Computer Security Auditing

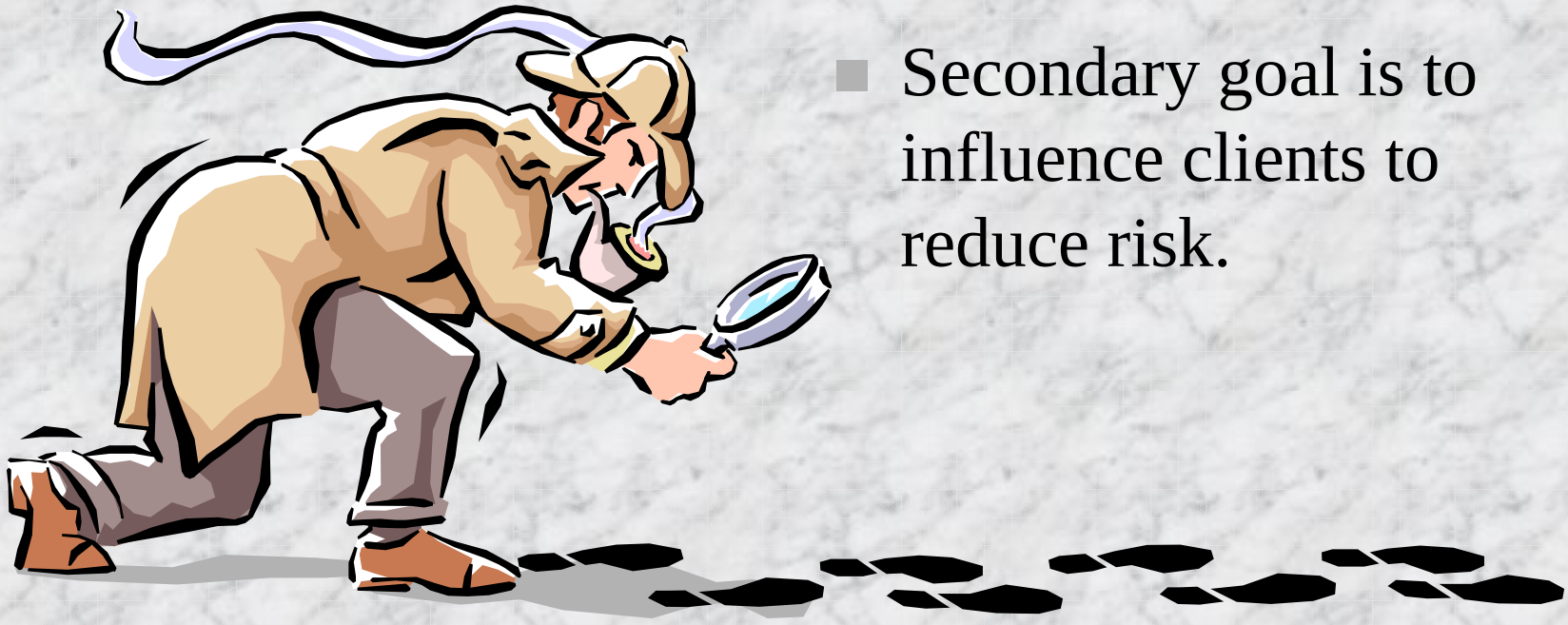
Fundamentals of A Security Audit

Bill Hayes - Omaha World Herald Company

Computer Security Audits

- Security Audit Definition
- Security Policies
- Security Audit Standards
- Security Audit Planning
- Security Audit Fieldwork
- Security Audit Reporting

