Workbook

How to Transition to Digital Safely and More Profitably

We have seen research consistently show that clients want an accounting expert that understands their business, providing proactive advice and guidance to help them grow their company. As accounting professionals, we too often think that the main reason clients leave us is because we are too expensive. In reality, they want to see the best value for money, not necessarily the cheapest service. And how do we add value to their service? Well, we have to be proactive and become *advisors* – and to do that we need to give ourselves more time. Going digital is a great way to save ourselves time through automation of tasks and communication. But, when we move to a digital-first strategy, we need to first ensure our security procedures are watertight to avoid cyberattacks or data leaks.

The payoff of going fully digital means your practice will be better equipped to take on more clients without the need to recruit more staff. You'll also increase the time you have available to provide higher value, advisory level services at premium prices. In a nutshell: faster, time-saving technology means you can work less and make more money.

But no matter where you are on your digital practice journey, you need to ensure security policies and procedures are in place. Without it, the consequences for your business could be catastrophic.

The *How to Transition to Digital Safely and More Profitably* workbook is designed to help you assess what needs to be addressed within your firm to ensure you are compliant and secure. Once you have identified any weaknesses, it will help you create an action plan to address them. Once you have gone through each area and implemented your plan of change, you should be ready to make the switch to being fully digital.

Just remember, cybersecurity is always evolving and bad-habits can often creep in, so you should revisit this workbook regularly to ensure you are still adhering to best practices. Although it is impossible to protect yourself 100% from a cyberattack, you can drastically reduce the risk by following the advice in this workbook and **on my webinar.**

About the Author

Gabrielle Fontaine is a freelance Professional Bookkeeper and Advanced Certified QuickBooks ProAdvisor who assists tech-savvy consultants and self-employed professionals get their books under control, save taxes, and maximize cash flow and profits using the power of online apps. Gabrielle has been in business for over 25 years, and has been working 100% virtually since 2003. She is the author of the popular blog, **The Freelance Bookkeeper**, and produces online training programs, has been a popular guest speaker on business and accounting podcasts, as well as industry conferences.

Action Worksheet

Cybersecurity for Digital Accountancy

Areas of high risk for accountancy firms

☑ Check off the areas in your practice where you feel systems are needed or could be improved.

Email

- ☐ Sending / receiving sensitive information, (unencrypted)
- ☐ Opening email and/or attachments that contain malware
- ☐ Fraudulent messages asking for logins or sensitive information

File Sharing

- ☐ Inadequately protected online sharing tools (consumer level solutions)
- ☐ Sharing via mobile or apps that do not have adequate security / encryption

File Storage

- ☐ Sensitive info stored on local and / or removable devices without encryption
- ☐ No cloud-based, secure backups

Password Management

- ☐ Unencrypted storage / not using a secure password management program
- ☐ Using same and / or weak passwords for multiple logins
- ☐ Shared logins with clients and / or among team members
- ☐ Not using multi-factor authentication where it's available (especially bank logins)

Team / Workflow

- ☐ Local computer access (passwords? Shared devices?)
- ☐ Sensitive information printed to paper (physical file security / disposal)
- ☐ Team member tech security training
- ☐ Mobile device security procedures and protocols
- ☐ Internet access security (home network / public Wi-Fi)

Hardward / Software

- ☐ Outdated software with vulnerabilities (including website)
- ☐ Inadequate firewall / virus / malware protection
- ☐ Older hardware (routers, modems, firewalls)

Lack of Planning

- ☐ No cybersecurity insurance
- ☐ No disaster recovery plan
- ☐ No breach response plan
- ☐ No ongoing education and assessment plan (with accountability)

Action Worksheet

Cybersecurity for Digital Accountancy

Your Action Plan

Which area of risk will you focus on first, and by when?

Area of Risk: _____

By when will you work on it (date): _____

Who will hold you (or be) accountable? _____

Which area will you focus on next?

Area of Risk: _____

By when will you work on it (date): _____

Who will hold you (or be) accountable? _____

How will you continue to educate yourself and your team?

- ☐ Build an in-house / online library of resources and links

  Note: Trello is a free tool you could use for this purpose

- ☐ Set a regular plan to review and update systems to maintain protection
  - ☐ Quarterly
  - ☐ Semi-Annually
  - ☐ Annually

- ☐ How often will you require your team to be trained on cybersecurity best practices?
  - ☐ Quarterly
  - ☐ Semi-Annually
  - ☐ Annually

- ☐ Who will be in charge of making sure plans are carried out?

  Name: _____

Success Checklist

The New Perspective Accountancy Firm

The New Perspective Accountancy Firm is focused on long-term, premium value services for clients who want more than commodity level compliance support. For long-term, highly profitable growth in the digital age of accountancy, you need to provide what the high-volume automation-heavy competitors cannot – proactive, high-trust services that deliver a frictionless experience for your clients, and beyond.

The path to achieving this ideal is a three-phase approach...

- ☑ Streamlined technology-leveraged workflow
- ☑ Proactive systems designed to deliver a frictionless client experience
- ☑ Premium level strategic leadership focused on client growth and prosperity

Phase 1

Creating Your Streamlined Technology-Leveraged Workflow

- ☐ Document on a top level your current workflow for each core client / service offering
  - ☐ Identify any points of security risk for the path and handling of sensitive info
  - ☐ Identify the bottlenecks for completing processes effectively and timely
  - ☐ Identify points of friction / frustration for your clients based on behavior
- ☐ Standardise service delivery to address and resolve bottlenecks and security issues
  - ☐ Onboarding procedures and communication
  - ☐ Staff training, supervision and accountability
  - ☐ Consistent practice management and tracking
  - ☐ Gather client feedback and input for addressing points of friction for them
- ☐ Optimise systems using automation wherever possible
  - ☐ Identify functions that are repetitive and consistent across your client base
  - ☐ Implement the 6-step process for choosing and integrating automation into your workflow (see the **App Survival Guide**)

Get more support and guidance on improving your workflow and building the New Perspective Accountancy Firm

Schedule your free one-on-one workflow consultation surrounding document management and a streamlined client portal with SmartVault

Get the latest tips, tricks and training at The Freelance Bookkeeper Blog

Helpful Resources

Here are some web resources to get your education library/program started:

ICAEW's Guide to GDPR

Security info provided by SmartVault

Cyber Essentials and GDPR

GDPR and cyber security

GDPR info from an accountancy firm

The National Cyber Security Centre

Training resources recommended by Carbonite

Helpful articles and app for GDPR compliance and cybersecurity best practices by Astrid Online cybersecurity training classes

Managing Passwords for Your Accounting Clients: a free guide from Hubdoc & SmartVault