

CONTROL, AUDIT AND SECURITY OF INFORMATION SYSTEM

2.1 CONTROLS OF IS

- Methods, policies and procedures
- Ensures Protection of Organization's assets
- Ensures accuracy and reliability of records and operational adherence(support) to management standards

GENERAL CONTROLS

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

APPLICATION CONTROLS

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

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

PROTECTING THE DIGITAL FIRM

The **Digital Firm** is a general term for organizations that have enabled core business relationships with employees, customers, suppliers, and other external partners through **digital** networks

- **On-line transaction Processing:**

Transactions entered online are immediately processed by computer

- **Fault –tolerance computer systems:**

Contain extra hardware, software, and power supply components

- **High availability computing:**

Tools and technologies enabling system to recover from a crash.

- **Disaster recovery plan**

Runs business in event of computer outage (a period when a power supply or other service is not available or when equipment is closed down).

- **Load Balancing:**

Distributes large number of requests for access among multiple servers.

- **Mirroring:**

Duplicating all processes and transactions of server on backup server to prevent any interruption.

- **Clustering:**

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

2.2 AUDIT AND TESTING OF IS

OBJECTIVES

- Ensure computer based financial and other information reliable
- Ensure all records included while processing
- Ensure protection from frauds.

AUDITING AROUND COMPUTER

- Take ample inputs and manually apply processing rules and compare output with computer output

AUDITING THROUGH COMPUTER

- Establish audit trail (a record of the changes that have been made to a database or file) which allows examining selected intermediate results
- Control totals provide intermediate checks.
- Facility to trace transaction value and print intermediate results
- Selective printing of records meeting criteria specified by auditor.

- For example Inactive accounts, overactive accounts, accounts with high balance
- Comparing credit and debit balances
- Ensures logs are kept of who did what in critical data entry and processing to fix responsibility. Called an audit trail.
- Auditor's own check input and excepted outputs.

AUDITING WITH COMPUTER

- Extracting database on the specified criterion for inspection (e.g. Student with wide disparity in marks in two subjects)
- Totalling specified subset data for check
- Procedure to check sale discounts
- Process with independent data file created by auditor and v rify to see if system is per specifications

TESTING

1. PROGRAM TESTS

- Program tests with test data
- Normally individual modules tes ed then integration testing is done
- Test boundary conditions
- Test using loop counts

2. SYSTEM TESTS

- Results from a program fed as a input to a succeeding program.
- A string of programs run one after another
- All programs in a complete system are tested together as whole .Tested using unreasonable data a d non-key data besides normal test data for whole system.

3. PILOT TESTS

- Use data from manual system to test system when it is first implemented .If it is modification of earlier computer based system use data and output from that system.

4. PARALLEL RUNS

- Run both manual and computer based systems with same live data and see if both gives identical results
- If it is re-engineered (i.e. Modified) system run both old and new systems and compare results.

2.3 SECURITY OF IS

- Security means protection of data from accidental or intentional modification, destruction or disclosure to unauthorized persons

POTENTIAL THREATS TO SECURITY

- Natural disasters such as fire , floods , earthquakes
- Accidents such as disk crashes ,file erasure by inexperience operators
- Theft/erasure of data by disgruntled employees
- Frauds by changing programs, data by employees
- Industrial espionage (Spying involving corporations is known as industrial **espionage**)
- Viruses/Worms
- Hackers who break into systems connected to the int rnet
- Denial of service attacks by flooding with mail

HOW TO PROTECT DATA /PROGRAMS

- Regular back up of data bases everyday/or week depending on the time critically and size
- Incremental back up at shorter intervals.
- Backup copies kept in safe remote locations-particularly necessary for disaster recovery
- Duplicate systems run and all transactions mirrored if it is very critical system and cant tolerate any disruption b fore storing in disk
- Physical locks
- Password System
- Biometric a thentication(Fig: Finger Print)
- Encrypting sensitive data /programs
- Identification of all persons who read or modify data and logging it in a file
- Training employees on data care/handling and security
- Antivirus software
- Firewall protection when connected to internet

SECURITY COMPLEMENTARIES

- Data integrity is concerned with quality and reliability of raw as well as processed data

- Data privacy is concerned with protecting data regarding individuals from being accessed and used without permission/knowledge of concerned individuals.

