now.

Based on our technical analysis of your IT environment, we have customised a selection of audit items spread across one or more main areas of technology.

Each of these areas will give you important insight into the strengths and weaknesses of your IT plan.

Your Audit Score

Using the results of your audit, we calculated your overall score. The higher your audit score, the greater efficiency at which you are spending on technology.

Our goal is to drive your audit score as close to 100 as possible.

The comparative analysis page allows you to easily compare your baseline plan with other plans presented in this document to see qualitative, quantitative and financial results.

How to Read your Report

Each audit item has been colour coded to make it easy to visualise your results.

    I.   **Red indicates an audit item that requires immediate attention**
    II.   **Yellow indicates an audit item that needs improvement**
    III. **Green indicates an audit item that is satisfactory**
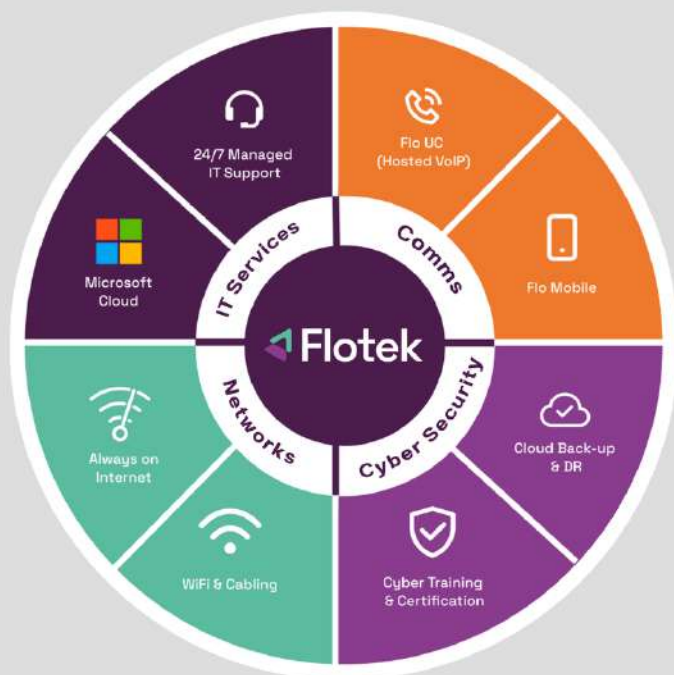
In addition to a summary page, you will find dedicated pages with colour coded summary statements for each individual audit item. Any audit item that isn't satisfactory is described in greater detail and its relative importance is explained in a single statement.

Who is **Flotek**

As a growing technology company based in Cardiff, Flotek strives to ensure customers are embracing the opportunities and efficiencies brought by the latest and greatest technology.

With regional sales and support locations across the UK, our ambitious growth is focused around our crucial values and fundamental rules, with every product and service delivered with expertise, passion and heart.

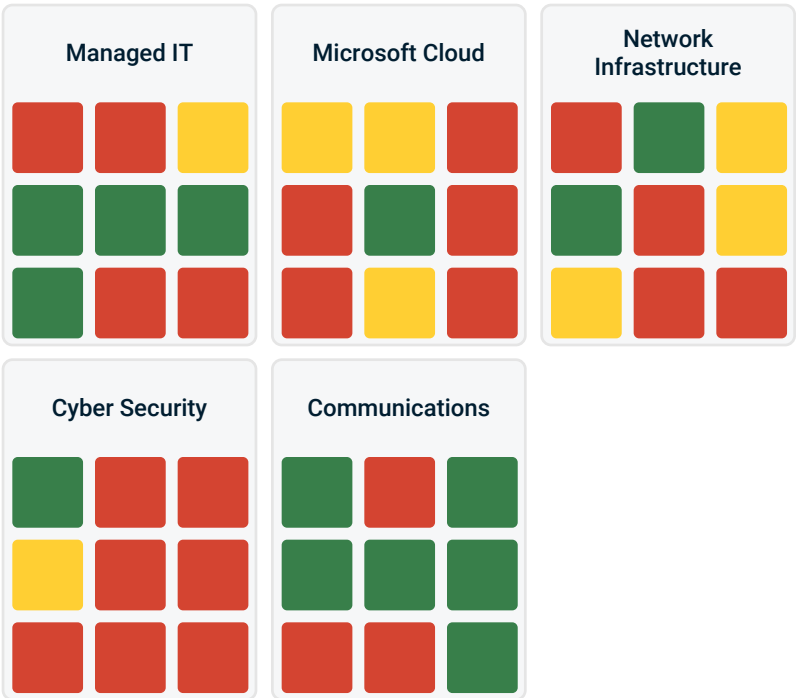**Discover why Flotek is the smarter Cloud partner for your business.**

