Re-solution

Security Audit

20/06/2023

Audit compiled for Acme Inc
Assessor Name Sean Draper

PREPARED FOR:
Joe Bloggs
Director

COMPANY DETAILS:
123 Street, London W1W 5PF
www.acme.com

CONTACT DETAILS:
joe.bloggs@acme.com
0203 880 8369

About us

Networks, Security, Cloud.

We're proud to be a Cisco only partner providing dedicated vendor expertise, staying at the forefront of the technology solutions we design, implement and support. Operating on a security first model with each and every one of our customers our reputation and credibility means everything to us.

Table of Contents

Objectives

What outcome do you want this audit to provide Acme Inc?
ACME is looking for a 3rd Party to conduct a high level infrastructure assessment. This audit should include as much of the customer infrastructure that is available throughout the assessment. There maybe areas that cannot be covered due to lack of customer documentation/awareness.

What is Acme Inc's view on technology as a business enabler?
We do see value in technology and how it can interact with our processes and people however this always comes down to a cost vs value.

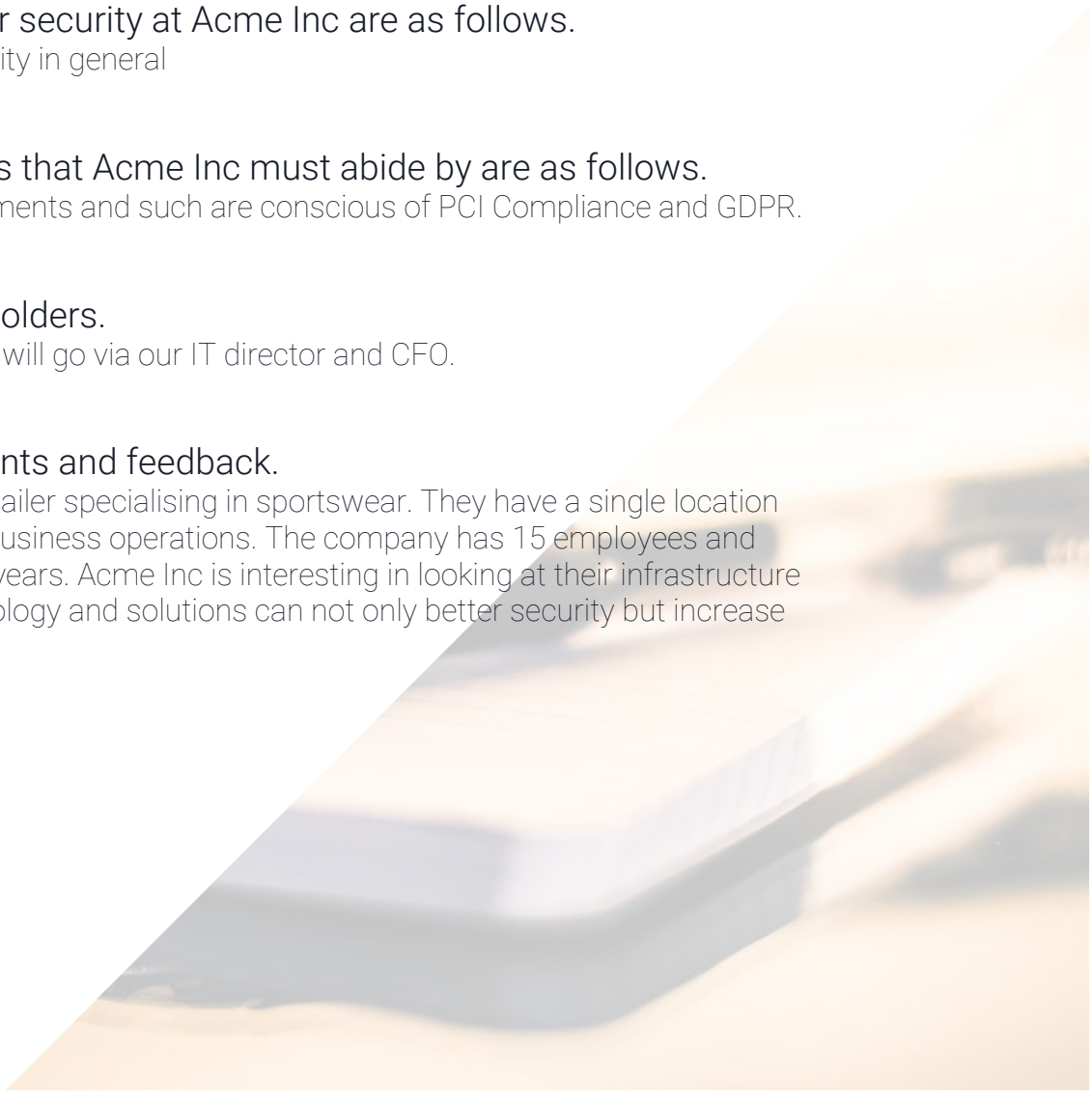
In the past 12 months has there been any security incidents?
No

The weakest links for security at Acme Inc are as follows.
User education on security in general

Laws and regulations that Acme Inc must abide by are as follows.
We take credit card payments and such are conscious of PCI Compliance and GDPR.

Acme Inc key stakeholders.
All technology decisions will go via our IT director and CFO.

Sean Draper comments and feedback.
Acme Inc is an online retailer specialising in sportswear. They have a single location where they conduct all business operations. The company has 15 employees and has been trading for 20 years. Acme Inc is interesting in looking at their infrastructure to see how better technology and solutions can not only better security but increase productivity.



Network Devices

Does Acme Inc have any existing documentation including diagrams?

No

How many switches are currently on the network?

8 x Cisco SMB200 Switches, 1 x ISP router

All of the devices are individually managed and patched. Having had a look at the end of life report from the vendor it appears that these switches are showing as end of life with no further software updates available for this platform. Acme Inc should look to alternatives to replace these devices in accordance to vendor guidelines.

How many Wireless Access Points are currently on the network?

12 x Ubiquity WAPs

Management of the Wireless platform can be cumbersome with limited centralised management of the entire wireless network. These WAPs require a software update to bring them up to the latest stable release per vendor recommendations. Joe has advised there are 2 SSIDs, 1 internal & 1 guest both of these SSIDs use pre shared keys to authenticate.

