THE INSTITUTE OF CHARTERED ACCOUNTANTS OF INDIA

(Set up by an Act of Parliament)

CHENGALPATTU DISTRICT BRANCH (SIRC)

(Formerly Known as Kanchipuram District Branch)

E- Newsletter
July 2024

Address : Flat No: 402, Fourth Floor No.1A, Periyalwar Street,
Sundaram Colony, East Tambaram, Chennai – 600059.
Phone : 044-22390098 | 8056244300 | 7550009811
Email : chengalpattu@icai.org
Website : www.chengai-icai.org

Contents

ARTICLES INVITED FROM MEMBERS

Note: Articles are invited from members for publishing in newsletter. The articles shall be either on the specific subject or a general article. Members can send their articles with Name, Membership Number, Mobile Number, Residential Address, Office Address & Photo to our E-mail id mentioned below:

E-mail id: chengalpattu@icai.org

Note: The views expressed in the articles published, are their own views and Chengalpattu District Branch does not endorse or take responsibility.

From the Chairman's Desk

My dear professional colleagues

It is with great pleasure that I extend my warmest greetings to each of you as we present another edition of our monthly journal for the month of July 2024.

Let me start my message by wishing all of you A very Happy CA Day to you all

As you all know, we are celebrating 1st of July evert year as Chartered Accountants day. CA day is being celebrated as a mark of respect for the dedication, expertise, excellence and integrity of Chartered Accountants who are all instrumental in shaping our profession. Chartered Accountants are always remembered and respected for our commitment to excellence and unwavering professionalism. On this CA DAY (1st of July) let us all celebrate the spirit that defines Chartered Accountants.

Our CA Journal serves not only as a record of memory but also serves as a medium for enriching the knowledge and spirit of continuous learning. It serves as a resource for innovation, inspiration, professional development and collectively helps to elevate the standards of our profession.

In this issue, you will find articles with wealth of insights, analysis and perspectives contributed by our members. and thought leaders in the field. These pieces reflect our commitment to staying at the forefront of developments in finance, auditing, taxation, and beyond.I request everyone to go through this newsletter and I am confident that it will give new ideas and lead us towards greater success.

Thank you for your continued support and engagement with the CA Journal. Together, let us continue to uphold the highest standards of professionalism and contribute to the advancement of our profession.

Together, let us continue to elevate the standards of our profession and make a positive impact in the world.

Once again Happy CA Day to all.

Jai Hind

CA Narasimma Raghavan R
Chairman

CPE MEETING

Topic : INVESTOR AWARENESS PROGRAM - WEALTH CREATION THROUGH MUTUAL FUNDS

Speaker : MR. RAMAKRISHNAN V NAYAK, DIRECTOR - DAKSHIN CAPITAL PVT LTD

Date : 1st June 2024, Saturday

Time : 6.00 PM to 8.00 PM

Venue : Our Branch Premises

CPE MEETING

Topic : PRACTICAL ASPECTS OF INFORMATION SYSTEMS AUDIT, CYBER SECURITY & DATA PROTECTION AND AUDIT AUTOMATION

Speaker : CA. AJAY MEHTA, CA. SATHYABAMA R & CA. NISHANTH KRISHNA PORURI & CA. NAREN VARMA KALIDINDI

Date : 08th June 2024, Saturday

Time : 9.30 AM to 1.30 PM

Venue : Our Branch Premises

TOPIC : BRANCH DAY CELEBRATION AND ARTIFICIAL INTELLIGENCE IN ICAI, OFFICE & AUDIT

Speaker : CA. DAYANIWAS SHARMA, CCM & CHAIRMAN OF AI, CA. AANAND P, MCM AND CA. REKHA UMA SHIVE, RCM

Date : 20th June 2024, Thursday

Time : 5.00 PM to 8.00 PM

Venue : Our Branch Premises















CPE MEETING

Topic: TWO DAYS WORKSHOP ON GST DEMANDS & APPELLATE REMEDIES

Speaker: CA. VISHAL V, CA. RENUKA S, CA. BHARATH KUMAR N K, CA. GANESH PRABHU B, CA. VIRAL M KHANDHAR & CA. SAMPATH KUMAR VV

Date: 21st & 22 nd June 2024, Friday and Saturday

Time: 10.00 AM to 5.00 PM

Venue: Our Branch Premises


Chengalpattu Branch
of SIRC OF ICAI
Intro. to Appeals under GST
&
Filing of Appeals

