08/24

Vidyalekhan

DATE
PAGE

* CERT-In : Computer Emergency Response Team India. } Ministry of Telecom & Engg.
The authority that deals with cyber security protocols in India
→ Director General - Dr. Sanjay Bahl
* NTRO, NCIIPC
→ National Cybersecurity Coordinator - Lt. Gen M.U. Nair
→ First National Cybersecurity Coordinator -
* ITA 2000, DPDP 2023 } Ministry of electronics
* I4C - Indian Cyber Crime Coordination Centre. } Ministry of Home Affairs
* Helpline number : 1930
* Project Chakshu - report spam/fraudulent calls.
* C-DAC, C-DOC → developed the initial software
* PARAM - supercomputer of India.
* DFSS - Directorate of Forensic Science Services.

Disha Sharma
Assignment 0
Prof. Dharmesh Dave
Cyber Security Audit & Compliance
08/08/2024

Network Attacks
Prevention & Tools

1] **Malware** : Malware or malicious software is a program or file that intentionally causes harm to a computer, server or network by leaking confidential information, gaining unauthorized access, denying service etc. Examples of malware include spyware, ransomware, virus, trojan horses, worms etc.

Prevention : i) Anti-virus / Anti-spyware software - Install this software so that it can scan computer files to identify & remove malware.

ii) Limit action privileges - Limit the number of possible entryways by restricting application priviledges on your device. Allow only the application features & functions that are absolutely necessary to get the work done.

iii) Control access to systems - Install or implement a firewall, intrusion detection system (IDS), intrusion prevention system (IPS).

Tools : Antimalware software - Bitdefender
Firewalls
Email Security Gateways.

2] DDOS/DOS (Distributed Denial of Service) : Disrupts the operations of the server by flooding it with unwanted internet traffic. At their worst, these attacks can knock a website or entire network offline for extended periods of time.

Prevention: i) Attack surface reduction - Limiting attack surface exposure such as restricting traffic to specific locations, implementing a load balancer, blocking communication from outdated or unused ports, protocols & applications.

ii) Caching - A cache stores copies of requested content so that fewer requests are serviced by origin servers. Using a content delivery network (CDN) to cache resources can reduce the strain on an organization's servers & make it more difficult for them to become overloaded by both legitimate & malicious requests.

iii) Rate limiting - Restricts the volume of network traffic over a specific time period, essentially protecting web servers from getting overwhelmed by requests from specific IP addresses.

Tools : Web application firewall
DDOS mitigation provider
L3-7 DDOS protection (Cloudflare)

3] Social Engineering (Phishing) - Tricking someone into divulging information or enabling access to data networks by mimicking human behaviour.

Prevention: i) Set spam filters - Every email program has spam filters, set them too high to keep away from spam to a large extent.

ii) Multi-factor Authentication - Add additional layers of security such as SMS confirmation codes or biometric authentication.

iii) Penetration Testing - A security exercise where a cyber-security expert attempts to find & exploit vulnerabilities in a computer system.

Tools: Honeypots
Biometrics
Pen-tests

4] Wireless Attacks: A malicious action against wireless system information or wireless networks.

Prevention: i) Use MAC filtering - Enable MAC filtering on your wireless router to control access to your network. By specifying which devices are allowed to connect based on their unique MAC addresses, you can prevent unauthorized access and enhance your network's security.

ii) Disable SSID broadcasting - Turn off SSID broadcasting to make your wireless network invisible to casual observers. This prevents your network from being easily discoverable & adds an extra layer of obscurity for potential attackers.

iii) Use WPA2 encryption - Utilize WPA2 encryption, the latest & most secure protocol, to safeguard your data as it travels b/w devices & access points. Encryption ensures that even if intercepted your data remains unintelligible to unauthorized entities.

Tools: Kevio Control
MAC
SSID

5] Man in the Middle Attack - A MITM attack is a general term for when a perpetrator positions himself in a conversation between a user and an application - either to eavesdrop or to impersonate one of the parties, making it appear as if a normal exchange of information is underway.

Prevention:
i) Setting up a VPN - VPNs can be used to set up a secure environment for sensitive information within a LAN.
ii) Public Key Pair Based Authentication - like RSA to help ensure integrity
iii) Strong WEP/WAP encryption on access points - prevents unwanted users from joining your network just by being nearby.

