



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

SYSTEM VULNERABILITY AND ABUSE

Why Systems are Vulnerable

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

SYSTEM VULNERABILITY AND ABUSE

Telecommunication Network Vulnerabilities

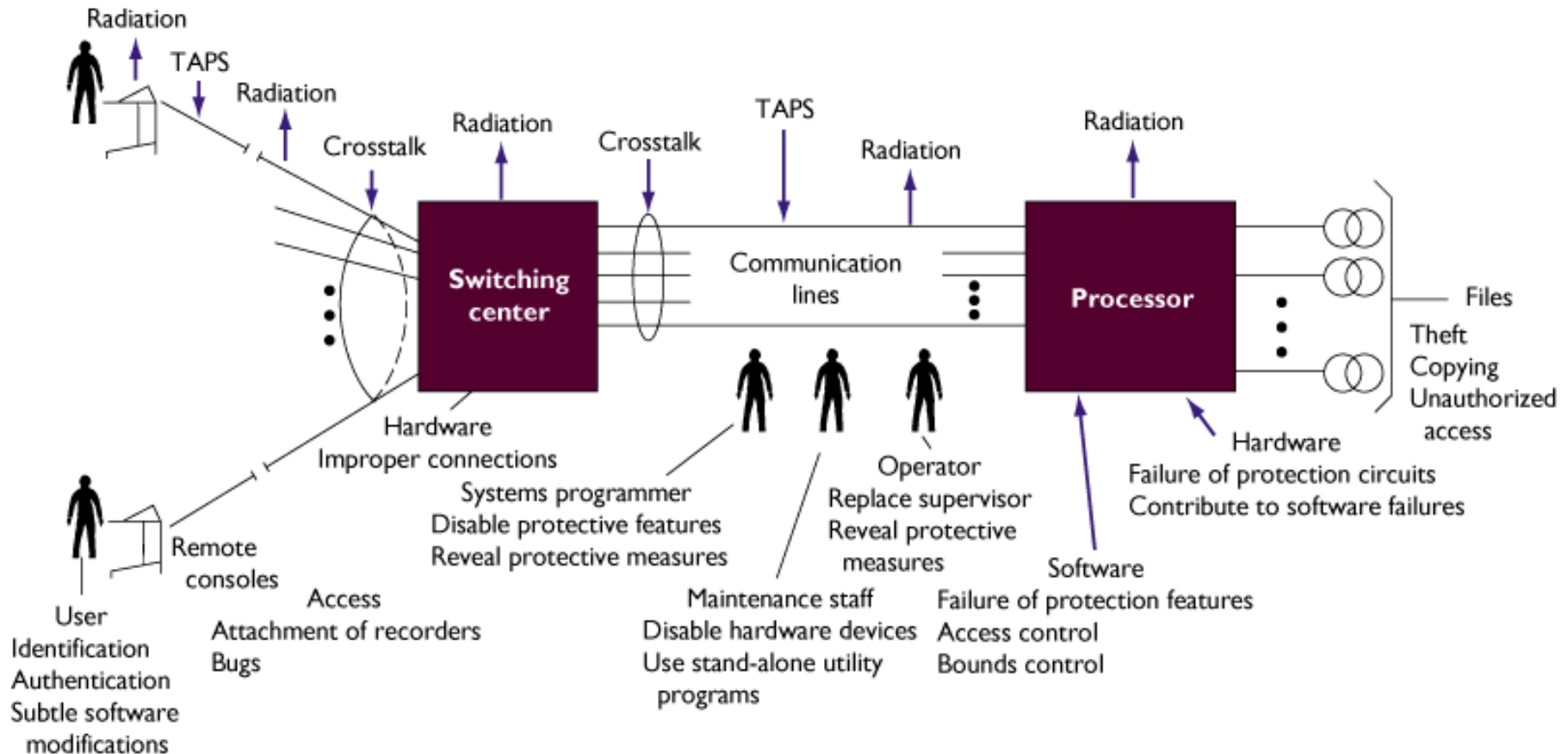


Figure 14-1

SYSTEM VULNERABILITY AND ABUSE

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

SYSTEM VULNERABILITY AND ABUSE

Concerns for System Builders and Users

Errors

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

SYSTEM VULNERABILITY AND ABUSE

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

SYSTEM VULNERABILITY AND ABUSE

Points in the Processing Cycle where Errors Can Occur

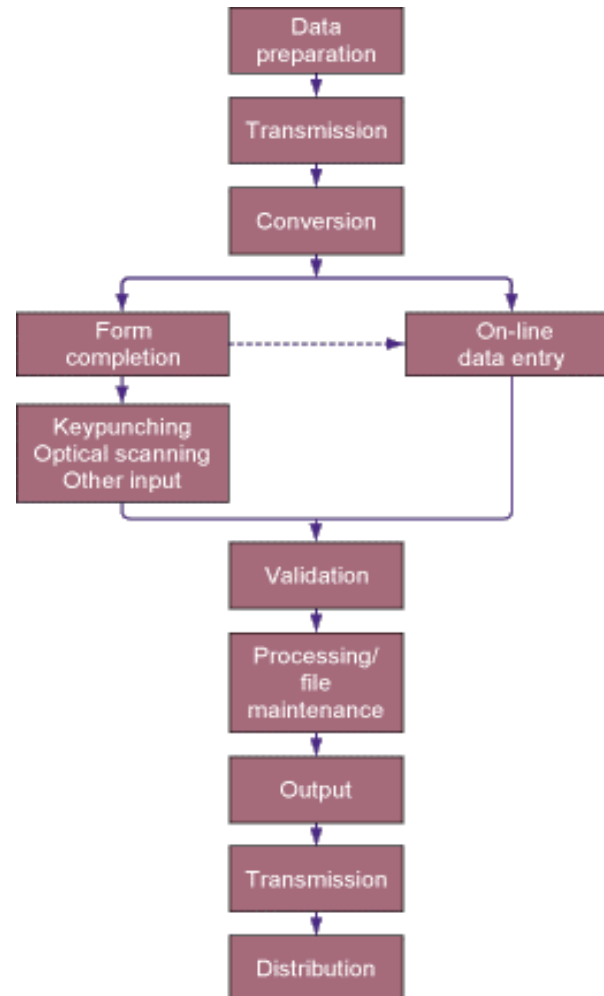


Figure 14-2

SYSTEM VULNERABILITY AND ABUSE

System Quality Problems: Software and Data

Data Quality Problems

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

SYSTEM VULNERABILITY AND ABUSE

The Cost of Errors over the Systems Development Cycle

Estimate of the relative cost of repairing errors based on consultant reports and the popular trade literature

