Checklist for small law firms

Steps you can take today to prepare your firm for the future

iManage

Making knowledge work

Table of contents

3 **Introduction**

4 **From surviving to thriving:** Technology readiness

- 5 Core software and tools
- 6 Assess cloud vendors
- 8 Cloud adoption
- 9 Change management and user engagement

10 **Plan B:** Business continuity & disaster recovery

- 11 Backup and recovery
- 12 Business continuity plan

13 **Safety first:** Data privacy & cybersecurity

- 14 Data audit
- 15 Create cybersecurity policies
- 16 Regular software updates and patch management

17 **Here, there, everywhere:** Hybrid work preparedness

- 18 Technology for remote work
- 19 Communication and collaboration

iManage
Making knowledge work

The legal market is rapidly changing, and small law firms must prepare themselves to compete in a field of evolving security concerns and increasing client demands.

You can't fully predict what the future will hold, but you *can* set yourself up for success by making a plan now for your technology, business continuity, and security. Our handy checklist will help your firm take the right steps to succeed now - and into the future.

iManage
Making knowledge work

I.

From surviving to thriving: **Technology readiness**

iManage
Making knowledge work

CORE SOFTWARE AND TOOLS

- [ ] **Have your IT team or consultant assess your current software and tools.**

  Are they achieving their intended purpose? If not, is it time to re-evaluate hurdles to end-user adoption, or consider a new vendor?

- [ ] **Update your software to the latest version.**

  If you are satisfied with your current technology, update and upgrade your existing software to the latest versions to ensure their security features are current.

- [ ] **Consider if now is the right time to move to the cloud if you haven't already.**

  Cloud-based technology allows small firms to compete on an even playing field with larger organizations.

- [ ] **Evaluate the feasibility of choosing cloud-based document management.**

  Cloud-based technologies empower legal professionals to work from anywhere, with enhanced security compared to on-premises systems.

ASSESS CLOUD VENDORS

A document management system (DMS) is often considered a better option for law firms compared to general-purpose cloud tools for several reasons:

- ☐ **Compliance measures:**

  A specialized DMS is designed with legal compliance in mind, providing features and safeguards to meet industry-specific requirements regarding data protection and client confidentiality.

- ☐ **Security features:**

  DMS platforms typically offer comprehensive security protections, including active threat detection and zero trust architecture. These features help ensure that confidential legal documents are protected from unauthorized access and tampering.

- ☐ **Version control:**

  Legal documents often go through multiple revisions. DMS solutions provide robust version control features, allowing users to track changes, revert to previous versions, and maintain an organized and auditable document history.

Section continues on the next page.

ASSESS CLOUD VENDORS (CONT.)

- [ ] **Role-based access:**

  DMS platforms allow law firms to set need-to-know access controls based on roles and responsibilities. This ensures that only authorized personnel have access to specific documents, preventing unauthorized viewing or editing of sensitive legal information.

- [ ] **Advanced search functionality:**

  With the sheer amount of documents law firms deal with day in and day out, creating a single source of truth for legal content is essential. Finding the right piece of information quickly, efficiently, and accurately through a DMS is done through advanced search functionalities, metadata tagging, and categorization.

- [ ] **Seamless integration:**

  Many DMS solutions are designed to integrate seamlessly with legal practice management software and other tools commonly used in law firms. This integration enhances overall productivity by allowing for a more cohesive, matter-centric, and connected workflow.

- [ ] **Collaboration tools:**

  While you may find that general-purpose cloud tools offer collaboration features, DMS platforms are often tailored to the specific needs of legal collaboration. This can include features like document commenting, annotation, and secure sharing with external parties.

CLOUD ADOPTION

☐ **Develop a plan for transitioning to the cloud, if applicable.**

Ready to make your move to the cloud? Our guide can help.

☐ **Explore new opportunities available in the cloud.**

Once you're in the cloud, you have a whole new world of innovation available:

- Consider investing in legal tech solutions for research and legal transaction management.
- Look into how your firm could employ the latest innovations, such as generative AI, automation, and collaboration tools, which are only available in the cloud.

CHANGE MANAGEMENT & USER ENGAGEMENT

- [ ] **Create a training plan for new technology.**

  Traditional one-and-done trainings aren't always the most effective. Consider ongoing short learning sessions, office hours with the resident expert on the technology, and online training videos offered by your vendor.

- [ ] **Identify technology skill gaps within your team.**

  Seeing uneven or disparate use of certain technology? Host a refresher session to get everyone up to speed.

