Global Information Assurance Certification Paper

We're Auditors – We're here to help

Ensuring Security Professionals are properly equipped

J. Michael Butler

GIAC Version 1.2f (Amended August 13, 2001)

October 11, 2001

'Auditors are the guys that show up after the battle in order to bayonet the wounded,' said the UNIX guru to the internal information systems (IS) auditor. Security professionals often treat auditors with derision. It is true that some auditors almost beg for such treatment. This former IS auditor, (turned security professional), circumvented derision with an approach to the subjects of the audit convincing them of the assistance we could provide. I saw our existence serving, in part, to help them reach their goals and objectives.

'An audit can be an empowering experience.' I would say, 'If you have issues you cannot solve due to lack of resources, and if the issues are truly significant enough to warrant attention, we can pass them on to Senior Management and you will get what you need!'

Auditors can empower you by convincing management to:

- provide personnel
- provide equipment
- provide software
- improve processes
- add other resources
- increase your budget

> "In addition to their skill at analytical techniques, internal auditors are well placed to make MIS improvements because they are one of the very few functions that are comfortable operating both vertically and horizontally in an organisation. They know exactly where information is coming from, how and where it goes to and what it is used for at all levels of management."[1]

Auditing will be a bittersweet experience, simply because no one likes criticism – even if it is constructive. As one subject said to me in an opening meeting, "…If you think you can do my job better than me, you're welcome to it!" That was before he had heard the speech, of course.

The intention of this document is to:

- Outline high level risks to senior officers, specific to information systems, mitigated by auditors
- Note areas of information systems audit normally examined by auditors
- List a few common exceptions or findings in information systems areas – (things to watch for)
- Itemize suggestions for security professionals to help them get the most from their audits

Security professionals can, hopefully, use this document as source material to help convince management to hire auditors to review the company's information systems. In addition, the common findings listed below may point security professionals to issues they need to deal with – hopefully before the auditor arrives.

Risks to Senior Officers

Audits are done to protect the senior officers of a company or corporation. Whether there is just a president, or there is a sea of "C"s, (CEO, COO, CFO, etc.), the risks are still there and they are still real. If found to be negligent in matters of protection of personal information, privacy issues, protection of company confidential information, or protection of client information, all of the company officers are liable and can be sued. In the public arena, that means stockholders – the ones who lose money when companies make mistakes – will be suing those senior officers and/or the board of directors. In the small business arena, it means the company owner/president and officers can be at risk, as well as their personal holdings. As the size of the company and the number of officers decreases, the potential for disaster on a personal basis goes up. There may be no one with whom you may share the blame. Then you have the most to lose, personally.

> "…corporate directors and officers face a greater likelihood of being sued because of their decisions that ever before.
> Every director and officer of a closely held organization or a public company is a potential target for serious financial loss. Suits can be brought by shareholders, employees, regulatory agencies and competitors, among others."[2]

The detail risks to the company will be discussed in the next section on audit areas. The decision to audit or not to audit, however, should be made by senior officers based upon direct potential loss. The direct risk to the officer is not that a hacker just stole 5,000 credit card numbers. The direct **personal** risk is that he or she could lose a material amount of money and/or, worst case scenario, a home, cars, and other personal belongings. The direct **business** risk is that the company could lose its reputation and/or its customers and revenue stream. Obviously, if this happens, more persons will be impacted than just the senior officers!

> "Shareholder lawsuits. They can be your worst nightmare. The source of 50% of all directors and officers liability (D&O) claims, shareholder suits typically name the corporation in addition to personally naming the directors and officers. According to the most recent Watson Wyatt survey, settlements in these cases average $7.6 million, with defense costs often adding another $1 million to the bill." [3]

Audit Areas

More than one organization has been established for the purpose of determining areas and objectives to be used for auditing. One of the widely accepted standards is COBIT, (Control OBjectives for Information and related Technology). Their mission statement follows:

> "To research, develop, publicise and promote an authoritative, up-to-date, international set of generally accepted IT Control Objectives for day-to-day use by business managers as well as security, control and audit practitioners.
> "COBIT has been developed as a generally applicable and accepted standard for good Information Technology (IT) security and control practices that provides a reference framework for management, users, and IS audit, control and security practitioners."[4]

I suppose this quote could also be read, 'We're from audit… We're here to help.' Auditors can be helpful to security professionals.