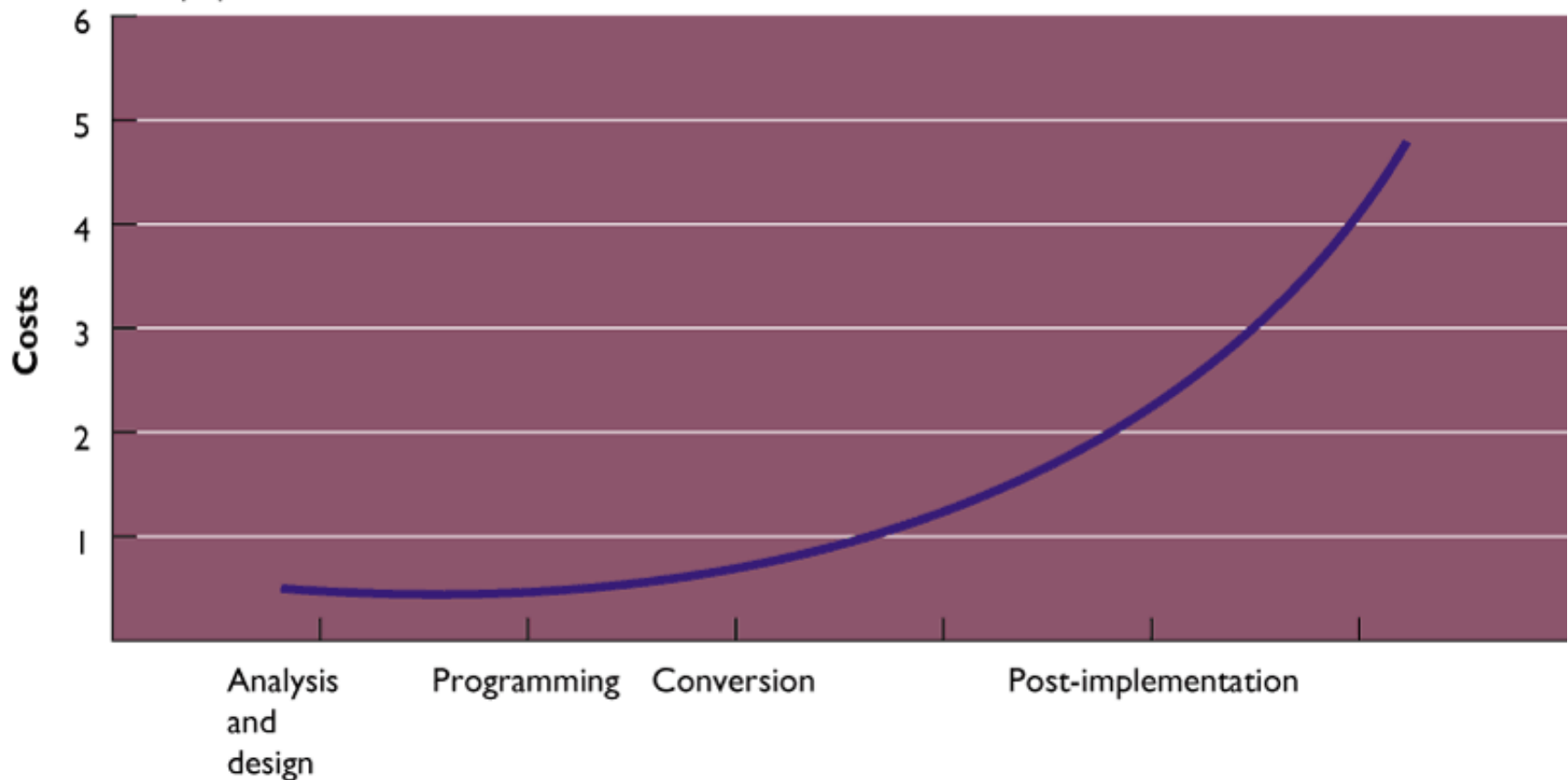


Figure 14-3

CREATING A CONTROL ENVIRONMENT

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**

CREATING A CONTROL ENVIRONMENT

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

CREATING A CONTROL ENVIRONMENT

Security Profiles for a Personnel System

SECURITY PROFILE 1	
User: Personnel Dept. Clerk	
Location: Division 1	
Employee Identification	
Codes with This Profile:	00753, 27834, 37885, 44116
Data Field Restrictions	Type of Access
All employee data for Division 1 only	Read and Update
<input type="checkbox"/> Medical history data	None
<input type="checkbox"/> Salary	None
<input type="checkbox"/> 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