II.

Plan B: **Business continuity & disaster recovery**

iManage
Making knowledge work

BACKUP AND RECOVERY

- [ ] **Regularly backup essential data and documents.**

  Manually backing up data is great, but it's even better to automate it. See below.

- [ ] **Implement an automated backup system.**

  This is a crucial step to prevent data loss. Where applicable, ensure your technology is configured to automatically back up data.

- [ ] **Develop a data recovery plan.**

  Identify business-critical data and have a plan in place to recover should disaster occur. See the next page for ideas on where to start.

BUSINESS CONTINUITY

- [ ] **Create a business continuity plan to address unexpected disruptions.**

  Natural disasters, international conflict, and global pandemics can and do happen. Make a plan now for how decisions will be made and communicated should disaster strike.

- [ ] **Maintain contact lists for staff and key stakeholders.**

  Don't be caught without a way to get in touch with your team.

- [ ] **Identify alternative office spaces in case of emergencies.**

  If an in-person meeting is required but the office is out of commission, designate a backup spot that can be easily reserved as needed, such as a coworking space or hotel conference room.

- [ ] **Ensure your team is able to work remotely if needed.**

  Even if your firm has returned to the office full-time, make sure you have a plan for how your team can work effectively if it's necessary to shelter in place. See Part IV for more.

III.

Safety first: **Data privacy & cybersecurity**

iManage
Making knowledge work

DATA AUDIT

- [ ] **Conduct a comprehensive data audit to identify sensitive client information.**

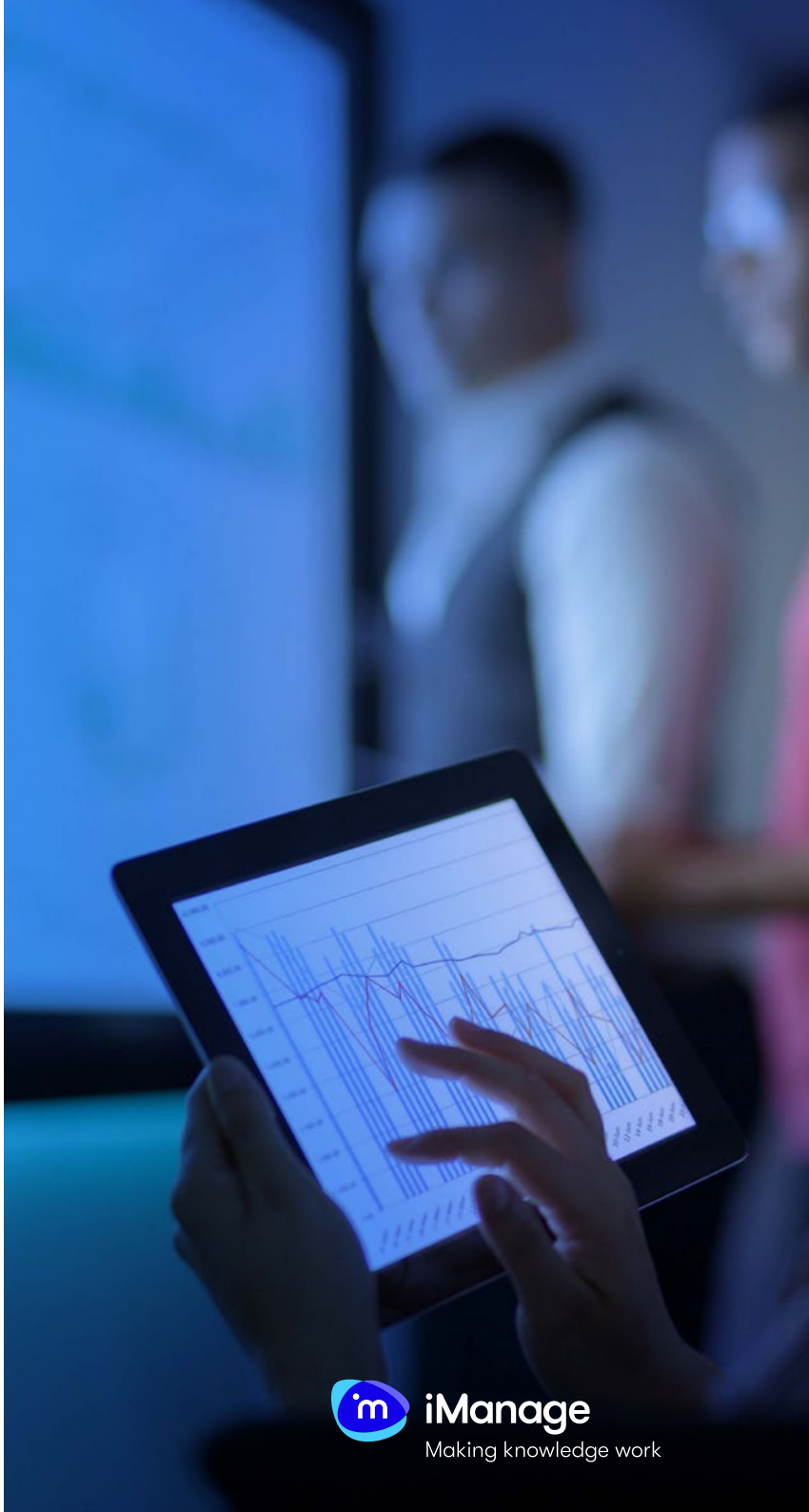
  Identify your clients' most sensitive data and ensure it is filed appropriately. It's easier to keep important information safe if you know where it is.

