Module 1: IT Auditing, Governance and Business Continuity

Module 1.1: IT Auditing

- Questions to be addressed in module 1.1 include:
  - What are the scope and objectives of audit work, and what major steps take place in the audit process?
  - What are the objectives of an information systems audit, and what is the four-step approach for meeting those objectives?
  - How can a plan be designed to study and evaluate internal controls in an AIS?
  - How can computer audit software be useful in the audit of an AIS?

THE NATURE OF AUDITING

- Auditors used to audit around the computer and ignore the computer and programs.
  - Assumption: If output was correctly obtained from system input, then processing must be reliable.
- Current approach: Audit through the computer.
  - Uses the computer to check adequacy of system controls, data, and output.
  - SAS-94 requires that external auditors evaluate how audit strategy is affected by an organization’s use of IT.
  - Also states that auditors may need specialized skills to:
    - Determine how the audit will be affected by IT.
    - Assess and evaluate IT controls.
    - Design and perform both tests of IT controls and substantive tests.

THE NATURE OF AUDITING

- The internal auditor’s responsibilities include:
  - Review the reliability and integrity of operating and financial information and how it is identified, measured, classified, and reported.
  - Determine if the systems designed to comply with these policies, plans, procedures, laws, and regulations are being followed.
  - Review how assets are safeguarded, and verify their existence.
  - Examine company resources to determine how effectively and efficiently they are used.
  - Review company operations and programs to determine if they are being carried out as planned and if they are meeting their objectives.

THE NATURE OF AUDITING

- Types of Internal Auditing Work
  - Three different types of audits are commonly performed.
    - Financial audit
    - Information systems audit
    - Operational or management audit

THE NATURE OF AUDITING

- An Overview of the Auditing Process
  - All audits follow a similar sequence of activities and may be divided into four stages:
    - Planning
    - Collecting evidence
    - Evaluating evidence
    - Communicating audit results
THE NATURE OF AUDITING

• Audit Planning
  – Purpose: Determine why, how, when, and by whom the audit will be performed.
  – The first step in audit planning is to establish the scope and objectives of the audit.
  – An audit team with the necessary experience and expertise is formed.
  – Team members become familiar with the auditee by:
    • Conferring with supervisory and operating personnel;
    • Reviewing system documentation; and
    • Reviewing findings of prior audits.

• Collection of Audit Evidence
  – Much audit effort is spent collecting evidence.

• Evaluation of Audit Evidence
  – The auditor evaluates the evidence gathered in light of the specific audit objective and decides if it supports a favorable or unfavorable conclusion.
  – If inconclusive, the auditor plans and executes additional procedures until sufficient evidence is obtained.
  – Two important factors when deciding how much audit work is necessary and in evaluating audit evidence are:
    • Materiality
    • Reasonable assurance

• Communication of audit results
  – The auditor prepares a written (and sometimes oral) report summarizing audit findings and recommendations, with references to supporting evidence in the working papers.
  – Report is presented to:
    • Management
    • The audit committee
    • The board of directors
    • Other appropriate parties
  – After results are communicated, auditors often perform a follow-up study to see if recommendations have been implemented.

THE NATURE OF AUDITING

• The audit should be planned so that the greatest amount of audit work focuses on areas with the highest risk factors.
• There are three types of risk when conducting an audit:
  – Inherent risk
  – Control risk
  – Detection risk
THE NATURE OF AUDITING

• The Risk-Based Audit Approach
  – A risk-based audit approach is a four-step approach to internal control evaluation that provides a logical framework for carrying out an audit. Steps are:
    • Determine the threats (errors and irregularities) facing the AIS.
    • Identify control procedures implemented to minimize each threat by preventing or detecting such errors and irregularities.
    • Evaluate the control procedures.
    • Evaluate weaknesses (errors and irregularities not covered by control procedures) to determine their effect on the nature, timing, or extent of auditing procedures and client suggestions.

INFORMATION SYSTEMS AUDITS

• The purpose of an information systems audit is to review and evaluate the internal controls that protect the system.
• When performing an information system audit, auditors should ascertain that the following objectives are met:
  – Security provisions protect computer equipment, programs, communications, and data from unauthorized access, modification, or destruction.
  – Program development and acquisition are performed in accordance with management’s general and specific authorization.
  – Program modifications have management’s authorization and approval.