CREATING A CONTROL ENVIRONMENT

General Controls and Application Controls

Application controls

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

CREATING A CONTROL ENVIRONMENT

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

CREATING A CONTROL ENVIRONMENT

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

CREATING A CONTROL ENVIRONMENT

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

CREATING A CONTROL ENVIRONMENT

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

CREATING A CONTROL ENVIRONMENT

Internet Security Challenges

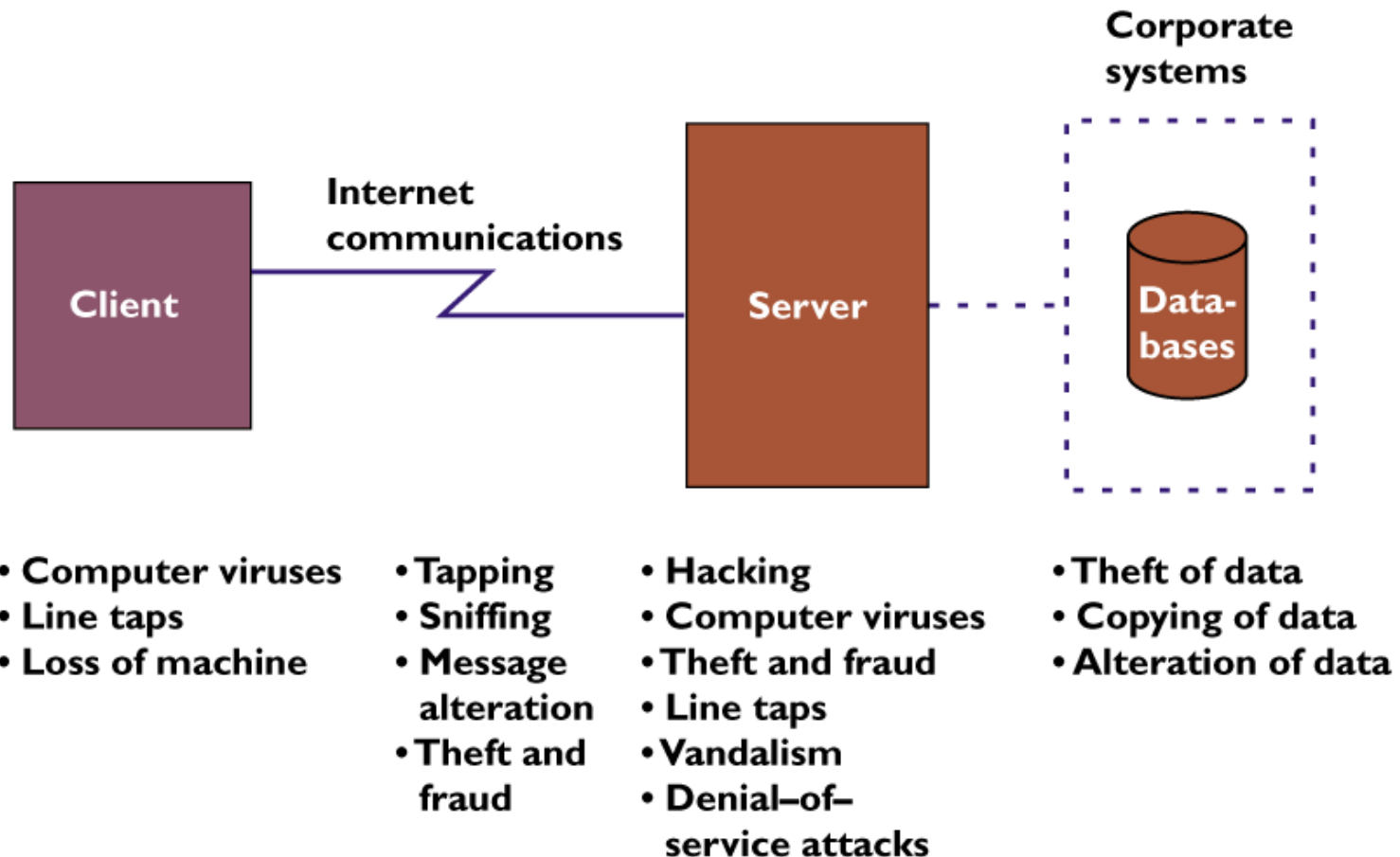


Figure 14-5

CREATING A CONTROL ENVIRONMENT

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

CREATING A CONTROL ENVIRONMENT

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

CREATING A CONTROL ENVIRONMENT

Public Key Encryption

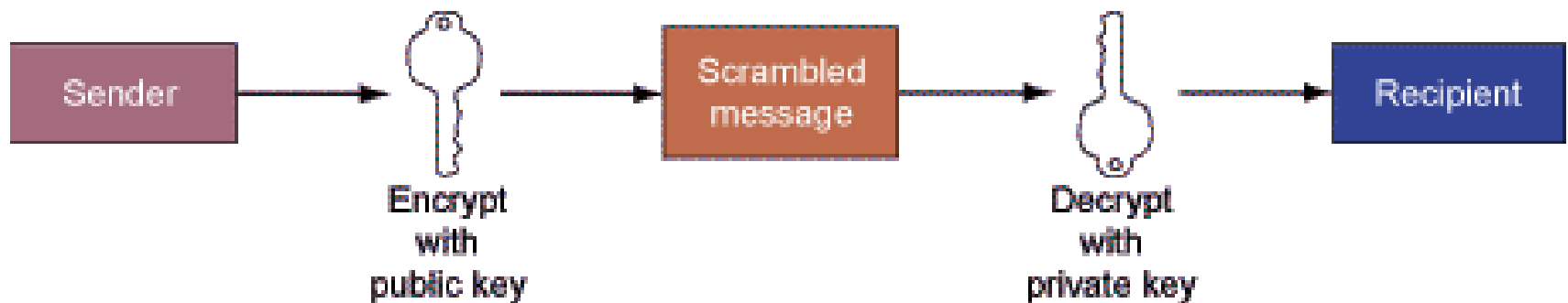