Based on COBIT, the following 4 domains and their associated processes are reviewed in whole or in part by IS auditors.

1. **Planning and Organization**
   - Define a strategic IT plan
   - Ensure compliance with external requirements
   - Manage human resources
   - Communicate management aims and direction
   - Manage the IT investment
   - Determine technological direction
   - Define the IT organisation and relationships
   - Define the information architecture
   - Assess risks
   - Manage projects
   - Manage quality
2. **Acquisition and Implementation**
   - Manage changes
   - Install and accredit systems
   - Acquire and maintain technology infrastructure
   - Develop and maintain procedures
   - Acquire and maintain application software
   - Identify automated solutions
3. **Delivery and Support**
   - Manage operations
   - Manage facilities
   - Manage data
   - Manage problems and incidents
   - Manage the configuration
   - Assist and advise customers
   - Educate and train users
   - Identify and allocate costs
   - Ensure systems security
   - Ensure continuous service
   - Manage performance and capacity
   - Manage third-party services
   - Define and manage service levels
4. **Monitoring**
   - Provide for independent audit
   - Obtain independent assurance
   - Assess internal control adequacy
   - Monitor the processes[5]

Each Domain and/or Process selected is examined at a deeper level as it pertains to the business being reviewed. For example, the “Ensure systems security” process could include an examination of any or all of the following:

- Manage Security Measures
- Identification, Authentication and Access
- Security of Online Access to Data

- User Account Management
- Management Review of User Accounts
- User Control of User Accounts
- Security Surveillance
- Data Classification
- Central Identification and Access Rights Management
- Violation and Security Activity Reports
- Incident Handling
- Reaccreditation
- Counterparty Trust
- Transaction Authorisation
- Non-Repudiation
- Trusted Path
- Protection of Security Functions
- Cryptographic Key Management
- Malicious Software Prevention, Detection and Correction
- Firewall Architectures and Connections with Public Networks[6]

For a complete listing of all the suggested areas, refer to COBIT available for purchase on line from www.isaca.org, or download it for free at http://www.isaca.org/cobit.htm. In addition, an excellent source for audit programs is: http://www.auditnet.org where one can sample around 350 different audit programs. This URL, http://www.auditnet.org/asapind.htm, points to their **ASAP** or **A**uditors **S**haring **A**udit **P**rograms section. The audits located at auditnet.org have been downloaded to the web site for other auditors. That gives any reader the opportunity to determine what auditors look for in their reviews. Some of the systems represented in these audits include AS400, Checkpoint Firewall, Cisco Routers, HP-UX, Internet, LAN, Lotus Notes, Novell, Oracle, PeopleSoft, SAP, Tandem, TCP Ports, Windows NT, ACF2, DB2, DEC VAX, MVS, RACF, and UNIX.[7]

Common Exceptions or Findings

Common Finding 1: A common finding in an IT audit is the lack of current or adequate proprietary documentation for systems. This refers to documentation of the exact procedures followed by the company's technical personnel, not the generic documentation available from vendors.

Documentation is usually the last thing to be done, if it is done at all. Technical personnel typically either don't have time to write documentation, don't like to write it, or both. In an audit conducted a couple of years ago, the auditor asked for the operations manuals for the internet group of a large corporation. He received a single printed page about half full of text. The document outlined, in terse two or three word steps, what the internet group did every day. In the distributed systems world, an auditor may not expect the hundreds (thousands?) of pages he or she expects from the mainframe operations world. It is reasonable to assume, however, that the UNIX, Windows, Netscape, Apache, or other system operators would have more daily, weekly, monthly, or other regular tasks than they could possibly fit on one piece of paper.

