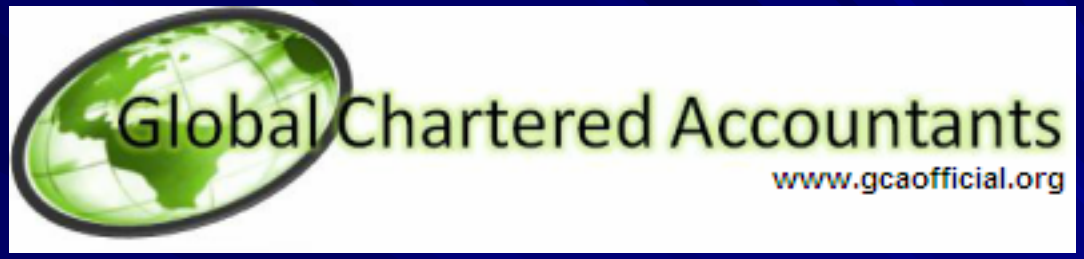

Protection of Information ASSETS

To evaluate Logical, Environmental and IT Infrastructure Securities to safeguarding information assets against unauthorized Use, Disclosure, Modification, Damage Or Loss

LOGICAL ACCESS EXPOSURES :

- ***Logical Access Exposures***
  - ***Trojan Horses***
  - ***Rounding Down***
  - ***Salami Techniques***
  - ***Virus***
  - ***Worms***
  - ***Logic Bombs***
  - ***Trap Doors***
  - ***Asynchronous Attacks***
  - ***Data Leakage***
  - ***Wire-Tapping***
  - ***Piggybacking***
  - ***Computer Shutdown***
  - ***Daniel of Services***

LOGICAL ACCESS EXPOSURES :

- ***Logical Access Control Software :***

  To prevent unauthorized access and modification to sensitive data and critical functions. It should be applied to networks, operating systems, databases and application systems

  - ***General OS Access Control Functions:***
  - ***Apply user ID and authentication***
  - ***Logon on specific terminal***
  - ***Multi-level access***
  - ***Individual accountability and auditability***
  - ***Create or change user profiles***
  - ***Log Events***
  - ***Log User Activities***
  - ***Report capabilities***

LOGICAL ACCESS EXPOSURES :

- ***Identification and Authentications :***

  Based on, something <u>You Know</u>, something <u>You have</u> and something <u>You Are</u>

  - ***Logon-IDs and Passwords***

    Something you know

  - ***Token Devices, One Time Access Control***

    Something you have

  - ***Biometrics Security Access Control (through Finger Prints, Eye Retina)***

    Something you are

LOGICAL ACCESS EXPOSURES : I&A

- ***Features of Passwords :***
  - ***It should be easy to remember for user but***
  - ***Difficult for perpetrator to guess***
  - ***Initial Password should be changed on first time log-on***
  - ***In result of entering wrong password ID should be held***
  - ***Re-activation of ID should be on written request/approval by security administrator.***
  - ***Password encryption and should be shadowed***
  - ***Changed periodically***
  - ***Must be unique to each user ID.***
  - ***Unused IDs should be deactivated and logged off***
  - ***Ideally length of Password is 5 to 8 characters***
  - ***Usage of Alphabets, Numeric, Lower case and special***

LOGICAL ACCESS EXPOSURES : I&A

- ***Token Devices, Once-Time Passwords***
- ***Biometrics :***
  - ***Palm : ridges, valleys etc***
  - ***Hand Geometry : 3 dim perspective of hand***
  - ***Iris : Eyes colored portion surrounded***
  - ***Retina***
  - ***Finger Prints***
  - ***Face***
  - ***Signatures***
  - ***Voice Recognition***

LOGICAL ACCESS EXPOSURES : I&A

- ***Single Sign-on (SSO)***
- ***Advantages :***
  - ***No need to remember multiple PWDs***
  - ***Improves administrators ability to manage user profiles***
  - ***Reduces Administrative overheads***
  - ***Reduces the time taken by user***
- ***Disadvantages :***
  - ***Support for all major OS is difficult***
  - ***Significant cost associated with SSO development***
  - ***Single point of failure and total compromise of an organization's IS assets***

NETWORK INFRASTRUCTURE SECURITY :

- ***Controls***
  - ***Technical Qualified Operators,***
  - ***Job rotation (wherever possible)***
  - ***Restricted operation of operators over operator activity logs etc.***
  - ***Audit trail of all operator activities and its periodical review by operations management.***
  - ***Availability of documented Network operations standards and protocols to operators and periodical review to ensure compliance.***
  - ***Analysis for workload balance, fast response time and system efficiency***
  - ***Encryption should be used wherever required***

NETWORK INFRASTRUCTURE SECURITY :

- ***LAN Security***
  - ***<u>Threats :</u> Loss of Data & Programs, less version control, Exposure to external Activities, viruses, Improper disclosure of data, Violating Software License, Illegal access by impersonating or masquerading, Internal user's Spoofing***
  - ***<u>Remedies :</u> Declaring ownership of programs, files and storage, Limiting access to read only, Record and File locking, enforcing ID/Passwords procedures.***
  - ***<u>Dial Up Control</u> : Encrypted Passwords, Dial-back modems for verification***

