Rey LeClerc
GSEC Version 1.2e

Audit and Security Control Issues when Conducting Information Security Reviews

Introduction

Information security professionals must frequently perform risk analyses to determine the key control areas. These risk analyses usually reveal that that the security software package is an important control that should be carefully reviewed. Unfortunately, reviewing a security package can be a very challenging task without a framework within which to analyze it. Without a proper framework, overall security parameters may be overridden by security access privileges, or vice versa. Security access privileges give the use authorization of usage of system resources.

At the basic level, security packages permit or restrict access to a resource or facility. A resource can be a data file, a program or library, a terminal, or a hardware device. A security package can restrict access to a resource or facility during certain times of the day or week, track all activity when a particular set of circumstances occur, or allow selected individuals to bypass all security checking.

These restrictions are imposed through the use of the security package's control statements, or rules. Typically, the security administrator will code rules through an on-line monitor or submit them by way of a batch job to update a central rules file. The operating system allows the security package to interrogate the rules file and determine whether a particular access request should be granted.

The poor construction of security access rules can lead to:
v access of data and programs by unauthorized individuals;
v restricted access to authorized individuals;
v the accidental destruction of programs and data by authorized employees.

Detecting these conditions may be difficult if the IT security professional has no previous exposure to the security package. This paper is designed to assist the IT security professional in the creation of a plan for the review of in-house security packages.

The security environment review will detail elements to ensure that the environments in which the information security software is or will be operational have been clearly defined and are readily identifiable for purpose of resource and facilities protection with the information security software and to identify facilities not specifically protected and address potential control concerns therein.

Describing audit and control procedures will ensure that audit and control facilities available within the information security package have been tailored to the existing environment and ensure that formalized procedures are in place to perform adequate monitoring of access violations and dataset access to sensitive data.

Finally, the last area of the review is to discuss the potential common areas of exposure to the information security software.

The Need for Security

The evolution of information security has progressed slowly since the early days of computing. In the 1940s, 1950s and part of the 1960s security revolved primarily around limiting physical access to the systems. At that time, security of information was not perceived as a critical IT issue. However, in the 1960s attention started turning from physical security to the security of information. Since the 1970s the sophistication and changes of computers and telecommunications technology have intensified considerably. The productivity and general daily activities of institutions such regular business, government, and educational institutions depend greatly on the availability of large amount of data. Some of this data is of critical or sensitive nature for the continuing operation of the institution.

Today, thousands of institutions, businesses and individuals go online everyday with the advances of the Internet. As a result, the security of data has become one of the most critical issues in IT. Continued reliance on computing systems, together with dramatic expansions of end-user computer systems and networks, demonstrates that the sky is the limit for use of computer technology.

Information security is the protection of information integrity, confidentiality, and availability of data. There are a variety of reasons why information security is necessary. First, the growing trend of technological advances has made information more available to the end-users, and at the same time more vulnerable. Second, the consolidation of information in business, government, and educational data processing systems has increased the public's concern about the privacy and misuse of data. This public awareness about the weaknesses of information controls has been a major influence for legislation to address this issue. Some legislation passed as a consequence of the information security issue include the Privacy Act of 1974, the Counterfeit Access Device and Computer Fraud and Abuse Act of 1984, and the Computer Fraud and Abuse Act of 1986. Third, both government and private organizations which process sensitive data require that information be processed in a secure and well-controlled environment. In government, the need for security is a major concern since it is responsible for national security. Finally, information security is necessary because of human and physical threats. Data must be protected from human errors, dishonest or malicious actions of employees or outsiders ('hackers'), and malicious code such as 'virus', 'worms', and 'Trojan horses'. Additionally, information needs protection from damages that can be caused by incidents such as a fire, flood, and electrical failures.

Logical Access Controls

Modern systems allow the employment of a great variety of controls: manual controls and automated controls. In the past, manual controls, like physical security and administrative procedures, were prevalent. New systems use more automated tools and innovating technologies; therefore, today's systems, in addition to the manual controls, have been forced to rely extensively on software controls. Software can be tailored to direct users to use only the functions that they should perform, and protect valuable data from being used in a non intended manner. Such software-provided controls are called logical access controls.

When reviewing logical access controls requirements, it is important to remember that while the goal is to protect systems resources, it is also possible to overcontrol. To avoid such extremes, it is recommended that an installation plans and evaluates the requirements, sensitivity, risk, and potential exposures of the data available to users.

