

Overview

Client A



Overview

Client A

spector  IT

Total Assets

148

Supported Users

64

Active Goals

5

Open Initiatives

7



Goals

5

Strategic objects and targets

Protect the Business from Cyber Threats

Target: 2026

On Track

Ensure Reliable & Supported Technology

Target: 2026

On Track

Meet Regulatory & Policy Obligations

Target: 2026

On Track

Prepare for the Unexpected

Target: 2026

On Track

Identity and Access Management

Target: 2026

On Track



Roadmap 7

Current initiatives and projects

Q1, 26 - Q4, 26



- Modernise & Secure Core Infrastructure (PCs) ! OPEN
- Establish Governance & Compliance ! OPEN
- Control Who Has Access to What !! OPEN
- Protect Devices & Endpoints !! OPEN
- Modernise & Secure Core Infrastructure (Network and Perimeter) ! OPEN
- Ensure Recovery Readiness !! OPEN
- Modernise & Secure Core Infrastructure (Servers) ● OPEN

Goals

Client A



Goals

Client A

Ongoing (5 goals)

On Track **Protect the Business from Cyber Threats** Target: 2026

INITIATIVES (1)

Protect Devices & Endpoints	OPEN	-		Cyber
-----------------------------	------	---	--	-------

On Track **Ensure Reliable & Supported Technology** Target: 2026

INITIATIVES (3)

Modernise & Secure Core Infrastructure	OPEN	-		Cyber
Modernise & Secure Core Infrastructure	OPEN	-		Cyber
Modernise & Secure Core Infrastructure	OPEN	-		Cyber

On Track **Meet Regulatory & Policy Obligations** Target: 2026

INITIATIVES (1)

Establish Governance & Compliance	OPEN	-		Cyber
-----------------------------------	------	---	--	-------

On Track **Prepare for the Unexpected** Target: 2026

INITIATIVES (1)

Ensure Recovery Readiness	OPEN	-		Cyber
---------------------------	------	---	--	-------

Ongoing (continued)

On Track

Identity and Access Management

Target: 2026

INITIATIVES (1)

Control Who Has Access to What

OPEN

-



Cyber

Roadmap

Client A




Roadmap Overview


Client A


Q1, 2026 - Q4, 2026

2026


Q2 3 initiatives


- 1 Protect Devices & Endpoints  [OPEN](#)

- 2 Ensure Recovery Readiness  [OPEN](#)


- 3 Modernise & Secure Core Infrastructure (Servers)  [OPEN](#)


Q3 2 initiatives

- 1 Control Who Has Access to What  [OPEN](#)

- 2 Modernise & Secure Core Infrastructure (Network and Perimeter)  [OPEN](#)

Q4 2 initiatives

- 1 Modernise & Secure Core Infrastructure (PCs)  [OPEN](#)

- 2 Establish Governance & Compliance  [OPEN](#)

Q2, 2026

Protect Devices & Endpoints

OPEN

Q2, 2026

Secure every device your team uses to do their work. This covers endpoint protection, encryption, patching, application control, screen lock policies, and local admin rights. Every unprotected or unmanaged device is a potential way in for an attacker, so consistent coverage across the board is essential.

Goals: Protect the Business from Cyber Threats



Ensure Recovery Readiness

OPEN

Q2, 2026

Make sure you can recover quickly and confidently if something goes wrong. This includes backup coverage, offsite storage, restore testing, recovery targets, disaster recovery planning, and backup monitoring. A backup you haven't tested is an assumption. Recovery readiness means knowing it works before you need it.

Goals: Prepare for the Unexpected



Modernise & Secure Core Infrastructure (Servers)

OPEN

Q2, 2026

Make sure the foundations of your IT environment are fit for purpose and your staff remain productive with minimal disruption. This covers end servers, storage and ancillary backup and DR equipment. The goal is to ensure everything is supported, scalable, and able to grow with the business rather than holding it back.

Goals: Ensure Reliable & Supported Technology



Q3, 2026

Control Who Has Access to What

OPEN

Q3, 2026

Make sure the right people have access to the right things and nothing more. This includes directory structure, MFA, password policies, onboarding and offboarding, privileged account management, and regular permission reviews. Access that isn't controlled or reviewed is one of the most common risks we see.