NETWORK INFRASTRUCTURE SECURITY :

- ***Client Server Security :***
  - ***Disabling the floppy drives***
  - ***Network Monitoring devices to inspect activities***
  - ***Data Encryption***
  - ***Application level Access control programs***

NETWORK INFRASTRUCTURE SECURITY :

- ***Internet Threats :***
  - ***Disclosure***
  - ***Masquerade or Spoofing (Disguise IP address etc)***
  - ***Unauthorized access***
  - ***Loss of Integrity***
  - ***Denial of service (Sys Flooding of messages / requests and keep machines busy)***
  - ***Theft of service and resources***
- ***Internet Security Controls:***
  - ***Risk assessment of web based application.***
  - ***Security awareness***
  - ***Firewall standards***
  - ***Intrusion Detection standards security***
  - ***Remote Access for coordinating and controlling centrally***
  - ***Encryption techniques***
  - ***Monitoring usage of unauthorized usage and notification to them.***

NETWORK INFRASTRUCTURE SECURITY :

- ***Firewall Security Systems*** :
  - ***General Features***
  - ***Firewall Types***
    - ***Router Packet Filtering***
    - ***Application firewall***
    - ***Stateful inspection***
  - ***Firewall Issues***
    - ***Creates false sense of security***
    - ***Other entry points, connections direct though Modems***
    - ***Mis-configuration***
    - ***Firewall without screening router is useless***
    - ***Irregular monitoring of activities***
    - ***Irregular maintenance of Firewall policies***

NETWORK INFRASTRUCTURE SECURITY :

- ***Intrusion Detection Systems (IDS) :***
  - ***Components of IDS***
    - ***Sensor, Analyzer, An administrator Console***
    - ***A user interface***
  - ***Features***
    - ***Intrusion Detection***
    - ***Gathering Evidence***
    - ***Automated response***
    - ***Security Policy***
    - ***Interface with system tools***
    - ***Security Policy management***
  - ***Limitations***
    - ***Weaknesses in the policy definition***
    - ***Application level vulnerabilities***
    - ***Backdoors into application***
    - ***Weakness in identification and authentication schemes***
  - ***Honeypots and Honeynets***
    - ***Software application pretend to be unfortunately hacked***
    - ***Network of honeypots making a false network for hackers to hack and caught***

- ***Encryption:***
  - *Is a process of converting a plaintext into a secure coded form of text (Cipher General Features)*
  - ***Key Elements of Encryption Systems***
    - ***Encryption Algorithm***
    - ***Encryption Keys***
    - ***Key Length***
  - ***Private Key Cryptographic system***
  - ***Public Key Cryptographic System***
  - ***Digital Signatures***
  - ***Digital Envalop***
    - ***Is used to send encrypted information and relevant keys along with it.***

AUDITING NETWORK INFRASTRUCTURE SECURITY :

- *Review network Diagram*
- *Identify Network Design*
- *Dissemination of policies and standards*
- *Experience/knowledge of security operators for internet*
- *legislative issues are considered against usage of internet based application*
- *Review of service level contract in case of outsourcing.*
- *Hardware and software are well upgraded to counter new vulnerabilities*

– *Auditing Remote Access*
– *Auditing internet "point of presence"*
– *Network penetration tests*
– *Full network assessment reviews*
– *LAN network assessment*
– *Development and Authorization of network change*
– *Unauthorized changes*
– *Computer forensics*

ENVIRONMENTAL EXPOSURES AND CONTORLS:

- ***Environmental Issues and Exposures :***
  - *Fire, Natural Disasters,*
  - *Power Failure*
    - *Total Failure*
    - *Severely reduced voltage*
    - *Sages, spikes and surges*
    - *Electromagnetic interference*
  - *Power Spike*
  - *Air conditioning Failure*
  - *Electric Shock*
  - *Equipment Failure*
  - *Water Damage / Flooding*
  - *Bomb Threat/attack*

ENVIRONMENTAL EXPOSURES AND CONTORLS:

Controls for Environmental exposures :

- *Alarm Control Panel*
- *Water Detectors*
- *Handheld Fire Extinguishers*
- *Manual Fire alarms*
- *Smoke detectors*
- *Fire Suppression System*
  - *Water-based, Halon system, FM-200, CO_2 system*
- *Logically Locating the Computer Room*
- *Regular Inspection by Fire Department*
- *Fire Proof Walls Floors and Ceilings surrounding the computer room*
- *Electrical surge Protector*
- *UPS / Generators*
- *Emergency Power Off Switch*
- *Power leads from two substations*
- *Wiring in electrical panels and conduit*
- *Prohibiting against eating, drinking and smoking within the information processing facility*
- *Fire resistant office material*
- *Documented and tested emergency Evacuation Plans.*

ENVIRONMENTAL EXPOSURES AND CONTORLS:

- ***Auditing Environmental Controls :***
  - ***Auditing of all above listed controls***

Global Chartered Accountants

www.gcaofficial.org