Do you have a firewall or something similar?

No dedicated firewall in place - we rely on our ISP router to perform this functionality.
Unsure of Model

The ISP router is currently doing all security and firewall features for ACME inc's network. This is usually fine for a home network but not ideal for a business that holds customer and payment information.

Are you currently using CCTV?

Yes we currrently have CCTV cameras, utilising a onsite DVR System. This is SWANN system

Acme currently has an on-site DVR based system. Acme is not looking to replace this system as it is deemed fit for purpose against the requirements.

Network Design

Do you know how your network is currently designed?
Yes

How are the sites connected, WAN/VPN/P2P/HSCN/WWW How is traffic to the WAN/WWW protected?
We have a single site.

How many VLANs are in use?
everything is on the same IP network space

How are the VLANs advertised and controlled? Where is the VLAN database located?
not sure

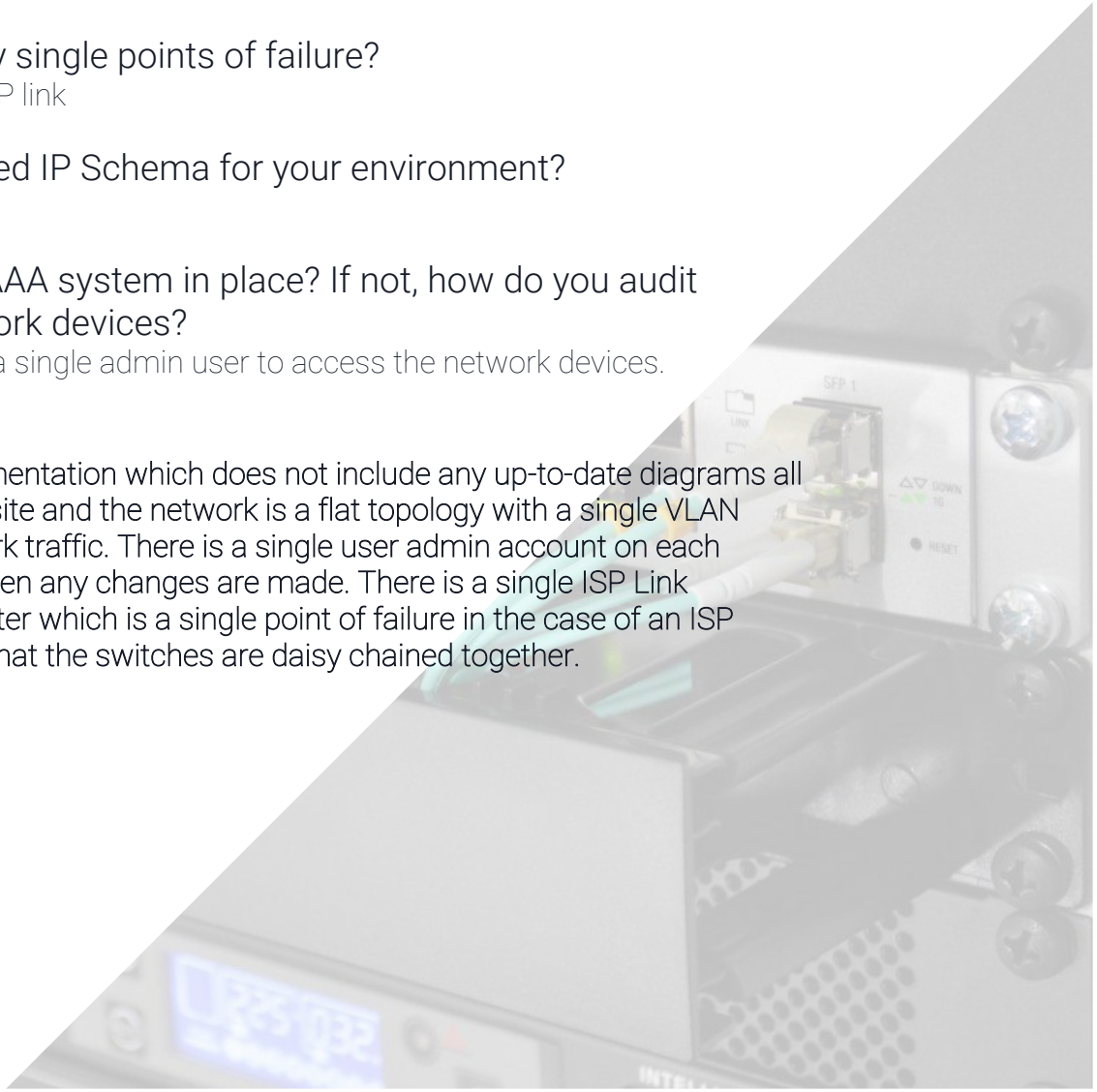
What L3 protocol is in use?
not sure

Are you aware of any single points of failure?
We only have a single ISP link

Do you have a detailed IP Schema for your environment?
No

Is there an existing AAA system in place? If not, how do you audit access to your network devices?
No - we do not - there's a single admin user to access the network devices.

Assessor Feedback
Acme has limited documentation which does not include any up-to-date diagrams all users reside at a single site and the network is a flat topology with a single VLAN being used for all network traffic. There is a single user admin account on each switch which is used when any changes are made. There is a single ISP Link connected to an ISP router which is a single point of failure in the case of an ISP outage. It's been noted that the switches are daisy chained together.



Licensing & Patching

Are systems hardware, firmware and software licensed in accordance with the publisher's recommendations?
Yes as far as we are aware.