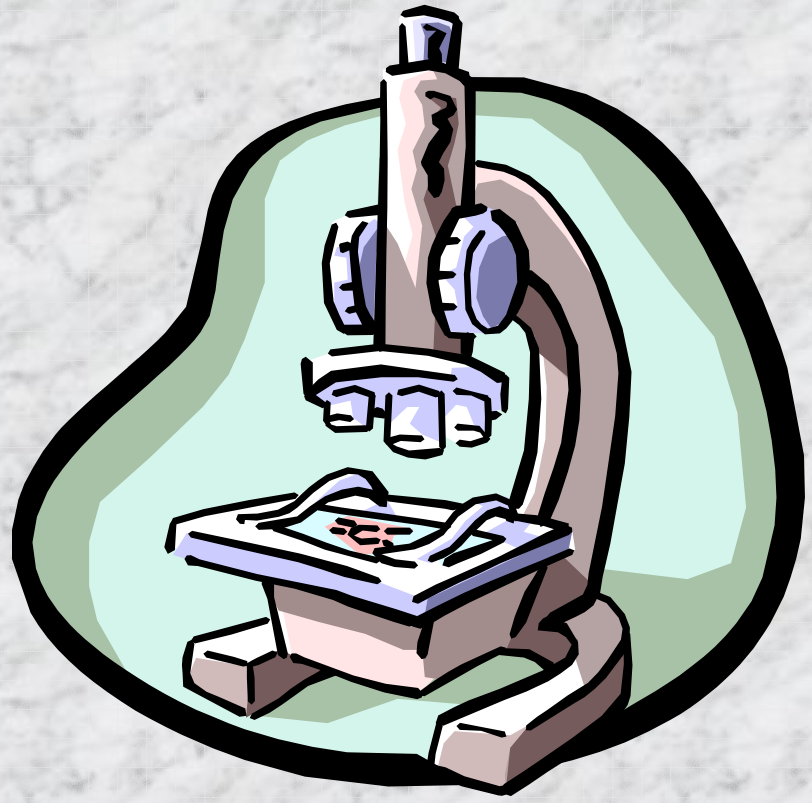
The Role of the Security Auditor



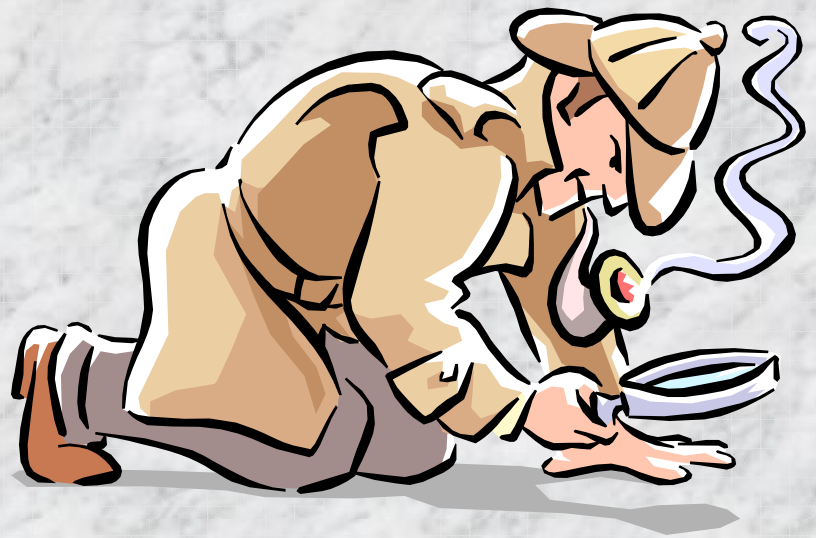
- Primary goal is to measure and report on risk.
- Secondary goal is to influence clients to reduce risk.

What’s a security audit?

- It’s is a systematic, measurable technical assessment of how the organization's security policy is employed at a specific site.



Penetration test vs. Security Audit



- A penetration test is a very narrowly focused attempt to look for security holes in a critical resource, often with little or no “inside” knowledge and usually conducted outside the firewall.

Security Audit vs. Penetration Test

- Computer security auditors work with the full knowledge of the organization, often with considerable inside information, in order to understand the resources to be audited.

The Security Policy

- Security policies help standardize security practices by having them codified (in writing) and honored by employees who agree to follow these practices.

What's in a security policy?

- The security policy lists acceptable practices for everyone to follow as they perform their daily tasks. They are based on "Industry Best Practices".

