

Technology Assessment Profile (TAP)

The TAP Process

Have you reviewed the state of your company's IT infrastructure? You're probably thinking, "why bother"? Everything is running OK and there are too many more important issues to deal with right now. Unfortunately, you could be overlooking some potentially significant problems.

HBS uses a program that is quite simple and straightforward, but one that gives you a comprehensive review (both positive and negative) of your company from an IT standpoint. The Technology Assessment Profile, or TAP, looks at 22 areas of your organization (see the TAP Overview) and how they are affected by your existing IT technology. We ask questions like:

- What IT systems do you have in place?
- Are they working successfully?
- What general "pain" IT issues can you identify?
- Do you have a network security program?

Those are only a few of the several hundred questions included in the TAP. However, we will tailor the TAP to your organization, asking you questions relevant to your company.

The 4 Stages to the TAP process

STAGE 1: The Interview

This interview is typically held at your location, a meeting with a HBS engineer and your key players, usually your company owner or department manager and existing IT staff. They are the best to know what you have and what you are missing.

It is an in-depth review of numerous issues, including your IT infrastructure, security, networking and communication. The amount of time it takes depends on the complexity of your organization.

STAGE 2: Compilation

HBS formalizes reviews and interprets the information obtained during the interview.

STAGE 3: Status Report

Very soon after completing the interview, HBS presents you with a comprehensive report detailing the current state of your technology environment.

STAGE 4: Recommendations

HBS makes recommendations based on the prepared report.

We don't stop at Step 4. HBS can work with you to determine an implementation plan, perform the installation or upgrade, troubleshoot if necessary, and follow up to make sure the work meets or exceeds your expectations.

The costs associated with a TAP are minor compared to the headache you could end up with by not reviewing the status of your company's IT program. Let HBS help you sort it all out.

*For additional information on the TAP Process, contact HBS.

INTRODUCTION TO TAP

The Technology Assessment Profile (TAP) allows HBS to quickly baseline your company's Information Technology (IT) status in most functional areas, and compare them to industry-accepted "Best Practices".

This assessment gives you the customer 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 business objectives. The TAP 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 business is at risk for downtime due to hardware failure, software issues or problems stemming from ineffective security measures.

The current version of TAP (TAP 6.0) is an interactive tool, used in a conversational environment to interview you and your IT staff. Following the interview, HBS provides you with a written recap of the information collected, and a priority list of any "hot" issues you may want immediately addressed. A comprehensive analysis and remediation plan is then typically provided as a follow-up.

TAP SUBJECT AREAS

The TAP process covers 22 areas, broken down into subsections. The total assessment encompasses multiple questions, which are condensed and tailored to your organization.

The areas investigated are:

- | | | |
|-----------------------|----------------------|-------------------------|
| 1. Client Information | 13. Communication | 17. Management & Admin |
| 2. VAR Information | a. PC's/Clients | a. IT Staffing |
| 3. Executive Summary | b. Servers/Networks | b. Network Management |
| 4. Introduction | 14. Mail Services | c. Training (clients) |
| 5. Current Situation | 15. Security | 18. Maintenance |
| 6. Desired Outcome | a. Data | a. Hardware |
| 7. Discovery | b. Physical | 19. Life Cycle Planning |
| 8. Applications | c. Hardcopy Material | a. Hardware |
| 9. Network Design | 16. Resources | 20. Internet |
| 10. Connectivity | a. Change Management | 21. E-Commerce |
| 11. Hardware | b. Host Networking | 22. Miscellaneous |
| a. PC's/Clients | c. WAN | |
| b. Servers | d. Printing | |
| c. Hubs/Switches | e. FAX | |
| 12. Software | f. Backup | |
| a. PC's/Clients | i. Services | |
| b. Servers | ii. PC's/Clients | |
| | g. Power | |
| | h. Disaster Recovery | |

EXCERPTS FROM A TAP AREA OF EXPLORATION

What follows here is an explanation for some of the components in one of the 22 sections of a TAP, Security. By including this, you will better understand why the areas covered in a TAP are so important to consider when developing a complete picture of your network.

Written Security Policy

A successful, comprehensive security policy must be written and maintained to reflect the needs of the company (security/liability of the company vs. the privacy/morale of the employees). A security plan must, at a minimum, address access, data, content, email and employee training. Failure to do so may leave your company open to external intrusion from outside hackers and/or competitors, vulnerable to harm from unscrupulous employees and legally liable for numerous issues.

Security training needs to be part of the new hire process and should also be reviewed at least annually with all employees.

Overall Network Vulnerability

HBS engineers have multiple tools at their disposal to check vulnerability at your network's "firewall", as well as at your servers, clients, email messages and remote users. Security audits can range from simple tests for current virus protection to comprehensive intrusion detection audits. While most security breaches are internal in nature (by existing employees) some are external, such that theft of data occurs without your knowledge.

The IT needs of your company, including location and type of public data and levels of Internet access necessary for your employees will drive the levels of security required by your network. HBS can assess your current level of protection and devise the most comprehensive means to secure your network assets.

Password Protection

Hackers intent on gaining access to your network are skilled at calling your company posing as IT professionals, security personnel, etc., and convincing your employees to divulge passwords and or access information.

Few people would give out their personal information over the phone to a stranger calling them at home, yet research indicates many will comply in the work environment. Password policy should extend to IT as well, in the form of forcing password changes, mandating more complex passwords, managing administrative passwords, etc.

Anti-Virus Software

Most people are aware of computer viruses. Having anti-virus software correctly installed on your system can prevent viruses, worms and trojans from entering your company. In addition to correct installation, these applications need systematic, regular updating to add new virus profiles and levels of protection. Many companies that purchase anti-virus software underutilize it.

Proper Configuration of the Mail / Proxy Server

This issue addresses not only security, but productivity as well. Employees are spending more time than ever online, communicating with your customers and suppliers via email and performing research using the Internet. These necessary and valuable functions need to be supported and made as responsive as possible. A correctly set up mail server will support your current users and allow for growth. Email should be correctly distributed and backed up, as many users now feel their message stores and contact databases are as important as their applications. In addition, a proxy server can not only monitor your employee's Internet use, but can also restrict access to a site containing objectionable content and/or sites that may interfere with company bandwidth.

Disaster Recovery Plan

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

Hardcopy Material

Most companies provide for the apparent destruction / disposal of their private records, yet don't actually verify the level of protection. Are your employees trained on separating private matter from general material prior to disposal?

A surprising amount of data ends up being disposed of without being properly shredded. Consider this: How much hardcopy material do you really need to print? Can a company Intranet or other formats such as Adobe Acrobat PDF™ be used to keep your "internal" information internal?

The areas above are representative of the questions TAP will review in your business. By conducting a careful and complete TAP, HBS can review and answer these questions (and more) with you and your staff, to begin establishing and maintaining a safe, secure and scaleable IT infrastructure!

For more information on the Technology Assessment Profile (TAP) contact us at:

Heritage Business Systems
13600 South Kenton
Crestwood, IL 60445
708-597-5005

www.hbspc.com