Figure 14-6

CREATING A CONTROL ENVIRONMENT

Digital Certificates

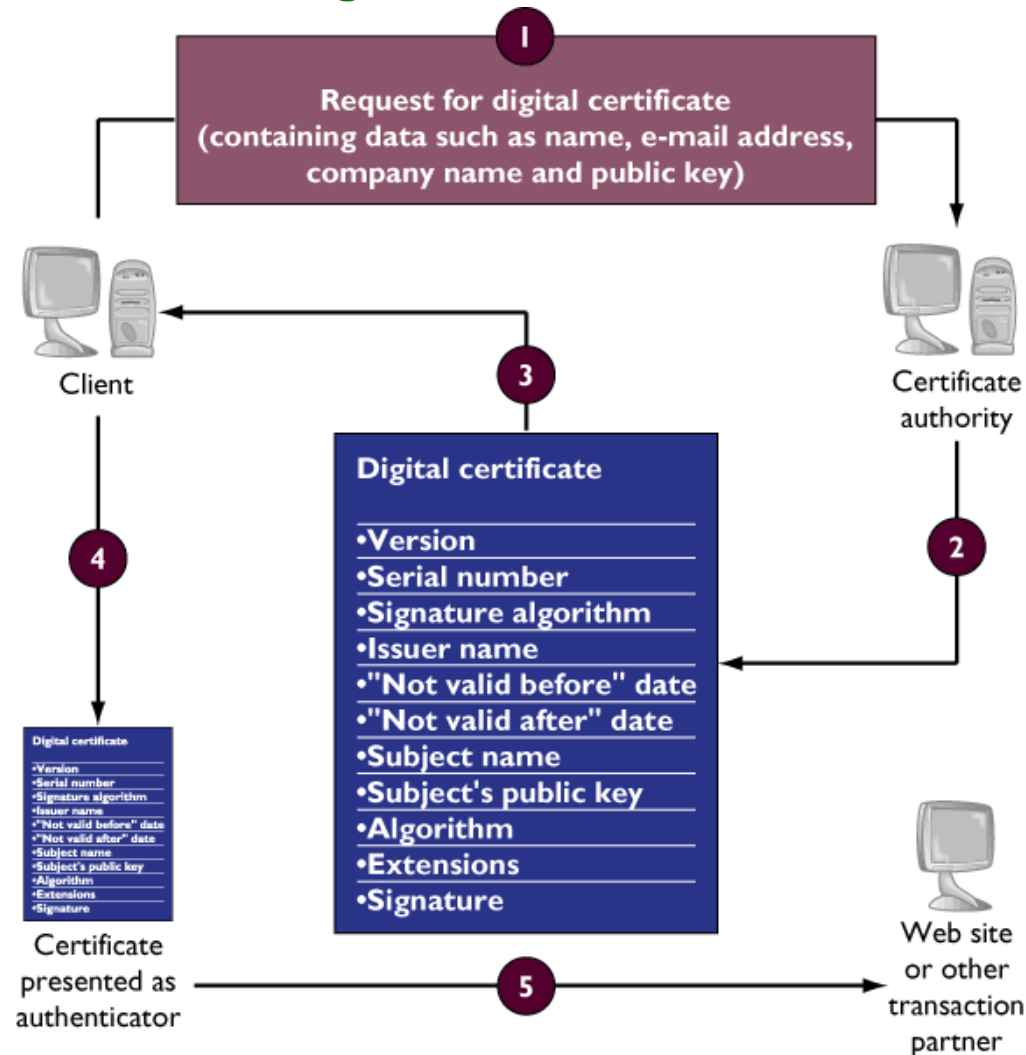


Figure 14-7

CREATING A CONTROL ENVIRONMENT

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

CREATING A CONTROL ENVIRONMENT

The Role of Auditing in the Control Process

MIS audit

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

CREATING A CONTROL ENVIRONMENT

Sample Auditor's List of Control Weaknesses

Function: Personal Loans _____
 Location: Peoria, Ill. _____

Prepared by: _____ J. Ericson _____
 Preparation date: ____ June 16, 2001 _____

Received by: _____ T. Barrow _____
 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. There are no regular audits of computer-generated data (interest charges).	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.
	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