Good documentation should include but not be limited to: setup/install procedures, daily operations, weekly operations, monthly operations, back-up

procedures, current patch levels, patch monitoring/update procedures, on call schedule, escalation lists with names, phone numbers (including cell, after hours, pagers, etc.), and any other special or proprietary procedures.

Risks: Risks of not having up to date documentation include, but are not limited to, inconsistent or inadequate operations, inability to recover quickly from disaster, extended training time, and/or an insecure system due to inadequate physical or logical monitoring. Without a well-defined list of daily tasks – a checklist if you like – operators will have a tendency to forget something. It is easy, for example to forget to make a backup, or to forget to unload backup tapes. This could cause a backup to be overwritten, or one to be skipped. System administrators are aware of the catastrophe waiting to happen when their backup is not current.

Without adequately documented install/setup procedures, a disaster could have a significant negative impact on business. Instead of being back up to speed in 1 or 2 days, it may take a few weeks or months to stabilize the rebuilt or new system.

Bringing on a new employee always impacts the production of others until the employee is up to speed. Without adequate documentation, that impact will be much more serious on personnel who are probably already overtaxed.

Finally, and most important for this context, without adequate documentation, there is no way for anyone – particularly management – to monitor the personnel responsible for operating the systems. There is no way to know what the employee should or should not be doing to the system. Even technically qualified individuals called in to observe may not recognize inappropriate activities on the system because of a lack of documented procedures. Though it may sound insignificant, the fact is that bad or missing documentation puts the operator, the manager, and the company at risk.

Mitigation: Perhaps the personnel who would be responsible for documentation are already working 80 hour weeks just keeping the systems running. In that case, an auditor can point out the deficiency and help management see the need both for the documentation as well as the staff needed to develop the documentation. If the company cannot afford the long term commitment to another employee, then a consultant could be an alternative. The third party person could observe and document what the operations personnel are doing as they do it. Then his observations could be turned into the needed documentation. The new documentation will quickly be out of date if your personnel do not have time to update it. In most cases, though, once documentation is created, it is much easier to keep it up to date than it is to create it.

Common Finding 2: Patch levels are not up to date or are not consistently applied to operating systems and/or virus detection software. Every system requires occasional patching. Some require more than others. (I'm not going to mention any corporation names…) Auditors are interested in what your patch level is, whether you test new patches before implementation, and whether you are consistent. Are your procedures for patching documented? Are all of your systems at the same patch level? Do you receive bulletins announcing the latest patches?

Risks: Code Red, Nimda, DOS, Trojans, hack attacks, zombie attacks, to name a few. If systems are not patched, one risks losing control of the server, other servers in the same domain, and/or the data that resides on any of the servers. The losses could be catastrophic for a company. What if credit card numbers and other personal information were being sent off to some unknown e-mail or chat address? What if

passwords of all users are collected as they are entered and sent off to the same address? What damage could be done to your company's reputation? What if a web server is compromised in your company's extranet and the user then has access to boxes in your trusted network? The risks are overwhelming!

Mitigation: We are receiving repeated warnings that the "latest" virus or worm is designed to attack known flaws. It takes time to develop mal-ware, just like it does to create good code. The more complex the mal-ware, (e.g. Nimda), the longer it takes to develop. If administrators would keep their systems patched appropriately, the incidents of computers being infected by viruses and worms would drop wonderfully. Exploits in the form of viruses, worms, denial of service attacks, or just general hacking, should be mostly harmless, if the system administrator has operating systems, web server systems, virus detection systems, and intrusion detection systems up to date.

