II. Before the Assessment

In this section, there is a discussion on what firms can do to prepare for a technology assessment to ensure efficiency and mitigate potential roadblocks.

Securing Funding

Firms can expect that a technology and security assessment done by a vendor will cost approximately $35,000 to $75,000, depending on the size of the organization and the services requested. This estimate accounts for the payment to the vendor and does not include costs of managing the assessment within the organization (e.g., funds for staff participation, a project manager, meeting time, etc.). This is a sizeable, though necessary, investment; thus, most firms apply for funding outside of their usual channels. Below are a few options to pursue when trying to find funding.

LSC's Technology Improvement Project Grant (TIP)8

The Legal Services Corporation (LSC) has funding available for certain LSC grantees[9] to support technology infrastructure improvement projects. According to LSC, this award is "intended to provide funding for appropriate consulting services to conduct a technology assessment, information security audit, business process improvement, or technology planning process." The maximum amount of these grants is $35,000. Project funding is for either 12 or 18 months. Applications are available on GrantEase, which is LSC's online grant management system. Applications historically have been due in May. See the TIP Category Application

Guide for more information.

Other Grantor Funding

Non-LSC funded organizations and organizations requiring more funds than the $35,000 available through TIP grants will need to look for other sources of funding for their technology assessments. The following resources may be helpful in the search for funding:

- **IOLTA**: State-based Interest on Lawyer's Trust Accounts--- or IOLTA--- is a program adopted in the early 1980's that uses the pooled interest collected on lawyer's trust accounts to fund a variety of civil legal aid causes. More information on IOLTA funding can be found at https://iolta.org/ A list of IOLTA programs by state may be found at https://iolta.org/program-directory/#us-programs .

- **Cy Pres and State Bar Foundations**: Cy Press distributions are residual funds in class action cases that are unclaimed or unallocated for any number of reasons. These funds may then be distributed by the courts to appropriate charitable causes, including legal aid organizations, under the Cy Pres doctrine. Cy Pres awards are often awarded to state bar organizations who may allocate this funding to civil legal programs.

- **State and local government**: Firms seeking additional funding should contact their state bar organization for more information on grants and available funding.

- **NLADA**: The National Legal Aid & Defender Association (NLADA) is a non-profit organization dedicated to increasing legal aid agency's access and capacity to "apply for, receive, and manage federal grant programs that target low-income populations and allow legal services to fulfill program goals." In an effort to build legal aid capacity to secure federal grant funding, NLADA has developed a resource list featuring federal grant opportunities for legal aid programs which can be found at https://legalaidresources.org/ .

Choosing a Vendor

sment, several factors need to be carefully considered to ensure a successful and valuable assessment. Here are some key points to keep in mind:

- **Expertise and Experience**: Look for vendors with a proven track record of conducting technology assessments for legal aid firms and non-profits of a similar size. Prior experience with legal aid can provide valuable insights into the unique technological needs and challenges of non-profit and grant-funded law firms.

- **Understanding of legal aid technology**: Legal aid firms tend to use case management systems that are not used by the legal industry as a whole. Ensure that the vendor understands the specific compliance requirements for legal aid organizations (e.g., LSC requirements, confidentiality requirements, etc.). The vendor should be familiar with the types of software the firm uses, data security requirements of the state and industry, and confidentiality concerns.

- **Cost and budget**: Assess the cost of the vendor’s services and whether these services align with budget constraints. Keep in mind that the cheapest option may not provide the best value.

- **References**: Ask the vendor for references from previous and current clients in the same field and of a similar size to gain an understanding of the vendor’s previous work and client satisfaction.

- **Customization**: The vendor should be able to articulate how an assessment will be customized to the size or type of legal aid organization and the kinds of technology used.

- **Security expertise**: Although the firm may be seeking a technology assessment separately from a security audit, given the sensitive and confidential nature of legal information, the vendor should have a strong background in IT security.

- **Clear deliverables**: The vendor should outline what the assessment will include —and, importantly, what it will not include — while also providing a clear plan for delivering assessment results, recommendations, and actionable insights.

