Amity School of Business

Amity School of Business

BBA General, 2nd Semester

System Analysis and Design

Arpan Sinha

Module- VI

System Security & Auditing

Topics

- System Security: Data Security
  - Backup
  - Recovery during System
  - Database failure
- Ethical Issues in System Development
- Threat and Risk Analysis
- Audit
  - System Audit
  - System Audit Standards (Planning, Implantation and Reporting Standards)
- System Analysis and Programming (Overview, Role & Duties of System Experts as Analyst and Programmer).

System Security

- The Protection of data or hardware against accidental or international damage from a defined threat.
- The system security problem can be divided into four related issues :
  - Security
  - Integrity
  - Privacy
  - confidentiality

- **System Security** refers to the technical innovation and procedures applied to the hardware and operating systems to protect against deliberating or accidental damage from a defined threat.
- **System Integrity** refers to the proper functioning of hardware and programs, appropriate physical security, and safety against external threats.
- **Privacy** defines the rights of the users or organizations to determine what information they are willing to share with or accept from others and how the organization can be protected against unwelcome, unfair excessive dissemination of information about it.
- **Confidentially** is a special status given to sensitive information in a database to minimize the possible invasion of privacy.

Data Security, Backup & Recovery

- **Data Security :-** Protection of data from loss, disclosure, modification, or destruction.
- **Backup & Recovery :-** Restoring a damage database is generally done by *rollforward* or rollback procedure.
  - The *rollforward* approach involves updating a prior valid copy of the data base with the necessary changes to produce a current version of database.
  - The rollback approach starts current invalid state and removes the record of activity to produce the prior valid state of the database. Either approach depends largely on the software to bring the backup copy up to date and determine the cause of failure.
- Backup can be extremely important in a recovery procedure. If database is physically damage, one could not rollback because of the damage database – only roll forward.

Database Failure

- In a database environment, there are three types of failures : **Catastrophic, logical, and structural**
- **Catastrophic failure** is one where part of a database is unreadable. It is restoring using rollforward method of recovery.
- A **logical failure** occurs when activity to the database is interrupted with no chance of completing the currently executing transaction.
- **Structural** damage is that when a pointer incorrectly stored in a record that points to unrelated or nonexistent data.

Ethical Issues In System Development

- Ethical behavior of the analysts and computer professionals has led to the development of standards and codes of behavior by a number of professional associations. Three association are worth mentioning :
  - Association for Computing Machinery (ACM)
  - Data Processing Management Association (DPMA)
  - Institute for Certificate of Computer Professional (ICCP)
- Ethics can be described as Fairness, Justice, Equity, Honesty, Trustworthiness, and equality.
- Stealing, cheating, lying or backing out of one's words all describe lack of Ethics.
- Code of Ethics: is a declaration of the principles and beliefs that govern how employees of an organization are expected to behave.

Threats & Risk Analysis

- Threat analysis improves our understanding of adversaries' organization, capabilities, operations, and support mechanisms and informs strategic planning and development of effective countermeasures.
- Risk analysis considers threat, vulnerability, and consequence of informed decision making.
- Risk management is a guiding principle of our nation's security strategy. Throughout our government at all levels, organizations must allocate scarce resources to minimize risks posed by a vast and diverse array of both man-made threats and natural challenges.

What is Audit ?

- Evaluation of a person, organization, system, process, project or product.
- An audit provides a baseline of the existing system from which new investment can be accurately planned, avoiding excessive or inappropriate expenditure.
- The goal of an audit is to express an opinion on the person/organization/system in question, under evaluation based on work done.

- Audit is performed by an AUDITOR
- There are two types of auditors –
  - Internal Auditor
  - External Auditor

1. ***Internal Auditors*** – Employees of the company hired to assess and evaluate its system of internal control. To maintain independence, they present their reports directly to the top level management.
2. ***External Auditors –*** Independent staff assigned by an auditing firm to assess and evaluate financial statements of their clients or to perform other agreed upon evaluations. They are called on from outside the company.

System Audit

- It is also called Process Audit: can be conducted for any activity. Usually made against a specific document such as operating procedure, work instruction, training manual, etc.
- A series of activities in which a system auditor, an impartial position independent of the object of audit, performs overall inspection and evaluation of an information system, issues advice and recommendations, and provides any necessary follow-up.

