Global Information Assurance Certification Paper

Considerations of Systems Access Control

Abstract

The intent of this paper is to provide an overview of vital considerations for implementing a Systems Access Control procedure. With information systems being the lifeblood of modern day business solutions, companies must ensure that the systems and information they use are kept confidential where required; information integrity is maintained at all times; availability of both systems and information is provided on an as is required basis. Achieving this goal will be more easily accomplished if you implement a structured process for granting access to your systems and system objects

Systems and system objects must be protected by making users accountable for their actions. Information must be safe guarded against accidental and malicious changes including changes and deletions of files and libraries; changes to registry keys and system parameters; adoption of higher user authority through various means. The **Handbook of Information Security Management, 1999** defines the intent of Access Control Systems as "The protection of the system and resident information against unauthorized disclosure, modification, or destruction." [1]

I have defined in my own words three terms which are the purpose of information security management today:

Confidentiality

The ability to protect information from unauthorized disclosure. That is, people only have access to that information for which they have been explicitly granted. Information is not available to unauthorized persons.

Integrity

Information is accurate and has not been modified to be misleading or to present a false notion or misrepresentation.

Availability

Systems and information are available on a timely basis. To define this further, resources are available and ready for use any time that they are required.

To design a Systems Access Control procedure, from now on referred to as SAC, several parameters must be defined:
1 – Policies must be written which define the allowable use of systems and information. I feel that the two most important policies pertaining to systems access are an Information Security Policy and an Acceptable Use policy.

[1] Krause & Tipton. Access Control Systems and Methodology, page 1

2 – Data ownership and classification must be considered and defined and data custodians appointed.

3 – User roles must be defined so that access can be granted based upon those roles. Some of the most common user roles are that of end users, programmers, system operators, and system administrators.

4 – An access request media must be created which will allow for three types of relevant access:
ADD for a new user setup or new object creation
CHANGE for additional or less access for an existing user or object
DELETE for removal of access from an employee who has been terminated or no longer has a requirement for system access. Also for the deletion of obsolete system objects.

5 – Access administrators must be appointed. These will be the people that have the daily responsibility for ensuring that users have the correct access to systems, system objects and information.

6 – Finally, an audit procedure must be established. The audit trail will provide confirmation that access has been granted as requested and has been approved through the proper channels. Regular access audits may detect discrepancies between the way things are and the way things should be.

I will now expand on each of these six areas; any one would make a good topic to write a paper on such as this, however for the context of this paper I will stick to a high level overview.

1 The policies written will play an authoritative role in deciding whether or not requested access is granted, therefore it is crucial that senior management has signed-off on any policy that has been created. This will be your assurance that you have management's approval to challenge requests that may introduce security vulnerabilities or do not conform to policy. As well as defining what is acceptable practice and usage it can be some times as important to explicitly define non-acceptable usage and behavior such as surfing pornography on the web, sending distasteful emails, or for storing personal data on company systems. A good resource for creating policies is available from SANS at www.sans.org/resources/policies. There you can find sample policies and primers for creating policies specific to your organization.

2 Data ownership and classification is necessary to ensure that information is available to only those groups of users who have been explicitly granted access. By categorizing data as Public Information, Company Public, Company Private or Secret Confidential, the data can be labelled and access granted accordingly. Users can then be assigned to predefined user groups which have appropriate access to each category of information. Assigning data owners and having those owners give final approval to access requests ensures that someone in a position of accountability is aware that access is being granted.

3 User roles need to be structured such that users only have minimal access, in other words, not more than is required to perform their job. Identification and authentication of users are necessary to ensure that the correct people are getting access to the required objects. A userid must be unique to an individual and provide accountability to that person. The authentication method must confirm that the user really is who they say they are. There are several authentication methods available, each of which involves one or more of the following criteria: something you have; something you know; something you are. A smart-card is an example of something you have; a password is something you know and a facial feature is something you are. Combining any of the three is a step towards layered security which helps ensure that your data is protected as well as can be reasonably expected. Anyone with even a bit of information security experience must realize that absolute security does not exist, therefore we as security professionals must strive to achieve a level of security that denies as much unauthorized access as possible while at the same time allowing authorized personnel to perform their jobs without restriction.