St. Asaph

Nuneaton

Swansea

Cardiff

Bridgend

Basingstoke

Plymouth

24/7 Managed IT Support

Flo UC (Hosted VoIP)

IT Services

Comms

Microsoft Cloud

Flo Mobile

Flotek

Networks

Cyber Security

Always on Internet

Cloud Back-up & DR

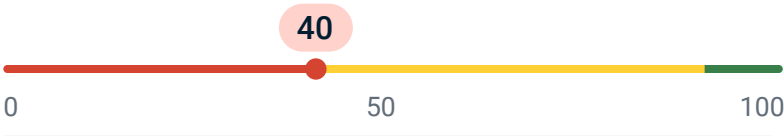WiFi & Cabling

Cyber Training & Certification

Bringing Technology Together.

At last, an IT & Comms service provider taking SMEs to the Cloud with confidence, clarity and clout.

Thanks to our range of innovative, cost-effective, tried & tested solutions that ensure your tech, team and data are always on, always secure and always together, wherever they are.

Audit Score

40

0   50   100

Managed IT

Microsoft Cloud

Network Infrastructure

### Cyber Security

Communications

Base Plan Summary

The results of each category of your base plan audit is summarized here using color coded boxes. Utilizing a weighted scoring system, the results were combined and averaged into an overall audit score.

Individual category scores and details for each audit item are shown in subsequent pages. Your base monthly IT expense is shown as a range and has been converted into an effective IT monthly expense based upon your audit score. This helps to level the playing field when comparing plans.

■ Requires Immediate Attention   ■ Needs Improvement   ■ Satisfactory

Flotek group

Managed IT

50

0   50   100
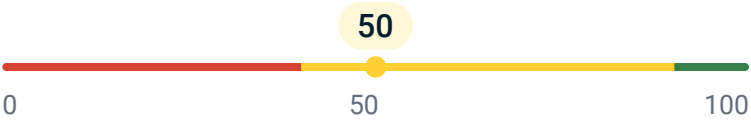
Managed IT Support & Services is the most efficient way to minimize reactive support and proactively manage your infrastructure. In exchange for a fixed monthly fee, outsourcing support helps improve operations while reducing your overall expense. This detailed analysis page represents an overview of the state of your Base Plan Managed Support & Services. Each audit item is summarized and colour coded for easy identification and the results for this section are reflected in the Managed Support & Services audit score.

| Workstation Condition	Server Evaluation	Backup & Disaster Recovery
The workstations are over 5 years old, out of warranty or running a non-supported operating system	Old and On-site servers	Backups exist but not routinely tested or only partial coverage (e.g. missing cloud data or endpoints).
Windows & Application	**Single Sign On (SSO)**	**Proactive Maintenance &**
Automatic patching configured and monitored; updates tested and deployed within standard timelines.	Centralised identity platform in place (e.g. Azure AD, Okta); users authenticate via SSO with MFA.	Proactive tools in place (RMM); alerts reviewed and acted on; preventative maintenance scheduled.
Help Desk Support	**Business Continuity**	**IT Strategy Reviews**
Remote Help Desk Support is included for all supported endpoints and services.	No Business Continuity exists to run the business in the case of disaster	No IT strategy; decisions made ad hoc; no visibility of future tech requirements or risks.

Microsoft Cloud

27

| 0 | 50 | 100 |
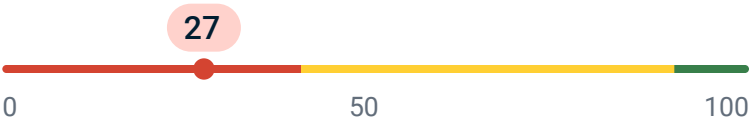
The Microsoft Cloud is an open cloud platform made up of products and solutions that empower organizations to thrive in a changing world. It offers a variety of tools to help businesses manage challenges and meet their goals,drive value faster, and build for the future. It also helps protect and defend your business with security, compliance, identity, and management solutions that work across all your platforms, clouds, and apps.

Admin Role Overlap
Some users have admin privileges without clear justification.

Multi-Factor Authentication
MFA is partially deployed or only used for admin accounts.

Email Security Measures
No effective email filtering, posing a high phishing and malware risk.

Baseline Security
No consistent monitoring of security settings or risk indicators.

Monitoring & Threat
24/7 monitoring tools are in place to detect threats early.

