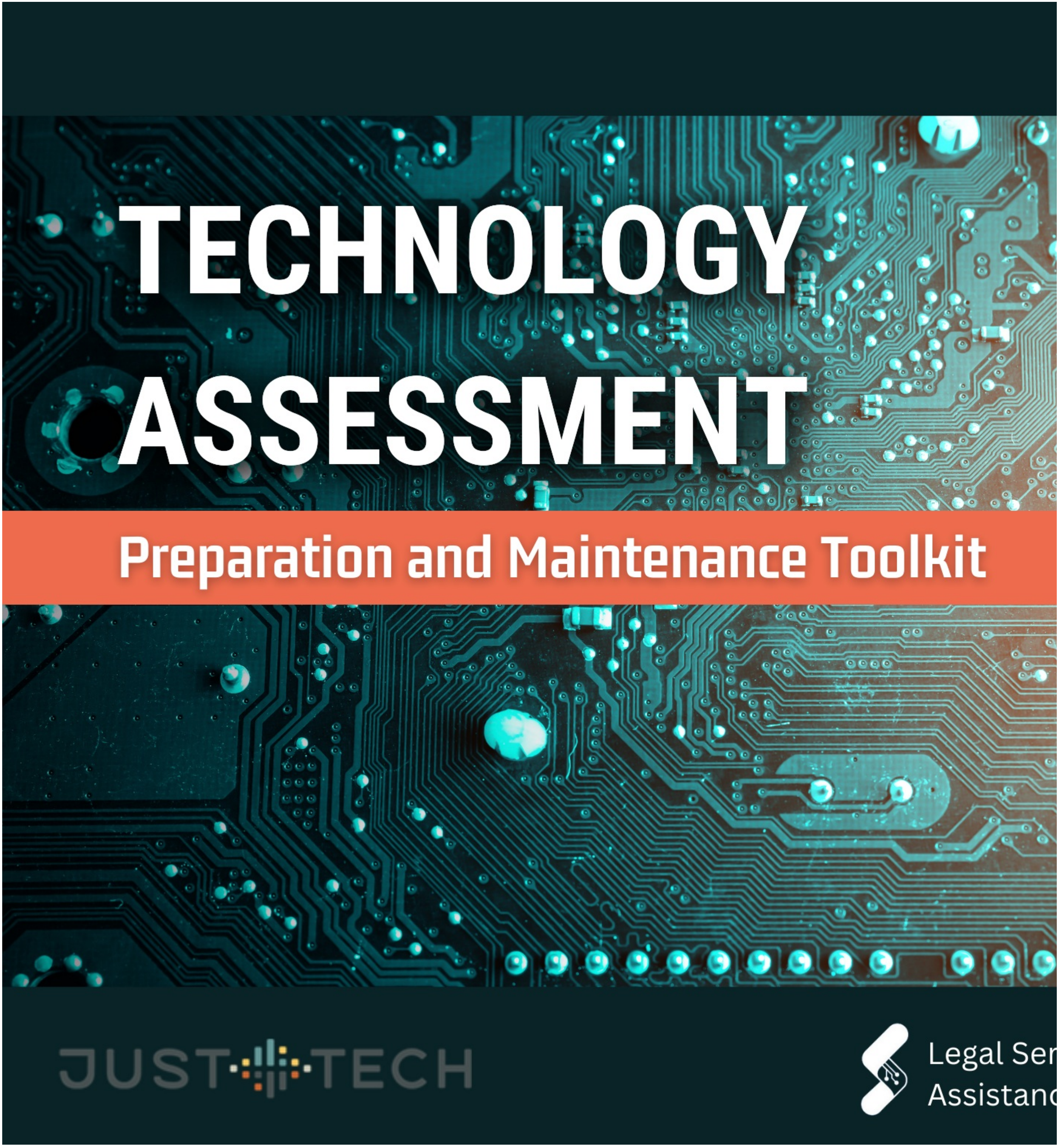
Technology Assessment Preparation and Maintenance Toolkit

Submitted by GravityWorks on Fri, 02/14/2025 - 11:42 AM



Introduction

How to Use This Toolkit

This toolkit is designed as a resource that offers guidance and actionable insights for legal aid programs seeking an enhanced understanding of technology assessments. Its intended audience is legal aid IT staff, executives/management, or tech-responsible staff who may be planning for a technology assessment, are unfamiliar with technology assessments within the legal aid context or are interested in learning more about the added value of assessment projects.