Programme : Yoga Day
Date : 21th June 2024, Friday
Venue : Our Branch Premises

CPE MEETING

Topic: INTERNATIONAL MSME DAY - ENRICHING THE ENTREPRENEURSHIP SKILLS FOR CA'S

Speaker: DR. SUBRAMANIAM R

Date: 26th June 2024, Wednesday

Time: 5.00 PM to 8.00 PM

Venue: Our Branch Premises

Programme : CA Run
Date : 30th June 2024, Sunday
Venue : Our Branch Premises













Programme : CA Day
Date : 1st July 2024, Monday
Venue : Our Branch Premises















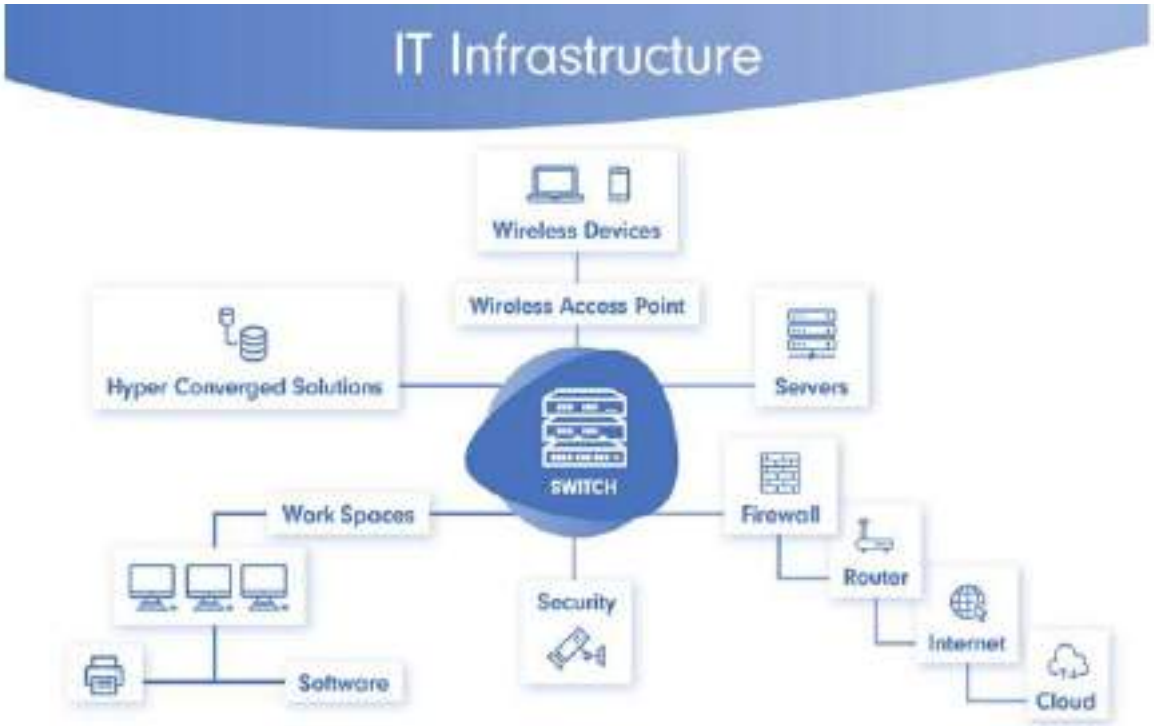


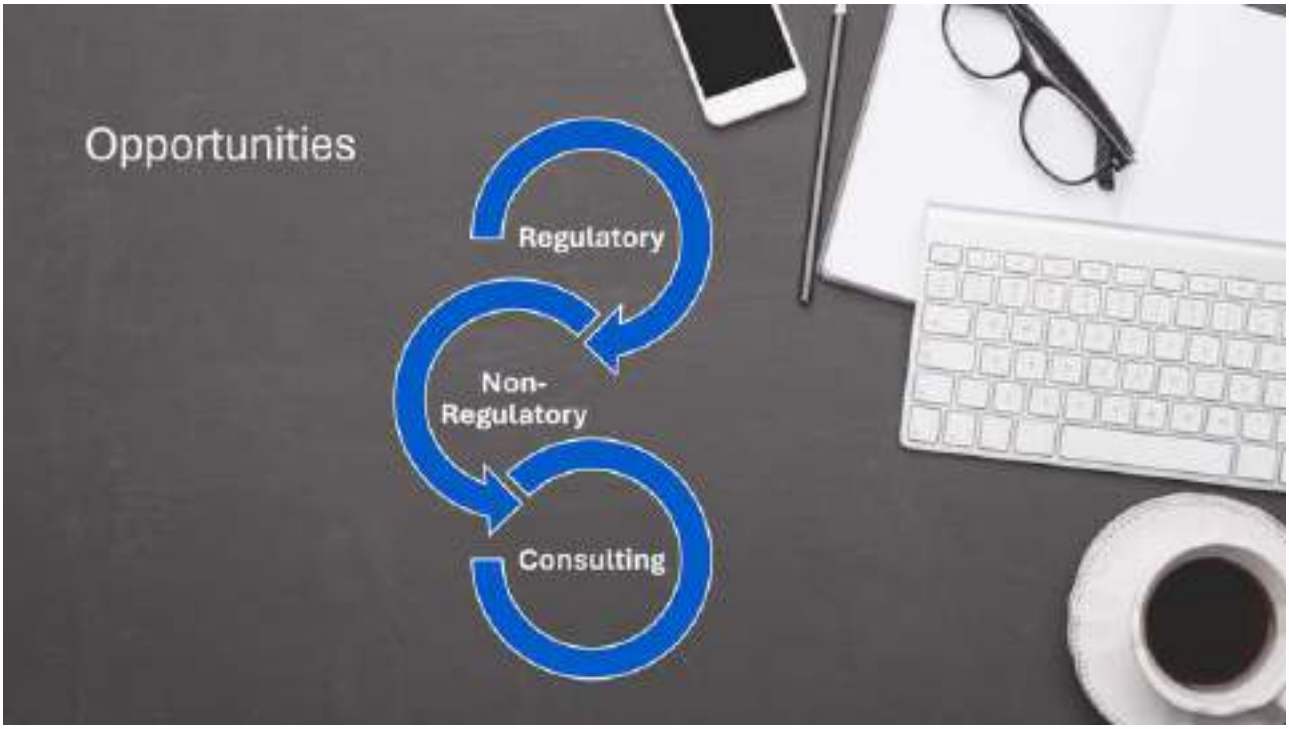
CA. AJAY MEHTA

Practical Aspects of Information Systems Audit

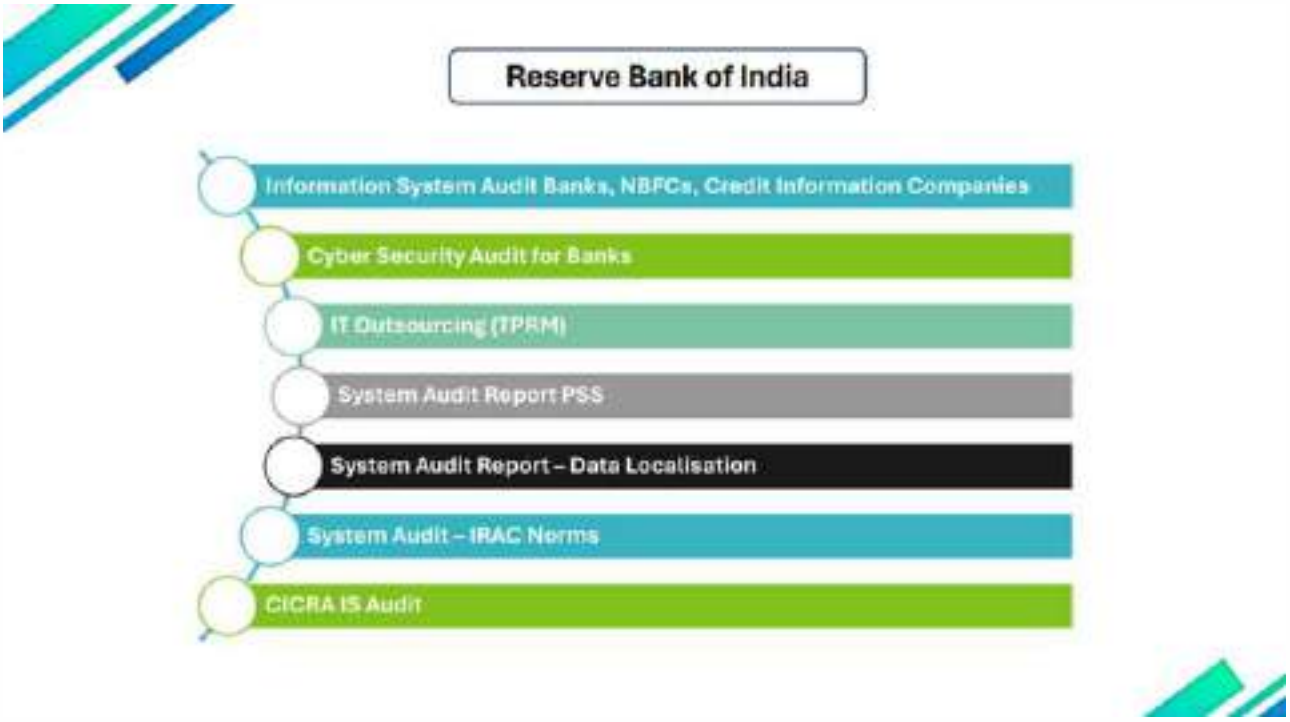
Introduction

Information System	Information System is a combination of resources that **collects, processes, stores, and communicates** information to achieve organizational objectives.
Information System Components	Combination of **hardware, software, infrastructure, and trained personnel**
Information System Audit	The purpose of an Information System Audit is to **evaluate the effectiveness** of an organization's information system controls.




Opportunities
Regulatory
Non-
Regulatory
Consulting


Regulatory Bodies and IS Audit Requirements in India
Reserve Bank of India (RBI)
Securities Exchange Board of India (SEBI)
Insurance Regulatory and Development Authority of India (IRDAI)
National Housing Board (NHB)
National Bank For Agricultural and Rural Development (NABARD)
Unique Identification Authority of India (UIDAI)
Ministry of Company affairs (MCA) : Companies Act 2013
This is not exhaustive list



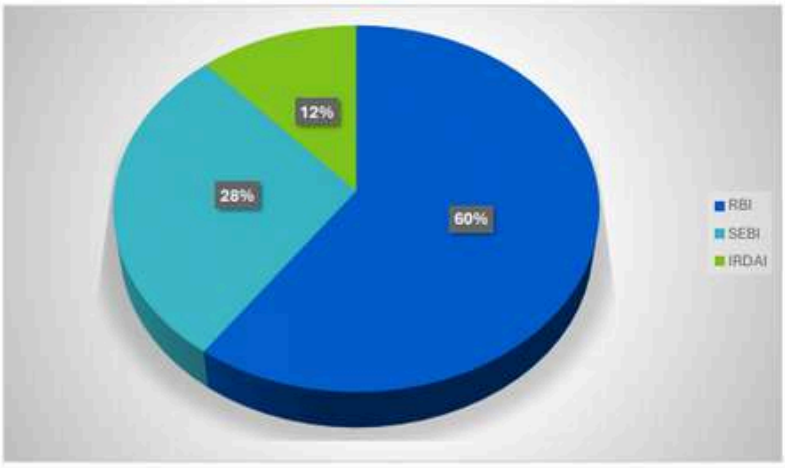
Securities and Exchange Board of India	Annual System Audit
	Cyber Security & Cyber Resilience
Insurance Regulatory and Development Authority of India	Cyber Security Assurance Audit
	Insurance Self- Network Platform (ISNP) Audit

POV : Quantitative Consolidated Opportunities

S.no	Eligible Entities	Count
1	Scheduled Commercial banks (Incl PSB, Pvt, Foreign)	78
2	Small Finance Banks	11
3	Payments Banks	4
4	Primary (Urban) Co-operative Banks	1,488
5	State Co-operative Banks	34
6	District central co-operative banks	355
7	Rural Regional Bank	43
8	All India Financial Institutions	4
9	Credit Information Companies	4
10	Non – Banking Financial Institution (Upper & Middle Layer)	415
11	Non – Banking Financial Institution (AUM less than 1000 CR)	8,842
12	Payment system operators	95
13	AUA / KUA Agencies	176
14	Stock Exchanges	7
15	Clearing Corporation	5
16	Depositories	2
17	Stock Brokers	4,889
18	Depository Participants	610
19	Insurers	78
20	Insurance Intermediaries	2,157
	Total	19,297

Note: This is just 25 % of coverage in terms of Quantitative requirement

POV : Quantitative Consolidated Opportunities



Note: This is just 25 % of coverage in terms of Quantitative requirement

Companies Act 2013 - IFC

IFC - Applicability

Responsibility	Type of Company		
	Public Limited (Listed)	Public Limited (Unlisted)	**Private Limited** *(refer note 1)**
Board / AC	IFC	IFCFR	**IFCFR**
Auditors	IFCFR	IFCFR	**IFCFR**

Note 1 - *Reporting not applicable if turnover less than INR 50 crores as per latest audited financials **AND** borrowings (from banks and FIs or any body corporate) less than INR 25 crores in the relevant financial year*

IFC – Responsibility or Accountability

S.no	Statutory Provisions	Area	Regulatory mandate	Applicability
1	Section 134 (5)(e) of Companies Act 2013	Directors Responsibility Statement	Board of Directors have to confirm that they have laid down IFC and that such IFC are adequate and were operating effectively	Listed Entities
2	Section 177 of Companies Act 2013	Audit Committee	Should evaluate IFC and risk management systems. Call on the auditors to comment on IFC	All Entities having an Audit committee
3	Section 149 (7), Schedule IV of the Companies Act 2013	Independent directors	Should satisfy themselves on the integrity of financial information and that financial controls and systems of risk management are robust and defensible	All Entities having independent directors
4	Section 143 (3)(i) of Companies Act 2013*	Auditors Report	Auditors have to report whether the company has adequate internal financial controls and the operating effectiveness of such controls	All Entities (Listed/ unlisted)
5	Rule 8 (5) of Companies Accounts Rules	Board of Directors report	The details in respect of adequecy of internal financial control with reference to financial statements	All Entities (Listed /Unlisted)

IFC – Framework

Source: ICAI GN ON IFC over FR

IFC – Information & Communication

Information Technology General Controls

- ITGCs include controls in the areas of access security, system change control, data centre and network operations.

Information Technology Application Controls

- Application controls relate to the transactions and master file, or standing data pertaining to each automated application system, and are specific to each application.
- They ensure the accuracy, integrity, reliability and confidentiality of the information and the validity of the entries made in the transactions and standing data resulting from both manual and automated processing.

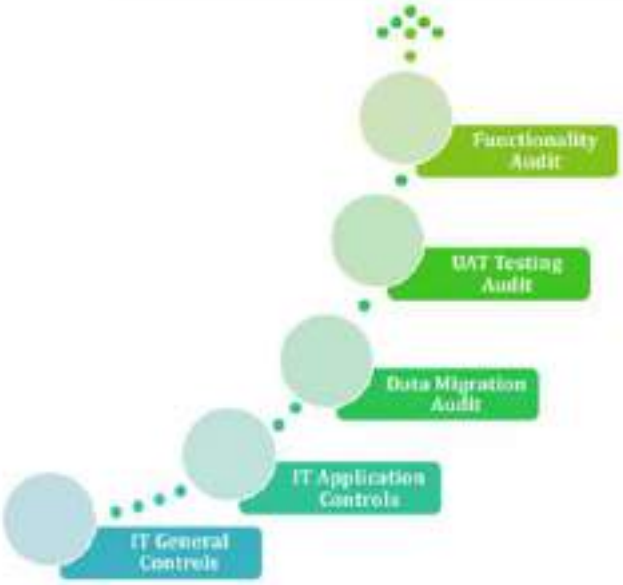
Source: ICAI GN ON IFC over FR

Companies Act 2013 Audit Trail

Audit Trail	Audit trail is record of what, when, & who, for **all type** of transaction (i.e., **Add, Modify, Delete**) **What** : What data input, modification, deletion was taken place in a transaction **When** : Date & Time Stamp **Who** : User executing the transaction
Applicability*	Applicable from 01st April 2023 to all categories of Companies which uses accounting software for maintaining its books of account.
Assessment Objective*	whether the audit trail feature is **configurable** (i.e., if it can be disabled or tampered with)?
	whether the audit trail feature was enabled/operated **throughout the year**?
	whether **all transactions** recorded in the software are covered in the audit trail feature?
	whether the audit trail has been **preserved** as per statutory requirements for record retention?

