Control Audit And Security Of Information System

Units

1 Controls in Information systems
2 Need and methods of auditing Information systems
3 Testing Information systems
4 Security of Information systems

Learning Goals

- Why controls are necessary in Information systems
- Methods of controlling Information systems
- How controls are introduced in Information systems
- Why Information systems need auditing
- How are systems audited
- The methods used to test Information systems
- How the security of an Information system is ensured

Motivation For Controls

- It is very important to ensure the reliability of reports produced by an information system
- If unreliability is seen by users the entire credibility of the system is lost
- Ensuring reliability is not difficult for small systems but when a system has to handle massive data it is a challenge
- Systematic controls are thus essential when a system is designed

Motivation For Audits

- Many organizations are now entirely dependent on computer based information system
- These information systems contain financial data and other critical procedures
- It is essential to protect the systems against frauds and ensure that sound accounting practices are followed
- It is necessary to trace the origin and fix responsibilities when frauds occur
- Audit methods primary purpose is to ensure this.

Motivation For Testing

- Systems contain many individual subsystems
- Usually sub-systems and programs are individually tested
- However when a whole system is integrated unforeseen errors may be seen
- Thus before releasing a system the entire operational system should be tested for correctness and completeness

Motivation For Security

- Systems contain sensitive data about the organization and also about persons working in the organization
- Sensitive data should be protected from spies, thieves or disgruntled employees.
- Thus access should be carefully controlled and provided only on a need to know basis
- When computers are networked corruption may take place due to viruses
- Services may be disrupted due to denial of service attacks
- Thus systems should be designed with appropriate security measures.

Motivation For Disaster Recovery

- Organizations depend on Information systems for their entire operations
- It is thus essential to ensure continuity of service when unforeseen situations such as disk crashes, fires, floods and such disasters take place.
- Thus it is essential to ensure quick recovery from disasters and ensure continuity of service.

Control Audit and Security of Information System

• **CONTROL-** Method to ensure that a system processes data as per design and that all data is included and are correct

• **AUDIT AND TESTING -** Ensure that the system is built as per specifications and that processed results are correct. Protect systems from frauds.

• **SECURITY-** Protection of data resources, programs, and equipment from illegal use, theft, vandalism, accidents, disasters etc.

Need Of Controls

- Information systems handle massive amounts of data – accidents such as not including some data can cause serious damage
- Incorrect data entry can lead to high monetary losses
- Credibility in the information system may be lost if errors are found in operational systems

Objectives Of Controls

- To make sure data entering the computer are correct
- Check clerical handling of data before it is input to a computer
- Provide means of detecting and tracing errors which occur due to bad data or bad program
- Ensure legal requirements are met
- To guard against frauds

Control Techniques

• **ORGANIZATIONAL MEASURES**

Well defined responsibility for input preparation, delivery output use, operation and maintenance

- Changes in program and data (if any) should be documented
- Performance of task and recording must be by different persons to prevent frauds

Control Techniques

- **INPUT PREPARATION CONTROL**
  - -Sequence numbering
  - -Batch controls
  - -Data entry and verification
  - -Record totals
  - -Self checking digits

