# BUILDING INFORMATION SYSTEMS SECURITY AND CONTROL

# OBJECTIVES

- Why are information systems so vulnerable to destruction, error, abuse, and system quality problems?
- What types of controls are available for information systems?
- What special measures must be taken to ensure the reliability, availability and security of electronic commerce and digital business processes?

# OBJECTIVES

- What are the most important software quality assurance techniques?
- Why are auditing information systems and safeguarding data quality so important?

## MANAGEMENT CHALLENGES

- Designing systems that are neither over-controlled nor under-controlled
- Applying quality assurance standards in large systems projects

## Why Systems are Vulnerable

- Advances in telecommunications and computer software
- Unauthorized access, abuse, or fraud
- Hackers
- Denial of service attack
- Computer viruses

## Telecommunication Network Vulnerabilities

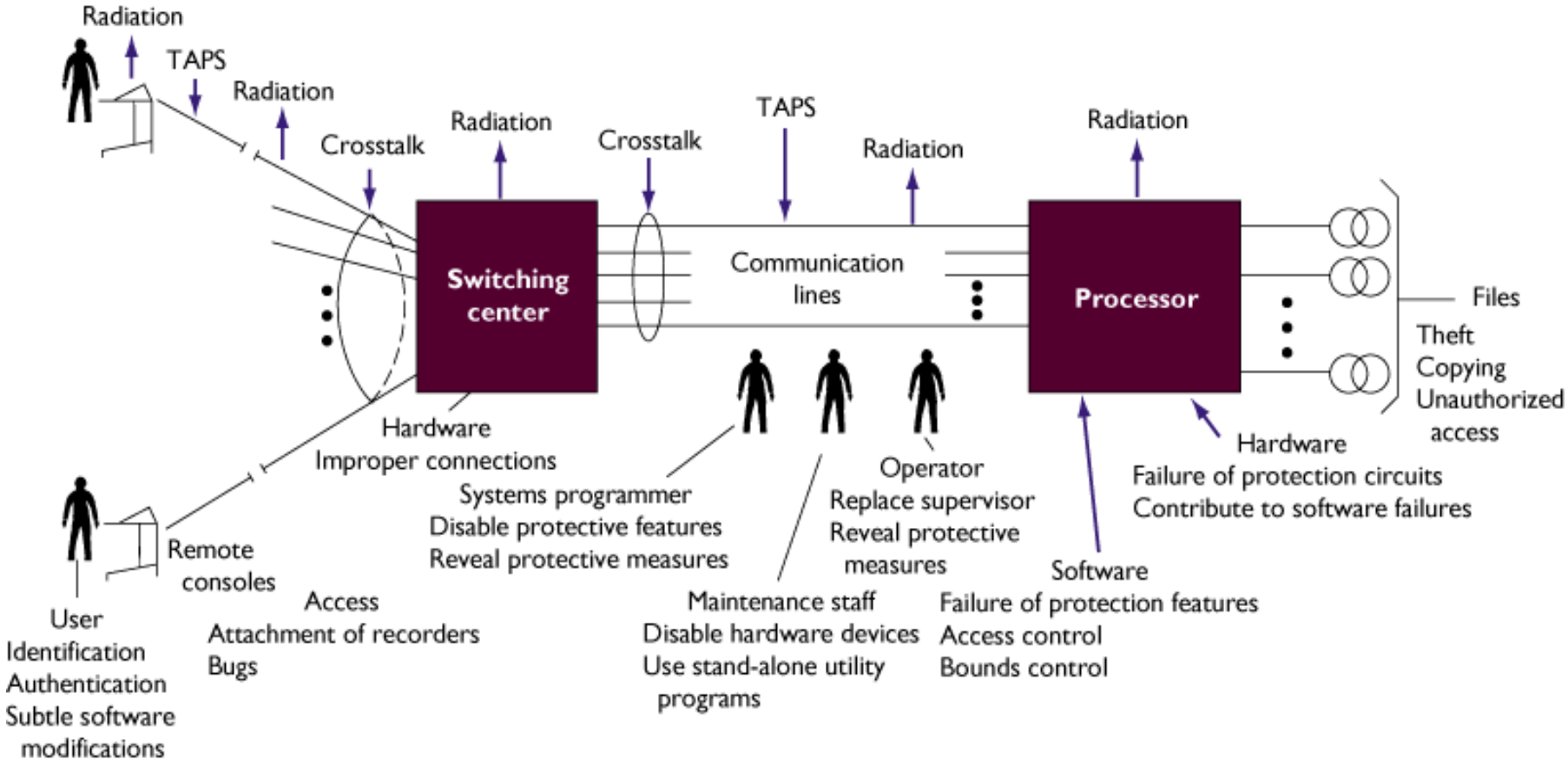



**Figure 14-1**

## Concerns for System Builders and Users

# Disaster

- Destroys computer hardware, programs, data files, and other equipment

# Security

- Prevents unauthorized access, alteration, theft, or physical damage

## Concerns for System Builders and Users

# Errors

- **Cause computers to disrupt or destroy organization's record-keeping and operations**