OBJECTIVE 1: OVERALL SECURITY

• Types of security errors and fraud faced by companies:
  – Accidental or intentional damage to system assets.
  – Unauthorized access, disclosure, or modification of data and programs.
  – Theft.
  – Interruption of crucial business activities.

OBJECTIVE 2: PROGRAM DEVELOPMENT AND ACQUISITION

• Types of errors and fraud:
  – Two things can go wrong in program development:
    • Inadvertent errors due to careless programming or misunderstanding specifications; or
    • Deliberate insertion of unauthorized instructions into the programs.
OBJECTIVE 2: PROGRAM DEVELOPMENT AND ACQUISITION

• Control procedures:
  – The preceding problems can be controlled by requiring:
    • Management and user authorization and approval
    • Thorough testing
    • Proper documentation

OBJECTIVE 3: PROGRAM MODIFICATION

• Control Procedures
  – When a program change is submitted for approval, a list of all required updates should be compiled by management and program users.
  – Changes should be thoroughly tested and documented.
  – During the change process, the developmental version of the program must be kept separate from the production version.
  – When the amended program has received final approval, it should replace the production version.
  – Changes should be implemented by personnel independent of users or programmers.
  – Logical access controls should be employed at all times.

OBJECTIVE 3: PROGRAM MODIFICATION

– To test for unauthorized program changes, auditors can use a source code comparison program to compare the current version of the program with the original source code.
  • Any unauthorized differences should result in an investigation.
  • If the difference represents an authorized change, the auditor can refer to the program change specifications to ensure that the changes were authorized and correctly incorporated.

OBJECTIVE 3: PROGRAM MODIFICATION

– Two additional techniques detect unauthorized program changes:
  • Reprocessing
    – On a surprise basis, the auditor uses a verified copy of the source code to reprocess data and compare that output with the company’s data.
    – Discrepancies are investigated.
  • Parallel simulation
    – Similar to reprocessing except that the auditor writes his own program instead of using verified source code.
    – Can be used to test a program during the implementation process.

OBJECTIVE 4: COMPUTER PROCESSING

• Processing Test Data
  – Involves testing a program by processing a hypothetical series of valid and invalid transactions.
  – The program should:
    • Process all the valid transactions correctly.
    • Identify and reject the invalid ones.
  – All logic paths should be checked for proper functioning by one or more test transactions, including:
    • Records with missing data
    • Fields containing unreasonably large amounts
    • Invalid account numbers or processing codes
    • Non-numeric data in numeric fields
    • Records out of sequence

OBJECTIVE 4: COMPUTER PROCESSING

• The following resources are helpful when preparing test data:
  – A listing of actual transactions
  – The transactions that the programmer used to test the program
  – A test data generator program, which automatically prepares test data based on program specifications
OBJECTIVE 4: COMPUTER PROCESSING

• Concurrent audit techniques
  – Millions of dollars of transactions can be processed in an online system without leaving a satisfactory audit trail.
  – In such cases, evidence gathered after data processing is insufficient for audit purposes.
  – Also, because many online systems process transactions continuously, it is difficult or impossible to stop the system to perform audit tests.
  – Consequently, auditors use concurrent audit techniques to continually monitor the system and collect audit evidence while live data are processed during regular operating hours.

OBJECTIVE 4: COMPUTER PROCESSING

• Concurrent audit techniques use embedded audit modules.
  – These are segments of program code that:
    • Perform audit functions;
    • Report test results to the auditor; and
    • Store collected evidence for auditor review.
  – Are time-consuming and difficult to use, but less so if incorporated when programs are developed.

OBJECTIVE 4: COMPUTER PROCESSING

• An ITF technique places a small set of fictitious records in the master files:
  – May represent a fictitious division, department, office, customer, or supplier.
  – Processing test transactions to update these dummy records will not affect actual records.
  – Because real and fictitious transactions are processed together, company employees don’t know the testing is taking place.