Auditing Technology for Information Systems

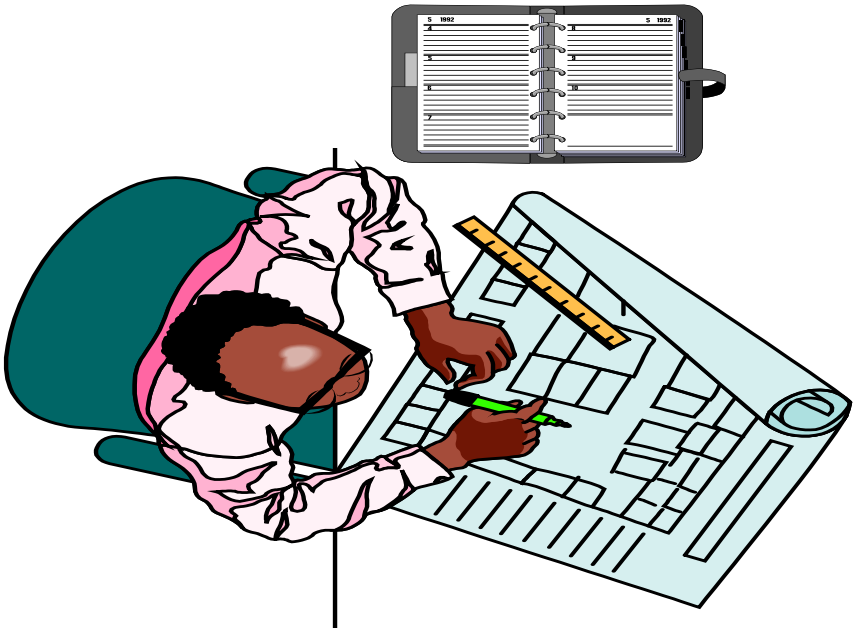
A. Review of Systems Documentation

B. Test Data

C. Audit Software

A. Review of Systems Documentation

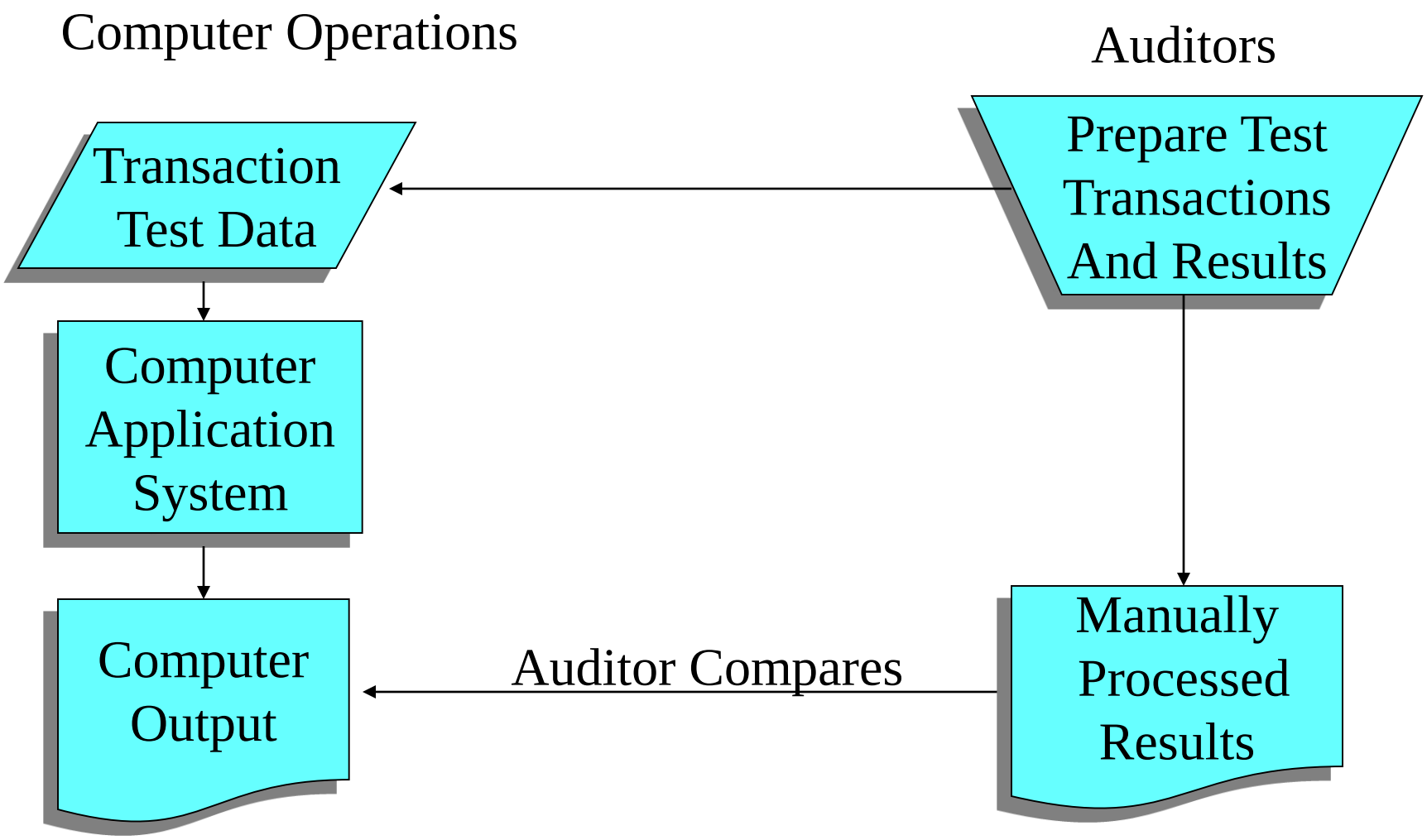
The auditor reviews documentation such as narrative descriptions, flowcharts, and program listings. In desk checking the auditor processes test or real data through the program logic.



B. Test Data

The auditor prepares input containing both valid and invalid data. Prior to processing the test data, the input is manually processed to determine what the output should look like. The auditor then compares the computer-processed output with the manually processed results.

Illustration of Test Data Approach



C. Audit Software

Computer programs that permit computers to be used as auditing tools include:

1. Generalized audit software

   Perform tasks such as selecting sample data from file, checking computations, and searching files for unusual items.

2. P.C. Software

   Allows auditors to analyze data from notebook computers in the field.

What is Security?