## System Quality Problems: Software and Data

# Bugs

- Program code defects or errors

# Maintenance Nightmare

- Maintenance costs high due to organizational change, software complexity, and faulty system analysis and design

## Points in the Processing Cycle where Errors Can Occur

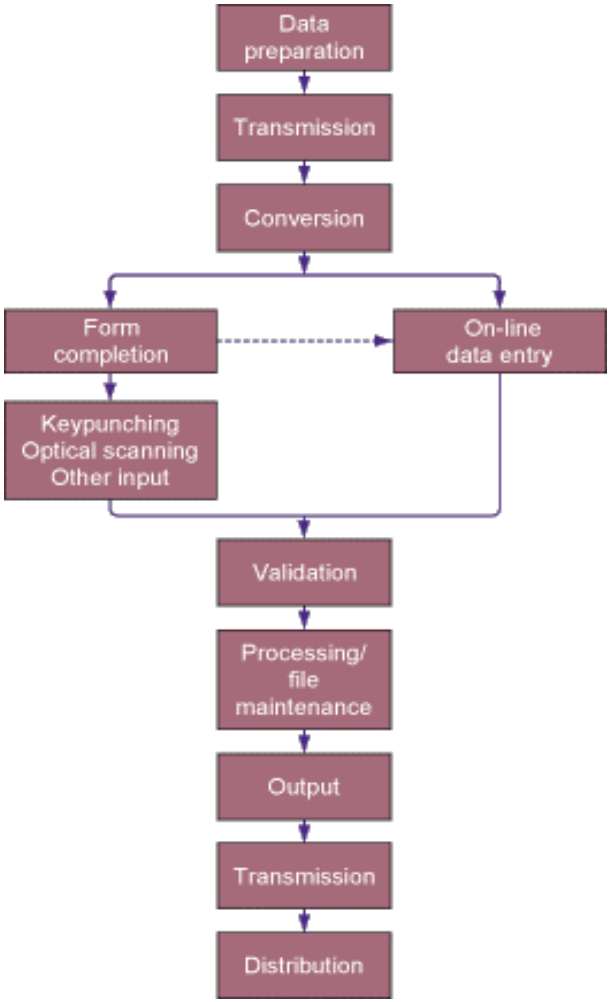



**Figure 14-2**

System Quality Problems: Software and Data

# Data Quality Problems

- Caused due to errors during data input or faulty information system and database design