- **Communication skills**: The vendor should be able to explain complex technical concepts in a way that is easy for non-technical stakeholders to understand.

- **Project management**: Discuss the vendor's approach to project management and the allocation of project management tasks throughout the assessment.

- **Time Commitment**: Ask the vendor to articulate the organization's time commitment will be. Below are some questions to consider:

- How many staff will be required to participate?

- How much time does the vendor anticipate requiring from the staff?

- Will certain staff be required to commit more time than others (e.g., Executive Director/CEO, administrative staff, IT staff, tech committee staff, "tech-responsible" staff, etc.)?

- **Future-focused**: A valuable vendor will be able to identify current issues and provide progressive recommendations that align with the organization's larger goals and technology trends.

- **Flexibility**: Ensure that the vendor will consider the firm's schedule, staffing, and other requirements when creating and adjusting the project schedule.

- **Confidentiality and non-disclosure**: Keep in mind that in most states, lawyers are responsible for supervising non-lawyer legal assistants. Vendors must ensure that clients' confidential information

is adequately protected.[10] Ask the vendor what security protections are in place to protect client and firm information, how credentials will be transmitted and stored securely, and whether/how information will be destroyed after the project is completed.

How to Prepare for a Technology Assessment

After securing funding and selecting a vendor but before beginning a technology assessment, it is recommended to do the following:

1. Identify a project team.

2. Prepare a priority/needs assessment.

Each of these steps will be discussed in-depth below.

Identify a Project Team

A technology assessment is a significant undertaking. Organizations should prepare by identifying select staff or designating a project team that will be made available throughout the process to guide the assessment, make decisions, and help the vendor access the information and resources needed to complete a successful assessment. As part of identifying a project team, some organizations may benefit

from forming a technology committee or leveraging an existing one. (However, in some programs, small staff size, limited capacity, or other challenges could mean a technology committee would not be feasible or a prudent use of staff time).

The Tech Committee

Forming a technology committee involves bringing together individuals with diverse expertise to guide technology decisions, strategies, and implementations, and to bring forth staff technology needs. If the firm already has a technology committee, this group is a good place to start for planning the tech assessment. If the firm does not have a technology committee, one should be convened. Keep in mind that the group can be scaled up or down depending on the size and needs of an organization. The tech committee should be comprised of the following staff:

- **CIO/vCIO or CTO**: The firm's Chief Information Officer (CIO), virtual Chief Information Officer (vCIO), or Chief Technology Officer (CTO) is responsible for overseeing the firm's overall technology strategy, infrastructure, and operations.

- **IT Manager/Director**: This IT professional is responsible for managing the day-to-day IT needs of the firm. Many firms have an IT Director or a CIO/vCIO/CTO but may not have both.

- **Upper Management/Administration**: A high-level representative of the firm's leadership can provide insights into the firm's strategic goals, business priorities, and financial considerations.

- **Practice Area Representatives**: Attorneys from different practice areas can provide input on how technology aligns with the specific needs of each practice and how it can improve client service and case management.

- **Operations Manager**: Staff from the operations team can monitor how technology fits in with the firm’s operations, workflows, and processes to ensure that it integrates seamlessly and enhances efficiency.

- **Financial Representative**: If the upper management/administration representative does not have a solid understanding of the firm’s finances, it can be helpful to have someone from the finance team who can provide input on budgeting, cost-effectiveness, and the financial implications of technology decisions.

- **Compliance Officer**: A member of the compliance team can weigh in on grant and funder requirements as well as firm needs surrounding data privacy and security.

- **Support Staff**: Support staff, including legal assistants, paralegals, and secretaries should be included on the committee to provide insights into existing needs and challenges.

- **Change Management Specialist**: If the firm has a staff member responsible for change management, this person should be included to manage the transition to new technologies, ensuring the staff adapt to these changes smoothly and effectively.

- **“Tech/Computer Responsible People”**: Many firms have one or more tech or computer responsible people (“TRP”s or “CRP”s) from each office to assist with technology troubleshooting within the office if there is no IT staff on site. These individuals should be included on the tech committee to represent the IT needs of each office.