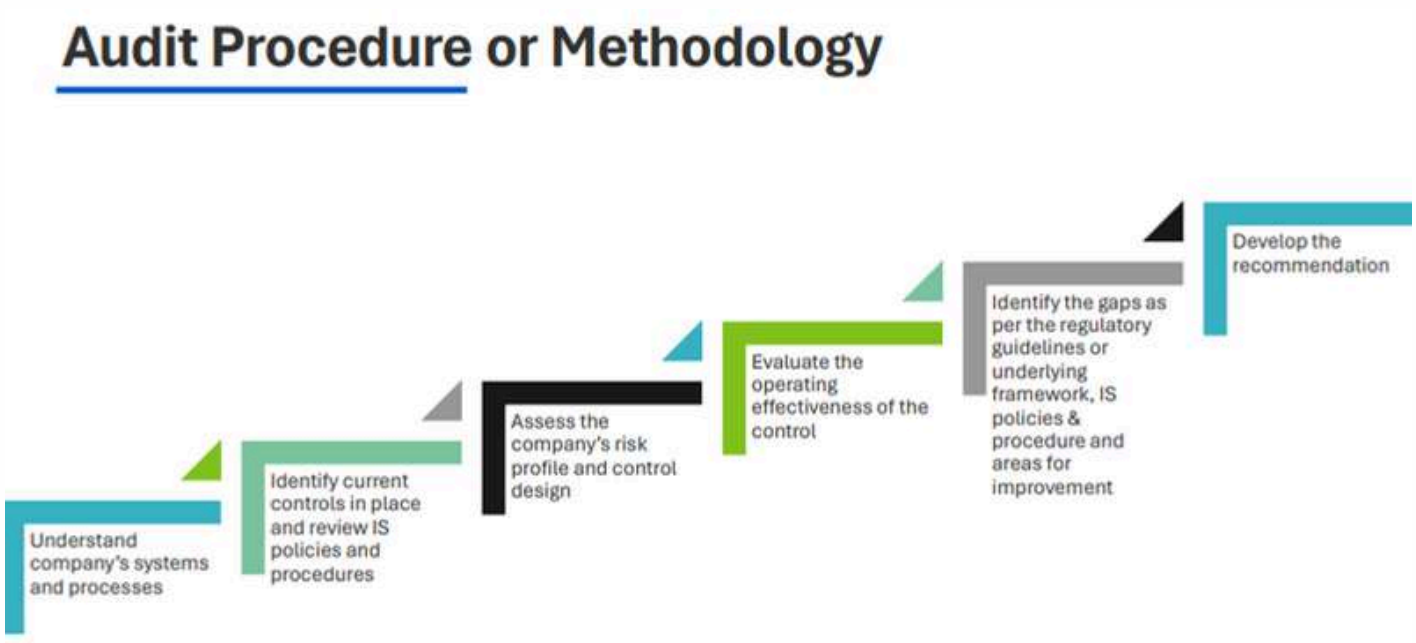
***Source: ICAI GN ON Audit Trail**

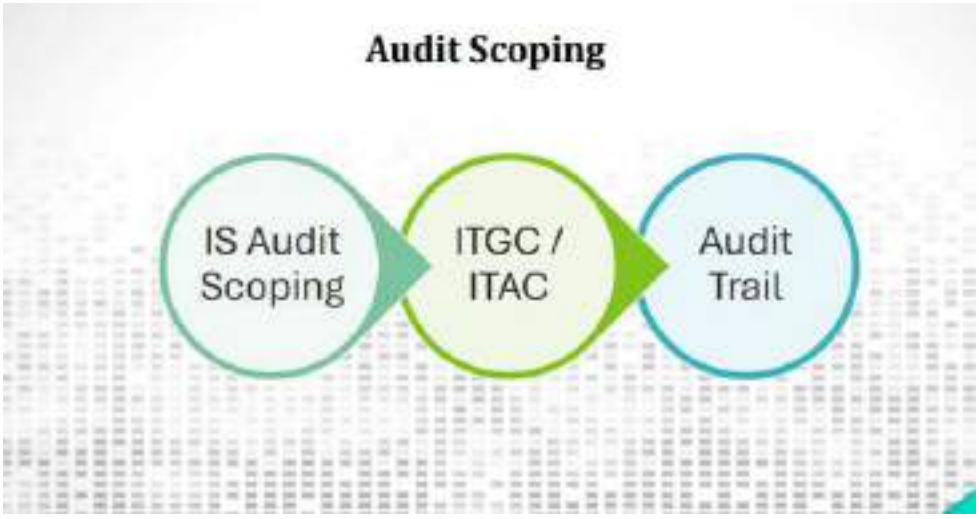
Non – Regulatory Information System Audit



Information Security Consulting opportunities


Practical Walkthrough
Audit Procedure or Methodology
Audit Scoping
Control Areas
Checklist Overview
Report Walkthrough


Audit Procedure or Methodology
Understand company's systems and processes
Identify current controls in place and review IS policies and procedures
Assess the company's risk profile and control design
Evaluate the operating effectiveness of the control
Identify the gaps as per the regulatory guidelines or underlying framework, IS policies & procedure and areas for improvement
Develop the recommendation

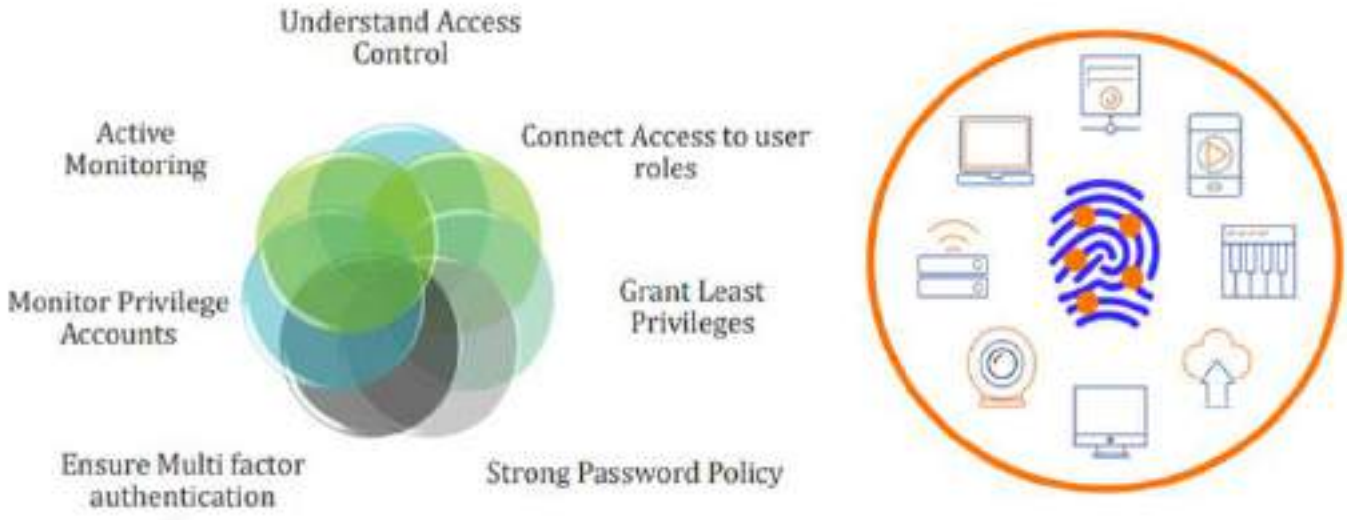

Audit Scoping
IS Audit Scoping
ITGC / ITAC
Audit Trail


Controls Areas
Information Security Governance
IT Risk Assessment
Business Continuity & Disaster Recovery
Access Management & Password Controls
Asset Management
Change Management
Incident Management
Logging and Monitoring
Backup and Restoration Controls
Patch & Vulnerability Management
Capacity Management
Physical and Environmental Security

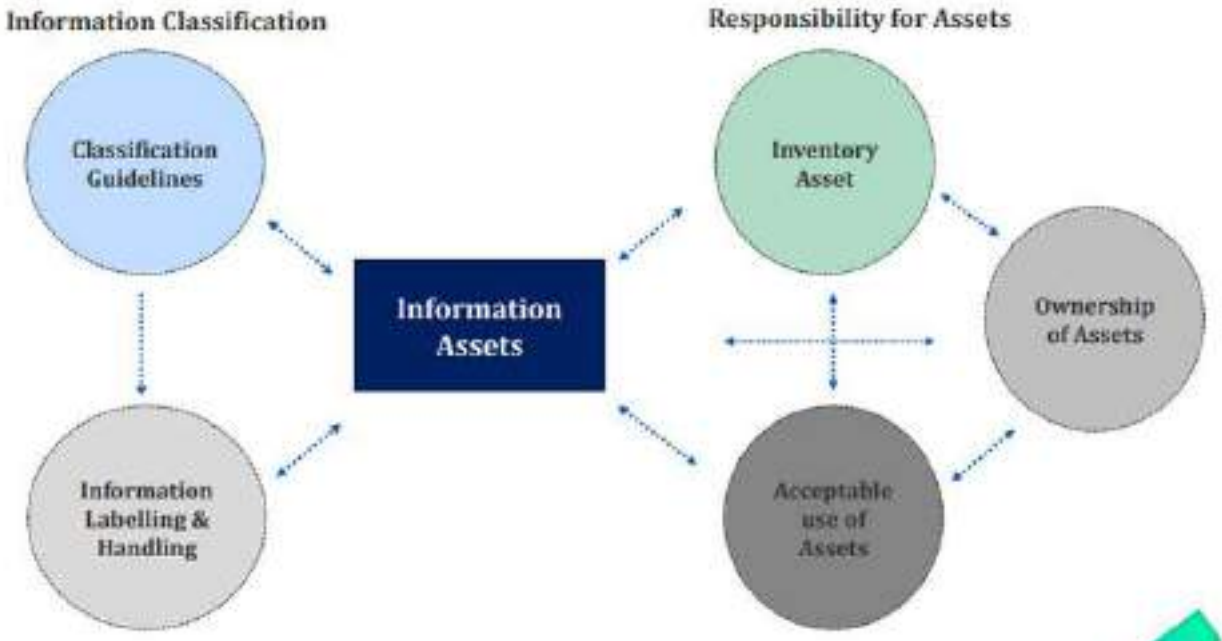
Controls Areas

- Network Security
- Data Security
- Human Resource Security
- IT Project Management
- Vendor/Third Party Risk Management
- Secure Testing and Source code Review
- E-mail Security
- Endpoint Hygiene