> "Graham Cluley, of antivirus company Sophos, said the outbreak of Nimda may well have caused more damage to other worms and viruses such as Sir Cam by forcing admins to patch up their systems."[8]

Common Finding 3: User ID and Password problems are very common. Some of the most common user account problems would include

- active accounts for terminated employees
- back door accounts created by administrators
- generic accounts used by more than one person
- active guest accounts with inappropriate access to data
- admin/supervisor accounts with weak or no password

Common password problems include

- badly constructed passwords including only dictionary words
- users allowed to work with weak or no password
- exposed password files that can be used with password cracker programs
- sharing of IDs and passwords with other employees
- IDs and passwords that are inadvertently revealed by users while others are watching over their shoulder
- groups of personnel using the same password so that everyone knows everyone else's password.

Risks: Internal "bad guys" exist. Most vulnerabilities pertaining to IDs and passwords are related to internal personnel, not outside hackers. Social engineering – mostly from the inside, but potentially from the outside as well (e.g. Kevin Mitnick) – can trick users into giving up their IDs and passwords. These are the keys to the company's data. The company's data, most likely, is the reason for the company's existence. So, worst case scenario, if the company data is stolen, the company could go away. Best case scenario, there are significant costs associated with determining what data was taken, who has it, what the impact will be from the loss, and recovery of the data, if it has been destroyed.

Most of the risk associated with ID or Password issues will be internal. That certainly does not reduce the liability. Keep in mind that insiders understand where the soft underbelly of the company is. They know how best to hurt the company with their actions.

> *"Insiders*. The disgruntled insider (a current or former employee of a company) is a principal source of computer crimes for many companies. Insiders' knowledge

of the target companies' network often allows them to gain unrestricted access to cause damage to the system or to steal proprietary data. The just-released 2000 survey by the Computer Security Institute and FBI reports that 71% of respondents detected unauthorized access to systems by insiders."[9]

Mitigation: Employee education is the number one defense in regard to ID and password problems. Start by making sure that every employee signs a document that, among other things, specifies that they will never reveal their password to anyone else. Ensure that they understand what makes a password good – mixing upper and lower case letters with numbers and symbols in a non-word format. Don't allow them to file or post passwords where others can find them. (Make sure they don't hide the password under the monitor or keyboard.) Your employees will be your best security, once they understand the issues and the risks.

Security awareness programs are necessary due to employee turnover or just lapse of time and memory. Memos, e-mails, posters, and top down management direction all play a part in increasing employee awareness.

Other controls can be introduced automatically. Many systems allow for the security administrator to specify that passwords meet certain criteria, (e.g. minimum length, must contain at least one number and/or one symbol, etc.).

Security personnel could, with permission from management, run cracker tools against password files and report inadequate passwords back to the responsible personnel. Some tools will even check passwords without reporting what they are – just that they are weak – and will automatically use the company mail system to forward a message to the offending user.

Good HR procedure will have all terminated employees listed and forwarded to appropriate security administrators for timely disabling of the users' IDs. It is imperative that disgruntled employees be disabled immediately as they would have the most reason for "striking back" at the corporation through some malicious act. Don't forget RAS or other dial in accounts. In fact, they should be disabled first, since a former employee is most likely to try those accounts first.

Use of good self-auditing tools, (e.g. Bindview), will mitigate risk by finding weaknesses in the system, in accounts, and passwords. Such tools can be used to find everything from current server patch levels to unusual or inappropriate permissions for users. Reports can be printed and reviewed by security personnel, as well as Business Unit managers.

Common Finding 4: Inadequate monitoring of systems. It is common to find that logs are not being kept, or that the saved logs are never or seldom reviewed. Usually this finding points to a lack of written procedure or documentation. (See finding 1)

Risks: Without logs, there can be no real time or forensics monitoring done of security controls for users. If an administrator is not regularly reviewing logs and/or occasionally watching the creation of logs real time, unauthorized users could be having their way with his or her system. There would be no way to know the box was compromised. There would be no way to know how long the box had been compromised or any clue as to what the unauthorized user had been doing while on the box.