Tools :

6] Keylogger - A program or hardware that secretly records keystrokes on a keyboard or a device.

Prevention:
i) Update your system - because there are vulnerabilities in outdated softwares.
ii) Install a password manager - using tools that auto-fill forms will keep your passwords & personal information safe & secure.
iii) Set up a firewall

Tools :

7] ARP Poisoning - Address Resolution Protocol (ARP) Poisoning is a type of cyber attack carried out over a LAN that involves sending malicious ARP packets to a default gateway on a LAN in order to change the pairings in its IP to MAC address table. ARP protocol translates IP → MAC address.

Prevention:
i) Static ARP tables - statically map all the MAC addresses in a network to their rightful IP addresses.
ii) Switch Security - Dynamic ARP Inspection (DAI), these features evaluate the validity of each ARP message & drop packets that appear suspicious or malicious.
iii) Network Isolation - Concentrating imp. resources in a dedicated network segment where enhanced security is present.

Tools:

8] MAC Flooding - A cyber attack that targets network switches on a local area network to compromise their security & steal user data.

Prevention:
i) Port security - Limit the number of new MAC addresses that can be added to the forwarding table or select a specific number of addresses that are not to be overwritten when the table runs out of space.
ii) MAC address filtering - Configuring a MAC address switch to only accept packets from known MAC addresses.
iii) Network monitoring - to scan for MAC flooding indicators.

Tools:

ute Force - Uses trial & error method to guess all possible mbinations of a password, encryption key, or any login informa

) Limit login attempts - Use plugins to allow you to enter the umber of logins you want your visitors to have.

) Monitor IP Addresses - Limit login attempts to users coming from ecified IP address or range.

) Two-factor Authentication - requires a user to validate their entity when logging into an account before being granted access

oofing: When a cybercriminal sends a fraudulent communicati at appears to come from a legitimate source.

ide your IP address - Get in the habit of hiding your IP addre en surfing the web to prevent IP spoofing.

Be wary of strange attachments - Don't ~~upon~~ open attachment they have unusual file extensions.

Use a dedicated secure browser - one that's less vulnerable hijacking attempts.

11] Exploit : Uses a piece of code or program to take advantage of a security flaw or vulnerability in software or hardware.

Prevention :
i) Update system software - this often fixes known vulnerabilities.
ii) Firewall - helps block unauthorized access attempts to your network & systems.
iii) Penetration tests - help identify vulnerabilities & weaknesses before cybercriminals find them.

Tools :

12] Sniffing : A network attack where a hacker uses a packet sniffer to intercept & access unencrypted data packets as they travel across a network.

Prevention :
i) Use encrypted connections - secure your internet traffic.
ii) Firewall - monitor & control inbound & outbound traffic.
iii) 2FA - extra layer of protection.

Tools :

13] Buffer overflow : Occurs when the amount of data in the buffer exceeds its storage capacity. That extra data overflows into adjacent memory locations & corrupts or ~~overwrites~~ overwrites the data in those locations.

Prevention : i) Address space randomization - randomizing add. space locations of data regions to not know the locality of executable code.

ii) Data execution prevention - flags certain areas of memory as non-executable or executable.

iii) Structured Exception Handler overwrite protection (SEHOP) - helps stop malicious code from attacking Structured Exception Handling (SEH) a built-in system for managing hardware & software exceptions.

Tools :

14] Supply Chain : Uses third party tools/services to infiltrate a target's system or network.

Prevention : i) Run a third-party risk assessment - implementing correct security policies.

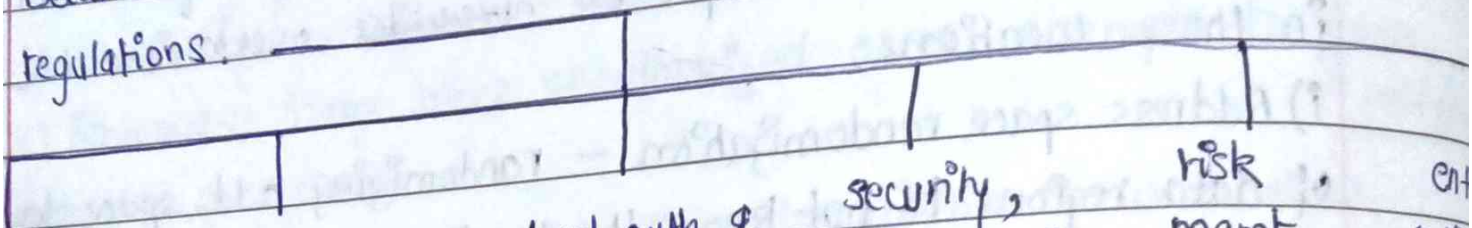
ii) Malware Prevention - automatically scan devices for malicious code.

iii) Adopt browser isolation - isolate webpage code before it executes on end-user devices.