ACCESS CONTROL

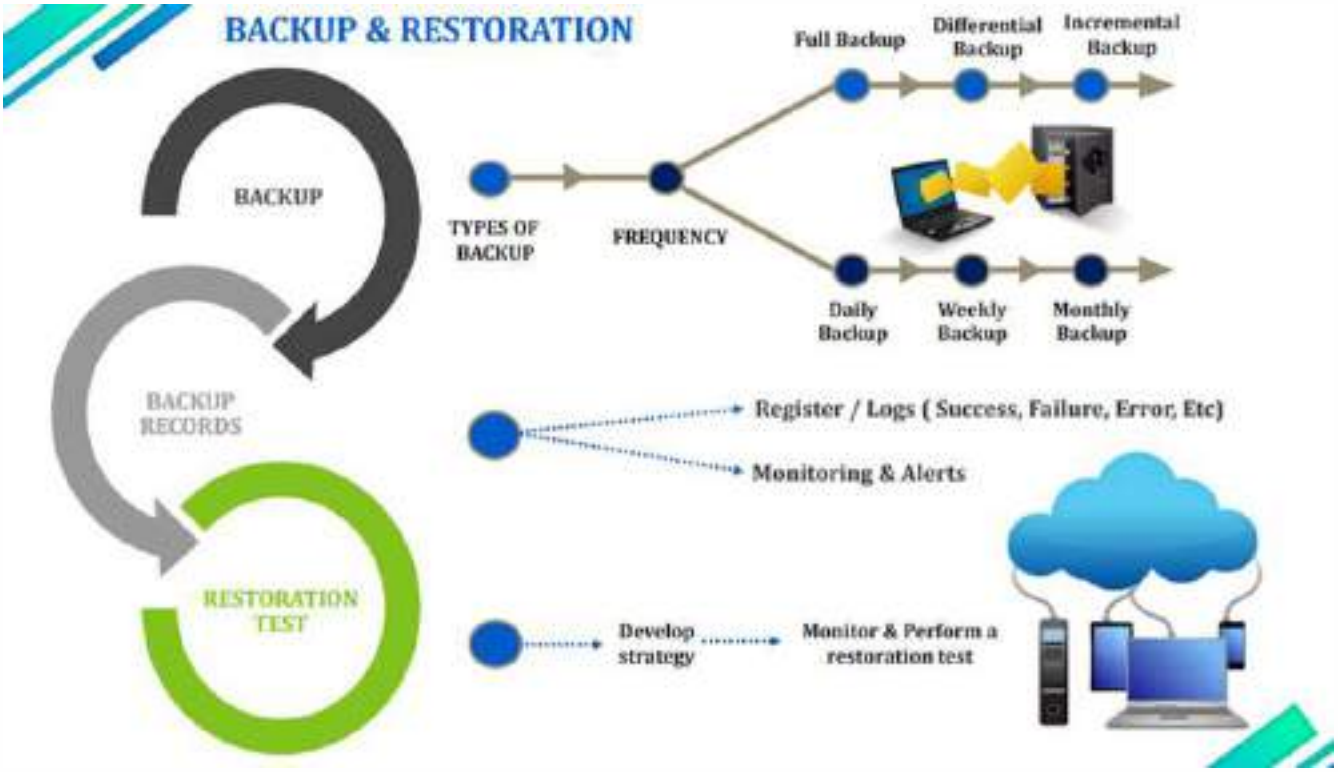


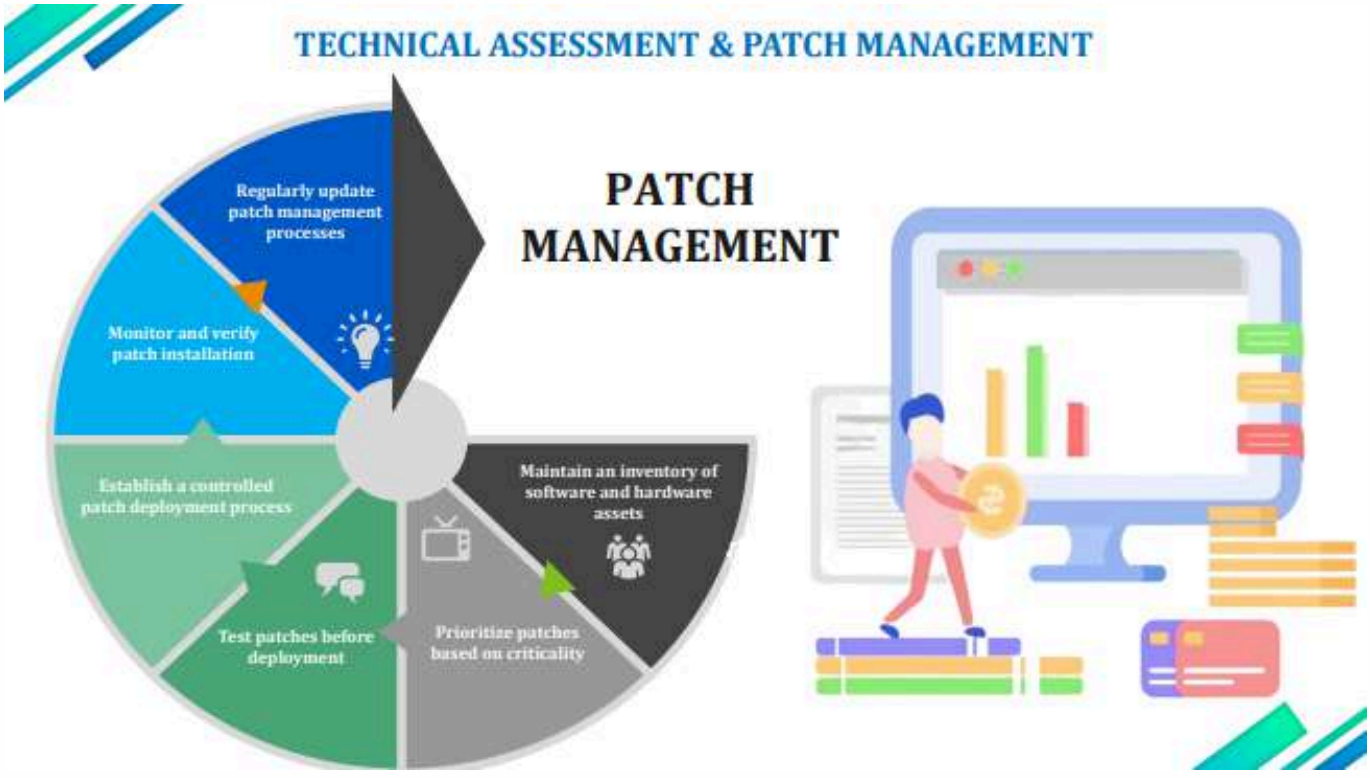
ASSET MANAGEMENT



CHANGE MANAGEMENT

- Initiation
- Change Request
- Change Evaluation
- Change Planning
- Change Testing
- Change Approval
- Change Implementation
- Change Review and Monitoring
- Documentation and Reporting
- Change Closure

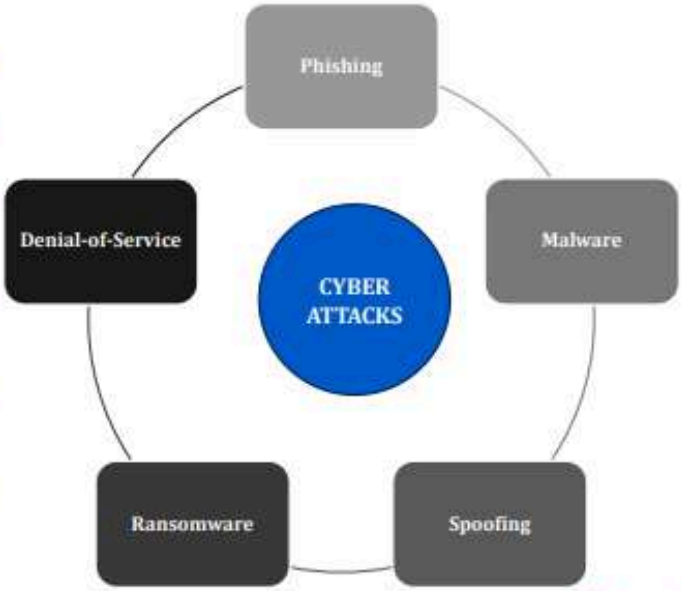

BACKUP & RESTORATION
BACKUP
BACKUP RECORDS
RESTORATION TEST
TYPES OF BACKUP
FREQUENCY
Full Backup
Differential Backup
Incremental Backup
Daily Backup
Weekly Backup
Monthly Backup
Register / Logs (Success, Failure, Error, Etc)
Monitoring & Alerts
Develop strategy
Monitor & Perform a restoration test


TECHNICAL ASSESSMENT & PATCH MANAGEMENT
PATCH MANAGEMENT
Regularly update patch management processes
Monitor and verify patch installation
Establish a controlled patch deployment process
Test patches before deployment
Prioritize patches based on criticality
Maintain an inventory of software and hardware assets

INCIDENT RESPONSE & MANAGEMENT

INCIDENT APPROACH

1. IDENTIFY Your Assets
2. PROTECT Your Assets
3. DETECT Incidents
4. RESPOND With a plan
5. RECOVER Normal Operations



ENDPOINT SECURITY

Endpoint such as Laptops, Mobiles, Desktop, IoT Devices / Sensors


Checklist Overview
Overview
Bank Branch IS Audit
Audit Trail


Report Walkthrough
Bank IS Audit
Application Audit
Audit Trail
IFC IT Controls


IS Audit Skill Set
50%
Audit Skill
Process Understanding
20%
Knowledge Upgradation
DISA / CISA / CEH / ISO 27001
30%
Practical Experience
encryption
privacy
phishing
online
data
protection
internet
threats

CA. SATHYABAMA R

CYBER SECURITY & DATA PROTECTION MEASURES FOR SAFEGUARDING SENSITIVE FINANCIAL INFORMATION

Agenda

- Sensitive Financial Information
- What is Cyber security – concepts Explained
- Cyber security threats /risks
- Measures of Cyber security
- Data Privacy – Definition of Personal Identifiable Information
- DPDP Act

Sensitive Financial Information

Personal : Bank account details, PAN, Adhaar card, investments, credit /debti card numbers, UPI id, Userid /passwords to various portals

Corporates : Budgets, strategy documents, Internal workings for capex, opex, performance data – anything that is not published publicly.