Goals: Identity and Access Management



Modernise & Secure Core Infrastructure (Network and Perimeter)

OPEN

Q3, 2026

Make sure the foundations of your IT environment are fit for purpose and your staff remain productive with minimal disruption. This covers end core networking and perimeter infrastructure. The goal is to ensure everything is supported, scalable, and able to grow with the business rather than holding it back.

Goals: Ensure Reliable & Supported Technology



Q4, 2026

Modernise & Secure Core Infrastructure (PCs)

OPEN

Q4, 2026

Make sure the foundations of your IT environment are fit for purpose and your staff remain productive with minimal disruption. This covers end user PCs, and laptop devices. The goal is to ensure everything is supported, scalable, and able to grow with the business rather than holding it back.

Goals: Ensure Reliable & Supported Technology



Establish Governance & Compliance

OPEN

Q4, 2026

Put the policies and frameworks in place that underpin everything else. This includes security policies, incident response planning, data classification, security awareness training, and cyber insurance. Without governance, there's no agreed standard to measure against and no clear plan when things go wrong.

Goals: Meet Regulatory & Policy Obligations



Assessments

Client A



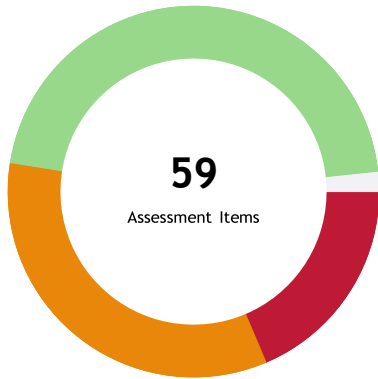
March, 2026

Overall Assessment Score

62.1%

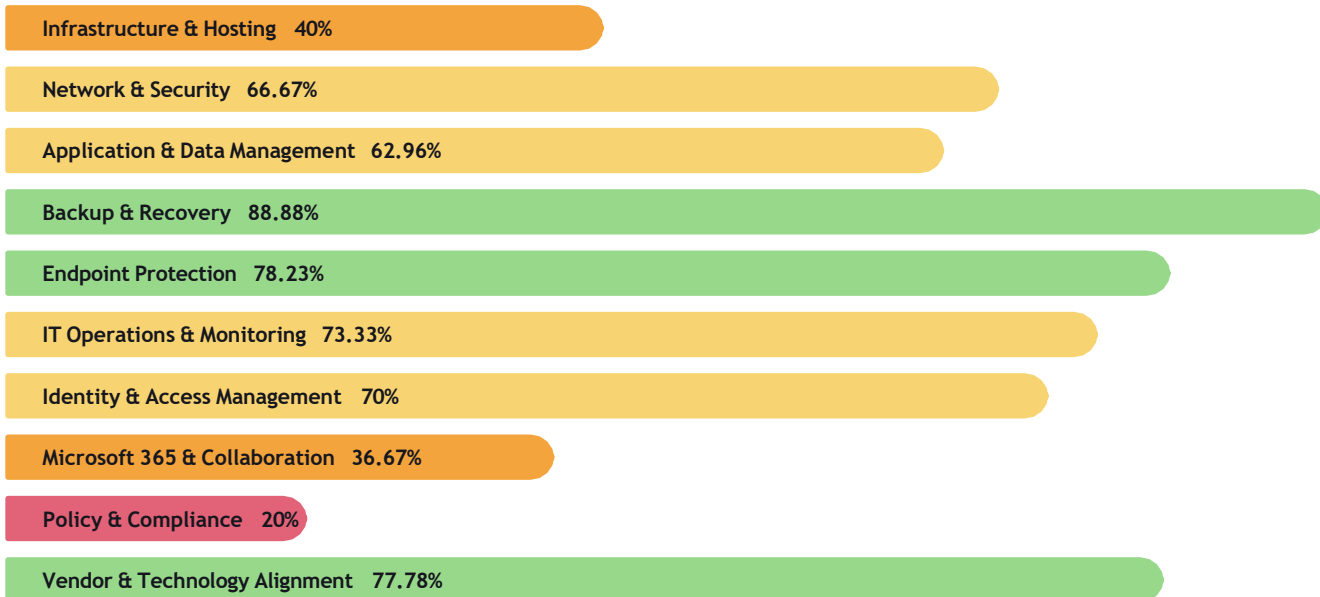


Results Distribution



At Risk	11
Needs Attention	20
Satisfactory	27
Not Applicable	1

Score by Category



Infrastructure & Hosting

40.0%



This category evaluates infrastructure & hosting practices, controls, and business readiness to ensure risk is managed and services remain reliable and secure.