ENSURING SYSTEM QUALITY

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

ENSURING SYSTEM QUALITY

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

ENSURING SYSTEM QUALITY

Data Flow Diagram for Mail-in University Registration System

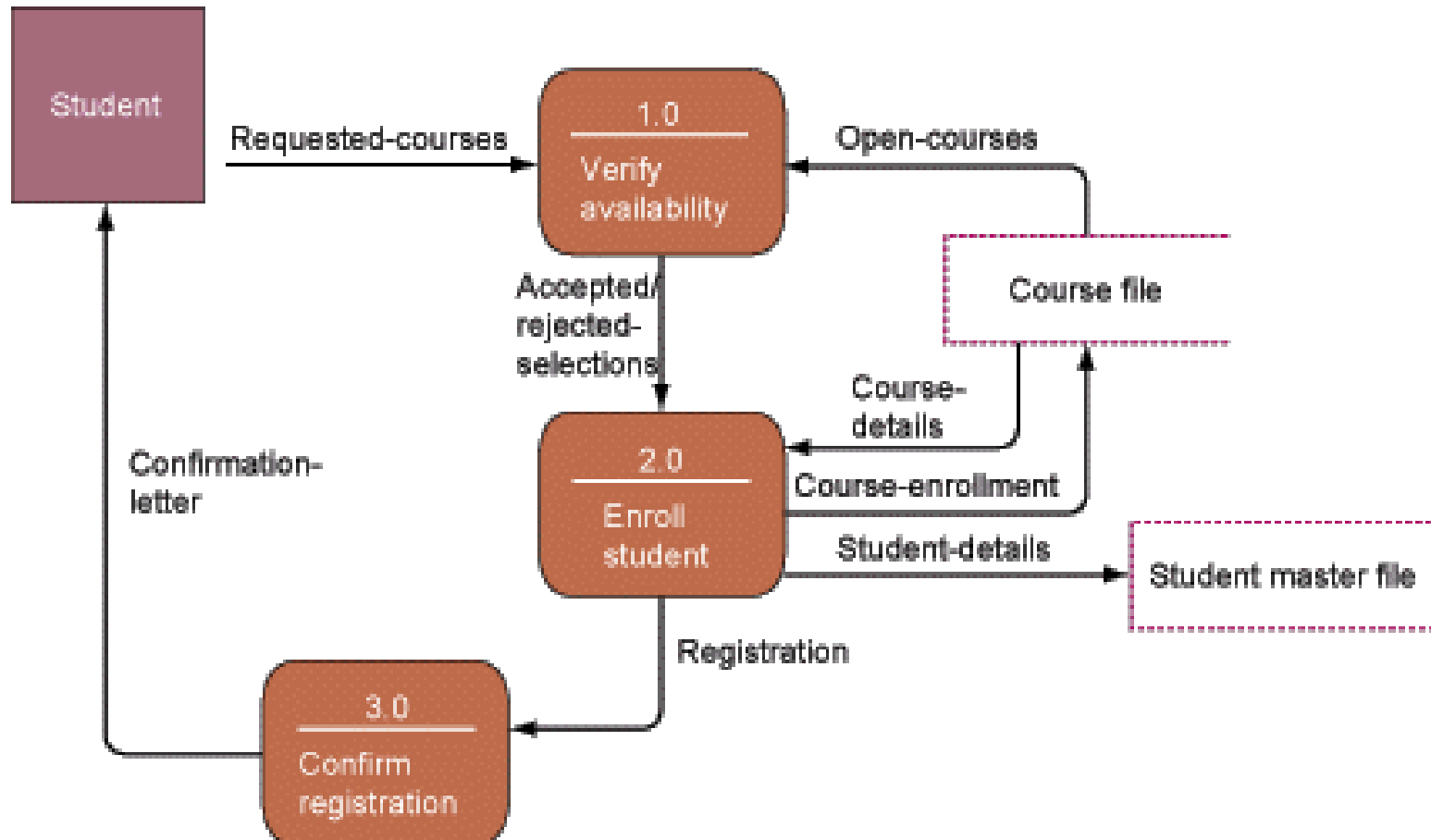


Figure 14-9

ENSURING SYSTEM QUALITY