The site must identify all its resources and users by taking inventories of these two categories. Information assets must be classified according to their sensitivity and importance to the organization (e.g. confidential, restricted, internal use, unclassified). Users should be classified by different types of user needs (e.g., end-users, application programmers, system programmers, security administrators).

The classification methodology applied for resources and users should not be just performed at the beginning of the security implementation process and then forgotten. Data and user needs change for different reasons. Therefore, a structured mechanism is required to ensure that the classification rating remains current and correct. In short, a solid planning process is essential to ensure that an organization's logical access control meet its real needs.

Planning for Security

In order to establish logical access controls using any security software package there are a series of crucial aspects that need to be addressed. These aspects are:

Definition of a Information Security Function - Establishment of an information security function is one of the first steps that need to be specified after the global security direction has been defined. The individuals involved in this function should report directly to top management wherever possible. This will provide the function independence from other functional group within the organization. The person in charge of this function should be someone who is knowledgeable of information technology and security controls, has a high degree of responsibility, and is aware of all the political demands of the environment. Additionally, this individual should be a trusted and respected individual within the organization, must have good analytical, organizational and interpersonal skills. In addition to the security leader, other security administration staff need to be selected. These individuals will assist in the implementation and daily maintenance of security. Finally, the site must determine if the information security function will be a centralized or decentralize function.

Assign an Implementation Team - The implementation of security will require the effort of many individuals and areas of an organization. To direct and coordinate this project an implementation team should be created. It is recommended that this team be composed of representatives from information security, system software, application software, operations professionals, and end-users. There should be a project manager assigned to lead the group. Cooperation from the team members will be essential to their success. This group will be involved in activities such as the development of a security policy, standard and procedures, and a security implementation plan.

Definition of a Security Policy - This document should address security software issues, physical security, employee clearance and privacy of data. As a minimum, the security policy should cover the following:

v Security goals for the installation
v Scope of security protection
v Ownership of resources
v Responsibility for the integrity of resources
v Requirements to access resources
v Statement on how to handle security system activities and violations
v User accountability
v Account protection requirements
v Responsibility for the support and enforcement of the security direction

Development of Security Standards and Procedures - This involves the development of all security related standards and procedures such as naming standards, security maintenance procedures, testing standards, password handling procedures, violation handling procedures, backup and recovery procedures, and emergency and troubleshooting procedures.

Security Implementation Plan - This plan will provide the direction required for the implementation process. The plan should cover all the major tasks required to implement security. The plan should provide flexible schedules because the exact number of users, resources, and other factors are going to be unknown. The plan should emphasize critical security issues and applications and then cover less critical areas. A comprehensive listing of all tasks required should be developed considering independent versus dependent tasks. The basic components of this plan should include:

v Product installation
v Product testing
v Inventory of resources and users and exposure analysis
v Defining implementation strategy
v Security file design

- Definition of violation and reporting strategies
- Testing new security controls and features
- Customization of the security system software
- Security awareness programs
- Ongoing security needs assessment and evaluation

Information Security Software Administration Function

It is extremely important that the installation develops comprehensive security guidelines, policies and standards and procedures detailing resources that need protection, steps and measures required to establish and maintain security, and users responsibilities. Guidelines, policies and standards should be clear and precise. When they are extensive and complicated, users tend to ignore them. Users often resist attempts to restrict their work, therefore, control techniques should be effective, but at the same time practical, and easy to understand and use. All these guidelines should be formally documented and communicated to relevant personnel. The site should provide adequate training to motivate security awareness among their users. Users who understand the reasons and needs for controls are more likely to apply them at work.

In order to properly control the implementation and maintenance of the information security software, it is important that a security software administrator's role is established. A person, or persons, assigned to this role should only be responsible for the implementation, modification, monitoring and enforcement of access strategy and security that is developed by the company. The sole implementation of an access control package may provide a false sense of security. Security involves much more than implementing a security package. For this reason, the role of the security software administrator is essential.

In an installation, a security software administrator is the individual who has the responsibility to identify users, resources, and access to resources. The security administrator has several options to control the overall security. Security can be controlled in a centralized or decentralized manner. Centralized security administration gives an individual group control over the entire organization. Decentralized control gives functional groups within a company responsibility for their area.