Cloud Backup & Recovery
No cloud backups; recovery in the event of data loss is not guaranteed.

File Storage & Access
File storage is poorly managed or not aligned to Microsoft best practice.

Microsoft Licensing
Some licences are not aligned to user roles; inefficiencies exist.

End User Training Program
No training provided, leading to under-utilisation and increased user error.

Summary   Detail   Business Impact

Flotek group

Network Infrastructure

38

0   50   100
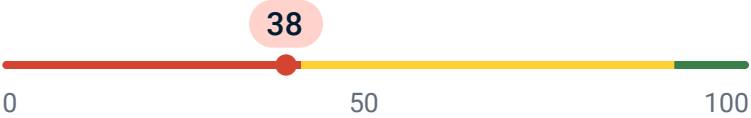
Network infrastructure is the foundation upon which all of your technology rests. Just like with a house, it's extremely important to verify its integrity before you begin to build on top of it. Poor initial design decisions can lead to downtime, lost sales and ultimately drive up your total cost of ownership. This detailed analysis page represents an overview of the state of your Base Plan Infrastructure. Each audit item is summarized and colour coded for easy identification and the results for this section are reflected in the Infrastructure audit score.

Cabling	Managed Network Router	Switching
Using Cat5 or old cabling	Business-grade router in place, secured and actively managed.	Unmanaged switches or 100Mb ports limiting performance.

Wireless Networks	Network Isolation	Guest Wireless Services
Wi-Fi is strong, secure, and accessible throughout the premises.	No network segmentation, increasing risk of cross-traffic issues or breaches.	Has a password protected separate wireless network for guests, not compliant due to no client portal in place

Remote Accessibility	Content Filtering	Secure Print Management
VPN in use but no MFA	No web filtering; users can access inappropriate or risky sites.	No security measures on network printers.

Cyber Security

16

0   50   100

Cyberattack risk refers to the potential threats and vulnerabilities that organizations or individuals face from malicious digital actions. These actions aim to disrupt, damage, or gain unauthorized access to computer systems, networks, or data. Cyberattack risks can include various forms of attacks and is why managing cyberattack risks involves implementing various security measures to detect and mitigate potential threats.

Device Security	Endpoint Encryption	Password Policy &
Devices are protected by MDR (Managed Detection & Response) and ransomware protection.	No encryption; data on lost/stolen devices is at risk.	No password policy; users manage passwords independently; passwords reused or shared.

Firewall Security	Security Awareness Training	Cyber Essentials
Basic business-grade firewall in place.	There is no baseline security phishing test nor an ongoing security awareness training program in place.	Not certified and little/no alignment with Cyber Essentials standards.

Incident Response Plan	Dark Web Monitoring	Domain Records
No incident response plan.	No monitoring or awareness of credential leaks; no breach response strategy.	No records or misconfigured; domain vulnerable to spoofing and impersonation.

Summary   Detail   Business Impact

Flotek group

Communications

66

0   50   100

Telecommunications is one of the fastest evolving areas of technology. Traditionally viewed as a separate cost centre, the proliferation of voice over IP (VoIP) solutions has helped many businesses save more money while greatly improving upon their business continuity. This detailed analysis page represents an overview of the state of your Base Plan Telecommunications. Each audit item is summarized and colour coded for easy identification and the results for this section are reflected in the communications audit score.

Primary Internet Service	WAN Redundancy / Failover	Phone System Assessment
Reliable, high-speed connection that meets current business needs.	No backup internet connection; single point of failure.	Modern, cloud-hosted VoIP system with flexibility and scalability.

Handset Security	VoIP Quality of Service	Call Recording
Handsets up-to-date and supported with regular firmware updates.	QoS is enabled and ensures clear, uninterrupted calls.	All calls are recorded and securely stored where required.

Call Analytics	CRM Integration	Remote Working Evaluation
No monitoring or visibility of call data.	No CRM integration.	All users can securely work remotely with full access to systems.

Summary   Detail   Business Impact

Call Analytics   Communications

Problem State: No monitoring or visibility of call data.

Impact: Lack of call reporting means missed opportunities to improve response times, team performance, or sales effectiveness.

CRM Integration   Communications

Problem State: No CRM integration.

Impact: No integration means lost productivity and missed context when dealing with clients, leading to inefficiencies and errors.

WAN Redundancy / Failover   Communications

Problem State: No backup internet connection; single point of failure.

Impact: No internet backup means a single outage can stop operations, causing missed calls, delayed work, and client dissatisfaction.