- System audits will help spot any errors in configuration which can leave vulnerabilities in the most secure products.
- Audits can help overcome 'rule-creep' as small system changes over time cumulatively produce a significant shift in overall system security.
- A policy audit will check that the security policies which management has communicated are being adhered to.

System Auditor

A person who engages in system audits with the following knowledge and abilities:

- Basic knowledge of information systems
- Knowledge of system audits
- Ability to perform system audits
- Related knowledge for the performance of system audits

System Audit Standard

- Purpose
- Definitions of Terms
- Composition of the Standards
- Philosophy behind the Implementation Standards
- General Standards
- Implementation Standards

System Audit Standard

- ***Purpose*** - The purpose of the Standards is to improve the reliability, security, and efficiency of information systems and thus contribute to the realization of a healthy information society by enumerating the matters necessary for system audits.

- ***Definitions of Terms***

These are the principal terms used in the Standards

i. ***System Audit :*** A series of activities in which a system auditor, an impartial position independent of the object of audit, performs overall inspection and evaluation of an information system, issues advice and recommendations, and provides any necessary follow-up.

ii. ***System Auditor :*** A person who engages in system audits with the following knowledge and abilities:

a. Basic knowledge of information systems.

b. Knowledge of system audits.

c. Ability to perform system audits.

d. Related knowledge for the performance of system audits.

iii. ***Improvement of reliability:*** To improve the quality of information systems, prevent failure, minimize the effects of failure, and speed up recovery.

iv. ***Improvement of security:*** To make an information system more secure from natural disasters, unauthorized access, and destructive actions.

v. ***Improvement of efficiency***: To improve the cost performance of an information system by making the most of its resources.

vi. ***Basic plan***: A general plan of system audits to be performed during any given year.

vii. ***Individual plan:*** A plan for any of the individual system audit operations based on a basic plan.

viii. ***Risk analysis:*** To identify the risks that may arise from or in connection with the use of an information system and analyze the degrees of their effects.

ix. ***Audited division***: A division that is an object of a system audit

x. ***Matter noted:*** A problem pointed out by a system auditor according to his or her criteria and noted on a system audit report.

xi. ***Recommendation of improvement:*** A matter noted that is judged by a system auditor as requiring improvement and noted as such on a system audit report

xii. ***Follow-up***: The measure or measures taken by a system auditor to ensure the audited division carries out any recommendations of improvement

Composition of the Standards

The Standards are composed of -

- General Standards
- Implementation Standards
- Reporting Standards

General Standards

General Standards outline the principles of an audit plan that provides a basis for a system audit, the qualifications of a system auditor, and so forth.

1. **System**

   The organization shall prepare a system for proper implementation of system audit

2. **Audit Plan**

   Preparation of a basic plan and individual plan for system audit.

3. **Responsibility and Authority of a system auditor**
   - The system auditor shall make the grounds for each of his or her judgments clear.
   - The system auditor may demand data and materials from the audited division.
   - The system auditor may demand a report on the implementation of improvement be issued by the head of an organization to an audited division.
4. **Professional Ethics**

   The system auditor shall firmly maintain his or her position as an impartial evaluator.

   The system auditor shall be aware of the ethical demands on himself or herself and meet the internal and external trust by performing an accurate and sincere system audit.

5. **Confidentiality**

   The system auditor must not divulge any secret he or she may come to know in the course of performing his or her job or use such secret for any undue purpose.

Implementation Standards

1. **Planning**
   - ✓ Information Strategy
   - ✓ Formulation of a General Plan
   - ✓ Formulation of a Development Plan
   - ✓ System Analysis and Definitions of Requirements
2. **Development**
   - ✓ Development Procedures
   - ✓ System Design
   - ✓ Program Design
   - ✓ Programming
   - ✓ System Tests
   - ✓ Conversion

3. **Operation**
   - ✓ Operation Control
   - ✓ Input Management
   - ✓ Data Management
   - ✓ Output Management
   - ✓ Software Management
   - ✓ Hardware Management
   - ✓ Network Management
   - ✓ Configuration Management
   - ✓ Management of Buildings and Related Facilities