The Unwritten Security Policy

- The unwritten security policy is the actual way security is implemented in an organization. It relies on workplace customs. Because it’s unwritten, it isn’t always understood by everyone.

Looking at the whole picture

- Security audits have to be able to gauge both the written and unwritten security policies. Auditors therefore rely on many methods to get a clear picture of an organization.

IT Security Audit Standards

- There are a number of IT security standards. These standards represent the best security practices of a particular work sector and are tailored for that sector.

IT Security Audit Standards

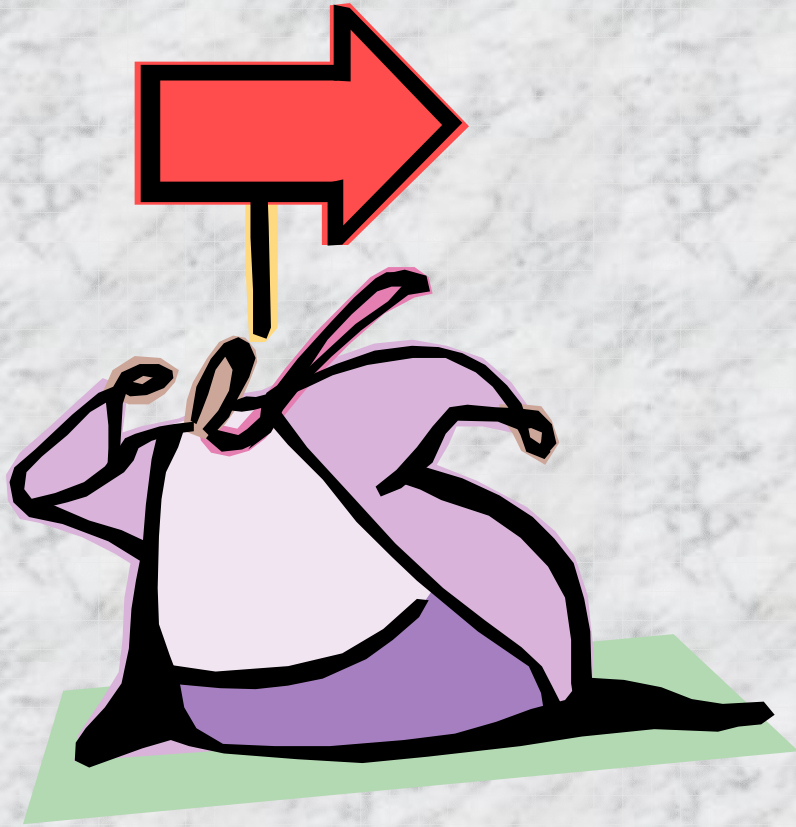
- Security audit standards are checklists examining specific procedures that should be followed to ensure that IT resources are adequately safeguarded.

IT Security Audit Standards

- **COBIT - C**ontrol **OB**jectives for **I**nformation and related **T**echnology was developed by the Information Systems Audit and Control Association (isaca.org). COBIT is in widespread use.

IT Security Audit Standards

- FISCAM - (Federal Information Systems Control Audit Manual) Used by some segments of the U.S. government and developed by the Government Accounting Office.



IT Security Audit Standards

- ISO17799 is "*a comprehensive set of controls comprising best practices in information security*". Developed by the British, it is an international information security standard now gaining widespread acceptance.