It is also vitally important to maintain segregation of user duties. Dividing responsibility for each step of a process helps ensure that no one individual gets enough privilege to work the system for his own benefit. For example, any person that can create a cheque or purchase order should not have enough authority to also approve the same. With such a segregation of responsibility, collusion would be necessary to commit fraud. Though many users see security as a necessary evil, they fail to realize that the same security that is restricting their actions is the same security that can prove their innocence during an investigation. If it can be proven that an individual did not have enough user privileges to access a system or resource then one can be confident that the suspected person was not involved in the alleged event.

4 When creating the SAC form it is important to use a media which is secure and cannot be altered at any time after the initial approval routing. You wouldn't want additional access to be requested on the form after it has been approved by the data custodian or designated approver for the department which is responsible for the data being accessed. The SAC could be a paper or electronic format but must be such that it can be preserved to provide an audit trail for future reference. As well the SAC should incorporate a secure notification method to advise the user's manager or designate that the requested access has been provided. Since this notification may include the userid and password it is crucial that the information not be intercepted by an unauthorized person. Such information could be used to gain access which is above that which a person is allowed. Privilege escalation would be beneficial to a user who wants to just 'look around' to see what he can get into or to a disgruntled employee who is looking to cause mischief or damage.

5 When appointing access administrators it will be beneficial to select people who have a sound understanding of the corporate environment and business strategy. The administrators must know what they are giving people access to and the impact of doing so. People from the helpdesk and operations usually

have a broad knowledge of the business environment and corporate culture, this makes them potential candidates for the position of systems access administrator. In '**Handbook of Information Security Management, 1999**' the authors Micki Krause and Harold Tipton concur that "Proper technical training is considered to be perhaps the single most important safeguard in reducing human errors."[2] I have observed that technical training without a sound understanding of security essentials is of only half value in effecting a secure computing environment and may even present more risk than value. Administrators must understand the impact of their actions from a security perspective. The most important step you can take when appointing access administrators is to ensure that those people get the proper training for them to form a solid understanding of information security: not only theoretical knowledge but the ability to apply that knowledge in the real world. As cyber attacks become more complex and sophisticated it is more important than ever to ensure that your security department can recognize, prevent and control these ever increasing attacks.

SANS lists the number one security vulnerability caused by management error[3] "To be that of appointing untrained or unqualified people to security posts and duties and furthermore they fail to provide adequate training after doing so." The number two security vulnerability caused by management was that they fail to understand the consequences of poor information security management. It can be a hard sell for security professionals to convince management that security is a worthy investment. Though information security management cannot be billed as a revenue generator, it must be stressed that good information security management can play a major role in preventing financial loss: this could be in the form of human error, lost data, damaging viruses and other such malware that can consume huge employee resources to repair damage. As well, public embarrassment could lead to future lost revenue resulting from a loss of consumer confidence. For example, a company which has exposed its customer's confidential information on the internet is not likely to see those same customers returning for future business and potential customers would be more likely to look elsewhere. That's another good reason why your security team should be provided the training necessary to secure an enterprise from all attack vectors. The few thousand dollars spent on continuous training each year may result in future attacks against your enterprise being unfruitful, and that's money that won't have to be spent on damage control and repair.

To stress the point that it is important to appoint honest and trustworthy staff to positions within your security department, I have included the results of polls taken by two reputable firms. The polls have shown that internal fraud alone can account for millions of dollars in lost revenue and resources each year. Though an exact figure cannot be pinpointed due to varying percentages of loss, it has been established that employee fraud is prevalent at all companies. A study by the firm Corporate Combat[4] has revealed that 5% of all professional hires have criminal records and that 75% of internal theft goes undetected.

---

[2] Blanding, Steven F. Security Awareness and Training, page 126

[3] www.sans.org/resources/errors.php

[4] www.corporatecombat.com/statistics1.htm

Another study conducted in 2002 by Ernst & Young[5] points out that 20% of Canadian professionals are aware of fraud that is occurring in their workplace. For this reason it is good policy to ensure that employees are aware of the consequences of such actions and that it is communicated to all personnel that reporting known cases of internal fraud and theft is the right thing to do.