- “The quality or state of being secure—to be free from danger”
- A successful organization should have multiple layers of security in place:
  - Physical security
  - Personal security
  - Operations security
  - Communications security
  - Network security
  - Information security

Types of Security

- Physical Security: To Protect physical items, object or areas
- Personal Security: To protect the individual or group of individuals who are authorized
- Operation Security: To protect the details of a particular operation or activities.

Types of Security

- Communication Security: To protect communication media, technology and content
- Network Security: To protect networking components, connections and contents
- Information Security: To protect information assets

What is Information Security?

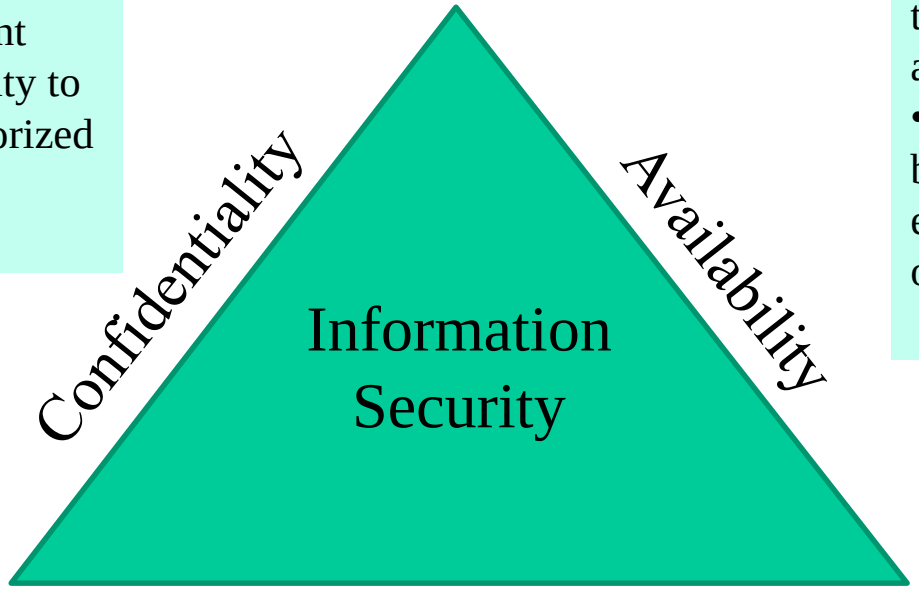
- The protection of information and its critical elements, including systems and hardware that use, store, and transmit that information
- Necessary tools: policy, awareness, training, education, technology
- C.I.A. triangle was standard based on confidentiality, integrity, and availability
- C.I.A. triangle now expanded into list of critical characteristics of information

CIA triangle “Security triad”

- Confidentiality: Making sure that those who should not see information
- Integrity: Making sure that the information hasn’t been changed from it’s original
- Availability: Making sure that the information is available for use when you need it.

Information Security C.I.A triangle

•Data and information is classified into different levels of confidentiality to ensure that only authorized users access the information