- [ ] **Categorize data based on its level of sensitivity and confidentiality.**

  And keep it organized based on these categories. Don't let confidential information get mixed up with other files.

- [ ] **Ensure proper encryption and access controls.**

  Don't let those who shouldn't see certain information access it. Careful access control can prevent a lot of problems down the road.



CREATE CYBERSECURITY POLICIES

- [ ] **Review and update your law firm's cybersecurity policies and procedures.**

  When's the last time your firm reviewed your security policies? If it's been over a year, it's probably time to revisit them. If you can't remember the last time you reviewed the policies, it's *definitely* time to revisit them.

- [ ] **Develop an incident response plan in case of a data breach.**

  Cybercrime is on the rise, and it's not a question of *if* so much as *when* your firm will be targeted. Create a plan now on how you will rectify a breach and communicate with clients in the event of an incident.

- [ ] **Ensure that all staff members are aware of and adhere to security protocols.**

  The weak link of any security plan is people, meaning creating a culture of security at your firm is non-negotiable. Educate and re-educate your team on your firm's security protocols and best practices often.

REGULAR SOFTWARE UPDATES & PATCH MANAGEMENT

- [ ] **Create a schedule for regular software updates and security patches.**

  If your technology is in the cloud, this will be done for you automatically! If not, ensure that any updates and patches are installed promptly to avoid falling behind on security.

- [ ] **Implement a robust antivirus and anti-malware system.**

  Even the best security training can't prevent everyone from clicking on a well-crafted phishing email. Ensure that any viruses that sneak into your systems can't get far by investing in a quality antivirus and anti-malware system.

- [ ] **Consider the use of intrusion detection systems.**

  The best offense is a good defense. Choose an intrusion detection system to monitor for malicious activity or policy violations.

IV.

Here, there, and everywhere: **Hybrid work preparedness**

iManage
Making knowledge work

TECHNOLOGY FOR REMOTE WORK

- [ ] **Reassess the tools and technology your team is using to work remotely.**

  Are your employees able to do the same quality of work at home as in the office? If not, what tools do they need to make that possible?

- [ ] **Ensure secure access to documents and case information from any location.**

  Document security is essential no matter where you're working. If remote workers cannot securely access firm documents, it may be time to upgrade your document management system.

- [ ] **Confirm compliance to approved storage and devices.**

  Make sure employees are not using their personal laptops or unapproved consumer storage platforms to store sensitive client information.

COMMUNICATION AND COLLABORATION

- [ ] **Set up effective communication channels.**

  Ensure your team can communicate securely via chat, voice call, or video call as needed to get the job done. Consider how content shared on these platforms remains secure and governed.

- [ ] **Implement collaboration tools to streamline teamwork.**

  Task management software makes it easier for everyone to stay on the same page in a remote work environment.

- [ ] **Ensure that client communication remains secure.**

  If possible, save important client emails in your document management system so the information remains securely accessible.

Looking ahead

By making a plan now for technology, business continuity, and security while aligning people and processes, your firm will be better prepared to embrace the new realities of legal work, from cloud computing to generative AI.

If new technology is part of your plans, schedule a demo with us today!

twitter.com/imanageinc

youtube.com/imanage

linkedin.com/company/imanage

www.imanage.com

iManage
Making knowledge work