OBJECTIVE 4: COMPUTER PROCESSING

• The snapshot technique examines the way transactions are processed.
  – Selected transactions are marked with a special code that triggers the snapshot process.
  – Audit modules in the program record these transactions and their master file records before and after processing.
  – The selected data are recorded in a special file and reviewed by the auditor to verify that all processing steps were properly executed.

OBJECTIVE 4: COMPUTER PROCESSING

• The system control audit review file (SCARF) uses embedded audit modules to continuously monitor transaction activity and collect data on transactions with special audit significance.
  • Data recorded in a SCARF file or audit log include transactions that:
    – Exceed a specified dollar limit;
    – Involve inactive accounts;
    – Deviate from company policy; or
    – Contain write-downs of asset values.
  • Periodically the auditor:
    – Receives a printout of SCARF transactions;
    – Looks for questionable transactions among them; and
    – Investigates.

• Audit hooks are audit routines that flag suspicious transactions.
  • Example: State Farm Life Insurance looking for policyholders who change their name or address and then subsequently withdraw funds.
  • When audit hooks are used, auditors can be informed of questionable transactions as they occur via real-time notification, which displays a message on the auditor’s terminal.
OBJECTIVE 4: COMPUTER PROCESSING

• Continuous and intermittent simulation (CIS) embeds an audit module in a database management system.
• The module examines all transactions that update the DBMS using criteria similar to those of SCARF.
• When a transaction has audit significance, the module:
  – Processes the data independently (similar to parallel simulation);
  – Records the results;
  – Compares results with those obtained by the DBMS.
• If there are discrepancies, details are written to an audit log for subsequent investigation.
• Serious discrepancies may prevent the DBMS from executing the update.

OBJECTIVE 4: COMPUTER PROCESSING

• The following software packages can help:
  – Automated flowcharting programs
  – Automated decision table programs
  – Scanning routines
  – Mapping programs
  – Program tracing

OBJECTIVE 5: SOURCE DATA

• Audit Procedures: Tests of Controls
  – Observe and evaluate data control department operations and specific data control procedures
  – Verify proper maintenance and use of data control log
  – Evaluate how items recorded in the error log are handled
  – Examine samples of accounting source data for proper authorization
  – Reconcile a sample of batch totals and follow up on discrepancies
  – Trace disposition of a sample of errors flagged by data edit routines

OBJECTIVE 5: SOURCE DATA

• Auditors should ensure the data control function:
  – Is independent of other functions
  – Maintains a data control log
  – Handles errors
  – Ensures overall efficiency of operations
• Usually not feasible for small businesses and PC installations to have an independent data control function.
OBJECTIVE 5: SOURCE DATA

- To compensate, user department controls must be stronger over:
  - Data preparation
  - Batch control totals
  - Edit programs
  - Physical and logical access restrictions
  - Error handling procedures
- These procedures should be the focus of the auditor’s systems review and tests of controls when there is no independent data control function.

OBJECTIVE 6: DATA FILES

- The sixth objective concerns the accuracy, integrity, and security of data stored in machine-readable files.
- Data storage risks include:
  - Unauthorized modification of data
  - Destruction of data
  - Disclosure of data
- Many of the controls discussed in Chapter 8 protect against the preceding risks.
- If file controls are seriously deficient, especially with respect to access or backup and recovery, the auditor should strongly recommend they be rectified.

OBJECTIVE 6: DATA FILES

- Auditing-by-objectives is a comprehensive, systematic, and effective means of evaluating internal controls in an AIS.
  - Can be implemented using an audit procedures checklist for each objective.
  - Should help the auditor reach a separate conclusion for each objective and suggest compensating controls.
- A separate version of the checklist should be completed for each significant application.

COMPUTER SOFTWARE

- Computer audit software (CAS) or generalized audit software (GAS) are computer programs that have been written especially for auditors.
- Two of the most popular:
  - Audit Control Language (ACL)
  - IDEA
- Based on auditor’s specifications, CAS generates programs that perform the audit function.
- CAS is ideally suited for examination of large data files to identify records needing further audit scrutiny.