Is firmware and software patched regularly in accordance with the publisher's recommendations?
We do this when we can, but believe that this could be a bigger issue

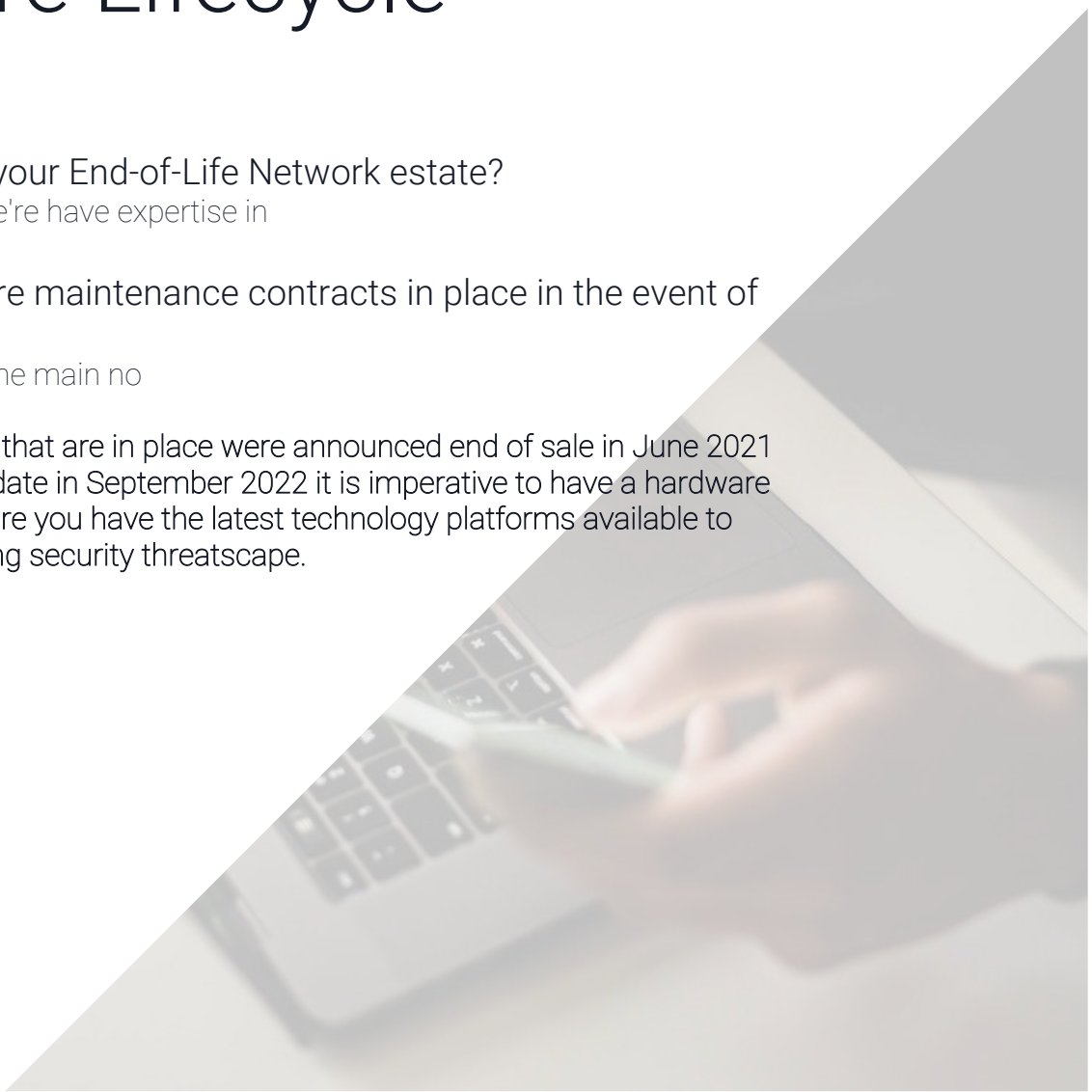
Looking through the existing firmware versions the as is installed patches are out of date and should be updated to the recommended release version 2.1.4.2.1.

Hardware Lifecycle

How do you assess your End-of-Life Network estate?
This is not something we're have expertise in

Do you have hardware maintenance contracts in place in the event of failures?
Where possible - but in the main no

The Cisco 200 Switches that are in place were announced end of sale in June 2021 with the last security update in September 2022 it is imperative to have a hardware lifecycle process to ensure you have the latest technology platforms available to combat the ever changing security threatscape.



Applications

What applications are used on a day-to-day basis and considered critical by the business?
o365, One drive and internet

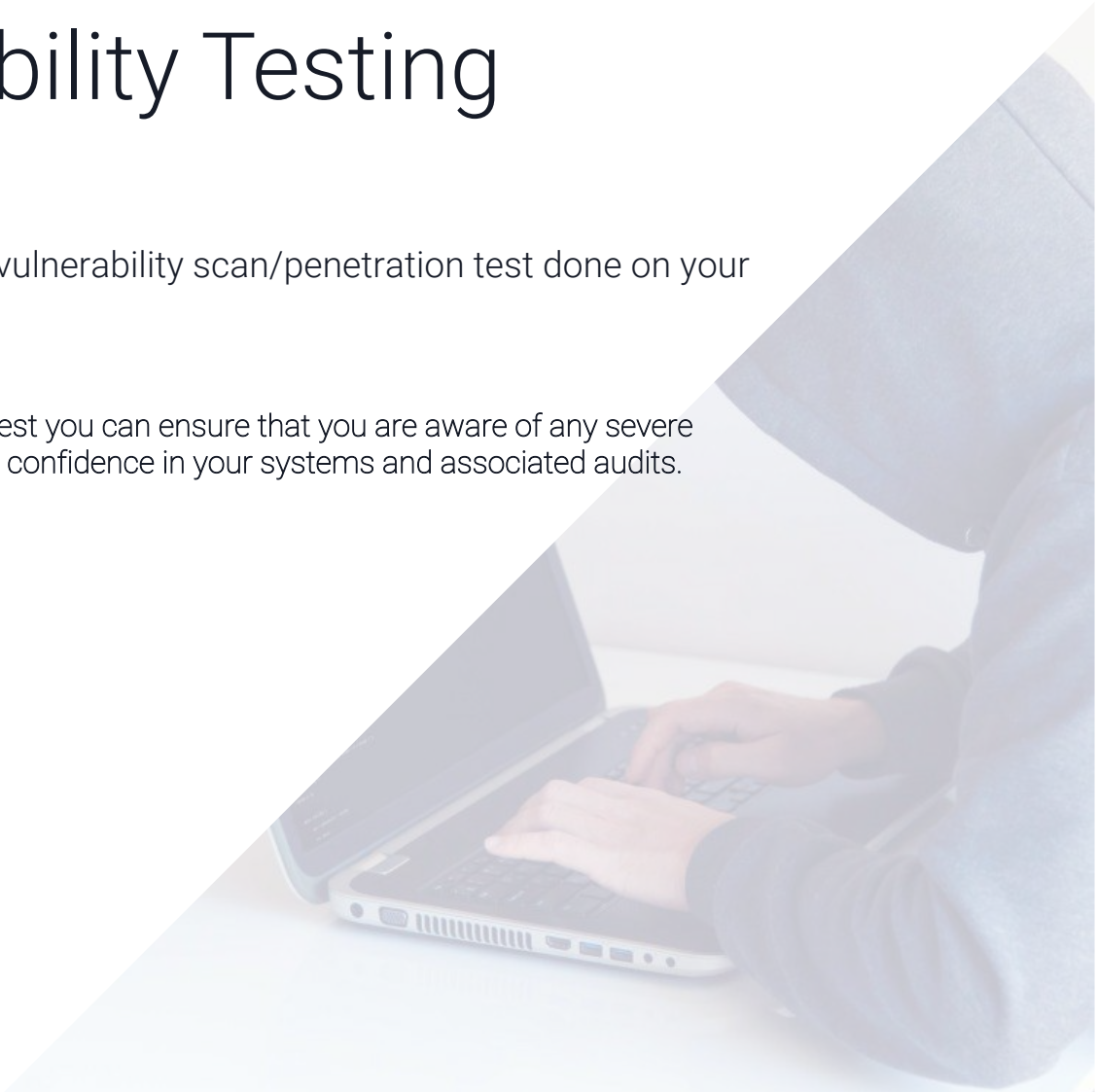
Are your applications secured by 2FA/MFA if so, what are you using?
No

