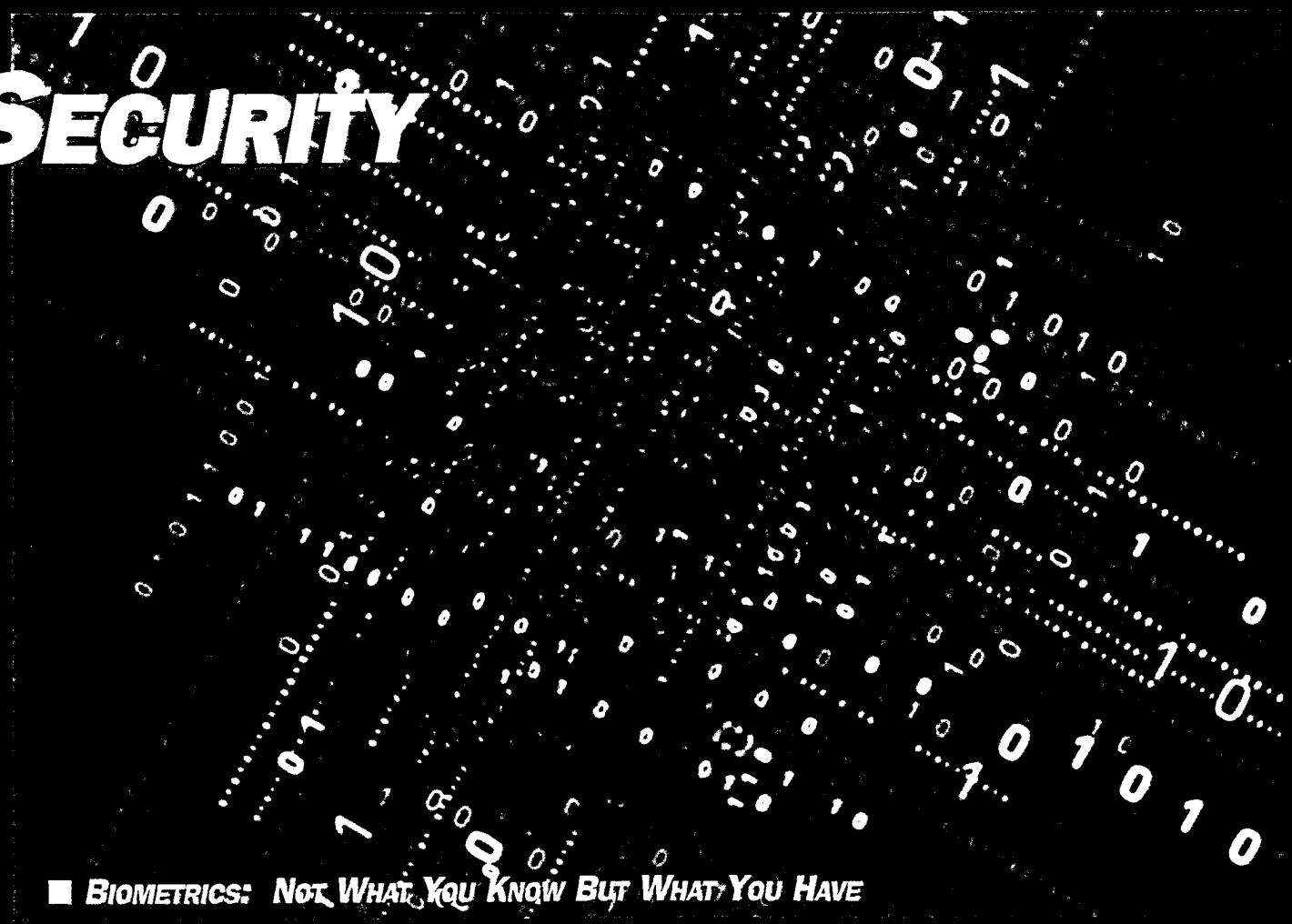
AWARD WINNING

IS AUDIT & CONTROL JOURNAL

VOLUME III, 1999



- BIOMETRICS: NOT WHAT YOU KNOW BUT WHAT YOU HAVE
- SECURING JAVA™
- SECURITY IN A PEOPLESOFT ENVIRONMENT

THE JOURNAL OF

INFORMATION SYSTEMS AUDIT AND CONTROL ASSOCIATION

Successful Audits in New Situations

By Jennifer Bayuk, CISA

Even the most technical of auditors will sometimes be assigned to an audit that is outside his or her scope of technical expertise. Though vendor manuals and interviews with auditees may be enough to get started, these rarely lead directly to the area of highest risk in implementation. This article provides strategies for successfully completing audits in areas where the auditor has little direct experience. It provides tips for handling the audit process when the auditor feels there is not enough information to adequately plan the Preliminary Data Gathering and Opening Meeting.

