



Law Enforcement Software Solutions

Focused On Results™

Detailed Agency Technology Assessment (DATA)

The DATA Process

Is your agency fully taking advantage of technology to achieve its mission? Has your agency ever reviewed the state of its IT infrastructure? Is the existing infrastructure functioning properly and can it support any future upgrades? What technology improvements can be made that will assist in achieving agency goals and objectives?

Law Enforcement Software Solutions uses a simple and straightforward yet detailed process that provides a comprehensive review of your agency from an IT perspective. The Detailed Agency Technology Assessment, or DATA, looks at 37 areas (see below) of your organization and how they are affected by your existing IT technology. We ask questions like:

- What are your agencies goals and objectives?
- What IT systems do you have in place?
- Are they working successfully?
- What general “pain points” relative to IT issues can you identify?

Those are just a few examples of the more than several hundred questions that are included in the DATA. We customize and tailor each DATA to suit your organization by asking questions relevant to your agency.

The 3 Stages of the DATA Process

Stage 1: The Interview

The interview is a fact finding process that is typically held at your location with representatives from Law Enforcement Software Solutions and your key players, usually your department or agency head, designated representatives and existing IT staff (if any).

An in-depth interview is then conducted on numerous issues including (but not limited to) IT infrastructure, security, networking and communication. The amount of time spent on the interview depends on the complexity of your organization.

Stage 2: Analysis

Law Enforcement Software Solutions then compiles the information gathered during the interview process, reviews and interprets the information.

Stage 3: Executive Report

A comprehensive report detailing the current state of your technology environment is prepared and presented to the law enforcement executive. Appropriate recommendations are also outlined in the report based upon the information provided and gathered throughout the process.

We won't leave you out in the cold after stage 3. Law Enforcement Software Solutions can work with you to formulate an implementation plan, coordinate with vendors, and assist with project management.

The costs associated with the DATA process are minor compared to overall project costs and the risks involved with unsuccessfully implemented solutions.

Introduction to DATA

The Detailed Agency Technology Assessment (DATA) allows an executive from Law Enforcement Software Solutions to assess your agency's Information Technology (IT) status in most functional areas and compare them to industry accepted "Best Practices."

The assessment in turn gives you a detailed look at where your IT investment dollars are currently being spent, and perhaps more importantly, where they should be going relative to your agency's goals and objectives. The DATA also uncovers areas of concern, both those known and unknown to your management. This review provides you with a proactive opportunity to review whether your agency is at risk for downtime due to hardware failure, software issues or problems stemming from ineffective security measures.

The current DATA process is an interactive tool, used in a conversational environment to interview you and your IT staff. Following the interview, the Law Enforcement Software Solutions executive provides you with a written recap of the information collected including a network diagram and a priority list of any "critical" issues you may want immediately addressed. A three year IT plan is also provided as a tool to achieve longer term goals.

DATA Subject Areas

The DATA process covers 37 areas of concern. The total assessment encompasses multiple questions in each section which are customized and tailored to your organization.

The areas investigated are:

1. Client Information
2. Agency Demographics
3. Key Personnel
4. Vision and Strategy
5. Current IT Layout and Landscape Overview
6. IT Experience, Staff Resources, & Support
7. Major Agency Projects-Ongoing/Upcoming
8. Regulatory or Compliance Issues
9. Lifecycle Management
10. Agency Purchasing Process
11. Primary Pain Points
12. Agency Strengths
13. Agency Weaknesses
14. Agency Opportunities
15. Agency Threats
16. Business Processes, Policies and Procedures
17. Communication Methodology
18. Business Continuity and Disaster Recovery
19. Internet Presence
20. Hardware
 - a. Servers
 - b. PC's
 - c. Printers
 - d. Fax Machines
21. Software
 - a. Operating Systems
 - b. Applications
 - c. Licensing
22. Network Infrastructure
23. Connectivity, Internet, and Email
24. Wireless
25. Network Storage
26. Power
27. Technology Management
28. Security
29. Internet Use
30. Spam, Malware, and Anti-Virus
31. Backup
32. Proactive Maintenance and Monitoring

- 33. Patch and Service Pack Management
- 34. Data Storage
- 35. Mail Storage
- 36. Remote Access
- 37. Training

DATA Areas of Emphasis

During the DATA process, particular emphasis is placed in the area of Security. Within the subject of Security, the following areas are closely examined to minimize risk and liability:

- **Written Security Policy**
 - A written security policy is fundamental to network security and must be written, maintained and communicated to employees. The policy should be structured to address the security/liability of the agency while balancing the privacy/morale of the employees. A security policy should include (at a minimum) access, data, content, email and employee training. Failure to do so may leave your agency vulnerable to outside intrusion or harm from disgruntled employees.
- **Overall Network Vulnerability**
 - We have tools available to check vulnerability at your network's firewall as well as your agency's servers, workstations, email messages and remote users. Security audits can range from testing for current virus protection to comprehensive intrusion detection audits. While most security breaches are internal in nature from existing employees, some are external and can result in a loss of data without your knowledge.
- **Password Policy**
 - Hackers intent on penetrating your network are often skilled at using pretexts to obtain password information from your employees by posing as IT professionals, security personnel, etc. and convincing them to divulge username, password, or other access information. Password policy should extend to IT as well and should encompass forcing password changes, utilizing "strong" passwords, managing administrative passwords, etc.
- **Anti-Virus Software**
 - The issue of computer viruses is well known to many. The installation of anti-virus software can prevent viruses, worms, and/or trojans from entering your system and potentially destroying valuable data or hardware. In addition to proper installation, these applications require systematic and regular updating to address the latest threats. Many agencies that have anti-virus software are found to underutilize it.
- **Configuration of the Mail/Proxy Server**
 - This issue is not only addressed in the context of security, but productivity also. Employees are spending more time than ever

communicating with colleagues and members of the community via email and performing research over the Internet. These necessary and valuable systems need to be supported and made responsive as possible. A correctly set up mail server will support your current users, allow for growth and be properly configured for security related issues. Email should be correctly distributed and backed up as many users consider their message stores and contact databases to be as important as their applications. In addition, a proxy server can monitor your employee's Internet usage and/or restrict access to web sites with objectionable content and those affecting bandwidth to assist in mitigating risk and liability.

- **Disaster Recovery Plan**

- Every agency experiences security breaches, most of which are minor in scope. Few agencies take the time to fully research, analyze and document these to prevent reoccurrence, provide legal indemnification or even verify that access isn't continuing. From running port scanning software to verifying removable media has been "cleaned," how a company recovers from a breach is nearly as important as preventing it.

For more information on the DATA process or to see how Law Enforcement Software Solutions can assist you in achieving your technology goals, contact us at **626.389.3939** for a **free initial consultation**.