- Between June 2018 and March 2022, Indian banks reported 248 successful data breaches by hackers and criminals; the government notified Parliament on Aug 2, 2022
- The Indian government has reported 11,60,000 cyber-attacks in 2022. It is estimated to be three times more than in 2019. India has been the target of serious cyberattacks,
- Over 300 billion passwords are being used by humans and machines all over the world. (Cybersecurity Media)
- Between 2005-2020, there have been 11,762 major security breaches. (ID Theft Resource Center)
- The information security market is estimated to reach $170.4 billion by 2022. (Gartner)
- Hacking featured 45% of the total breaches, while 17% involved malware attacks and 22% involved phishing attacks. (Verizon)
- Cybersecurity risks are increasing day by day, feels 68% of the business leaders (Accenture)
- 86% of the breaches were financially driven while 10% were motivated by espionage. (Verizon)
- 88% of companies around the world experienced spear-phishing attempts in 2019. (Proofpoint)
- Human errors caused 95% of the total cybersecurity breaches. (Cybintsolutions)

Significance of Cyber Risk in the Financial Sector:

Types of Cybercrime:

- All businesses, regardless of size, are at risk. Small businesses may feel like they are not targets for cyber attacks either due to their size or the perception that they don't have anything worth stealing.
- Only a small percentage of cyber attacks are considered targeted attacks, meaning the attacker group is going after a particular company or group of companies in order to steal specific data.
- The majority of cyber criminals are indiscriminate; they target vulnerable computer systems regardless of whether the systems are part of a Fortune 500 company, a small business, or belong to a home user.

Online Scams	Identity Theft
Cyber Stalking	Denial of Service attack
Phishing attacks	Illegal Content
Malware(Trojan, Virus, Worms etc..)	Hacking

Types of Cybercrime:

Phishing

- Phishing is a fraudulent attempt, usually made through email, to steal your personal information.
- Phishing is the attempt to obtain sensitive information such as username, password and credit card details, often for malicious reasons through an electronic communication (such as)-mail).
- A common online phishing scam starts with an email message that appears to come from a trusted source(legitimate site) but actually direct % recipients to a fraudulent web site.

Denial of Service attack

- This is an act by the criminals who floods the Bandwidth of the victims network.
- In the DoS attack, a hacker uses a single internet connection to either exploit a software vulnerability or flood a target with fake request-usually in an attempt to exhaust server resources.
- On the other hand, DDoS attacks are launched from multiple connected devices that are distributed across the internet.
- DoS = When a single host attacks.
- DDoS = when multiple hosts attack **simultaneously and continuously**.

Malware

- It's malicious software (such as Virus ,Worms & Trojan) , which specifically designed to disrupt or damage computer system or mobile device.
- Hackers use malware for any number of reasons such as, extracting personal information or passwords, stealing money, or preventing owners from accessing their device.
- Viruses are programs that attach themselves to a computer or a file and then circulate themselves to other files and to other computers on a network. They usually affect the data on a computer and mobile device either by altering or deleting it.

ATM Skimming

- It is a technique of compromising the ATM machine by installing a skimming device on top of the machine keypad to appear as a genuine keypad or a device made to be affixed to the card reader to look like a part of the machine.
- Additionally, malware that steals credit card data directly can also be installed on these devices.
- Successful implementation of skimmers cause in ATM machine to collect card numbers and personal identification number codes that are later replicated to carry out fraudulent transaction.

Steps to protect from Threats:

- Social Engineering
- Data Leakage via Malicious Apps
- Unsecured Public WiFi
- End-to-End Encryption Gaps
- Internet of Things (IoT) Devices
- Spyware
- Poor Password Habits
- Lost or Stolen Mobile Devices
- Out of Date Operating Systems

Business Email Compromise

Business Email Compromise

Outsider Threats:

An **Outsider** threats are unauthorized entity outside the security domain that has the potential to harm an information system through destruction, disclosure, modification of data, and/or denial of service.

Defense Plan:

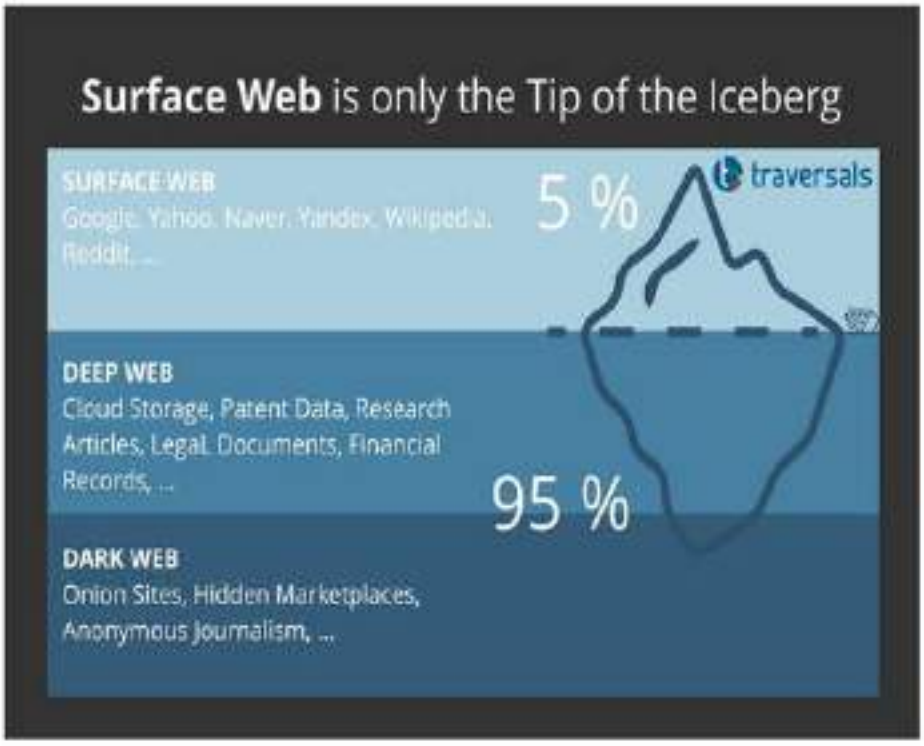
- Endpoint threat detection
- Process execution
- Visibility
- Data classification
- A platform approach
- Network integration

Insider Threats:

An **Insider** threat in cybersecurity refers to an individual using their authorized access to an organization's data and resources to harm the company's equipment, information, networks, and systems.

Defense Plan:

- Identify and discover where your sensitive files live.
- Train your employees to adopt a data security mindset.
- Apply security analytics to alert on abnormal behaviors.
- Determine who has access to that data and who should.
- Monitor activity, files, and emails on your core data sources.
- Maintain a least privilege model through your infrastructure.



THE CIA TRIAD OF INFORMATION SECURITY

- **Confidentiality:** Ensures that data or an information system is accessed by only an authorized person.
- **Integrity:** Integrity assures that the data or information system can be trusted. Ensures that it is edited by only authorized persons and remains in its original state when at rest.
- **Availability:** Data and information systems are available when required.

CONFIDENTIALITY AVAILABILITY INTEGRITY

What is cyber security?

- Cyber Security is the protection of internet-connected systems, including hardware, software & data, from cyberattacks.
- In a computing context, security comprises cybersecurity and physical security – both are used by enterprises to protect against unauthorized access to data centers and other computerized system.
- Cyber security is a subset of Information security, which is designed to maintain the confidentiality, integrity and availability of data.

Importance of Cyber Security:

7 Layers of Security:

Types of Cyber Security:

Application Security:

- **Access Management Controls**
  - User Access Creation
  - User Access Modification
  - User Access Revocation
  - Privilege access
  - Audit Trails
- **Changes Management Controls**
  - Change Register
  - User Acceptance Testing
  - Review of Changes
- **Vulnerability Scanning of the Application**
- **Penetration Testing of the Application**
- **Patch Management**

Database Security:

- **Protect Sensitive Data from**
- Unauthorized Disclosure
- Unauthorized Modification
- Denial of service attacks

- **Security Controls:**
  - Security Policy
  - Access control models
  - Integrity Protection
  - Privacy Problems
  - Faults Tolerance and Recovery

Operating System Security:

Authentication

Username / Password

User Card / Key

User Attribute

Multi Factor Authentication

One Time Passwords:

Random Numbers

Secret Key

Network Password

Program Threats:

Trojan Horse

Trap Door

Logic Bomb

System Threats:

Worm

Port Scanning

Denial of service

Cloud Security:

What is Cloud Security?

Cloud Security is the set of control-based technologies and policies designed to adhere to regulatory compliance rules and protect information, data applications and infrastructure associated with cloud computing use.

Cloud Security:

- Agentless
- API Driven
- Highly Scalable
- Standard
- Controls
- One Touch Security

Network Security

- Network security involves protecting networks from external threats, including unauthorized access, viruses, malware, denial of service attacks, spam, phishing, etc.
- Regardless of their organization's scale, type, or infrastructure, Network Security Solution protect them from the always evolving attacks cyber threats.
- The goal is to keep your network safe from hackers who want to steal information or disrupt operations.