The majority of application access is cloud driven with the use of O365 applications. The lack of MFA in todays technology needs to be addressed.

Vulnerability Testing

Have you ever had a vulnerability scan/penetration test done on your network?
No

By having a penetration test you can ensure that you are aware of any severe vulnerabilities to give you confidence in your systems and associated audits.



Monitoring & Reporting

Do you have monitoring tools on your network? What are they? What do they monitor? Are the logs stored remotely?

No there are no monitoring tools

Are information security incidents investigated to establish their cause and impacts with a view to avoiding similar events?

Yes - however we do not believe that we've ever had a security incident

Are all breaches of the Security Policy and other information security incidents or suspected weaknesses reported and recorded?

Yes - however we do not believe that we've ever had a security incident

Comments and feedback.

It is clear that without monitoring tools the company is not aware of the status of their infrastructure particularly on the network. The more visibility that the customer has over their network the quicker they can remediate problems as and when they occur.

Virtual Private Network

Do you have any remote access VPN for remote workers?
No

Assessor Comments.
Acme does not have a requirement for employees to work remotely.

Managed Endpoints & Users

How do you manage all endpoints? Do you have an MDM solution? Or are all assets managed individually?
We do not have a centralised management of coporate assets.

What do you use for Antivirus / Anti Malware across your Endpoints?
Microsoft Defender

Do you authenticate endpoints before they connect to the network?
No

What types of devices are allowed to authenticate?
Only company devices are allowed to connect.

How do you manage all users? Do you have Active Directory or are users managed individually?
All users have an Office 365 account

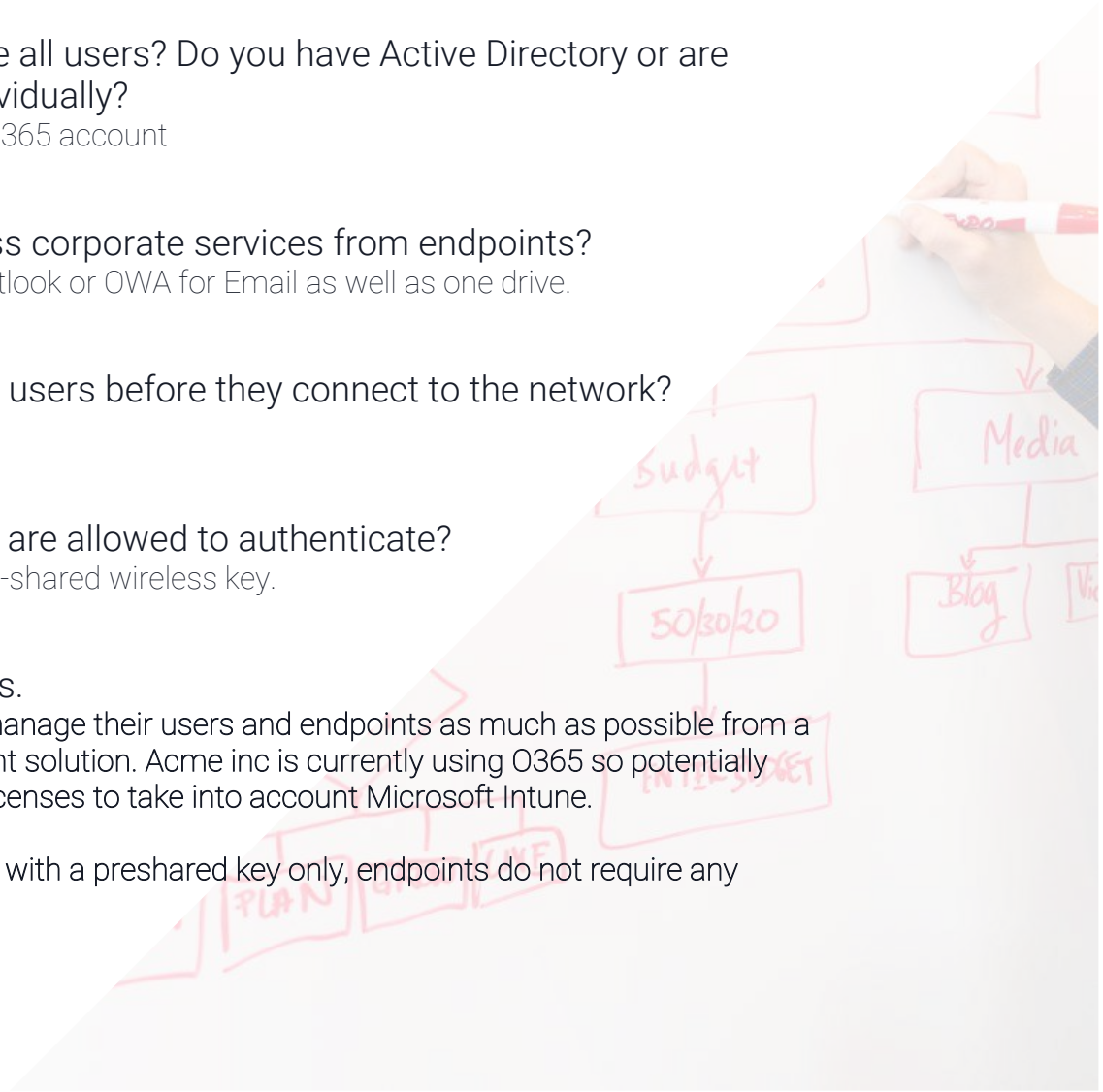
How do users access corporate services from endpoints?
Users can either use outlook or OWA for Email as well as one drive.

