Checklist for midsize 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 Cloud adoption
- 6 Change management and user engagement
- 7 Explore new opportunities available in the cloud

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

- 9 Backup and recovery
- 10 Business continuity plan

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

- 12 Data audit
- 13 Create cybersecurity policies
- 14 Regular software updates and patch management

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

- 16 Technology for remote work
- 17 Communication and collaboration

iManage
Making knowledge work

The legal market is rapidly changing, and midsize 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.

I.

From surviving to thriving: **Technology readiness**

iManage
Making knowledge work

CLOUD ADOPTION

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

Cloud-based technology allows midsize firms to compete on an even playing field with larger organizations by offering the best performance, agility, and scalability to every firm.

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

Cloud-based technologies empower legal professionals to work from anywhere, with enhanced security and powerful new functionality.

□ **Assess cloud vendors.**

Not all cloud offerings are the same. Evaluate potential vendors on their:

- Cloud architecture
- Security features
- User experience
- Scalability
- Post-deployment support

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

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

CHANGE MANAGEMENT & USER ENGAGEMENT

□ **Create a training plan for new technology.**

Traditional one-and-done trainings aren't always the most effective. Consider a change management approach built around your users, incorporating 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.

EXPLORE NEW OPPORTUNITIES AVAILABLE IN THE CLOUD

□ **Maximize the value of your documents with knowledge management.**

Integrating a knowledge search and management solution with your DMS can make it much easier for lawyers to quickly find best practice work product so they can deliver faster, higher-quality client service.

□ **Simplify legal transactions.**

If your firm works with transactional deals, consider investing in a solution for legal transaction management that integrates with your DMS.

□ **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.

□ **Prepare for the future with generative AI.**

Look into how your firm could leverage the value of generative AI while minimizing security risks.

II.

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

BACKUP AND RECOVERY

☐ **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.

III.

Safety first: **Data privacy & cybersecurity**

iManage
Making knowledge work

DATA AUDIT

□ **Conduct a comprehensive data audit to identify sensitive client information.**

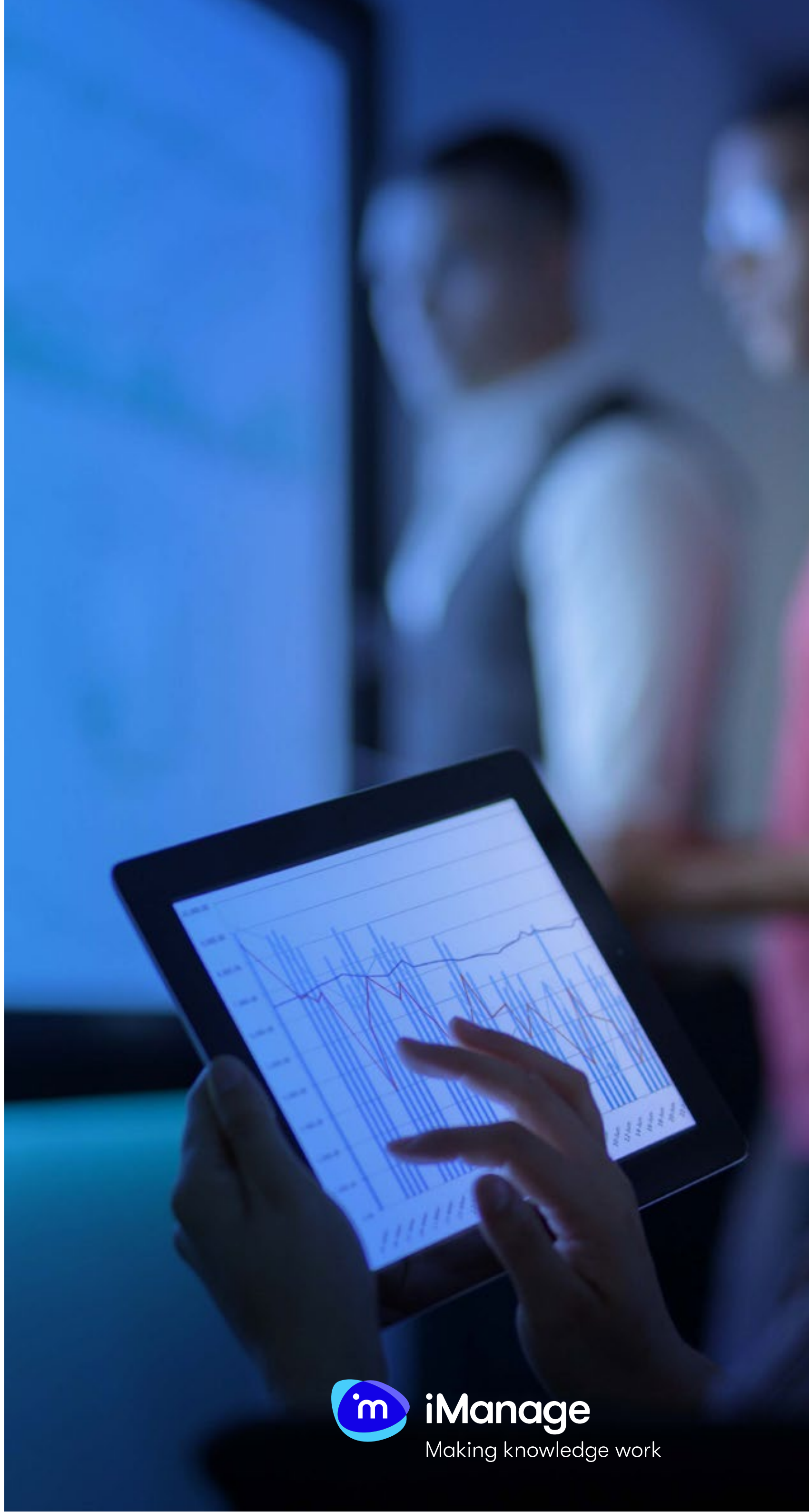
Identify your clients' most sensitive data and ensure it is filed appropriately. It's easier to keep important information safe if you know where it is.

□ **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.**

Define and implement security rules to govern access to content. Careful access control can prevent a lot of problems down the road.



iManage
Making knowledge work

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.

☐ **Integrate chat communication with your document management system.**

If using a chat tool like Microsoft Teams, integrating it with your document management system will allow your firm to save important communications along with other matter documents.

☐ **Ensure that client communication remains secure.**

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

iManage
Making knowledge work

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