Consideration must be given to the data that resides on the box, or is accessible from the box. Further, the risk is not just for the data. The risk includes legal liability for an inadequate job of administration. If we do not perform due diligence, we are liable to consumers, clients, and shareholders. If for no other reason, logging and regular review of those logs must be implemented to protect the company and its officers from legal action.

Mitigation: Usually for the sake of avoiding "impact to production," logging can be and often is turned off. While it is most likely is not necessary to log every keystroke of the users, there are certain acts that should always be logged. Those should definitely include failed logon attempts, failed attempts to change to super user status, account creation – particularly administrative/super user accounts, changes to privileges, privileged use – such as administrator or super user logon and access, changes to policy, failed attempts to access critical restricted disk areas or files. In addition, there may be other events or actions that need monitoring for a system depending upon the way(s) it is utilized in one's environment.

In addition to the traditional server view, one must also consider other equipment capable of being monitored and logged. Examples may include routers, switches, critical workstations, firewalls, PBX systems, security systems, etc.

Finally, consideration should be given to collecting all logs centrally. There are at least two reasons for central logging. First, it makes it simpler to review the logs because they are all in one place. Second, and more important, the logs will be protected by being saved somewhere other than the host system. This is critical for preserving the state of the logs in the case(s) where super user/administrator accounts have been compromised. Normally, an authorized user will open logs and delete any reference to their activities. If those logs are collected elsewhere on a system to which they do not have access, then they will be unable to hide their unauthorized activities by removing them from the logs.

Getting the most from your Audit

Making the audit happen will be your first step. If your company does not have an internal audit department, then you may require a third party information systems auditor to do such work. In any case, bringing in someone from the outside - at least outside your department - will add credibility to what you are doing. Internal information system auditors should have a better feel for the company's business and the historical weaknesses. Third party auditors may be more independent and/or may look in areas not normally examined by the internal auditors.

From the opening to the exit, subjects of audits will help themselves and their company by:

- dedicating personnel to the audit to assist the auditors
- instructing personnel to be fully cooperative and to practice full disclosure
- providing all the hard copy and system data requested by the auditors in a timely fashion
- take any opportunity to share your issues and concerns with the auditors, even if they have not been requested
- recognize the auditor's responsibility to ask the questions they ask – if they are internal auditors, they will be directly responsible to the board of directors

- keep a file of all materials provided to the auditors indicating the request that prompted that item, the date, and the source for the information (to help with future audits)
- If you are using any automated tools, such as Bindview, be sure that the auditor is aware of and receives the data provided by the tool

Conclusion

Regardless of the auditor's personality, the unpleasant prospect of being criticized, or the probable questions from management, someone from outside your business unit should do an audit of your security on a regular basis. With the input, on an annual basis, of an independent eye, your security will potentially be improved. It isn't automatic, of course. There is work involved in mitigating risks. Resources – time, money, and/or people – will be required to accomplish mitigation.

However, the good news is that your senior management should be concerned enough about security issues to provide the resources you need. We are making the assumption, of course, that CEOs, presidents, board members, and owners are concerned about their job, their company, their money, and their personal belongings. Their eyebrows and their awareness will go up in response to a well written audit report. They should be ready to equip you for your task, if they have not been before.

Do what you can to mitigate risks, schedule an audit, celebrate the areas where there are no significant findings, and fix the others. Then you can thank the auditor for making you a hero. They really are "here to help."