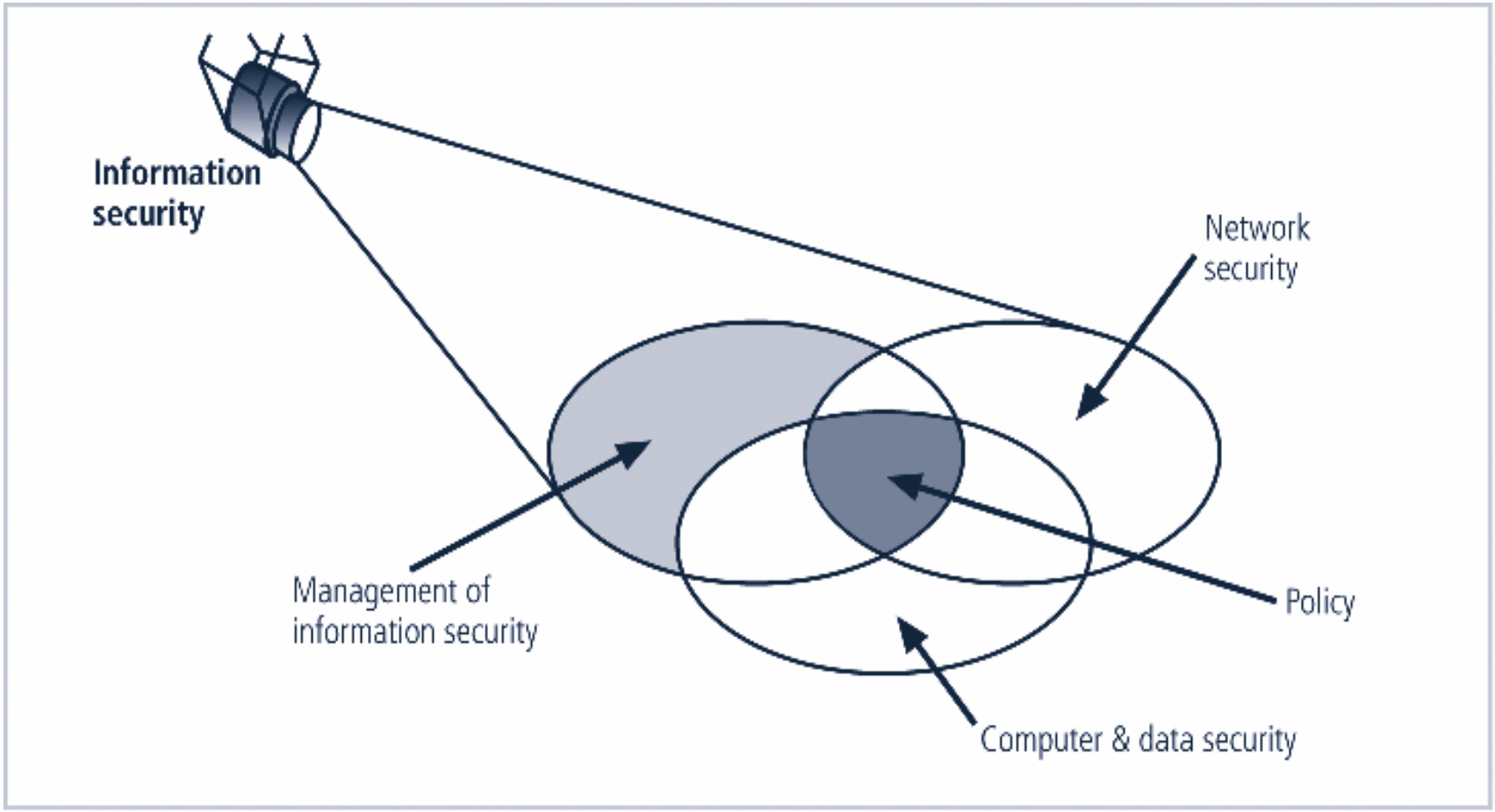


•System is available at all times only for authorizes and authenticated persons.
•System is protected from being shut down due to external or internal threats or attacks

•Data and information is accurate and protected from tampering by unauthorized persons.
•Data and information is consistent and validated.

Critical Characteristics of Information

- The value of information comes from the characteristics it possesses:
  - Availability
  - Accuracy
  - Authenticity
  - Confidentiality
  - Integrity



Components of Information Security

A Final Word

- Treat your password like you treat your toothbrush. Never give it to anyone else to use, and change it every few months.

LAYERED SECURITY

- Layered security, in its simplest form, consists of stacking security solutions, one on top of the other, to protect a computer from malware attacks.
- Malware: It refers to software programs designed to damage or do other unwanted actions on a computer system.

  Examples of malware include viruses, worms, trojan horses and spyware.

Why do we need it?

- To providing adequate computer system protection.

A CONSUMER LAYERED SECURITY APPROACH

- **Backup:** Consider where you would be if your layered security strategy failed. If you've ever lost critical data to a malware infection, no doubt you already consider it of primary importance.
- Free backup utilities are readily available
  - ❖ Hard Drive Cloning is Easy with Free Ease us Disk Copy
  - ❖ Free Drive Image XML- the best way to backup data

Consumer Layered

- **Firewall** – is an application, or a hardware appliance, designed to block unauthorized access to your computer from the Internet, at the same time permitting authorized communications.
- **Antimalware** – A front line antimalware application is absolutely critical to avoid system infection.
- For free antimalware click "Tech Thoughts Top & Free antimalware application"

Consumer Layered

- **Antivirus** – An antivirus application is another critical component in a layered defense strategy to ensure that if a malicious program is detected, it will be stopped dead in its tracks!
- **Web Browser Security** – Install a free Internet Browser add-on such as WOT(Web of Trust). WOT tests web sites you are visiting for spyware, spam, viruses, browser exploits, unreliable online shops, phishing, and online scams, helping you avoid unsafe web sites.

Enterprise Layered Security

- A modern enterprise security strategy uses a layered identity approach as the underpinning of its security.
- All enterprise systems, applications, information systems, facilities, buildings and rooms are assigned as enterprise risk.
- As the user digitally or physically approaches higher risk applications or a physical location the stronger authentication is used.
- As consider the enterprise firewall and the use of Id and passwords for login.

Implementing a Layered Identity Strategy: Enterprise Layered

- This could take the form of digital certificates, security tokens, smart cards and biometrics. It could also take the form of transactional security.
- While the user may successfully use their Id and password, the transaction security software would examine the IP address that the user is coming in from, their geographic position, the time of day, the type of physical computer the user is using and their behavioral pattern.
- If any of these differ from the past, then system alarm bells may start ringing resulting in the user being asked more personal questions, the action being stopped.