Infrastructure hosting model

This question evaluates: Infrastructure hosting model

Satisfactory

Comment

Cyber Analyst, 04/03/2026

All servers are hosted on-premises in the offices on an ESXi host. This is appropriate for the client as their workflow involves a large amount of data and moving to the cloud completely would not suit.

Virtualization software

This question evaluates: Virtualization software

Needs Attention

Comment

Cyber Analyst 04/03/2026

While the Dublin host is running ESXi 8.0.3 and is within its lifespan, the Cork host is running ESXi 6.7 which is end of life. This should be upgraded or replaced as end of life software can introduce critical vulnerabilities into the environment.

Server hardware age and support status

This question evaluates: Server hardware age and support status

Needs Attention

Comment

Cyber Analyst, 04/03/2026

While all the Dublin servers are within their lifespan and within warranty until 2027, the Cork server is on end of life hardware and should be replaced.

Server operating system versions and support

This question evaluates: Server operating system versions and support

At Risk

Comment

Cyber Analyst, 04/03/2026

vFileServer, which is the main file server, is currently running Windows 2012. This operating system has been end of life for a while now and is no longer supported by Microsoft. Any vulnerabilities that exist in the operating system are currently exploitable and will not be fixed by Microsoft.

Power protection and environmental controls

This question evaluates: Power protection and environmental controls

Satisfactory

Comment

Cyber Analyst, 13/03/2026

You have power protection and cooling in place, but they haven't been reviewed or maintained recently. UPS batteries degrade over time and air conditioning units need regular servicing. If either fails when you need it most, the protection you thought you had simply isn't there. Getting these onto a regular maintenance and testing schedule will make sure they actually do their job when it counts. We suggest that Conor performs a regular test of the UPS to verify battery functionality.

Internet connectivity and redundancy

This question evaluates: Internet connectivity and redundancy

At Risk

Comment

Cyber Analyst, 04/03/2026

There is a good primary internet connection in place, however there is currently no secondary internet connection. This means that if the primary goes down, the entire site will go down and in extreme cases it may take days for the internet provider to fix the issue.

Workstation lifecycle and operating system management

This question evaluates: Workstation lifecycle and operating system management

Satisfactory

Workstation Replacement Policy

This question evaluates: Workstation Replacement Policy

Needs Attention

Comment

Cyber Analyst, 13/03/2026

Based on the evidence there is a plan in place internally to replace equipment, however Spector isn't currently involved outside of fulfilling orders as needed. It is best to define a replacement strategy for all device types. This makes budgeting and replacement strategy simpler for your internal team. We suggest 3 years on common firewalls and 5 years for PC/Laptop and networking equipment. The same 5 year replacement strategy holds for servers and NAS units.

Network & Security

66.7%



This category evaluates network & security practices, controls, and business readiness to ensure risk is managed and services remain reliable and secure.

Network segmentation and VLAN strategy

This question evaluates: Network segmentation and VLAN strategy

Needs Attention

Comment

Cyber Analyst, 13/03/2026

Some separation exists i.e. Staff and Guest wireless, but it's not consistent. It's worth checking whether third-party vendors are properly isolated from each other and your core systems, and whether your backups are segmented from the standard data network. If backups can be reached from the same network as daily operations, they're still vulnerable. Tightening these areas up will make a real difference to your cybersecurity posture.

Wireless network security and guest access

This question evaluates: Wireless network security and guest access

Satisfactory

Comment

Cyber Analyst, 13/03/2026

Your Wi-Fi uses modern encryption with guest access properly isolated from your internal network. There's clear management of who and what can connect. This is exactly where you want to be.