Tools :

What is compliance audit?

Detailed review of organization's loyalty towards uphold of rules & regulations.



→ to assess if the organization's compliance program is effective or not.
→ to bring out non-compliance in front of management

→ ensure that the company meets the guidelines from govt. agencies.
→ improve org. efficiency in the business environment
→ uphold faith of stakeholders
→ comply with various other laws
→ ensure std. operating procedure has been followed throughout.

r organization

Identify the need & extent of audit → Select the auditor → meet the requirements.

Auditor

List out statutory laws applicable to the entity → obtain a list of inte policies → engage → segregate / prioritize → plan the audit → revie → feedback.

Types of compliance audits

1) SOC 2 : Service Organization controls 2 is a cybersecurity compliance framework & audit report that evaluates a service organizations information security practices. It is based on the American Institute of Certified Public Accountants (AICPA) auditing standards board.
2) ISO 27001 : Applies to companies & organizations that manage the security of assets such as employee or third-party data, financial information & intellectual property.
3) General Data Protection Regulation - process data of Europeon citizens.
4) Obligatory Compliance Audit - Any organization that wants to conduct an audit can do so by appointing any person who might be an internal auditor or any other person who meets the qualification criteria

---

16/08/2024

- Cybersecurity audit began in 2001.
- Anron - US based company, top firm in energy sector, auditors : Aurthur & Anderson
- Donald Trump 2016 presidential election - Cambridge analytics, England ; R&D project on user behaviour analytics (UBA - SIEM); collected data on Facebook ; cyber psychology ; Julian Trump - connections with Russia ; Hack into democrats ;
- Digital Personal Data Protection Act (2023)
- Internet Relay Chats (IRCs)

Vidyalekhan
DATE
PAGE

Defn: Audit - Audit is a process to assess & review of an organization's internal policies, controls & activities in accordance with guideline, framework or compliances.

20/08/24

- Difference b/w policy & law
- Audit can be used to assess the presence & effectiveness of IT controls & to ensure that these controls are compliant with stated policies.
- Audits provide reasonable assurance that organizations are compliant with applicable regulations & other industry requirements.

Types: Financial, compliance, Operational, Investigative, Information Technology.

Scope of an IT audit: Organizational, Compliance, Application, Technical

* Frameworks - Cobit, Osho

Defn: Compliance - The act or process of complying to a desire, demand, proposal, or regimen or to coercion. To comply is to conform, submit or adapt as required or requested.

Types: Internal compliance & External compliance.

Interpret the regulation & how it applies to the organization.
Identify the gap or determine where the organization stands w
the compliance mandate
Devise a plan to close the gap
Execute the plan.

Compliance is closely related to risk management and governanc
on all levels, be it technical, procedural or strategic.

What is Assessment?

In IT security assessment is a key activity that involves the manageme
f risk - an uncertainity that might lead to a loss.
ssessment is an evaluation process against the security perimeter
controls in the organization with respect to the standard or
mpliance.
risk-based approach to managing information security involves
e following:
1) Identifying & categorizing the information & information syster
2) Selecting and implementing appropriate security controls -
actions or changes to be applied to systems to reduce weakness
or potential losses.
3) Assessing the controls for effectiveness
4) Authorizing the systems by accepting the risk based upon
selected security controls.

29/08/24

Unit II - International Standard ISO 27002

- 93 controls.
- Policy for Information Security
- Information security roles & responsibilities.
- Segregation Duties.
- Management Responsibility
- Contact with authority.
- Contact with special interest tool.
- What is Intelligence? (Threat Intelligence)

30/08/24

* Case study - Enron, WorldCom, GDPR.