Approaching Unfamiliar Environments

Never go to the auditee as the first source of information about a topic. If it is discovered that an audit contains an unfamiliar topic while in a meeting with an auditee, politely refuse to discuss the approach until there has been a chance to familiarize yourself with the topic. This strategy will help avoid committing to an audit approach until there has been a chance to independently assess potential risks. It will also help avoid losing credibility from an auditee early in the audit process.

Yet before demurring from further discussion, it is important to obtain the correct spelling of the technical terms, products and vendor names. Also make sure to ask for full translations of any acronyms that are mentioned in connection with the topic. These small bits of information are essential to the efficiency of the discovery process. Many technical terms, acronyms, vendor and product names are similar. Say the topic is reliability in Electronic Data Interchange (EDI) and the auditee says they mitigate risks by using "ASN." ASN may stand for Access Stack Node, a fault tolerant router by Bay Networks. ASN may also stand for Abstract Syntax Notation, an International Organization for Standardization (ISO) standard used to maintain common data representation across platforms.

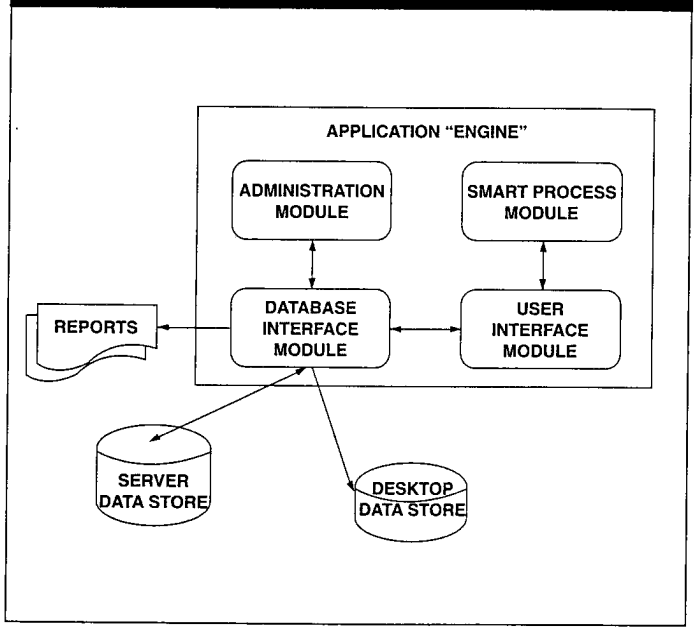
In addition, many vendors have multiple similar products in the same industry. Say an auditee says they are using Axent to "secure UNIX." Axent has a single sign-on product, an access control product, an administration-delegation product and a monitoring tool, all of which can be used to "secure UNIX." It is very disappointing to complete a few hours worth of research only to find you will be auditing a completely different product.

The best source of up to date information on technical environments is of course the Internet. In my experience, a search performed using *www.yahoo.com* has never failed to yield the web site for a technology company. On a vendor site, look particularly for a company's white papers concerning the product of interest. The white paper has its origin in university research lingo. Research conference organizers often ask potential presenters for white papers, 7-10 pages long, describing the history of the technology, and the researcher's contribution to the field. If the white paper was accepted, the submitter was given a slot on the conference agenda to introduce the research. Today, white papers are usually product marketing materials, but they do place the product in context. They generally describe what technical and/or business problem the product is intended to solve and how the product works.

For freeware or shareware products, try *www.exite.com* or *www.altavista.digital.com*. Try to find the web site that is maintained by the author of the code. It is bound to have more detailed explanations of how the technology works and what it was designed to do. If you cannot find the author, be biased toward sites that end in "edu." They are educational institutions and will sometime publish unbiased technical reports or white papers that describe the technology. If you find a site that seems authoritative, look for a "FAQ" page concerning the technology. FAQ stands for "Frequently Asked Questions." If the FAQ contain questions about the technology's control environment, it will also contain the answers.

Another type of Internet web site that offers an introduction to new technologies is the on-line subscription service. For example, *www.gartner.com* offers research on most types of technologies. For a yearly fee, subscribers may access documents that compare competing products in the same technology market. For the more widely-used products, they may even have an article describing both the technology and the company. In general, these types of reports do not yield enough detail to contribute to audit pro-

Figure 1: Application Engine



grams. Rather, they provide useful background information for understanding the technology in the context of business requirements.

Also useful, and better yet free, are Internet sites that allow archival searches through magazine articles. For example, *www.techweb.com* allows keyword search access to the past issues of many technical publications. These are useful for determining the maturity of the technology and for determining how other companies are implementing, or attempting to implement it. Sometimes research produces more acronyms than answers. If the product being researched has some component that is Internet-enabled, try searching for the acronyms at *www.rfc-editor.org/rfcsearch.html*. It contains the specification documents of the Internet protocol suite, as defined by the Internet Engineering Task Force (IETF) and its steering group (the IESG). The specifications are published as RFCs, or Requests for Comments. Vendors use these specifications to program their product to ensure compatibility with other vendor products using the same protocol. RFCs are dry reading, but do explain exactly how products work, assuming that the vendor has been true to the standard.