Firewall and unified threat management

This question evaluates: Firewall and unified threat management

Needs Attention

Comment

Cyber Analyst, 13/03/2026

There is a Sonicwall firewall in place, however due to the continued risk of vulnerabilities on SonicWall firewalls Spector does not recommend them. This matters because not all firewalls are equal in terms of capability, update frequency, and the level of management we can provide. Moving to an approved solution means we can ensure it's properly configured, monitored, and kept up to date on your behalf. We suggest replacement.

VPN and remote access security

This question evaluates: VPN and remote access security

Satisfactory

Comment

Cyber Analyst, 13/03/2026

Remote access is properly secured with MFA enforced, access tightly controlled, and activity logged. It's reviewed regularly to make sure it stays that way. This gives your team the flexibility to work remotely without compromising security. While the security controls are in place. There are known remote access vulnerabilities in the Sonicwall firewall that leave the remote access sessions open to compromise. Suggest replacement of the firewall with a Sophos UTM unit.

DNS security and content filtering

This question evaluates: DNS security and content filtering

Satisfactory

DNS security and content filtering

This question evaluates: DNS security and content filtering

Satisfactory

Comment

Mark Hurley, 13/03/2026

DNS filtering was added to your contract as of January. This is currently in discovery mode and we have a plan to activate it with Conor. It will have minimal impact on end users providing content protection is applied across your environment with sensible policies and reporting in place. Your team is protected wherever they work, whether in the office, at home, or on the move. We expect this to be activated by the end of March 2026.

Network monitoring and alerting

This question evaluates: Network monitoring and alerting

Needs Attention

Comment

Cyber Analyst, 13/03/2026

Basic monitoring exists in the Unifi controller on the servers, however these are not currently cloud managed and alerts don't go to Spector when devices are down. We suggest a review of the core infrastructure to assess whether alerting across the entire network is possible. This will take place as part of our initiatives and goal setting for Q2, 2026.

Application & Data Management

63.0%



This category evaluates application & data management practices, controls, and business readiness to ensure risk is managed and services remain reliable and secure.

Line of business application currency and support

This question evaluates: Line of business application currency and support

Satisfactory

Comment

Cyber Analyst, 13/03/2026

Critical applications such as the Adobe Suite, AutoCad are all licensed and up to date. Your key business applications are supported, maintained, and on current versions with clear vendor support arrangements in place. This means your team has access to the latest features, security patches, and a support path if anything goes wrong.

File sharing and collaboration platform strategy

This question evaluates: File sharing and collaboration platform strategy

Needs Attention

Comment

Cyber Analyst, 13/03/2026

Google Drive and Dropbox are both installed on multiple devices in the organisation. No preferred platform exists but exceptions are common and governance is light. When it's too easy to go around the standard, people will. The result is data spread across multiple places with inconsistent sharing rules and no clear picture of who has access to what. Tightening adoption and making sure the rules are applied consistently will bring this under control. Without DNS Filter installed, it's difficult to see what the full scope is, but there's likely many applications being used for file sharing.

Data retention and archival policies

This question evaluates: Data retention and archival policies

Needs Attention

Comment

Cyber Analyst, 13/03/2026

There is some level of archiving taking place currently with older projects being stored on longer term archives on NAS units. Some retention rules exist but they're not consistently applied or enforced. It is important to designate specific NAS devices and retention policies for all data and have this documented. This can be addressed as part of your DR planning.

Database management and maintenance practices

This question evaluates: Database management and maintenance practices

Not Applicable

Backup & Recovery

88.9%



This category evaluates backup & recovery practices, controls, and business readiness to ensure risk is managed and services remain reliable and secure.

Backup strategy and data coverage

This question evaluates: Backup strategy and data coverage

Satisfactory

Comment

Cyber Analyst, 13/03/2026

Your backups cover all key systems and data, with clear schedules and ownership in place. This gives you a solid foundation for recovery if something goes wrong. There remains a gap in terms of what is stored on the NAS devices. We have raised this and suggest the correct labelling and backup of the NAS units using the Synology native backup solution. We also need to be cognisant of large scale changes to file servers i.e. when archival or new projects are added as these can affect the speed at which backups hit our DR cloud platform and may affect recoverability.