Vidyalekhan

DATE
PAGE

TA1 - Notes

Unit 1 : The Need for Information Systems Security Compliance

Defn : IT Security Assessment - a key activity that involves the management of risk - an uncertainity that might lead to a loss. A risk based approach to managing information security involves :

- Identifying & categorizing the information & information systems.
- Selecting & implementing appropriate security controls - actions or changes to be applied to systems to reduce weaknesses or potential losses.
- Assessing the controls for effectiveness
- Authorizing the systems by accepting the risk based upon selected security controls.
- Monitoring the security controls on a continual basis

&

Defn : National Institute of Standards & Technology (NIST) - the technology agency of the US, department of commerce, provides a framework for effective security assessment plans in NIST special publication 800 - 53A.

→ Methods for conducting a security control assessment.

(a) Examination - Verify, inspect or review associated assessment objects to understand or obtain evidence to support the existence & effectiveness of the security control.

(b) Interview - Discuss associated assessment objects with groups or individuals to understand or obtain evidence to support the existence / effectiveness of the security control.

(c) Test - Put associated assessment objects under specific condition to compare actual behaviour with what is expected to obtain evidence to support the existence & effectiveness of the secur control.

Defn: Penetration Tests - an assessment method that aims to bypass contro & gain access to a specific system by simulating the actions of would-be attacker.

Defn: IT Security Audit - a process to assess & review an organization's internal policies, controls & activities in accordance with guidelines, framework or compliances.

Types: Financial, Compliance, Operational, Investigative, IT.

Scope: Organizational, Compliance, Application, Technical.

Defn: Compliance - the act or process of complying to a desire, demand, proposal or regimen or to coercion. To comply is to conform, submit or adapt as required or requested.

* Control Objectives for Information & related Technology (COBIT)

→ Difference b/w Audit & Assessment

- Audits can either pass or fail, assessment is an opportunity to assess the current state & make improvement

SO/IEC 27002 : 2022 (E) . pdf
)pti Managerial Control (5.4)

BC organization is a software development organization that velops that develops software for Google, MS, IBM & othe nwhinational companies.
e org. develops various modules, plugins, addons to the ove stated organizations. Apart from that ABC also has eir own products called Nuvence. The product helps anaging the CRN & DRP of an Institute.

YZ organization is one of the popular security firm o provides various cybersecurity services like security ression centre, VAPT, antivirus solutions, threat intelli . The firm also has their own product called DNIF an SOAR based tool. The firm has provided the e related service to various institute.

W organization is a financial firm who provides equi finance to any req. institute. DVW has recently signed Collaboration / MoU with NMT organization to provide m with financial support to manufacture cars

④ SSP organization is providing its services related to content management & document preperations. SSP is providing services to various banks, MFs, fintech org, as well as MSMEs. Recently they have provided a service to XYZ company to prepare their documentation related to policies & procedures.

⑤ CMS is the organization who provides ATMs & its accessories & installation to various banks accross the globe. CMS has received a contract from a national bank of UAE to provide ATM machines with the integration of CBS (Core banking system).

1) Information Security Project Management (How will you maintain?)
2) How will you maintain IS in that project.
3) " " " " " " " " "
4) Prepare an information security policy for them.
5) What things as a security controls are req for this integration & the privacy / risk identification. Solutions / Controls to mitigate with.

ISO 27002 : CONTROLS

5.1 Policy for Information Security

Requirements: 1) business strategy 2) regulations, law, statutory bodies
3) current & projected risks & threats.

→ definition, principles, objectives, commitment, assignment of responsibilities, procedures / methods.

→ allocated to relevant personnel based on appropriate level of security & technical competency.

Detail	IS Policy	TS Policy
Level of mgmt	High / General	Specific
	Top Management	App. level of mgmt

5.2 Information Security Roles & Responsibilities.

→ defined, approved & understood structure for implementation of information security.

→ protection of assets, specific processes, risk mgmt, personnel. (why?)

→ Information Security Manager.

5.3 Segregation of Duties.

→ conflicting areas of duties should be segregated. (reduce risk of fraud)

Examples: change, access rights, code, software, app, databases, controls.

5.4 Management Responsibilities.

→ management should ensure that personnel obey IS policy.

→ briefing, expectations, mandate, awareness, compliance, qualifications, confidentiality, resources

5.5 Contact with Authorities.

→ ensure proper flow of information.