COMPUTER SOFTWARE

- CAS functions include:
  - Reformattting
  - File manipulation
  - Calculation
  - Data selection
  - Data analysis
  - File processing
  - Statistics
  - Report generation
OPERATIONAL AUDITS OF AN AIS

- Techniques and procedures in operational audits are similar to audits of information systems and financial statement audits.
- The scope is different.
  - IS audit scope is confined to internal controls
  - Financial audit scope is limited to system output
  - Operational audit scope is much broader and encompasses all aspects of information systems management.
- Objectives are also different in that operational audit objectives include evaluating factors such as:
  - Effectiveness
  - Efficiency
  - Goal achievement

1.2.A: Computer Fraud and Abuse Act of 1986

- Federal regulation, USC Title 18, Section 1030
- Updates to USC title 18
  - National Information Infrastructure Protection Act of 1996
  - Homeland Security Act of 2002

Computer Fraud and Abuse Act

- Criminalizes intentional access of protected computers without authorization or in excess of authorization (Hacking)
- Criminalizes the transmission of a program, information, code, or command that intentionally causes damage without authorization of a protected computer (Denial-of-Service and Viruses)
- Punishment
  - For first offenses, usually 1-5 years; usually 10 years for second offenses
  - For theft of sensitive government information, 10 years, with 20 years for repeat offense
  - For attacks that harm or kill people, up to life in prison

Electronic Communications Privacy Act of 1986 (ECMA)

- U.S. C., Title 47
- Also referring as Federal Wiretapping Act
- Regulates interception and disclosure of electronic information

Digital Millennium Copyright Act (DMCA) of 1998

- Addresses copyright related issues
- Makes the following things illegal
  - Remove or alter copyright management information from digital copies of copyrighted works
  - Bypass technical measures used by copyright owners to protect their works
  - Manufacture or distribute technologies primarily designed to circumvent technical measures used by copyright owners to protect their works

Module 1.2: IT Governance

- A. Laws Governing Hacking and Other Computer Crimes
- B. Corporate Auditing
- C. Governance Frameworks
- D. Risk Analysis
Laws Around the World Vary

• The general situation: lack of solid laws in many countries
• Cybercrime Treaty of 2001
  – Signatories must agree to create computer abuse laws and copyright protection
  – Nations must agree to work together to prosecute attackers

1.2.B: Compliance Laws and Regulations

• Compliance laws and regulations create requirements for corporate security
  – Documentation requirements are strong
  – Identity management requirements tend to be strong
• Compliance can be expensive
• There are many compliance laws and regulations, and the number is increasing rapidly

The Sarbanes-Oxley Act of 2002 (1)

• Makes internal controls a legal requirement
• Affects corporate governance, financial disclosure and the practice of public accounting
• To restore the public’s confidence in corporate governance by making chief executives of publicly traded companies personally validate financial statements and other information
  – After Enron/Worldcom
• http://www.aicpa.org/sarbanes/index.asp

The Sarbanes-Oxley Act of 2002 (2)

• Section 404 of the Sarbanes-Oxley Act mandates that all public organizations
  – demonstrate due diligence in the disclosure of financial information and
  – implement a series of internal controls and procedures to communicate, store and protect that data.
• Public organizations are also required under Section 404 to protect these controls from internal and external threats and unauthorized access, including those that could occur through online systems and networks
• Publicly traded companies need to file SOX reports to SEC
• Need to be certified by external auditors

Privacy Protection Laws (1)

• The European Union (E.U.) Data Protection Directive of 2002
• Many other nations have strong commercial data privacy laws
• The U.S. Gramm–Leach–Bliley Act (GLBA)
• The U.S. Health Information Portability and Accountability Act (HIPAA) for private data in health care organizations

Privacy Protection Laws (2)

- Data Breach Notification Laws
  - California’s SB 1386
  - Requires notification of any California citizen whose private information is exposed
  - Companies cannot hide data breaches anymore
- Federal Trade Commission (FTC)
  - Can punish companies that fail to protect private information
  - Fines and required external auditing for several years
### PCI-DSS
- Payment Card Industry–Data Security Standards
- Applies to all firms that accept credit cards
- Has 12 general requirements, each with specific subrequirements