Flotek group

Cyber Essentials   Cyber Security

Problem State: Not certified and little/no alignment with Cyber Essentials standards.

Impact: Non-compliance may affect insurance, tenders, and your ability to work with government or regulated industries.

Dark Web Monitoring   Cyber Security

Problem State: No monitoring or awareness of credential leaks; no breach response strategy.

Impact: If leaked data isn't identified and addressed, criminals may exploit it without your knowledge, leading to account hijacks or fraud.

Domain Records   Cyber Security

Problem State: No records or misconfigured; domain vulnerable to spoofing and impersonation.

Impact: Misconfigured records can lead to spoofed emails, spam blacklisting, and loss of client trust — and you may not even know it's happening.

Endpoint Encryption   Cyber Security

Problem State: No encryption; data on lost/stolen devices is at risk.

Impact: Unencrypted devices risk exposing all business data if lost or stolen, breaching GDPR and other data protection laws.

Firewall Security   Cyber Security

Problem State: Basic business-grade firewall in place.

Impact: A weak firewall is like leaving the front door open to cyber criminals — it invites attack and increases the likelihood of a serious incident.

Incident Response Plan   Cyber Security

Problem State: No incident response plan.

Impact: Without a response plan, your business will be caught off guard during an attack, leading to longer downtimes and higher recovery costs.

Password Policy & Management | Cyber Security

Problem State: No password policy; users manage passwords independently; passwords reused or shared.

Impact: Weak or reused passwords are a leading cause of breaches, often exploited by attackers to access entire networks.

Summary

Detail

Business Impact

Backup & Disaster Recovery | Managed IT

Problem State: Backups exist but not routinely tested or only partial coverage (e.g. missing cloud data or endpoints).

Impact: Without reliable backups, your business could suffer critical data loss in the event of a cyberattack or accidental deletion, delaying recovery and increasing costs. Backups have not been tested

Server Evaluation | Managed IT

Problem State: Old and On-site servers

Impact: 2016 Server, running datto, approx 1TB Storage allowance, using 500GB - needs to go to cloud

Workstation Condition Assessment | Managed IT

Problem State: The workstations are over 5 years old, out of warranty or running a non-supported operating system

Impact: Multiple machines, mainly TM's are end of life

Baseline Plan

Flotek group

Admin Role Overlap — Microsoft Cloud

Problem State: Some users have admin privileges without clear justification.

Impact: Weak admin account control can lead to full system compromise if credentials are stolen, resulting in potential data loss, downtime, and financial penalties. No 2FA on Cisco VPN

Baseline Security Management — Microsoft Cloud

Problem State: No consistent monitoring of security settings or risk indicators.

Impact: Lack of ongoing security checks means threats can go undetected, exposing the business to avoidable vulnerabilities and compliance issues.

Email Security Measures — Microsoft Cloud

Problem State: No effective email filtering, posing a high phishing and malware risk.

Impact: Inadequate email protection makes the business a prime target for phishing attacks, ransomware, and spam, which can lead to data breaches and reputational damage.

End User Training Program — Microsoft Cloud

Problem State: No training provided, leading to under-utilisation and increased user error.

Impact: Without user training, staff may misuse tools or fall for common scams, increasing both security risk and IT support workload.

File Storage & Access Management — Microsoft Cloud

Problem State: File storage is poorly managed or not aligned to Microsoft best practice.

Impact: Poor file management can lead to data sprawl, version confusion, and unauthorised access, hurting collaboration and compliance. Storage is on sharepoint for TM's & Server for Head office staff

Microsoft Licensing Compliance — Microsoft Cloud

Problem State: Some licences are not aligned to user roles; inefficiencies exist.

Impact: Improper licensing may lead to unnecessary costs, reduced system capabilities, or legal penalties for non-compliance with Microsoft terms. Microsoft Basic x 10 and Standard x 24

Summary | Detail | Business Impact

Multi-Factor Authentication   Microsoft Cloud

Problem State: MFA is partially deployed or only used for admin accounts.

Impact: Without MFA, accounts are far more vulnerable to password theft, increasing the risk of unauthorised access and cyberattacks. No 2FA in place.

Cabling — Network Infrastructure

Problem State: Using Cat5 or old cabling

Impact: Outdated or messy cabling can cause poor connectivity, slower speeds, and safety issues, impacting daily productivity.

Content Filtering — Network Infrastructure

Problem State: No web filtering; users can access inappropriate or risky sites.

Impact: Without content filtering, employees may access harmful or inappropriate websites, risking malware infection and legal concerns.