TYPES OF SECURITY LAYERS

1. Consumers Layered Security Strategy
2. Enterprise Layered Security Strategy

2.4 CONSUMER LAYERED SECURITY STRATEGY

- Extended validation (EV) SSL certificates
- Multifactor authentication (Multifactor authentication (MFA) is a security system that requires more than one method of authentication from independent categories of credentials to verify the user's identity for a login or other transaction.)
- Single Sign-on (SSO) (Single sign-on (SSO) is a session/user authentication process that permits a user to enter one name and password in order to access multiple applications.)
- Fraud detection and risk based authentication
- Transaction signing and encryption
- Secure Web Ghimire, Dept and-mail
- Open fraud intelligence network

2.5 ENTERPRISE LAYERED SECURITY STRATEGY

- Workstation application whitelisting (Application whitelisting is a computer administration practice used to prevent unauthorized programs from running)
- Workstation system restore solution
- Workstation and network authentication
- File, disk and removable media encryption
- Remote access authentication
- Network folder encryption
- Secure boundary and end-to-end messaging
- Content control and policy-based encryption
- Practice of combining multiple mitigation security controls to protect resources and data

- Also known as layered defense.

2.6 EXTENDED VALIDATION AND SSL CERTIFICATES

SSL CERTIFICATE

- SSL Stands For Secure Socket Layer
- It is standard security technology for establishing an encrypted link between a web server and a web browser. This link ensures that all data passed between the web server and browsers remain private and integral.
- To be able to create an SSL connection a web server require SSL Certificate
- SSL Certificate are small data files that digitally bind a cryptographic key to an organization's detail. When installed on web server it activates the padlock and the http protocol (over port 443) and allows secure connections from a web server to a browser.

Typically SSL is used to secure credit card transactions, data transfer and logins and more recently is becoming the norm when securing browsing of social media sites.

- SSL certificate bind together
 1. A domain name, server name or hostname
 2. An organizational identity (i.e. Company name and location)
- An organization needs to install the SSL Certificate onto its web server to initiate secure sessions with browsers.
- Depending on the type of SSL Certificate applied for the organization will need to go through different levels of vetting
- Once installed, it is possible to connect to the website over <https://www.domain.com> as this tells the server to establish a secure connection with the browser.
- Once a secure connection is established, all web traffic between the web server and web browser will be secure. Browsers tell visitors a website is SSL secure via several visible trust indicators.

SSL CERTIFICATE EXAMPLE

- Consider an example of <http://facebook.com>



- The green color over padlock and https indicates Facebook is SSL Certified. This tells that the connection between browser and Facebook is secure.

TYPES OF SSL CERTIFICATES

- Why there are different types of certificates?
 1. Some organizations need SSL simply for confidentiality Science, NEC.g. encryption
 2. Some organizations wish to use SSL to enhance trust in their security and identity e.g. they want to show customers they have been vetted and are a legitimate organizations (according to law; lawful)

There are basically three types of SSL Certificate

1. OV SSL CERTIFICATES

Assures the validity of a web site by verifying that the applicant is a legitimate business. Before issuing the SSL certificate, the CA performs rigorous validation procedures, including checking the applicant's business credentials (such as the Articles of Incorporation) and verifying the accuracy of its physical and web addresses.

2. DV SSL CERTIFICATES:

The validation procedure is less rigorous for a Domain Validated SSL Certificate. When issuing a Domain Validated SSL Certificate. When issuing a Domain Validated SSL Certificate, the CA checks only the applicant's name and contact information matches the registration information in the WHOIS database for a domain name associated with applied for SSL certificate

2. **EV SSL CERTIFICATES:** The Certificate application process itself is more through the validation criteria more rigorous for EV certification, whose applicants, at least initially, are limited to certain types of business entities and government agencies.

EXTENDED VALIDATION

1. Extended Validation or EV SSL, raises the bar on standard SSL validation processes, incorporating some of the highest standards in identity assurance to establish the legitimacy of online entities.