6 Establishing a good audit procedure should be the final step to ensuring that your SAC procedure is functioning properly and is not being bypassed by others trying to circumvent the system for their own advantage. As well, the human errors that are bound to occur are more likely to be detected. Auditing can be made easier if access administrators have written procedures and each administrator sets up user and system security in the same manner. Anomalies become more obvious when there is a standard in place and the chance of human error is reduced when the procedure becomes routine.

Baseline reports are useful auditing tools for comparing current status reports against those which have been established according to the security policies. Any discovered violations must be investigated and corrected and in most cases management should be made aware. Regular user profile audits will play an important role in identifying dormant accounts which may exist after an employee has left the company or has changed jobs and no longer requires the access that was originally granted to them. Though the SAC will most certainly be involved in the user deletion process, it is important to ensure that the human resources department has a method of notifying the security department, in a timely fashion, any time that an employee ceases employment with the company. This is especially true in the case of an unfriendly departure. In cases such as that the person's access should be immediately disabled until the SAC form arrives and provides instruction for the handling of the user's data. It may be necessary to assign a new owner or data custodian for data which was created by or owned by the individual. In any case, it is good practice to maintain a copy of the employee's data until it can be reviewed by a department head to ensure that no vital data is deleted.

It has been my experience that human resources personnel can be lax in notifying the security department when an employee parts company with the organization. Monthly audits reveal that this is the case in the organization I work for, a conglomerate of over fifty companies privately owned. Each company or division relies on the information security department of the Information Technology Division to perform security administration, however most companies utilize their own human resources department and do not consider notifying the IT Division each time an employee is terminated.

Remember this point: your audit trail must be kept secure and not available for public disclosure. Your SAC form will contain a lot of pertinent information that could be used to gain unauthorized access to company 'jewels'

---

[5] www.ey.com/global/content.nsf/Canada/Media_-_2002_-_workplace_fraud

and secured systems. What easier way could there be to breach system security than to view a form detailing a user profile, password and even the access available ? Keep the SAC locked up after completion.

Foundstone has developed several auditing tools which are freely available on the internet and are located at www.foundstone.com. I highly recommend that security administrators become familiar with these tools and add them to their arsenal of utilities that help them to perform their job more efficiently.

Strive for Automation!

A good point to remember: users create errors! In an effort to reduce the chance of human error and to make the administration of user profiles an efficient task, it may be desirable to implement an automation process that will do the work for you or possibly even allow the end user to create their own user profile according to the rules you define in the software. There are several vendors offering automation software that can aide in key areas such as profile creation and deletion and password management. At companies where no self-serve password management tool is available, a great portion of all calls received by the helpdesk is to have passwords reset. The result is lost productivity from the end user as well as tying up a helpdesk resource for the duration of the call. A recent poll conducted by SearchSecurity.com found that nearly 80% of the people that responded required six or more passwords in order to perform their daily duties[6]. A Single Signon solution could help reduce user downtime because the user would not be required to remember all of those passwords, thus the chance of forgetting the password would be reduced. Some available resources for managing user accounts and passwords are listed at the end of this paper[i].

Before going ahead with an automation process it will prove beneficial to research various products that are currently on the market. Though every product will boast that they are the best, most up to date, be cautious to select a product that can meet your needs as well as fit into your budget. It will be a good idea to install and test a trial version of any product that is worthy of consideration. Without setting up a lab version of the product, it may be difficult to discover unsuspected conflicts between the product and your network. It won't make much sense to purchase a product that is not compatible with your network and finding out after the fact will not be condusive to a long lasting career. There are drawbacks to automation processes and the largest prohibitor will most often be the financial burden incurred to purchase the product as well as the investment of man-hours to get the product up and running. John Noad of CAUDIT has written a report detailing some of the problems and drawbacks of using Single Signon solutions: www.caudit.edu.au/caudit/information/projects/SSOreport.html

[6] http://www.searchsecurity.com/originalContent/0,289142,sid14_gci902867,00.html

Once you've invested a considerable amount of time creating your SAC procedure it will be most important to ensure that the process cannot be easily circumvented. Consider for instance the extra privileges that your helpdesk staff possess to carry out their duties. Having the ability to reset passwords and unlock user accounts makes your helpdesk center a prime target for social engineering tactics. For this reason it is crucial that the helpdesk has written procedures for resetting passwords and unlocking accounts. A rogue user may find that it's more enticing to get escalated privilege by falsely obtaining someone else's userid and password than it would be for them to go through the proper channels. 'People Hackers' are those who study methods of social engineering and pride themselves in convincing others to succumb to their wishes. Sarah Granger has written a good paper on social engineering 'Social Engineering Fundamentals: Hacker Tactics'. This can be viewed online at http://online.securityfocus.com/infocus/1527.