Other IT Security Audit Standards

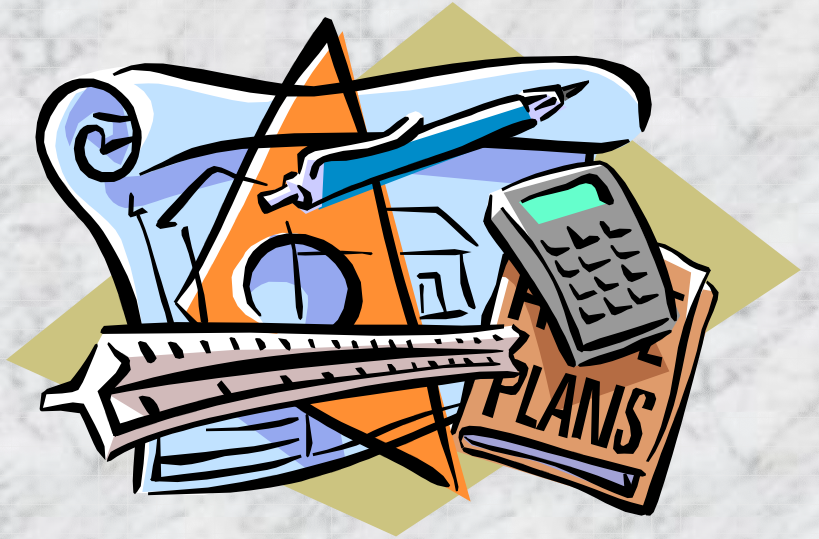
- **HIPAA - H**ealth **I**nsurance **P**ortability and **A**ccountability **A**ct Of 1996. Federal law governing privacy of patient information.
- **Sarbanes Oxley Act of 2002**. It how regulates pubic companies handle fiscal information.

Security Audit Methods

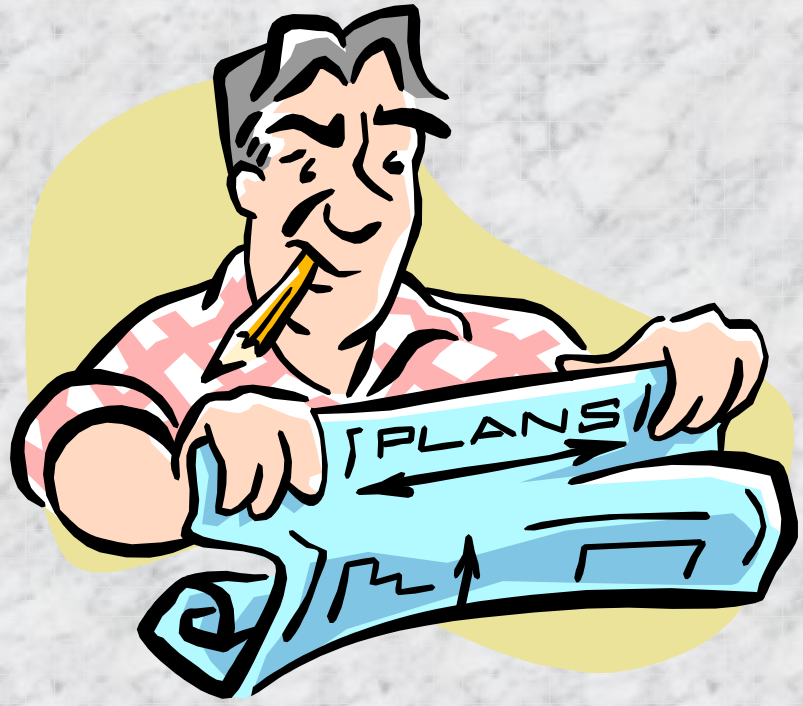
- Data is collected through a variety of methods, including interviews, site surveys, questionnaires, researching historical data, and using vulnerability assessment tools.

Security Audit Planning

- In preparing for an audit, auditors consult previous audit results, site surveys, and questionnaires. In addition, they consult with the client in order to limit the scope of the audit.



Site Surveys



- Site surveys are provided by the client. They are technical descriptions of the network resources to be audited. They list computers, operating systems, and have network diagrams.

Conducting the Audit

- The Computer Security audit is conducted in stages with a fair amount of coordination between client and auditor. The audit consists of an arrival briefing, data collection and departure briefing.

Entry Briefing

- During the arrival briefing, the auditor meets with the key players to outline the conduct of the audit, the tasks performed and who will need to be interviewed. Last minute questions are answered.