Extended Validation (EV) Certificate

- An extended validation (EV) certificate is a data security or anti-fraud measure recommended in 2006 by the Certificate Authority Browser Forum.
- Certificate Authority/Browser Forum (CAB Forum): An open voluntary association of certification authorities and software developers.
- The first version of the *Extended Validation SSL Certificate Guidelines* was ratifed in June 2007.
- The EV identity verification process requires the applicant to prove exclusive rights to use a domain, confirm its legal, operational and physical existence, and prove the entity has authorized the assurance of the Certificate.

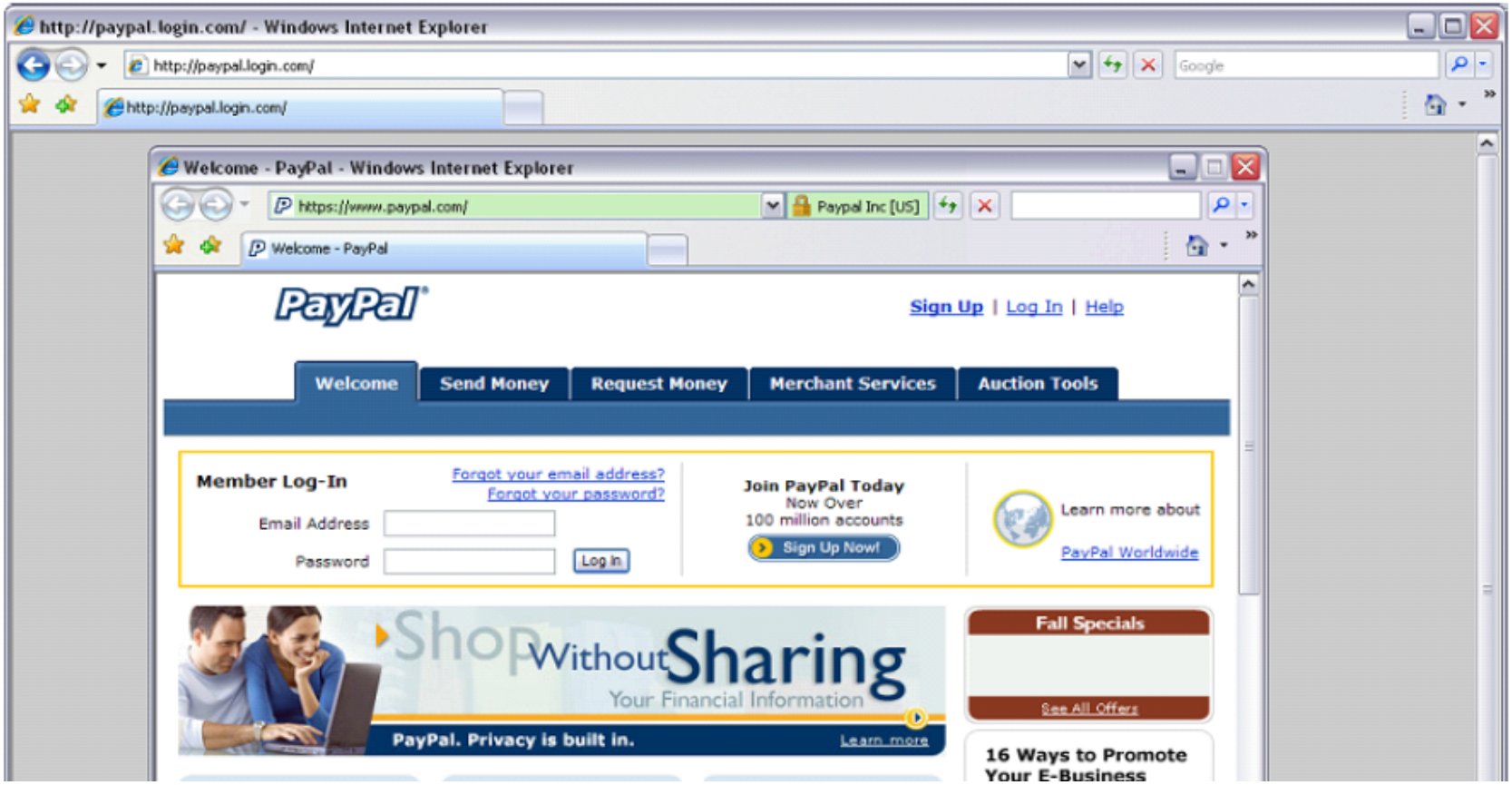
Extended Validation (EV) Certificate

- EV Certificates provide a higher level of validation and are available to all business and government entities, but are not available to individuals.
- The EV process is more rigorous and detailed than for any other Certificate and will require additional steps, which may include obtaining signatures from several people within the applying company, legal verification of the business's existence, etc.

The primary purposes of an EV Certificate

- To identify the legal entity that controls a website which provide a reasonable assurance to the user of an Internet browser that the website which the user is accessing is controlled by a specific legal entity identified in the EV Certificate by name, address of Place of Business, and Registration Number.
- To enable encrypted communications with a website which facilitate the exchange of encryption keys in order to enable the encrypted communication of information over the Internet between the user of an Internet browser and a website.