Wireless Security:

WEP:

The first wireless security protocol was WEP (Wired Equivalent Privacy). It was the standard method of providing wireless network security from the late 1990s until 2004. WEP was hard to configure, and it used only basic (64-/128-bit) encryption. WEP is no longer considered secure and should be replaced by a newer protocol such as WPA2, described below.

WPA:

WPA (Wi-Fi Protected Access) was developed in 2003. It delivers stronger (128-/256-bit) encryption than WEP by using a security protocol known as Temporal Key Integrity Protocol (TKIP). Along with WPA2, WPA is the most common protocol in use today. But unlike WPA2, it is compatible with older software.

WPA2:

WPA2, a later version of WPA, was developed in 2004. It's easier to configure and provides even greater network security than WPA by using a security protocol known as the Advanced Encryption Standard (AES). Versions of the WPA2 protocol are available for individual users and enterprises.

WPA3:

A new generation of WPA, known as WPA3, is designed to deliver simpler configuration and even stronger (192-/256-/384-bit) encryption and security than any of its predecessors. It is also meant to work across the latest Wi-Fi 6 networks.

Mobile Security

Mobile device security is an important to keep our smartphones, tablets, and other portable devices safe from cyber criminals and hackers. The main goal of mobile device security is to keep our devices and other electronic devices safe from being hacked or other illegal activities. In our daily lives, it is very crucial to protect our private information from strangers and hackers. Mobile device security acts as a shield to ensure that our digital life remains secure

Data Leakage Prevention

Identify where holes or exit points where leaks may occur

- Instant messaging
- P2P file sharing (e.g: Whatsap, Skype etc..)
- Web mail (Yahoo mail, Gmail, Hotmail)
- USB storage devices/Removable drives
- Printers

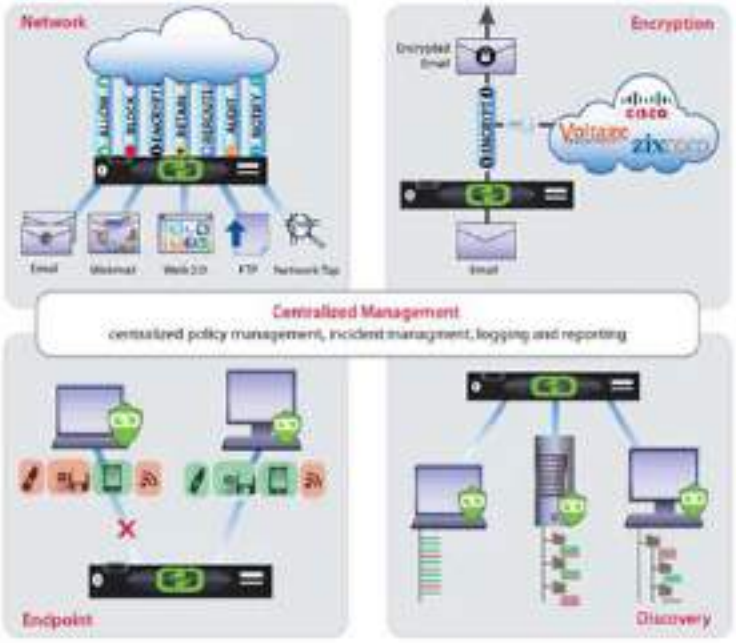
How data are flagged and identified

- Initial predefined policies
  - Social security numbers
  - Prescribed in SOX, DPDP etc. (Bank account numbers, PII..)
- Data Discovery
  - Looks into the content and not just the file type
  - Examine context considerations
  - Structured data matching (PII, credit card numbers, etc)

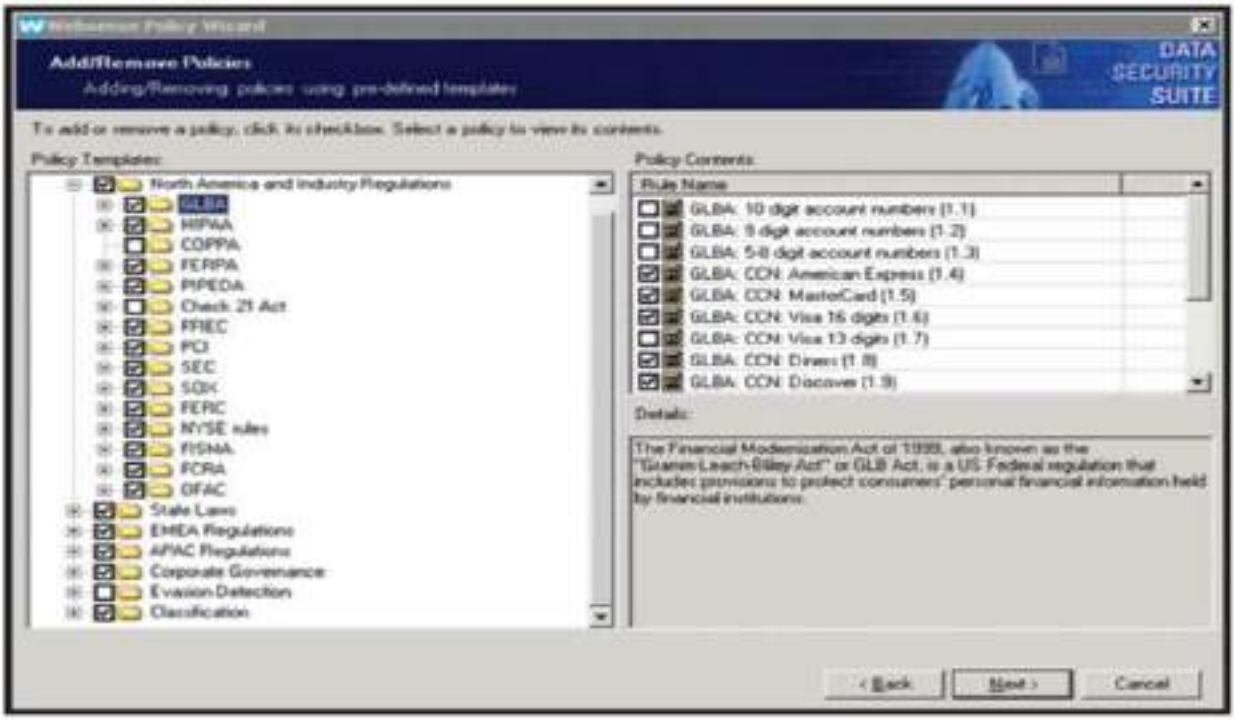
Data Leakage Prevention – Levels of DLP

– Three different levels of DLP solution

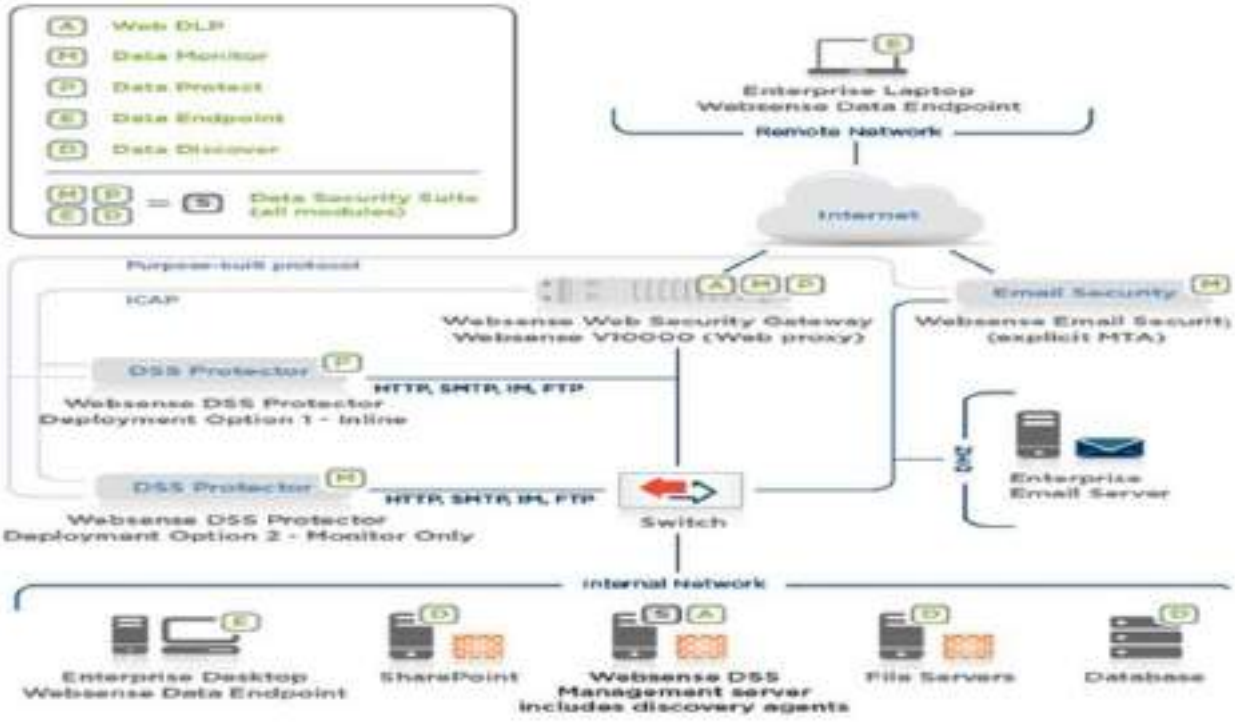
- Data in Motion
  - Data which uses HTTP, FTP, P2P and SMTP protocols are mirrored in the DLP server for inspection where visibility is enhanced
- Data at Rest
  - Data in file servers, databases, hosts computers set for file sharing, etc.
- Data at End Points
  - Data which sits on end user hosts (workstations and notebooks)