Fieldwork

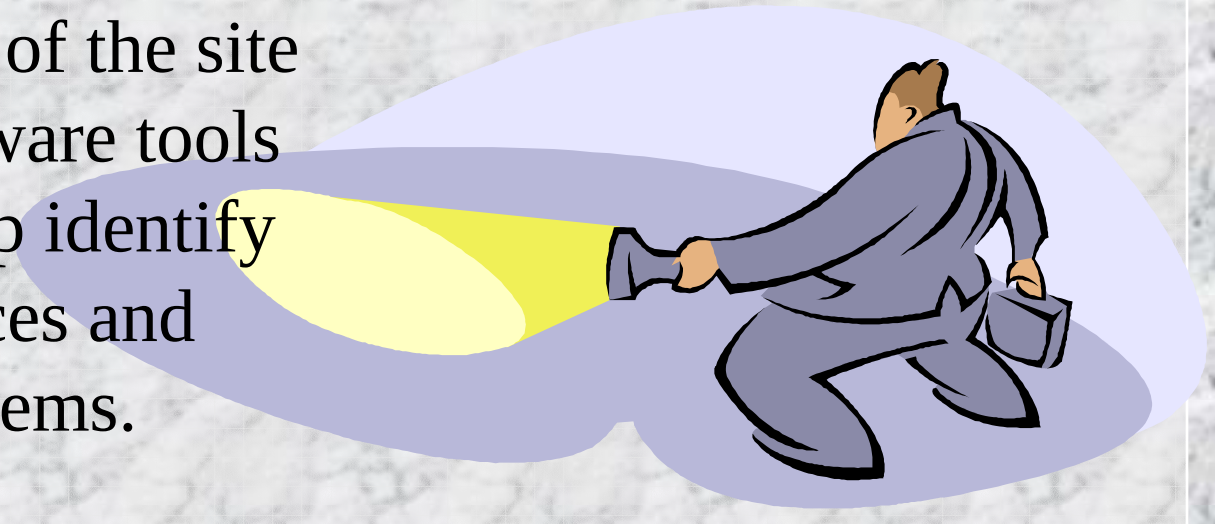
- The process of collecting audit data is called fieldwork. Data comes from a variety of sources, including interviews, software tools, and system logs. An auditor can collect megabytes of data in a very short time.

Fieldwork - Interviews

- Interviews are used to collect data from the client's employees. Audit checklists are standardized groups of questions that are designed to get clear and concise answers.

Fieldwork - Network Discovery

- Network discovery is the process of reconciling the real network against the paper records of the site surveys. Software tools like nmap help identify network devices and operating systems.



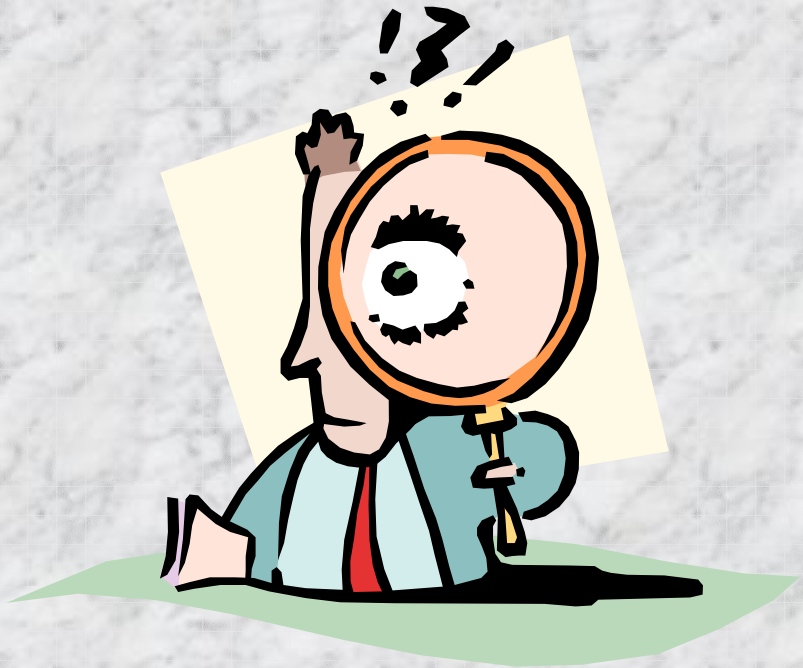
Fieldwork - Vulnerability Assessment

- Vulnerability assessment tools examine the state of services that could be used to compromise or cause denial of service conditions. Network based tools and host based tools perform the work.