Preliminary Data Gathering

Once some background on the technology and business purpose for the product has been accumulated, the auditor has the start of a contextual, conceptual model. You have theory. The next step is to apply the theory to the actual environment to be audited. At this point, phone or email the auditee with specific questions about the architecture in the scope of the audit. (A face-to-face meeting may still be premature, as you are not prepared to address specific risks.) If research has yielded a generic diagram of the system then make use of it in this preliminary data-gathering session with the auditee. Mark up the generic vendor diagram to correspond to the installation under review (see Figure 1). If no diagram is available, instead create a list of alternative choices in implementation platforms. Checkmark the alternatives chosen for the installation under review (see Figure 2).

Each of these components will have its own set of associated risks. Check the vendor web page for a list of security patches. Use *www.cert.org* and *www.cs.purdue.edu/coast* to find out what security vulnerabilities may exist in each.

At this point, the auditor is ready to make use of a copy of the system manual. Many vendors now have their entire set of manuals available on their web site. If not, ask the auditee to borrow a set. Start with the administrator's manual rather than the user's guide. In that manual, there are install instructions, configuration instructions and user administration instructions. Install instructions indicate exactly which files were installed on each platform to make up the application. Configuration instructions show which files and programs control product customization. User administration instructions describe which information is stored concerning users, what options there are for segregating functions, and sometimes, where the user information is stored within the system.

At this point, research has revealed how the software is intended to be used and how it is used by other companies. Now the auditor has a good handle on the system architecture and operation from an administrator's viewpoint. The next step is to understand it from the point of view of the user. Consult the user manual to become familiar with the different modules that are available and the options for control strategies within those modules.

Figure 2: Example Options for Implementation

Operating System
- Microsoft Windows NT v4.0 (Server recommended)
- Service Pack 3 installed
- SunSoft Solaris v2.5
- SunSoft Solaris v2.5.1
- SunSoft Solaris v2.6
- IBM AIX 4.1.5
- HP-UX 10.x
- HP-UX 11.x

Database
- Oracle 7.3.4 [US English]
- SQL*Net v2.3.3.x.x.x.x
- SQL*PLUS or Server Manager
- SQL Server v6.5 with Service Pack 4 installed [US only]
- SQL net configuration
- Sybase Adaptive Server 11.5

Web Server
- Netscape Enterprise Server v3.5.1
- Microsoft IIS v3.0
- Microsoft IIS v4.0

Opening Meeting

After seeing the system from both the administrator and user point of view, the auditor can determine whether some of the existing audit programs make sense to reuse. The auditor can now schedule a meeting with the auditee and map out the scope of the review. At the very least, the auditor can apply basic standard auditing techniques to complete the risk picture. For example:

- What assets are controlled by the system?
- Is there an expectation that the amount or type of assets will expand with continued system deployment?
- How are users authorized?

In addition, the auditor can bring in knowledge of general risks that had been previously seen with components for the environment and ask how the technical implementation of this system addresses those risks. For example:

- Which options are you using in the user administration screen?
- How do you control direct access to Oracle?
- Do you have controls to prevent disclosure of data traveling through the corporate WAN?
- How are the UNIX files that were installed as part of the application protected from tampering after install?
- Do users have access to change configuration options on their desktop?

Do not be disappointed if all of your questions are not answered at the opening meeting. The opening meeting may be scheduled with the system's business sponsor or system support team. It is enough for them to know that you have these questions. The person that can answer these questions is the system engineer.

Some companies don't have a formal title for systems engineering work. So the person who engineered the system may actually be a developer, a project manager, or even an administrator. But it is important to seek the person who engineered the system for the local environment early in the process. This will be the person or set of people who decided:

- The operating system platform or platforms that would be used to house the system.
- Where on the network to position the system.
- How the customizable configuration options would be set.
- Whether to add on supplemental products or use customized development to meet any business needs not fulfilled by the core system.
- Anything else concerning the installation process or operation that was not the default provided by the vendor.

Consider the discussion with the systems engineer an extension of the opening meeting. Discussion with the system engineer may lead to abandonment of some assumptions initially held concerning potential risks that were based on the auditor's own experience in prior audits. If so, independently verify that the systems engineer's explanations are correct. The discussion may also lead to consideration of risks that were not apparent from research. The engineer may be in the process of addressing a particular risk and may need the auditor's support.

Out of this discussion will come an outline for audit steps. Specific risks associated with each system component should be identified and controls sought out. This process will produce an audit plan that makes sense to auditees.

Jennifer Bayuk, CISA
is associate director for corporate security at Bear, Stearns, & Co., Inc. Her responsibilities include policy development, security software evaluation and infrastructure monitoring. She has been a manager of information systems audit, a Big 5 audit manager and a software engineer. Jennifer has published on information security topics ranging from security process management to client/server application controls. She has lectured for organizations that include ISACA, NISSC and CSI. She has Masters degrees in Computer Science and Philosophy.