4. **Maintenance**
   - ✓ Maintenance Procedures
   - ✓ Maintenance Plan
   - ✓ Implementation of Maintenance
   - ✓ Confirmation of Maintenance
   - ✓ System Conversion
   - ✓ Disposal of Old Systems

5. **Common Work**
   - ✓ Document Management
     - ✓ Preparation
     - ✓ Management
   - ✓ Progress Management
     - ✓ Implementation
     - ✓ Evaluation
   - ✓ Personnel Management
     - ✓ Responsibility and Authority
     - ✓ Implementation of Work
     - ✓ Education and Training
     - ✓ Health Management

- ✓ Outsourcing
  - ✓ Outsourcing plan
  - ✓ Selection of service providers
  - ✓ Service agreements
  - ✓ Contents of services
- ✓ Measures against Disasters
  - ✓ Risk Analysis
  - ✓ Anti-Disaster Plan
  - ✓ Backup
  - ✓ Alternative Processing and Recovery

Reporting Standards

1. Preparation of Reports
   - The system auditor must prepare a system audit report.
   - The system audit report must state the results of evaluation of the reliability, security, and efficiency of an information system.
   - The system audit report must state, as matters noted, the problems based on the results of the audit.
   - The system audit report must state, as recommendations of improvement, the important matters that need to be improved.
   - The system audit report must state improvements that can be proposed for the matters that need to be improved.
   - The system auditor must state on his or her system audit report any other matters he or she considers necessary.

2. Reporting - The system audit report must be submitted to the head of the organization.
3. Follow-up - The system auditor must try to grasp the progress of improvement made based on recommendations of improvement and promote that improvement.

System Analyst

The System Analyst designs and implements systems to suit the organization's needs. He plays a major role in seeking business benefits from computer technology. His job is not just confined to data processing, but also deals heavily with people, procedures and technology.

Skills of System Analyst

Interpersonal Skills – Communication, Understanding, Foresightedness and Vision, Adaptability, Flexibility, Teaching, Selling, Patience and Rationality, Sound Temperament, Managerial Skills, Leadership Skills, Training and Documentation Capability.

Technical Skills – Creativity, Problem Solving, Project Management, Dynamic Interface, Questioning Attitude and Inquiring mind, Knowledge.

7 Roles of a System Analyst

- Change Agent
- Investigator and Monitor
- Architect
- Psychologist
- Salesperson
- Motivator
- Politician

Change Agent

The system analyst may select various styles to introduce change to the user organization –

- Persuader (mildest form of intervention)
- Catalyst (helper)
- Confronter (severe)
- Imposer (the most severe form of intervention)

Investigator and Monitor

- To investigate why the present system does not work well and what changes will correct the problem.
- To undertake and successfully complete a project, the analyst must monitor programs in relation to time, cost, and quality. Time is the most important resource. If time is wasted, the project suffers from increased costs and wasted human resources.

Architect

- The architect's primary function as liaison between the client's abstract design requirements and the contractor's detailed building plan may be compared to the analyst's role as liaison between the user's logical design requirements and the detailed physical system design. As architect, the analyst also creates a detailed physical design of candidate systems. He aids users in formalizing abstract ideas and provides details to build the end product- the candidate system.

Psychologist

- The analyst plays the role of a psychologist in the way he reaches people, interprets their thoughts, assesses their behavior, and draws conclusions from these interactions. In other words, understanding inter-functional relationships is important.

Salesperson

- Selling change can be as crucial as initiating change. Selling the system actually takes place at each step in the system life cycle. However, Sales skills and persuasiveness are crucial to the success of the system.

Motivator

- A candidate system must be well designed and acceptable to the user. System acceptance is achieved through user participation in its development, effective user training, and proper motivation to use the system. The analyst's role as a motivator is obvious during the first few weeks after implementation and during time when turnover results in new people being trained to work with the candidate system.

Politician

- Related to the role of motivator is that of politician. In implementing a candidate system, the analyst tries to appease all parties involved. Diplomacy and finesse in dealing with people can improve acceptance of the system. As much as a politician must have the support of his/her constituency, so is the analyst's goal to have the support of the users' staff. He represents their thinking and tries to achieve their goals through computerization.

Thank You
&
All the best !