Operationally, the site should be able to establish and enforce security requirements more easily if the implementation and maintenance of the rules is centralized. However, when the size of the data processing activities is too large, it may be necessary to decentralize some of the security functions.

The security function should be separated from the rest of the data processing organization since there is a tendency to apply application or system programmers design and control security. From a control point of view, allowing programmers to function as information security personnel is a breakdown in the desirable aspect of segregation of duties. It is important for an IT security auditor to understand the scope of the security administrator's authority and to determine how the rules are organized. Poor organization may lead to an inefficient maintenance environment and can result in conflicting access privileges being granted.

The security administrator's role is to act on behalf of the owners of the application and system files and libraries. Some of the areas that the administrator should be responsible for are:

- Developing a security implementation plan.
- Granting, implementing, and revoking access to the system according to the data owners' request.
- Allocating and withdrawing special facilities from the system users.
- Control over changes to the authorization established.
- Ensuring that changes and status of employees are appropriately reflected in their security authorizations (e.g. transfer of an employee from one department to another, termination of employees).
- Monitoring and following up on apparent attempted unauthorized access both successful and repeated unsuccessful attempts.
- Revoking privileges when apparent fraudulent or other unauthorized activity appears to be taken place. The security administrator should not have to wait to act until it is proven that unauthorized activity has taken place. He/she should have the authority to act first and ask questions later.

Additionally, it is important that the security administrator not be allowed to act unless appropriately authorized by the owners of the data. The administrator is acting as an agent on behalf of others. Unilateral decision on his/her behalf should be strictly forbidden. All activities performed by the administrator should be subject to the review and approval by the owners of the data and systems. The IT security professional should check authorized documents and signatures for changes made to access privileges. A change request or memo should support changes, and an authorized signature should be affixed to the request. In addition, all changes should be traced back to the security administrator that made the change and to the supporting request. Although some changes are made without formal paperwork, this should be the exception to the rule.

In general, the scope of the security administrators should be limited to only the resources and authorities required by them to perform their duties.

The access rules created by security administrators can lock-out unauthorized users and enforce division of duties among system users. Special attention should be given when security access rules are defined because if they are too strict they can severely affect productivity; however, if they are not strict enough, some resources might be inadequately protected.

When security officers define access rules, the different types of users need to be considered. Some general guidelines include:

- End users - Typically, they represent the largest class of users. They usually know about the system and have the most access to physical assets and data. In general, their access should be the most restricted. General end-users should not have access to programming and system function. Their access should be strictly limited to the resources needed to perform their responsibilities. The data owners (department user's management) have the ultimate responsibility of deciding what level of protection should be applied to their data.

- Application Programmers - Different from end-users, application users require access to programming and system functions to perform their duties. However, their access should be limited to the test programs and files required to perform their job assignments. They should not be granted access to production application programs and system libraries. Programmers should not have access to production files or any other production resources normally used by end-users. Their use of powerful utilities should be restricted and monitored.

- System Programmers - Systems programmers may be a special concern. Technical support employees are responsible for the maintenance of hardware and software. These individuals can gain access to practically all aspects of the system. Their activities must be restricted to the extent practical, and their work must be supervised. They should not have the access to production application libraries and production files, except for troubleshooting tasks. Whenever possible, their activities should be logged, and reviewed periodically. In general, their access should be limited only to the system libraries of the particular software that they maintain.

It is recommended that changes to the information security data bases be periodically reviewed by management. At a minimum, a sample of changes should be reviewed at a weekly basis and be properly authorized. Information security should require that all changes be properly controlled and they be supported by authorization from the owners. If all the changes have been properly authorized there should be a way of referencing the authorization when the changes occur. Information security data bases can be updated only by users with the appropriate security privileges. It is important that security officers review and actively follow-up potential problem using the logging and violation reports capabilities. Reviewing security changes will give the IT security professional an appreciation of the administrative controls over the usage of the security package.

The security officer or security administrator should routinely review changes made to the access privileges to verify that he or she has followed documented standards and procedures and to make sure that no one else has used the administrator's user ID. If there are decentralized security administrators, the IT security professional should also verify that documented standards and procedures are being followed.

Information security administrators have a responsibility to review the reports used for logging and violations. Primarily, logging should be reviewed to determine if there is any abuse of privileges granted. Additionally, if the logs are the result of the security implementation process, these logs should be reviewed to ensure the timely completion of such plans.