Designed for Banks and Large E-commerce sites



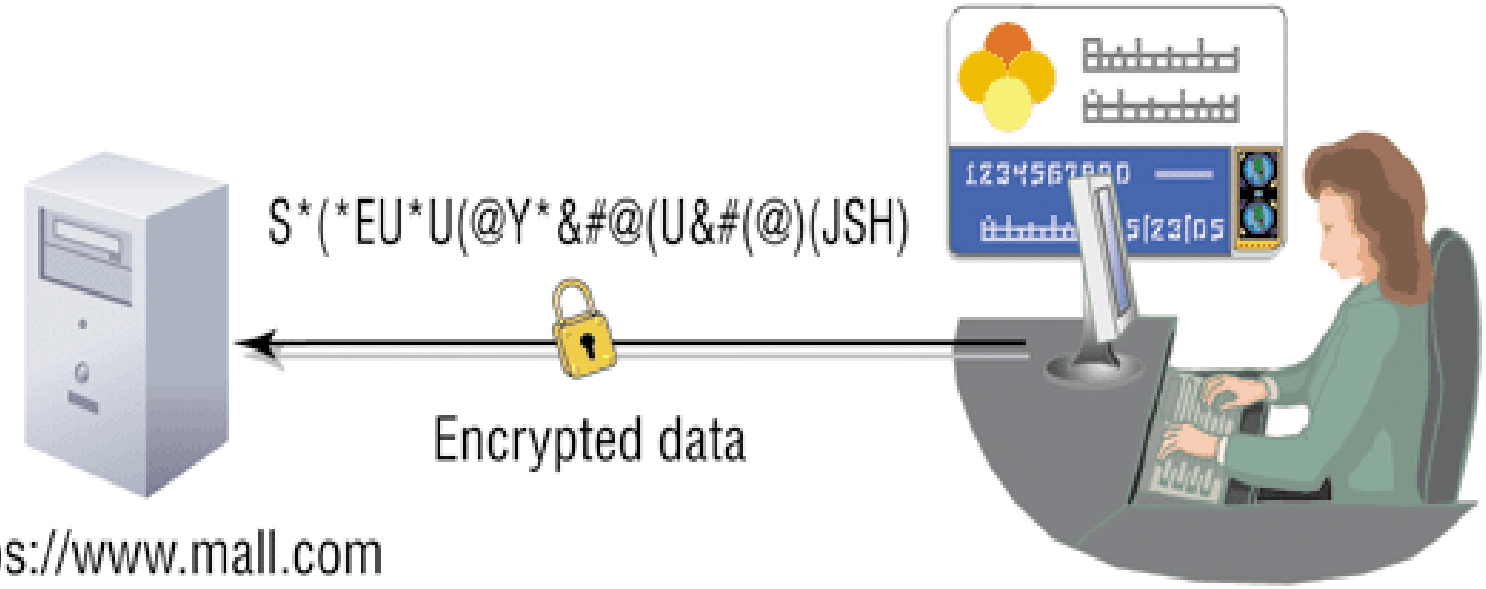
SSL Certificate

Secure Sockets Layer (SSL)

- Digital certificates combined allows for encrypted communications to occur between Web browser and Web server

FIGURE 8.34 • Secure Sockets Layer (SSL)

SSL encrypts data sent over the Web and verifies the identity of the Web server.



What is SSL Certificate?

- SSL (Secure Sockets Layer) is the transaction security protocol used by websites to protect online communications.
- The most common use of SSL is to provide protection for confidential data, such as personal details or credit card information, entered into a website.
- Ecommerce security cannot be an after-thought in your business plans. Today's online shoppers look for the visual cues provided by SSL Certificates, such as the closed padlock and the “https”.

Extended Validation SSL Certificate

- **Show your customers that your site is secure.** Our Extended Validation SSL Certificate features our instant verification green address bar, so your customers can easily see that they're protected. Provide your customers with the highest level of online assurance.
- **When customers see their address bar change to green, they know they can trust your business.** That's because the inspection process for an Extended Validation SSL is more extensive than for any other type of security certificate, verifying your organization's identity, the validity of your request and the overall legitimacy of your business.

