

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

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 Audit¹?

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.

1. Security audits may also be referred to as security assessments

2. 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.

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 4.10 on Effective Use of Technology, p. 154); 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)

7. 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)

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