## The Cost of Errors over the Systems Development Cycle

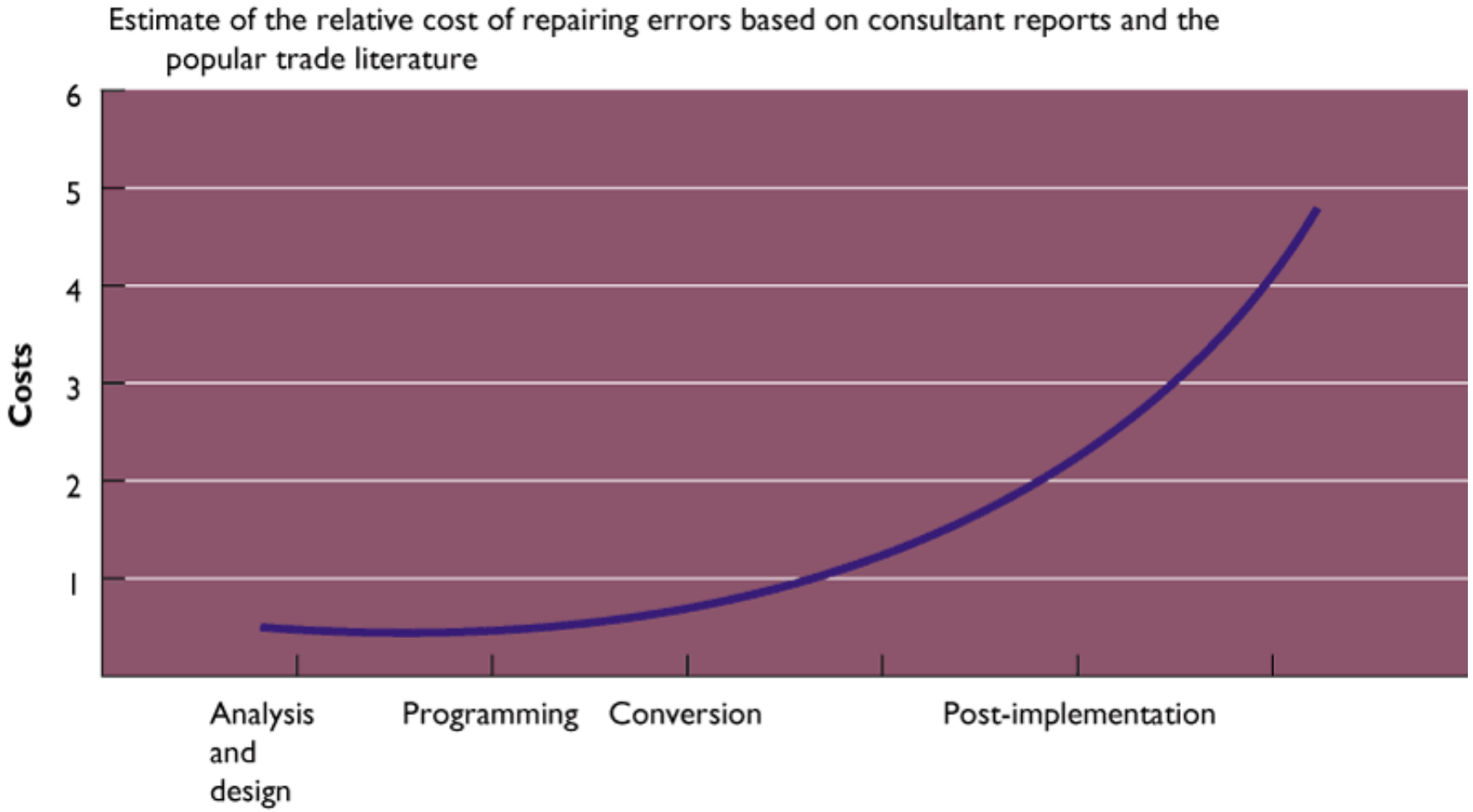



Figure 14-3

Overview

# Controls

- **Methods, policies, and procedures that ensure protection of organization's assets**
- **Ensure accuracy and reliability of records, and operational adherence to management standards**

## General Controls and Application Controls

# General controls

- **Establish framework for controlling design, security, and use of computer programs**
- **Include software, hardware, computer operations, data security, implementation, and administrative controls**

## Security Profiles for a Personnel System

**SECURITY PROFILE 1**

User: Personnel Dept. Clerk

Location: Division 1

Employee Identification Codes with This Profile: 00753, 27834, 37665, 44116

| Data Field Restrictions | Type of Access |
|---|---|
| All employee data for Division 1 only | Read and Update |
| ☐ Medical history data | None |
| ☐ Salary | None |
| ☐ Pensionable earnings | None |

**SECURITY PROFILE 2**

User: Divisional Personnel Manager

Location: Division 1

Employee Identification Codes with This Profile: 27321

| Data Field Restrictions | Type of Access |
|---|---|
| All employee data for Division 1 only | Read Only |

**Figure 14-4**

# Application controls

- Unique to each computerized application
- Include input, processing, and output controls

## Protecting the Digital Firm

- **On-line transaction processing:**
  **Transactions entered online are immediately processed by computer**

- **Fault-tolerant computer systems:**
  **Contain extra hardware, software, and power supply components to provide continuous uninterrupted service**

## Protecting the Digital Firm

- **High-availability computing:** Tools and technologies enabling system to recover quickly from a crash
- **Disaster recovery plan:** Runs business in event of computer outage
- **Load balancing:** Distributes large number of requests for access among multiple servers

## Protecting the Digital Firm

- **Mirroring:** Duplicating all processes and transactions of server on backup server to prevent any interruption in service

- **Clustering:** Linking two computers together so that a second computer can act as a backup to the primary computer or speed up processing