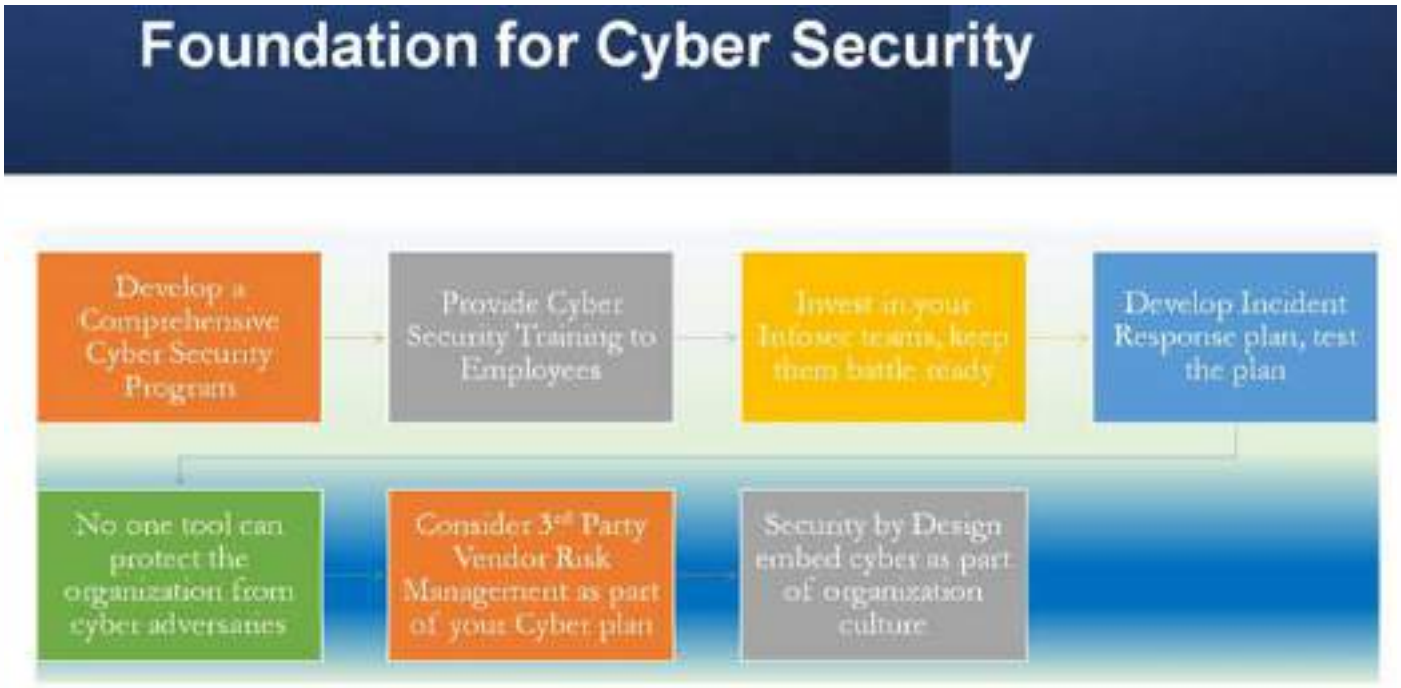


Data Leakage Prevention – Websense Policy Wizard



Data Leakage Prevention

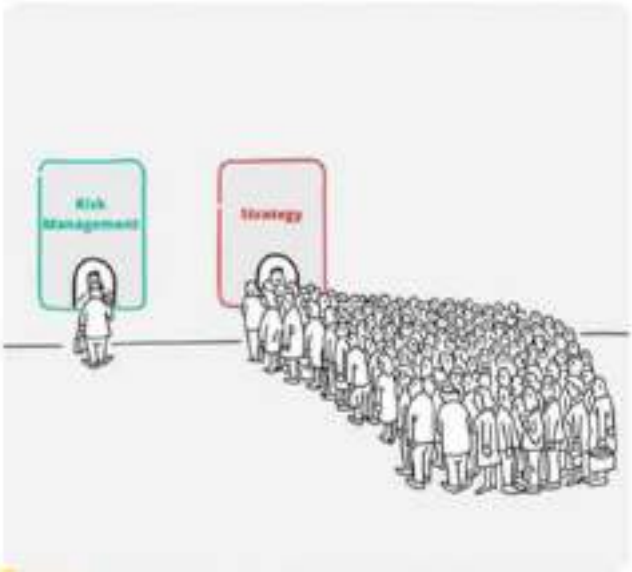



Foundation for Cyber Security
Develop a Comprehensive Cyber Security Program
Provide Cyber Security Training to Employees
Invest in your Infosec teams, keep them battle ready
Develop Incident Response plan, test the plan
No one tool can protect the organization from cyber adversaries
Consider 3rd Party Vendor Risk Management as part of your Cyber plan
Security by Design embed cyber as part of organization culture


Recommended Steps For Securing Your data:
Security Governance
develop and communicate security roles, responsibilities, policies, processes, and procedures
Security Assurance
monitor, evaluate, manage, and improve the effectiveness of your security and privacy programs
Identity and Access Mgmt
manage identities and permissions at scale
Threat Detection
understand and identify potential security misconfigurations, threats, or unexpected behaviors
Vulnerability Management
continuously identify, classify, remediate, and mitigate security vulnerabilities
Infrastructure Protection
validate that systems and services within your workload are protected
Data Protection
maintain visibility and control over data, and how it is accessed and used in your organization
Application Security
detect and address security vulnerabilities during the software development process
Incident Response
reduce potential harm by effectively responding to security incidents


Foundation for Cyber Security
Develop a Comprehensive Cyber Security Program
Provide Cyber Security Training to Employees
Invest in your Intosec teams, keep them battle ready
Develop Incident Response plan, test the plan
No one tool can protect the organization from cyber adversaries
Consider 3rd Party Vendor Risk Management as part of your Cyber plan
Security by Design embed cyber as part of organization culture


Recommended Steps For Securing Your data:
Security Governance
develop and communicate security roles, responsibilities, policies, processes, and procedures
Security Assurance
monitor, evaluate, manage, and improve the effectiveness of your security and privacy programs
Identity and Access Mgmt
manage identities and permissions at scale
Threat Detection
understand and identify potential security misconfigurations, threats, or unexpected behaviors
Vulnerability Management
continuously identify, classify, remediate, and mitigate security vulnerabilities
Infrastructure Protection
validate that systems and services within your workload are protected
Data Protection
maintain visibility and control over data, and how it is accessed and used in your organization
Application Security
detect and address security vulnerabilities during the software development process
Incident Response
reduce potential harm by effectively responding to security incidents



Challenges in Implementing Cybersecurity

- **Lack of Resources:** Implementing a cyber security program requires a significant investment of resources, including time, money, and personnel
- **Complexity:** Cyber security is a complex field, and implementing a comprehensive program can be challenging
- **Lack of Awareness:** Some organizations may not fully understand the importance of cyber security or the risks they face
- **Compliance Requirements:** Many organizations are subject to regulatory requirements related to cyber security, such as those issued by the IRDAI
- **Emerging Threats:** Cyber threats are constantly evolving, and organizations find it difficult to stay up to date with the latest threats and vulnerabilities

IT Audit Framework:

- The Committee of Sponsoring Organizations (COSO)
- Control Objectives for Information and Related Technologies (COBIT)
- The Public Company Accounting Oversight Board (PCAOB) standards
- National Institute of Standards and Technology (NIST)
- ISO 27001, ISO 27701, ISO Series
- General Data Protection Regulation (GDPR)
- Information Technology Infrastructure Library (ITIL)

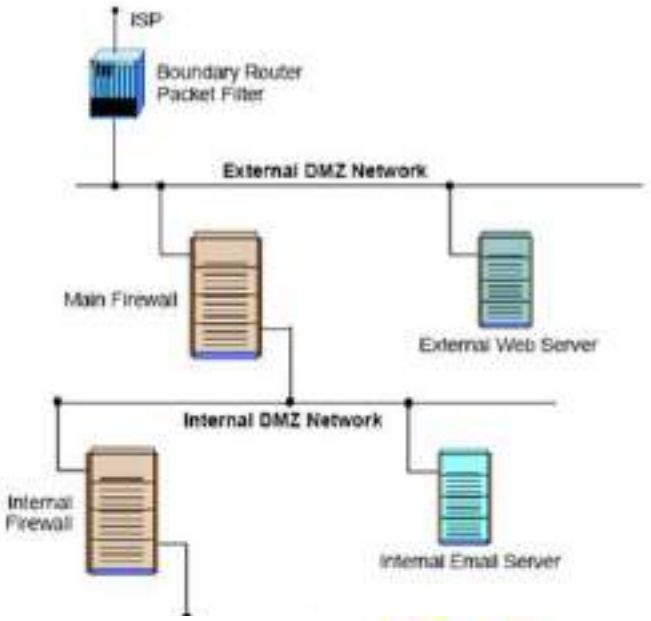
Firewall

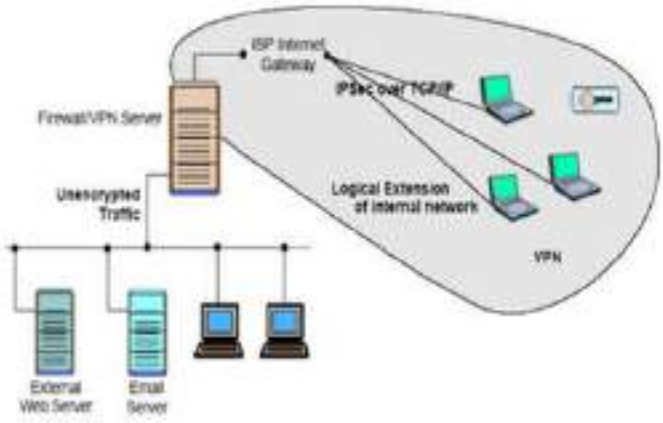
What is Firewall?