### FISMA
- Federal Information Security Management Act of 2002
- Processes for all information systems used or operated by a U.S. government federal agencies
- Also by any contractor or other organization on behalf of a U.S. government agency
- Certification, followed by accreditation
- Continuous monitoring
- Criticized for focusing on documentation instead of protection

### 1.2.C: Governance Frameworks

### COSO - Background
- **Origins**
  - Committee of Sponsoring Organizations of the Treadway Commission (www.coso.org)
  - Ad hoc group to provide guidance on financial controls
- **Focus**
  - Corporate operations, financial controls, and compliance
  - Effectively required for Sarbanes-Oxley compliance
  - Goal is reasonable assurance that goals will be met

### COSO Components
- Control Environment
  - General security culture
  - Includes "tone at the top"
  - If strong, specific controls may be effective
  - If weak, strong controls may fail
  - Major insight of COSO
- Risk assessment
  - Ongoing preoccupation
- Control activities
  - General policy plus specific procedures
- Monitoring
  - Both human vigilance and technology
  - Information and communication
  - Must ensure that the company has the right information for controls
  - Must ensure communication across all levels in the corporation

### Enterprise Risk Management (COSO)
- Intent of ERM is to achieve all goals of the internal control framework and help the organization:
  - Provide reasonable assurance that company objectives and goals are achieved and problems and surprises are minimized.
  - Achieve its financial and performance targets.
  - Assess risks continuously and identify steps to take and resources to allocate to overcome or mitigate risk.
  - Avoid adverse publicity and damage to the entity’s reputation.
CONTROL FRAMEWORKS

• Basic principles behind ERM:
  – Companies are formed to create value for owners.
  – Management must decide how much uncertainty they will accept.
  – Uncertainty can result in:
    • Risk
    • Opportunity

• ERM Framework Vs. the Internal Control Framework
  – The internal control framework has been widely adopted as the principal way to evaluate internal controls as required by SOX. However, there are issues with it.
    • It has too narrow of a focus.
    • Focusing on controls first has an inherent bias toward past problems and concerns.

• These issues led to COSO’s development of the ERM framework.
  – Takes a risk-based, rather than controls-based, approach to the organization.
  – Oriented toward future and constant change.
  – Incorporates rather than replaces COSO’s internal control framework and contains three additional elements:
    • Setting objectives.
    • Identifying positive and negative events that may affect the company’s ability to implement strategy and achieve objectives.
    • Developing a response to assessed risk.

• The ERM model is three-dimensional.
• Means that each of the eight risk and control elements are applied to the four objectives in the entire company and/or one of its subunits.

CONTROL FRAMEWORKS

– Controls are flexible and relevant because they are linked to current organizational objectives.
– ERM also recognizes more options than simply controlling risk, which include accepting it, avoiding it, diversifying it, sharing it, or transferring it.

INTERNAL ENVIRONMENT

• The most critical component of the ERM and the internal control framework.
• Is the foundation on which the other seven components rest.
• Influences how organizations:
  – Establish strategies and objectives
  – Structure business activities
  – Identify, access, and respond to risk
• A deficient internal control environment often results in risk management and control breakdowns.
**INTERNAL ENVIRONMENT**

- Internal environment consists of the following:
  - Management's philosophy, operating style, and risk appetite
  - The board of directors
  - Commitment to integrity, ethical values, and competence
  - Organizational structure
  - Methods of assigning authority and responsibility
  - Human resource standards
  - External influences

**INTERNAL ENVIRONMENT**

- The following policies and procedures are important:
  - Hiring
  - Compensating
  - Training
  - Evaluating and promoting
  - Discharging
  - Managing disgruntled employees
  - Vacations and rotation of duties
  - Confidentiality insurance and fidelity bonds

**OBJECTIVE SETTING**

- Objective setting is the second ERM component.
- It must precede many of the other six components.
- For example, you must set objectives before you can define events that affect your ability to achieve objectives

**OBJECTIVE SETTING**

- Objective-setting process proceeds as follows:
  - First, set strategic objectives, the high-level goals that support the company's mission and create value for shareholders.
  - To meet these objectives, identify alternative ways of accomplishing them.
  - For each alternative, identify and assess risks and implications.
  - Formulate a corporate strategy.
  - Then set operations, compliance, and reporting objectives.