Creating a well-rounded tech committee comprised of key staff from each of the areas of expertise listed above ensures that decisions will be made that benefit all areas of an organization. Technology assessments— before, during, and after— may impact the function of each of these departments. Including key staff in the decision-making process ensures that changes are implemented smoothly and effectively.

The Project Manager

While the technology assessment vendor should have a solid project management plan available at the beginning of the project, an internal project manager should be appointed to ensure the availability of firm resources and to guide the project through to a successful outcome. This person can be the point of contact with the vendor and should be responsible for the following:

- **Planning and Scope**: The project manager should work with the internal team and the vendor to monitor the scope, objectives, and deliverables for the project. The project manager should also be involved in helping the vendor create a detailed project plan that outlines tasks, timelines, milestones, and responsibilities.

- **Resource Allocation**: The project manager should be responsible for ensuring that the appropriate resources are available for the project. These resources include personnel, tools, and budget.

- **Coordination**: The project manager should act as the central point of contact between the internal assessment team, the vendor, and other stakeholders.

- **Timeline Management**: The project manager should ensure that the project stays on track and help identify potential delays.

- **Risk Management**: The project manager can identify potential risks and challenges that might arise during the assessment and develop strategies to mitigate these issues.

- **Documentation**: The project manager should work with the vendor to oversee the documentation of changes to internal processes that will come out of the assessment.

- **Stakeholder Engagement**: The project manager should engage with key stakeholders within the firm to elicit input and ensure any concerns are considered throughout the assessment.

For more information on Project Management, see LSNTAP's Project Management Toolkit.

Prepare a Priority/Needs Assessment

Once a project team is identified, organizations should consider conducting a priority or needs assessment to identify and highlight organizational goals for the technology assessment. Although technology assessment projects may include

surveying staff to gather feedback on technology, training needs, and pain points, this preparatory step will lay the foundation for a successful technology assessment process and ensure that the technology assessment project scope aligns with the identified goals and priorities.

Rather than a needs assessment that focuses on substantive issues or client populations, a priority/needs assessment in this context (i.e., preparing for a technology assessment) focuses on the organization's goals and objectives to improve its delivery of legal services and the use of technology to serve clients. When engaging in a technology assessment project, this type of information would be useful to communicate with vendors during the project kickoff or when scoping the project.

Examples of Identified Needs or Priorities May Include:

- Improving security policies and practices.
- Implementing a hosted phone system.
- Streamlining document management.

A sample technology self-assessment is below. Firms should review the information below ahead of a formal technology assessment and can also use the tool to do reviews in between formal assessments.

Technology Self-Assessment for Legal Aid Providers[11]

Instructions:

1. For each area, assess your current technology status.

2. Outline specific actions and strategies for improvement in each area.

3. Identify the areas with the most urgent needs and prioritize them for immediate attention.

4. Develop an action plan for technology enhancement and allocate resources accordingly.

5. Regularly revisit this assessment to track progress and adapt to changing needs.

Sample Tech Assessment for Legal Aid Agencies

Area of Assessment	Sub-Area	Considerations
IT Infrastructure		

	Hardware	• **Inventory all hardware, note anything missing, damaged or outdated.** • **Ensure that default credentials on routers, modems, printers, IOT devices, etc. have been changed.** • **Note warranties and ways to contact support.** • **Develop a plan for retiring equipment. Implement secure data destruction practices to prevent data breaches through discarded documents or hardware.** • **Ensure that servers and other hardware are protected from heat, water, and unauthorized access.**

	Software	• **Review security features of the software, including data encryption, user authentication, and access control.** • **Assess whether the software complies with data privacy or other regulations.** • **Ensure that software applications receive regular updates and security patches.** • **Evaluate the availability of user training and support resources available.** • **Verify that the firm has appropriate licenses for all software used.** • **Ensure that software applications have reliable data backup and recovery mechanisms in place.** • **Ensure that the software complies with legal industry standards and regulations, including those related to legal ethics and client confidentiality.**