- Firewalls control the flow of network traffic
- Firewalls operate on number of layers
- Can also act as VPN gateways
- Active content filtering technologies

DMZ Environment:

- Can be created out of a network connecting two firewalls
- Boundary router filter packets protecting server
- First firewall provide access control and protection from server if they are hacked





VPN(Virtual Private Network)

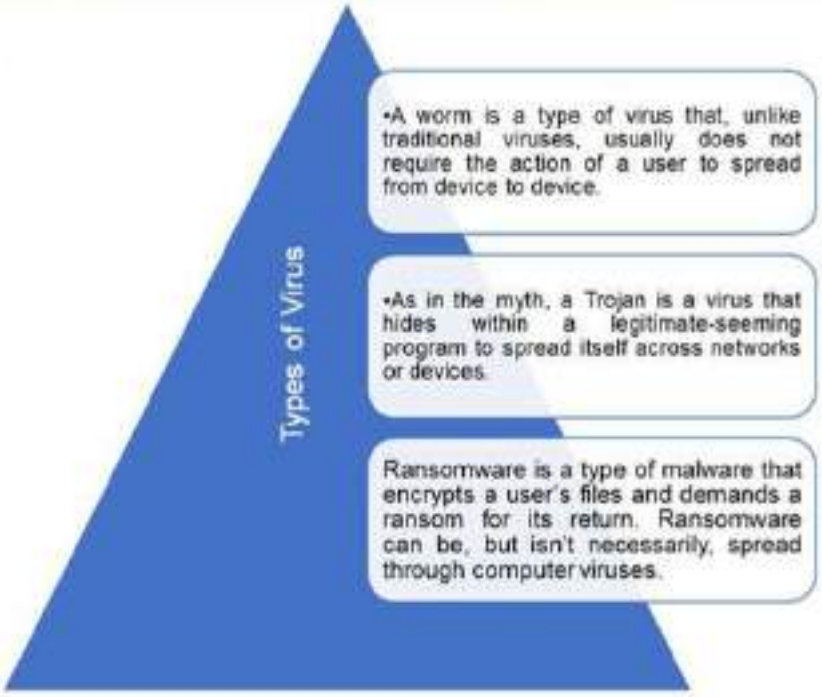
- VPN is used to provide secure network links across networks
- VPN is constructed on top of existing network media and protocols
- On protocol level IPsec is the first choice
- Other protocols are PPTP, L2TP

Virus

A malicious set of code meant to harm you and your computer

What can a Virus Do:

- Record your keyboard strokes
- Break/Damage your computer
- Hold your files hostage
- Use your processing power
- Steal/copy your files
- Steal other important information such as passwords, credit card numbers, etc.



Anti-virus

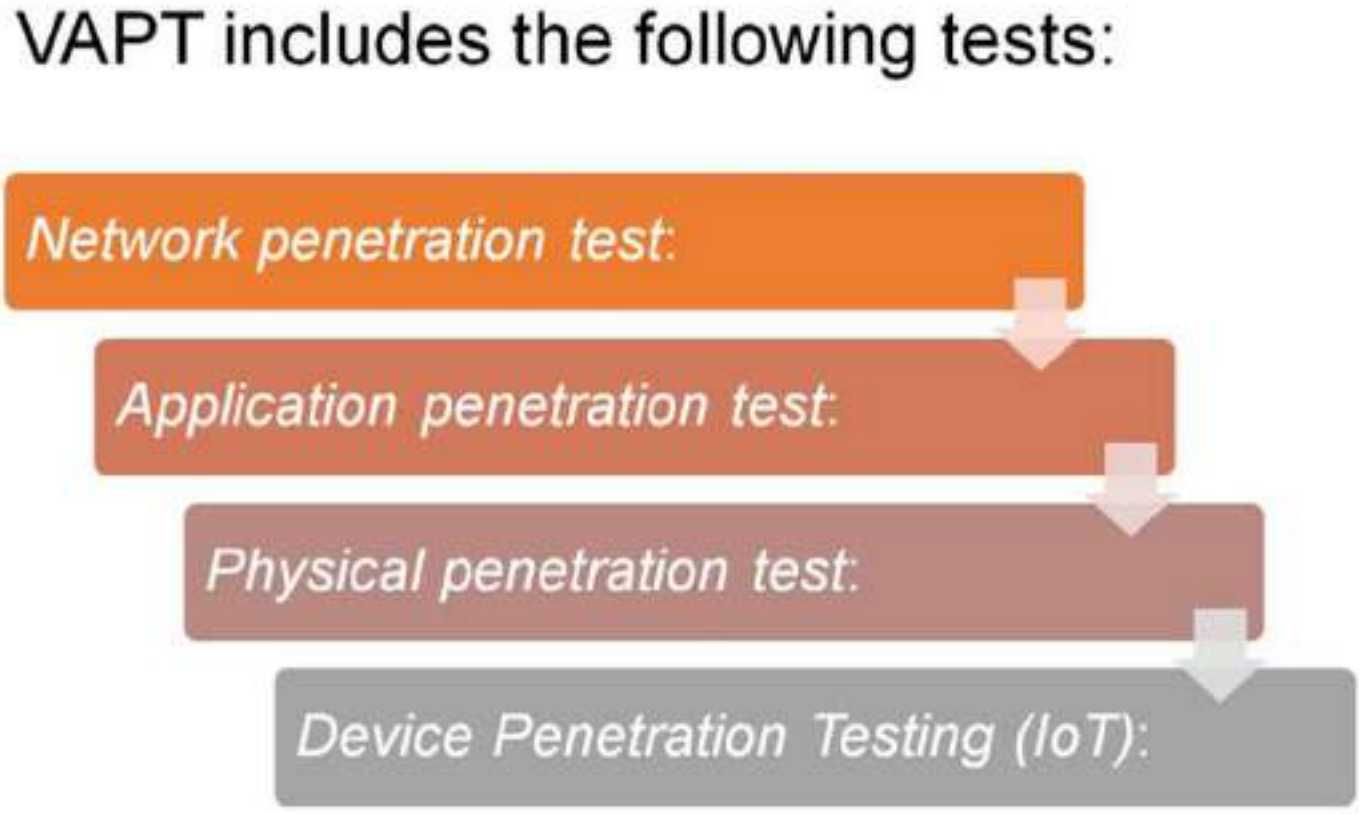
An **anti-virus** is a software which comprises programs or set of programs which can detect and remove all the harmful and malicious software from your device. This anti-virus software is designed in a manner that they can search through the files in a computer and determine the files which are heavy or mildly infected by a virus.

Common Anti-virus:

Norton
CrowdStrike
Kaspersky
AVAST
McAfee
TrendMicro


Single Sign-
on &
Multi Factor
Authenticatio
n:


Fortified
Single sign-on
Multi-factor authentication
Access multiple applications with one login
Access one or more applications using two different authentication methods
Users only need to remember one set of login credentials
Requires users to provide additional forms of ID
Reduce password fatigue
Reduce password complexity
Simplifies password authentication
Enhances security


VAPT includes the following tests:
Network penetration test:
Application penetration test:
Physical penetration test:
Device Penetration Testing (IoT):

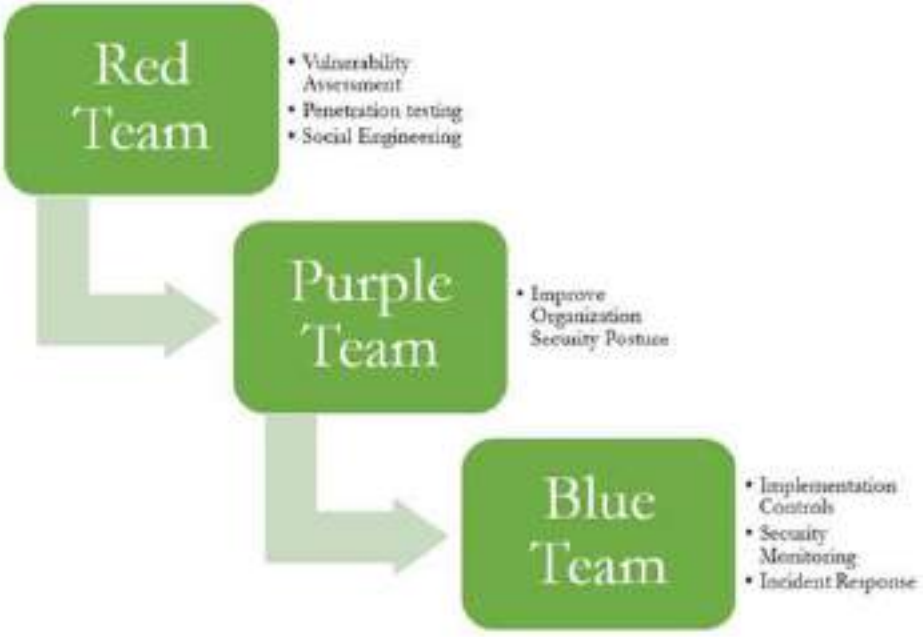
Types of Security Tools

Types of Security Tools

Wireshark is a network packet analyzer. A network packet analyzer will try to capture network packets and tries to display that packet data as detailed as possible. You could think of a network packet analyzer as a measuring device used to examine what's going on inside a network cable, just like a voltmeter is used by an electrician to examine what's going on inside an electric cable (but at a higher level, of course). In the past, such tools were either very expensive, proprietary, or both. However, with the advent of Wireshark, all that has changed. Wireshark is perhaps one of the best open source packet analyzers available today.

Nmap (Network Mapper) is a free and open source utility for network discovery and security auditing. Useful for tasks such as network inventory, managing service upgrade schedules, and monitoring host or service uptime. Nmap uses raw IP packets in novel ways to determine what hosts are available on the network, services (application name and version) those hosts are offering, operating systems (and OS versions) they are running, type of packet filters/firewalls are in use, and dozens of other characteristics. It was designed to rapidly scan large networks it will work against single host too. Nmap runs on all major computer operating systems.

Nessus is a remote security scanning tool, which scans a computer and raises an alert if it discovers any vulnerabilities that malicious hackers could use to gain access to any computer you have connected to a network.. It does this by running over 1200 checks on a given computer, testing to see if any of these attacks could be used to break into the computer or otherwise harm it.



Personally Identifiable Information:

1. **Access Confidentiality Impact Level for PII Collected and used by the Organization.**
2. **Prepare Incident Responses for Data Breaches.**
3. **Implement Appropriate Controls:**
   - Operational Safeguards
   - Privacy Safeguards
   - Security Controls

Privacy Bill - overview

Upcoming Programs

THE INSTITUTE OF CHARTERED ACCOUNTANTS OF INDIA

(Set up by an Act of Parliament)

CHENGALPATTU DISTRICT BRANCH (SIRC)

Topics : All About NRI Taxation And Permanent Establishment As Per IT Act - An Analysis

Speakers : CA. Bharathy G, CA. Sirish M I And CA. Ramesh R

Date : 06-07-2024, Saturday

Place : Our Branch Premises

Topics : ICAI MSME & Startup Yatra 2024

Speaker : Eminent Speaker

Date : 11-07-2024,Thursday

Place : Our Branch Premises