→ when, by whom, how contact must be established

5.6 Contact with Special Interest Groups.

Membership: Knowledge, understanding, warnings, advice, information, liason points (meetings)

5.7 Threat Intelligence.

→ info relating to threats should be collected & analyzed

Why? to take app. mitigation actions, reduce impact

Layers strategic, tactical, ~~insightful~~ operational

Should be relevant, insightful, contextual, actionable

Activities obj, sources, collecting, processing, analyzing, communicating info.

Use cases risk mgmt, fw, IDS, malware detection, techniques input

5.8 Information Security in Project Mgmt.

→ Integrated into project mgmt. throughout project life cycle.

Requirements: early risk mgmt, early compliance mgmt, securing risks, reviews & monitoring,

↑

Considerations: what info, protection needs, level of confidence, access provisioning, informing users, req. of ISP, confidence of third parties.

ISO ~~2500~~ 21500 / 21502 : Concepts of proj. mgmt

ISO 27005 : concepts of risk mgmt.

5.9 Inventory of Information & other associated assets.

→ preserve their information security & assign appropriate ownership.

Inventory: regular interviews, inventory update, dynamic list

Ownership: of assets assigned, classification

Owner Duties: inventoried, classified, reviewed, listed, req, restrictions, removal, risks, roles

ISO 19770-1: IT asset mgmt.

ISO 55001: asset mgmt.

5.10 Acceptable use of information & other associated assets.

→ rules identified, documented, implemented

→ topic specific policy on acceptable use.

TSP states: expected & unacceptable, permitted, prohibited, monitoring

Considerations: access restrictions, record maintainance, protection, storage, marking, auth.

5.11 Return of Assets.

→ personnel should return assets upon their termination

Assets: endpoint devices, storage devices, special equip, auth. hardware, phy. copy & info.

→ difficult to return assets that are not owned by the organization.

5.12 Classification of Information.

→ classification based on needs of the org & CIA.

→ owners of info. should be accountable for their classification.

→ Overclassification & underclassification

Scheme: no harm, minor, short term, long term.

5.13 Labelling of Information.

→ communication & support automation (why?)

→ omitting labelling, how to label, impossible labelling.

Example: physical, header, footer, metadata, watermarking, rubber stamps

→ Classified assets can be easier to identify by attackers.

5.14 Information Transfer.

→ rules, procedures, agreements.

General: controls, protection, traceability, contacts, liabilities, labelling system, reliability, availability, TSP guidelines, retention, disposal, contractual

Electronic: malware, attachment, wrong address, approval, authentication, restrictions, advising

Physical: transmission, addressing, packaging, auth., identification, tamper-resistance, verification, approval, logs.

Verbal: confidentiality, screening, room controls, sensitivization.

5.15 Access Control

→ physical & logical

TSP: type of access, security, physical access, auth, privileges, seg. of duties, legislation, seg of access control, formal authorization, access rights, loggi

Considerations: consistency, available connections, dynamic access control

Principles: need to know, need to use

Care: PoLP, labelling, user permissions

5.16 Identity Management.

→ unique identification of individuals & systems

Guidance: 1-1 mapping, 1-many mapping, non human identities, removal, Identity - Entity, records

5.17 Authentication Information

→ management process & personnel

Allocation: PINs, verification, protected channel, acknowledgement, defaults, records.

User: confidentiality, integrity, strong pwds

Pwd Mgmt: change, strong, login, reuse, hidden, protected

5.18 Access Rights.

Provision: auth, business req, seg of duties, removal, temporary, levels, record, modification, removal

Review: user, auth.

Termination: initiation, responsibility, values

5.19 Information security in supplier relationships

→ agreed level of IS, TSP

→ supplier's products or services.

types of suppliers, selection, IS control, org info, infra

To maintain an agreed level of Information security in supplier relationships

Addressing Information Security within Supplier Agreements

→ agreement b/w organization & supplier
description, classification, legal, obligation, rules, procedures,
requirements, remediation, IRM, training, provisions, contacts,
screening, evidence, audit, delivery, resolution, backup, availability,
phy. security, info transfer, termination, destruction, handover.