Internet Security Challenges

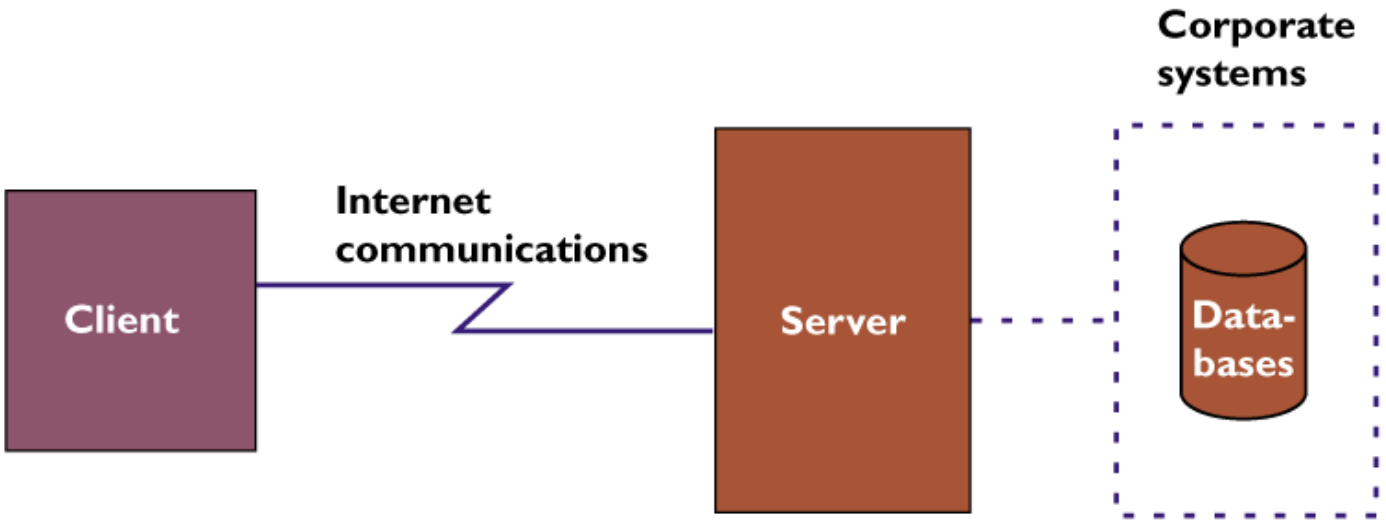
## Firewalls

- Prevent unauthorized users from accessing private networks
- Two types: proxies and stateful inspection

## Intrusion Detection System

- Monitors vulnerable points in network to detect and deter unauthorized intruders

## Internet Security Challenges




- Computer viruses
- Line taps
- Loss of machine

- Tapping
- Sniffing
- Message alteration
- Theft and fraud

- Hacking
- Computer viruses
- Theft and fraud
- Line taps
- Vandalism
- Denial–of–service attacks

- Theft of data
- Copying of data
- Alteration of data

Figure 14-5

## Security and Electronic Commerce

- **Encryption:** Coding and scrambling of messages to prevent their access without authorization
- **Authentication:** Ability of each party in a transaction to ascertain identity of other party
- **Message integrity:** Ability to ascertain that transmitted message has not been copied or altered

## Security and Electronic Commerce

- **Digital signature:** Digital code attached to electronically transmitted message to uniquely identify contents and sender

- **Digital certificate:** Attachment to electronic message to verify the sender and to provide receiver with means to encode reply

