

TECHNOIDS TECHNOLOGY SECURITY REVIEW SERIES

Accounting & Tax Firm Technology Security Checklist

A practical review worksheet for client data, tax-season readiness, Microsoft 365, endpoints, backups, WISP, and security visibility.

YES / NO / NOT SURE / N/A

This is not a pass/fail cybersecurity test.

A No or Not Sure identifies an area worth understanding more closely.

Technoids Techs

Knowledge Is Part of Protection.

Digital Technology. Real-World Care.

Accounting & Tax Firm Technology Security Checklist

Knowledge Is Part of Protection. Use this worksheet to review the technology and security areas that commonly matter to accounting and tax firms: client information, identity, endpoints, Microsoft 365, networks, backups, WISP readiness, monitoring, and peak-season operations.

How to use this checklist	Review each question and mark the answer that best reflects your current visibility. The goal is not to score your firm. The goal is to identify what you understand, what may need attention, and what would be useful to discuss with Technoids Techs.	
Firm _____ _____	Completed by _____	Date _____

YES	A control or process appears to exist.
NO	An area may deserve further evaluation.
NOT SURE	An area where visibility may be missing.
N/A	Not applicable to your environment.

This is not a pass/fail cybersecurity test. A No or Not Sure identifies an area worth understanding more closely.

Client & Financial Information

Review question	YES	NO	NOT SURE	N/A
Do we know where sensitive client and taxpayer information is stored?				
Do we know which employees can access sensitive client information?				
Is access limited based on employee responsibilities?				
Do we periodically review who has access?				

Identity & Access

Review question	YES	NO	NOT SURE	N/A
Is MFA enabled for Microsoft 365?				
Is MFA enabled for tax/accounting applications where supported?				
Does every employee have an individual account?				
Are shared employee passwords avoided?				
Are former employees' accounts promptly disabled?				
Are administrator privileges limited?				

Computers & Endpoints

Review question	YES	NO	NOT SURE	N/A
Are all business computers centrally inventoried?				
Are operating systems and applications regularly patched?				
Are computers protected with managed endpoint security?				
Do we use EDR or equivalent advanced endpoint monitoring?				
Are laptops encrypted?				
Do devices automatically lock after inactivity?				

Email & Microsoft 365

Review question	YES	NO	NOT SURE	N/A
Is business email protected against phishing and malicious messages?				
Is Microsoft 365 actively administered rather than simply licensed?				
Are suspicious sign-ins monitored?				
Do employees know how to report suspicious email?				

Network Security

Review question	YES	NO	NOT SURE	N/A
Is the business firewall actively managed?				
Is business Wi-Fi appropriately secured?				
Is guest Wi-Fi separated from business systems?				
Are unsupported network devices identified and replaced?				

Backup & Recovery

Review question	YES	NO	NOT SURE	N/A
Is critical business information backed up?				
Is Microsoft 365 data included in our recovery planning?				
Are backups protected from ransomware or unauthorized access?				
Are backup failures monitored?				
Have we tested recovery?				

WISP, Monitoring & Incident Readiness

Review question	YES	NO	NOT SURE	N/A
Does our firm maintain a current Written Information Security Plan?				
Does the WISP reflect our actual technology environment?				
Do we periodically assess technology/security risk?				
Is security activity monitored outside normal business hours where appropriate?				
Do employees receive security-awareness training?				
Do we have a documented incident-response process?				
Can we confidently answer our cyber-insurance security questions?				

Busy-Season Readiness

Review question	YES	NO	NOT SURE	N/A
Do we review device health before tax season?				
Are known technology risks addressed before filing deadlines?				
Is backup/recovery readiness reviewed before peak periods?				
Do we know which equipment may need replacement within 12 months?				

What Did You Discover?

This checklist is not designed to give your firm a cybersecurity grade. Technology environments are too different for a simple score to tell the entire story. Instead, look at your answers and use them to guide the next conversation.

YES	_____	NO	_____
NOT SURE	_____	N/A	_____

How to Interpret Your Answers

YES	A control or process appears to exist.
NO	An area may deserve further evaluation.
NOT SURE	An area where visibility may be missing.
N/A	Not applicable to your environment.

Do not start with the product. Start with the questions: What are we protecting? Who has access? Which technology do we depend on? Where are our largest risks? What do we not know? What should we address first?

Areas I Want to Review

1. _____
2. _____
3. _____

Questions for Technoids Techs

1. _____
2. _____
3. _____
4. _____

Want Help Reviewing Your Answers?

Bring your completed checklist to a Technoids Technology & Security Review. We'll help you understand what your answers may mean, which areas deserve closer attention, and what practical next steps may make sense for your firm.

Schedule a Technology & Security Review

Technoids Techs

Knowledge Is Part of Protection.

Digital Technology. Real-World Care.

Practical managed technology, cybersecurity, compliance support, and planning for organizations where digital systems affect real people, real responsibilities, and real operations.

Educational-use disclaimer: This checklist is provided for general educational purposes and is not a certification, audit, legal opinion, regulatory determination, or guarantee of cybersecurity or compliance. Organizations should consult appropriate legal, regulatory, insurance, or compliance advisors for requirements specific to their situation.