**EVENT IDENTIFICATION**

- Events are:
  - Incidents or occurrences that emanate from internal or external sources
  - That affect implementation of strategy or achievement of objectives.
  - Impact can be positive, negative, or both.
  - Events can range from obvious to obscure.
  - Effects can range from inconsequential to highly significant.

**EVENT IDENTIFICATION**

- By their nature, events represent uncertainty:
  - Will they occur?
  - If so, when?
  - And what will the impact be?
  - Will they trigger another event?
  - Will they happen individually or concurrently?
EVENT IDENTIFICATION

- Management must do its best to anticipate all possible events—positive or negative—that might affect the company:
  - Try to determine which are most and least likely.
  - Understand the interrelationships of events.
- COSO identified many internal and external factors that could influence events and affect a company’s ability to implement strategy and achieve objectives.

EVENT IDENTIFICATION

- Some of these factors include:
  - External factors:
    - Economic factors
    - Natural environment
    - Political factors
    - Social factors
    - Technological factors

EVENT IDENTIFICATION

- Some of these factors include:
  - Internal factors:
    - Infrastructure
    - Personnel
    - Process
    - Technology

EVENT IDENTIFICATION

- Companies usually use two or more of the following techniques together to identify events:
  - Use comprehensive lists of potential events
  - Perform an internal analysis
  - Monitor leading events and trigger points
  - Conduct workshops and interviews
  - Perform data mining and analysis
  - Analyze processes

RISK ASSESSMENT AND RISK RESPONSE

- The fourth and fifth components of COSO’s ERM model are risk assessment and risk response.
- COSO indicates there are two types of risk:
  - Inherent risk

RISK ASSESSMENT AND RISK RESPONSE

- The fourth and fifth components of COSO’s ERM model are risk assessment and risk response.
- COSO indicates there are two types of risk:
  - Inherent risk
  - Residual risk
RISK ASSESSMENT AND RISK RESPONSE

- Companies should:
  - Assess inherent risk
  - Develop a response
  - Then assess residual risk
- The ERM model indicates four ways to respond to risk:
  - Reduce it
  - Accept it
  - Share it
  - Avoid it

RISK ASSESSMENT AND RISK RESPONSE

- Risks that are not reduced must be accepted, shared, or avoided.
  - If the risk is within the company’s risk tolerance, they will typically accept the risk.
  - A reduce or share response is used to bring residual risk into an acceptable risk tolerance range.
  - An avoid response is typically only used when there is no way to cost-effectively bring risk into an acceptable risk tolerance range.

CONTROL ACTIVITIES

- Generally, control procedures fall into one of the following categories:
  - Proper authorization of transactions and activities
  - Segregation of duties
  - Project development and acquisition controls
  - Change management controls
  - Design and use of documents and records
  - Safeguard assets, records, and data
  - Independent checks on performance

CONTROL ACTIVITIES

- The following independent checks are typically used:
  - Top-level reviews
  - Analytical reviews
  - Reconciliation of independently maintained sets of records
  - Comparison of actual quantities with recorded amounts
  - Double-entry accounting
  - Independent review

INFORMATION AND COMMUNICATION

- The seventh component of COSO’s ERM model.
- The primary purpose of the AIS is to gather, record, process, store, summarize, and communicate information about an organization.
- So accountants must understand how:
  - Transactions are initiated
  - Data are captured in or converted to machine-readable form
  - Computer files are accessed and updated
  - Data are processed
  - Information is reported to internal and external parties
• According to the AICPA, an AIS has five primary objectives:
  – Identify and record all valid transactions.
  – Properly classify transactions.
  – Record transactions at their proper monetary value.
  – Record transactions in the proper accounting period.
  – Properly present transactions and related disclosures in the financial statements.

• The eighth component of COSO’s ERM model.
  Monitoring can be accomplished with a series of ongoing events or by separate evaluations.