## Public Key Encryption

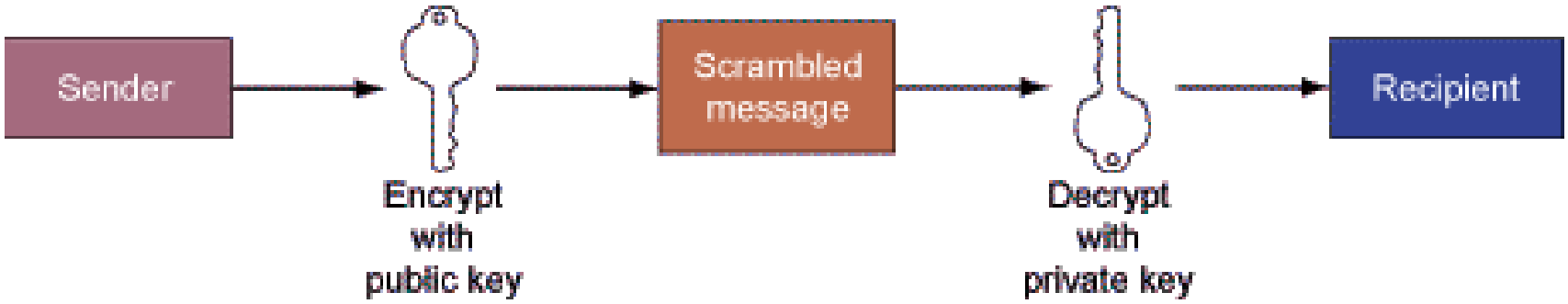



**Figure 14-6**

# Digital Certificates

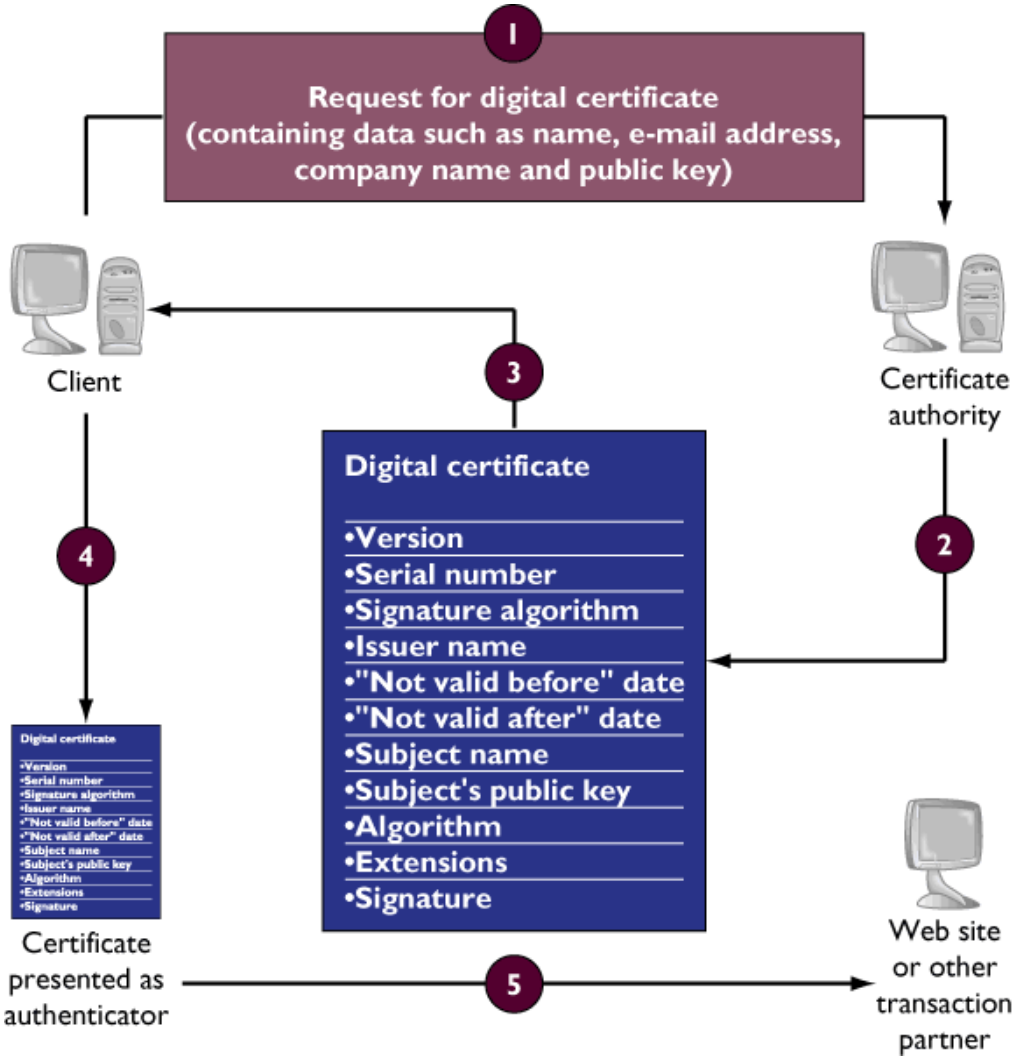



**Figure 14-7**

## Developing a Control Structure: Costs and Benefits

# Criteria for determining control structure

- Importance of data
- Efficiency, complexity, and expense of each control technique
- Level of risk if a specific activity or process is not properly controlled

## The Role of Auditing in the Control Process

# MIS audit

- **Identifies all controls that govern individual information systems and assesses their effectiveness**

## Sample Auditor's List of Control Weaknesses

Function: Personal Loans _____ Prepared by: ____ J. Ericson _____ Received by: _____ T. Barrow _____
Location: Peoria, Ill. _____ Preparation date: __ June 16, 2001 _____ Review date: _____ June 28, 2001 _____

| Nature of Weakness and Impact | Chance for Substantial Error | | Effect on Audit Procedures | Notification to Management | |
|---|---|---|---|---|---|
| | Yes/ No | Justification | Required Amendment | Date of Report | Management Response |
| Loan repayment records are not reconciled to borrower□s records during processing. | Yes | Without a detection control, errors in individual client balances may remain undetected. | Confirm a sample of loans. | 5/10/01 | Interest Rate Compare Report provides this control. |
| There are no regular audits of computer-generated data (interest charges). | Yes | Without a regular audit or reasonableness check, widespread miscalculations could result before errors are detected. | | 5/10/01 | Periodic audits of loans will be instituted. |
| Programs can be put into production libraries to meet target deadlines without final approval from the Standards and Controls group. | No | All programs require management authorization. The Standards and Controls group controls access to all production systems, and assigns such cases to a temporary production status. | | | |

Figure 14-8

## Software Quality Assurance Methodologies and Tools

- **Development methodology:** Collection of methods, for every activity within every phase of development project

- **Structured:** Refers to fact that techniques are carefully drawn up, step-by-step, with each step building on a previous one

## Software Quality Assurance Methodologies and Tools

- **Structured analysis:** Method for defining system inputs, processes, and outputs, for partitioning systems into subsystems or modules

- **Data Flow Diagram (DFD):** Graphically illustrates system's component processes and flow of data

