NISTIR 5495
(Supersedes NISTIR 4846)

Computer Security Training & Awareness Course Compendium

Kathie Everhart
Editor

U.S. DEPARTMENT OF COMMERCE
Technology Administration
National Institute of Standards
and Technology
Gaithersburg, MD 20899

NIST

NISTIR 5495

(Supersedes NISTIR 4846)

Computer Security Training & Awareness Course Compendium

Kathie Everhart
Editor

U.S. DEPARTMENT OF COMMERCE
Technology Administration
National Institute of Standards
and Technology
Gaithersburg, MD 20899

September 1994

U.S. DEPARTMENT OF COMMERCE
Ronald H. Brown, Secretary

TECHNOLOGY ADMINISTRATION
Mary L. Good, Under Secretary for Technology

NATIONAL INSTITUTE OF STANDARDS
AND TECHNOLOGY
Arati Prabhakar, Director

Preface

This National Institute of Standards and Technology (NIST) Interagency Report (NISTIR) is a compendium of computer security training and awareness courses. The purpose of this publication is to assist federal agencies locate computer security training resources. This publication is part of a continuing NIST effort to support federal agencies in accordance with NIST's mandate under the Computer Security Act of 1987. In addition to the table of contents, which lists the courses, there are four appendices: A) lists the courses by training areas within audience categories as defined in NIST Special Publication 500-172, Computer Security Training Guidelines; B) lists the vendors that participated in this effort; C) lists the specific products for which training is available; and D) lists the product specific courses.

NIST Special Publication 500-172 was developed to provide a framework for identifying computer security training requirements for diverse audiences. It focuses on learning objectives based upon the extent to which computer security knowledge is required by individuals as it applies to their job function.

A training matrix was introduced in Special Publication 500-172 to assist agencies in designing training that meets the learning objectives for a particular group. The training and awareness courses in this compendium have been mapped to the matrix (see appendix E) by the training organization/vendor.

NIST makes no claim or endorsement of the computer security courses or their currency in this compendium. Courses listed in this compendium were obtained from a public data call during the 1993 calendar year. The data call consisted of a letter of invitation to known sources of trainers as provided by the Federal Computer Security Program Managers' Forum; and the Federal Information Systems Security Educators' Association (FISSEA). In addition, a NIST CSL Newsletter was disseminated nationwide inviting vendors to participate in this effort. Therefore, this listing is not a complete source of all available security related courses.

Vendors already listed are encouraged to continue to send in changes/updates and new vendors are invited to send in their computer security courses (See address below.) NIST expresses its appreciation to the many federal, academic, and vendor organizations that participated in this effort for their time and interest in mapping their courses to the matrix in NIST Special Publication 500-172. A special thanks to those members of FISSEA who participated in the organization of this compendium.

Questions or comments regarding this publication should be addressed to Kathie Everhart, Office of the Associate Director for Computer Security, Computer Systems Laboratory, Building 225, Room B154, National Institute of Standards and Technology, Gaithersburg, MD, 20899.

Additional copies of this NISTIR may be purchased through the National Technical Information Service, Springfield, VA. 22161, telephone: (703) 487-3238.

TABLE OF CONTENTS

COURSE TITLE

LIST OF APPENDICES

COURSE TITLE: Telecommunications for Information Systems Security Analysts
COURSE LENGTH: 32 HRS

VENDOR:
DATAPRO Educational Services
600 Delran Parkway
Delran, NJ 08076
(609) 764-0100

This course provides an introduction of basic telecommunications systems and mediums for the System Security analyst and an understanding of the integral role they play in successful protection of the system's data. They will learn current regulatory and control concepts, gain a working knowledge of telecommunications principles and develop an understanding of the products and services offered from various vendors. They will also learn proactive techniques that support diverse information transmission mediums and develop an understanding of telecommunication systems vulnerabilities. They will learn how to evaluate the present contingency plan and how to develop a risk analysis formula. They will develop a project plan for contingency implementations of hardware and software that support disaster recovery.

COURSE TITLE: Computer Security Executive Overview
COURSE LENGTH: 3 HRS.

VENDOR:
MACRO International, Inc.
8850 Stanford Boulevard
Columbia, MD 21045
(410) 290-2800

This briefing is designed for executive personnel and will present an overview of applicable laws and other requirements for computer security. The course will emphasize implementation of these requirements at the executive management level, and the role of senior management in supporting security initiatives.

COURSE TITLE: ADP Security Officers (ADPSO) Concepts
COURSE LENGTH: 8 HRS

VENDOR:
Naval Computer and Telecommunications Station
ATTN Code N823
PO Box 357056
San Diego, CA 92135-7056
(619) 545-8628 - DSN 735-8628

This one-day course is an overview of what is involved in implementing a command AIS Security Program and discusses the DoD and DON Minimum Program Requirements policy. This course is excellent for a beginner ADPSO or other AIS Security staff members. The course outlines the responsibilities of DON management and command AIS Security Staff members, identifies the steps necessary for accreditation, and the structure of the DON AIS Security Program which includes a discussion on the Controlled Access Protection (CAP) Guidebook (NAVSO P-5239-15). The course discusses aids in solving common AIS Security problems and discusses methods in determining system security levels. This course is conducted at the NAVCOMTELSTA San Diego facility or at your command.

COURSE TITLE: Computer Security For End Users
COURSE LENGTH: 1 DAY

VENDOR:
USDA, Graduate School
600 Maryland Ave, SW
Washington, DC 20024
(202) 447-7124

This workshop will give you an overview of the threats to, and vulnerabilities of, computer systems, and appropriate safeguards to protect those systems. We will stress your role in the protection of sensitive data, and in the prevention and detection of computer crime. You will receive checklists and suggestions for becoming more aware of possible computer security problems in your office, and you will be able to get advice on how to deal with concerns that are specific to your agency or installation.

COURSE TITLE: Computer Security For Executives
COURSE LENGTH: 3 HRS

VENDOR:
USDA, Graduate School
600 Maryland Ave, SW
Washington, DC 20024
(202) 447-7124

This briefing will give you a basic understanding of computer security. It includes an overview of threats and vulnerabilities to computer systems and your responsibility for the assessment of your agency's computer security program. We will review briefly the history of computers, then examine current dependencies on computers, applicable laws and regulations, computer crime, viruses, and touch on espionage. Bring your questions because the briefing is designed to be responsive to your needs. Time has been reserved at various points for you to raise concerns from your individual agency perspective.

COURSE TITLE: Computer Security Awareness Training
COURSE LENGTH: 3 HRS

VENDOR:
GSA Training Center
P.O. Box 15608
Arlington, VA 22215-0608
Joan Bender: (703) 603-3213

Participants learn to be aware of threats to and vulnerabilities of computer systems, as well as to encourage use of improved security practices. Topics include: Computer Security Act of 1987; computer fraud, waste, and abuse; and types of computer hackers. Also discussed are natural disasters and human errors relating to computer security.

COURSE TITLE: Information Risk Assessment & Security Management
COURSE LENGTH: 1 SEM

VENDOR:
University of Maryland, University College
University Boulevard at Adelphi Road
College Park, MD 20742-1614
(301) 985-7155

An examination of the proliferation of corporate data bases and the development of telecommunications network technology as gateways or invitations to intrusion. Ways of investigating the management of the risk and security data and data systems are presented as a function of design through recovery and protection. Issues of risk and security, as they relate to specific industries and government, are major topics in the course. Examples are presented of how major technological advances in computer and operating systems have placed data, as tangible corporate assets, at risk. Both quantitative sampling techniques for risk assessment and for qualitative decision-making under uncertainty are explored.

COURSE TITLE: Federal AIS Computer Security Requirements
COURSE LENGTH: 1 DAY

VENDOR:
COMSIS
8737 Colesville Road, Suite 1100
Silver Spring, MD 20910
Ronald E. Freedman: (301) 588-0800

This course begins with a review of the Federal Computer Security framework and an introduction to the key players and legislation that has shaped Federal Computer Security policy.

COURSE TITLE: Information Systems Seminar For Internal Auditors
COURSE LENGTH: 5 DAY

VENDOR:
Ernst & Young
2000 National City Center
Cleveland, OH 44114
Morton T. Siegel: (800) 289-5745

This introductory seminar of computer concepts and controls is designed for the MIS or internal auditing professional who needs to learn about basic computer concepts, computer controls and security, system life cycle planning and control, and contingency planning. Individuals with these backgrounds who complete this seminar will be exposed to every major aspect of information systems auditing and should be able, with the tools provided in the seminar, to perform basic IS Audits. In addition, the seminar will emphasize how ISA is integrated with the internal audit process. This is a five-day, classroom program consisting of stand-alone modules that can be presented as a whole or modules can be selected to provide training on specific subjects in shorter-duration programs. Call the vendor for more information regarding which of the following modules have been selected for this particular training area.
Module 1-Introduction to the Seminar
Module 2-Information Systems Auditor's Role
Module 3-Getting Started
Module 4-Planning the IS Audit
Module 5-Overview of the ISA Function
Module 6-Overview of Computer Operations
Module 7-A Management Approach to Computer Fraud
Module 8-Introduction to General Controls
Module 9-Organization and Administration
Module 10-System Development Life Cycle
Module 11-Change Control and Management
Module 12-Case Study
Module 13-The Time Bomb
Module 14-Access Control
Module 15-Case Study
Module 16-Program Execution
Module 17-Continuity of Operations
Module 18-Outsourcing and Other Alternative Processing

Module 19-Cloak and Data
Module 20-Data Bases
Module 21-Minicomputer Systems-Audit and Control Considerations
Module 22-Microcomputers-Audit and Control Considerations
Module 23-Introduction to Application Control Reviews
Module 24-Input Control Objectives and Procedures
Module 25-Case Study-Input Controls
Module 26-Processing Control Objectives and Procedures
Module 27-Output Control Objectives and Procedures
Module 28-Case Study-Processing and Output Controls
Module 29-Generalized Audit Software and Other CAATs
Module 30-Summary

COURSE TITLE: EDP Concepts For Business
COURSE LENGTH: SELF-PACED

VENDOR:
Ernst & Young
2000 National City Center
Cleveland, OH 44114
Morton T. Siegel: (800) 289-5745

EDP Concepts for Business is an interactive computer-based training (CBT) program. The student receives information and is coached based upon the answers to teaching questions. This was designed to involve the student, be flexible, and be responsive to the student's needs; this format focuses on the student. You need only an IBM PC, XT, AT, or any IBM-compatible microcomputer with at least 192K memory. Call the vendor for more information regarding which of the following modules have been selected for this particular training area.
Module 1-Computers and Their Components
Module 2-Data and Data Processing
Module 3-Programs and Languages
Module 4-The System Development Life Cycle
Module 5-EDP Personnel
Module 6-Access Control and Security

COURSE TITLE: Computer Security Awareness
COURSE LENGTH: 1 HR

VENDOR:
Booz-Allen & Hamilton Inc.
8283 Greensboro Drive
McLean, VA 22102-3838
(703) 902-5201

The purpose of this course is to provide participants with an awareness of computer security, to sensitize them to the need for computer security policies and practices in the workplace, and to motivate each individual to practice effective computer security techniques. The instructional content of the course is composed of:requirements of computer-security-related laws and circulars; definitions and examples of basic computer security terms; the increasing concern to protect computer assets; and basic computer practices, controls, and countermeasures. NOTE:Contact the vendor for information concerning specialized agency training.

COURSE TITLE: Microcomputer Security
COURSE LENGTH: 2 HRS

VENDOR:
Booz-Allen & Hamilton Inc.
8283 Greensboro Drive
McLean, VA 22102-3838
(703) 902-5201

The purpose of this microcomputer security course is to sensitize participants to the need for microcomputer security and to provide each individual with some practical tools to protect their microcomputer assets, especially the stored information. The course provides practical information on computer security that microcomputer users can implement immediately. NOTE:Contact the vendor for information concerning specialized agency training.

COURSE TITLE: Computer Security Awareness (CBT)
COURSE LENGTH: 5-8 HRS

VENDOR:
DPEC
1679 Old Henderson Road
Columbus, OH 43220-3644
(800) 223-3732

This is a Computer Based Training (CBT) course using the framework of administrative, physical and logical security. Computer Security Awareness explains contingency planning and precautions against computer crime from the viewpoint of mainframe computers and micros; a computer security checklist is included. This is a modular course lasting 5 - 8 hours. The number of hours is based upon a student interacting with approximately 60-120 screens per hour.

COURSE TITLE: Marketplace Implications of the Evolution of Evaluation Criteria
COURSE LENGTH: 8 HRS

VENDOR:
Grumman Data Systems & Services
839 Elkridge Landing Rd. Suite 106
Linthicum, MD 21090
Bruce Levy
(410) 859-0123

This seminar covers the current state of the Evolution of Trusted Computer Product Evaluation schemes, of North America and Europe, the products which are evaluated and the conclusions which can be drawn. The discussions will concentrate on the US Federal Criteria and the implications of the proposed Common Criteria, for the marketplace in general, and for the integration of COTS products specifically. The briefing is designed to be responsive to your needs, and time is reserved for in-depth discussions of issues which affect you most critically.

COURSE TITLE: The Systems Integrator's Perspective on AIS Security Strategies
COURSE LENGTH: 8 HRS

VENDOR:
Grumman Data Systems & Services
839 Elkridge Landing Rd. Suite 106
Linthicum, MD 21090
Bruce Levy: (410) 859-0123

This course presents the application of system integration and composition concepts to the management and acquisition of AIS, especially where sensitive data is concerned. A major portion of the seminar concentrates on determining the security implications of alternative approaches and involvement of the appropriate players during the acquisition process. Managers responsible for the acquisition of sensitive computing resources will benefit from this seminar.

COURSE TITLE: Continuity of Operations/Disaster Recovery Planning: Part I
COURSE LENGTH: 1 DAY

VENDOR:
COMSIS
8737 Colesville Road, Suite 1100
Silver Spring, MD 20910
Ronald E. Freedman: (301) 588-0800

This course outlines the steps to be performed to determine backup/recovery requirements, and effectively plan and develop a COOP/DRP for both applications and installations.

COURSE TITLE: Executive AIS Security Briefing
COURSE LENGTH: 1/2 DAY

VENDOR:
COMSIS
8737 Colesville Road, Suite 1100
Silver Spring, MD 20910
Ronald E. Freedman: (301) 588-0800

This course provides a brief overview of Federal Computer Security requirements and objectives and explores Senior Managements role in protecting assets.

COURSE TITLE: Keeping Out of Trouble with the Software Police
COURSE LENGTH: 1 DAY

VENDOR:
MIS Training Institute
498 Concord Street
Framingham, MA 01701-2356
Sharon G. Friedman: (508) 872-7990

The common practice of copying and sharing is no longer being tolerated by software publishers. Organized under the umbrellas of the Software Publishers Association (SPA), they are waging an all-out war against abusers of copyright law. In this special, one-day session, you will learn how to keep your organization "software legal." Without a lot of confusing "legalese," you will learn: what you need to know about software license and copyright laws; the methods being used to enforce software licenses and to prosecute copyright infringement; how to recognize potential violations in your organization; and step-by-step guidelines for establishing and implementing a practical code of software ethics.

COURSE TITLE: LAN Security Overview
COURSE LENGTH: 16 HRS

VENDOR:
DATAPRO Educational Services
600 Delran Parkway
Delran, NJ 08076
(609) 764-0100

This course will provide the Systems Security analyst with a basic understanding of the security implications of the Local Area Networks and familiarize the students with the functional considerations of LAN security routines. The class format will provide a controlled forum for the analyst to discuss the various security routines and procedures currently in use by the government, their establishment and design. there will also be discussions on the various types of security measures integrate into the Network Operating Systems of Novell, Banyan, SCO UNIX and Starian.

COURSE TITLE: PC-LAN and Data Security
COURSE LENGTH: 40 HRS

VENDOR:
DATAPRO Educational Services
600 Delran Parkway
Delran, NJ 08076
(609) 764-0100

This course is intended to give a perspective of the various types of security threats to the first and second level managers of the Telecom and MIS departments. It has a broad scope, however, it provides a good foundation for future courses to focus on individual issues and develop security plans.

COURSE TITLE: Advanced Technology Conference
COURSE LENGTH: 3 DAYS

VENDOR:
The Institute of
Internal Auditors
249 Maitland Avenue
Altamonte Springs, FL 32701
(407) 830-7600 ext. 1

The Institute of Internal Auditors' annual Advanced Technology Conference presents world-renowned technology experts who will share the solutions, tools, and techniques needed to validate and enhance job performance.

This interactive program addresses a variety of technology challenges that auditors face. Attendees are provided the opportunity to stay on top of emerging trends as well as the knowledge to utilize the tools and techniques available for auditing today's technology.

Security professionals will find the sessions informative from the standpoint of learning the business concerns, risks, and related control techniques involved in current and emerging technology.
Participants have the opportunity to:

- Discuss the newest advances in audit technology.
- Hear the most informed and experienced speakers.
- Understand cutting-edge emerging technologies.

The conference provides a forum in which to learn and exchange information on all aspects of audit, control, and security technologies.

COURSE TITLE: Introduction to LAN Security
COURSE LENGTH: 3 DAYS

VENDOR:
MIS Training Institute
498 Concord Street
Framingham, MA 01701-2357
(508) 872-7999

Protecting increasingly sensitive LANs is now the most critical security issue facing today's enterprise. In this intensive, three-day seminar you will benefit from and experience-based, real-world approach to LAN security. You will gain an understanding of basic LAN technology and security threats. You will learn the specific components that ensure a solid LAN security program and how security should be designed into the system. You will leave this high-impact session prepared to plan and implement effective and responsive LAN

COURSE TITLE: Detecting and Preventing Computer Fraud
COURSE LENGTH: 3 DAYS

VENDOR:
MIS Training Institute
498 Concord Street
Framingham, MA 01701-2357
Sharon G. Friedman: (508) 872-7990

As the gap between computer technology and computer security widens, IS and Internal Auditors are relied upon more than ever to ensure the integrity and security of organizational data. In this high-impact seminar you will focus on the risks and threats inherent in computer environments and the controls that are necessary to assure management that exposures are held to acceptable levels. Through case studies and "real-life" exercises, you will explore areas of computer fraud, risk management, and treats. You will leave this three-day seminar knowing the controls for preventing computer fraud and methods for detecting it, should it occur.

COURSE TITLE: Practical Aspects of Acquiring and Owning a Multilevel Secure Network
COURSE LENGTH: 8 HRS

VENDOR:
Grumman Data Systems & Services
839 Elkridge Landing Rd. Suite 106
Linthicum, MD 21090
Bruce Levy: (410) 859-0123

Objectives of the course: Give managers and Technical personnel the tools to make appropriate acquisition and operating decisions regarding MLS Information Systems. Following custom modules:

Module A. The Technology with MLS added. Mandatory Access Control labels, Exploring operational impacts of MLS: MAC vs DAC - vulnerabilities New audit considerations - impact of MLS and MAC on the makeup and sensitivity of the Audit Trail data.

Module B. The Environment with MLS added. Impact of an MLS accreditation on configuration management. Hardware, ancillary equipment, software, especially upgrading to new functionality. Maintaining accreditation - documentation for the Life cycle A checklist of warning signs for the Admin/Security staff Addressing security violations (vulnerabilities) in the MLS environment. How to use the CERT to best advantage.

Module C. Acquisition of Trusted Systems. A seminar for local procurement initiators, managers, and procurement technicians to review the appropriate usage of language in an RFP for Trusted Systems, or MLS Network components. This seminar discusses specification language for the SOW, how to use CDRLs for acquiring Assurance documentation, and pitfalls to avoid in preparation of the procurement plan.

COURSE TITLE: Practical Considerations for Acquiring and Implementing a MultiLevel Secure Network
COURSE LENGTH: 8 HRS

VENDOR:
Grumman Data Systems & Services
839 Elkridge Landing Rd. Suite 106
Linthicum, MD 21090
Bruce Levy: (410) 859-0123

Objectives of the Course: Give managers and technical personnel the tools to select acquire and implement cost effective security technologies in information systems.

Module A. Sorting out the technologies defined by NCSC
A discussion of the subtleties of the "Rainbow" books

Module B. Overview of the State-of-the-Art
A Look beyond the Hype at the marketplace of Trusted Systems

Module C. Acquisition of Trusted Systems: A seminar for local procurement initiators, managers, and procurement technicians to review the appropriate usage of language in an RFP for Trusted Systems, or MLS Network components.

COURSE TITLE: Practical Aspects of Planning to Acquire Multilevel Security in an Open Systems Environment
COURSE LENGTH: 8 HRS

VENDOR:
Grumman Data Systems & Services
839 Elkridge Landing Rd. Suite 106
Linthicum, MD 21090
Bruce Levy: (410) 859-0123

Objectives of the Course: Give managers and technical executives the tools to plan and acquire cost effective technologies for ensuring the enforcement of their security policies in information systems.Custom modules include:

Module A. Organizational Responsibilities
DoD Security Policy Refresher. complying with DoD Inst 5200.28

Module B. Understanding which Technology is for which Problem
(Getting there -from here)

Module C. Acquisition of Trusted Systems

A seminar for local procurement initiators, managers, and procurement technicians to review the appropriate usage of language in an RFP for Trusted Systems.

COURSE TITLE: Practical Considerations for Planning and Implementing Multilevel Security in an Open Systems Environment
COURSE LENGTH: 16 HRS

VENDOR:
Grumman Data Systems & Services
839 Elkridge Landing Rd. Suite 106
Linthicum, MD 21090
Bruce Levy: (410) 859-0123

Objectives of the Course: Give technical executives the tools to plan and select cost effective technologies and to make cost-effective Operational decisions regarding the enforcement of their security policies in MLS Information Systems. This course is a tailored set of modules customized from among:
Organizational Responsibilities [2 hrs]
Sorting out the technologies defined by NCSC [4 hrs]
Overview of the State-of-the-Art [2 hrs]
Understanding which Technology is for which Problem
(Getting there -from here) [3 hrs]
The Technology with MLS added [3 hrs]
The Environment with MLS added [2 hrs]

COURSE TITLE: Case Studies in Multilevel Secure Networking
COURSE LENGTH: 8 HRS

VENDOR:
Grumman Data Systems & Services
839 Elkridge Landing Rd. Suite 106
Linthicum, MD 21090
Bruce Levy: (410) 859-0123

Objectives of the course: Give on-site managers and Technical personnel tools based on specific local cases, to make cost-effective Operational decisions regarding migration to MLS Information Systems. This briefing will cover: The Customer Environment with MLS Added, Identifying your accreditor, Reviewing requirements for Internal Review Audits, Coordinating with the CM/QA team on-site, Tracing the flow of ADP Security Reporting Reviewing specific responsibilities and requirements for co-location of CRYPTO or other NSA approved/controlled items, Exploring which state-of-the-art systems might meet specific local requirements, while being within the range of our resources. Sampler of Evaluated Operating Systems, Workstations, Networking Components and Specialty Components. Specific information about levels of expertise required to implement a system on-site with them.

