CSE 543 Information Assurance and Security

Administrative Security Controls

Professor Stephen S. Yau

Spring 2022



- Logging: Recording of events and statistics to provide information about system use and performance
- Auditing: Analysis of log records to present information about the system in a clear and understandable manner



Auditing (cont.)

- What happened?
- When did it happen?
- Who did it?
- What went *wrong*?
- Who had *access* to key information?

. . .



Auditing Systems

- Three components:
 - Logger: collects data
 - Analyzer: analyzes the collected data
 - Notifier: reports the results of analysis



• Logger:

- The type and quantity of information decided by system or program configuration parameters
- Information may be recorded in binary or human-readable form or transmitted directly to an analysis system



- **Auditable events:**
 - Login
 - Logoff
 - Operating system changes
 - User-invoked operating system commands



- User-invoked applications
- Read of data
- Creation of objects
- Network events

• • •



Analyzer:

- Input from logger and analyzes it.
- Results of analysis may lead to changes in the data being recorded, or detection of some events or problems, or both.
- Example:
 - Used by an intrusion detection system



Notifier:

- Informs the analyst and other entities of the results of the audit.
- Actions may be taken in response to these results.
- Example:
 - When a user's failed login attempts 3 times, the audit system will invoke the notifier, which will report the problem to administrator and disable the account.



Audit Process

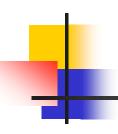
Audit Team

- Federal or State Regulators Certified accountants, CISA from Dept. of Justice, etc.
- Corporate Internal Auditors Certificated accountants, CISA.
- Corporate Security Staff Security managers, CISSP, CISM.
- IT Staff and needed expertise varies



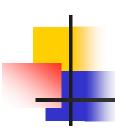
Audit Process (cont.)

- CISA Certified Information Systems Auditor
- CISM Certified Information Systems
 Manager
- CISSP Certified Information Systems Security Professional
- * ISACA (Information Systems Audit and Control Association)



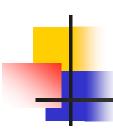
Audit Process (cont.)

- 1. Planning Phase
- 2. Testing Phase
- 3. Reporting Phase



Planning Phase

- Entry Meeting
- Define Scope
- Learn Controls
- Historical Incidents
- Past Audits



Planning Phase (cont.)

- Site Survey
- Review Current IA Policies
- Questionnaires
- Define Objectives
- Develop Audit Plan / Checklist



- Evaluate Audit Plan
 - What data will be collected?
 - How/when the data will be collected?
 - Site employees' involvement?
 - Other relevant questions?



Testing Phase (cont.)

- Data Collection
 - Based on scope/objectives
- Types of Data
 - Activities involving physical security
 - Interview staff
 - Vulnerability assessments
 - Access control assessments



Reporting Phase

- Exit Meeting Short Report
 - Immediate problems
 - Question & answer for site managers
 - Preliminary findings
 - Does NOT give in-depth information



Reporting Phase (cont.)

- Long Report After Going
 Through Data
 - Objectives/scope
 - How data was collected
 - Summary of problems



Reporting Phase (cont.)

- In-depth description of problems
- Glossary of terms
- References
- Any computer misuse or abuse should be reported, and law enforcement may be involved if needed.

S. S. Yau

References

- Michael E. Whitman, Herbert J. Mattord, *Principles of Information Security*, Course Technology, 2018
- M. Merkow, J. Breithaupt, Information Security: Principles and Practices, Prentice Hall, August 2005, ISBN 0131547291
- Matt Bishop, Introduction to Computer Security, Addison-Wesley, 2004, ISBN: 0321247442
- Matt Bishop, Computer Security: Art and Science,
 Addison- Wesley, 2002, ISBN: 0201440997