The violation should also be reviewed by the information security groups for several reasons. Violations are the result of failed attempts to access information. Information security should be using this as an indication of problems in information security administration to determine its effectiveness. They should also use these to determine if there was a breath of security. Trends in attempted access should be observed. A series of violations on sensitive data sets indicates a possible fishing expedition.

Information systems security professionals should make sure the security administrator review the violations log periodically and that a procedure exists to follow up on serious security violations. Unfortunately, in many cases, this procedure is often bypassed by an overworked security administrator because it can be boring and time-consuming. Some security administrators believe that the violations log review is meaningless because properly constructed access privileges will prohibit unauthorized access and improperly constructed access privileges will not create a violation. However, what many information technology security professionals fail to recognize is that without at last a cursory review of the violations numerous repetitive violations may go unnoticed, which may indicate that someone is trying to methodically hack at the established access privileges or that frustrated user is prohibited from performing a valid function.

Review of follow up procedures is important. If the security administrator merely reviews the violations log and takes no action, the review process is meaningless. In some cases, additional user training is necessary, whereas in others, the rules may be too stringent. The security policy should indicate the action to be taken against those users who intentionally violate the rules.

Some security package utilities and commands are also heavily used by IT security professionals when evaluating the controls implemented for the package. Periodic security reviews should be performed by information system security professionals to ensure that the package is being used to provide a secure system environment.

Packages Familiarity

When preparing for an audit, the IT security professional should to gain an overall understanding of the security package in detail. Most software vendors offer a training course for their software packages. If the IT security professional is not part of the initial training process, the vendor may offer standalone courses for an additional fee. Some third-party vendors also offer security package training. IT security professionals should be careful when selecting a course to make sure that they don't attend a training program that has prerequisites.

Another way to become familiar with a package is to attend national or local user group conferences and meetings. These meetings are usually sponsored by the vendor organized by users. IT security professionals group meetings are yet another place to attend a course or presentation on the package.

The security package may have an on-line tutorial or help facility. Although this may not be the most efficient way to become familiar with the package, it does offer the least costly way of doing so.

Auditing Tools

Some security packages have sections of the security manual devoted to auditing. This can provide an invaluable method for pinpointing the key areas of concern to an security professional.

The security professional's manual may contain a full-blown audit program. If it does, the IT security professional should carefully review the audit program, which will cut out of preparation time and make the results of the audit much more effective.

Some packages permit IT security professionals to run reports or view access rules on-line but prevent them from making any changes to the files. IT security auditors should have a broad a scope as possible to facilitate the review of the entire access rules file. In addition, the IT security auditor should obtain a copy of the applicable security policies, standards, and procedures. If no security policy exists, the auditor should recommend that one be developed and endorsed by top management.

Installation of Information Security Software

Security packages usually have overall default parameters that are put into effect every time the packages are started. The IT security professional should review these carefully to ensure that they are appropriate. One of the main items of concern is password administration. Password changes should be required periodically. The installation parameters should indicate that by default passwords must be changed every 30 to 90 days. Passwords for sensitive user IDs should be changed more frequently. This requirement is usually associated with the particular user ID in question and is set when the user ID is created.

A review of the password file is essential when reviewing information security software. The IT security professional should make sure that passwords cannot be listed from an unencrypted file and that common passwords (e.g., the current day or month, first names) are not being used. The practice of guessing password would result in the deactivation of the user ID after a predetermined number of invalid attempts.

Modes of operation are another item for installation review. Many security software allow for different modes to allow for easy implementation. Modes are extremely important because they dictate the type of resource made to security violations. Depending on which mode is being used, user's attempt to access unauthorized resources can generate warning messages or complete the user's action and log the violations. Different modes may be provided to allow installations to gradually implement system protection, while at the same time, provide the ability to secure critical resources.

If the overall mode that the package is not operating at its maximum, e.g. fail or abort, the tightest security rules in the world may be meaningless. A particular security rule may indicate that a type of action is prohibited, but if the start-up parameters indicate that no one is stopped from violating the rules, the action will be permitted.

General appropriateness of the installation parameters should be reviewed. The IT security professional should compare the installation parameters to the manual to determine how aggressive or passive the computer security program is at the company being audited.