• Key methods of monitoring performance include:
  – Perform ERM evaluation
  – Implement effective supervision
  – Use responsibility accounting
  – Monitor system activities
  – Track purchased software
  – Conduct periodic audits
  – Employ a computer security officer and security consultants
    – Engage forensic specialists
  – Install fraud detection software
  – Implement a fraud hotline

• Control Objectives for Information and Related Technologies
• CIO-level guidance on IT governance
• Offers many documents that help organizations understand how to implement the framework

The CobiT Framework
– Four major domains
  1. Planning and Organization
  2. Acquisition and Implementation
  3. Delivery and Support
  4. Monitoring

• Four major domains (Figure 2-26)
• 34 high-level control objectives
  – Planning and organization (11)
  – Acquisition and implementation (60)
  – Delivery and support (13)
  – Monitoring (4)
• More than 300 detailed control objectives
CobiT

- Dominance in the United States
  - Created by the IT governance institute
  - Which is part of the Information Systems Audit and Control Association (ISACA)
  - ISACA is the main professional accrediting body of IT auditing
  - Certified information systems auditor (CISA) certification

The ISO/IEC 27000 Family of Security Standards

- ISO/IEC 27000
  - Family of IT security standards with several individual standards
  - From the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC)

- ISO/IEC 27002
  - Originally called ISO/IEC 17799
  - Recommendations in 11 broad areas of security management

The ISO/IEC 27000 Family of Security Standards

- ISO/IEC 27002: Eleven Broad Areas

<table>
<thead>
<tr>
<th>Security Policy</th>
<th>Access Control</th>
</tr>
</thead>
<tbody>
<tr>
<td>Organization of information security</td>
<td>Information systems acquisition, development and maintenance</td>
</tr>
<tr>
<td>Asset management</td>
<td>Information security incident management</td>
</tr>
<tr>
<td>Human resources security</td>
<td>Business continuity management</td>
</tr>
<tr>
<td>Physical and environmental security</td>
<td>Compliance</td>
</tr>
<tr>
<td>Communications and operations management</td>
<td></td>
</tr>
</tbody>
</table>

1.2.D: Risk Analysis

- Asset Value (AV)
  - Percentage loss in asset value if a compromise occurs

- X Exposure Factor (EF)
  - Annual probability of a compromise

- Single Loss Expectancy (SLE)
  - Expected loss in case of a compromise

- Annualized Loss Expectancy (ALE)
  - Expected loss per year from this type of compromise

<table>
<thead>
<tr>
<th>SLE</th>
<th>X Annualized Rate of Occurrence (ARO)</th>
</tr>
</thead>
<tbody>
<tr>
<td>$100,000</td>
<td>$100,000</td>
</tr>
</tbody>
</table>

- Annualized Rate of Occurrence (ARO)
  - Annual probability of a compromise

<table>
<thead>
<tr>
<th>Single Loss Expectancy (SLE)</th>
<th>Annualized Loss Expectancy (ALE)</th>
</tr>
</thead>
<tbody>
<tr>
<td>$80,000</td>
<td>$20,000</td>
</tr>
</tbody>
</table>

- Annualized Loss Expectancy (ALE)
  - Expected loss per year from this type of compromise

<table>
<thead>
<tr>
<th>Annualized Loss Expectancy (ALE)</th>
<th>Annualized Net Countermeasure Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>$40,000</td>
<td>$30,000</td>
</tr>
</tbody>
</table>

- Annualized Net Countermeasure Value
  - Expected loss per year from this type of compromise

<table>
<thead>
<tr>
<th>Countermeasure Cost</th>
<th>Annualized Net Countermeasure Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>$17,000</td>
<td>$13,000</td>
</tr>
</tbody>
</table>

- Countermeasure A should reduce the exposure factor by 75%
Problems with Classic Risk Analysis Calculations

• Uneven Multiyear Cash Flows
  – For both attack costs and defense costs
  – Must compute the return on investment (ROI) using discounted cash flows
  – Net present value (NPV) or internal rate of return (ROI)

• Many-to-Many Relationships between Countermeasures and Resources
  – Classic risk analysis assumes that one countermeasure protects one resource
  – Single countermeasures, such as a firewall, often protect many resources
  – Single resources, such as data on a server, are often protected by multiple countermeasures
  – Extending classic risk analysis is difficult

Problems with Classic Risk Analysis Calculations

• Impossibility of Knowing the Annualized Rate of Occurrence
  – There simply is no way to estimate this
  – This is the worst problem with classic risk analysis
  – As a consequence, firms often merely rate their resources by risk level
Problems with Classic Risk Analysis Calculations