For IT staff, this toolkit may be used to coordinate with management to ensure adequate internal capacity and resources for a successful technology assessment. Executives and management can utilize this toolkit to gain a high-level overview of the assessment's significance, thereby enabling informed decision-making and resource allocation. Tech-responsible staff involved in the judicious planning of technology assessments will find valuable strategic insights and best practices. By tailoring information to suit different roles and levels of expertise, this toolkit aims to facilitate a collaborative approach to assessing technology effectively within legal aid firms.

How is This Toolkit Organized?

Information is broken down into the following sections:

What is a Technology Assessment?: Understand how a technology assessment is defined for the purposes of this toolkit and how it differs from a security audit and internal assessment.

Before the Assessment: Learn suggestions that will help in preparing for an assessment. Examples include securing funding, assessing vendors, and conducting internal efforts to prepare the firm.

During the Assessment: Gain familiarity with what to expect throughout a technology assessment and what is generally in the scope of an assessment.

After the Assessment: Plan for suggested next steps following completion of a technology assessment project, action that should be taken during the interim periods, and building a culture of continuous improvement.

Toolkit Description

The layout of this toolkit is intended to guide the reader throughout the stages of a technology assessment— from the preparation leading up to the assessment to the work that follows once an assessment is completed.

Disclaimer

This document is provided for informational purposes only. Users of this document must recognize the critical significance of IT security. Law firms should engage qualified vendors to ensure proper implementation of any technology and security recommendations. The authors are not accountable for any adverse outcomes resulting from misapplication; by using this document, readers accept that the authors bear no liability. It is the firm's responsibility to seek skilled personnel and unbiased IT recommendations. This document does not establish a client-consultant relationship.

I. What is a Technology Assessment in the Legal Aid Community?

Submitted by GravityWorks on Fri, 02/14/2025 - 11:46 AM

Technology Assessment Defined

A technology assessment generally involves a comprehensive evaluation of an organization’s current technology use, Information Technology (“IT”) infrastructure and systems, hardware and software, security practices, and policies and procedures. This resulting report should identify the firm’s IT strengths and areas where improvement is needed, recommend solutions, and provide a plan for implementation or a roadmap for improvement.

The Legal Services Corporation (“LSC”) recommends that legal aid organizations conduct an external assessment at least every three years, which can be broad or focused in scope, based on current initiatives or needs. A technology assessment is typically conducted by an external vendor or consultant and is an important step towards ensuring that an organization’s technology environment is properly designed, maintained, and managed to better support the delivery of legal services and program operations. Additionally, assessments can take into consideration trends and developments in the legal aid technology community and legal aid budget constraints.

While the timeframe and scope for technology assessments may vary depending on firm size, staffing, and funding, organizations that undergo a technology assessment project can expect the assessor to:

- Assist provider leadership in better understanding the existing technical environment and capacity.
- Inform providers of major security or business continuity risks uncovered through the discovery and data gathering process.
- Develop specific hardware, software, and service recommendations which can inform a roadmap plan to address critical needs and may be rolled into provider technology plans.
- Identify opportunities to make significant infrastructure improvements in an economical fashion.
- Benchmark performance on some of the core technology baselines established by LSC.
- Gain insight into support, engineering, and IT management needs.
- Analyze and report on any additional specialized systems or technologies as requested by the provider (e.g., case management, document management, accounting systems, enhanced security audits, penetration testing, and web services).

How is a Technology Assessment Different from a Security Audit?

