INVESTMENT ADVISER

CYBER SECURITY AWARENESS CAMPAIGN

For Stakeholders of Investment Adviser (In pursuance of SEBI / BASL compliances initiative)

2022 - 23

SANJAY KADEL & CO.
chartered accountants

ARIA
Association of Registered Investment Advisers

ARIA Partners

Platinum *Partners..*

HDFC MUTUAL FUND
BHAROSA APNO KA

navi mutual fund

WHITEOAK CAPITAL MUTUAL FUND
THE ART AND SCIENCE OF INVESTING

Gold *Partners..*

Edelweiss | MUTUAL FUND

L&T Financial Services Mutual Fund

TATA MUTUAL FUND

Silver *Partners..*

MIRAE ASSET Mutual Fund

ICICI PRUDENTIAL MUTUAL FUND
TARAKKI KAREIN!

Introduction & Agenda

"Our intention creates our reality." – Wayne Dyer

1. Intent

Establish the knowledge, importance and need for Cyber Security, and commitment towards it.

Build awareness of ➔ the elements of cyber security

2. Infrastructure

ICT Infrastructure Environment & Controls related

3. Practices

Secured Practices / Process related

4. Continuity

Business continuity and Incident management related

5. Compliance

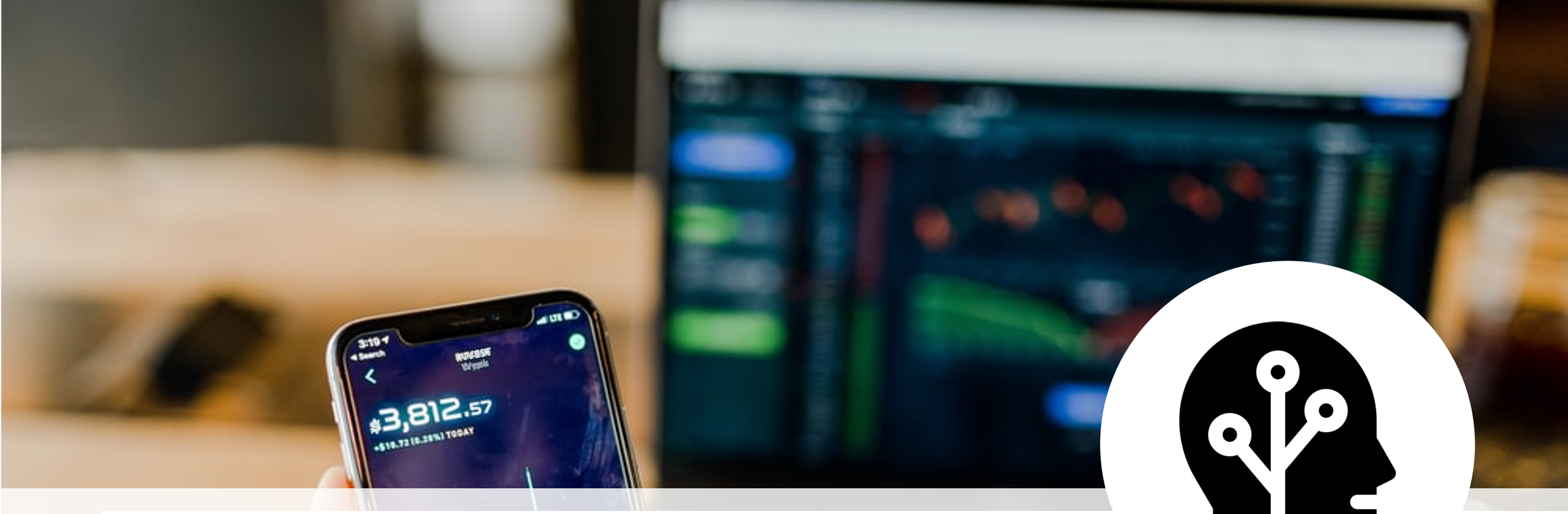
Policies, Contractual, Legal & Regulatory related

For Stakeholders of Investment Adviser (In pursuance of SEBI / BASL compliances initiative)

2022 - 23

SANJAY KADEL & CO.
chartered accountants

ARIA
Association of Registered Investment Advisers



Part 1. Intent

Establish the knowledge, importance and need for Cyber Security, and commitment towards it.