	Network	• **Document the current network topology, including hardware devices (routers, switches, firewalls), network segments, and interconnections.** • **Review security measures in place, such as firewalls, intrusion detection and prevention systems, and antivirus software.** • **Assess the strength of network access controls, including user authentication and authorization mechanisms.** • **Ensure that sensitive data transmitted over the network is encrypted, particularly when accessing client information.** • **Evaluate network monitoring tools and procedures to detect and respond to unusual network activity or security threats in real-time.** • **Review remote access solutions (e.g., VPNs) to facilitate secure access for remote and mobile staff.** • **Assess network redundancy and failover capabilities to minimize downtime in case of hardware failures or network disruptions.** • **Monitor network performance to ensure that it meets the**

	Security[12]	• **Understand what data the firm is storing and classify it based on sensitivity. Differentiate between public, internal, sensitive, and confidential data to determine appropriate security measures.** • **Implement strict access controls to ensure that only authorized personnel can access sensitive data (e.g., human resources and employment data).** • **Use role-based access controls (RBAC) to assign permissions based on job roles.** • **Enforce strong, unique passwords and use multi-factor authentication (MFA) whenever available.** • **Employ endpoint security solutions (e.g. antivirus software, endpoint detection and response) to protect devices from malware and data breaches.** • **Implement secure file-sharing solutions that allow secure, controlled sharing of documents and data with clients and within the firm.** • **Ensure that employees are not using unsanctioned/unsecured file-sharing platforms for confidential data.**

	Data Backup	• **Regularly back up data and test data recovery processes to ensure business continuity in case of data loss or cyberattacks.** • **Check backup frequency to ensure that critical data is backed up regularly (real-time or daily).** • **Review the types and security of backups in use, such as full backups, incremental backups, differential backups, on-prem, or cloud. Consider a combination of backup types for efficiency, redundancy, and flexibility.** • **Examine where backup data is stored – in a secure location, separate from the primary data source, to protect against physical disasters or theft.** • **Confirm that backup data is replicated and stored off-site to safeguard against site-specific disasters like natural disasters.** • **Ensure that backup data is encrypted both in transit and at rest to protect it from unauthorized access.** • **Ensure backups of software being used.**

Case Management System		

	Security	• **Implement role-based access controls (RBAC) to restrict system access based on user roles and responsibilities.** • **Enforce MFA.** • **Implement secure user authentication mechanisms to verify the identity of users before granting access to the CMS.** • **Review the vendor’s encryption policies of data in the case management system.** • **Ensure that the system maintains detailed audit logs of user activities within the system.** • **Ensure that documents and case files stored within the system are secure and that access is restricted to authorized personnel only.** • **Regularly back up case data and develop a robust data recovery plan to minimize downtime in case of data loss.** • **If the system allows for SMS texting outside of the system, ensure that staff know how to use the SMS feature and are aware of the security risks of communicating with clients in this way.**

	Integrations	• **Assess the security measures implemented by the integration to protect sensitive data. Ensure it complies with legal ethics requirements.** • **Verify that data transmitted between the CMS and the integration is encrypted and securely stored.** • **Evaluate the level of support and maintenance provided by the integration vendor. Ensure that they offer timely updates, bug fixes, and customer support.** • **Assess how the integration handles data backup and recovery.** • **Confirm that the integration complies with legal and industry-specific regulations, especially those related to data privacy and confidentiality.** • **Clarify ownership and control of data within the integration. Ensure the firm retains control over its data.** • **Develop an exit strategy in case the integration no longer meets the firm’s needs or if the vendor discontinues support.**

Document Management		

	Document Storage	• **Use document management systems (DMS) with access controls and versioning to track document changes and maintain data integrity.** • **Implement encryption for data at rest and in transit to safeguard documents from theft or interception.** • **Verify that the document storage solution complies with the legal ethics requirements.** • **Implement a data classification system to categorize documents based on their sensitivity and apply appropriate access controls accordingly.** • **Maintain detailed access logs and audit trails to track who accessed which documents and when, facilitating compliance and incident investigation.** • **Develop a backup and disaster recovery strategy to prevent data loss and to ensure business continuity in the event of hardware/software failures, data corruption, or natural disasters.** • **Evaluate the search and retrieval capabilities of the document storage system. It should allow for efficient document location and retrieval.**