COURSE TITLE: Managing the Acquisition of MLS Resources
COURSE LENGTH: 4 HRS

VENDOR:
Grumman Data Systems & Services
839 Elkridge Landing Rd. Suite 106
Linthicum, MD 21090
Bruce Levy: (410) 859-0123

Objectives of the course: Give on-site managers and Technical personnel tools to make cost-effective procurement decisions regarding migration to MLS Information Systems. Specific topic discussed: Acquisition of Trusted Systems: A seminar for local procurement initiators, managers, and procurement technicians to review the appropriate usage of language in an RFP for Trusted Systems, or MLS Network components. This seminar discusses specification language for the SOW, how to use CDRLs for acquiring Assurance documentation, and pitfalls to avoid in preparation of the procurement plan. You will also receive a copy of the NSA and NIST Acquisition guidance for trusted systems.

COURSE TITLE: Practical Aspects of Owning a Multilevel Secure Network
COURSE LENGTH: 8 HRS

VENDOR:
Grumman Data Systems & Services
839 Elkridge Landing Rd. Suite 106
Linthicum, MD 21090
Bruce Levy: (410) 859-0123

Objectives of the course: Give managers and Technical personnel the tools to make cost-effective Operational decisions regarding MLS Information Systems. Course Curriculum consists of: The Technology with MLS added The Information Systems equivalents to Markings, Caveats, handling instructions - Mandatory Access Control labels Exploring operational impacts of MLS: MAC vs DAC-vulnerabilities New audit considerations - impact of MLS and MAC on the makeup and sensitivity of the Audit Trail data. Tracking an atomic action through several audit trails. Enhancing the security profile of an MLS system Impact of an MLS accreditation on Configuration Management A checklist of warning signs for the Admin/Security staff Addressing security violations How to use the CERT to best advantage Impact of having a CRYPTO in the closet. You will receive checklists and suggestions for operating sensitive systems daily.

COURSE TITLE: Practical Considerations for Implementing a MultiLevel Secure Network
COURSE LENGTH: 8 HRS

VENDOR:
Grumman Data Systems & Services
839 Elkridge Landing Rd. Suite 106
Linthicum, MD 21090
Bruce Levy: (410) 859-0123

Objectives of the Course: Give managers and technical personnel the tools to select and use cost effective security technologies in information systems. Specific topics: technologies defined by NCSC The TCSEC "Orange Book", The TNI "Red Book": MIAD components, The TDI "Purple Book": TCB subsets, The CSSI "Powder Blue Book": components which support the security policy in a more restrained fashion, The ISSPSC: there's more in there than the EPL. The definitive catalog of NSA evaluated technology. A Look beyond the Hype at the marketplace of Trusted Systems IBM's MVS/ESA RACF (B1), CA's B1 Security Amdahl's Trusted MDF, Unisys OS-1100 (B1)Workstations CMWs Networks and components Xerox XEU, LEAD, Motorola NES, Blacker A sampler of specialty components (subsystems) Making an informed decision to use non-evaluated product and the cost of getting smart enough to be able to evaluate it yourself.

COURSE TITLE: Practical Considerations for Planning Multilevel Security in an Open Systems Environment
COURSE LENGTH: 8 HRS

VENDOR:
Grumman Data Systems & Services
839 Elkridge Landing Rd. Suite 106
Linthicum, MD 21090
Bruce Levy (410) 859-0123

Objectives of the Course: Give managers and technical executives the tools to plan and select cost effective technologies for planning the enforcement of their security policies in information systems. Specific topics: Organizational Responsibilities DoD Security Policy Refresher, Complying with DoD Inst 5200.28, Accreditation Requirements, What Certification means, How Evaluation helps, Documentation of your system (network), Cost effective steps toward MLS, Avoiding common password headaches, Some Practical approaches to all that Audit trail. You will get expert advice on what works and what your installation needs to enter the distributed age of computing.

COURSE TITLE: Introduction to Computer Security for First-Level Supervisors
COURSE LENGTH: 8 HRS.

VENDOR:
MACRO International, Inc.
8850 Stanford Boulevard
Columbia, MD 21045
(410) 290-2800

This program is designed for first-level supervisors and emphasizes the role of the supervisor in implementing and managing computer security programs. The course discusses approaches for instilling security awareness in staff, training, security administration, and incident management and reporting. An overview of threats, protection strategies, and implementation of policies and procedures is presented, emphasizing requirements for different levels of system sensitivity.

COURSE TITLE: Introduction to Computer Security for Non-ADP Managers
COURSE LENGTH: 8 HRS.

VENDOR:
MACRO International, Inc.
8850 Stanford Boulevard
Columbia, MD 21045
(410) 290-2800

This program is designed to provide mid-level managers with an overview of computer security program planning and management. Presentation will emphasize compliance with P.L. 100-235 and other laws and requirements for classified and unclassified systems. Discussion will also emphasize the threat against sensitive systems; capabilities of potential adversaries; asset value; sensitivity and definition of protection levels appropriate to the threat; contingency planning; and management risk acceptance. The course will also cover the development of security plans emphasizing human resource management practices, the implementation of computer security programs within budget and staff constraints.

COURSE TITLE: Computer Security for Security & ADP Program Managers
COURSE LENGTH: 3 DAYS

VENDOR:
MACRO International, Inc.
8850 Stanford Boulevard
Columbia, MD 21045
(410) 290-2800

This course is designed for ADP program managers and computer security program managers. It provides an overview of Public Law 100-235 and other laws and requirements for computer security. Discussion will emphasize various types of threats against sensitive systems; capabilities of potential adversaries; areas of vulnerability; and control techniques.

This course provides a comprehensive understanding of the full range of potential threat and the effectiveness of alternative security controls against different threats. This course is oriented toward those with prior programming and systems development experience.

COURSE TITLE: Information Security Principles and Practices
COURSE LENGTH: 4.5 DAYS

VENDOR:
George Mason University
Department of Information & Software Systems Engineering
School of Information Technology and Engineering
Fairfax, VA 22030-4444
Ravi Sandhu: (703) 993-1659

This course introduces fundamental issues and concepts of information security, emphasizing the Trusted computer System Evaluation Criteria (TCSEC), which is the seminal publication providing authoritative guidance concerning trust technology; and its eventual successor, the Federal Criteria for Information Technology Security. Security policy, risk management, certification and accreditation are discussed in their supporting roles. The threat of viruses and other rogue programs is discussed; a case study reinforces the lessons learned. Practical advice for trusted system integration is provided.

COURSE TITLE: COMPUSEC
COURSE LENGTH: 2 DAYS

VENDOR:
Security Engineering Services, Inc.
5005 Bayside Road
Chesapeake Beach, MD 20732
Bruce Gabrielson: (301) 855-4565

This class is an unclassified overview of COMPUSEC requirements, issues and related COMSEC and TEMPEST information. Attendees should be able to intelligently address technical vulnerability issues in their ADP systems.

Topics Covered
Laws and DoD Specifications, Trusted Computer Systems, Risk Management, Configuration Management, Data Remnance, Software Disk Protection, Virus Protection, Network Overviews, COMSEC Protection,
TEMPEST Protection, OPSEC Issues
Student Background: Intended for entry level security people.

COURSE TITLE: Basics of Computer Security
COURSE LENGTH: 2 DAYS

VENDOR:
Thomas R. Hardy & Associates, Inc.
P.O. Box 5631
Derwood, Maryland 20855
(301) 921-0595

This course is designed for end users and management personnel - it presents the elements necessary for developing a secure computer system environment. The class addresses the needs of small and large systems, and network configuration. Topics include: Planning and design; Threats and Vulnerabilities; Countermeasures; Contingency planning and disaster recovery; Backup site planning; Responsibilities.

COURSE TITLE: Understanding Trusted Systems
COURSE LENGTH: 1 DAY

VENDOR:
Booz•Allen & Hamilton
8th Floor, Room 822
8283 Greensboro Drive
McLean, VA 22102-3838
Butch Chaboudy: (703) 902-5265

This course provides an understanding of the Trusted System Evaluation Criteria (Orange Book) and the Trusted Network Criteria and Trusted Database Management interpretation. The student will gain a working knowledge of the security fundamentals, the features of each class and the assurance required of these features. Additionally, the student will be introduced to other appropriate rainbow series books.

COURSE TITLE: Implementing & Managing a Computer Security Program
COURSE LENGTH: 1 DAY

VENDOR:
COMSIS
8737 Colesville Road, Suite 1100
Silver Spring, MD 20910
(301) 588-5922

This course provides an overview of a computer security program, and describes the requirements and rationale for each program element.

COURSE TITLE: Risk Assessment
COURSE LENGTH: 1 DAY

VENDOR:
COMSIS
8737 Colesville Road, Suite 1100
Silver Spring, MD 20910
(301) 588-5922

This course provides a global examination of computer security risk assessment and the techniques for applying risk assessment.

COURSE TITLE: Disaster Recovery Planning: Strategies to Develop and Maintain Provable Recovery Capability (W9912)
COURSE LENGTH: 2.5 Days

VENDOR:
Skill Dynamics - An IBM Company
One IBM Plaza, 19th Floor
Chicago, IL 60611
(800) IBM-TEACH (800) 426-8322

This course teaches you how to develop, maintain, and test your disaster recovery plan. The objective is to develop provable recovery capability, not paper documentation. The focus is on what the organization - I/S and the business functions - must put in place now, keep current and test to the satisfaction of responsible executives that the business can survive the loss of processing capability. The course discusses strategies that are independent of any particular hardware or software implementation. This is a management course, not a technical course.

COURSE TITLE: Data Center Recovery Planning (M2040)
COURSE LENGTH: 2.5 Days

VENDOR:
Skill Dynamics - An IBM Company
One IBM Plaza, 19th Floor
Chicago, IL 60611
(800) IBM-TEACH (800) 426-8322

This course provides you with a basic understanding of the disaster recovery planning process within a data center environment. The course focuses on the recovery of the data center and communications to and from business units/departments. All phases of the recovery planning process, from disaster declaration through relocation to a new facility, are discussed

COURSE TITLE: PC/LAN Recovery Planning (M2042)
COURSE LENGTH: 2.5 Days

VENDOR:
Skill Dynamics - An IBM Company
One IBM Plaza, 19th Floor
Chicago, IL 60611
(800) IBM-TEACH (800) 426-8322

This course provides you with a basic understanding of the disaster recovery planning process encompassing personal computers (PCs) and local area networks (LANs). The course focuses on the recovery of stand-alone PCs, LANs (the file server environment), and LAN communications to and from business units/departments. All phases of the recovery planning process, from disaster declaration through relocation to a new facility, are discussed.

COURSE TITLE: Business Impact Analysis (M2044)
COURSE LENGTH: 2 Days

VENDOR:
Skill Dynamics - An IBM Company
One IBM Plaza, 19th Floor
Chicago, IL 60611
(800) IBM-TEACH (800) 426-8322

This course teaches you how to perform a risk analysis to ascertain the impact that a disaster may have on your business. You will also learn how to analyze your important business functions and the consequences, if lost, to the organization. You will learn the time period after which this loss becomes critical and the priorities that each important business function has within the overall recovery process. You'll learn to use a process involving a thorough impact analysis focusing on all aspects of the business, not just computerized processes. The course enables you to build an impact analysis and better understand your overall business process.

COURSE TITLE: Business Resumption Planning (M2046)
COURSE LENGTH: 2.5 Days

VENDOR:
Skill Dynamics - An IBM Company
One IBM Plaza, 19th Floor
Chicago, IL 60611
(800) IBM-TEACH (800) 426-8322

This course teaches you the many facets of preparing a Business Resumption Plan (BRP). To be able to resume normal business operations within an organization after a serious outage, an effective recovery plan must be in place. This course focuses on the business reasoning of such a plan and identifies some of the obstacles that will have to be overcome. Having a Business Resumption Plan in place may prevent unnecessary loss to your organization if a disaster affects your manual or automated business functions. The course shows how to build an effective BRP for your organization. Full attention will be given to the different aspects of the plan, auditors who must review the competency of an organization's recovery plans.

COURSE TITLE: Network Recovery Planning (M2056)
COURSE LENGTH: 2.5 Days

VENDOR:
Skill Dynamics - An IBM Company
One IBM Plaza, 19th Floor
Chicago, IL 60611
(800) IBM-TEACH (800) 426-8322

This course teaches you the fundamentals of handling adverse conditions on networks and recovering functionality even after complete shutdown or network failure. Different data exchange protocols and their benefits and vulnerabilities are presented along with the use of servers, routers, and gateways. Typical local area networks (LANs) and wide area networks (WANs) that mix topologies are also examined. Particular attention is given to preventing the network failure or shutdown, and to minimizing its effect.

COURSE TITLE: Data Security Planning: Strategies for Effective Information Security (W9898)
COURSE LENGTH: 2.5 Days

VENDOR:
Skill Dynamics - An IBM Company
One IBM Plaza, 19th Floor
Chicago, IL 60611
(800) IBM-TEACH (800) 426-8322

This course teaches you how to plan and implement data security. It is based upon and uses examples from successful programs. It takes an organizational view of information and presents many policies, standards and guidelines of IBM and other organizations. The course discusses strategies that are independent of any particular hardware or software implementation. This is a management course, not a technical course. The course discusses programs and processes within the context of end-user computing and shows how they can enhance protection.

COURSE TITLE: Protecting Your Networks from Hackers, Viruses, and Other Attacks
COURSE LENGTH: 3 DAYS

VENDOR:
MIS Training Institute
498 Concord Street
ramingham, MA 01701-2357
Sharon G. Friedman: (508) 872-7999

Hackers, phone phreaks, viruses, corporate spies, and disgruntled employees are all real threats to today's organizations. In this three-day technical seminar you will examine the nature of these significant security threats and vulnerabilities. You will learn practical, cost-effective security and audit techniques that will dramatically improve your success in reducing risk while enabling you to go systematically monitor your organization's security strengths and weakness. You will leave this high-tech session with sample checklists, a set of valuable software tools, and "how-to" reference materials that will increase your effectiveness and decrease of attacks on your network.

COURSE TITLE: How to Manage an Information Security Program A Guide for Newly Appointed Managers
COURSE LENGTH: 3 DAYS

VENDOR:
MIS Training Institute
498 Concord Street
Framingham, MA 01701-2357
Sharon G. Friedman: (508) 872-7999

This three-day session will be your guide to establishing and managing a workable information security program. You will learn the components of a comprehensive plan, covering access control software applications; telecom/network security measures; physical protection of the computer facility; and the legal and regularity aspects of information security. You will learn how to protect your organization from computer crime and viruses. You will explore disaster recovery and the key elements of an effective business continuity program. You will leave this session with a blueprint for building an information security program or for measuring an existing one.

COURSE TITLE: Audit and Security of Client/Server Architectures
COURSE LENGTH: 3 DAYS

VENDOR:
MIS Training Institute
498 Concord Street
Framingham, MA 01701-2357
Sharon G. Friedman: (508) 872-7999

As more critical applications continue to move onto networks, the open architecture concept, a lack of true separation of duties, poor administration, and often unfamiliar network tools leave organizations open to risk. In this timely seminar you will review the basics of client/server architectures, uncover the risks within the technology, and identify cost-effective controls for plugging these loopholes. You will learn how to spot poorly designed client/server applications and how to identify connection risks. You will explore communications protocols, distributed databases, and the most commonly used network operation systems, including NetWare, VINES, Unix, NT and OS/2. You will leave this in-depth seminar with a checklist that you can use as a foundation for a customized workplan for your own client/server audits.

COURSE TITLE: A Fraud Update: Forensic and Investigative Auditing
COURSE LENGTH: 3 DAYS

VENDOR:
MIS Training Institute
498 Concord Street
Framingham, MA 01701-2357
Sharon G. Friedman: (508) 872-7999

As incidents of fraud continue rise, management now more than ever looks to Audit as its first line of defense against this bottom-line busting crime. Using case studies and interactive exercises, this three-day seminar will be your road map through the major fraud concerns facing organizations today. You will cover investigative principles, forensic auditing, rules of evidence, and federal fraud statue and sentencing guidelines. You will learn how to develop evidence to support fraud allegations and what the responsibilities of the audit committee are when fraud is discovered. This high-impact session will provide you with a solid understanding of contemporary fraud issues and Audit's role in protecting the organization from this pervasive and complicated crime.

COURSE TITLE: Risk Management
COURSE LENGTH: 24 HRS

VENDOR:
Naval Computer and Telecommunications Station
ATTN Code N823
PO Box 357056
San Diego, CA 92135-7056
(619) 545-8628 - DSN 735-8628

This three-day course is a comprehensive study of Risk Management and is given in a workshop type environment. This course will provide the attendee with a definition of what comprises Risk Management and will explain the different components of Risk Management. Instruction will consist of discussion on Risk Analysis, Contingency Planning, and Security Test and Evaluation (ST&E). Attendees will have a thorough understanding of each of these Risk Management phases and how to prepare them. Course will provide the attendee with actual hands-on exercises for each of these phases. Risk Analysis instruction will include preparation of a Risk Analysis using the three different methods. Also the Risk Analysis portion will include principles for performing a Risk Analysis on a Local Area Network (LAN). Strongly recommend completion of the ADPSO Concepts course before taking this course. This course is conducted at the NAVCOMTELSTA San Diego facility or at your command.

COURSE TITLE: Recent Developments in Information Security
COURSE LENGTH: 4.5 DAYS

VENDOR:
George Mason University
Department of Information & Software Systems Engineering
School of Information Technology and Engineering
Fairfax, VA 22030-4444
Ravi Sandhu: (703) 993-1659

This intensive course presents a comprehensive approach to recent developments in Information Technology (IT) security. Technology and policy issues for secure operations employing both Computer Security (COMPUSEC) and Communications Security (COMSEC) components of Information Security (INFOSEC) are presented. Contemporary issues addressed include: encryption, key escrow, and key management for authentication, integrity, and confidentiality; proposed standards such as Digital Signature and Clipper; challenges in developing international criteria; database issues such as polyinstantiation, inference, and aggregation; and access control beyond the TCSEC (Orange Book).

Discussions will include the use of empirical and theoretical computer and database system and network design approachers. Broader issues will also be presented, such as integrating security with computer, database, and network systems design and development requirements; and evaluating the degree of security available for a given computer, database and/or network system. Extensive practical advice for trusted system integration is provided.

COURSE TITLE: Secure Systems Design and Program Management
COURSE LENGTH: 2 DAYS

VENDOR:
Security Engineering Services, Inc.
5005 Bayside Road
Chesapeake Beach, MD 20732
Bruce Gabrielson: (301) 855-4565

Participants learn technical rational and requirements that lead to formal management decision making regarding security issues. Topics Covered: Org. Security, Systems Security Engineering Management, Risk Management, Audit Controls, Contingency Planning, Risk Analysis, System Test and Evaluation, System Design, Network Administration, UNIX, Apple System 7, Config. Management, Life Cycle Management, Virus Protection, COMSEC, Control, TEMPEST Control and Vulnerability Assessments

COURSE TITLE: Writing Security Plans
COURSE LENGTH: 2 DAYS

VENDOR:
Booz•Allen & Hamilton
8th Floor, Room 822
8283 Greensboro Drive
McLean, VA 22102-3838
Butch Chaboudy: (703) 902-5265

This course is designed to provide the System Security Officer with the knowledge to develop an ADP security plan that will meet the requirements to PL 100-235 and D/CID 1/16. Practical exercises are provided allowing students to develop key sections of a security plan as part of a work group. Each exercise is conducted following appropriate instruction in "how to" write the plan. Upon completion of the course, the student will know what information is needed in the development of a security plan, what the plan should include, where that information can be obtained and how to write policy statements and security requirements.

COURSE TITLE: Managing Org-Wide Information Security Program
COURSE LENGTH: 3 DAY

VENDOR:
Computer Security Institute
600 Harrison Street
San Francisco CA 94107
(415) 905-2626

This program examines key issues in building and maintaining a security program that serves more than one division...a program that cuts across traditional boundaries and must deal with geographically and organizationally distinct units. Practical, cost-effective ideas on how to structure a plan, tools for evaluating risks and safeguards, and ways to encourage participation and commitment from all levels of the organization. Legislative and regulatory pressures including but not limited to the Foreign Corrupt Practices Act, copyright protection, and the Computer Security Act of 1987. Take-home materials include articles, checklists, forms, and information sources. NOTE: Ask about available discount for government hosted classes.

COURSE TITLE: Building Information Security Awareness
COURSE LENGTH: 2 DAY

VENDOR:
Computer Security Institute
600 Harrison Street
San Francisco CA 94107
(415) 905-2626

This seminar shows how to "educate" managers, users, and DP personnel on the importance of protecting information resources. Top managers need to know in macro, bottom-line terms. Data security professionals need detailed technical training. Computer users, operators, and programmers must be shown what they can do on a day-to-day operational basis. This program delivers practical ideas and techniques on how to tailor a computer security training/orientation program to each of these diverse groups. You will learn how to plan a program. You will be shown what types of information should be gathered for presentation, how it should be logically organized for maximum impact, and which meeting and presentation techniques are most effective. And finally, you will be given specific ideas on how to measure the effectiveness of your security awareness program. As a "deliverable," you will develop an individualized training plan to be used in your own environment. NOTE: Ask about available discount for government hosted classes.

COURSE TITLE: Data Communications Security
COURSE LENGTH: 2.5 DAYS

VENDOR:
COMSIS
8737 Colesville Road, Suite 1100
Silver Spring, MD 20910
(301) 588-5922

This course provides an overview of network processing technologies, security threats, safeguards, and protection strategies. The data communications environments covered in this course include Local Area Networks, Wide Area Networks, Distributed Data Processing, and remote mainframe access.

COURSE TITLE: Developing Computer Security Policies & Procedures
COURSE LENGTH: 2 DAY

VENDOR:
Computer Security Institute
600 Harrison Street
San Francisco CA 94107
(415) 905-2626

This seminar is for DP managers, data security managers, and security officers responsible for developing computer security policies and procedures and integrating them into a comprehensive data processing security manual. You will learn how to determine what policies are needed, what areas a manual should cover, and how to gather the necessary information. Two different approaches - step-by-step "cookbook" procedures vs. more generalized policy statements. How to establish working liaisons with support staff in other areas, what's needed to get your policies and manual reviewed and approved, and pitfalls that must be avoided. Critique actual samples of procedures and policies currently in use. NOTE: Ask about available discount for government hosted classes.

COURSE TITLE: LAN Security
COURSE LENGTH: 2 DAY

VENDOR:
Computer Security Institute
600 Harrison Street
San Francisco CA 94107
(415) 905-2626

Local area networks (LANs) are significantly impacting the way organizations do business. As more and more critical work migrates from mainframes to LANs, the need for better controls becomes apparent. Learn about the security and control issues involved with LANs; the types of critical and sensitive data now residing on LANs; the impact of loss, change or disclosure; and realistic remedies for identified vulnerabilities. How transition technologies, topologies, and architectures create complex security, recovery, and integrity problems. Security features of popular LAN systems software and add-on packages. The need for policies, procedures, and administrative controls. NOTE: Ask about available discount for government hosted classes.

COURSE TITLE: Protecting Networks & Small Systems
COURSE LENGTH: 3 DAY

VENDOR:
Computer Security Institute
600 Harrison Street
San Francisco CA 94107
(415) 905-2626

Widespread use of microcomputers and telecommunications technology offers greater opportunities for increasing white-collar productivity...and the risk that this technology will proliferate out of control. This seminar provides a security and control perspective of the opportunities and pitfalls in this new environment. It will be valuable for data processing management, communications management and specialists, office automation management, EDP auditors, security officers, and users of small systems. Participants are encouraged to bring a list of specific, relevant security problems currently being faced within their own organizations. Selected "cases" will be analyzed and discussed. NOTE: Ask about available discount for government hosted classes.