Technology assessments and security audits are two distinct projects that organizations often deploy to evaluate existing technology infrastructure and security practices; however, key differences exist between the two. A technology assessment is a broad evaluation of an organization's overall technology environment. Its primary focus is to examine the efficiency, performance, and suitability of the technological systems in place to meet an organization's objectives. Security audits involve the use of a suite of commercial and proprietary tools to perform an assessment of a firm’s network at both the systems and network level.

Key aspects of a technology assessment process and report may include:

- Assessing health, reliability and redundancy of existing systems and equipment.
- Reviewing IT-related policies, procurement processes, technology plans, technical documentation, network infrastructure, hardware inventory, software inventory, and backup procedures.
- Using discovery methods (e.g., staff interviews, surveys, etc.) to understand and document current staff usage of systems (e.g., Case Management, Document Management, Phone System) across an organization.
- Evaluating areas for technology updates and upgrades.

Key aspects of a security audit process and report may include:

- Configuration and systems level vulnerability review.
- Security posture assessment to assess the status of a firm’s security measures, policies, and procedures.
- Network security audit to review all network infrastructure and systems accessible through the internet.
- Vulnerability assessment to determine systemic weaknesses in a security system.
- Penetration testing, or a simulated cyberattack, to help identify and fix what vulnerabilities and weaknesses exist within a system.
- Phishing testing or training to help staff better identify and report spam and potential security compromises.

Succinctly, a technology assessment focuses on the overall efficiency of technology and alignment of technology with business objectives, while a security audit provides a detailed analysis of the organization's security posture and potential vulnerabilities and risks. Both evaluations are essential for organizations to ensure that existing technology structures function optimally and that security practices remain up to date.

Internal Assessment vs. External Assessment

Although this toolkit does not address internal assessments in depth, the tools below cover a breadth of considerations that organizations should review before conducting an assessment. The following sections primarily cover external assessments. Understanding the distinctions between internal and external approaches is essential for making informed decisions that align with organizational goals and resource capacities.

An internal technology assessment involves using an organization's own resources, such as IT staff or an in-house Managed Services Provider (“MSP”), to evaluate the current technology landscape. This approach offers the advantage of familiarity with an organization's specific needs, workflows, and challenges. Internal assessments can be cost-effective and expedient, leveraging in-house knowledge to identify opportunities for optimization and improvement. However, potential drawbacks include limited objectivity as internal teams might have an interest in maintaining existing systems and the risk of overlooking blind spots due to pre-existing familiarity with the technology landscape.

External assessments, on the other hand, entail enlisting the expertise of third-party vendors, technology firms, or specialists to evaluate an organization's technology infrastructure. This approach offers a fresh perspective, unbiased evaluation, and specialized insights that may be overlooked internally. External assessments can surface hidden inefficiencies, identify cutting-edge solutions, and align strategies with industry best practices. It is crucial to thoroughly vet and select reputable partners to ensure the credibility and relevance of the assessment.

The decision between internal and external assessments depends on an organization's financial resources, time constraints, internal expertise, and the complexity of the technology landscape. Small legal aid programs with limited budgets may find internal assessments more feasible, while larger organizations with intricate systems could benefit from the specialized insights of external experts. In some cases, a hybrid approach that leverages internal expertise in collaboration with external vendors may offer more robust insights by combining institutional knowledge with fresh perspectives.

Ultimately, the choice between internal and external assessments is a strategic one that requires a comprehensive understanding of a firm's goals, challenges, and available resources. By carefully considering the pros and cons of each approach, legal aid programs can embark on a technology assessment that paves the way for more efficient, effective, and technologically empowered services.

LSC Baselines and ABA SCLAID Standards

What are the LSC Baselines?

As part of a broader commitment to enhancing the quality of legal services, LSC— in conjunction with various stakeholders and both LSC-funded and non LSC-funded organizations— has developed a set of technology capacities, or Baselines, that its grantees should have in place.

These Baselines are intended for use by any legal aid organization that provides a full range of legal services and are used by LSC as a guideline for its regular review of grantee program quality assessments. First launched in 2006, the LSC Baselines were updated in 2008, 2015, and again in 2023.