Managing Information Security in the ICT supply chain

definition, requirements, practices, info, functions, monitoring,
documenting, assurance, implementation
cloud service provisioning, IOT, hosting services

Monitoring, Review & Change Management of Supplier Services

monitor service performance levels, changes, review, audit,
respond, identify, ensure, evaluate

Information Security for use of Cloud Services

TSP, cloud service provider & customer
ISR, selection criteria, roles, which info, obtaining, managing, procedu
SoIs, access controls, processing, support, backup, return

END SEMESTER PREPARATION

Unit II & Unit III Notes :

- Planning & Implementation of an IT infrastructure audit for compliance.
- Conducting an IT infrastructure audit for compliance.

Defn: Controls - Security controls refer to any safeguards or countermeasures used to avoid, detect, counteract or minimize security risks to physical property, information, computer systems or any other assets. [Maximizing CIAA]

Goal Based Controls

1) Preventive
2) Detective
3) Corrective
4) Deterrent
5) Compensating
6) Common

Implementation Based

1) Technical
2) Management
3) Operational

Defn: CAATs - Computerized - Assisted Audit Techniques ~~are~~ is the software that helps auditors evaluate application controls, & select & analyze computerized data for substantive audit tests.

- evaluate the integrity of an application.
- determine compliance with procedures
- continuously monitor processing results.

Examples: ACL - Audit ~~Cobol~~ Command language
IDEA - Interactive Data Extraction & Analysis.

- CAAT for Sampling
  - Judgemental: Auditor's Knowledge & experience
  - Statistical: random and/or probability

User Domain

what constitutes UD?

1) Employees
2) Contractors
3) Guests

Trust ↓

Controls

1) RACI Matrix
2) IT Asset AUP
3) Internet AUP
4) Email AUP
5) HR

Workstation Domain

what constitutes WD?

1) UPS
2) Laptop/PC
3) Smartphone
4) Tablet
5) Printer
6) SM

Maximizing CIA

(C): AC, Encryption
(I): Anti-malware
(A): UPS, backup

Controls

1) Access Control Lists (ACL)
2) Authentication / Identity mgt
3) OS patch mgmt
4) App. patch mgmt
5) IT security policy

what consti
* same as
switch, hub,

what cons
Switch, r
proxy,
IDS, IPS

what
WSP,
L2/L3
Redu

LAN Domain

What constitute LD?

* Same as WD

switch, hub, router, server

Maximizing CIA

(C) : AC, encryption, PP

(I) : Anti-malware, audit

(A) : Recovery, Backups

Controls

1) Access Control
2) Comm. Control
3) Soft. patch mgmt
4) Recovery / Backup
5) Config. changes
6) Monitoring Tools

LAN-WAN Domain

What constitutes LWD?

Switch, router, firewall, proxy, DMZ, Honeypot, IDS, IPS, DLP

Maximizing CIA

(C) : Encrypting, DLP

(I) : VPN, Config mgmt

(A) : Backup, Dual ISP, Firewall, BCP/DRP, VAPT

Controls

1) Traffic monitoring
2) Config. change mgmt
3) Firewall rules
4) ACL
5) NAC 6) VAPT

WAN Domain

What constitutes WD?

WSP, Circuits, MPLS, L2/L3 switch, backup, Redundancy links

Maximizing CIA

(C) : Encryption

(I) : Redundancy, SOC

(A) : SLA, Recovery, Backup

Controls

1) WAN optimizer
2) Traffic monitoring
3) ACL 4) VPN

Scope for audit, rev for audit, Obtaining info, Documentation & resources, Security control formulation, Control implementation, Min Acceptable Risk, Baseline Defns, Audit Report

Vidyalekhan

DATE

PAGE

Remote Access Domain

What Constitute RAD?

Remote users, remote PC, AC, Auth. server, VPN, ISPs

Controls

1) Privacy 2) Encryption
3) App. Control 4) Sys enc.
5) RA AUP 6) RA VPN
7) ACL 8) VPN

System Application Domain

What Constitutes SAD?

Mainframe, MC, server, UPS
Datacenter SC, SD, app.

Maximizing CIA

Ⓒ : Encryption, PP
Ⓘ : ACL, VM
Ⓐ : BCP, DRP

Controls

1) Isolation 2) Limit Acc
3) Protect 4) PAC
5) Env. control 6) Fire
7) DR site 8) Sft config
9) QA QT 10) ACL

* Truth, Transparency, Tactics are characteristics of a good auditor.