Consider also the computer room. Is this a secure location with physical access controls in place? If an intruder is able to gain access to your consoles and primary displays would he find them already logged on? If so, your SAC is defeated! Perhaps the intruder would find the consoles locked, however the profile of the last logged on user might be displayed on the screen. That would provide a useful piece of information for a hacker attempting a brute force password attack. Keeping firewall management consoles and IDS locked down prevents them from being tampered with by unauthorized personnel who may have other reasons for having access to the computer room. Taking a few extra precautions to secure the computer room and its devices will go a long way to ensuring that access to your companies systems and information will be via authorized and audited controls.

Finally, there will always be exceptions to your policies and procedures. Business must go on and some times an exception to your policies may be deemed to be an acceptable business risk. SANS defines a risk as threat times vulnerability. If you have a known vulnerability and threat that it may be exercised, then you have a risk. After risks are analyzed, senior management may give the go-ahead to defy your own policies for the sake of doing business. Ensure that any such exceptions are catalogued; this will be necessary to protect yourself from scrutiny and to explain discrepancies that might show up during an audit. Keep the catalogue in a secure location where it cannot be reviewed by non-security personnel and make it a point to review the exceptions regularly. When the exceptions are reviewed regularly they become more familiar to you and you may discover over time that the exception is no longer required.

To summarize, remember the intent of a Systems Access Control procedure: to keep your systems and information confidential, available, and accurate. That goal will be accomplished by having access controls in place which define: the classification of information; the roles of users; data ownership; and related security policies. Assign trustworthy and knowledgeable people to security posts and ensure that those people have the proper training to carry out the job. Establish an audit trail that will reveal who requested the access; who

approved the access; who received the access; and who created the access. Above all, keep your SAC secure: from the delivery, to the approval, to the notification, ensure that your SAC cannot be tampered with or intercepted by unauthorized individuals.

I hope this paper has provided the information security community with beneficial considerations for creating a secure and effective Systems Access Control procedure of its own.

References

Handbook of Information Security Management, 1999
Krause, Micki and Tipton, Harold
Printed by CRC Press, 1999 Auerbach

SANS Institute Reading Room
The SANS Security Policy Project
2002 – 2003 The SANS Institute
www.sans.org/resources/policies

SANS Institute Reading Room
The 7 Top Management Errors That Lead to Computer Security Vulnerabilities
2003 – 2003 The SANS Institute
www.sans.org/resources/errors.php

Search Security.com
Security News & Analysis
Survey: Most Workers Must Remember Six Passwords or More
Hurley, Edmond May, 2003
http://www.searchsecurity.com/originalContent/0,289142,sid14_gci902867,00.html

Caudit
Report on Common Problems in Provision of Single Signon
Noad, John Caudit, 2003
www.caudit.edu.au/caudit/information/projects/SSOreport.html

Security Focus
Social Engineering Fundamentals, Part I : Hacker Tactics
Granger, Sarah
Dec., 2001
http://online.securityfocus.com/infocus/1527

Corporate Combat
Loss Prevention Specialists, Inc
Minnesota, USA
www.corporatecombat.com/statistics1.htm

Ernst & Young
One in Five Canadians Say Fraud Occurs in Their Work Place
Aug. , 2002
www.ey.com/global/content.nsf/Canada/Media_-_2002_-_workplace_fraud

Security Essentials Courseware
Published 2001, SANS Institute

Foundstone
2003 Foundstone, Inc
www.foundstone.com

Microsoft
www.microsoft.com

SXC
www.sxc.co.uk

---

[i] Resources for managing user accounts and passwords

Microsoft
Windows 2000 Professional Automated Deployment Options: An Introduction
www.microsoft.com/windows2000/techinfo/planning/client/autodeploy.asp