	Version Control	• **Implement version control mechanisms to track changes to documents and ensure that the latest version is always accessible.**
	Collaboration Tools	• **See LSNTAP's Collaboration Toolkit for further consideration.**
Legal Research Tools		
	Access to Legal Databases	• **Review whether staff have access to significantly robust legal research tools and legal databases.** • **Ensure that users are regularly trained on legal research best-practices and the potential for malpractice liability.**
Client Communication		

	Email Encryption	• **Ensure that email encryption is available for times when it is prudent for staff to use; for example, when sending privileged documents or those containing confidential and/or sensitive information.** • **Assess whether the encryption solution is easy to use and integrates seamlessly with the existing email platform and other communication tools.** • **Look for features that allow for auditing and reporting of email access and encryption activities.** • **Ask the vendor where it stores your email data and review the applicable data protection laws in that jurisdiction.** • **Ensure that users are trained on when to use encrypted email and how to use it.** • **Determine how encrypted emails are retained and archived, keeping in mind the firm’s data retention and destruction policies.**

	Secure Client Portal	• **Assess the portal’s security features, including encryption, access controls, and MFA.** • **Evaluate how user-friendly the portal is. Consider that many clients will need to access the portal using mobile devices.** • **Define user roles and access permissions to control who can view, edit, and upload information within the portal.** • **Ensure that the portal maintains logs of user activities.** • **Implement backup and recovery procedures to safeguard client data in case of data loss.** • **Clarify with the vendor data ownership (should be retained by the firm) and client data portability rights.** • **Confirm that the firm’s data will be returned if the firm switches portal providers or discontinues use.**

	Virtual Meetings	• **Ensure that the platform offers robust security features, including encryption, meeting passwords, and waiting rooms.** • **Assess whether the platform will be easy for clients to access and use.** • **Confirm that clients will be able to access the platform via their mobile devices and without having to download software.** • **For more, see LSNTAP's Collaboration Toolkit.**
Cybersecurity		

	Employee Training	• **Regularly train staff on the firm’s security policies and procedures, including incident response plans, data breach response, and acceptable use policies.** • **Regularly train staff on cybersecurity best practices, cybersecurity threats, and their roles in maintaining security.** • **Emphasize the importance of recognizing and avoiding phishing attacks.** • **Train employees in strong password creation and password management and the use of MFA and SSO.** • **Consider periodic security testing, including phishing simulations and vulnerability assessment.**

	Firewall and Antivirus	• **Ensure that all devices are protected with up-to-date endpoint security.** • **See LSNTAP's Security Toolkit for more information.**
	Incident Response	• **Investigate suspicious activity immediately. Do not wait for the problem to worsen.** • **Review the firm's incident response plan (or create one if one does not exist) to ensure that it is comprehensive, up-to-date, and aligned with industry best practices.** • **Ensure that employees are aware of how to report a suspected or confirmed incident and what an incident might look like.** • **Be prepared to comply with legal requirements for notifying affected parties in the event of a data breach.**
IT Budget and Planning		

	Budget Allocation	• **Budget for technology and security assessments.** • **Review and keep up to date the inventory of the firm’s technology assets, including hardware, software, and infrastructure.** • **Use the inventory to identify areas that currently need or will need upgrades or replacement.** • **Assess the need for infrastructure upgrades and use this assessment to budget for future upgrades.** • **Allocate sufficient funds for robust data backup and disaster recovery solutions.** • **Set aside budget for compliance and risk management services.** • **Consider purchasing cyber insurance to provide protection in the event of a data breach or other cyber incident.** • **Allocate budget for ongoing training and education for staff.** • **Review vendor contracts and budget for software licenses, support contracts, and other technology-related services.**