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

ENSURING SYSTEM QUALITY

High-Level Structure Chart For a Payroll System

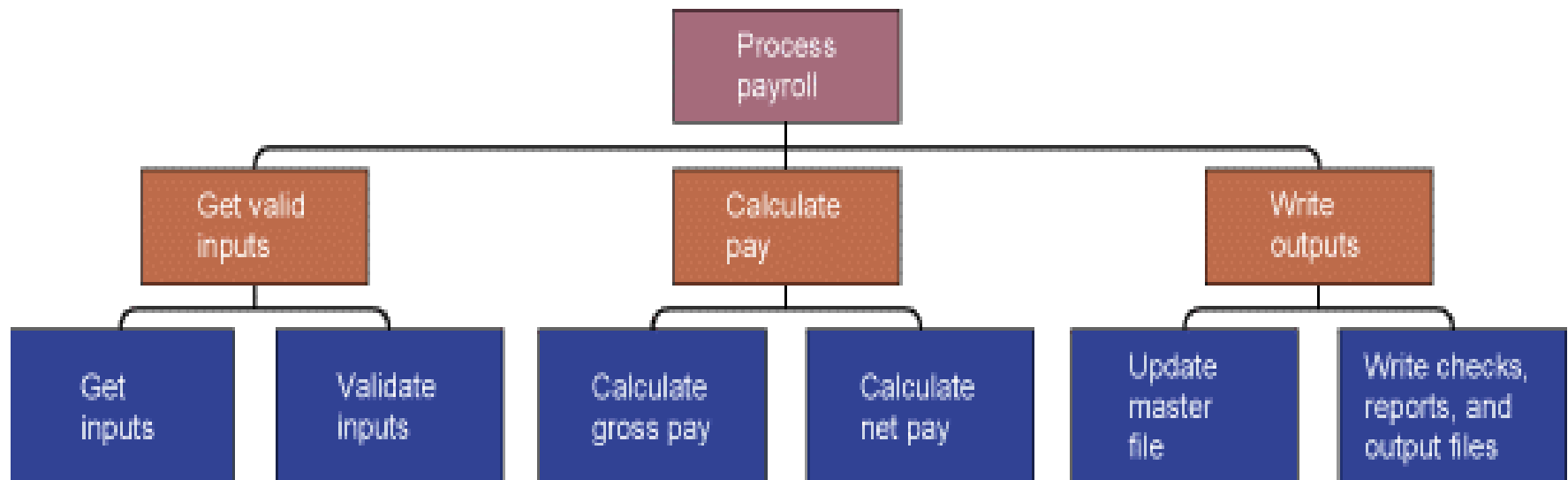


Figure 14-10

ENSURING SYSTEM QUALITY

Limitation of Traditional Methods

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

ENSURING SYSTEM QUALITY

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.