Do you authenticate users before they connect to the network?
No

What types of users are allowed to authenticate?
Anyone that has the pre-shared wireless key.

Assessor Comments.
The customer should manage their users and endpoints as much as possible from a centralised management solution. Acme inc is currently using O365 so potentially investigate upgrading licenses to take into account Microsoft Intune.

WiFi users authenticate with a preshared key only, endpoints do not require any authentication.

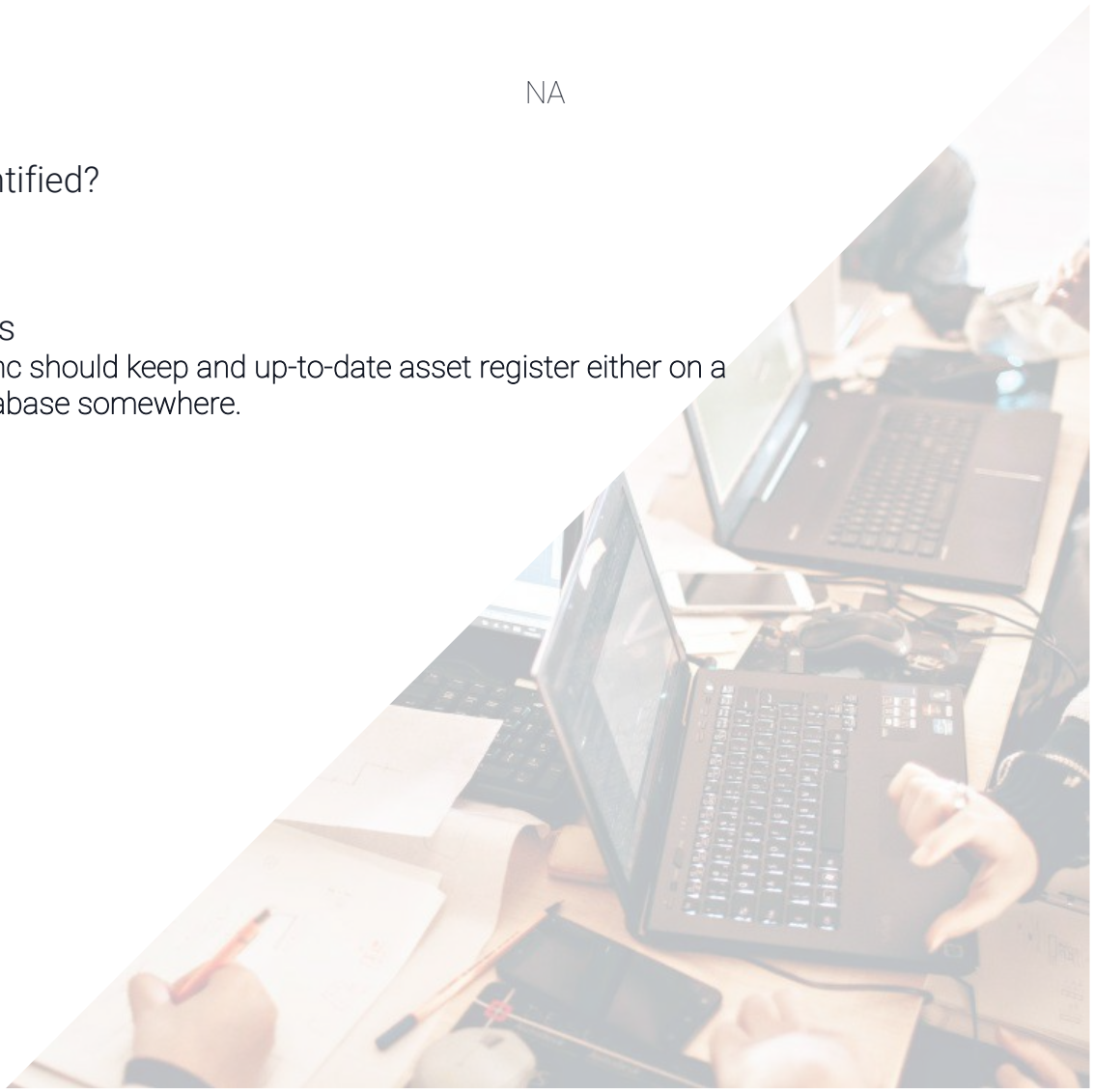


Acme Inc Assets

Do you have an up-to-date asset register?	No
Number of Corporate Desktops/Laptops?	10
Number of Phones?	4
Number of Printers?	1
Number of VC systems?	1
Number of Corporate Mobile Devices?	2
Number of UPS?	0
Number of Servers?	
Other?	NA

How are assets identified?
Serial Number

Assessor Comments
Where possible Acme Inc should keep and up-to-date asset register either on a spreadsheet or in a database somewhere.