COURSE TITLE: Application Security Reviews
COURSE LENGTH: 1 DAY

VENDOR:
COMSIS
8737 Colesville Road, Suite 1100
Silver Spring, MD 20910
(301) 588-5922

This course examines the requirements and objectives of application security and describes the techniques and tools for conducting application security reviews. The course includes the planning process, review of the baseline security goals, sensitivity and criticality determination, data collection methods, and control weaknesses and safeguards determination.

COURSE TITLE: Computer Security For Managers
COURSE LENGTH: 1 DAY

VENDOR:
USDA, Graduate School
600 Maryland Ave, SW
Washington, DC 20024
(202) 447-7124

This workshop will show you how to develop computer security awareness for end-users, and your role in program management, planning, personnel security, contingency planning, and the systems development life cycle. We will briefly review the Computer Security Act of 1987, and cover threats to, and vulnerabilities of, computer systems and appropriate safeguards, and various approaches to risk assessment. You will receive checklists and suggestions for becoming more aware of possible computer security problems in your office, and you will be able to get advice on how to deal with concerns that are specific to your agency or installation.

COURSE TITLE: Continuity of Operations/Disaster Rec. Planning: Part II Workshop
COURSE LENGTH: 3 DAYS

VENDOR:
COMSIS
8737 Colesville Road, Suite 1100
Silver Spring, MD 20910
Ronald E. Freedman: (301) 588-0800

This course will be specifically tailored toward the individual course audiences' environment. To accomplish this, research questionnaires must be completed by course participants prior to attending. These questionnaires will provide the baseline hardware, software, physical, and operational environments critical to the development of a discreet COOP/DRP.

COURSE TITLE: Physical Security for Data Processing
COURSE LENGTH: 2 DAYS

VENDOR:
COMSIS
8737 Colesville Road, Suite 1100
Silver Spring, MD 20910
(301) 588-5922

This course provides essential training to personnel in the areas of physical and environmental security in both large scale (mainframes) and small scale (PC) processing environments.

COURSE TITLE: Audit, Control, and Security of LAN and Mainframe Connectivity
COURSE LENGTH: 3 DAYS

VENDOR:
MIS Training Institute
498 Concord Street
Framingham, MA 01701-2357
Sharon G. Friedman: (508) 872-7999

In this fast-paced, three seminar you will focus on the control, security, and management aspects that should be included in any LAN evaluation. After a general overview of a LAN environment, you will review the Open Systems and OSI "standardized" models of any computing/communication system and develop a layered audit/analysis work plan based on the models. With this work plan as a guide, you will investigate: LAN topologies; protocols; LAN interconnections to wide area networks (WANs); client-server and peer-to-peer LAN architectures; LAB Network Operating Systems; connecting LANs to mainframes; and many more related topics. Keeping jargon and technology in its proper perspective, emphasis will be placed on those aspects of LAN operation with the greatest audit and security concerns. A basic understanding of the fundamentals of microcomputers and PC-based applications such as spreadsheets and database management is strongly recommended.

COURSE TITLE: Computer Viruses
COURSE LENGTH: 3 HRS

VENDOR:
USDA Graduate School
600 Maryland Ave., S.W.
Washington, D.C. 20024
(202) 447-7124

This briefing is designed to provide you with a basic understanding of the nature of computer viruses and suggested methods and procedures for identifying and dealing with them. The material will focus primarily on the microcomputer based environment but network and mini-computer virus issues will be discussed as well.

COURSE TITLE: Computer Security
COURSE LENGTH: 5 DAY

VENDOR:
GSA Training Center
P.O. Box 15608
Arlington, VA 22215-0608
Joan Bender: (703) 603-3213

Participants learn about federal computer security regulations and guidelines and their implementation in government agencies. Topics include: a threat overview, national computer security policies, an overview of the National Institute of Standards and Technology and the National Computer Security Center, physical security considerations, microcomputer security considerations, introduction to risk assessment, qualitative risk assessment, quantitative risk assessment, other risk assessment methodologies, contingency planning, design reviews and system tests, and security certification and accreditation.

COURSE TITLE: Information Security and Policy
COURSE LENGTH: 1 SEMESTER

VENDOR:
George Washington University/GSAS
2000 G Street, NW
Washington, DC 20077-2685
(202) 994-7061

Computer fraud and effective countermeasures for computer system security. The social and legal environment of information systems, including data privacy and ethics in database management. Information access policy, data security, contracts. Antitrust and other business implications of policies, transborder data flow, technology transfer, electronic funds transfer systems, criminal justice information systems, cross-cultural differences, computer infringement of copyright, and protection or property rights in software. Prerequisite: AdSc 202 and 203.

COURSE TITLE: Planning an EDP Disaster Recovery Program
COURSE LENGTH: 3 DAY

VENDOR:
Computer Security Institute
600 Harrison Street
San Francisco CA 94107
(415) 905-2626

This seminar examines the critical components of the disaster recovery planning process in detail and offers a practical framework for implementing a disaster recovery program. A "big think" approach is required, because recovery planning is tedious, time-consuming, and requires management commitment plus cooperation from all levels of user personnel. Less than 20% of the top 1,000 U.S. firms have workable EDP disaster recovery plans that have been successfully tested. Indeed, many organizations today have no formal plans at all. Some have tried to formulate a plan but failed because they underestimated the scope and complexity of the task. Although a 3-day seminar cannot provide all the details necessary for a comprehensive program, this seminar will give you a firm grounding in the knowledge and skills needed for a successful disaster recovery planning effort. NOTE: Ask about available discount for government hosted classes.

COURSE TITLE: Security in Software Applications
COURSE LENGTH: 3 HRS

VENDOR:
USDA Graduate School
600 Maryland Ave., S.W.
Washington, D.C. 20024
(202) 447-7124

This briefing is designed to provide participants with a basic understanding of features and techniques for incorporating computer security into the design and development of software applications. The material covered explores a variety of computer security design and programming techniques to enable programmers and system designers to build security into their applications.

COURSE TITLE: Introduction to Secure Systems
COURSE LENGTH: 2 DAYS

VENDOR:
Booz•Allen & Hamilton
8th Floor, Room 822
8283 Greensboro Drive
McLean, VA 22102-3838
Butch Chaboudy: (703) 902-5265

This class provides the student with an understanding of the basic principles to follow in the development and operation of secure systems--that is, systems that we can trust to protect sensitive or classified information. This course provides the fundamentals of determining security requirements for trusted systems, determination of mode of operation, calculation of the level of trusted needed for a system, and an understanding of the collective impact of security features on a system.

COURSE TITLE: UPS: Design, Selection and Specification
COURSE LENGTH: 2 DAY

VENDOR:
University of Wisconsin, Milwaukee
929 North 6th Street
Milwaukee, WI 53203
(800) 222-3623

Program objectives of this institute will have been accomplished if, upon completion, the attendee can answer satisfactorily the following questions: Where is UPS needed? When is UPS needed? Should the system be redundant? How should components be chosen? How is a system designed? What level of protection is appropriate? What are the system maintenance requirements? What grounding and noise problems need consideration? How can satisfactory performance be achieved while satisfying the NEC? **NOTE:**Previous attendees will find that material has been added to the program since they last attended.

COURSE TITLE: Computer Security In Application Software
COURSE LENGTH: 2 DAY

VENDOR:
Booz-Allen & Hamilton Inc.
8283 Greensboro Drive
McLean, VA 22102-3838
(703) 902-5201

This course presents a logical sequence of overall computer security activities during the application development life cycle. The course will assist application developers, sponsors, and owners in identifying security activities that should be considered for applications, whether they are being developed, significantly enhanced, or routinely debugged. This course is primarily intended for application software managers and support personnel. **NOTE:**Contact the vendor for information concerning specialized agency training.

COURSE TITLE: Computer Security
COURSE LENGTH: 1 SEM

VENDOR:
Montgomery College
51 Mannakee Street
Rockville, MD 20850
(301) 279-5185

This course surveys major topics in assessment and development of security procedures for a variety of computer system. Emphasis is on analysis of security needs, risk assessment and practical measures for security management. topics include LAN security, protection for personal computers, physical security, hardware and software protection and products, virus countermeasures and the human aspects of computer security.

COURSE TITLE: Micro Security for Information Systems Security Analysts
COURSE LENGTH: 32 HRS

VENDOR:
DATAPRO Educational Services
600 Delran Parkway
Delran, NJ 08076
(609) 764-0100

Security Analysts and functional Security coordinators will develop basic microcomputer security skills and understand the integral role they play in successful protection of system-wide data. Participants will learn various methods for proper disk handling and secure storage, determine proper data backup techniques and learn techniques for controlling access to data hardware and software. They will learn how to evaluate the present contingency plan and develop a risk analysis formula and also will develop a project plan for contingency implementations of hardware and software.

COURSE TITLE: Network Auditing (M2034)
COURSE LENGTH: 2.5 Days

VENDOR:
Skill Dynamics - An IBM Company
One IBM Plaza, 19th Floor
Chicago, IL 60611
(800) IBM-TEACh (800) 426-8322

This course teaches you the fundamentals of performing a security audit on a computer network. The course will begin with a review of positive and negative aspects of today's most commonly used networks. The security facts and assumptions of each network topology are explored in lecture and classroom exercises. This examination of networks includes all elements of network security (the node, the media, and the control unit). Different data exchange protocols and their benefits and vulnerabilities are examined along with the use of servers, routers, and gateways. Typical local area networks (LANs) and wide area networks (WANs) that mix several topologies are also examined for their vulnerabilities.

COURSE TITLE: PC/LAN Auditing (M2028)
COURSE LENGTH: 2.5 Days

VENDOR:
Skill Dynamics - An IBM Company
One IBM Plaza, 19th Floor
Chicago, IL 60611
(800) IBM-TEACh (800) 426-8322

This course teaches you how to review the security controls in a PC/LAN environment. You will explore the hardware and software components that impact the protection of the PC/LAN environment. You will learn the types of information needed to assess the strength of implemented controls as well as how to perform the collection of this information. Examples are presented that allow you to gain experience in interpreting security related data.

COURSE TITLE: Auditing the Data Center (M2020)
COURSE LENGTH: 2.5 Days

VENDOR:

Skill Dynamics - An IBM Company
One IBM Plaza, 19th Floor
Chicago, IL 60611
(800) IBM-TEACh (800) 426-8322

This course teaches you how to develop a data center audit for environmental, operational, and procedural issues and how to prepare for such an audit. You will learn how to locate potential problems within your data center that could result in significant losses. This course focuses not only on the technological issues but on the business issues as well. You will learn how to report the findings to management with words that will get their attention. The classroom exercises will illustrate 200+ questions that can be utilized within the audit process and that will help you in preparing a data center checklist specifically for your environment.

COURSE TITLE: Introduction to EDP Auditing (M2022)
COURSE LENGTH: 3 Days

VENDOR:
Skill Dynamics - An IBM Company
One IBM Plaza, 19th Floor
Chicago, IL 60611
(800) IBM-TEACh (800) 426-8322

This course teaches you the fundamentals of auditing electronic data processing (EDP) information systems. Reviewing the integrity and security of the business information processed by computers and their applications requires specialized skills. This course provides the initial education for those skills by presenting an audit approach to computerized information systems. You will learn about some of the tools and techniques necessary to audit a computerized environment. The focus is on the computing center, distributed processing, application development, operating systems, and the applications themselves. Classroom exercises will show you how to identify the important elements of these systems and how to write effective audit reports.

COURSE TITLE: PC Security (M2004)
COURSE LENGTH: 1 day

VENDOR:
Skill Dynamics - An IBM Company
One IBM Plaza, 19th Floor
Chicago, IL 60611
(800) IBM-TEACh (800) 426-8322

This course teaches you the fundamentals involved in providing effective and comprehensive protection of personal computers and the information they contain. You will learn how to examine the various components of PCs and to identify problems that can impact the protection of the PC assets. Typical threats to and concerns about the data residing on PCs will be discussed. Guidance on countermeasures for implementing effective controls will also be given.

COURSE TITLE: LAN Security (M2006)
COURSE LENGTH: 1.5 Days

VENDOR:
Skill Dynamics - An IBM Company
One IBM Plaza, 19th Floor
Chicago, IL 60611
(800) IBM-TEACh (800) 426-8322

This course teaches you the basics of how and where to implement effective controls in a local area network (LAN). Security pitfalls existing in both the hardware and software components that make up a LAN will be identified. The significant challenges presented by the fast growth of LANs in the workplace will be met head on with guidelines for reducing security exposures. Although this course does not address the specific implementations of any single network operating system (LAN Network Manager, NetWare, Banyan, etc.), the topics discussed apply to any and all of these.

COURSE TITLE: Business Fraud (M2008)
COURSE LENGTH: 2 Days

VENDOR:
Skill Dynamics - An IBM Company
One IBM Plaza, 19th Floor
Chicago, IL 60611
(800) IBM-TEACh (800) 426-8322

This course teaches you about some of the most common frauds and criminal activities that your organization could fall prey to. You will learn how to recognize and detect them before your business is exploited. You will learn which tools to use to review your organization for on-going fraudulent activities and what to do when they are detected. Crimes against business, such as industrial espionage, telemarketing crimes, computer crimes, and employee crimes, are a part of U.S. business today. This course will help you to understand their symptoms, their effects, and the methods to reduce their impact. Classroom exercises illustrate ways to detect some of them and to avoid becoming their next victim.

COURSE TITLE: Computer Fraud (M2010)
COURSE LENGTH: 2.5 Days

VENDOR:
Skill Dynamics - An IBM Company
One IBM Plaza, 19th Floor
Chicago, IL 60611
(800) IBM-TEACh (800) 426-8322

This course teaches how to detect and prevent the use of the computer for fraudulent activities. The ease of use that computers have provided to business has created an ease of use for the perpetrator of computer fraud. You will learn how to recognize the signs of unauthorized computer activity. You will be taught the basic ways that your organization can fall prey to these activities and the ways to prevent or minimize the threat. The crimes discussed will range from actual programming issues to manipulation of computer for fraudulent goals.

COURSE TITLE: Audit and Control of Electronic Data Interchange
COURSE LENGTH: 2.5 DAYS

VENDOR:
The Institute of
Internal Auditors
249 Maitland Avenue
Altamonte Springs, FL 32701
(407) 830-7600 ext. 1

This seminar explains clearly the risks and exposures that can result from opening the organization's computer platform to additional users - both internal and external to the organization. This course covers the basics of Electronic Data Interchange (EDI) and stresses internal controls that should be implemented to protect the organization's assets.

Attendees will learn:

- EDI concepts and terminology.
- The benefits and risks of EDI.
- Internal control requirements for internal and external users.
- The basics of telecommunications and third party value-added networks.

Participants will perform a self-assessment of their organization's internal controls regarding EDI and will develop an audit program throughout the course. An appendix will include a risk, control, and audit step matrix, a generic audit program, current readings, and a glossary.

COURSE TITLE: Audit and Control of End-user Computing (EUC)
COURSE LENGTH: 2.5 DAYS

VENDOR:
The Institute of
Internal Auditors
249 Maitland Avenue
Altamonte Springs, FL 32701
(407) 830-7600 ext. 1

Audit and Control of End-user Computing focuses on the auditor's role in reviewing controls surrounding end-user developed applications. Attendees learn:

- EUC concepts and terminology.
- The benefits, risks, and exposures of EUC applications.
- EUC controls.
- How organizations should administer EUC applications.
- What to include in the organization's EUC policy.

During this hands-on seminar, participants will use an IBM/Novell local area network (LAN) for class exercises. LANSchool is used by the instructor for display of the class discussion material. Other packages demonstrated or used include Lotus 123, Lotus FreeLance, Clear Software's ALLClear (flowcharting package), Audit Command Language's ACL for networks, Software Publishers Association's SPAudit, and WordPerfect.

Participants are provided the SAC Toolkit End-user Audit Program, Module 7 of the SAC report End-user and Departmental Computing, sample EUC policies and responsibilities, a glossary of terms, and a sample EUC survey document.

COURSE TITLE: Auditing Information Systems
COURSE LENGTH: 4.5 DAYS

VENDOR:
The Institute of
Internal Auditors
249 Maitland Avenue
Altamonte Springs, FL 32701
(407) 830-7600 ext. 1

This course explains the functions and controls required to safeguard assets in a computer processing environment. It focuses on the auditor's role in reviewing systems management and those general or environmental controls that affect applications operating within a given organization or network.

Key topics include:

- The challenging issues and functions of information system units.
- Internal audit's role in information system reviews.
- Management information systems (MIS) standards.
- Understanding data security and program change management.
- Exploring system development life cycle concepts.
- Understanding data bases, data processing standards, and processing support.
- Disaster-recovery planning procedures.
- Operating systems, distributed systems, and end-user computing.
- Understanding network security and administration.

Sample audit programs, a glossary, and a bibliography of course-related reading materials provide an excellent starting point for attendees preparing to audit information systems.

COURSE TITLE: Integrated Auditing: The Basics
COURSE LENGTH: 4.5 DAYS

VENDOR:
The Institute of
Internal Auditors
249 Maitland Avenue
Altamonte Springs, FL 32701
(407) 830-7600 ext. 1

This seminar offers the know-how to perform applications reviews in the computerized arena. The course teaches basic EDP auditing skills and knowledge, and defines the "integrated auditor". The seminar includes a comprehensive case study of a total audit. Participants are provided a sample audit program, a glossary of terms, sample computer policies, and a sample user security manual.

Attendees learn:

- The basics of computer controls, both within and around applications.
- An approach to audit planning including
  - risk analysis.
  - identifying risks and exposures.
  - development of test objectives.
  - evaluation of results of auditing.
  - reporting to management.
- Minimal computer programming standards.
- Tools and techniques needed to perform a review of modern automated applications, including stand-alone applications and fully integrated mainframe applications.

Integrated Auditing: The Basics is tailored to auditors just entering the EDP audit arena, including auditors in departments moving toward integration and financial/operational auditors performing functional audits involving automated applications.

COURSE TITLE: Computer Security for Security and MIS Professionals
COURSE LENGTH: 3 DAYS

VENDOR:
MIS Training Institute
498 Concord Street
Framingham, MA 01701-2357
Sharon G. Friedman: (508) 872-7999

The very technologies that have streamlined today's organizations have created vast opportunities for computer crime and misuse. With PCs on virtually every desktop and networks to link one workstation to another, computer-savvy criminals and disgruntled employees have more ingenious ways to gain access to critical data and confidential information. This plan-English seminar is an eye-opener that will be your road map through a maze of high-tech, high risk exposures. You will discover how to plug the security loopholes in computer systems, networks, E-mail, voice-mail, and fax transmissions that leave your organization vulnerable to attack. The seminar covers: strategies for establishing polices and procedures that will keep costly abuse to a minimum; employee security awareness techniques; sensitive legal issues surrounding employee privacy rights and software copyright infringement; and more. You will leave this seminar with valuable guidelines and real-world models for preventing, detecting, and responding to criminal attacks, virus infections, and accidental errors in your own organization.

COURSE TITLE: Intro. to Auditing Micros and LANs: Controlling End-User Computing
COURSE LENGTH: 3 DAYS

VENDOR:
MIS Training Institute
498 Concord Street
Framingham, MA 01701-2357
(508) 872-7999

LANs and microcomputers have placed the tools for processing and storing data directly on the decks of end users. In this three-day seminar you will learn the fundamentals of microcomputer and LAN technology, and how to classify the risks microcomputer and end-user computing have introduced into the organization. You will examine the control techniques currently available to address these risks and how to conduct an audit using a detailed audit program you can bring back for use in your own organization.

COURSE TITLE: Basic Security For PC Users
COURSE LENGTH: 8 HRS

VENDOR:
Naval Computer and Telecommunications Station
ATTN Code N823
PO Box 357056
San Diego, CA 92135-7056
(619) 545-8628 - DSN 735-8628

This one-day course provides the attendees with a basic understanding of the AIS Security Program fundamentals. This course satisfies the awareness training requirements prescribed in the Public Law 100-235 which mandates that all users of computers must have awareness training. Course training focuses on ways to eliminate or control potential problems in a microcomputer and Local Area Network (LAN) environment. This course discusses the DON policy and Minimum Program Requirements that must be met to comply with policy mandates. The attendees will be given techniques to enhance their awareness of vulnerabilities in a microcomputer and LAN operating environment and the appropriate protective measures available to reduce operating risks. This course is conducted at the NAVCOMTELSTA San Diego facility or at your command.

COURSE TITLE: INFOSEC
COURSE LENGTH:

VENDOR:
Security Engineering Services, Inc.
5005 Bayside Road
Chesapeake Beach, MD 20732
Bruce Gabrielson: (301) 855-4565

This course presents a comprehensive overview of information security (INFOSEC) focusing on network ADP security and other technical issues seldom covered in general introductory level courses. DoD requirements for government (NSA-NCCS, Air Force, MC, Navy, Joint Staff) and defense industry (DIS) are discussed. Related OPSEC issues are presented.

Attendees should leave this course with a full understanding of the technically based INFOSEC security issues.

COURSE TITLE: Security Technology in the Real World
COURSE LENGTH:

VENDOR:
Canaudit Inc.
P.O. Box 4150
Simi Valley, CA 93093
(805) 583-3723

SEMINAR OUTLINE

A. THE NEW SECURITY IMPERATIVE :* Why technology security is on everyone's mind * Our growing dependence on computers and communications * The range of threats: Some "horror stories"- Internal: - Error and omissions - Disgruntled employees - Natural disasters External: - Hackers - Competitors - Viruses and Worms.

B. COMPUTER SECURITY RESEARCH:* Hot Topics: computer science point of view -Cryptography - Identification - Distributed Database Security * Hot topics: business point of view - Security awareness in industry - Level of security planning - Future plans protection.

C. WORKSHOP - IDENTIFYING KEY ISSUES FOR SEMINAR PARTICIPATION: *Introduction * Worktime * Presentations.

D. GROUP DEBRIEFING ON WORKSHOP PROBLEMS OF IMPORTANCE

E. A METHODOLOGY FOR STRATEGIC RISK MANAGEMENT - ORGANIZATION MODELLING * Functional model * Situation assessment * Situation simulation * Strategic systems planning and integration * Data classification Exercise: Data classification questionnaire * Implementation of Data classification - Mainframe - Unix environment.

F. UNIX SYSTEM SECURITY CONSIDERATIONS * Unix history with respect to security * Access protection - owner, group, public - files and directories - listing file access (1s-1) - changing file access (chmod) * Common Unix security problems - Password cracking - Getting root access - Superuser abuse - Spoofing - Intelligent terminal problems * Unix network problems - Anonymous ftp - Competitors - Remote logins - Worm programs.

G. WORKSHOP - SECURING FILES IN UNIX:* Background * Command writing exercise.

H. PHYSICAL SECURITY: * Access control * Fire protection * Flood/water damage * Theft protection * Off site backup.

I. INSURANCE ASPECTS OF TECHNOLOGY: * Loss of assets * Loss of data * Loss of confidentiality * Valuable papers * Business interruption * Software escrow.

J. LOGICAL ACCESS SECURITY :* Defining user IDs * Privilege fields * ID registration.

K. LEGAL ASPECTS OF T SECURITY: * What makes a "computer crime"? * Criminal Codes - Unauthorized use of computer - Mischief against data * Civil remedies * Copyright infringement * Theft * Fraud * Trade secrecy provisions * Working with law enforcement personnel.