Control SA
www.sxc.co.uk/pdf/controlsa.pdf

IBM
Tivoli Identification Manager (TIM)
www.tivoli.com

ID Synch
http://idsynch.com

P Synch
http://psynch.com

General Masters, Inc
www.gmasterinc.com/security/sign-on.htm

Last Updated: May 29th, 2017

Upcoming Training

Security Operations Center Summit & Training	Washington, DC	Jun 05, 2017 - Jun 12, 2017	Live Event
SANS Houston 2017	Houston, TX	Jun 05, 2017 - Jun 10, 2017	Live Event
Community SANS Ottawa SEC401	Ottawa, ON	Jun 05, 2017 - Jun 10, 2017	Community SANS
SANS San Francisco Summer 2017	San Francisco, CA	Jun 05, 2017 - Jun 10, 2017	Live Event
SANS Charlotte 2017	Charlotte, NC	Jun 12, 2017 - Jun 17, 2017	Live Event
SANS Rocky Mountain 2017 - SEC401: Security Essentials Bootcamp Style	Denver, CO	Jun 12, 2017 - Jun 17, 2017	vLive
SANS Secure Europe 2017	Amsterdam, Netherlands	Jun 12, 2017 - Jun 20, 2017	Live Event
Community SANS Portland SEC401	Portland, OR	Jun 12, 2017 - Jun 17, 2017	Community SANS
SANS Rocky Mountain 2017	Denver, CO	Jun 12, 2017 - Jun 17, 2017	Live Event
SANS Minneapolis 2017	Minneapolis, MN	Jun 19, 2017 - Jun 24, 2017	Live Event
SANS Cyber Defence Canberra 2017	Canberra, Australia	Jun 26, 2017 - Jul 08, 2017	Live Event
SANS Paris 2017	Paris, France	Jun 26, 2017 - Jul 01, 2017	Live Event
SANS Columbia, MD 2017	Columbia, MD	Jun 26, 2017 - Jul 01, 2017	Live Event
SANS London July 2017	London, United Kingdom	Jul 03, 2017 - Jul 08, 2017	Live Event
Cyber Defence Japan 2017	Tokyo, Japan	Jul 05, 2017 - Jul 15, 2017	Live Event
SANS Munich Summer 2017	Munich, Germany	Jul 10, 2017 - Jul 15, 2017	Live Event
SANS Cyber Defence Singapore 2017	Singapore, Singapore	Jul 10, 2017 - Jul 15, 2017	Live Event
Community SANS Minneapolis SEC401	Minneapolis, MN	Jul 10, 2017 - Jul 15, 2017	Community SANS
SANS Los Angeles - Long Beach 2017	Long Beach, CA	Jul 10, 2017 - Jul 15, 2017	Live Event
Community SANS Phoenix SEC401	Phoenix, AZ	Jul 10, 2017 - Jul 15, 2017	Community SANS
Mentor Session - SEC401	Macon, GA	Jul 12, 2017 - Aug 23, 2017	Mentor
Mentor Session - SEC401	Ventura, CA	Jul 12, 2017 - Sep 13, 2017	Mentor
Community SANS Atlanta SEC401	Atlanta, GA	Jul 17, 2017 - Jul 22, 2017	Community SANS
Community SANS Colorado Springs SEC401	Colorado Springs, CO	Jul 17, 2017 - Jul 22, 2017	Community SANS
SANSFIRE 2017	Washington, DC	Jul 22, 2017 - Jul 29, 2017	Live Event
Community SANS Charleston SEC401	Charleston, SC	Jul 24, 2017 - Jul 29, 2017	Community SANS
SANSFIRE 2017 - SEC401: Security Essentials Bootcamp Style	Washington, DC	Jul 24, 2017 - Jul 29, 2017	vLive
Community SANS Fort Lauderdale SEC401	Fort Lauderdale, FL	Jul 31, 2017 - Aug 05, 2017	Community SANS
SANS San Antonio 2017	San Antonio, TX	Aug 06, 2017 - Aug 11, 2017	Live Event
SANS Prague 2017	Prague, Czech Republic	Aug 07, 2017 - Aug 12, 2017	Live Event
SANS Boston 2017	Boston, MA	Aug 07, 2017 - Aug 12, 2017	Live Event