Guest & BYOD Services

Do you offer Guest services? (Wired/Wireless or Both)
Yes - Wireless

How do you restrict access to sensitive data?
permissions are set on our one drive account

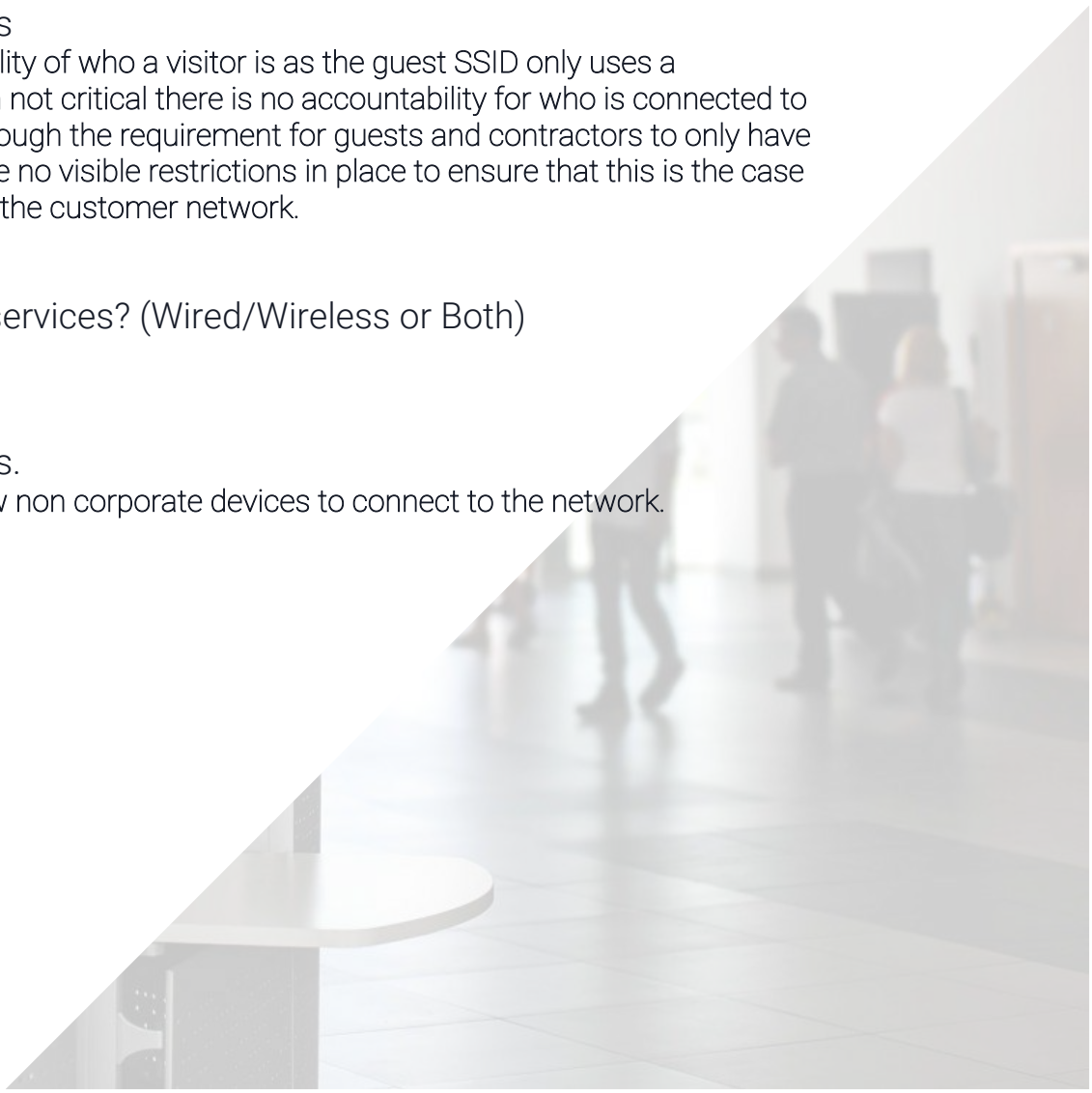
What access level should guest users have?
internet access only

What access level should external contractors have?
internet access only

Assessor Comments
There is little to no visibility of who a visitor is as the guest SSID only uses a preshared key. Although not critical there is no accountability for who is connected to the guest network. Although the requirement for guests and contractors to only have internet access there are no visible restrictions in place to ensure that this is the case due to the flat nature of the customer network.

Do you offer BYOD services? (Wired/Wireless or Both)
No

Assessor Comments.
Acme Inc does not allow non corporate devices to connect to the network.