Simply reviewing the system installation parameters may not always be sufficient. Some information system security professionals may be fooled into believing that the stringent parameters shown in the initialization file of the security package library are actually the same as those currently in use, when that is not the case.

The current parameters should be listed on-line and compared with the installation parameters. If they are different, the cause should be determined. The security administrator may have issued a command at the master console to temporarily modify one of the default parameters, or part of a daily or weekly procedure may include the automatic modification of these parameters.

If the current parameters are found to be different, the method by which they are changed should be carefully reviewed. For example, if an automatic procedure exists that allows parameters to be modified, the security professional should make sure that the only person that can change the automatic procedure is the security administrator. If the parameters were changed manually at the master console, the security auditor should ensure that only the security administrator has the authority to make changes.

Access Review

The IT security professional must do more than review parameters to understand the level of security in effect. As every security professional learns, things that appear on paper or on screen do not always work as they should. No audit would be complete without a thorough test of the access privilege rules to make sure that they are working properly.

The security professional should obtain access rules and draw an organization chart of the security rules. Security rules are usually written in a structured fashion along divisional or department lines. The organization chart will help the security professional to quickly visualize the structure of the rules file.

A review of the rules may identify multiple rules that were created for the same reason. These redundant rules make maintenance difficult for the security administrator because the removal of an obsolete rule may require the location and deletion of several independent rules. As the rule file grows, extraneous rules begin to hamper a through review of the file. The security professional should ensure that rules that apply across the board should be implemented in one place only.

One possible test is simulating resource access. Simulating resource access involves accessing the rules file - but not the resource - in a way that the security package still permits or denies access. This is the safest audit technique because the security professional can prevent the accidental destruction or disclosure of information and the security package can identify which rule allowed or denied access to the source. This is extremely useful for large files for which organized reviews are difficult and time-consuming. In addition, this technique allows the security professional to perform what-if tests to determine whether a particular access would be permitted or denied under a specific set of circumstances.

The security professional should attempt to update a production program or file to determine whether the controls are effective. If the security professional's understanding of the rules file is correct, the access will be permitted or denied in accordance with the predetermined analysis.

Another testing technique is attempting unauthorized access. Unless properly executed, attempting an unauthorized access could be the most risky of the auditing techniques. It is important for the security professional to obtain approval before attempting unauthorized access to a resource. If the access is successful, the security professional may have a hard time explaining that the access obtained was only part of a test. If the access results in the generation of a live monetary transaction or the destruction of a production file, the rapport built with the auditee may be destroyed. IT security professionals are in the position to learn many weaknesses in the security system and should not use this privileged knowledge without notifying the appropriate individuals.

Most packages give selected user IDs exceptional authority to override any security rules and parameters in place. The security professional should conduct a review of the individuals provided this exceptional authority and purpose of these exceptions.

One of the most basic reviews for the security professional to perform is that of user IDs that are allowed to bypass security checking. Although this authority is necessary, the IT security professional should determine whether the practice is prevalent and uncontrolled.

A listing of all user IDs that are authorized to bypass security should be generated by any utility program or report writer that can read the rules file. Although some system tasks may require security bypassing, it is not usually needed by users or programmers. Sometimes the capability is permitted while the security package is being installed and, because of oversight, it is not removed when the installation process has been concluded.

The security professional should ensure that an automated log of activities that are exempt from security rules is maintained. Because some can bypass security checking, a complete log of exempted activity is needed to ascertain how much of this activity has occurred in the past. The current level of exempted activity may not be indicative of past levels.

The security professional should determine the prevalence of exempt activity. If there are many user IDs that are exempt from security rules or checking, this is an indication of ineffective rules enforcement.

Certain security packages allow protection on a terminal basis. Critical application should be restricted to selected terminal on a need basis. Of particular concern is the usage of the system console.

The ability to make system changes is not always limited to the master console in the computer room. Permission to make console changes should usually be limited to the operations personnel. Any requests by the applications development staff or by the systems programmer should be carefully reviewed. If changes are permitted outside of the computer room, the identification of the command issuer should be logged by the system. The identification method should be active, rather than passive, to prohibit an unauthorized individual from issuing a command without proper identification. The only type of console commands to be issued should be restricted to those that require a job function to be performed.

The security professional should review the appropriateness of the authority given to each individual and recommend removal of those functions not needed.