The most recent updates to the baselines in 2023 emphasize the importance of current and secure technology and how to best integrate these technologies into new and existing systems within the office. The full LSC Baselines may be found at https://www.lsc.gov/i-am-grantee/model-practices-innovations/technology/resources.

What are the ABA SCLAID Standards?

The American Bar Association's (ABA) Standing Committee on Legal Aid and Indigent Defense (SCLAID) has promulgated standards to guide legal aid organizations in their provision of high-quality legal services to clients. The standards were revised in 2021 and can be found at http://ambar.org/legalaidstandards. The SCLAID Standards are considered aspirational, but some funders do use them as a baseline measurement for firms seeking funding.2

The 2021 changes to the SCLAID Standards updated many of the standards related to technology, particularly regarding how clients now use technology.3 According to the new standards, legal aid organizations must consider the effects on clients of technology tools used by advocates and by tribunals.4 Advocates should aim to integrate the technology systems they use with those used by the courts and administrative agencies to enhance client experience while working more efficiently and preserving confidentiality.5

The revised standards also focus on safeguarding client data to prevent its misuse and to ensure that clients are aware of the ways that their data is being used by the organization.6 Further, the standards discuss the implications of the use of artificial intelligence (AI) and how it might affect clients.7

How can a firm use the Baselines and SCLAID Standards to prepare for a technology assessment?

Firms should use the Baselines and the SCLAID Standards as benchmarks upon which to measure technological health. By reviewing conformity with these aspirational standards, firms can identify areas for improvement and make informed decisions about technology investments.

Note: Security audits may also be referred to as security assessments.

Reference Material:

1. American Bar Association. (2021, August). Standards for the Provision of Civil Legal Aid Standing Committee on Legal Aid and Indigent Defense; Vail, J., Cassidy, J., Ehman, M., & Powell-Boudreaux, L. (2021). The Revised ABA Standards for the Provision of Civil Legal Aid. Management Information Exchange Journal, Winter 2021, 15-21, 55.
2. ABA (2021, Standard 4.10 on Effective Use of Technology, p. 154); Vail et al. (2021, p. 17)
3. ABA (2021, Standard 4.10 on Effective Use of Technology, p. 154); Vail et al. (2021, p. 17)
4. ABA (2021, Standard 4.10 on Effective Use of Technology, p. 154); Vail et al. (2021, p. 17)
5. ABA (2021, Standard 2.2 on Effective Leadership and Standard 4.10 on Effective Use of Technology, pp. 50, 157, 159, 186-87); Vail et al. (2021, p. 17)
6. ABA (2021, Standard 2.2 on Effective Leadership and Standard 4.10 on Effective Use of Technology, pp. 50, 157, 159, 186-87); Vail et al. (2021, p. 17)

II. Before the Assessment

Submitted by GravityWorks on Fri, 02/14/2025 - 1:32 PM

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 grantees9 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

When selecting a vendor to conduct a technology assessment, 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:

- Developing more centralized and efficient intake and referral systems.
- 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

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.

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 firm’s needs.
- Review the security of the firm’s wireless network.
- Evaluate the firm’s policies for employee-owned devices (BYOD) connected to the network.
- Ensure that network data is regularly backed up and that there’s a reliable disaster recovery in place.
- Allocate a budget for network maintenance, upgrades, and security enhancements.
- Periodically conduct penetration testing and vulnerability assessments to identify and address security weaknesses.

Security12

- 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.
- Conduct regular security awareness training for all employees to educate them about cybersecurity risks and best practices.
- Train staff to recognize and report suspicious activities.
- Assess the security practices of third-party vendors and service providers, especially those handling client data. Ensure vendors comply with data security standards and regulations.
- Conduct regular compliance audits.

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.
- Restrict access to backup data to authorized personnel only, following the principle of least privilege.
- Maintain comprehensive documentation of the backup strategy, including backup schedule, retention policies, and recovery procedures.