Support & Change Management

Do you support your own infrastructure?
Yes

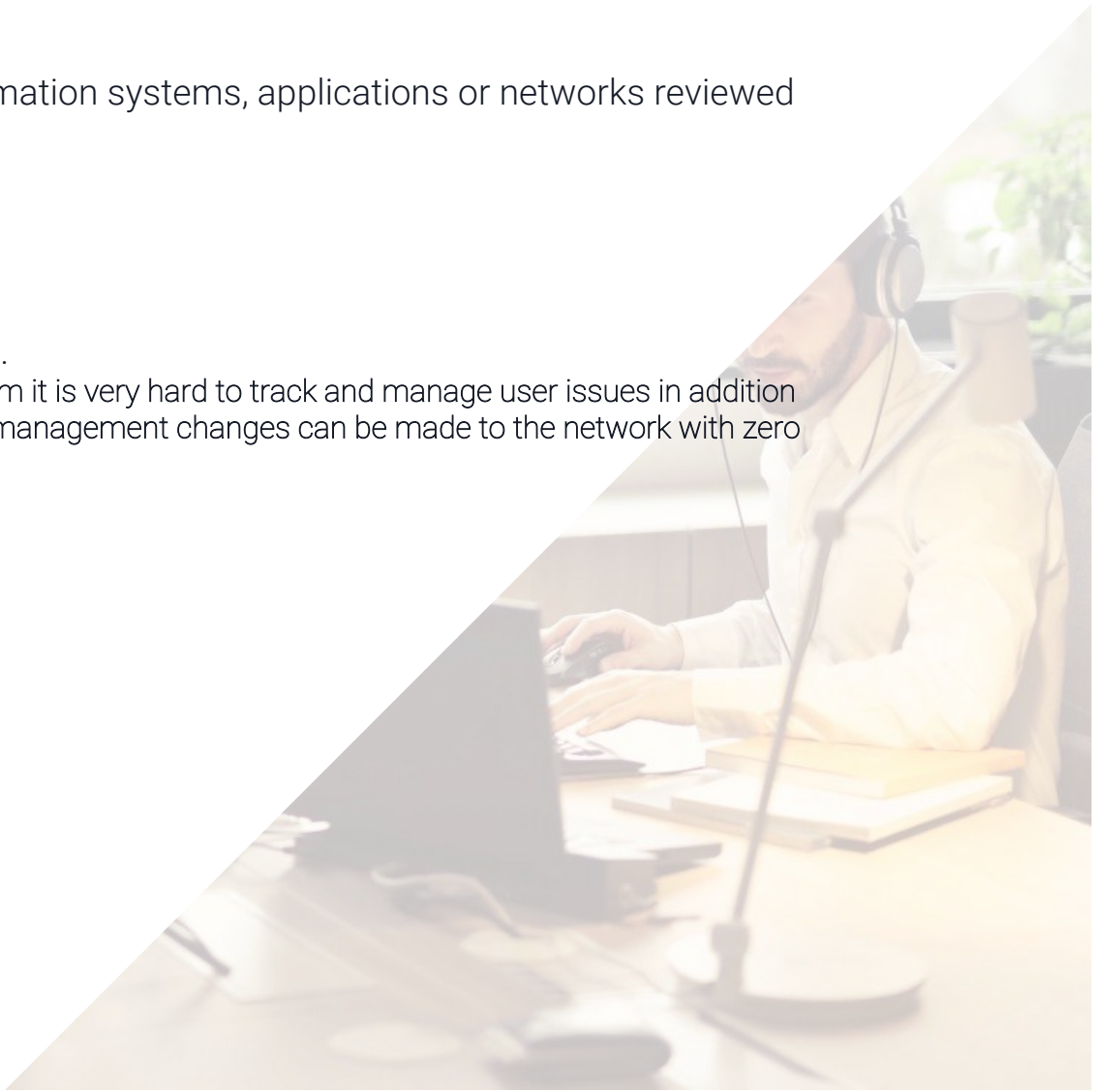
Are support staff trained for any new security technology, process, and policy?
We train our staff where we can on the setup of infrastructure technology

How do support staff troubleshoot support calls?
Usually with the user and/or vendor as needed.

Is there a ticketing system?
No - e-mails only

Are changes to information systems, applications or networks reviewed and approved?
No

Assessor Comments.
Without a ticketing system it is very hard to track and manage user issues in addition without defined change management changes can be made to the network with zero accountability.



Disaster Recovery & Backups

Do you have a business continuity plan?
No

How often do you review this?

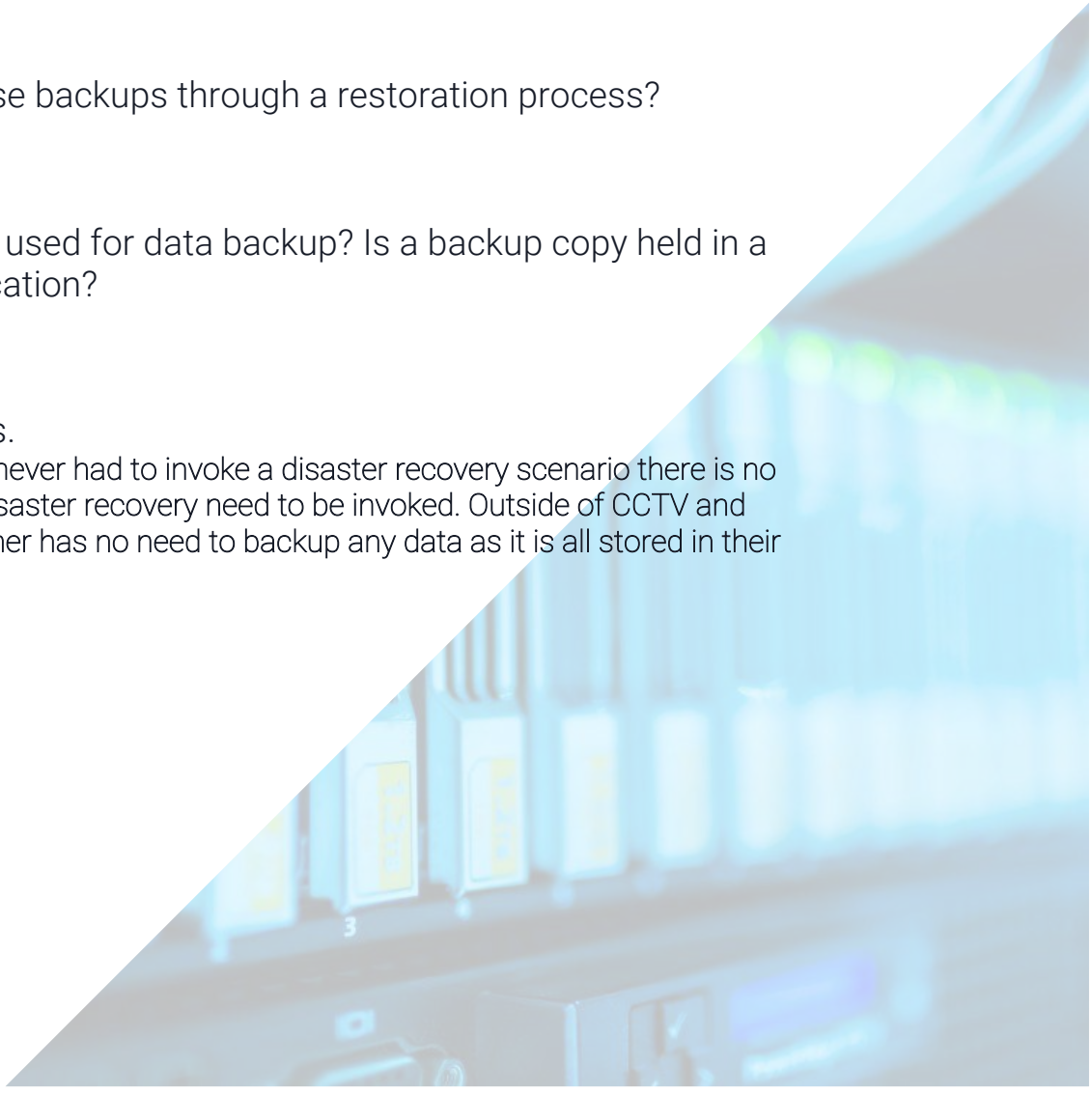
What do you do in a disaster recover scenario?
we've never had to invoke a disaster recovery scenario so not sure.