Backup retention and offsite storage

This question evaluates: Backup retention and offsite storage

Satisfactory

Comment

Cyber Analyst, 13/03/2026

Backups are stored off-site in the Axcient cloud with appropriate retention and immutability in place. This means even in a worst-case scenario, your backup data is protected from deletion or tampering and available for recovery. There needs to be a review of the data stored on NAS devices. This is under review in Q2, 2026.

Backup testing and restore validation

This question evaluates: Backup testing and restore validation

Satisfactory

Comment

Cyber Analyst, 13/03/2026

Spector performs basic testing regularly. We recommend a full disaster recovery test to open premise hardware as the next step. This requires planning and testing with our professional services team. We will recommend a test plan and provide a quote accordingly as part of the Initiatives for Q2/Q3, 2026.

Recovery time and point objectives alignment

This question evaluates: Recovery time and point objectives alignment

Needs Attention

Comment

Cyber Analyst, 13/03/2026

Recovery targets exist but they haven't been validated against what your current setup can actually deliver. There's no point having a target of four hours if your backup infrastructure would take two days to restore. Aligning your expectations with your actual capability will highlight any gaps that need to be addressed. This can only be achieved through a full DR test. DR test should be performed annually.

Disaster recovery planning and documentation

This question evaluates: Disaster recovery planning and documentation

At Risk

Comment

Cyber Analyst, 13/03/2026

There's no written disaster recovery plan in place. Recovery depends entirely on individuals and their memory of what to do. If that person is unavailable, on holiday, or has left the business, you're starting from scratch in the middle of a crisis. A documented plan with clear roles, contacts, and step-by-step actions means anyone can pick it up and follow it when it matters most. This will be accommodated by a full DR test.

Backup monitoring and failure alerting

This question evaluates: Backup monitoring and failure alerting

Satisfactory

Comment

Cyber Analyst, 13/03/2026

Backup health is actively monitored with clear alerts and a regular review process. When something fails, it's picked up and addressed before it becomes a gap in your protection. This gives you genuine confidence that your backups are doing what they're supposed to.

Endpoint Protection

78.2%



This category evaluates endpoint protection practices, controls, and business readiness to ensure risk is managed and services remain reliable and secure.

Antivirus and endpoint detection/response

This question evaluates: Antivirus and endpoint detection/response

Satisfactory

Comment

Cyber Analyst, 13/03/2026

Centrally managed endpoint protection (Huntress EDR with Managed Microsoft Defender) is deployed across your devices with timely updates and alert handling in place. This gives us full visibility and the ability to respond quickly to any threats. Alerts are sent to Spector and the Huntress SOC ensuring that alerts can be responded to 24/7 as needed.

Device encryption and data protection

This question evaluates: Device encryption and data protection

Satisfactory

Comment

Cyber Analyst, 13/03/2026

Encryption is enforced across your devices and recovery keys are securely managed. This means if a device is lost or stolen, your data stays protected. It's one of those protections you hope you'll never need, but you'll be very glad it's there if you do.

Patch management and update process

This question evaluates: Patch management and update process

Satisfactory

Comment

Cyber Analyst, 13/03/2026

Workstations are all automatically patched by Spector's RMM agent. Critical updates are installed daily, and non-critical updates are installed 14 days after release.

Application control and software restrictions

This question evaluates: Application control and software restrictions

Satisfactory

Comment

Cyber Analyst, 13/03/2026

AutoElevate is in place, ensuring that Admin permissions are removed. A privileged access management solution is in place, giving your team the ability to request software installations through a controlled, logged process. This means no unnecessary admin rights, full visibility of what's being installed, and a smooth experience for your users.

Device compliance and screen lock policies

This question evaluates: Device compliance and screen lock policies

Needs Attention

Comment

Cyber Analyst, 13/03/2026

Policies exist but enforcement is inconsistent or there are too many exceptions. If some devices lock after two minutes and others never lock at all, the policy isn't doing its job. Making sure compliance is applied consistently and reporting on any devices that fall outside the standard will close the gap. We suggest a root and branch review of Group Policy in the company as part of ongoing maintenance in discussion.