L. WORKSHOP: DEALING WITH A VIRUS THREAT:* Problem description * Worktime * Presentation of solutions.

M. COMMUNICATIONS SECURITY: * Wiretapping, low and high tech * Local area networks * Cellular telephones * Fax modems * Voice mail systems.

N. RCMP EDP SECURITY: Bulletin #33 (reproduced with permission).

O. CONTINGENCY PLANNING :* Focus on corporate business issues * Proactive aspects * Reactive aspects * Risk management issues * Key issues.

P. FOCUS ON ISSUES RAISED BY PARTICIPANTS: * Defining the problem * Seeking a solution - at what cost?

Q. CREATING A SECURITY PLAN FOR YOUR ORGANIZATION:* Elements of a good security plan * Who should do it * How to implement it * The need for regular review and testing.

R. CONTROLS IN A MICROCOMPUTER ENVIRONMENT: * Introduction * The acquisition process * Installation and maintenance * Inventory control * Troubleshooting * Application development * Training * Documentation * File back-up and data security
* Computer Viruses * Hardware Security * Input/Output and Processing Controls
* Application Dependency Model.

S. FUTURE TRENDS IN COMPUTER SECURITY

T. CONCLUDING REMARKS

COURSE TITLE: Using Investigative Software to Detect Fraud
COURSE LENGTH:

VENDOR:
Canaudit Inc.
P.O. Box 4150
Simi Valley, CA 93093
(805) 583-3723

This seminar is designed to teach the concepts of investigative software and provide participants with the skills required to design, develop and install investigative software routines upon completion of the course material. Each participant will receive a compendium of suggested investigative software routines for specific industries and applications.

COURSE TITLE: Auditing System Development: New Techniques for New Technologies
COURSE LENGTH:

VENDOR:
Canaudit Inc.
P.O. Box 4150
Simi Valley, CA 93093
(805) 583-3723

This seminar focuses on the effect new technologies have on the audit approach and explores methods to ensure that the audit requirement is met without slowing the project or becoming a drain on project resources. Special emphasis is placed on early identification of control requirements and the rapid reporting techniques that are required in today's dynamic system development environment.

COURSE TITLE: Auditing EDI Applications
COURSE LENGTH:

VENDOR:
Canaudit Inc.
P.O. Box 4150
Simi Valley, CA 93093
(805) 583-3723

This seminar will provide you with an understanding of EDI and provide you with the skills and techniques required to audit in this complex environment. Each participant will receive suggested audit programs and checklists, to assist in performing application audits in and EDI environment.

COURSE TITLE: The Integrated Audit Workshop
COURSE LENGTH:

VENDOR:
Canaudit Inc.
P.O. Box 4150
Simi Valley, CA 93093
(805) 583-3723

This workshop is designed for auditors who will be using the integrated audit approach. It explains both manual and computerized controls and provides a complete audit approach for auditing modern applications. At the end of the workshop, participants will be able to identify and evaluate the controls in a computerized application through the use of control matrices. This workshop can be modified for in-house presentation to the entire audit department.

COURSE TITLE: Audit Software for the 21st Century
COURSE LENGTH:

VENDOR:
Canaudit Inc.
P.O. Box 4150
Simi Valley, CA 93093
(805) 583-3723

In the past audit software has been the domain of the I.S. auditor. Recent technology breakthroughs now provide each internal and external auditor with software capability that is easy to use and increases audit coverage. In preparing for the 21st century all audit departments require strategies to automate audits, perform silent and remote audits and improve audit productivity. This seminar explores existing technologies and provides participants with the knowledge to acquire, create and implement the software tools that will form the basis of the audit philosophy of the 21st century.

The open system concept has traditionally created a software dilemma for auditors in that computer assisted audit techniques had to be rewritten for each mainframe and minicomputer. Now PC based products enable auditors to circumvent this situation to create software once for multiple platform execution. This capability not only provides significant economies of scale by reducing software development costs, but it also enables greater consistency in audit software tests while maximizing auditor productivity. The availability of pc compatible tape drives and high capacity hard disks provide large file processing capability so that mainframe applications can now be readily audited using the PC.

In addition to learning new techniques, participants will be provided with a free authorized demonstration copy of ACL, the industry standard PC product for audit software. Participants will then be able to reinforce what they learned in the seminar with examples they can code and test when they return to the office so that they can demonstrate the 21st century audit concept to their management.

COURSE TITLE: Information Systems Audit Workshop
COURSE LENGTH: 4 DAYS

VENDOR:
Canaudit Inc.
P.O. Box 4150
Simi Valley, CA 93093
(805) 583-3723

This 4 day workshop is designed for auditors who will be conducting audits in a computerized environment. It assumes no prior knowledge of EDP audit concepts or procedures and provides participants with a sound understanding of the audit risks relating to information systems. Once the groundwork is laid, participants will learn the controls required in computerized applications and a step by step approach to effectively evaluate the EDP control structures. As their understanding increases, participants progress to more complicated IS audit topics including local area networks, data security, telecommunications networks and operating systems. Participants will receive the skills, audit programs and checklists required for them to perform information systems audits on their return to the office.

COURSE TITLE: Auditing Client/Server Technology
COURSE LENGTH:

VENDOR:
Canaudit Inc.
P.O. Box 4150
Simi Valley, CA 93093
(805) 583-3723

Client/Server technology is rapidly becoming the preferred processing methodology for both large and small organizations. Larger organizations are looking to client/server technology to replace traditional large scale mainframes. Management is looking to client/server technology to provide productivity improvement, empower employees and to provide better service levels at a reduced cost. As with any new technology, the shift to a client/server environment poses many risks to the business and the business control structure. This seminar will provide participants with a sound knowledge of client/server technology and the control mechanisms required to ensure a safe and secure processing environment.

COURSE TITLE: Control and Security of LANS
COURSE LENGTH: 3 DAY

VENDOR:
Canaudit Inc.
P.O. Box 4150
Simi Valley, CA 93093
(805) 583-3723

As local area networks (LAN's) permeate the organization, security and control issues are often ignored. This seminar takes a hard look at the audit concerns of LAN's and how to install effective controls in this dynamic computer environment. Participants will learn what can go wrong in the LAN environment and what preventive and detective controls are available to mitigate control weaknesses within the LAN or from external connections. LAN Management and the role of the LAN officer is discussed in detail. Special emphasis is placed on management of the hardware and connectivity along with the selection of software. These key items often limit the overall usefulness of the LAN and inhibit the achievement of connectivity and productivity objectives. Each participant will receive detailed audit programs, common control weaknesses and sample recommendations. These are the key tools they need to conduct LAN audits.

COURSE TITLE: Auditing Datacomm Networks
COURSE LENGTH: 3 DAY

VENDOR:
Canaudit Inc.
P.O. Box 4150
Simi Valley, CA 93093
(805) 583-3723

Wide area networks are the lifeblood of corporate information processing and connectivity, yet many organizations have yet to do a complete audit of network operations and management. This seminar provides the IS auditor with a structured audit approach directed to identifying critical control weaknesses in the network, the carriers, the media and network management. Proven solutions to common control weaknesses will be provided to each participant. Focus in this seminar is on a complete audit approach for data and voice communications from a security and cost perspective. Network management tools and problem resolution techniques are the cornerstone of network operations. Special emphasis is placed on using NETVIEW, a popular network management tool to identify network problems. Participants in this session will receive detailed audit programs and checklists which will provide a strong starting point for their first Network Audit.

COURSE TITLE: Computer Security & Contingency Planning
COURSE LENGTH: 3 DAY

VENDOR:
Canaudit Inc.
P.O. Box 4150
Simi Valley, CA 93093
(805) 583-3723

Security Administration is now a reality in many organizations. Other companies that do not currently have a security administration function are considering, or are in the process of creating the security function. This seminar is designed to remove the mystery surrounding data security, and to provide participants with a proven approach to securing their computer systems. At the end of the session, participants will understand security administration and the critical items that must be included to enable the function to perform effectively. They will be able to classify data by criticality and confidentiality. They will have an understanding of logical access security, disaster contingency planning, and how to develop and implement security procedures in their organization.

COURSE TITLE: Auditing Advanced Information Technology
COURSE LENGTH: 3 DAY

VENDOR:
Canaudit Inc.
P.O. Box 4150
Simi Valley, CA 93093
(805) 583-3723

When Canaudit set out to rewrite the popular ADVANCED EDP AUDITING seminar, the objective was to make it the most comprehensive Information Systems audit course currently available in the public marketplace. Only a completely new seminar, AUDITING ADVANCED INFORMATION TECHNOLOGY, could incorporate all of the enhancements. AUDITING ADVANCED INFORMATION TECHNOLOGY provides the Information Systems Auditor with the skills required to perform audits of Operating Systems, Local Area Networks, Wide Area Networks, Access Security and DB2. In addition to generic audit programs, participants will receive detailed product specific checklists for MVS, Tandem VAX, AS/400 and Novell. These checklists will enable the IS auditor to conduct audits of those critical components of information technology necessary to ensure their organization's information processing is secure, controlled and effective. Emphasis is placed on improving the quality of management techniques and controls to enable organizations to operate effectively in today's complex information technology environment.

COURSE TITLE: EDP Auditing: The First Step
COURSE LENGTH: 3 DAY

VENDOR:
Canaudit Inc.
P.O. Box 4150
Simi Valley, CA 93093
(805) 583-3723

This seminar provides financial auditors or new information systems auditors with the skills required to audit complex automated applications. Detailed coverage of computerized controls is provided to ensure participants understand the key controls and how to audit them. They will also learn how to audit the data center, data security, systems under development and how to design audit software tests. In addition, we have included a special section on EDI which explains the concepts, the economics and key controls available to ensure electronic transactions are processed accurately and efficiently. A special section on Auditing Trading Partner Agreements is devoted to minimizing the negative impact of EDI and protecting your organization. Each participant will receive detailed checklists and comprehensive audit programs so they can perform Information Systems audits. The audit experiences related by the instructors provides valuable insight on how to locate, identify and rectify control weaknesses in a computerized environment.

COURSE TITLE: Control and Security of Local Area Networks
COURSE LENGTH:

VENDOR:
Canaudit Inc.
P.O. Box 4150
Simi Valley, CA 93093
(805) 583-3723

As local area networks (LAN's) permeate the organization, security and control issues are often ignored. This seminar takes a hard look at the audit concerns of LAN's and how to install effective controls in this dynamic computer environment. Participants will learn what can go wrong in the LAN environment and what preventive and detective controls are available to mitigate control weaknesses within the LAN or from external connections.

LAN Management and the role of the LAN officer is discussed in detail. Special emphasis is placed on management of the hardware and connectivity along with the selection of software. These key items often limit the overall usefulness of the LAN and inhibit the achievement of connectivity and productivity objectives. Each participant will receive detailed audit programs and checklists, common control weaknesses and sample recommendations. These are the key tools they need to conduct LAN audits. A special module has been created that provides a specific control approach for the Novell Netware and another module for Unix.

COURSE TITLE: Computer Security for Managers Seminar
COURSE LENGTH: 1 Day

VENDOR:
ARCA
Commerce Center
10320 Little Patuxent Parkway
Suite 1005
Columbia, MD 21044
(410) 715-0500

This session will introduce computer security concepts and management activities and policies for a successful security program. Individuals will learn the life-cycle approach for protecting systems and how to create effective policy. Other topics include threat and risk analysis, developing and implementing incident handling procedures, legal issues, and how to establish and maintain cost effective programs.

COURSE TITLE: Becoming An Effective Data Security Officer
COURSE LENGTH: 3 DAY

VENDOR:
Computer Security Institute
600 Harrison Street
San Francisco CA 94107
(415) 905-2626

As a Data Security Officer, you may be responsible for creating a data security program or administering and improving one already in place. To a great extent, you will be defining your own role as you proceed. But where do you begin? What skills do you need to do the job? Where do you get the information to enhance your own skills? Who are the "k[illegible]s" within your organization, and how do you get them committed to making security hap[illegible]hat are the advantages of the job? The disadvantages? How have others succeeded, and what pitfalls should you avoid? This practical 3-day program will deliver the know-how to help you become a more effective, proficient, and successful Data Security Officer. NOTE: Ask about available discount for government hosted classes.

COURSE TITLE: Auditing Fraud: Prevent, Detect, & Control
COURSE LENGTH: 3 DAY

VENDOR:
MIS Training Institute
498 Concord Street
Framingham, MA 01701
(508) 879-7999

Internal auditors are relied upon more and more to recognize the characteristics of potentially fraudulent activities, and to be knowledgeable about where fraud is most likely to occur in the organization. This intensive seminar examines where and why all types of fraud occur, including white collar crime, computer fraud, insider fraud, and external fraud. In this session you will learn to recognize red flag areas of fraud and strategies for reducing it. This seminar is your short cut to learning how to incorporate prevention, detection, and prosecution of fraud into your annual audit plans.

COURSE TITLE: INFOSEC Foundations Seminar
COURSE LENGTH: 2 DAYS

VENDOR:
ARCA
Commerce Center
10320 Little Patuxent Parkway
Suite 1005
Columbia, MD 21044
(410) 715-0500

This foundations seminar focuses on system security fundamentals. Individual sessions review TCSEC requirements, the NCSC's evaluation process, RAMP, environment guidelines, policy fundamentals, assurance, trusted application development concerns, and secure system integration issues. Other sessions describe efforts to develop international standards for trust, introduce the products on the Evaluated Products List, highlight the concept of risk management, overview database and network security concerns, and discuss the perils and pitfalls of secure system integration.

COURSE TITLE: On-Line, Dist Comm Sys:Control, Audit & Security
COURSE LENGTH: 3 DAY

VENDOR:
MIS Training Institute
498 Concord Street
Framingham, MA 01701
(508) 879-7999

In this seminar you will learn the basic concepts of computer communications systems and a simple audit/analysis technique which can help you expose risks with very little in-depth knowledge of the technology. Through examination of the major functions and audit/security concerns in each layer of the ISO "Reference Model," you will learn the components of a more in-depth communications audit and the design and evaluation criteria of internal security controls. The sample work plans you receive, and the guidelines, audit tools, and techniques you learn will be immediately useful in auditing any communications system.

COURSE TITLE: Advanced Data Comm Networks: Security/Auditability
COURSE LENGTH: 3 DAY

VENDOR:
MIS Training Institute
498 Concord Street
Framingham, MA 01701
(508) 879-7999

This seminar builds on the tools and techniques learned in On-Line and Distributed Communications Systems: Control, Audit, and Security, providing a comprehensive study of the data network portions of a computer communications system-OSI layers 1-4. You will explore, in-depth, the audit and security concerns in each layer, and examine the design and evaluation criteria of internal security controls. At the end of this intensive session, you will understand how protocols, public and private communication systems, and local area networks function. You will know how to perform a data communications audit. Participants should first attend "On-Line and Distributed Communications Systems." Participants are invited to bring network maps, protocol lists, and data traffic load statistics from their own installation.

COURSE TITLE: The Data Center: Auditing For Profit
COURSE LENGTH: 2 DAY

VENDOR:
Canaudit Inc.
P.O. Box 4150
Simi Valley, CA 93093
(805) 583-3723

The audit programs provided in this course are specifically designed to enable the participants to conduct the data center audit with little or no need for additional support. Throughout this session emphasis is placed on ensuring that appropriate preventive controls are in place to prevent unscheduled interruption of processing or inappropriate data access. Disaster contingency planning is discussed in depth, with each participant receiving a copy of our general disaster recovery program. Canaudit has also added a module on out-sourcing which provides auditors with a good understanding of the concepts and the related risks. As with all Canaudit courses, this seminar makes extensive use of examples and classroom discussion to supplement the lecture.

COURSE TITLE: EDI: New Frontiers For Auditors
COURSE LENGTH: 1 DAY

VENDOR:
Canaudit Inc.
P.O. Box 4150
Simi Valley, CA 93093
(805) 583-3723

Electronic Data Interchange is emerging as a major component of many financial, retail and manufacturing applications. Several major companies have made a public commitment to full EDI implementation in the near future. this technology presents the auditor with many new control and security issues in auditing EDI applications. The elimination of physical transactions and paper audit trails will force each financial auditor to perform functions formerly done by the EDP Auditor. This session is designed specifically for those auditors who require a comprehensive audit approach. Modules presented in this seminar include an overview of EDI technology and standards, critical functions of EDI, the controls available in the X12 standard and how to implement them. Each participant will receive a comprehensive audit program as part of the seminar handout.

COURSE TITLE: LAN Tuning and Performance for Audit and Security Personnel
COURSE LENGTH: 2 DAYS

VENDOR:
MIS Training Institute
498 Concord Street
Framingham, MA 01701-2357
Sharon G. Friedman: (508) 872-7990

This comprehensive, two-day seminar attacks LAN vulnerabilities head-on and provides you with the know-how to analyze LAN activity to determine if sensitive network traffics is secured and if the network is performing at an effective service level. Working with diagnostic tools for both Ethernet and token-ring networks, you will learn how to read and manage network traffic. You will discover how to use 100 dynamic network tests to verify that your LANs are meeting your organization's objectives ins secured manner. This session will provide immediately useable network monitoring techniques that are applicable for any diagnostic or network management tool you are currently running. You will leave this high-payback session with the know-how to spot network problems before they become end-user problems. Attendees should have some familiarity with LANS.

COURSE TITLE: Audit and Security of Relational Databases and Applications
COURSE LENGTH: 3 DAYS

VENDOR:
MIS Training Institute
498 Concord Street
Framinghan, MA 01701-2357
Sharon G. Friedman: (508) 872-7990

Relational technology has become the industry standard. Today an organization may run several database systems. Auditors may need to know the specifics of three different relational databases. This three-day course was designed so you could come to one place and learn what you will examine and compare the features, audit and security strengths, and accounting log capabilities of 14 leading relational database systems: DB2, Oracle, Paradox, Sybase, SQL Server, Informix, Interbase, dBase, Rdb, NetWare, SQL, IDMS, Foxbase, and AS/400. You will learn the new risks of relational technology, and the associated controls built into each of these specific systems. In addition, you'll review third-party security software products. You will leave this power-packed session with useable programs for audition your systems environment, and the design, development, and operation of a typical application within each specific environment.

COURSE TITLE: CS 229 - Computer Security Systems I
COURSE LENGTH:

VENDOR:
The George Washington University
Department of Electrical Engineering & Computer Science
Professor Lance Hoffman
Washington, DC 20052
(202) 994-4955

Techniques for security in computer systems. Authentication, logging, authorization, encryption. Effects of operating systems and machine architecture, countermeasures, risk-analysis systems. Companion course to EE 250. Prerequisite: CSci 144 (Concepts of Programming Languages) or equivalent.

COURSE TITLE: CS 329 - Computer Security Systems II
COURSE LENGTH:

VENDOR:
The George Washington University
Department of Electrical Engineering & Computer Science
Washington, DC 20052
Professor Lance Hoffman: (202) 994-4955

Advanced topics in information systems security. Intrusion detection in expert systems related to computer security. Viruses. Efficacy of anti-viral techniques under various architectures. Advanced risk analysis methodologies, the developing standard computer security methodology, and its relationship to other computer security models such as those of Bell and LaPadula, Biba, and Clark and Wilson. Issues in computer network security. Advanced protection methods against statistical inference. Prerequisite: CS 229 or permission of instructor.

COURSE TITLE: EE 250 - Telecommunications Security Systems
COURSE LENGTH:

VENDOR:
The George Washington University
Department of Electrical Engineering & Computer Science
Washington, DC 20052
Professor Lance Hoffman: (202) 994-4955

Cryptography. Speech and data scrambling. Nonlinear transformations. Block and stream ciphers. DES algorithm and public key cryptography. Key management, digital signatures, and authentication. Data communication security protocols. Secure voice communications. The CLIPPER initiative and escrowed-key schemes. Companion course to CS 229. Prerequisite EE 204 (Stochastic signals and noise) or equivalent.

COURSE TITLE: AIS Security Strategies
COURSE LENGTH: 8 DAYS

VENDOR:
Information Resources Management College
National Defense University
Ft. Lesley J. McNair
Washington, DC 20319-6000
(202) 287-9321

This course is designed to provide the knowledge necessary for designers, developers reviewers and approvers of new and updated Automated Information Systems to make sound decisions about the security aspects of the system. In particular, the primary audience is managers who are responsible for system design and specification, program management, oversight, certification and/or accreditation of Automated Information Systems. The secondary audience for the course includes staff from other disciplines, including technical staff personnel working in such areas as system security, contracting, inspections or auditing, as well as members of the functional community. The course does lean towards Department of Defense (DoD)-level guidance for security in the data processing environment, but the concepts presented are also applicable to non-DoD systems, and to DoD embedded and C^3I systems, as well.

Security professionals have emphatically asserted that security issues must be considered from the very beginning of the planning of the system, in order to avoid significant problems in terms of cost, schedule, and operational capability that occur when the need for security is not recognized until late in the system development process. Therefore, the emphasis in this course is on the early stages of system specification and acquisition, especially Functional Requirements Definition, Security Requirements Definition, Concepts Development, and System Design. The principal notion conveyed is the importance of performing these and all other steps throughout the development and acquisition process in such a manner as to facilitate the eventual accreditation of the system. Although the course is not oriented towards a security manager having operational responsibilities (e.g., the Information System Security Officer for a local area network or for a data processing installation), nevertheless many of the concepts taught are also applicable in an operational environment.

COURSE TITLE: The CMW: Administrator Tutorial
COURSE LENGTH:

VENDOR:
Trusted Systems Training, Inc.
1107 South Orchard Street
Urbana, IL 61801-4851
Steve Sutton: (217) 344-0996

The course addresses the security administration of Compartmented Mode Workstations based on the SecureWare technology, including SecureWare's CMW+, Hewlett-Packard's BLS, and Digital's MLS+. It teaches the management of all new security features, like Protected Subsystems, user accounts, security auditing, secure import/export, the CMW "Encodings file," and trusted (MaxSix) networking. The course book and accompanying textbook include written and on-line, self-paced exercises that form the basis for classroom learning.

COURSE TITLE: Computer Viruses, Trojan Horses, and Logic Bombs
COURSE LENGTH: 2 DAY

VENDOR:
Computer Security Institute
600 Harrison Street
San Francisco CA 94107
(415) 905-2626

This seminar examines the insidious threats to computer systems posed by [illegible] programming, including viruses, Trojan horses, worms, logic bombs, and trap doors. We will examine the broad spectrum of harmful code, the people who create it, how viruses get into systems, demonstrations of illicit programs, and countermeasures. The impact of malignant programming extends well beyond any immediate file damage. Hidden losses, such as reconstruction of programs and data, and exhaustive detective work may be necessary. What types of people would infect our systems....are they employees, competitors, outsiders? We will review the latest legal cases relating to viruses and logic bombs, Examples of anti-virus software - what these "digital pharmaceuticals" can and cannot do. Realistic approaches for controlling the problem, and solutions which have worked. Note: Attendees are encouraged to provide examples, from their own experience, of destructive programming threats and effective technical and administrative countermeasures they have used. NOTE: Ask about available discount for government hosted classes.