ENSURING SYSTEM QUALITY

Basic Program Control Constructs

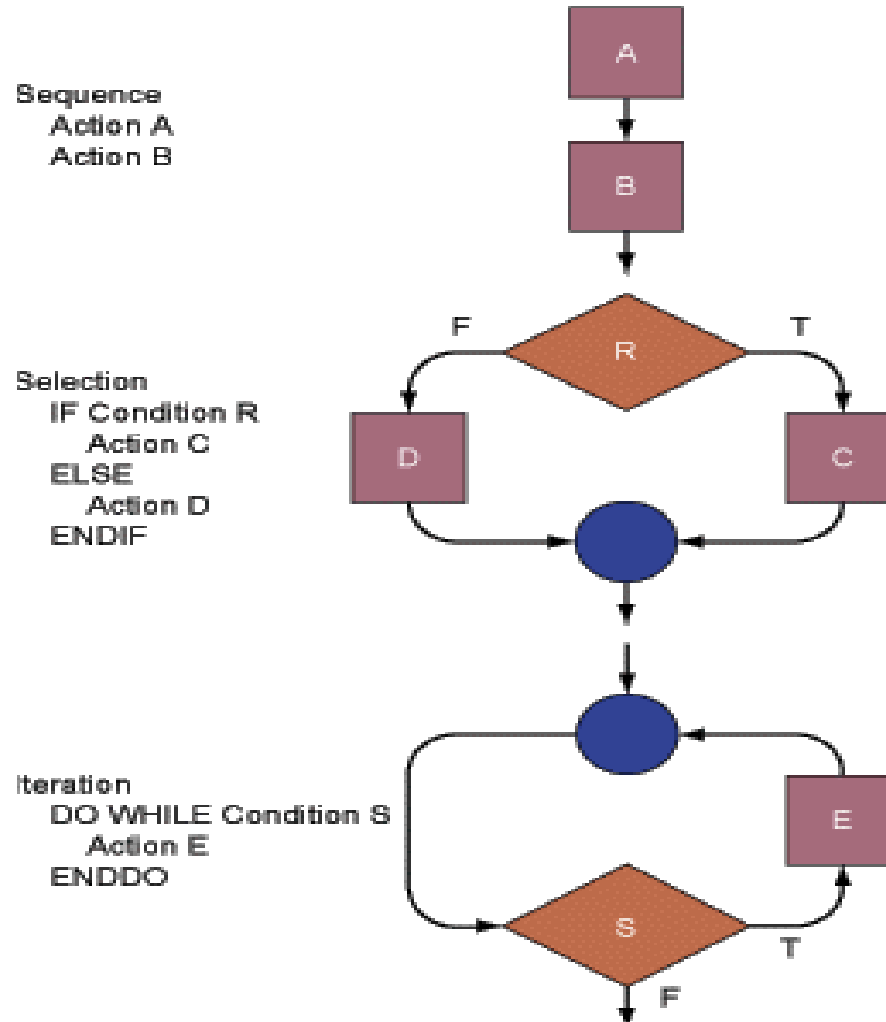


Figure 14-11

ENSURING SYSTEM QUALITY

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**

ENSURING SYSTEM QUALITY

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**

ENSURING SYSTEM QUALITY

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

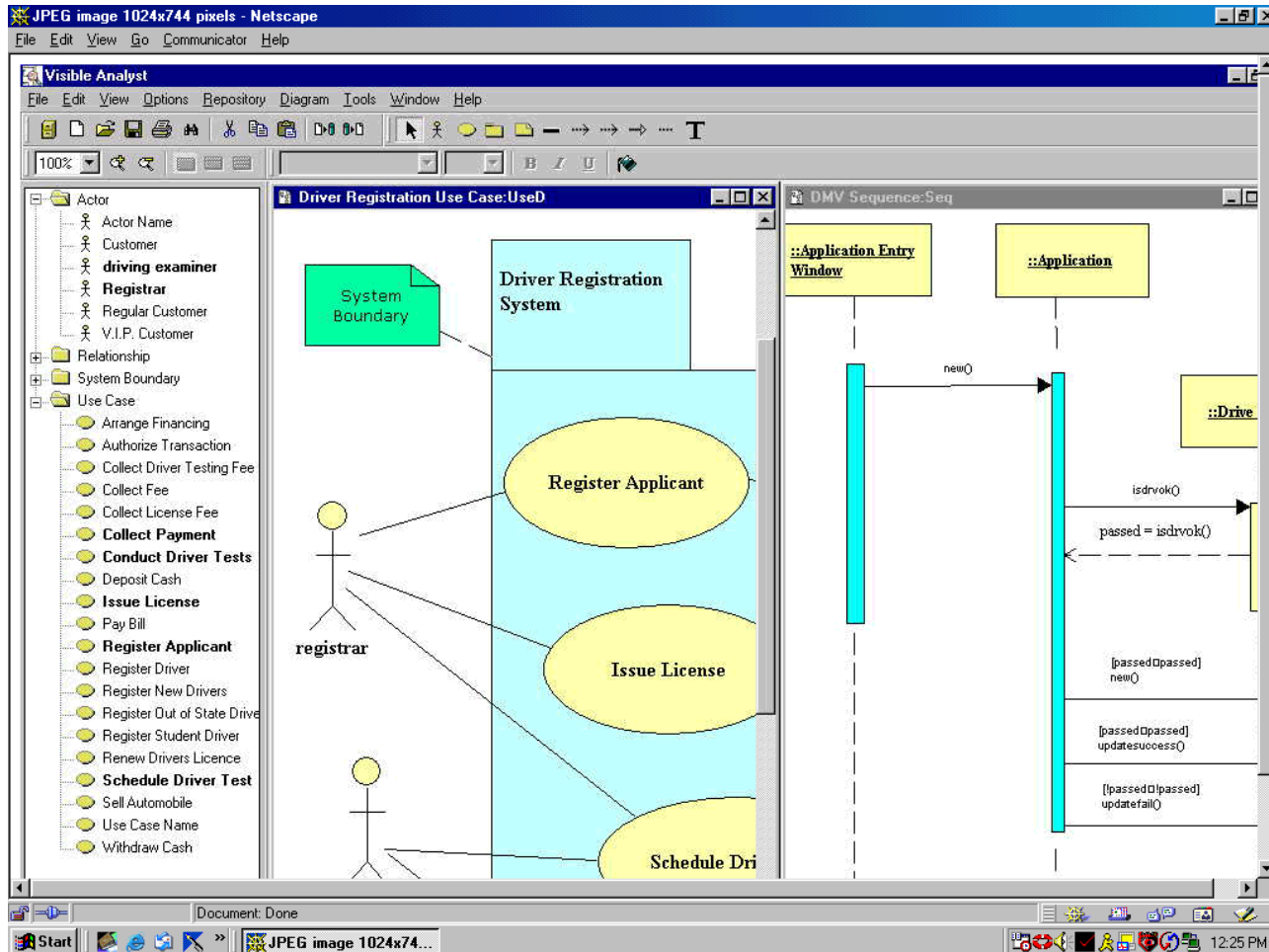


Figure 14-12

ENSURING SYSTEM QUALITY

Resource Allocation During Systems Development

Resource allocation

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

ENSURING SYSTEM QUALITY

Software Metrics

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

ENSURING SYSTEM QUALITY

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

ENSURING SYSTEM QUALITY

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