- **How can I recognize websites using EV SSL Certificates?**

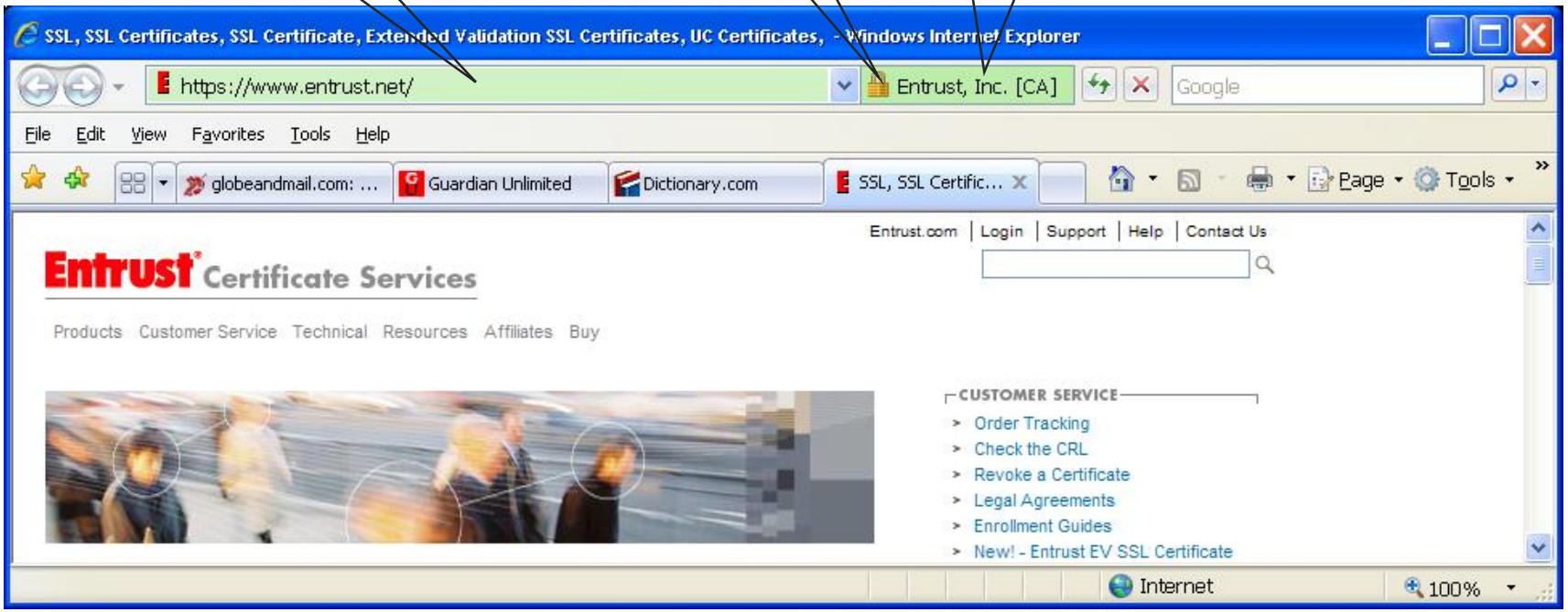
  A website using EV SSL Certificate will activate highly visible indicators directly on the browser address bar:
- **The green address bar, https:// and the padlock icon**
- **The name of the Organization that owns the website and the name of the Certification Authority that issued the EV SSL Certificate.**

Websites using EV SSL Certificates

Assumed name, registered name and country alternating with the issuer's name

Golden padlock

Green address bar



Remote Access Authentication

- Remote access authentication is the process whereby computer users can securely communicate with a network.
- A shared theme to all of these methods is the use of a digital certificate that contains information that identifies the user to a server and provides their credentials.
- Remote access authentication protocols make it safer to conduct business online as well as use ATMs.

RADIUS

- Most modern wireless networks do user authentication using Remote Authentication Dial-In User Service (RADIUS) protocol.
- RADIUS handles the overall authentication process of the user's session on the wireless device as well as also handling the authorization and auditing.
- The RADIUS system takes the (EAP) Extensible Authentication Protocol Authentication Method, challenges the user with the appropriate authentication method, receives the authentication response and then verifies it.

RADIUS

- If the authentication is successful, the RADIUS server will then authorize IP addresses, the tunneling protocol used to create virtual private networks.
- Further, the RADIUS server keeps tracks of when a user session begins and ends.
- For senior executives, who do require quite open access to the applications and information systems via their wireless device.
- Issue them with something like a secureID from (Rivest-Shamir-Adleman)RSA one time password generator and have the executives be required to enter this in order to authenticate their wireless device to the network. RSA algorithm

Policy-based encryption

- The Policy Based Encryption gateway automatically encrypts specific emails based on company-defined policies – that is, a set of rules designed to analyze all email, and encrypt any email that matches the pre-defined conditions.
- The concept of policy-based encryption is a promising paradigm for trust establishment and authorization in large-scale open environments like the Internet and Mobile Networks.
- On policy-based encryption which allow to encrypt a message according to a policy so that only entities fulfilling the policy are able to decrypt the message.

Policy-based encryption

- More generally, policy-based encryption belongs to an emerging family of encryption schemes sharing the ability to integrate encryption with access control structures.
- A policy-based encryption scheme has to fulfill two primary requirements: on one hand, provable security under well defined attack models.
- On the other hand, efficiency, especially when dealing with the conjunctions and disjunctions of credential-based conditions.