COURSE TITLE: Microcomputer Security
COURSE LENGTH: 3 DAY

VENDOR:
Computer Security Institute
600 Harrison Street
San Francisco CA 94107
(415) 905-2626

This participative program examines the security issues around microcomputer use, with emphasis on identifying issues and developing plausible solutions for your real-world environment. The development of PC security issues and what the future holds. Security weaknesses of microcomputers and where PC security differs from mainframe security. Physical protection for the machines and associated media, plus data access control and virus prevention, with demonstrations of related products. Contingency planning for personal computers. Policies and procedures for controlling the spread and use of PCs. Software piracy and how to prevent it in the workplace. The value of a comprehensive and continually updated security awareness program in achieving your PC security objectives. Designed for DP and information center managers, security officers, and EDP auditors. NOTE: Ask about available discount for government hosted classes.

COURSE TITLE: Computer Security For Security Officers
COURSE LENGTH: 2 DAY

VENDOR:
USDA, Graduate School
600 Maryland Ave, SW
Washington, DC 20024
(202) 447-7124

This workshop will show you how to improve the computer security program in your agency. Through lectures, discussion, case studies and checklists you will be able to determine the strength of your current security program, and to pinpoint potential problem areas that need attention. You also will learn about your responsibilities with your agency management in terms of policy development and contingency planning.

COURSE TITLE: CS 230 - Information Policy
COURSE LENGTH:

VENDOR:
The George Washington University
Department of Electrical Engineering & Computer Science
Washington, DC 20052
Professor Lance Hoffman: (202) 994-4955

Issues related to computers and privacy, equity, freedom of speech, search and seizure, access to personal and governmental information, professional responsibilities, ethics, criminality, and law enforcement. This course examines these policy issues using the current literature and written, electronic, and videotape proceedings of recent major conferences and government hearings. Prerequisite CS 131 (Programming of Data Structures) or equivalent.

COURSE TITLE: Security and Control in Automated Systems-Audit IS
COURSE LENGTH: 3 DAYS

VENDOR:
USDA Graduate School
600 Maryland Ave., S.W.
Washington, D.C. 20024
(202) 382-8620

Internal auditors have a major role in reviewing the security and controls in sensitive automated systems. This course provides practical guidelines ant techniques for auditing and evaluating the adequacy of security and internal controls in sensitive automated systems. Major problem areas are discussed and examples illustrating the results of inadequate security and controls are presented. In addition, the responsibilities of management, internal audit, and data processing personnel are discussed. This course also provides the attendee with a comprehensive methodology for conducting security and internal control audits of sensitive data processing systems. Using a case study approach, the course illustrates how to identify and quantify the vulnerabilities of automated systems to fraud, disclosure, delay and other threats. The internal control techniques which can be applied to address these vulnerabilities are discussed, as well as the requirements of OMB circulars A-127 and A-130.

COURSE TITLE: Fundamentals of Computer Security for Federal Information Systems
COURSE LENGTH: 5 DAY

VENDOR:
USDA Graduate School
600 Maryland Ave., S.W.
Washington, D.C. 20024
(202) 447-7124

This five-day course provides those responsible for computer security with an overview of security issues specifically related t the federal government. Designed to introduce and cover the fundamentals areas of concern facing computer security officers, from mainframe to PC's. The objectives are covered by lecture, group discussion, slide and video presentations. The instructor will provide extensive insights into computer security based on operational experiences. In addition, hands-on risk analysis exercises will be performed. The student will be provided with extensive materials, including demonstration diskettes and public domain anti-virus software.

COURSE TITLE: Computer Security Seminar
COURSE LENGTH: 3 DAYS

VENDOR:
ARCA
Commerce Center
10320 Little Patuxent Parkway
Suite 1005
Columbia, MD 21044
(410) 715-0500

This computer security seminar focuses on the hardware and software mechanism which can be used to implement specific TCSEC security functionality. Computer security concepts, requirements, and implementation examples are presented for policy enforcing mechanisms, accountability mechanisms, and underlying architectures supporting the reference monitor concept. Issues on integrity, covert channels and trusted applications are also discussed. In-class exercises and practical examples reinforce the important concepts presented in the lecture materials. The seminar concludes with discussions of several evaluated products.

COURSE TITLE: Network Security Seminar
COURSE LENGTH: 3 DAYS

VENDOR:
ARCA
Commerce Center
10320 Little Patuxent Parkway
Suite 1005
Columbia, MD 21044
(410) 715-0500

In this seminar you will learn how to integrate and implement secure networks. You will be introduced to network security concepts, fundamentals, network threats, and the Trusted Network Interpretation [TNI] of the TCSEC. Security properties required of a trusted network, secrecy, integrity and availability are described per the OSI security services model. Interconnection of separately accredited AIS systems is discussed focusing on possible cascading problems. The group project has students design a hypothetical network security architecture, identify the necessary evaluation class(es), analyze the network data flows, and specify the assurance requirements. The seminar concludes with an overview of secure networking products and efforts.

COURSE TITLE: Database Security Seminar
COURSE LENGTH: 3 DAYS

VENDOR:
ARCA
Commerce Center
10320 Little Patuxent Parkway
Suite 1005
Columbia, MD 21044
(410) 715-0500

This seminar addresses how to use multilevel databases management systems effectively and as an integrated part of a system solution. The seminar introduces database security issues and problems and familiarizes participants with the NCSC's Trusted Database Management System Interpretation [TDI] of the TCSEC. Several approaches to building multilevel database systems are presented: integrity lock, kernelized, layered, partitioned and distributed. Topics include; database design considerations view versus relation discretionary controls, mandatory controls, inference, and aggregation. Class exercises and practical examples are used to reinforce concepts.

COURSE TITLE: Comprehensive INFOSEC Seminar
COURSE LENGTH: 5 DAYS

VENDOR:
ARCA
Commerce Center
10320 Little Patuxent Parkway
Suite 1005
Columbia, MD 21044
(410) 715-0500

This seminar provides an intensive presentation of INFOSEC topics by combining ARCA's INFOSEC Foundations, Computer, Network, and Database Security seminars. Critical INFOSEC topics from these public seminars are presented in detail and other topics are summarized in a single week. This seminar provides an excellent start-up for an engineering organization starting an MLS or security program or expanding its security staff.

COURSE TITLE: Communication Security Principles & Practices
COURSE LENGTH: 2 DAY

VENDOR:
Computer Security Institute
600 Harrison Street
San Francisco CA 94107
(415) 905-2626

This workshop is for data processing managers, security officers, and auditors who have little or no knowledge in the communications area. Because communications systems are so complex and vulnerable, the data processing operation is a substantial risk. You will learn about the basic concepts and the terminology needed to communicate effectively with technicians. The emphasis, however , is on vulnerabilities and the practical security safeguards you can implement. Because the largest communications risk faced by most organizations is unauthorized access to their computers, considerable emphasis will be placed on how mainframe access control mechanisms interface with other communication security techniques. In particular, you will learn to address the three major risks - loss of network service, unauthorized access to your network and data center resources, and surveillance of your network traffic. "Special Note" You are encouraged to prepare, in advance of the Workshop, a description of specific communications security problems being faced within your own organization. Cases will be discussed as time permits and as issues arise during the Workshop. NOTE: Ask about available discount for government hosted classes.

COURSE TITLE: Managing Computer Security-Mergs, Acq, and Divestitures
COURSE LENGTH: 2 DAY

VENDOR:
Computer Security Institute
600 Harrison Street
San Francisco CA 94107
(415) 905-2626

Mergers, acquisitions, and divestitures are common in today's corporate environment. Unfortunately, while these situations can create serious information protection problems, security is usually considered only after the financial, legal, and structural issues have been settled. This seminar for security officers, DP managers, and auditors examines what to do before, during and after a major organizational change to ensure the adequate controls are in place. Computer security problems in merger/acquisition/divestiture situations, and what we can do about them. How major internal reorganizations, functional, consolidation, and plant closings affect security. These days many large corporations are "outsourcing" - getting out of the DP business by contracting all DP operations to an outside vendor. When this occurs, how do we ensure that the vendor properly protects our sensitive data and applications? What conditions increase an organization's vulnerability? Risk-reducing countermeasures. NOTE: Ask about available discount for government hosted classes.

COURSE TITLE: Computer Security And Privacy
COURSE LENGTH:

VENDOR:
Johns Hopkins University
9601 Medical Center Drive
Rockville, MD 10850
(301) 294-7070

This course surveys the broad fields of computer security and privacy, concentrating on the nature of the computer security problem by examining threats to systems, types of computer systems, and areas of system security and protection. Policy considerations related to the technical nature of the problem as manifested in government regulations and commercial practices are examined. The course develops the student's ability to assess system security weakness and formulate technical recommendations in the areas of hardware. Additional topics include access control (hardware/software), communications and network security, and the proper use of system software (op. system and utilities). The course addresses the social and legal problems of individual privacy in a data processing environment, as well as the computer "crime" potential of such systems. Several data encryption algorithms are examined. A student project or programming assignment may be required.

COURSE TITLE: Auditing the Data Center for Controls, Efficiency, and Cost-Effectiveness
COURSE LENGTH: 2 DAY

VENDOR:
MIS Training Institute
498 Concord Street
Framingham, MA 01701
(508) 879-7999

As an auditor in today's business environment, you must be familiar with the information processing function. In this seminar you will learn the components of a data center and the controls necessary to ensure accurate and reliable processing. The course covers data center operations, administration, scheduling, physical and data security, program change control, incident reporting, disaster recovery, and more. The seminar focus is on mainframe data centers, but includes security and audit responsibilities for mini and microcomputer environments as well. Participants should have attended IS Auditing and Controls or Auditing Automated Business Applications.

COURSE TITLE: Data Security Planning
COURSE LENGTH: 3 DAY

VENDOR:
IBM Management Institute
19th Floor
Chicago, IL 60611
(312) 245-3791

This course incorporates the latest thinking on data security planning and discusses practical methods used by leading companies. It presents the policies and guidelines of IBM and other organizations to help resolve the issues facing you and your organization. This course should be attended by staff or line management responsible for implementing or enhancing the data security program. It is also intended for data security administrators, auditors and others with a specific interest in data security. This is a management course, not a technical course. It is appropriate for organizations with large or small DP installations.

COURSE TITLE: Computer Viruses: Detect, Prevent, Cure Infections
COURSE LENGTH: 2 DAY

VENDOR:
CENTER for Adv. Professional Develop.
1820 E. Garry St.
Santa Ana, CA 92705
(714) 261-0240

Most of those who work with computers are aware of the existence of something called "computer virus," and the fact that it may be a danger to their computers or data. But it is hard to get good answers to the questions of what, exactly, a virus is, how great a danger it represents, and how to defend against any damage it might cause. Covering technical details where necessary, but always in non-technical language, this course will tell you what viri are, how they attack, how you can defend against them, and what the existence of viri mean to you and your use of computers. The course will give you a complete overview of all known ways that viri have "reproduced," and the various types of damage they have done. New viri are constantly being written so the course is constantly being updated, and research into ways that viri could attack, but haven't yet, will be reported.

COURSE TITLE: Disaster Recovery Planning
COURSE LENGTH: 3 DAY

VENDOR:
IBM Management Institute
19th Floor
Chicago, IL 60611
(312) 245-3791

The real objective is to develop and maintain recovery capability - not just for DP but - for the applications critical to the conduct of business. It is easier and cheaper to do this right. This course is designed for those who wish to understand the issues, the alternatives, those who have to put a recovery capability into place. Teams from both the DP and user communities are encouraged to attend together. This is a management course, not a technical course and the strategies discussed are independent of any particular hardware of software.

COURSE TITLE: Auditing the Systems Development Process
COURSE LENGTH: 3 DAY

VENDOR:
USDA Graduate School
600 Maryland Ave., S.W.
Washington, D.C. 20024
(202) 382-8620

Developing automated information and control systems is a critical, complex and costly undertaking for any organization. It is also an effort that is fraught with problems if not managed properly. This course will provide auditors in both the public and private sectors with an understanding of the systems development life cycle; a knowledge of problems that can and have been encountered in developing systems and the causes of such problems; and a methodology for auditing the systems development process and providing management with focused recommendations to prevent systems development efforts from failing. NOTE: This course is designed for all auditors who are, or will be, involved in audits of systems prior to installation into production. At least three years of auditing experience is required.

COURSE TITLE: Trusted Integration/System Certification
COURSE LENGTH: 2 DAYS

VENDOR:
ARCA
Commerce Center
10320 Little Patuxent Parkway
Suite 1005
Columbia, MD 21044
(410) 715-0500

This case-study workshop will introduce issues related to the procurement, development, certification and accreditation of a secure system solution for multilevel and multi-compartment information management. The individual will learn how to formulate and specify security requirements through a system security policy and security concept of operations. Participants learn how to develop a system security architecture and decompose it into cost-effective designs using trusted products as components. Seminar topics include integrating engineering plans, system and security requirements, system and security designs, system and security implementations, gathering assurance evidence and certification and accreditation.

COURSE TITLE: Risk Assessment Techniques For Auditors
COURSE LENGTH: 2 DAY

VENDOR:
MIS Training Institute
498 Concord Street
Framingham, MA 01701
(508) 879-7999

In this seminar you will learn how to design or select and implement a system for preparing your annual audit plan. You will learn ways to define an audit universe and auditable units. The risk concepts and methods you will learn will reduce your subjectivity and improve your efficiency and effectiveness in determining which audits to do when. The program examines techniques used by audit organizations today and compares strengths and weaknesses of the various methods. You will learn risk assessment, priority setting and decision making skills that will enable you to develop effective annual audit plans based upon risk.

COURSE TITLE: Operating System Security Concepts
COURSE LENGTH: 5 DAY

VENDOR:
National Security Agency
Airport Square
Baltimore
(301) 859-6417

An introduction to operating system concepts and terminology in computer security mechanisms. These concepts include operating system services, structures and processes; design principles; architectures; hardware security mechanisms; file systems; domain mechanisms; memory mapping; and device drivers. Specific threats, vulnerabilities and derived countermeasures to operating system security are emphasized. Specific case studies, e.g., MS/DOS, OS/2, MULTICS, UNIX, VAX/VMS, SCOMP and a variety of distributed operating systems. Problems and group exercises reinforce class presentations. Prerequisites: Bachelor's degree in Computer Science/Electrical Engineering/Mathematics or equivalent experience. Experience developing software employing operating systems capabilities is desirable. NOTE: This course is technical in nature. Call the vendor regarding a clearance.

COURSE TITLE: Trusted Systems Criteria and Concepts
COURSE LENGTH: 5 DAY

VENDOR:
National Security Agency
Airport Square
Baltimore
(301) 859-6417

A study which examines the principles and technology underlying the DoD Trusted Computer System Evaluation Criteria (TCSEC), and the related topics of trusted system evaluations and accreditation. Specific topics include basic principles of trusted systems, mandatory and discretionary access control (MAC & DAC), user accountability, security architectures, formal security models, TCSEC interpretations and other assurance techniques. Students examine how to build secure applications for a trusted system without invalidating the system's evaluation. Students reinforce class presentations by using the Xenix 2 software package in laboratory exercises. Prerequisites: Familiarity with operating systems and a Bachelor's degree in Computer Science/Electrical Engineering/Mathematics or equivalent experience. NOTE: This course is technical in nature. Call the vendor regarding a clearance.

COURSE TITLE: Theoretical Foundation/Trust of Information Systems
COURSE LENGTH: 5 DAY

VENDOR:
National Security Agency
Airport Square
Baltimore
(301) 859-6417

A study of fundamental concepts of models in computer security. Develops techniques necessary to identify and describe problems in computer security using mathematical and logical concepts. Addresses the development of a formal model for computer security, demonstrates that the model is consistent with its axioms and that the model is used in designing secure systems. Instruction covers classic Bell La Padula (BLP) model, as well as access control, information flow, non-interference, concurrence, network security and take-grant models. Surveys newer models: database, integrity and event-based. Prerequisites: CP-510 and a Bachelor's degree in Computer Science/Electrical Engineering/Mathematics of equivalent experience. Familiarity with mathematical logic is desirable. NOTE: This course is technical in nature. Call the vendor regarding a clearance.

COURSE TITLE: Architecture for Secure Systems
COURSE LENGTH: 5 DAY

VENDOR:
National Security Agency
Airport Square
Baltimore
(301) 859-6417

A study of the basic architectural features to support secure computer systems. Using requirements of trusted computer systems evaluation criteria, the student will study design and implementation of various protection systems by addressing required protection and domain separation mechanisms. Prerequisites: CP-510 and a firm understanding of the Bell La Padula Model. A Bachelor's degree in Computer Science/Electrical Engineering/Mathematics or equivalent experience. Experience in developing software using operating systems capabilities is desirable. NOTE: This course is technical in nature. Call the vendor regarding a clearance.

COURSE TITLE: Network Security Architecture
COURSE LENGTH: 2 DAY

VENDOR:
National Security Agency
Airport Square
Baltimore
(301) 859-6417

A study covering networking and protocol concepts important for building secure systems in a variety of areas including: (1) network security concepts related to different types of computer networks (2) layered protocol-security in general and the OSI Reference Model in particular (3) the Government Open Systems Interconnection Profile (GOSIP), including a description of the security options supported (4) OSI Security Architecture, describing the OSI security services, mechanisms and management (5) network security design factors for confidentiality, integrity and assured service. Prerequisites: Bachelor's degree in Computer Science/Electrical Engineering/Mathematics or equivalent experience. Familiarity with data communications and computer security concepts/terminology is desirable.----CP-533 and 535 are specifically structured to present a complete component of network information during a five-day week; we highly recommend students take both courses. NOTE: This is technical in nature. Call the vendor regarding a clearance.

COURSE TITLE: Advanced Network Security Architecture
COURSE LENGTH: 3 DAY

VENDOR:
National Security Agency
Airport Square
Baltimore
(301) 859-6417

A study covering advanced secure network and protocol concepts important for building secure systems in a variety of areas including: (1) the OSI Security Architecture (2) detailed protocol descriptions (i.e., IEEE 802 Standards; data link protocols, X.25 and related standards; Transmission Control Protocol/Internet Protocol (TCP/IP); Security Protocol 4 (SP4)/Security Protocol 3 (SP3); File Transfer, Access and Management (FTAM) Protocol; and Key Management Protocol (KMP)) (3) Secure network performance analysis using probability theory, queuing theory and simulation (4) Integrated Services Digital Network (ISDN) and its relationship to computer security and the OSI Reference Model (5) security services provided by protocols such as confidentiality, integrity and assured service (6) specific network applications including SDNS, BLACKER, CANEWARE, IBM's SNA, Novell's NetWare, Defense Data Network (DDN), FTS 2000 and Electronic Data Interchange (EDI). Prerequisites: CP-533 and a Bachelor's degree in Computer Science/Electrical Engineering/Mathematics or equivalent experience.---CP-533 and 535 are specifically structured to present a complete component of network information during a five-day week; we highly recommend students take both courses. NOTE: This course is technical in nature. Call the vendor regarding a clearance.

COURSE TITLE: Model Interpretations
COURSE LENGTH: 5 DAY

VENDOR:
National Security Agency
Airport Square
Baltimore
(301) 859-6417

A study covering the interpretation and subsequent application of the rules of formal security policy models. Student will compare (map) these rules to a system's software to ensure that the system's performance accurately complies with the formal models. Comparison will require application of these rules to lower specification levels of both operating systems and hardware architectures. Course will also cover state-of-the-art applications of formal models. Prerequisites: CP-510, 520 and 530. Bachelor's degree in Computer Science/Electrical Engineering/Mathematics or equivalent experience. Experience with mathematical logic is desirable. NOTE: This course is technical in nature. Call the vendor regarding a clearance.

COURSE TITLE: Introduction to Software Verification
COURSE LENGTH: 15 DAY

VENDOR:
National Security Agency
Airport Square
Baltimore
(301) 859-6417

A study covering the state-of-the-art in verification techniques and practice using two, endorsed NCSN verification tools. Techniques include a comparison between code and design verification. Student will read, write and execute basic specifications and understand first-order logic and verification systems. Student will develop and prove properties of formal specifications. Prerequisites: MP470 or working knowledge in predicate calculus and first-order logic, CP-510 and a Bachelor's degree in Computer Science/Electrical Engineering/Mathematics or equivalent experience. NOTE: This course is technical in nature. Call the vendor regarding a clearance.

COURSE TITLE: INFOSEC Evaluations Using Formal Methods
COURSE LENGTH: 5 DAY

VENDOR:
National Security Agency
Airport Square
Baltimore
(301) 859-6417

A study covering the verification paradigm in detail; derivation of the security policy and its corresponding formal model; formulation of a Formal Top Level Specification (FTLS) and Descriptive Top Level Specification (DTLS); and mapping of the FTLS to implementation. Each of the parts of the paradigm will be investigated in terms of content and sufficiency to meet the design specification and verification requirements for the information security system being developed. Examples will cover how verification can be used with cryptographic Communications Security (COMSEC) products. Prerequisites: CP-510 and a Bachelor's degree in Computer Science/Electrical Engineering/Mathematics of equivalent experience. Knowledge of mathematical logic is desirable. NOTE: This course is technical in nature. Call the vendor regarding a clearance.

COURSE TITLE: COMSEC
COURSE LENGTH: 1 Day

VENDOR:
Security Engineering Services, Inc.
5005 Bayside Road
Chesapeake Beach, MD 20732
Bruce Gabrielson: (301) 855-4565

Participants are provided an in-depth technical presentation of both design requirements and theoretical issues.

Topics Covered
Security Overview, RED/BLACK Concepts, Encryption, CCEP and Military Devices
Facility Design, SCIF Issues, System/Network Design, Hardware Box Level Design, TSRD, Security Fault Analysis, TEMPEST Countermeasures

Student Background: BSEE or equivalent design experience. Not intended for non-technical end users.

Sponsor Required - Classified: (SECRET) - Coursebook: (UNCLASSIFIED)
**Note: There is also a confidential version of this course.

COURSE TITLE: Network Security
COURSE LENGTH: 1 Day

VENDOR:
Security Engineering Services, Inc.
5005 Bayside Road
Chesapeake Beach, MD 20732
Bruce Gabrielson: (301) 855-4565

Participants learn the "how to" of integrating network security into their overall ADP security program. This course is intended to provide formal training for computer security engineers.

Topics Covered
UNIX/Apple/Novel Security Models, Software/Hardware Protection, Hackers and Crackers, Network Cracking, Gateway protection, Proactive Security, Examples

Student Background: BSCS or equivalent background, Network management experience

COURSE TITLE: GBA 578: Security and Privacy of Information Systems
COURSE LENGTH:

VENDOR:
California State Polytechnic, Univ, Pomona
College of Business Administration
Computer Information Systems Department
3801 West Temple Avenue
Pomona, CA 91768-4083
Dan Manson: (714) 869-3244

The purpose of the course is to introduce students to security and privacy issues at two levels. The textbook provides a view of information protection issues from a management viewpoint. The audit project will give students an opportunity to translate information protection requirements from management theory to a practical level by reviewing access controls in an actual computer system. Concepts of information security and privacy. Understanding information protection, physical and logical security of information systems. Prerequisite: CIS 433, GBA 577 or permission of instructor.

COURSE TITLE: CIS 433, EDP Auditing
COURSE LENGTH: 10 WEEKS

VENDOR:
California State Polytechnic Univ, Pomona
College of Business Administration
Computer Information Systems Department
3801 West Temple Avenue
Pomona, CA 91758-4083
Dan Manson: (714) 869-3244

Auditing in a computer information systems environment involves evidence that originates or is maintained in a computer system. The course provides students with an understanding of the role of the EDP Audit function, the purpose of controls in a computer environment, and skills required to perform EDP Audits. Fundamentals of EDP auditing. Understanding EDP controls, types of EDP audits, risk assessment and concepts, and techniques used in EDP audits. Prerequisite: ACC 419 or CIS 406 or permission of instructor.