- Functions of Controls - Identify, Protect, Detect, Respond, Recover
- States of Data - Rest, Transit, Process

* Formula
Step 1 : Categor
Step 2 : Identif
Step 3 : Categ
Step 4 : Categ
Step 5 : Descr
Step 6 : Selec
Step 7 : Iden
Step 8 : Form

- The
by
su
de
- Co
- St
1) S
2)
3)
4)
5)
6)
7)
8)
9)

* Formulation & Development of Security Controls –

Step 1: Categorizing ICT Systems – Low, Moderate, High.

Step 2: Identifying Information Types

Step 3: Categorization of Information Types – [CL; IL; AL]

Step 4: Categorization of Information Systems – [CL; IL; AL]

Step 5: Description of Information Systems

Step 6: Selection of Security Controls

Step 7: Identification of Common Controls

Step 8: Formal Security Control Selection

- The information produced during control assessments can be used by an organization to – identify risks, prioritize risks, support monitoring activities, facilitate security authorization decisions, inform budgetary decisions.

- Components of Security Control Assessment – Examine, Interview, Test

- Standard Security Principles Derived from Standards –

1) Strategic planning – policy controls
2) Operational security controls
3) Asset classification & control
4) Personnel Security
5) Physical & Environmental security
6) Access control
7) System Development & Maintainance
8) Continuity Management
9) Compliance

Vidyalekhan
DATE
PAGE

Unit IV Notes:

- Risk Assessment & BCP, DR Planning.

Defn: Risk - Risk is the probability of a negative / harmful event occurring as well as the potential of scale (impact) of that harm.

Defn: Threat - An expression of intention to inflict evil injury or damage. Attacks against key security services - CIA.

Defn: Vulnerability - A vulnerability is a flaw or weakness in an asset's design, implementation, operation & maintainance that could be exploited by a threat.

Defn: Risk Analysis - Identifying the most probable threats to an organization & its related vulnerabilities & their analysis.

Defn: Risk Assessment - involves evaluating existing security controls & assessing their adequacy relative to the potential threats to the organization.

Defn: Risk Management - systematic application of management policies, procedures & practices to the tasks of establishing the context, identifying, analyzing, evaluating, treating, monitoring & communicating risk.

Reactive
responds as events occur

Proactive
responds before events occur

- Risk Management Process -

1) Resource Profiling
2) Risk Assessment
3) Risk Evaluation
4) Document
5) Risk Mitigation
6) Validation
7) Monitoring & Audit

Types of Risk Analysis

Qualitative

- Quick, Accurate, Consistent, Structured, Flexible
- Severity - Low, Moderate, High, Critical
- Likelihood - Neg., Low, Mod, High, V. High

Quantitative

- Value, ALE, Inaccurate, costly
- Impact x Probability
- Scope, Team, Threats, Threat Prioritization, loss, Total, Controls, Cost Analysis, Rank Controls, Communicate Results.

- Risk Registry - Risk Opportunity, Level, Cost, Controls, Mitigation, Internal Controls (optional)

Defn: Business Impact Analysis - proportion of impact an individual unit would sustain subsequent to a significant disruption of its services.

Defn: Disaster Recovery Plans - procedures for emergency response.

BCP
• The ~~BIA~~ Process -

1) Project Mgmt. & Initiation
   a) Need / Scope
   b) Mgmt Support / Team / Resources (4)
   c) Work Plan

2) BIA
   a) Info gathering
   b) Customize / Analyze collected info (8)
   c) Determine MTD
   d) Prioritization & Documentation

3) Disaster Recovery Strategy
   a) Documentation & cost estimates
   b) SLA & resumption strategies (6)
   c) BRP & Documentation

4) Plan, Design, Development
   a) Priorites & Scope
   b) Assumptions & Strategies
   c) Resumption & Location for DRS (15)
   d) DRP, BRP
   e) FRP, Response Procedures
   f) Gather & Review

5) Implementation
6) Testing
7) Maintainance.

Defn

D

Vidyalekhan

DATE
PAGE

Unit V Notes :

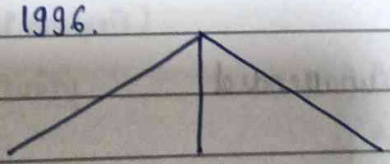
- Cyber Law & Auditing Standards / Frameworks.