## Data Flow Diagram for Mail-in University Registration System

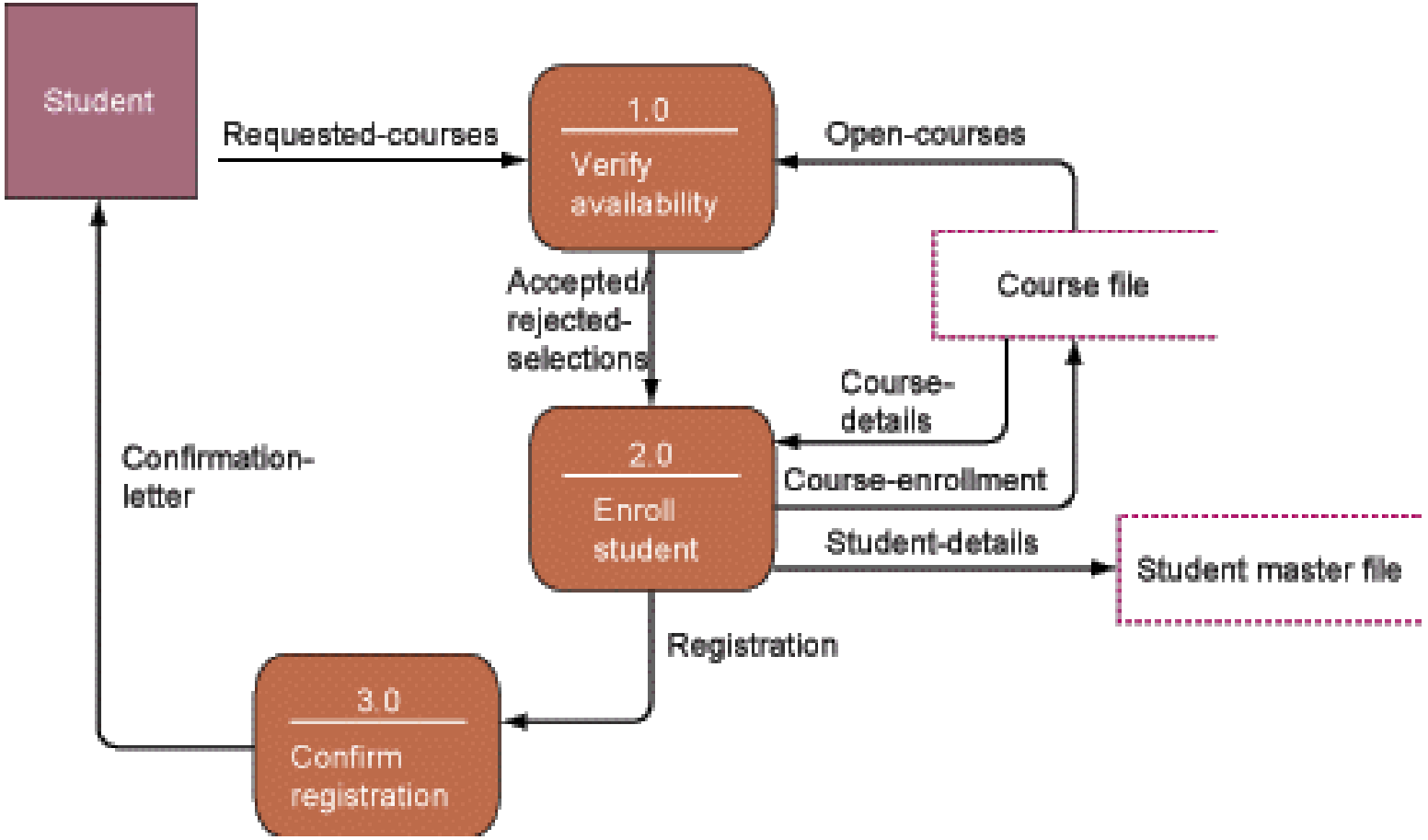



Figure 14-9

## Software Quality Assurance Methodologies and Tools

- **Structured design:** Encompasses set of design rules and techniques for designing systems from top down

- **Structured programming:** Organizing and coding programs that simplify control paths