Common Exposures

Most of the security packages do not guarantee that they can control all application systems, interface with all third-party software, or prohibit a knowledgeable technician from circumventing the rules that have been created. The IT security professional should determine whether these exposures exist and what controls have been put in place to offset or correct them.

Common exposures include the existence of conflicting security rules. Security rules can sometimes nullify each other. For example, one security rule may provide read-only access to a sensitive file, and another rule, which may take precedence, could provide update access to all files. Depending on how the rules are constructed, the rule that permits update access to all files may be used instead of the more restrictive rule. In this case, the security professional may believe that the rules are working in concert, when one rule actually supersedes the other.

Another item of concern is the ability to turn off security. Some system programmers have the ability to turn off security software at any time. Because this ability is necessary for systems testing, the computer system must sometimes operate without the security package in place. The sessions should be carefully monitored and controlled.

Most security packages interface with a third-party software package. However, some security packages must be told that the third-party software packages exist and viceversa. If these steps are not taken, the security software may not actually be in place. Testing the facility interface should detect this situation. In addition, the security manual and the third-party software manual usually provide details concerning the effective use of the security interface. The security professional should review this documentation if there is a question about the interface.

Unless an automated process has been created to remove terminated employees from the rules file, many user IDs of former employees may still be valid. The security professional should run a report that shows the user IDs that have not been used in a certain number of days. These IDs can then be automatically deactivated or matched to an active employee file to pinpoint problems.

Conclusion

The IT security professional should take the following steps to prepare for a security package audit:

- Obtain appropriate training and manuals. The security professional should allow sufficient lead time because some courses are offered only a few times a year and some manuals may be difficult to obtain.

- Use established audit programs and utility programs. Security professionals should become familiar with the terms and procedures used in conjunction with the security package.

- Obtain copies of rules, changes, and violation files and summarize overall trends and patterns by using charts or graphs.

- Develop a sound test plan. The security professional should develop an outline to establish a benchmark by which to compare results from audit to audit.

The adequacy of the information security software package depends on the integrity of the operating system to be intact. It is important that the information security software package access rules provide adequate restriction to the operating system libraries. The security professional should also conduct reviews of the operating system and the system programming unit to ensure that the security package cannot be bypassed. And, most important, the security professional should ensure that management indicates its commitment to sound controls through the issuance of security policies.

Because data is a valuable and critical asset for most companies, security software products like the information security software package must be carefully implemented and their controls be periodically reviewed to ensure the integrity of the system.

Bibliography

AuditServe. *System Software Product Implementation Review Methodology*. URL: http://www.auditserve.com/articles/asis3.htm

AuditServe. *Security Administration and EDP Auditing: Interchangeable Job Functions*. URL: http://www.auditserve.com/articles/art_2.htm

AuditServe. *Audit Serve Security Evaluation Criteria (ASSEC)*. URL: http://www.auditserve.com/articles/art_37.htm

Buck, John. *Introduction to Information security and Controls*, QED Information Sciences Inc., 1982.

Coopers & Lybrand. *Handbook of EDP Auditing*. Warren, Gorham & Lamont, Inc., 1989.

DeVoney, Chris. *Step Up Your IT Security*. August 22, 2000.
URL: http://www.zdnet.com/filters/printerfriendly/0,6061,2618285-92,00.html

Engel, Howerton. *Computer Security: A Management Audit Approach*, Amacon, 1990.

Enger, Normal L. *Computer Security*, Amacon, 1990.

Federal Financial Institutions Examination Council. *Information Systems Volume 1,* 1996 FFIEC IS Examination Handbook. URL: http://www.FFIEC.gov

Helsing, Cheryl. Swanson, Marianne. Todd, Mary Anne. *Computer User's Guide to the Protection of Information Resources*. URL: http://nsi.org/Library/Compsec/usergide.txt

Hutt, Arthur E. *Computer Security Handbook 3rd Edition*. John Wiley and Sons, 1995.

Leiss, John. *Principles of Information Security*, Plenum Press, 1992.

Holbrook, P. and Reynolds, J. RFC 1244: Site Security Handbook. URL: http://csrc.ncsl.nist.gov/secplcy/rfc1244.txt

Tipton, Harold. Krause, Micki Krause. *Information Security Management Handbook, 4th Edition*, Auerbach Publications, 2000.