COURSE TITLE: GBA 560 Legal Environment of Information Systems
COURSE LENGTH:

VENDOR:
California State Polytechnic Univ, Pomona
College of Business Administration
Computer Information Systems Department
3801 West Temple Avenue
Pomona, CA 91768-4083
Frederick Gallegos: (714) 869-3244

This course is intended to provide the student with a fundamental working knowledge of a number of legal areas of the data processing industry. The course will stress the area of contract contents and interpretation, tort liability including negligence and misrepresentation in the computer industry and intellectual property rights analysis, including a survey of the areas of copyright, patent and trade secrets and trademark law.

It is hoped that the student would obtain a fundamental knowledge of the legal concepts involved such that as problems arise, the student will be able to recognize, in a working environment. that legal issues must be addressed.

COURSE TITLE: GBA 577: Advanced EDP Auditing
COURSE LENGTH: 3.5 HRS.

VENDOR:
California State Polytechnic Univ, Pomona
College of Business Administration
Computer Information Systems Department
3801 West Temple Avenue
Pomona, CA 91768-4083
Dan Manson: (714) 869-3244

Auditing in a computer information systems environment involves evidence that originates or is maintained in a computer system. The course provides students with an understanding of the role of the EDP Audit function, the purpose of controls in a computer environment, and skills required to perform EDP Audits. Advanced concepts in EDP Auditing. Understanding EDP controls, types of EDP audits, risk assessment and concepts, and techniques used in EDP audits. Prerequisite: CIS 433 or permission of instructor.

COURSE TITLE: Computer Security for the End-User
COURSE LENGTH: 1 DAY

VENDOR:
COMSIS
8737 Colesville Road, Suite 1100
Silver Spring, MD 20910
Ronald E. Freedman: (301) 588-0800

This course provides training to end-users who operate sensitive and mission-critical systems and/or rely upon automated information systems to perform their work.

COURSE TITLE: Information Systems Security (CSI 214)
COURSE LENGTH: 1 SEMESTER

VENDOR:
Anne Arundel Community College
Engineering and Computer Technology
Careers 219
101 College Parkway
Arnold, MD 21012-1895
Gail Reese: (410) 541-2758

A survey of topics in data retention and control and techniques associated with data, computer systems, network and installation security. The student will obtain skills related to occupations in data libraries and data security at computer installations. NOTE: Three semester hours; prerequisite: CSI 113 or permission of department head.

COURSE TITLE: TEMPEST Program Management and Systems Engineering
COURSE LENGTH: 2 DAYS

VENDOR:
Security Engineering Services, Inc.
5005 Bayside Road
Chesapeake Beach, MD 20732
Bruce Gabrielson: (301) 855-4565

This course provides students with a technical background of what TEMPEST is and how it is applied to insure secure information is protected at the system/user level. In addition, the course provides managers with the requisite background to successfully manage a commercial or military TEMPEST program.

Introduction and History, Theory Overview
Program Management: Military and Commercial, ETPP, SSEM Aspects
Requirements: DID's
Relationship to COMSEC and EMC
Introduction to RED/BLACK Systems: Network Overview, Cabling, Fiber Optics
Facility Design: Shielding, Power Systems, Isolation Transformers, Portable Enclosures
TEMPEST Vulnerability Assessments
Overview of Network Testing, Test Labs, and Zones
Emerging Issues

Student Background: Experienced Security Officers, TEMPEST Engineers or Managers

Sponsor Required - Classified: (SECRET) - Coursebook: FOUO

COURSE TITLE: CSMN 655 - Information Risk Assessment and Security Management
COURSE LENGTH: 1 Sem.

VENDOR:
University of Maryland, University College
Graduate School of Management & Technology
University Boulevard at Adelphi Road
College Park, MD 20742-1614
Associate Professor P.F.G. Keller: (301) 985-7989

This course provides an in-depth study of the physical, logical, and personnel vulnerabilities of information and telecommunications systems operations. It examines the historical, philosophical and emerging trends in risk assessment methodology and the parallel contributions to security and the control of information environments. This course fosters a deeper understanding of the elements of management through an analysis of industry and government information resource recovery procedures and develops insights into problems associated with regulation of computer and information resources.

COURSE TITLE: Computer Crime & Industrial Espionage
COURSE LENGTH: 1 DAY

VENDOR:
Computer Security Institute
600 Harrison Street
San Francisco CA 94107
(415) 905-2626

By the year 2000, projections suggest that an amazing 2.5 billion people will have access to computer systems. Clearly, our old concepts of doing business are changing! The opportunity for misuse of computers increases each day. This seminar is designed to help data processing managers, plant and DP security personnel, and auditors understand the unique nature of computer crime and the vulnerability of their critical and sensitive information to misuse. We will examine the current state of computer crime and explore specific methods used for illicit information gathering. Unauthorized attempts to access corporate data are no longer likely to be teenage hackers playing games. Industrial espionage has become a significant threat as many major corporations adopt the philosophy that it's more important to know what the competition is doing than what the customer wants. You will learn where confidential corporate information is leaking and what can be done to reduce the threat. You will hear about a number of actual incidents of computer-aided crime and the specific steps you can take to prevent similar abuses from occurring in your organization. NOTE: Ask about available discount for government hosted classes.

COURSE TITLE: A Practical Approach to Certifying a System
COURSE LENGTH: 2 DAY

VENDOR:
Computer Security Institute
600 Harrison Street
San Francisco CA 94107
(415) 905-2626

This course shows you how to go about certifying the security of a system, whether IBM, DEC, another vendor, or a combination of equipment and software on a network. The approach used in the class will provide you with flexible techniques to conduct risk assessments, to obtain consensus on the standard (whether or not a formal standard exists), to develop a framework for certification, and to identify and evaluate the controls on the system against this framework. The result is a documented summary of the risks and controls, organized in a way that permits easy follow-up and modification if needed. These techniques can be applied to any organizational culture. NOTE: Ask about available discount for government hosted classes.

COURSE TITLE: The Security-Audit Alliance
COURSE LENGTH: 3 DAY

VENDOR:
Computer Security Institute
600 Harrison Street
San Francisco CA 94107
(415) 905-2626

This one day session is intended for both auditors and security controls. It will provide both groups of professionals with specific ideas to improve their effectiveness and productivity by working together in non-traditional ways. NOTE: Ask about available discount for government hosted classes.

COURSE TITLE: Operational Network Security Seminar
COURSE LENGTH: 2 DAYS

VENDOR:
ARCA
Commerce Center
10320 Little Patuxent Parkway
Suite 1005
Columbia, MD 21044
(410) 715-0500

This seminar will teach the individual how to assess the level of operational network security required in different networking environments and how to implement security measures in these environments. Participants will gain a knowledge of basic operational network security principles, and an understanding of current threats to network security. This session will enable the individual to understand the differences in operational environments and to gain knowledge of network security architectures and their effectiveness in achieving security. The individual will gain an understanding of gateway-level solutions, including firewalls, and secure routers and a familiarity with network security tools including intrusion detection systems.

COURSE TITLE: Computer Viruses Seminar
COURSE LENGTH: 1 Day

VENDOR:
ARCA
Commerce Center
10320 Little Patuxent Parkway
Suite 1005
Columbia, MD 21044
(410) 715-0500

The Computer Viruses Seminar will teach individuals how to detect viruses on PC and Macintosh platforms, how to determine what a virus is programmed to do and how to respond efficiently to a virus infection in stand-alone systems and local area networks. The curriculum covers what a virus is and how virus code differs from other types of malicious code, typical virus structures and modes, virus replication, activation and survival mechanisms. You will learn the symptoms and effects of virus infections and the basic mechanisms of virus detection and eradication software. Also covered are the advantages and limitations of major virus detection and eradication software.

COURSE TITLE: Business Impact Analysis
COURSE LENGTH: 2 DAYS

VENDOR:
Disaster Recovery Institute
1810 Craig Road, Suite 213
St. Louis, MO 63146-4761
Bill Langendoerfer: (314) 434-2272

This course is designed for contingency planners who will be involved in organizing, managing, and conducting a Business Impact Analysis (BIA). It is appropriate for all levels of contingency planning experience.

Topics to be addressed include discussions of an organization's contingency program and planning methodology. Participants are introduced to the business impact analysis and the importance of this element in the Functional Requirements Phase of corporate contingency planning. Attendees will address how to plan and successfully conduct a business impact analysis project. Class participation and team utilization of ideas will be emphasized.

Upon completion of the course, students will be able to understand the need and commitment required to conduct a BIA; plan the BIA project to determine the scope, resources, and time requirements; conduct the data gathering; analyze the data to reach conclusions; document the findings to achieve results; and obtain acceptance of the findings and approval to go to the next step.

COURSE TITLE: Communications Technologies
COURSE LENGTH: 2.5 DAYS

VENDOR:
Disaster Recovery Institute
1810 Craig Road, Suite 213
St. Louis, MO 63146-4761
Bill Langendoerfer: (314) 434-2272

This course is the second of four courses intended for novices in the area of disaster recovery planning. It is designed for disaster recovery planners who are unfamiliar with communications technologies as well as prospective contingency planners, data communications managers, and others who will be involved in the development or management of the contingency plan and the recovery of communications networks.

Participants will be introduced to network components, network loading analysis, voice network analysis, and other significant aspects of network recovery planning. Attendees will also learn to identify and evaluate alternative configurations and techniques. Class participation and team utilization of concepts will be emphasized.

Upon completion of the course, students will be able to understand the concepts of electronic communications, identify the components in a data communications network, identify and examine alternative configurations and techniques for the backup and recovery of networks, and begin emergency planning and control of communications recovery teams.

COURSE TITLE: Managing and Developing a Disaster Recovery Plan
COURSE LENGTH: 2.5 DAYS

VENDOR:
Disaster Recovery Institute
1810 Craig Road, Suite 213
St. Louis, MO 63146-4761
Bill Langendoerfer: (314) 434-2272

This course is designed for those who have limited experience in the area of disaster recovery planning. It was developed for prospective contingency planners, operations managers, data communications managers, disaster planning and recovery team members, and others who will be involved in the development or management of the contingency planning and recovery functions.

The course will prepare participants for managing the planning project, developing the actual plan, and preparing the plan's documentation. Students will review verbal and written communications techniques, the basics of disaster recovery plan design using project teams, the selection of alternative procedures, and basic documentation standards. Class participation and team utilization of concepts will be emphasized.

Upon completion of the course, participants will be able to apply improved project and time management skills for managing the planning project, use improved verbal and written communications skills and techniques to communicate with organization management and disaster recovery teams, develop the basic design of the disaster recovery plan, produce standardized documentation of the plan, and use improved management report presentation techniques and skills to assist in gaining plan approval.

COURSE TITLE: Implementing and Testing the Disaster Recovery Plan
COURSE LENGTH: 2.5 DAYS

VENDOR:
Disaster Recovery Institute
1810 Craig Road, Suite 213
St. Louis, MO 63146-4761
Bill Langendoerfer: (314) 434-2272

This course is designed for those who have limited experience in the area of disaster recovery planning. It was developed for prospective contingency planners, operations managers, data communications managers, disaster planning and recovery team members, and others who will be involved in the development or management of the contingency planning and recovery functions.

The course will prepare participants to develop the detailed procedures within the disaster recovery plan and be prepared to teach those procedures when training other disaster recovery teams. Other topics to be explored include the development of a testing and assessment program, as well as periodic maintenance of the plan. Class participation and team utilization of concepts will be emphasized.

As part of this course, participants will learn to develop and conduct specialized training courses for those participating in the design and implementation of the plan; implement the plan by developing detailed recovery procedures; develop a disaster recovery plan testing program that incorporates various scenarios, periodic use of recovery teams, and documentation of the test results; and apply methods and procedures for reviewing the recovery plan controls, maintaining the plan, and evaluating its effectiveness.

COURSE TITLE: The CMW: Application Programming
COURSE LENGTH:

VENDOR:
Trusted Systems Training, Inc.
1107 South Orchard Street
Urbana, IL 61801-4851
Steve Sutton: (217) 344-0996

The course addresses programmers who create or port trusted applications for Compartmented Mode Workstations based on the SecureWare technology, including SecureWare's CMW+, Hewlett-Packard's BLS, and Digital's MLS+. It teaches the secure use of all new security features, like Protected Subsystems, sensitivity and information labels, and trusted (MaxSix) networking. The course book and accompanying textbook include many programming examples and written exercises that form the basis for classroom learning.

COURSE TITLE: PC SECURITY
COURSE LENGTH: 1 DAY

VENDOR:
Booz•Allen & Hamilton
8th Floor, Room 822
8283 Greensboro Drive
McLean, VA 22102-3838
Butch Chaboudy: (703) 902-5265

This course provides a basic understanding of Information Security as it applies to Personal Computers and PC networks. The student will learn the key elements of information security and gain an understanding of concepts such as risk management, trusted products and certification and accreditation as it applies to the PC environment. User responsibilities are stressed and user actions that lead to security problems are discussed. Additionally, the student will gain an understanding of the security attributes of basic network topologies and be able to apply user action to protect their system as part of a network or when operating in a stand-alone configuration.

COURSE TITLE: LAN Security
COURSE LENGTH: 16 HRS

VENDOR:
DATAPRO Educational Services
600 Delran Parkway
Delran, NJ 08076
(609) 764-0100

This course will provide the student with a comprehensive view of the issues involving the security of the Local Area Networks. It will also provide a basic knowledge of the management of ARLs. user rights, and login-password routines of Novell, Starian and Banyan. The instructor and students will discuss the various policy issues and the tactics required to involve management on the security LAN installations, and selling security to the end-users.

COURSE TITLE: The CMW: User Tutorial
COURSE LENGTH:

VENDOR:
Trusted Systems Training, Inc.
1107 South Orchard Street
Urbana, IL 61801-4851
Steve Sutton: (217) 344-0996

The course addresses the day-to-day users of Compartmented Mode Workstations based on the SecureWare technology, including SecureWare's CMW+, Hewlett-Packard's BLS, and Digital's MLS+. It teaches the principles and use of all new security features, like the Trusted Path, authorizations, access control lists, and sensitivity and information labels. students learn all they need to know to securely use these systems. The course book and accompanying textbook include written and on-line, self-paced exercises that form the basis for classroom learning. This course also serves as the basis for more advanced CMW courses.

PRODUCT SPECIFIC COURSES

RACF

COURSE TITLE: SE02: RACF for Security Officers
COURSE LENGTH: 1 DAY

VENDOR:
Grumman Data Systems
2411 Dulles Corner Park, Suite 500
Herndon, VA 22071
Bruce Levy: (703) 713-4121

Objectives of the Course: Give Security Officers the ability to monitor and control access to data and resources for projects on an MVS system using RACF. Specifically they will learn to list and describe the options available under RACF, use RACF to authorize the use of resources and control access to data, and to monitor compliance with security procedures.

Specific topics include an overview of RACF, how it provides security, Dod requirements, setting RACF options including tape protection, reporting activity, protecting system resources, programs and datasets, RACF and TSO, monitoring security using AUDITOR, and RACF recovery.

COURSE TITLE: SE01: RACF for Project Managers
COURSE LENGTH: 2 DAYS

VENDOR:
Grumman Data Systems
2411 Dulles Corner Park, Suite 500
Herndon, VA 22071
Bruce Levy: (703) 713-4121

Objectives of the Course: Give Project Managers the ability to manage and control authorization to access and modify data and userid resources for projects under their jurisdiction. Specifically they will learn to manage and control access to project related data, list and describe the userid controls available under RACF.

Specific topics include an overview of RACF, global access checking, discretionary and mandatory access controls, discussions of what makes a system secure and DoD requirements, using RACF commands, RACF groups, resource profiles and permits, and the control of userids.

COURSE TITLE: Auditing RACF
COURSE LENGTH: 2 DAY

VENDOR:
RSH Consulting, Inc.
29 Caroline Park
Newton, MA 02168
Bob Hansel: (617) 969-9050

This course is designed to give auditors and security administrators who are new to RACF a foundation and framework for reviewing controls. It provides an introduction to RACF and presents a structured program for conducting a RACF audit in an MVS environment. The course begins by providing basic information on the function, features, options, and components of RACF. Users, groups, and resources will be described, and their relationships will be defined. The logic RACF uses to determine whether access administrative authorities will also be discussed. Lastly, audit tools, techniques, and strategies will be described. Sample RACF reports will be used to examine RACF controls and identify vulnerabilities. The course provides a comprehensive set of tools and techniques required for conducting an effective audit.

COURSE TITLE: Effective RACF™ Administration (H3927)
COURSE LENGTH: 4.5 DAYS

VENDOR:

Skill Dynamics - An IBM Company
One IBM Plaza, 19th Floor
Chicago, IL 60611
(800) IBM-TEACh (800) 426-8322

This lab course teaches you how to RACF effectively to implement resource access control for MVS and VM systems. Course emphasis is on preparing you to be an effective security administrator when you return to your job. Through a combination of lecture and hands-on lab exercises you will gain experience and confidence in using RACF. Classroom lecture topics are reinforced with hands-on lab exercises where you will use RACF commands and panels to define users, set-up a group structure, protect resources, and produce audit reports.

*RACF is a trademark of the IBM Corporation

COURSE TITLE: RACF™ Installation (H3837)
COURSE LENGTH: 1.5 DAYS

VENDOR:

Skill Dynamics - An IBM Company
One IBM Plaza, 19th Floor
Chicago, IL 60611
(800) IBM-TEACh (800) 426-8322

This course teaches you how to install and support RACF in MVS and VM environments.

*RACF is a trademark of the IBM Corporation

COURSE TITLE: RACF: Proper Implementation and Security
COURSE LENGTH: 3 DAY

VENDOR:
MIS Training Institute
498 Concord Street
Framingham, MA 01701
(508) 879-7999

This course introduces you to the facilities of RACF that have an impact upon audit and control objectives. It provides a complete overview of all important functions and terminology associated with RACF. You will learn to identify how RACF functions within your MVS installation and how to audit its use and administration. The course covers the Data Security Monitor and other Auditability enhancements in versions 1.7 and 1.8. You will also learn the internal security features of RACF and how you can conduct tests to insure that control and audit mechanisms are implemented properly. The seminar outline is subject to change based on enhancements and changes to the RACF product. Participants should have attended OS/MVS Operating:Security and Audit. NOTE: A 2-DAY WORKSHOP IS ALSO AVAILABLE.

COURSE TITLE: How to Get the Most Out of RACF
COURSE LENGTH: 5 DAYS

VENDOR:
the Henderson Group
6101 Wynnwood Road
Bethesda, MD 20816
(301) 228-7187

This course provides data security officers, auditors, and RACF administrators with a comprehensive foundation in RACF, how it works, and how to use it, including the new features of RACF 1.9.2. (RACF is IBM's strategic security software for mainframe computers.) Students learn: all the operands of all the commands; how to use each resource class; a strategy for rapid, effective, roll-out of RACF protection; and a non-technical understanding of RACF internals, architecture, and philosophy. This course covers how to use RACF with: CICS, VM, DB2, IMS, SMS, and other software such as job schedulers. Students receive a 350-page workbook/reference manual as part of the course. Handouts include exercises and diagrams showing the relation between RACF and other system software.

COURSE TITLE: Practical Approach to Auditing RACF
COURSE LENGTH: 2 DAYS

VENDOR:
the Henderson Group
6101 Wynnwood Road
Bethesda, MD 20816
(301) 228-7187

You cannot have effective security in an MVS installation without security software such as RACF, ACF2, or TopSecret. This course provides EDP auditors and security administrators with a basic understanding of what RACF is and how it works, and then shows you how to audit or review it. Attendees develop their own RACF audit or security review program as a class exercise. The course workbook provides forms for data collection and analysis, as well as a checklist of items to consider incorporating into the plan. Handouts include exercises and diagrams showing the relation between RACF and other system software. This course addresses all the features of RACF 1.9 and 1.9.2. Attendees learn: how RACF works in non-technical terms; how to evaluate RACF protection; how to evaluate delegation of authority and the RACF group structure; what data to gather, how to gather it, and how to analyze it to audit RACF efficiently.

DB2

COURSE TITLE: Practical Approach to Auditing DB2 Security
COURSE LENGTH: 2 DAYS

VENDOR:
the Henderson Group
6101 Wynnwood Road
Bethesda, MD 20816
(301) 228-7187

DB2 (IBM's strategic database management software for mainframe computers) has its own approach to security. This approach is very different from that found with ACF2, RACF, or TopSecret. An effective security program will provide for integration of DB2 security and administration with the rest of the security program on a mainframe. DB2's security approach is different because it has its own mechanisms for identifying users and for determining what each user is permitted to do. In this seminar you will learn how these mechanisms work, and to identify how they are implemented in a given installation. This seminar provides auditors and security administrators with a basic introduction to DB2 concepts and SQL (Structured Query Language). You will have the opportunity to develop your own DB2 audit or security review program as a class exercise. Attendees receive a 100-page reference manual and a variety of handouts including exercises and diagrams showing the relation between DB2 and other software in the computer. You will learn: how to investigate and evaluate DB2 security; how DB2 security relates to security software such as ACF2, RACF, or TopSecret; use of DB2 tools such as referential integrity for data integrity and data quality; what data to gather, how to gather it, and how to analyze it to evaluate DB2 security efficiently; and DB2 security and control considerations for designing and application or for conducting an application controls review. (An application controls review provides for review of an application system, either after or during its development, to identify ways to improve controls over data integrity and reliability.)

COURSE TITLE: Auditing DB2
COURSE LENGTH: 2 DAY

VENDOR:
Canaudit Inc.
P.O. Box 4150
Simi Valley, CA 93093
(805) 583-3723

IBM's DB2 language is now an accepted standard. As a result, auditors are currently faced with yet another area where they must perform a highly technical audit. This seminar provides the auditor with a detailed understanding of DB2, the audit issues and concerns, as well as useful audit programs which address DB2, security and the interfaces with IMS and CICS. This intensive session prepares the auditor for their first DB2 audit. Special emphasis is placed on the controls inherent in DB2 and how to use them.

COURSE TITLE: Audit & Security of DB2
COURSE LENGTH: 3 DAY

VENDOR:
MIS Training Institute
498 Concord Street
Framingham, MA 01701
(508) 879-7999

In this course you will learn how IBM's newest relational data base operates and how it affects the integrity, security, and control of application systems. You will first gain a thorough understanding of the specific ways in which DB2 exposes your organization to threats such as data security, integrity, reliability, backup and recovery. You will then learn specific audit controls to employ to reduce those risks. You will leave the seminar knowing all the control points and retrieval utilities that are available within DB2. More importantly, you will take back to the job a tested audit approach to use in your DB2 environment. NOTE: A 2-DAY WORKSHOP IS ALSO AVAILABLE.