Guest Wireless Services — Network Infrastructure

Problem State: Has a password protected separate wireless network for guests, not compliant due to no client portal in place

Impact: Patchy or slow Wi-Fi reduces productivity and can frustrate staff and clients, especially in collaborative environments.

Network Isolation — Network Infrastructure

Problem State: No network segmentation, increasing risk of cross-traffic issues or breaches.

Impact: Lack of traffic segregation increases the risk of data leaks and performance issues, especially with voice or guest traffic.

Remote Accessibility — Network Infrastructure

Problem State: VPN in use but no MFA

Impact: Insecure remote access exposes sensitive business systems to external threats, jeopardising data and client trust.

Secure Print Management — Network Infrastructure

Problem State: No security measures on network printers.

Impact: Insecure print setups can lead to sensitive information being accessed or printed without authorisation, breaching confidentiality.

Switching	Network Infrastructure

🟨 **Problem State:** Unmanaged switches or 100Mb ports limiting performance.

Impact: Low-speed or unmanaged switches limit efficiency and network growth, affecting cloud services, VoIP, and file access.

Financial Summary:

We've detailed all your **current costs** <u>vs</u> **our proposed** solution so you can compare like for like.

Current Monthly Costs (Averaged)	
Managed IT Support, Backup & Non Security Licenses (30 Users)	£1700.00
Cyber Security Licensing	£300.00
Microsoft Licensing	£384.00
Communications	£643.00
Internet (SoGea No Backup)	£48.00
Managed Print	£185.00
Total	**£3260.00**

Proposed Monthly Costs (Averaged)	
Managed IT Support & Non Security Licenses (30 Users)	£1200.00
Cyber Security Licensing	£210.00
Microsoft Licensing	£309.00
Communications	£360.00
Internet (FTTP With 5G Backup)	£70.00
Managed Print	£130.00
Total	**£2289.00**

Proposed Savings	
Monthly	£971.00
Annual	£11,652.00
Over 5 Years	£58,260.00

Flotek Business Recommendations / Comments:

Due to requirements for broadband availability, I would recommend a dedicated line and SIEM Security with a SonicWALL.

Get Your Tech Fast, Next-Day Delivery!

Need laptops, desktops, firewalls, or WiFi access points quickly?

Meet Lewis

We've got you covered! Our next-day delivery service brings thousands of items straight to your team. Just contact our sales team and your tech is on its way—saving you the hassle of searching and the cost of waiting.

We don't just deliver fast; we ensure reliability. Every product comes pre-vetted, ready to integrate seamlessly into your workspace. Trust in our expertise to provide not only the technology you need but the confidence that it all works perfectly. Simplify your tech procurement and focus on what truly matters to your business.

Reach out today for swift, dependable tech solutions!

Email: Sales@Flotek.io

Laptops & Desktops

High Secure Firewalls

HP Enterprise Server & Storage

WiFi and Networking

Data & Fibre Installation

Customer Acceptance of Flotek Group Limited's standard terms and conditions:

I/We confirm that I/We have read and understood the terms and conditions as set out by Flotek Group Limited and confirm that the above information is correct.

I confirm that I'm authorised to sign this order and direct debit mandate and that all company details provided are accurate.

By signing this document, you agree to Flotek Group Limited's terms and conditions provided or alternatively found at https://Flotek.io/terms-and-conditions

If your order is related to any Microsoft Cloud Licensing, you are agreeing to the Microsoft End User Licensing agreement found at:
https://aka.ms/customeragreement

Demo UK Limited:

Name: Demoro Bobero

Date:

Getting started, what's next?

Once we receive your digitally signed order, we'll assign your order to a project manager who will be your point of contact from signed order to completion.

We'll be here every step of the way and ensure 100% customer satisfaction.

Flotek group

T: 0292150 8000

E: Hello@Flotek.io

W: www.Flotek.io

Unit 4
Bocam Park
Pencoed
Bridgend
CF35 5LJ

Flotek Group Limited is Registered in England & Wales.

Company Number: 13882299
VAT Registration Number: GB 4060 18239

Read our Terms & Conditions

Baseline Plan

Initial Assessment Summary

Audit Score

0   50   80   100

Managed IT
Microsoft Cloud
Network Infrastructure

Cyber Security
Communications

Base Plan

The results of ea
base plan audit is
using color coded
weighted scoring
were combined an
overall audit score.
Individual category
for each audit item a
subsequent pages. Y
IT expense is shown a
has been converted in
monthly expense base
audit score. This helps
playing field when comp