Local administrator access control

This question evaluates: Local administrator access control

Needs Attention

Comment

Cyber Analyst, 13/03/2026

Local admins are removed with AutoElevate controlling all admin permissions. Admin rights have been reduced but exceptions are unmanaged or haven't been reviewed. Over time these exceptions build up and before you know it, you're back where you started. A regular review of who has admin access and why will keep things tight.

IT Operations & Monitoring

73.3%



This category evaluates it operations & monitoring practices, controls, and business readiness to ensure risk is managed and services remain reliable and secure.

Infrastructure monitoring and proactive alerting

This question evaluates: Infrastructure monitoring and proactive alerting

Satisfactory

Comment

Cyber Analyst, 13/03/2026

Key details are monitored by Spector in their RMM such as server performance through Disk Space, CPU usage and RAM usage. Alerts are raised for anomalies and actioned as needed. Key systems are monitored with actionable alerts and a clear response process. Problems are identified and addressed early, which means fewer surprises and less downtime for your team. This is proactive IT management working the way it should.

System documentation and configuration management

This question evaluates: System documentation and configuration management

Needs Attention

Comment

Cyber Analyst, 13/03/2026

Some documentation is in place from the Spector side, however some discovery work and collaboration is needed to bring it up to standard. A site visit is required to review network equipment as SNMP monitoring has not been enabled and network management is not completely in place.

Change management and approval processes

This question evaluates: Change management and approval processes

Needs Attention

Comment

Cyber Analyst, 13/03/2026

Spector have an internal change management process, however your company doesn't appear to have a change management policy currently in place. Some approvals and records exist but the process is informal or inconsistently followed interanlly. When changes are only sometimes documented, you lose the ability to trace problems back to their cause. Formalising the process doesn't need to be bureaucratic, it just needs to be consistent so that every change is recorded, approved, and reversible.

Performance monitoring and capacity planning of Networking equipment and servers

This question evaluates: Performance monitoring and capacity planning of Networking equipment and servers

Satisfactory

Comment

Cyber Analyst, 13/03/2026

Basic monitoring is in place but older equipment is limiting what's possible. You're getting some data, but not enough to plan ahead with confidence. Upgrading monitoring capability and putting a clear view of equipment age and capacity in front of decision-makers will help you budget for replacements before they become emergencies. This is part fo the suggested network monitoring for Q2/Q3.

Service level agreements and performance metrics

This question evaluates: Service level agreements and performance metrics

Satisfactory

Comment

Cyber Analyst, 13/03/2026

Spector have clearly defined SLAs which are consistently achieved. Clear targets and performance metrics are tracked, reviewed, and used to drive continuous improvement. You know exactly what level of service you're getting and there's a process for addressing any areas that fall short.

Asset inventory and lifecycle tracking

This question evaluates: Asset inventory and lifecycle tracking

Needs Attention

Comment

Cyber Analyst, 13/03/2026

Spector maintains an asset inventory through Datto RMM, however an audit should be done of Active Directory to ensure all devices are present in monitoring. Many devices for example are still in Active Directory that are no longer in use. There are also NAS devices that need to be functionally labelled and named to improve traceability as to what data lives where.

Identity & Access Management

70.0%



This category evaluates identity & access management practices, controls, and business readiness to ensure risk is managed and services remain reliable and secure.

Directory services and organizational structure

This question evaluates: Directory services and organizational structure

Satisfactory

Comment

Cyber Analyst, 13/03/2026

Active Directory is in place as the primary directory for you. Your directory is well structured and maintained with clear groups, roles, and documentation. This gives us a solid foundation to manage access, apply security policies consistently, and handle onboarding and offboarding efficiently.

Multi-factor authentication implementation

This question evaluates: Multi-factor authentication implementation

Satisfactory

Comment

Cyber Analyst, 13/03/2026

MFA is enforced across your key systems for both standard users and administrators, with sensible policies governing when and how it's applied. This is one of the most effective protections any business can have in place.

Password policies and complexity requirements

This question evaluates: Password policies and complexity requirements

At Risk

Comment

Cyber Analyst, 13/03/2026

Passwords are weak with a very poor localised password policy, it is not properly controlled, or being shared between staff. Without proper standards in place, it only takes one easily guessed password to give an attacker a way in. Password sharing is equally dangerous because there's no way to trace who did what if something goes wrong. Getting a clear, enforced password policy in place is a fundamental step.