Is data stored on the business premises backed up regularly and restores tested at appropriate intervals (at least weekly)?
No all of this is in Microsoft Cloud

Do you ever test these backups through a restoration process?
N/A

Is an offsite location used for data backup? Is a backup copy held in a different physical location?
MS Cloud

Assessor Comments.
Although Acme Inc has never had to invoke a disaster recovery scenario there is no plan in place should a disaster recovery need to be invoked. Outside of CCTV and local devices the customer has no need to backup any data as it is all stored in their Microsoft tenancy.



Risk & Remediation Table

Number	Section	Issue/Risk	Description	Severity	Impact	Recommended Mitigation
6	Switches	EOL	Hardware is end of life and not subject to security updates	1	Switches have potential security vulnerabilities that Acme Inc is not aware of.	Update switches to the latest software version (if available) whilst considering upgrade options.
11	Wireless	Outdated software on WAPs	Outdated software on WAPs	2	Potential security flaws and potentially reduced features/performance.	Update to the latest recommended release.
12	Wireless	Wireless Authentication	Preshared keys are being used on both internal and guest SSIDs	3	If preshared keys are not changed often enough then anyone that has previously connected will still be able to access the network. This effectively means that a user could create a bottleneck in the network without your knowledge.	Change the pre shared key on a regular basis with the guest to be changed on a weekly basis and the internal on an ad-hoc basis based on new starters / leavers etc.

16	Firewalls	No dedicated corporate firewall in place.	No dedicated corporate firewall in place.	2	No visibility from the ISP router of any user connected traffic or what users may be accessing.	Recommendation to trial an enterprise level firewall in a proof of concept environment to understand the benefits.
21	CCTV	DVR Failure / Theft	Data is all stored locally on DVR system	5	If the system fails or is stolen then there is no backup of footage.	Look into either backing up the footage to a cloud based provider or utilise a cloud based CCTV network dependant on business requirements.
56	AAA	Flat VLAN topology	All users are on a single VLAN/IP Subnet space	3	Any user that has a potential problem on their machine has the impact to compromise everyone else.	Split the network topology so that VLANs are segmented where possible.
57	AAA	ISP/Firewall Single point of failure	ISP/Firewall Single point of failure	2	If the ISP circuit or device fails then the entire business will be affected.	Either have a secondary link or alternatively look into a 4/5G failover service.
58	AAA	Single user admin account	Single user admin account	2	Anyone with the admin password can make changes	Have separate usernames for users that are

					with no accountability.	allowed access/to make changes.
59	AAA	Single user admin account	Single user admin account	1	There is only a single account if a username/password is lost then the device will need to be factory reset resulting in loss of service.	Have a backup admin account with username/passwords stored securely for selected personnel.
60	AAA	Daisy Chaining of Switches	Daisy Chaining of Switches	2	Potential performance issues	Remove the Daisy Chained connections and allocate one switch to be the aggregated switch for all others.
61	Licensing & Patching	Regular update schedules	Software update schedules	5	Potential vulnerabilities if software/firmware is not consistently reviewed and updated.	Implement a firmware patching review schedule
66	Hardware Lifecycle	Lack of hardware lifecycle process	Lack of hardware lifecycle process	2	More susceptible to security threats	Put a hardware lifecycle plan in place so that the hardware is reviewed frequently.

71	Applications	Lack of MFA	Lack of MFA	1	If a users credentials are compromised there is no failsafe	Implement a 2FA/MFA solution.
76	Vulnerability Testing	Lack of penetration test	Lack of penetration test	4	No insight to vulnerabilities, open ports could be externally accessible that Acme is unaware of.	Engage with a reputable penetration testing company to perform a test.
81	Monitoring & Reporting	Lack of network visibility		3	Without being able to see the network status Acme Inc cannot respond to any potential issues.	Implement a network monitoring solution or as part of your hardware upgrades look into a system that proactively monitors.
91	Endpoints & Users	Centralised Management		3	Endpoints may have inconsistent policies for example passwords / windows updates etc.	Ensure all devices are enrolled in a management platform for group centralised policies.
92	Endpoints & Users	Allowing internal users to connect to the internal network via PSK (preshared key)		2	There is no visibility of who is connecting to the network.	Change you internal SSID to use SAML/username password authentication
96	Assets & Devices	No asset register		5	It is very difficult to track and identify	Give each asset a unique identifier and

					Acme Inc owned assets	include in an asset register.
101	Guest	No visibility/accountability		2	There could be unforeseen issues as a result of no visibility of guest users.	Explore options of how to enhance visibility of connected guest users.
102	Guest	Guests/Contractors are not restricted to internet only access		2	Guests/Contractors may have access to resources on the network including sensitive information.	Enforce access by means of either segmentation or a policy enforcement solution.
111	Support & Change Management	No ticketing system		3	Unable to track issues in a structured way / link multiple issues to same problem.	Implement a ticketing solution.
112	Support & Change Management	No Change management process		3	Without a change management process issues arising from any changes may be hard to resolve.	Define and implement a change management process.
116	Backups & Recovery	No Disaster recovery plan		1	Complete loss of service for Acme Inc in the event of an outage.	Put a disaster recovery plan in place and review annually.

Conclusion

Acme Inc Security Audit

Joe Bloggs, we're grateful for the opportunity to provide you with a complimentary security audit. With the identified potential vulnerabilities, a member of the team will be in touch to see how we can work together to proactively fortify your network against cyber threats.