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.
- Review the security of any third-party integrations or plugins used with the CMS to prevent vulnerabilities.
- Provide training to users to educate them about security best practices, such as avoiding phishing emails and protecting login credentials.
- Develop and test an incident response plan outlining procedures for responding to security incidents, data breaches, or system compromises.
- Conduct regular security audits and assessments of the case management system to identify vulnerabilities and ensure ongoing security.
- Ensure procedures are in place for revoking system access when users leave the firm or their roles change.

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.
- Clarify ownership and portability of data within the document storage solution to ensure that the firm retains control over its documents.
- Decide whether to opt for cloud-based document storage or an on-premises solution.

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.
- Account for ongoing maintenance and support costs for hardware, software, and infrastructure.
- Set aside a contingency fund for technology-related expenses.
- Develop a multi-year technology budget plan that accounts for anticipated technology advancements.

Technology Roadmap13

- 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

III. During the Assessment

Submitted by GravityWorks on Fri, 02/14/2025 - 1:47 PM

This section provides an overview of the common steps, scope, and expectations or a technology assessment. Organizations may find that a security audit is included as part of the technology assessment; the specifics of a security audit and what to expect can be found here. The purpose of this section is to provide what is generally in scope for a technology assessment.

What to Expect from the Technology Assessment Process

The technology assessment process involves a series of systematic steps aimed at evaluating an organization's existing technology infrastructure, systems, processes, and needs. This process helps identify opportunities for improvement, strategic alignment, and the effective utilization of technology. Technology assessments generally include reviewing IT-related policies, procurement processes, technology plans, technical documentation, network infrastructure, hardware inventory, software inventory, and backup procedures. To the extent some needed information is non-existent or out-of-date, the technology assessment is the impetus for the development or updating of such documents. Although the process may vary depending on the vendor selected, organizations can generally expect the following:

- Discovery and Data Collection: Information and data gathering will be an essential part of understanding the organization's technology landscape to properly assess and provide well-informed recommendations. The vendor that is selected to conduct a technology assessment will likely have a few methods for its discovery process. Some examples may include any combination of the following:
- Inventory spreadsheet of hardware, software, networks, etc.
  - - Staff survey(s).
  - - Focus groups or interviews.
  - - Network scanning.
  - - Virtual or onsite visit.
  - - Policy/procedure review, if applicable.

Analysis/Synthesis of Information: After discovery is completed, the vendor will begin to analyze and synthesize the gathered information to gain insights into the organization's strengths, areas of improvement, inefficiencies, pain points, security concerns, etc. Based on the analysis, the vendor will also begin to identify gaps where the organization's technologies or technology use are not meeting organizational needs.

Report and Recommendations: Following completion of the vendor's discovery process and analysis/synthesis of information and data collected, there may be ongoing follow-ups to confirm findings, but report development will have begun. The main deliverable at the end of the project will be a report with specific recommendations and a final meeting with provider leadership to review the report, findings, and recommendations. Providers should consider the final meeting as an opportunity to raise any questions and receive guidance from the vendor on how to best review the report and any other materials provided.

IV. After the Assessment

Submitted by GravityWorks on Fri, 02/14/2025 - 1:50 PM

The report and presentation provided by the technology assessment vendor is just the beginning of the technology assessment process. Firms must be dedicated and prepared to address the issues that have been identified in the report, a process which could take days, months, or years. The firm must be prepared with staff and a budget to tackle the most immediate challenges. Firms can look to vendors for assistance and additional support that may be needed to develop new or updated technology plans, implement select recommendations, or train existing technology staff.

The first step after the assessment has been completed is to identify and agree upon a list of issues that need to be resolved. The list should be comprehensive and should be ranked by urgency. Security issues will need to be resolved immediately, while other issues, like minor technological annoyances, can be put near the bottom of the list. The technology assessment vendor should be able to help prioritize issues.

After the list of issues has been completed and agreed upon by key stakeholders, IT staff should research the costs of fixing each item (by priority) and estimate how long these fixes will take. For larger issues that require more than a few weeks to fix, IT staff should identify milestones to serve as checkpoints to track progress and ensure that the project stays on track.