## High-Level Structure Chart For a Payroll System

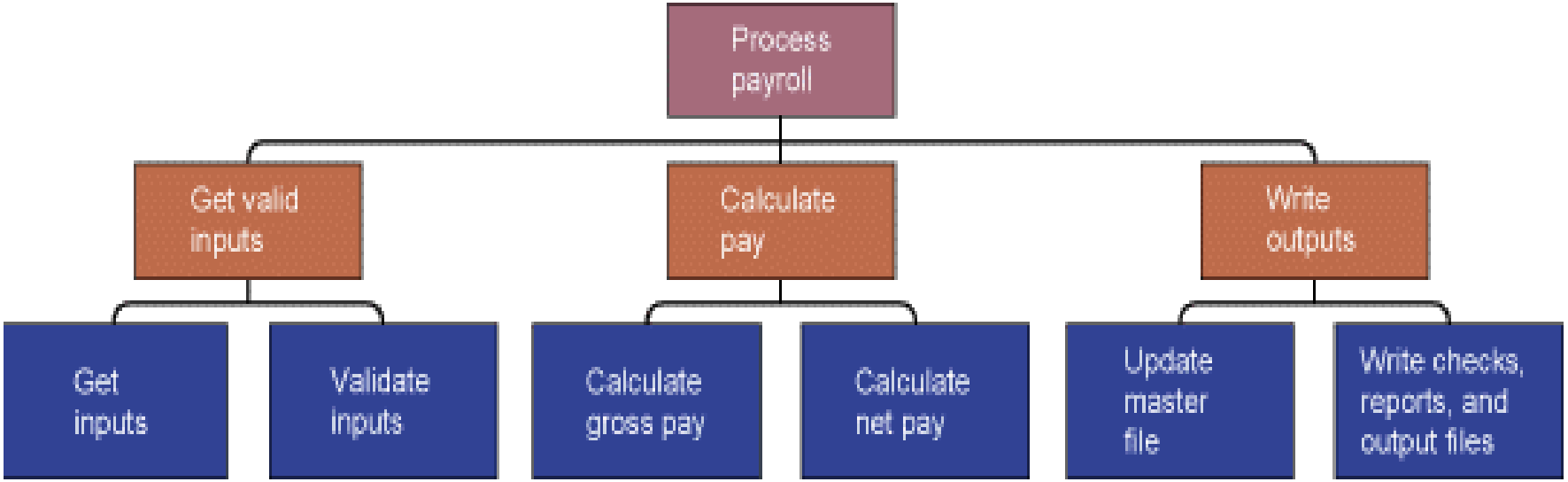



**Figure 14-10**

## Limitation of Traditional Methods

- **Inflexible**
- **Time-consuming**

## Tools and Methodologies for Object-Oriented Development

- Unified Modeling Language (UML) has become industry standard for analyzing and designing object-oriented systems.
- Structural diagrams describe the relation between classes.
- Behavioral diagrams describe interactions in an object-oriented system.

# Basic Program Control Constructs

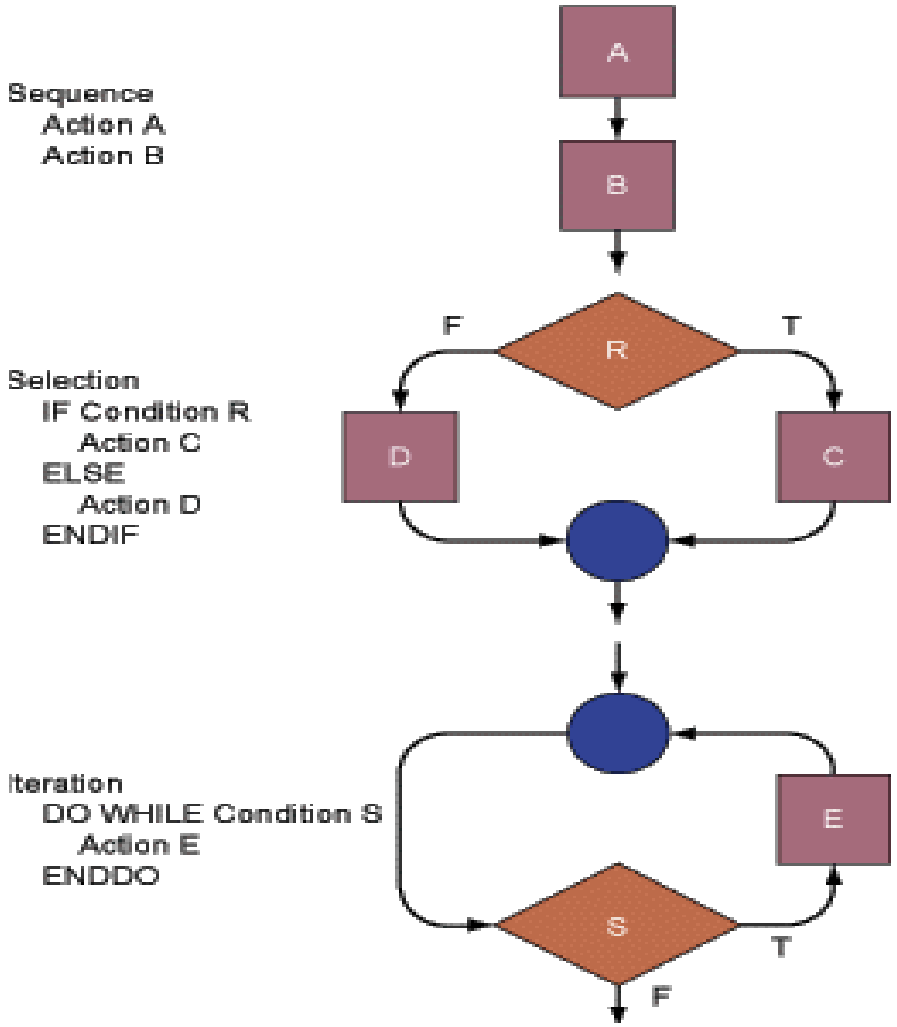



Figure 14-11

## Computer-Aided Software Engineering (CASE)

- **Automation of step-by-step methodologies for software and systems development**
- **Reduces repetitive work**
- **Enforces standard development methodology and design discipline**
- **Improves communication between users and technical specialists**