User onboarding and offboarding process

This question evaluates: User onboarding and offboarding process

Satisfactory

Comment

Cyber Analyst, 13/03/2026

A standard onboarding and offboarding process is in place. Access is role-based, removed promptly when someone leaves, and there's clear ownership at every step. New starters get what they need on day one, and leavers don't take access with them.

Privileged account management and monitoring

This question evaluates: Privileged account management and monitoring

At Risk

Comment

Cyber Analyst, 13/03/2026

Admin accounts are shared or there's no separation between someone's everyday user account and their admin access for your key MS 365 tenancy. This is considered a very high risk. Admin accounts should be separated from day to day accounts and protected with very high security passwords, MFA and strict conditional access. If a shared admin account is compromised, there's no way to trace who did what, and the attacker has the keys to the kingdom. A solution like AutoElevate ensures every admin action is tied to a named individual, logged, and only granted when genuinely needed.

Access permissions and regular review process

This question evaluates: Access permissions and regular review process

At Risk

Comment

Cyber Analyst, 04/03/2026

There is no evidence currently of access reviews occurring.

Microsoft 365 & Collaboration

36.7%



This category evaluates microsoft 365 & collaboration practices, controls, and business readiness to ensure risk is managed and services remain reliable and secure.

Microsoft 365 security and compliance configuration

This question evaluates: Microsoft 365 security and compliance configuration

Needs Attention

Comment

Cyber Analyst, 13/03/2026

Some protection is in place, however the licensing level of the tenancy restricts what could be used (Conditional Access for example). Some protections have been enabled but settings are inconsistent or haven't been reviewed since they were first configured. Microsoft regularly adds new security features and your Secure Score may have drifted as a result. What was good enough a year ago may have gaps today. A review against our baseline and your current Secure Score will identify what needs tightening up. This will require an upgrade to MS Business Premium for all users. Prices have come down for Premium and risen for Standard, so the time is now to act in terms of making that change.

SharePoint and OneDrive governance

This question evaluates: SharePoint and OneDrive governance

Needs Attention

Comment

Cyber Analyst, 13/03/2026

Policies exist but they're not consistently applied. External sharing and permissions aren't being regularly reviewed, which means access granted six months ago for a specific project may still be active today. A review of what's shared, with whom, and whether it's still appropriate will tighten things up significantly.

Microsoft Teams security and external access

This question evaluates: Microsoft Teams security and external access

Needs Attention

Comment

Cyber Analyst, 13/03/2026

External access is allowed but the governance around it is weak. There's no clear policy on who can invite guests, what they can see, or when their access should be reviewed and removed. Tightening the controls and putting a review process in place will make sure external access is intentional rather than accidental.

Email security and advanced threat protection

This question evaluates: Email security and advanced threat protection

Needs Attention

Comment

Cyber Analyst, 13/03/2026

A dedicated email filtering solution is in place with custom rules configured. This is a significant step up from the default. To fully protect your domain and reduce the risk of spoofing, we also need to make sure SPF, DMARC, and DKIM are configured correctly. In plain English, these are settings that prove your emails are genuinely coming from you and help stop attackers sending emails that look like they're from your domain. Advanced email protection is in place with SPF and DKIM setup, however the DMARC record is currently set to none. This means that it's not enforced. Enforcing the DMARC record ensures that OCMA accounts cannot be spoofed and used to phish other email addresses for example. As we do not manage your DNS records we will need this change made.

Mobile device management and application protection

This question evaluates: Mobile device management and application protection

At Risk

Comment

Cyber Analyst, 13/03/2026

There's no mobile device management in place, which means if a phone or tablet is lost or stolen, there's no way to remotely wipe company data from it. Personal devices may also be accessing company email, files, and systems with no controls whatsoever. Without MDM, you have no visibility of what devices are connecting to your environment and no ability to protect the data on them.

License management and optimization

This question evaluates: License management and optimization

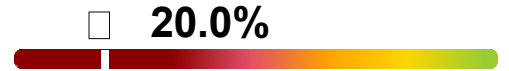
Satisfactory

Comment

Cyber Analyst, 13/03/2026

Licenses are actively managed with regular reviews and clear ownership. Your licensing matches the roles and needs across your organisation, which means you're getting full value from your investment without unnecessary spend.