2. Certificate Authorities put applicant websites through rigorous evaluation procedures and meticulous documentation checks to confirm their authenticity and ownership
3. This systematic authentication process, also known as the extended validation standard, is based on a set of guidelines prescribed for CAs to adhere to when they receive a request for a digital certificate from an organization or business entity.

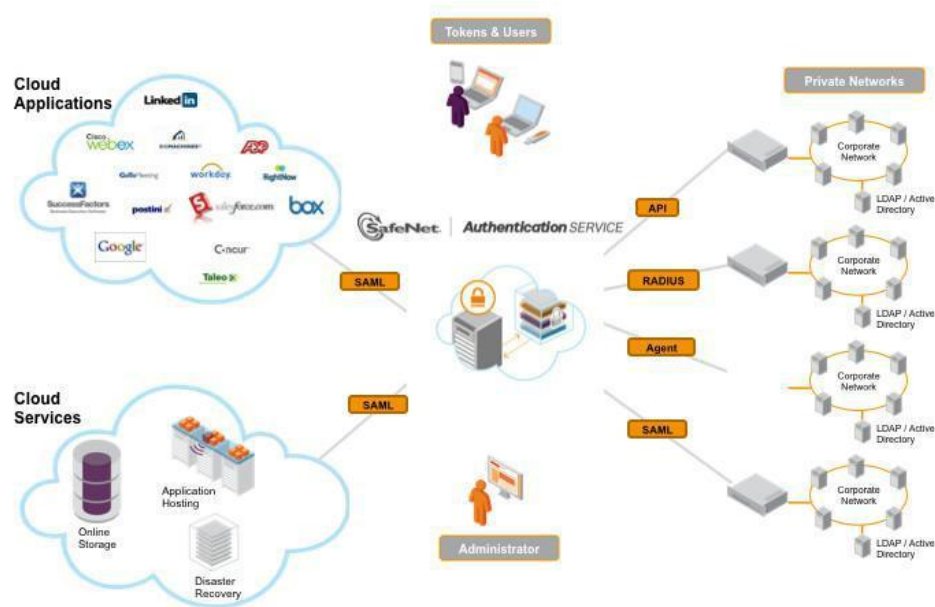
These guidelines include:

1. Establishing the legal, physical and operational existence of the entity
 2. Verifying that the entity's identity matches official records like incorporation and business licensing information.
 3. Confirming that the entity owns or has exclusive rights to use the domain mentioned in the application for certification
 4. Confirming that the request for an EV certificate has been authorized by the entity. The objectives of EV insurance process is to enable users to distinguish legitimate websites from phishing sites, building their trust in online commercial transactions and increasing participation.
- Consider the examples of <http://paypal.com/np>
 - The address bar turns from white to green, indicating to visitors the website is using Extended Validation SSL
 - Inside the green wrapper shows the legally incorporated company name. Extended SSL is the only way for a company to get its name displayed in the browser address bar.



2.7 REMOTE ACCESS AUTHENTICATION

- Remote access is the ability to get access to a computer or network from remote distance through wired or wireless connection
- Authentication is the method of providing the subject's identity.
- Examples: Password, Passphrase, PIN
- Validating remote subject's identity before accessing computer or network



WHY REMOTE ACCESS AUTHENTICATION?

- To prevent
- Accessing private data and information transferring between server and users i.e. Channel attack.
- Direct attacks from hackers into network
- Brute force, software attacks

AUTHENTICATION METHODS

- Biometrics
- Passwords
- Cognitive passwords
- Card Based
- One-time or Dynamic Passwords(token Based)

IMPORTANCE TODAY?

- Today everything is electronics and internet based like e-banking, e-commerce ,e-learning ,e-governance ,m-banking ,etc.
- Companies have many branches worldwide so data and information are distributed among branches offices.

- User do transaction remotely using internet using different handheld devices.
- All information of enterprise are centralized at server which is shared/distributed remotely among concerned people worldwide.