Once these steps have been completed, the real work begins. Technology maintenance and improvement is a continuous process (see Building a Culture of Continuous Improvement below) and must remain a top priority for the firm in order to protect clients and employees. The technology committee should continue to meet regularly throughout the process of fixing the issues identified in the technology assessment and should continue to meet occasionally after the issues have been resolved to ensure the firm's technology remains a priority.

What to do Between Assessments

Formal technology assessments led by a vendor can be expensive and firms will likely not be able to perform one every year. Firms should plan to engage a vendor in a formal assessment as frequently as possible, and every five years at a minimum. In between technology assessments, the firm should engage in a variety of activities to ensure that their technology strategy remains effective and aligned with organizational goals. Using the Technology Self-Assessment Tool above annually is a good place to start.

Here are some other things firms should do:

- IT staff and leadership should monitor emerging trends, technologies, and threats.
- Regularly elicit feedback from clients and staff regarding their use of the firm's technology.
- Continuously review and update cybersecurity measures and compliance protocols.
- Encourage and celebrate staff's safe, efficient, and creative use of technology.
- Regularly review vendor privacy and contractual agreements.
- Train staff often on efficient use of technology and cybersecurity threats.
- Keep a technology budget and ensure that updates to technology are part of the firm's long-term planning.
- Review technology use to ensure that it conforms to any new or updated laws or regulations.
- Use the LSC Baselines as a guide to determine what the firm's technology priorities should be.

Building a Culture of Continuous Improvement

Effective collaboration is essential, both for conducting a productive and useful technology assessment, and for continuing to improve and expand upon a firm's existing systems. Building a culture of continuous improvement is critical to provide better services to clients, increase efficiency, and enhance overall program performance.

A culture of continuous improvement must come from leadership. Firm leaders much be committed to and visibly support a culture in which technology is respected and embraced but continually reviewed as well. Leadership must define a clear set of values that emphasize the importance of continuing to improve client services and how technology can be harnessed to do so.

Leadership should encourage all employees, including lawyers and support staff, to actively participate in identifying areas for technological improvement. Firms must provide ongoing training and development opportunities to ensure that employees have the necessary technological skills and knowledge to protect client information and provide excellent client services.

Firms should establish feedback mechanisms, such as regular surveys or technology meetings, to gather input from clients and staff regarding their use of technology. Data collected by the firm should be used to identify areas of improvement or inefficiencies that have the potential to impact client services most significantly.

Managers should consider adding technological competence and use to performance reviews and encourage staff to continue their improvement of that use via incentives like firm-wide shout-outs or small gift cards. Firms should celebrate and communicate successful improvements.

By implementing these strategies, firms can create a culture that values and prioritizes continuous improvement, ultimately benefiting clients, employees, and the organization as a whole.

V. Conclusion

Submitted by GravityWorks on Fri, 02/14/2025 - 1:52 PM

To properly protect client and employee information, while providing high quality and efficient legal assistance, legal aid firms can no longer treat technology as an afterthought. The legal aid community faces unique challenges, particularly when it comes to budgeting and client access. By leveraging the information in this toolkit with a thorough technology assessment from an outside vendor, firms can take critical steps towards addressing technological hurdles.

Keep in mind that technology assessments are not just about compliance; they are about leveraging technology to better serve the community. By embracing the principles outlined in this toolkit and collaborating within the organization and with other similarly situated organizations, legal aid providers can harness the power of technology to enhance legal services and fulfill their missions.

IT professionals, legal aid leadership, and other technology-responsible staff members should explore the tools and resources provided here and reach out to the broader legal aid community for support and to share experiences. Together, providers can empower each other with the tools they need to thrive in an ever-evolving technological landscape.

Tools and Resources

Resource	Links
TechSoup Sample Assessment	https://assessment.techsoup.org/
LSC Needs Assessment	https://www.lsc.gov/i-am-grantee/model-practices-innovations/plan-strategically/comprehensive-needs-assessment-priority-setting