Fieldwork - Log files

- Log files provide excellent information. Log files can validate vulnerability scan results. The sheer volume of log file entries can make data retrieval time consuming. Tools like perl really help.

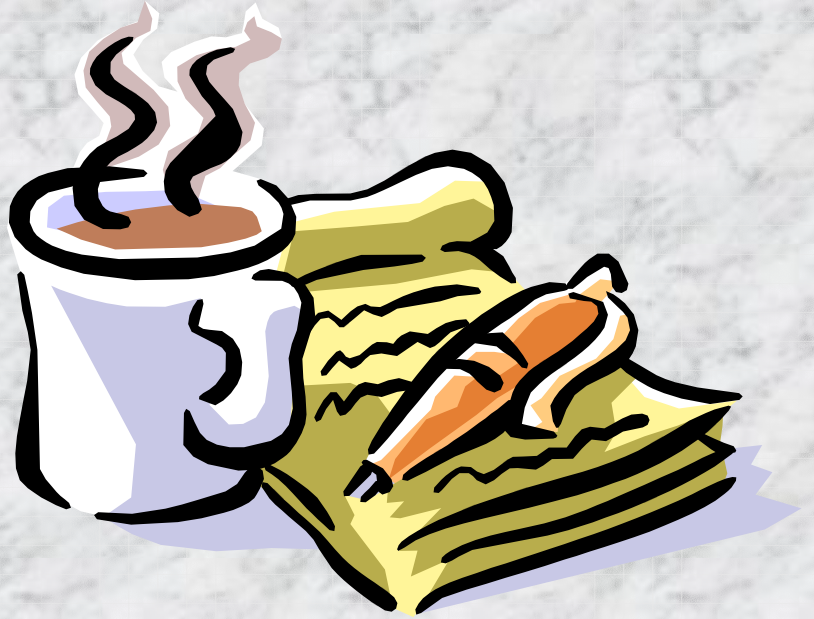
Fieldwork - Analysis



- At some point the data collection stops and the data must be examined and conclusions drawn. Significant items discovered are called findings.

Report writing

- Audit findings are organized and assessed against the client's security policy. Prior to departure from the site either a preliminary or final report is prepared.



Preparing the Audit Report

- Auditors should have strong writing skills. The audit report should be written in a clear and concise manner. The findings should be presented with recommended remedies.

Conducting the Exit Briefing

- The exit briefing provides key players with the information they need to correct the negative findings of the security audit. It should be brief and to the point, drawing on the key conclusions of the audit.

Audits are all part of the show

- The audits are part of a continuing assessment of an organization’s security policy. The auditor may take his bows but he will be back to start the process again.

Conclusion

- Audits are used to examine an organization’s security policy.
- The security policy is both written and unwritten. Auditors have to consider both.
- The audit is less about tools and checklists and more about identifying good and bad security practices in a fair and concise manner.

Resources

- http://www.hhs.gov/ocr/hipaa/
- http://www.ignet.gov/pande/faec/fiscam.pdf
- http://www.isaca.org/cobit.htm
- http://www.iso-17799.com
- http://www.sans.org
- http://www.aicpa.org/info/sarbanes_oxley_summary.htm?
- http://www.securityfocus.com/foundations

Resources - Tools

- http://www.atstake.com
- http://www.cisecurity.org
- http://www.eeye.com
- http://www.foundstone.com/
- http://www.insecure.org/nmap
- http://www.nessus.org
- http://www.networkview.com
- http://www.systernals.com/