2.8 CONTENT CONTROL AND POLICY BASED ENCRYPTION

- Services for the security of email content in an organization
 - Email content like:
 - Credit card no, account information, etc.
 - Organization vital information, customer vital information

EMAIL CONTENT CONTROL

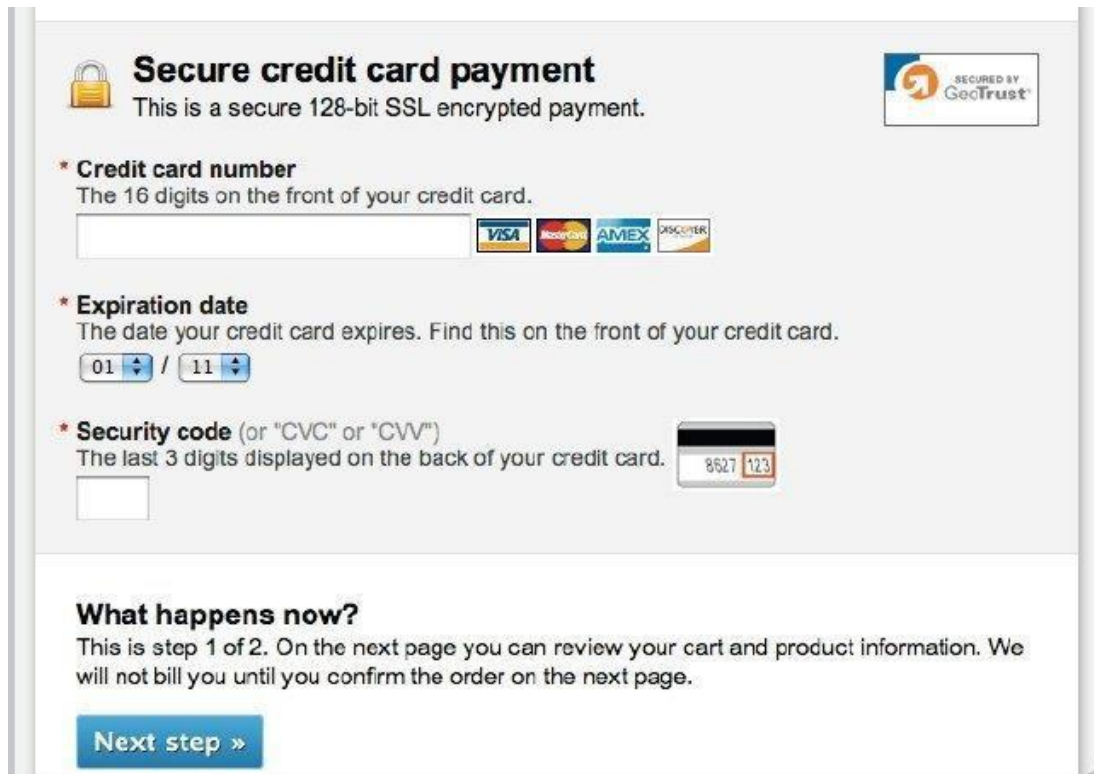
- This service contains the rules that defines: -
 - whether an email is to be encrypted or not. -
 - which block or header in email to be encrypted

POLICY BASED ENCRYPTION (PBE)

- It's a service that encrypts specific emails based on policy
 - Set of rules designed to analyze all email
- PBE uses the Email Content Control rules to identify which email needs to be encrypted
- The PBE Service is managed through the same control panel that you use to manage your Anti-Virus
- PBE Service is closely integrated with the Email Content Control Service
 1. Atomically applies email encryption based on the organization's email security policies
 2. Data loss prevention AND email messages security policies are consistently and accurately applied.
 3. Eliminates email encryption key management, backup and administration burdens
 - uses software-as-a service(SaaS)infrastructure.

Security is a serious concern for many. Besides making payments actually secure by using SSL, tell people about it.

This is an example of a form made to look secure:



- Different background color (you can have that only for the credit card number field)
- SSL logo
- Written statement: “Secure credit card payment. This is a secure 128-bit SSL encrypted payment.”
- Explanations for expiry and security code

Note that if your audience is not tech savvy, they might not know what SSL and https are, so better to speak in plain terms

<http://conversionxl.com/how-to-design-an-ecommerce-checkout-flow-that-converts/>

Check for more information