- **Problems with “Hard-Headed Thinking”**
  - Security benefits are difficult to quantify
  - If only support “hard numbers” may underinvest in security

- **Perspective**
  - Impossible to do perfectly
  - Must be done as well as possible
  - Identifies key considerations
  - Works if countermeasure value is very large or very negative
  - But never take classic risk analysis seriously

---

2-16: Responding to Risk

- **Risk Reduction**
  - The approach most people consider
  - Install countermeasures to reduce harm
  - Makes sense only if risk analysis justifies the countermeasure

- **Risk Acceptance**
  - If protecting against a loss would be too expensive, accept losses when they occur
  - Good for small, unlikely losses
  - Good for large but rare losses

- **Risk Transference**
  - Buy insurance against security-related losses
  - Especially good for rare but extremely damaging attacks
  - Does not mean a company can avoid working on IT security
  - If bad security, will not be insurable
  - With better security, will pay lower premiums

- **Risk Avoidance**
  - Not to take a risky action
  - Lose the benefits of the action
  - May cause anger against IT security

- **Recap: Four Choices when You Face Risk**
  - Risk reduction
  - Risk acceptance
  - Risk transference
  - Risk avoidance

---

Module 1.3: Business Continuity Process

- The basic principle of BCP is to protect people first
  - Evacuation plans and drills
  - Never allow staff members back into unsafe environments
  - Must have a systematic way to account for all employees and notify loved ones
  - Counseling afterwards
Principles of Business Continuity Management

- People have reduced capacity in decision making during a crisis
  - Planning and rehearsal are critical
- Avoid rigidity
  - Unexpected situations will arise
  - Communication will break down and information will be unreliable
  - Decision makers must have the flexibility to act

Business Process Analysis

- Identification of business processes and their interrelationships
- Prioritization of business processes
  - Downtime tolerance
    (in the extreme, mean time to belly-up)
  - Importance to the firm
  - Required by higher-importance processes
- Resource needs (must be shifted during crises)
  - Cannot restore all business processes immediately

Business Continuity Planning

- Testing the Plan
  - Difficult because of the scope of disasters
  - Difficult because of the number of people involved
- Updating the Plan
  - Must be updated frequently
  - Business conditions change and businesses reorganize constantly
  - People who must execute the plan also change jobs constantly
  - Telephone numbers and other contact information must be updated far more frequently than the plan as a whole
  - Should have a small permanent staff

Business Continuity versus Disaster Response

IT Disaster Recovery

- IT Disaster Recovery
  - IT disaster recovery looks specifically at the technical aspects of how a company can get its IT back into operation using backup facilities
  - A subset of business continuity or for disasters that only affect IT
  - All decisions are business decisions and should not be made by mere IT or IT security staffs
Types of Backup Facilities
- Hot sites
  - Ready to run (power, HVAC, computers): Just add data
  - Considerations: Rapid readiness at high cost
  - Must be careful to have the software at the hot site up-to-date in terms of configuration
- Cold sites
  - Building facilities, power, HVAC, communication to outside world only
  - No computer equipment
  - Less expensive but usually take too long to get operating
- Site sharing
  - Site sharing among a firm's sites (problem of equipment compatibility and data synchronization)
  - Continuous data protection needed to allow rapid recovery

IT Disaster Recovery
- Office Computers
  - Hold much of a corporation's data and analysis capability
  - Will need new computers if old computers are destroyed or unavailable
    - Will need new software
    - Well-synchronized data backup is critical
  - People will need a place to work

IT Disaster Recovery
- Restoration of Data and Programs
  - Restoration from backup tapes: Need backup tapes at the remote recovery site
  - May be impossible during a disaster
- Testing the IT Disaster Recovery Plan
  - Difficult and expensive
  - Necessary

AVAILABILITY
- Key components of effective disaster recovery and business continuity plans include:
  - Data backup procedures
  - Provisions for access to replacement infrastructure (equipment, facilities, phone lines, etc.)
  - Thorough documentation
  - Periodic testing
  - Adequate insurance