## Computer-Aided Software Engineering (CASE)

- **Organizes and correlates design components**
- **Automates tedious and error-prone portion of analysis and design, code generation, testing, and control rollout**

# Visible Analyst: A Tool to Automate Object-Oriented Analysis and Design

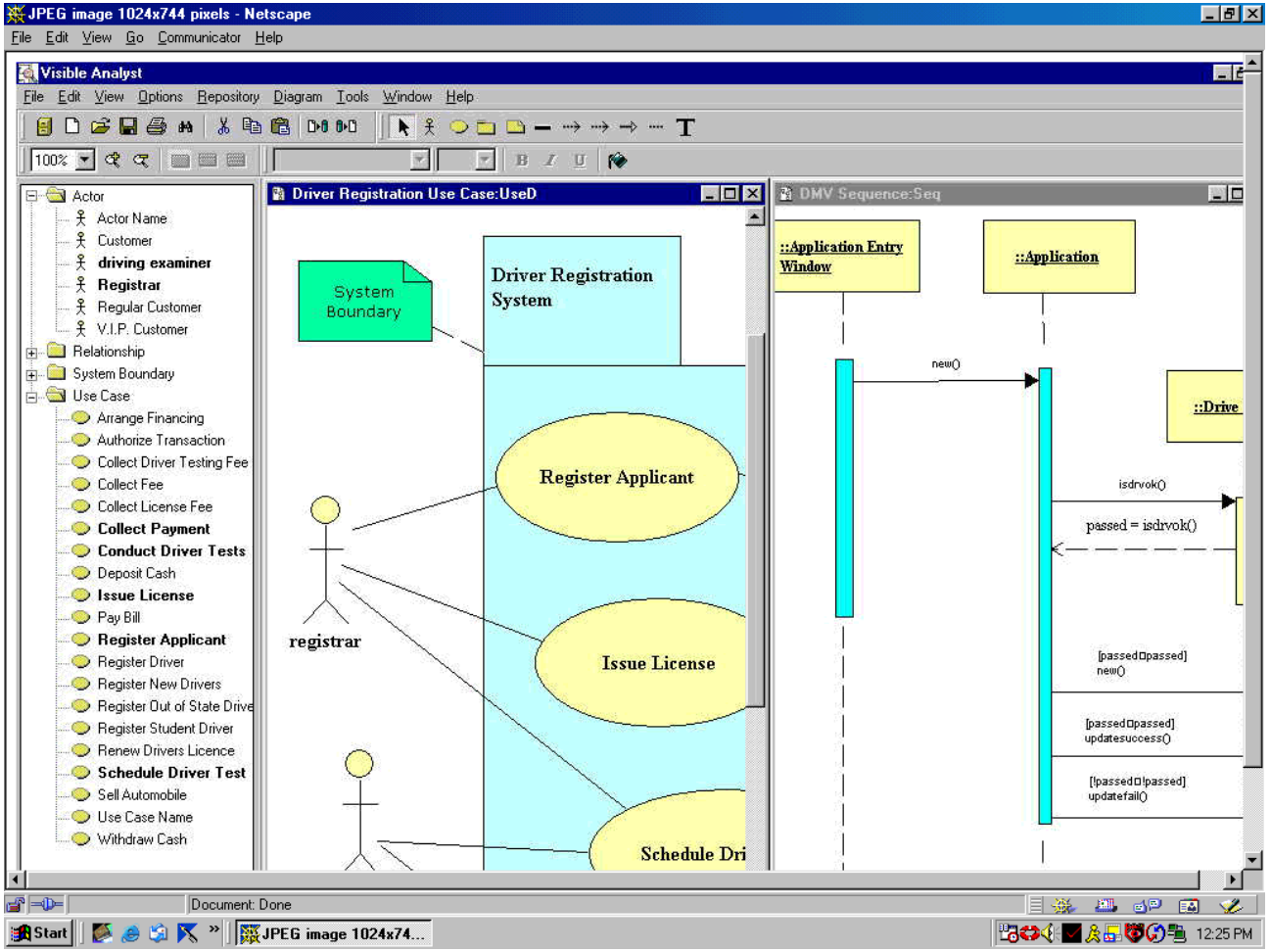



Figure 14-12

# Resource allocation

- **Determines how costs, time, and personnel are assigned to different phases of systems development project**

## Software Metrics

- **Objective assessment of software used in the system in form of quantified measurements**

## Testing

- **Walkthrough:** Review of specification or design document by small group of people

- **Debugging:** Process of discovering and eliminating errors and defects in program code

## Data Quality Audit and Data Cleansing

# Data quality audit

- Survey and/or sample of files
- Determines accuracy and completeness of data

# Data cleansing

- Correcting errors and inconsistencies in data to increase accuracy