E-Commerce

- Electronic commerce
  - Systems that support electronically executed business transactions
  - The fundamental purpose of e-commerce is to execute online transactions
- E-commerce is not new; however, recent rapid development of the Internet is surely responsible for the popularity of e-commerce.
- The new way of commerce through the Internet creates vast opportunities, but at the same time, it poses challenges.

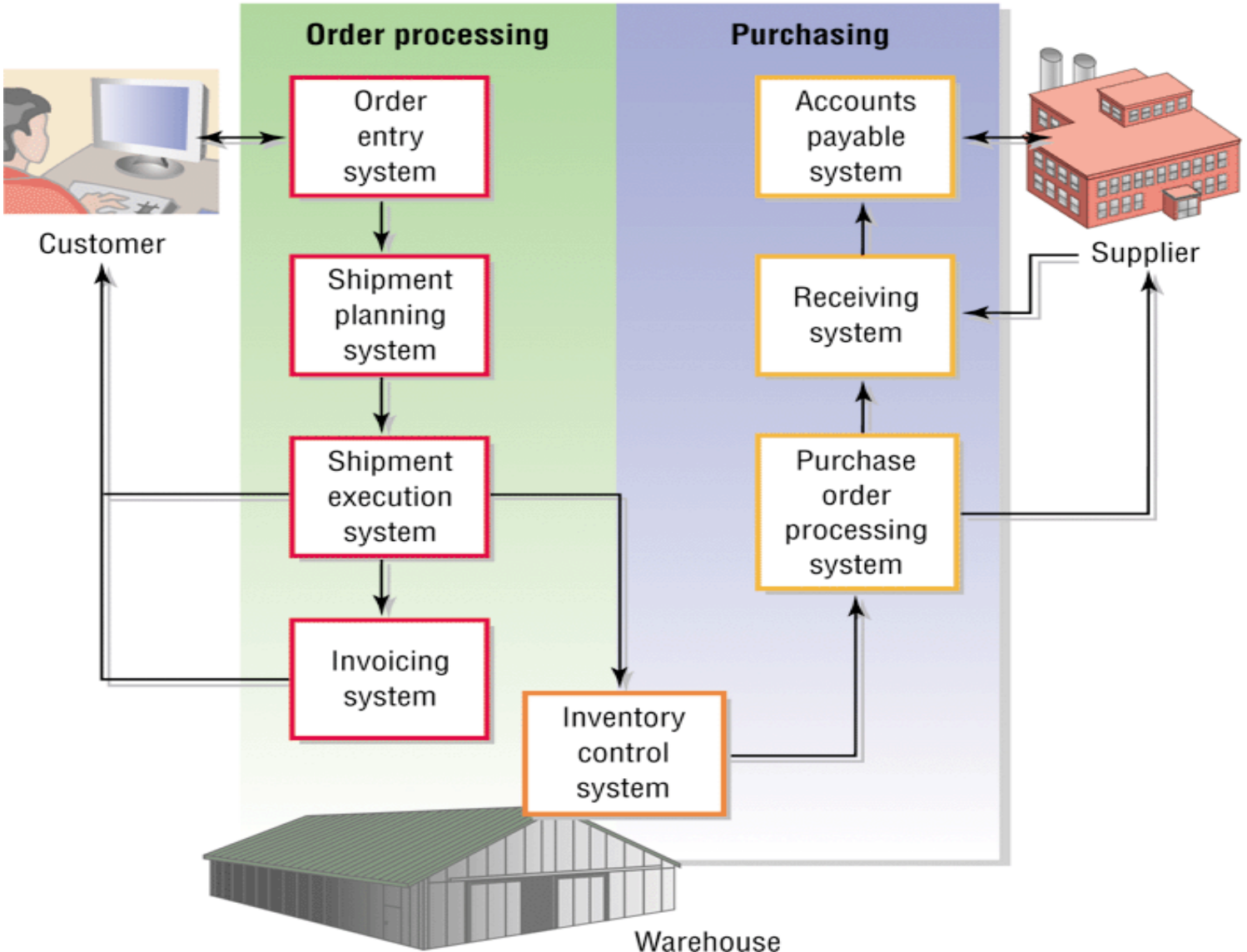
Types of E-Commerce

- Business-to-consumer e-commerce (B2C)
  - Connects individual consumers with sellers , cutting out the middleman
  - E.g. Amazon.com
- Business-to-business e-commerce (B2B)
  - Supports business transactions on across private networks, the Internet, and the Web
- Consumer-to-consumer e-commerce (C2C)
  - Connects individual sellers with people shopping for used items
  - E.g. ebay.com

Different Transaction Processing for Different Needs

FIGURE 8.6 • Transaction processing system interaction

Transaction processing typically makes use of many interconnected systems and subsystems.



Thank You