Policy & Compliance



This category evaluates policy & compliance practices, controls, and business readiness to ensure risk is managed and services remain reliable and secure.

Security policy framework and documentation

This question evaluates: Security policy framework and documentation

At Risk

Comment

Cyber Analyst, 13/03/2026

There are no documented security policies in place, or what exists is significantly outdated and unknown to staff. Without a clear policy, there's no agreed standard for how your business handles security, data, or technology. It also makes it very difficult to hold anyone accountable, whether that's staff, vendors, or partners. A documented information security policy is the starting point for everything else in this space.

Incident response plan and procedures

This question evaluates: Incident response plan and procedures

At Risk

Comment

Cyber Analyst, 13/03/2026

Aside from Spector's internal incident response plan, there is no plan currently in place. There's no internal incident response plan in place. If something goes wrong, whether it's a cyberattack, data breach, or major system failure, the response is improvised. That means no defined contacts, no clear roles, and no agreed steps to follow. In the middle of a crisis is the worst time to figure out who does what. Having a plan ready to go means the first hour of an incident is spent responding, not scrambling.

Data classification and handling procedures

This question evaluates: Data classification and handling procedures

At Risk

Comment

Cyber Analyst, 13/03/2026

There's no data classification or handling rules in place, which means sensitive data is treated the same as everything else. A confidential client contract gets the same level of protection as last year's Christmas party photos. Without clear rules on what's sensitive, who can access it, and how it should be stored and shared, you're relying on people to make the right judgement call every time. That's not a strategy, it's a gamble.

Security awareness training program

This question evaluates: Security awareness training program

Satisfactory

Comment

Cyber Analyst, 13/03/2026

Quarterly security awareness training and phish testing is setup by Spector for the users. Completion rates are currently about 60-70%, which is good but could be higher. We expect this engagement number to improve as you follow up on the training campaigns.

Cyber liability insurance coverage

This question evaluates: Cyber liability insurance coverage

At Risk

Comment

Cyber Analyst, 13/03/2026

You either have no cyber insurance or your coverage is unknown or outdated. If you experience a cyberattack, data breach, or ransomware incident, the costs can escalate quickly, from forensic investigation and legal fees to regulatory fines and business interruption. Without appropriate cover, your business absorbs all of that. It's also worth noting that many insurers now require a minimum level of security controls before they'll provide cover at all.

Vendor & Technology Alignment

77.8%



This category evaluates vendor & technology alignment practices, controls, and business readiness to ensure risk is managed and services remain reliable and secure.

IT vendor relationship and contract management

This question evaluates: IT vendor relationship and contract management

Satisfactory

Comment

Cyber Analyst, 13/03/2026

Key apps are supported and maintained, with a clear plan for updates and vendor support.

Technology stack standardization and coherence

This question evaluates: Technology stack standardization and coherence

Satisfactory

Comment

Cyber Analyst, 04/03/2026

Spector's standard tool stack is in place and compliance is 100%.

IT strategy alignment with business objectives

This question evaluates: IT strategy alignment with business objectives

Needs Attention

Comment

Cyber Analyst, 13/03/2026

A clear IT roadmap aligns to business goals and is reviewed and updated regularly. While we only need to meet formally twice annually, it would be an idea to keep the initiatives coming from this scorecard more regular with defined outcomes for the internal IT function.

Technology budgeting and financial planning

This question evaluates: Technology budgeting and financial planning

Needs Attention

Comment

Cyber Analyst, 13/03/2026

Budget exists but forecasting and tracking are limited or updated infrequently. This is easily corrected in our next Strategic Business Review meeting.

Innovation appetite and technology adoption strategy

This question evaluates: Innovation appetite and technology adoption strategy

Satisfactory

Comment

Cyber Analyst, 04/03/2026

All tools introduced by Spector follow a defined rollout process including pilot groups where needed.

Support escalation and service management

This question evaluates: Support escalation and service management

Satisfactory

Comment

Cyber Analyst, 13/03/2026

Clear service process (ticketing, priorities, escalation, communication) with reporting and continuous improvement, meeting defined ITIL standards.