VTAM

COURSE TITLE: What Data Security Officers & Auditors Need to Know and Do About VTAM Security
COURSE LENGTH: 1 DAY

VENDOR:
the Henderson Group
6101 Wynnwood Road
Bethesda, MD 20816
(301) 228-7187

This course provides you with an understanding of VTAM (IBM's Virtual Telecommunications Access Method) and how it works, along with a description of the critical control points in a network definition. Since VTAM both determines and controls the paths into your system, you need to understand VTAM security to provide comprehensive computer security. This course will show you how, even if you have no experience with telecommunications. The workbook provides forms for data collection and analysis, as well as a reference of VTAM terms and concepts. Handouts include exercises and diagrams showing the relations of VTAM components to each other, and to other system software.

MVS

COURSE TITLE: OS/MVS and SMF: Security and Audit Facilities
COURSE LENGTH: 4 DAYS

VENDOR:
MIS Training Institute
498 Concord Street
Framingham, MA 01701-2357
Sharon G. Friedman: (508) 872-7990

This intensive four-day seminar focuses on the facilities available within MVS for solving audit and security programs. You will learn how MVS works, how you can use MVS utilities as an audit tool, and the essentials of TSO/ISPF. You will cover, in detail, the operation of SMF, the MVS audit trail. You will learn potential audit exposures within the SMF installation, and the various audit trail records that can be extracted from SMF and then analyzed. You will leave this session with and understanding of MVS and the MVS utilities, and with the know-how to use SMF as an audit tool. NOTE: Participants should have attended IS Audit and Control and have IS audit experience.

COURSE TITLE: MVS/ESA as a Server, Peer and Open System Audit, Control, and Security
COURSE LENGTH: 2 DAYS

VENDOR:
MIS Training Institute
498 Concord Street
Framingham, MA 01701-2357
Sharon G. Friedman: (508) 872-7990

In this high-octane session, you will explore the new features available in the MVS/ESA operating system that counteract its weakness as an open system. You will examine the open system-based networks that provide users a more direct window into the data processing of the enterprise, and address the resulting control and security issues. The MVS operating system as an open system is a reality and its role as a peer will continue to expand as hardware platforms that run MVS become powerful , two-day session to discover the client/server systems and facilities that allow MVS/ESA to be a server of servers and to learn what you need to know to audit and secure it.

COURSE TITLE: SECO2-M: MVS Security for Security Officers
COURSE LENGTH: 1 DAY

VENDOR:
Grumman Data Systems
2411 Dulles Corner Park, Suite 500
Herndon, VA 22071
Bruce Levy: (703) 713-4121

Objectives of the Course: Give Security Officers the ability to monitor and control access to an MVS system. Students will learn to write appropriate security procedures for an MVS system with ACF2, implement ACF2 security rules, and to monitor compliance with security procedures.

Specific topics include discussion of security policies, directives and procedures, an overview of ACF2 features and capabilities, ACF2 database resource access rules and how to maintain/modify them, ACF2 commands for userid record maintenance, TSO records and defaults, batch processing options and rules, reporting of violations and testing.

COURSE TITLE: SECO1-M: MVS Security for Project Managers
COURSE LENGTH: 2 DAYS

VENDOR:
Grumman Data Systems
2411 Dulles Corner Park, Suite 500
Herndon, VA 22071
Bruce Levy: (703) 713-4121

Objectives of the Course: Give MVS project managers an understanding of how to monitor and control access to data within the scope of their authority.

Specific topics include: an overview of ACF2 features and capabilities, description of ACF2 databases, the rules which allow specific access to MVS datasets and how to write those rules, ACF2 commands, the use of NEXTKEY, testing procedures and the maintenance of basic userid characteristics. The project manager will be introduced to the use of ACF2 to enforce security on an MVS system.

COURSE TITLE: Auditing MVS in a CA-ACF2 Environment (M2030)
COURSE LENGTH: 1.5 DAYS

VENDOR:

Skill Dynamics - An IBM Company
One IBM Plaza, 19th Floor
Chicago, IL 60611
(800) IBM-TEACh (800) 426-8322

This course teaches you the necessity for and the implementation of effective controls in the MVS operating system within a CA-ACF2 environment. You will learn how to apply the controls provided within a CA-ACF2 system to the problems discussed in MVS Security (Course Code M2002) and MVS Auditing (Course Code M2024). You will also learn how to use CA-ACF2 security and audit tools to better understand the protection of your system.

COURSE TITLE: Auditing MVS in a CA-TOP SECRET™ Environment (M2032)
COURSE LENGTH: 1.5 DAYS

VENDOR:

Skill Dynamics - An IBM Company
One IBM Plaza, 19th Floor
Chicago, IL 60611
(800) IBM-TEACh (800) 426-8322

This course teaches you the necessity for and the implementation of effective controls in the MVS operating system within a CA-TOP SECRET environment. You will learn how to apply the controls provided within a CA-TOP SECRET system to the problems discussed in MVS Security (Course Code M2002) and MVS Auditing (Course Code M2024). You will also learn how to use CA-TOP SECRET security and audit tools to better understand the protection of your system. Hands-on labs will utilize CA-TOP SECRET tools to ascertain the current security status of an MVS system.

*CA-TOP SECRET is a trademark of Computers Associates, Inc.

COURSE TITLE: MVS Auditing (M2024)
COURSE LENGTH: 3.5 DAYS

VENDOR:

Skill Dynamics - An IBM Company
One IBM Plaza
Chicago, IL 60611
(800) IBM-TEACh (800) 426-8322

This course teaches you how to review the security controls in an MVS environment. You will explore the security sensitive areas of the MVS environment. You will learn the types of information needed to assess the strength of implemented controls as well as how to perform the collection of this information. Hands-on MVS system auditing will be conducted so that attendees may gain experience in performing audit procedures and in interpreting security related data. This course focuses on MVS systems in general and is not related to specific security package implementations.

COURSE TITLE: Auditing MVS in a RACF™ Environment (M2026)
COURSE LENGTH: 1.5 DAYS

VENDOR:

Skill Dynamics - An IBM Company
One IBM Plaza, 19th Floor
Chicago, IL 60611
(800) IBM-TEACh (800) 426-8322

This course teaches you the necessity for the implementation of effective controls in the MVS operating system with a RACF environment. You will learn how to apply the controls provided within a RACF system to problems discussed in MVS Security (Course Code M2002) and MVS Auditing (Course Code M2024). You will also learn how to use RACF security and audit tools to better understand the protection of your system. Hands-on labs will utilize RACF tools to ascertain the current security status of an MVS system.

*RACF is a trademark of the IBM Corporation

COURSE TITLE: MVS/ESA™-RACF™ Security Topics (H3918)
COURSE LENGTH: 2.5 DAYS

VENDOR:

Skill Dynamics - An IBM Company
One IBM Plaza, 19th Floor
Chicago, IL 60611
(800) IBM-TEACh (800) 426-8322

This course teaches you the new security facilities that are available, beginning with MVS/SP 3.1.3 and RACF 1.9. You will learn which of your installation's security needs may be satisfied by using the new security facilities. You will learn to select, plan for, and implement the new security features. Subjects include controlling job unit, SYSOUT, NJE, commands and consoles, using security labels, restructuring the RACF data base, and developing an implementation plan.

*MVS/ESA and RACF are trademarks of the IBM Corporation

COURSE TITLE: MVS Security (M2002)
COURSE LENGTH: 3.5 DAYS

VENDOR:

Skill Dynamics - An IBM Company
One IBM Plaza - 19th Floor
Chicago, IL 60611
(800) IBM-TEACh (800) 426-8322

This course teaches you the necessity for and the implementation of effective controls in the MVS operating system. You will learn the MVS security-sensitive areas and the associated system and business impact of exposures in these areas. You will learn the proper use and implementation of controls to reduce security risks. Through hands-on use of the MVS system functions, you will gain valuable experience in maintaining effective and consistent system security. Although this course does not address the implementation of any specific security program (RACF™, CA-TOP SECRET™, etc.) the topics discussed will apply to MVS environments in general.

*CA-TOP SECRET is a trademark of Computers Associates, Inc.

COURSE TITLE: Practical Approach to Auditing MVS Security
COURSE LENGTH: 1 DAY

VENDOR:
the Henderson Group
6101 Wynnwood Road
Bethesda, MD 20816
(301) 228-7187

MVS security (the security provided by IBM's Multiple Virtual System operating system) provides the basis for all other security on MVS mainframes, including VTAM, DB2, CICS, RACF, ACF2, and TopSecret. This means that understanding the material in this course will be critical to your providing effective security in your installation. The course provides auditors, security administrators, and anyone interested in managing MVS security effectively with an understanding of hardware and software controls used by MVS to provide the foundation for computer security. The workbook provides forms and checklists for data collection and analysis, and is also a useful reference to MVS controls.

UNIX

COURSE TITLE: Audit and Security of Unix-Based Operating Systems
COURSE LENGTH: 3 DAYS

VENDOR:
MIS Training Institute
498 Concord Street
Framingham, MA 01701-2357
Sharon G. Friedman: (508) 872-7999

This three-day seminar identifies the weaknesses of Unix-based operating systems and shows you how to detect and prevent unauthorized access to such systems. You will examine Unix loopholes and discover successful techniques for plugging them. Along with Unix System V, you will explore the security features and vulnerabilities of such Unix-based operating systems as SUN O/S, AIX. HP-UX, ULTRIX, SCO-UNIX, and BERKELEY Unix. You will leave this session with the know-how to set up, manage, and maintain an enforceable Unix security policy, and with a tried-and-true audit approach for securing Unix-based operating systems.

COURSE TITLE: Unix Workshop
COURSE LENGTH: 2 DAYS

VENDOR:
MIS Training Institute
498 Concord Street
Framingham, MA 01701-2357
Sharon G. Friedman: (508) 872-7990

In this interactive workshop you will apply security and control concepts to a Unix Lan case study. You will reinforce what you learned in the Audit and Security of Unix-Based Operating Systems seminar as you proceed through a comprehensive Unix system audit and application access review. In addition, you will learn how to read and write shell scripts to expedite the review process and to read and write shell scripts to expedite the review process and to enhance system security monitoring. NOTE: Participants in this workshop have attended Audit and Security of Unix-Based Operating Systems or have equivalent on-the-job experience.

COURSE TITLE: SECO3-U: Unix Security
COURSE LENGTH: 2 DAYS

VENDOR:
Grumman Data Systems
2411 Dulles Corner Park, Suite 500
Herndon, VA 22071
Bruce Levy: (703) 713-4121

Objectives of the Course: Give Security Officers the ability to control and monitor the security of a Unix system. Specifically they will learn to use Unix security related commands to establish access control and monitor security related activities.

Specific topics include discussion of security concepts and management (i.e. security for users, programmers and super-user administrators), security auditing, network security, control of groups, users and their passwords, the management of password expirations, restricted environments, adding and deleting users and file systems, data integrity, viruses and compromises, hints and common mistakes.

COURSE TITLE: UNIX/AIX™ Security (M2012)
COURSE LENGTH: 3 DAYS

VENDOR:

Skill Dynamics - An IBM Company
One IBM Plaza, 19th Floor
Chicago, IL 60611
(800) IBM-TEACh (800) 426-8322

This course teaches you how to use the fundamental and essential security controls within the UNIX or AIX operating system. You will discover the tools available with the environment to identify security vulnerabilities. The discussion will detail the necessary precautions to take through initial system setup and ongoing administration. The focus will be on reducing the inherent exposures in UNIX, without removing the benefits of an open environment. Hands-on experience in identifying and closing exposures will guide you in safeguarding your own systems from loss and damage.

*UNIX is a trademark of UNIX Systems Laboratories

COURSE TITLE: UNIX Systems Security
COURSE LENGTH: 3 DAY

VENDOR:
Trainix
1686 Bismark Drive
Deltona, FL 32723
(800) 538-9271

This course discusses UNIX security and how system managers and administrators can implement security measures on UNIX. The focus of the course is on the inherent security vulnerabilities commonly found on UNIX systems and how to correct them. Examples are presented which illustrate how to insure a high level of security confidence against unauthorized users from accessing the system. The common methods used to penetrate UNIX systems, gain unauthorized root access permission, become another user, plant trojan horses or spoofs, and other ways of circumventing the normal system protection are disclosed. Each attendee will receive detailed audit checklists and a diskette containing UNIX shell and C programs which will assist in performing security auditing and risk analysis. Prerequisites: UX001-Fundamentals of UNIX and UX006-UNIX System Administration. A knowledge of Shell and C programming is helpful.

COURSE TITLE: UNIX Security For Users
COURSE LENGTH: 1 DAY

VENDOR:
Trainix
1686 Bismark Drive
Deltona, FL 32723
(800) 538-9271

This seminar is designed to make all users aware of the UNIX security vulnerabilities and show them how to prevent an unauthorized user from compromising their login account or data. The security features which are provided as part of the operating system are first discussed. Then, some of the ways in which unauthorized people may use to gain access to a UNIX system or another users files and directories are discussed. Next, the ways of preventing unauthorized access are described in detail, along with exact descriptions of each UNIX command and the way it is used. Each attendee will be provided with a self-assessment checklist and sample programs which will allow them to perform a personal audit on their account. The seminar concludes with a discussion of the actions a user should take if they suspect compromise of their login and/or files.

COURSE TITLE: Auditing UNIX
COURSE LENGTH:

VENDOR:
Canaudit Inc.
P.O. Box 4150
Simi Valley, CA 93093
(805) 583-3723

This seminar will walk you through the UNIX operating system, describe the functions and control features and provide a step by step audit approach complete with detailed audit programs and checklists. This seminar focuses on the two main versions of UNIX, System V and the Berkeley Software Distribution (BSD). The course material includes the control features of both systems and provides control guidelines for each. At the end of the seminar the participants will be ready for their first UNIX audit. Limited after class telephone support is available to assist participants when they do the audit. In addition, Canaudit staff are available to perform on site audit assistance at reasonable rates. Participants should attend the EDP Audit Workshop of Information Systems Workshop prior to attending this seminar.

COURSE TITLE: UNIX Security
COURSE LENGTH: 4 DAYS

VENDOR:
George Mason University
Department of Information & Software Systems Engineering
School of Information Technology and Engineering
Fairfax, VA 22030-4444
Ravi Sandhu: (703) 993-1659

UNIX is intended to be an easy-to-use system with great flexibility-this makes protection of UNIX systems difficult. The tutorial is focused on UNIX in general, rather than any particular vendor's implementation, with many vendor-specific items provided throughout. Included are tips and techniques drawn from the instructor's years of experience as a UNIX system administrator, incident investigator, security researcher, professor and consultant. Both BSD and System V versions of UNIX are covered in the material.

This course will start with the very basics about UNIX security, including some common threats, what to monitor in the file system, standard but little-known tools and resources, how to secure NFS/NIS, and how to deal with denial-of-service attacks. More advanced topics include policy formation, firewalls, Kerberos, X Window system security, some legal implications, and how to write your own setuid/setgid programs. The course provides tutorials in UNIX tools for the system administrator. these include using the Korn shell (ksh), the Awk scripting language, the sed stream editor, and the Perl programming language. Modern security tools like COPS and Tripwire, are discussed as well as customizing local monitoring tools.

COURSE TITLE: UNIX Security Seminar
COURSE LENGTH: 2 DAYS

VENDOR:
ARCA
Commerce Center
10320 Little Patuxent Parkway
Suite 1005
Columbia, MD 21044
(410) 715-0500

In this seminar participants will learn how to identify security weaknesses in UNIX systems and how to implement measures to increase security. This session details the basic principles of UNIX security, including basic concepts, available security features and how capabilities vary in UNIX systems. Current threats and vulnerabilities are covered as well as what makes some UNIX applications more secure than others and what increases applications security. Individuals will also learn how to detect and respond to UNIX security incidents by participating in a security incident simulation.

NOVELL

COURSE TITLE: Audit and Security of Novell
COURSE LENGTH: 3 DAYS

VENDOR:
MIS Training Institute
498 Concord Street
Framingham, MA 01701-2357
Sharon G. Friedman: (508) 872-7999

NetWare V.4's decentralized database, NetWare Directory Services (NDS), globally controls all users , servers, and resources. Because NDS establishes security privileges across all servers and provides a centralized login point to the network, building and implementing it to reflect your organizational structure is critical. In this three-day crash course you will learn how to implement V.4 so that access can be assigned based on functional positions. You will identify which controls are critical to provide effective data and access integrity, and learn new approaches for monitoring the network. You will examine the audit trail system that allows you to review network activity. At the end of this session you will have built the framework for a controlled enterprise network/

To get the most out of this course, participants should have a good understanding of personal computing, and DOS operating system, commands, and batch language. Participants should first attend Audit and Security of Micros and LANS; Controlling End-User Computing and/or Introduction to LAN Security.

COURSE TITLE: Novell™ NetWare™ Security (M2000)
COURSE LENGTH: 3.5 DAYS

VENDOR:

Skill Dynamics - An IBM Company
One IBM Plaza, 19th Floor
Chicago, IL 60611
(800) IBM-TEACh (800) 426-8322

This course teaches you how to plan for and maintain effective protection with a NetWare LAN operating system. You will learn the essentials of implementing basic security controls. In addition, you will learn the requirements for ensuring an adequate level of access restrictions within the environment. Discover the security pitfalls and often overlooked issues within a NetWare environment. These sometimes complex issues are taken to their simplest level and developed into a comprehensive understanding of the technical security requirements. Hands-on labs and classroom exercises illustrate the proper techniques to isolate security controls and to improve the overall security within the NetWare environment. While learning how to use system utilities, like SYSCON, you will explore the ways in which you can uncover security vulnerabilities within your LAN.

*Netware and Novell are trademarks of Novell, Inc.

COURSE TITLE: Guide To Auditing Novell Networks V.3
COURSE LENGTH: 3 DAY

VENDOR:
MIS Training Institute
498 Concord Street
Framingham, MA 01701
(508) 879-7999

Local area networks, and Novell in particular, offer enormous productivity gains to organizations. Unfortunately, along with the benefits, come unique and complex security and control risks. If you are a computer auditor who now must audit networks, this course is for you. In this session you will gain a thorough understanding of basic networking concepts. You will learn the exposures and control concepts within Novell NetWare, the associated environmental control concerns, and the organizational and procedural issues which affect the integrity of networked LANs. The course will detail the specific access control facilities critical to the LAN implementation and administration. You will come away from this course with a framework for determining the auditability of a Novell LAN implementation, and with a foundation for building a LAN audit work program. Participants should have a good understanding of personal computing, the DOS operating system and DOS commands, and the DOS batch language.

COURSE TITLE: Hands-On-Lans: Auditing Novell Networks Workshop
COURSE LENGTH:

VENDOR:
Canaudit Inc.
P.O. Box 4150
Simi Valley, CA 93093
(805) 583-3723

This hands-on workshop provides participants with a detailed understanding of the Novell operating system, the security features and how to audit them. The Canaudit audit approach, complete with audit programs and comprehensive checklists, will provide participants with a sound starting point for conducting their first audit. The hands-on exercises provide the practice which auditors require to understand the necessary audit procedures and techniques.

Canaudit also provides a Novell LAN (release 3.11), consisting of five micro computers for use in this class at no additional cost. The instructor will bring the LAN to your site and set it up prior to the course. Alternately, the instructor is also prepared to use the client's LAN if it is more appropriate to do so.

For client's with Blind View, the instructor is prepared to demonstrate how to audit a Novell LAN using this product and how to use Blind View reports to reduce the total time required to perform the audit.

TANDEM

COURSE TITLE: Audit and Security of Tandem Systems
COURSE LENGTH: 2 DAYS

VENDOR:
Canaudit Inc.
P.O. Box 4150
Simi Valley, CA 93093
(805) 583-3723

This two day seminar will enable participants to perform a complex review of security features provided by the Tandem operating system and Safeguard security product. The instructor explains normal control weaknesses and potential security loopholes in depth. commands and utilities used to probe the system and detect control weaknesses are explained. A program for reviewing system security is also provided. We recommend that auditors attend the Information Systems Workshop or EDP Audit Workshop seminars, or their equivalents, prior to attending this session.

DECNET

COURSE TITLE: Auditing Decnet
COURSE LENGTH: 2 DAY

VENDOR:
Canaudit Inc.
P.O. Box 4150
Simi Valley, CA 93093
(805) 583-3723

Many Canaudit clients use the DEC VAX as an integral part of extensive network applications. It is essential that these applications be secure and that communications be safe and confidential. this seminar is specifically designed for Canaudit clients using DECnet, the primary communications architecture for Digital networks. Complete coverage of all aspects of DECnet security including network implementations, Network Control Program and network access control methodologies is included in this concentrated seminar. All participants will learn the critical control features of DECnet and how to evaluate the control structure. In addition they will receive complete audit programs and utilities to automate much of the audit. NOTE:AUDITING VAX:A COMPREHENSIVE APPROACH is the prerequisite for this course.

VAX

COURSE TITLE: Auditing VAX: A Comprehensive Approach
COURSE LENGTH: 3 DAY

VENDOR:
Canaudit Inc.
P.O. Box 4150
Simi Valley, CA 93093
(805) 583-3723

This session is the most comprehensive VAX Audit course currently available. It is intended for auditors who will be auditing the VAX operating system and its components. The seminar provides participants with an understanding of the hardware, software and security requirements as well as depth, along with detailed descriptions of utilities and System Generation controls. Because of the popularity of this topic, we recommend early registration. NOTE:We recommend that participants attend the AUDITING ADVANCED INFORMATION TECHNOLOGY or EDP AUDIT WORKSHOP seminars or their equivalents prior to attending this course.

COURSE TITLE: Introduction to DEC's VAX/VMS Operating System
COURSE LENGTH: 2 DAY

VENDOR:
MIS Training Institute
498 Concord Street
Framingham, MA 01701
(508) 879-7999

This course provides a thorough introduction to VAX/VMS from the perspective of audit and security personnel who need access to the systems-dependent facilities of VAX/VMS. Through case examples you will see demonstrated the major features of VAX/VMS, including DCL, utilities, and analysis of the system. This session is guaranteed to give you a basic knowledge of the VMS operating system and a comfort level in moving around it. The facilities, tools and techniques taught during these two days will dramatically increase your understanding of and productivity in the VMS environment. NOTE: ADVANCED COURSE AS A FOLLOW-ON ALSO AVAILABLE.

COURSE TITLE: Advanced Audit, Control, and Security/ DEC's VAX/VMS
COURSE LENGTH: 3 DAY

VENDOR:
MIS Training Institute
498 Concord Street
Framingham, MA 01701
(508) 879-7999

This advanced seminar builds on the concepts and facilities presented in "Introduction to DEC's VAX/VMS Operating System" and focuses on the critical points to consider when auditing VAX/VMS systems and applications. You will come away with a detailed understanding of the VAX/VMS architecture, DCL commands, Digital's Network Architecture (DNA), and VAX built-in and optional security features. Emphasis will be placed on important areas for audit concentration within VMS such as systems generation, systems dump analyzer, VMS protection and privilege levels, systems and user logs, and DECnet and LAN interfaces. Those attending should have experience in the VAX/VMS environment, or should have attended "Introduction to DEC's VAX/VMS Operating System."

AS/400

COURSE TITLE: AS/400™ Recovery and Availability Management (S6051)
COURSE LENGTH: 2 DAYS

VENDOR:

Skill Dynamics - An IBM Company
One IBM Plaza, 19th Floor
Chicago, IL 60611
(800) IBM-TEACh (800) 426-8322

This classroom course explains how to plan for, implement, and manage the back-up and recovery functions of the AS/400 system. In this course, the student also learns how to perform tasks like implementing recovery functions and practice these skill sin hands-on labs.