	Technology Roadmap[13]	• **While engaging in the technology assessment process, firms should create a technology roadmap that aligns with the firm's goals, enhances efficiency, and maintains security and compliance.**
Compliance and Regulation		

	Compliance regimes: Rules of Professional Conduct, GDPR, etc.	• **Ensure that the firm's technology systems and practices comply with the rules of professional conduct that apply to the firm's jurisdiction(s), including the duty of technological competence.[14]** • **Make sure that confidential client information is secure and that only authorized employees have access to that information.** • **Ensure that staff know how to use the firm's technology (likely the case management system) to properly check conflicts and which staff can ethically make conflict decisions per the jurisdiction's rules of professional conduct.** • **If the firm holds data of clients in California (CCPA), the European Union (GDPR), or other places with privacy regulations, ensure that the firm is handling that data in accordance to those regulations/law if they apply to the firm.**
Policies and Plans		

	User Policies	• **Review and update network usage policies, including acceptable use policies and policies for accessing and sharing client data.** • **Review and update remote work policies and ensure that remote workers follow security protocols.** • **Review and update policies on use of artificial intelligence (AI), especially when it comes to confidential client information.**
	Business Continuity Business Recovery	• **Check that there is a comprehensive plan that outlines the steps to restore data and systems from backups in case of a disaster or data loss incident.**
	Incident Response Plan	• **Develop an incident response plan outlining procedures to follow in case of a data breach or security incident.**

	Data Retention Destruction Policy	• **Define data retention polices and regularly review and delete data that is no longer needed in accordance with those polices.**
	Onboarding and Offboarding Policies	• **Have clear procedures for giving and revoking access to data and systems when employees join and leave the firm.**
	Security Policies	• **Develop and document comprehensive data security policies and procedures that cover all aspects of data protection.**

---

8. Legal Services Corporation. (n.d.). Technology Initiative Grant Program. https://www.lsc.gov/grants/technology-initiative-grant-program

9. Grantees of LSC Basic Field-General, Basic Field-Migrant, or Basic Field-Native American grants that are not subject to short-funding (less than one year) on the basic field grant

award. https://www.lsc.gov/grants/technology-initiative-grant-program/how-apply-technology-initiative-grant

10. See ABA Model Rules of Professional Conduct 1.1 (competence), 1.6 (confidentiality), 5.3 (non-lawyer legal assistance).

11. **DISCLAIMER**: This technology self-assessment tool has been developed as a resource to assist law firms in evaluating their technology infrastructure and practices. It is intended for informational purposes only and does not constitute legal advice or a professional opinion. Use of this tool does not create an attorney-client relationship with LSNTAP or Just-Tech, LLC. The information provided should not be construed as legal advice or a substitute for consulting with qualified professionals. Technology landscapes are constantly evolving. The information provided may not reflect the most up-to-date best practices or requirements. This tool is used at one's own risk and LSNTAP and Just-Tech, LLC. make no warranties or representations regarding the accuracy, completeness, or suitability of the tool for any particular circumstance.

12. See LSNTAP's Legal Aid Security Toolkit

13. A technology roadmap is a strategic tool used by organizations to outline their technology-related goals, objectives, and initiatives over a specific period. https://www.sciencedirect.com/science/article/pii/S0040162503000726?via%3Dihub

14. See ABA Model Rules of Professional Conduct 1.1 (competence), comment 8.

Last updated on January 11, 2024.

Print

Table of Contents

NEWS

News & publications

The news about recent activities for needed peoples.

More News

17 Dec 2024

Call for Speakers: Project Management, Second Chance Conference Sessions, and More

LSNTAP is planning our training sessions for 2025 and would like to hear from…

Continue Reading

11 Dec 2024

Resources for Supporting Child Victims & Witnesses Available

Passing along this message from the Center for Justice Innovation (https://www…

Continue Reading

Our Partners

MAP | MICHIGAN ADVOCACY PROGRAM

LSC | America's Partner for Equal Justice

LEGAL SERVICES CORPORATION