Defn : COBIT - Control Objectives for Information & Related Technologies provides an implementable set of controls over IT & organizes them around logical frameworks for IT related enablers. Developed by ISACA. COBIT 5 - 2012 (latest)

- COBIT 5 Principles - Responsibility, Strategy, Acquisition, Performance, Conformance, Human Behaviour.

1) Meeting Stakeholder Needs
2) Covering the Enterprise End-to-End
3) Applying a single integrated framework
4) Enabling a Holistic approach
5) Seperating Governance from management

Defn : HIPAA - Health Insurance Portability & Accountability Act passed by Congress in 1996.



Privacy Rule | Security Rule | Breach Notification Rule

Defn : PCIDSS - Payment Card Industry Data Security Standard.

Defn : GDPR - General Data Protection Regulation.

AUDIT FLOW CHARTS

Vidyalekhan

DATE
PAGE

Unit 1 : Cyber Security Audit & Compliance

Audit

- Types - Fin, Compliance, Operational, Investigative, Info.
- Scope - Organization, Tech, Compliance, Application
- Objectives of Audit -
  1) Examine existing controls
  2) Verify existing controls
  3) Verify implementation of these controls

Importance / Req. / Need

1) Safe org. IT Assets.
2) Report to identify gaps (GAP Analysis)
3) Best Budget Solution for Security

Auditing Advice

1) Auditors should never be involved in Internal auditing
2) Audits are independent
3) Audits are rigorous
4) Certification

Compliance

- Types - Int, Ext
  1) Interpret regulation
  2) Identify gap
  3) Devise Plan
  4) Execute Plan

Auditing within the IT Infrastructure

1) 7 Domains - User, W.S, LAN, LAN-WAN, WAN, Remote Access, Sys/App

Failure to Comply ?

1) Penalties
2) Business Disruption
3) Increased Risk
4) Discontinuity (eg. Bankruptcy)

Assessment

- Methods - Exam, Int, Test
  1) Identifying Info. systems
  2) Selecting security controls
  3) Assessing controls
  4) Authorizing systems
  5) Monitoring

Vidyalekhan
DATE
PAGE

Unit 2 & 3 : Planning & Implementation of Audit

Controls?

Safeguard or countermeasure to avoid risk

- How to select? - Depth/Breadth, Flexibility, Reasoning, Prioritization, Industry Acceptance

Types of Controls

Goal-Based

1) Preventive - Sys Hardening, Access Control
2) Detective - Log Monitoring, CCTV
3) Corrective - IDS, Backup
4) Deterrent - Cable Lock, Hardware Lock
5) Compensating - MFA, OTP
6) Common - IRM, Physical Security

Implementation-Based

1) Technical - Encryption, Firewall
2) Management - Risk Mgmt, VAPT
3) Operational - Contingency Planning, Phy/Env Security

CAATs

(Computer Assisted Audit Techniques)

Uses

1) Select Sample
2) Analyze data
3) Identify Trends
4) Eval data integrity

Tools

1) ACL
2) IDEA
3) Microsoft Excel
4) Microsoft Access

Sampling

1) Judgemental
2) Strategic

7 Domains of IT Infrastructure

User Domain

Devices: Emp, Contractor, Guest

Controls: RACI, AUP, HR

Workstation Domain

Devices: UPS, PC, Laptop, Storage Media, Phones

Controls: ACL, Authentication

C: ACL, Encryption

I: Anti-Malware

A: UPS, Backup

LAN Domain

Devices: PC, Laptop, Hub, Router, Switch, Server

Controls: ACL, Patch mgmt

C: ACL, Encryption

I: Anti-malware

A: Backup, Recovery

LAN-WAN Domain

Devices: Switch, Router, Firewall, DMZ, IDS/IPS

Controls: Monitoring, Firewall rules, VAPT, NAC

C: Encryption, DLP

I: VPN, Configuration Mgmt

A: UPS, BCP, DRP, VAPT

WAN Domain

evices: WSP, L2/L3, Circuits

ontrols: VPN, ACL, N/w Monitoring

C: ~~SOC, SLA~~ Encryption

I: SOC, SLA

A: Backup, Recovery

Remote Access Domain

Devices: Remote users, Auth servers

Controls: HTTPS, VPN, AUP, ACL

Sys/App Domain

Devices: Mainframe, Server, Data Centre

Controls: ACL, Isolation, QA-QT