*AS/400 is a trademark of the IBM Corporation

COURSE TITLE: AS/400™ Security Concepts and Implementations (S6050)
COURSE LENGTH: 2 DAYS

VENDOR:

Skill Dynamics - An IBM Company
One IBM Plaza, 19th Floor
Chicago, IL 60611
(800) IBM-TEACh (800) 426-8322

This classroom course explains how to plan for, implement, and manage the security and back-up and recover functions of the AS/400 system. This course also provides and introduction to problem determination and PTF application. You will learn how to perform tasks like creating security profiles and user environments, in addition to implementing recover functions. These skills are practiced in hands-on labs.

*AS/400 is a trademark of the IBM Corporation

COURSE TITLE: Audit, Control, and Security Of AS/400
COURSE LENGTH: 4 DAY

VENDOR:
MIS Training Institute
498 Concord Street
Framingham, MA 01701
(508) 879-7999

In this seminar you will learn about the architecture, security and integrity of AS/400, and about the system's unique object-oriented design and integrated data base management system (DBMS). You will examine the impact of on-line systems on the control objectives within an EDP environment in general, and the security-related concerns and control objectives specific to AS/400. You will leave the seminar with a methodology and techniques for testing and reviewing AS/400.

COURSE TITLE: Auditing AS/400: A Step By Step Approach
COURSE LENGTH: 2 DAY

VENDOR:
Canaudit Inc.
P.O. Box 4150
Simi Valley, CA 93093
(805) 583-3723

IBM's AS/400 computer series is rapidly becoming the work horse of the mini and midi computer world. With a broad industry base, this multi functional machine serves as a primary business platform, as a front end processor or as a process controller. This intensive seminar concentrates on the control and security concerns relating to the AS/400. The participants will learn how to automate the audit using ROBOT, utilities and AS/400 tools. Key control points are identified to enable auditors to focus their efforts to ensure a complete audit while reducing the audit duration. Actual case studies are used throughout the seminar to provide real life examples to reinforce the audit programs and techniques.

CA-ACF2

COURSE TITLE: Converting CA-ACF2™ to RACF™ (H3891)
COURSE LENGTH: 2 DAYS

VENDOR:

Skill Dynamics - An IBM Company
One IBM Plaza, 19th Floor
Chicago, IL 60611
(800) IBM-TEACh (800) 426-8322

This course teaches you how to effectively plan and perform a CA-ACF2 to RACF conversion for an MVS system. The course material is divided into three major topics: project management issues, converting the CA-ACF2 database to FACF, and interfacing other products to RACF. The discussion on database conversion includes how to us a conversion tool, with examples and sample output from a commonly-used migration aid.

*CA-ACF2 is a trademark of Computer Associates, Inc.
*RACF is a trademark of the IBM Corporation

COURSE TITLE: CA-ACF2: Proper Implementation and Security
COURSE LENGTH: 3 DAY

VENDOR:
MIS Training Institute
498 Concord Street
Framingham, MA 01701
(508) 879-7999

This intensive seminar has been updated to cover the newest features in Release 5.2, including the new GROUP feature and major changes to the CA-ACF2/CICS interface. In this in-depth session you will master the terms and concepts you need to know in order to understand how CA-ACF2 protects files and other resources in your MVS environment. You will discover all of the important testing tools available in this security package, and how to use them effectively. In addition, you will learn how to anticipate the deficiencies most commonly found in CA-ACF2 implementation and administration. You will leave this intensive session with tips for demonstrating risks and for selling common-sense recommendations that have proven track records for working. The course materials you receive will include an in-depth audit program and valuable sample reports. NOTE: A CONTINUING 2-DAY WORKSHOP IS AVAILABLE.

CA-TOP SECRET

COURSE TITLE: Converting from CA-TOP SECRET™ to RACF™ (H3890)
COURSE LENGTH: 2 DAYS

VENDOR:

Skill Dynamics - An IBM Company
One IBM Plaza, 19th Floor
Chicago, IL 60611
(800) IBM-TEACh (800) 426-8322

This course teaches you how to effectively plan and perform a CA-TOP SECRET to RACF conversion for an MVS system. The course material is divided into three major topics: project management issues, converting the CA-TOP SECRET database to RACF, and interfacing other products to RACF. The discussion on database conversion includes how to use a conversion tool, with examples and sample output from a commonly-used IBM migration aid.

*CA-TOP SECRET is a trademark of Computers Associates, Inc.
*RACF is a trademark of the IBM Corporation

COURSE TITLE: CA-TOP Secret: Proper Implementation and Security
COURSE LENGTH: 3 DAY

VENDOR:
MIS Training Institute
498 Concord Street
Framingham, MA 01701
(508) 879-7999

In this seminar you will learn the functions and components of TOP SECRET and the auditor tools within TOP SECRET to monitor the effective installation and on-going functions of the security system. You will learn all the important features of TOP SECRET and their relationship to the MVS operating system. The workshop covers the audit trails produced by the system and describes how these reports can be used as an effective detective control for monitoring both authorized and unauthorized access to system resources. Participants should first attend OS/MVS Operating System:Security and Audit. NOTE: A 2-DAY WORKSHOP IS ALSO AVAILABLE.

SNA

COURSE TITLE: Security & Auditing of SNA Networks/ACF/VTAM & NCP
COURSE LENGTH: 3 DAY

VENDOR:
MIS Training Institute
498 Concord Street
Framingham, MA 01701
(508) 879-7999

This comprehensive seminar presents the concepts, terminology, components, functions, access points, and use of SNA (System Network Architecture) networks. It provides the technical information necessary to ensure that appropriate controls are implemented and are being used. With the information you gain from this seminar you can enhance the integrity, control, and reliability of data transfers within SNA environments and to/from SNA networks. You will learn standard techniques and optional enhancements for implementing and maintaining proven audit and control procedures for SNA systems. The seminar covers IBM's environments. Practical audit and control issues to be addressed include; present and new communications controllers, protocol emulators, Netview and Netview/PC, front end hardware and software, terminal systems, and SNA network management programs. NOTE: A 2-DAY WORKSHOP IS ALSO AVAILABLE.

CICS/ESA

COURSE TITLE: Implementing Security for CICS™ Using RACF™ (H4001)
COURSE LENGTH: 3 DAYS

VENDOR:

Skill Dynamics - An IBM Company
One IBM Plaza, 19th Floor
Chicago, IL 60611
(800) IBM-TEACh (800) 426-8322

This lab course teaches you how to implement security in CICS/ESA V3™ and CICS/MVS V2™ using RACF™ as the external security manager. In the classroom you will learn both the CICS and RACF definitions necessary to establish your security environment. You will learn how to define CICS terminal users to RACF, control access to transactions, CICS resources, SPI commands, and installation-defined resources. This course covers security in both single-region and multi-region CICS systems (MRO and ISC). You will perform hands-on lab exercises that let you apply your new skills to actually set-up these definitions in both CICS and RACF. Also, we will discuss the security interface between CICS, RACF, and DB2. Additionally, we will discuss the RACF and CICS definitions necessary for secure access to CICS/ESA™ from other platforms via APPC.

*CICS, CICS/ESA, RACF, CICS/MVS are trademarks of the IBM Corporation

COURSE TITLE: Audit, Control and Security of CICS/ESA
COURSE LENGTH: 5 DAY

VENDOR:
MIS Training Institute
498 Concord Street
Framingham, MA 01701
(508) 879-7999

Telecommunications technology has created a whole new set of concerns regarding the control and auditability of on-line systems. This seminar will show you how to identify the available control and security features within CICS. You will learn how to audit CICS systems to insure those control measures are functioning properly. Participants should first attend "OS/MVS Operating System: Security and Audit." NOTE: A 2-DAY WORKSHOP IS ALSO AVAILABLE.

COURSE TITLE: MVS/ESA Disaster Recovery (J3716)
COURSE LENGTH: 2.5 DAYS

VENDOR:

Skill Dynamics - An IBM Company
One IBM Plaza, 19th Floor
Chicago, IL 60611
(800) IBM-TEACh (800) 426-8322

This course enables you to confront the issues of contingency planning and disaster recovery as they affect your MVS/ESA system. You will explore technical and procedural issues that cover a range of topics, including backup and recovery options, problem management within a disaster recovery environment, and automating backup and recovery procedures. Recommendations are provided for selecting critical applications and data for backup. By studying examples, you'll gain insight into techniques you can use to backup, recover, and synchronize system and application elements, including:

- Catalogs
- System libraries and data sets
- System parameters (e.g., PARMLIB, JES2, VTAMLIST, etc.)
- Job streams and procedures
- IOCP/MVSCP
- DFHSM control data
- Applications and application data

COURSE TITLE: Audit/Security Concepts-MVS/XA & MVS/ESA
COURSE LENGTH: 5 DAY

VENDOR:
MIS Training Institute
498 Concord Street
Framingham, MA 01701
(508) 879-7999

While attending this program you will develop your technical understanding of the MVS/XA and MVS/ESA operating system and gain the skills you need to successfully review any MVS installation. This session presents a foolproof methodology for conducting a successful MVS operating system review. You will apply this methodology for reviewing an installation and develop the steps for a complete audit program. NOTE: Participants should have attended OS/MVS Operating System: Security and Audit Facilities or have technical experience in the MVS environment, including familiarity with TSO or the use of IBM utilities.

COURSE TITLE: Enterprise Systems Analysis for MVS/ESA & MVS/XA
COURSE LENGTH: 4 DAY

VENDOR:
MIS Training Institute
498 Concord Street
Framingham, MA 01701
(508) 879-7999

This seminar address the external and internal workings of the MVS/XA and MVS/ESA operating systems, focusing on security and control aspects. This seminar will answer questions and fill in those technical areas you need to understand in order to perform more effective and detailed MVS reviews. NOTE: Participants should have attended "Audit and Security Concepts for the MVS Operating System" and completed one or more MVS reviews. Participants are requested to bring to the session technical data or code extracted from their own MVS installation.

MAXSIX

COURSE TITLE: MaxSix Trusted Networking
COURSE LENGTH: 1 Day

VENDOR:
Trusted Systems Training, Inc.
1107 South Orchard Street
Urbana, IL 61801-4851
Steve Sutton: (217) 344-0996

The course addresses network security administrators and programmers for Compartmented Mode Workstations based on the SecureWare technology, including SecureWare's CMW+, Hewlett-Packard's BLS, and Digital's MLS+. It teaches the secure use of all new networking security features, like setting up and installing the network security databases, and attribute mapping. (These topics are presented as a part of TST's other courses, but are also offered as this 1-day seminar.)

SAFEware

COURSE TITLE: SAFE = Security Awareness from Education
COURSE LENGTH:

VENDOR:
SAFEware
2953 Timber Wood Way
Herndon, VA 22071
Kyle Myers: (703) 758-8777

SAFE is not a course, it is an ongoing program. All presentations are animated, full color PC-based graphic shows or may be viewed in the VHS video format. [SAFE (in Q3 or 1993 will add full interactivity, hypertext and hotwords.] After being viewed just once, users immediately implement many of the points made because 1) they are common sense and users only need to see them once, 2) they are so easy to implement and 3) the user understands "what's in it for me" to become involved.

All of the presentation can be viewed with or without user intervention, constantly viewed in cafeterias and lobbies where the specific policies and practices of your organization may be presented in detail. These presentations are selected from the Windows launcher or the DOS menu.

SAFE is a comprehensive, coordinated PC-based security education and awareness program for commercial and federal users of PCthrough mainframe computers. SAFE recruits users to be involved in security--all of the time, educates users about common sense security issues, and reminds users to be security conscious on a daily basis.

BANYAN VINES

COURSE TITLE: Audit and Security of Banyan VINES
COURSE LENGTH: 3 DAYS

VENDOR:
MIS Training Institute
498 Concord Street
Framingham, MA 01701-2357
Sharon G. Friedman: (508) 872-7999

This seminar will provide you with a practical guide to auditing the VINES operating system and the applications running under it. You will learn the technical fundamentals of VINES as well as exposures and control concepts specific to VINES and to networking. You will learn recommended procedures for protecting the integrity of LANs and VINES specifically. You will cover the access control facilities critical to implementing and administering VINES networks, and witness a demonstration of a VINES server and workstation. You will return to your office with guidelines for ensuring that systems running under the VINES operating environment are auditable, and with a checklist you can use to conduct an audit or security review of your VINES.

COURSE TITLE: Security for Banyan VINES LANs
COURSE LENGTH: 1 DAY

VENDOR:
RSH Consulting, Inc.
29 Caroline Park
Newton, MA 02168
Bob Hansel: (617) 969-9050

This workshop provides basic information about the security features and capabilities of a Banyan VINES 5.x local area network. We will begin with an introduction to the VINES Network Operating System and its component services, such as Server Service, File Services, and VINES Security Service. We will also discuss the directory service StreetTalk and its role in security. Thereafter, user identification and authentication controls including Group and User Login parameters. Next, we will address resource access control, focusing on Access Rights Lists and console security. We follow this with a discussion on controls over WAN network links. Finally, we will address security administration and monitoring. this workshop will conclude with a discussion of tools and techniques for reviewing security in a VINES network.

VM

COURSE TITLE: SECO2-V: VM Security for Project Managers
COURSE LENGTH: 2 DAYS

VENDOR:
Grumman Data Systems
2411 Dulles Corner Park, Suite 500
Herndon, VA 22071
Bruce Levy: (703) 713-4121

Objectives of the Course: Give Project Managers the ability to manage and control access to data and userid resources on a VM system. Specifically they will learn to write appropriate security procedures for a VM system with ACF2 and VMSECURE, implement ACF2 security rules, and monitor compliance with security procedures.

Specific topics include discussion of the VM system structure, an overview of ACF2 features and capabilities, ACF2 databases, logon-id and minidisk access rules, ACF2 and VM SECURE commands and subcommands, VM user directory attributes, planning, writing, compiling, changing and testing ACF2 rules and testing procedures.

COURSE TITLE: SECO3-V: VM Security for Security Officers
COURSE LENGTH: 1 DAY

VENDOR:
Grumman Data Systems
2411 Dulles Corner Park, Suite 500
Herndon, VA 22071
Bruce Levy: (703) 713-4121

Objectives of the Course: Give Security Officers the ability to control and monitor the security of a VM system. Specifically they will learn to write appropriate security procedures for a VM system using ACF2, use ACF2 commands to establish security rules, establish and change system-wide ACF2 characteristics, and monitor compliance with security procedures.

Specific topics include discussion of security policies, directives and procedures, how they are created and implemented, the characteristics of VM and how DASD is used in a VM system, ACF2 databases logon-id, dataset access rules, resource access rules, ACF2 commands and reports, setting system-wide ACF2 specifications, VM records and defaults, and testing procedures.

PBX

COURSE TITLE: A Three Day Emergency Session on PBX Fraud
COURSE LENGTH: 2 DAYS

VENDOR:
MIS Training Institute
498 Concord Street
Framingham, MA 01701-2357
(508) 872-7999

In this two-day, crash briefing you will learn how to protect your organization against high-priced, high-tech PBX fraud. You will explore the world of phone hackers and discover how fraud and theft of services begins. You will look at the economic impact on and legal liability of your organization if it is "hit," and the responsibilities of your local/long distance carriers and federal law enforcement agencies. You will address the hardware and programming issues that must be taken into account to ensure that your network, PBX, voice mail, and automated attendant and adjunct processors are protected. You will leave this eye-opening session armed and ready to fight back when phone phreaks try to invade your PBX. NOTE: This course assumes that participants will have basic knowledge of phone systems and the telecommunications environment.

IBM

COURSE TITLE: IBM LAN Server: Audit and Security
COURSE LENGTH: 3 DAYS

VENDOR:
MIS Training Institute
498 Concord Street
Framingham, MA 01701-2357
Sharon G. Friedman: (508) 872-7999

This intensive, three-day seminar will provide you with a technical understanding of IBM and LAN Server and a practical guide to auditing it. You will discover the audit and control mechanisms built into LAN server. You will uncover LAN Server's inherent exposures and learn techniques that will provide a reliable, secure network environment for your organization. Topics covered include: the specific access control facilities that should be a part of your day-to-day security measures; how to provide network, server, and user security; how to enable specific auditing features; how to generate audit reports; and how to work around LAN Server's shortcomings. You will leave this session with an audit and security features in your own organization. NOTE: Seminar participants should have a working knowledge of DOS or OS/2 operating environments and understand PC architecture.

It is our intention to update this document as the need arises and we welcome any comments and corrections that will yield a better product. Please contact Kathie Everhart (301) 975-3868.

APPENDIX A

APPENDIX A
MAJOR CATAGORIES

COMPUTER SECURITY BASICS
EXECUTIVES

COURSE TITLE	PAGE
ADP Security Officers (ADPSO) Concepts	2
Computer Security Awareness (CBT)	7
Computer Security Awareness Training	3
Computer Security Executive Overview	1
Computer Security For End Users	2
Computer Security For Executives	3
Computer Security Awareness (CBT)	8
EDP Concepts For Business	6
Federal AIS Computer Security Requirements	4
Information Risk Assessment & Security Management	4
Information Systems Seminar For Internal Auditors	4
Microcomputer Security	7
Telecommunications for Information Systems Security Analysts	1

SECURITY PLANNING & MANAGEMENT
EXECUTIVES

COURSE TITLE **PAGE**

SECURITY PLANNING & MANAGEMENT
EXECUTIVES

COURSE TITLE	PAGE
ADP Security Officers (ADPSO) Concepts	2
Continuity of Operations/Disaster Recovery Planning: Part I	8
EDP Concepts For Business	6
Executive AIS Security Briefing	8
Federal AIS Computer Security Requirements	4
Information Systems Seminar For Internal Auditors	4
Information Risk Assessment & Security Management	3
Marketplace Implications of the Evolution of Evaluation Criteria	7
Telecommunications for Information Systems Security Analysts	1
The Systems Integrator's Perspective on AIS Security Strategies	8

COMPUTER SECURITY POLICY & PROCEDURES
EXECUTIVES

COURSE TITLE	PAGE
ADP Security Officers (ADPSO) Concepts	2
EDP Concepts For Business	6
Executive AIS Security Briefing	8
Federal AIS Computer Security Requirements	4
Information Systems Seminar For Internal Auditors	4
Information Risk Assessment & Security Management	3
Keeping Out of Trouble with the Software Police	9
Microcomputer Security	7

CONTINGENCY PLANNING
EXECUTIVES

SYSTEMS LIFE CYCLE MANAGEMENT
EXECUTIVES

COMPUTER SECURITY BASICS
PROGRAM & FUNCTIONAL MANAGERS

SECURITY PLANNING & MANAGEMENT
PROGRAM & FUNCTIONAL MANAGERS

COMPUTER SECURITY POLICY & PROCEDURES
PROGRAM & FUNCTIONAL MANAGERS

CONTINGENCY PLANNING
PROGRAM & FUNCTIONAL MANAGERS

SYSTEMS LIFE CYCLE MANAGEMENT
PROGRAM & FUNCTIONAL MANAGERS

COMPUTER SECURITY BASICS
IRM, SECURITY, & AUDIT

SECURITY PLANNING & MANAGEMENT
IRM, SECURITY, & AUDIT

Federal AIS Computer Security Requirements	4
Implementing & Managing a Computer Security Program	19
Information Security Principles and Practice	17
Information Systems Seminar For Internal Auditors	4
Information Risk Assessment & Security Management	3
INFOSEC	44
Integrated Auditing: The Basics	42
Microcomputer Security	62
Physical Security for Data Processing	31
Protecting Networks & Small Systems	29
Protecting Your Networks from Hackers, Viruses, and Other Attacks	23
Recent Developments in Information Security	25
Risk Assessment	19
Risk Management	25
Security Technology in the Real World	45
The CMW: Administrator Tutorial	61
Writing Security Plans	26

COMPUTER SECURITY POLICY & PROCEDURES
IRM, SECURITY, & AUDIT

CONTINGENCY PLANNING
IRM, SECURITY, & AUDIT

SYSTEMS LIFE CYCLE MANAGEMENT
IRM, SECURITY, & AUDIT

COMPUTER SECURITY BASICS
ADP MANAGEMENT AND OPERATIONS

SECURITY PLANNING AND MANAGEMENT
ADP MANAGEMENT AND OPERATIONS

COMPUTER SECURITY POLICY AND PROCEDURES
ADP MANAGEMENT AND OPERATIONS

CONTINGENCY PLANNING
ADP MANAGEMENT AND OPERATIONS

SYSTEMS LIFE CYCLE MANAGEMENT
ADP MANAGEMENT AND OPERATIONS

<u>COURSE TITLE</u> <u>PAGE</u>

COMPUTER SECURITY BASICS
END USERS

SECURITY PLANNING AND MANAGEMENT
END USERS

COMPUTER SECURITY POLICY AND PROCEDURES
END USERS

COURSE TITLE	PAGE
Audit and Control of End-user Computing (EUC)	40
Auditing Information Systems	41
Computer Security: For Security and MIS Professionals	43
Computer Security & Contingency Planning	51
EDP Concepts For Business	6
Information Systems Seminar For Internal Auditors	4
Integrated Auditing: The Basics	42
LAN Security	90
Microcomputer Security	7
TEMPEST Program Management and Systems Engineering	81
The CMW: User Tutorial	90

CONTINGENCY PLANNING
END USERS

SYSTEMS LIFE CYCLE MANAGEMENT
END USERS

APPENDIX B

APPENDEX B
VENDOR LIST

VENDOR NAME

Anne Arundel Community College
Page(s): 81

ARCA
Page(s): 53, 54, 64, 65, 66, 71, 84, 108

Booz-Allen & Hamilton Inc.
Page(s): 7, 19, 26, 34, 89

California State Polytechnic, Univ, Pomona
Page(s): 78, 79

Canaudit Inc
Page(s): 45, 47, 48, 49, 50, 51, 52, 56, 96, 107, 111, 112, 113, 117

CENTER for Adv. Professional Develop
Page(s): 69

Computer Security Institute
Page(s): 27, 28, 29, 33, 53, 61, 62, 66, 67, 82, 83

COMSIS
Page(s): 4, 8, 19, 28, 30, 31, 80

DATAPRO Educational Services
Page(s): 1, 9, 35, 90

Disaster Recovery Institute
Page(s): 85, 86, 87, 88

DPEC
Page(s): 7

Ernst & Young
Page(s): 4, 6

George Mason University
Page(s): 17, 25, 107

George Washington University/GSAS
Page(s): 32

APPENDIX C

APPENCIX C
PRODUCT LIST

APPENDIX D

APPENDIX D
PRODUCT SPECIFIC COURSES

APPENDIX E

TRAINING MATRIX

Training Area Audience Category	COMPUTER SECURITY BASICS	SECURITY PLANNING & MGMT.	COMPUTER SECURITY POLICY & PROCEDURES	CONTINGENCY PLANNING	SYSTEMS LIFE CYCLE MGMT.
EXECUTIVES	░	▦	░	░	░
PROGRAM & FUNCTIONAL MANAGERS	░	▤	▤	▨	▨
IRM, SECURITY, AND AUDIT	░	▨	▨	▨	▨
ADP MANAGEMENT AND OPERATIONS	░	▨	▨	▨	▨
END USERS	░	░	▨	▨	░

KEY: TRAINING LEVEL

AWARENESS	░
POLICY	▦
IMPLEMENTATION	▤
PERFORMANCE	▨