Sources

[1] Pasricha , Navin. "Count on internal audit to reduce your MIS frustrations." Copyright © 2000 PriceWaterhouseCoopers web site URL: http://www.pwcglobal.com/extweb/ncinthenews.nsf/DocID/A895C91051AE920A8525698300149DC7 (Access date 12 October, 2001)

[2] Chubb URL. Chubb & Son, a division of Federal Insurance Company. Copyright © 1995-2001. http://www.chubb.com/businesses/ep/dando/ (access date 12 October, 2001)

[3] Chubb URL. Chubb & Son, a division of Federal Insurance Company. Copyright © 1995-2001. http://www.chubb.com/businesses/ep/dando/lossscenario.html (access date 12 October, 2001)

[4] COBIT URL: http://www.isaca.org/cobit.htm (access date 11 October, 2001)

[5] COBIT®, 3rd Edition Control Objectives. COBIT Steering Committee and the IT Governance Institute™ available from URL: http://www.isaca.org/cobit.htm for download or purchase. Copyright © 1996, 1998, 2000 by the Information Systems Audit and Control Foundation (ISACF). p. 20.

[6] Ibid.

[7] Auditnet URL. AuditNet. Copyright © 1994-2001. http://www.auditnet.org/ (access date 12 October, 2001),

[8] Middleton, James. "Sir Cam poised to strike tomorrow." VNU Business Publications Ltd. Copyright © 1995-2001. URL: http://www.computing.vnunet.com/News/1126112 (Access date 15 October, 2001)

[9] Freeh, Louis J. "Statement for the Record of Louis J. Freeh, Director Federal Bureau of Investigation on Cybercrime." March 28, 2001. URL: http://www.fbi.gov/congress/congress00/cyber032800.htm (access date 15 October, 2001)

Last Updated: June 23rd, 2017

Upcoming Training

SANS Cyber Defence Canberra 2017	Canberra, Australia	Jun 26, 2017 - Jul 08, 2017	Live Event
SANS Columbia, MD 2017	Columbia, MD	Jun 26, 2017 - Jul 01, 2017	Live Event
SANS Paris 2017	Paris, France	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 Cyber Defence Singapore 2017	Singapore, Singapore	Jul 10, 2017 - Jul 15, 2017	Live Event
Community SANS Phoenix SEC401	Phoenix, AZ	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
SANS Munich Summer 2017	Munich, Germany	Jul 10, 2017 - Jul 15, 2017	Live Event
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
SANSFIRE 2017	Washington, DC	Jul 22, 2017 - Jul 29, 2017	Live Event
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 Boston 2017	Boston, MA	Aug 07, 2017 - Aug 12, 2017	Live Event
SANS Prague 2017	Prague, Czech Republic	Aug 07, 2017 - Aug 12, 2017	Live Event
Community SANS Omaha SEC401*	Omaha, NE	Aug 14, 2017 - Aug 19, 2017	Community SANS
SANS Salt Lake City 2017	Salt Lake City, UT	Aug 14, 2017 - Aug 19, 2017	Live Event
SANS New York City 2017	New York City, NY	Aug 14, 2017 - Aug 19, 2017	Live Event
Community SANS Trenton SEC401	Trenton, NJ	Aug 21, 2017 - Aug 26, 2017	Community SANS
SANS Virginia Beach 2017	Virginia Beach, VA	Aug 21, 2017 - Sep 01, 2017	Live Event
Community SANS San Diego SEC401	San Diego, CA	Aug 21, 2017 - Aug 26, 2017	Community SANS
Virginia Beach 2017 - SEC401: Security Essentials Bootcamp Style	Virginia Beach, VA	Aug 21, 2017 - Aug 26, 2017	vLive
SANS Adelaide 2017	Adelaide, Australia	Aug 21, 2017 - Aug 26, 2017	Live Event
SANS Chicago 2017	Chicago, IL	Aug 21, 2017 - Aug 26, 2017	Live Event
Mentor Session - SEC401	Minneapolis, MN	Aug 29, 2017 - Oct 10, 2017	Mentor
SANS Tampa - Clearwater 2017	Clearwater, FL	Sep 05, 2017 - Sep 10, 2017	Live Event
SANS San Francisco Fall 2017	San Francisco, CA	Sep 05, 2017 - Sep 10, 2017	Live Event
Mentor Session - SEC401	Edmonton, AB	Sep 06, 2017 - Oct 18, 2017	Mentor