Go to Index page

It's a digital world

[Part 1. Intent]

- Extensive reliance on computer systems and network to process / manage '***Information***'
- Inevitable spread of digital transformation, that has exposed our sensitive data to potential jeopardy.

Information!

[Part 1. Intent]

- '***Information***' is the most valuable asset
- It affects the behavior, decision, an outcome, and the destiny of the Organisation
- To be valuable, Information has to be ...
  - meaningful
  - relevant
  - accurate
  - timely
  - specific
  - organized
  - for a purpose
  - enhance understanding
  - reduce uncertainity

★★★★★

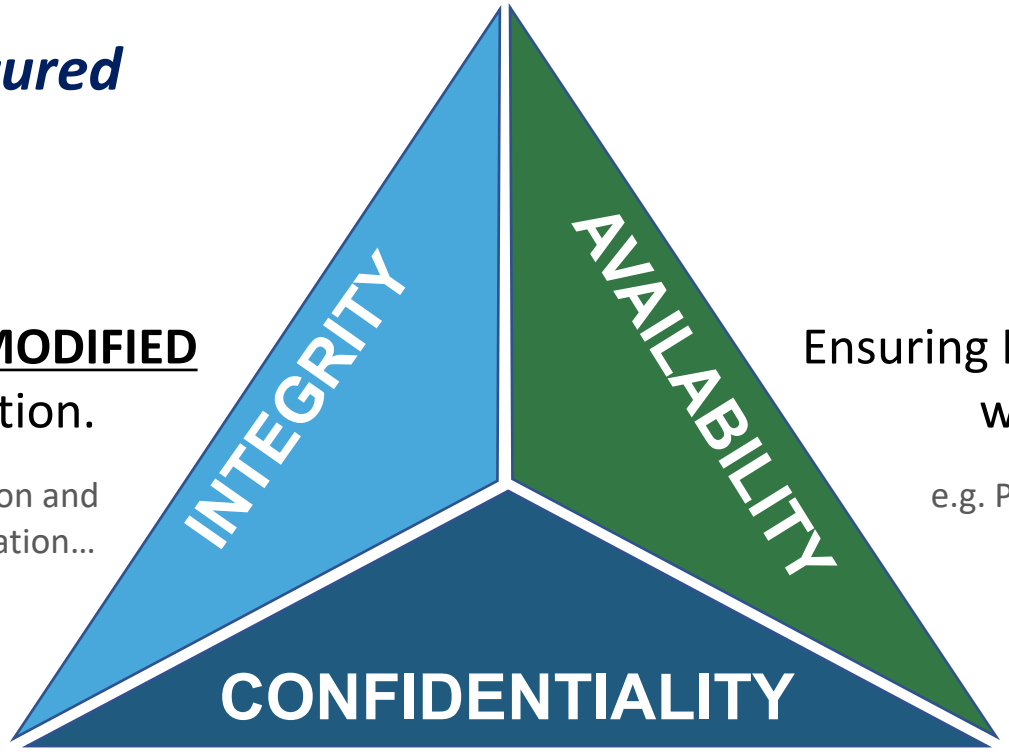
Information Security – CIA

[Part 1. Intent]

Information need to be secured by ensuring CIA

Ensuring data is **NOT MODIFIED** without authorization.

e.g. Modifying critical field values, virus infection and manipulation of numbers, website mis-information…



Ensuring Information is **AVAILABLE** when it is needed.

e.g. Power outages, DOS attacks…

Ensuring Information is not **DISCLOSED** to unauthorized individuals / systems.

e.g. Credit Card info theft, Password breach, Accidental access to sensitive data

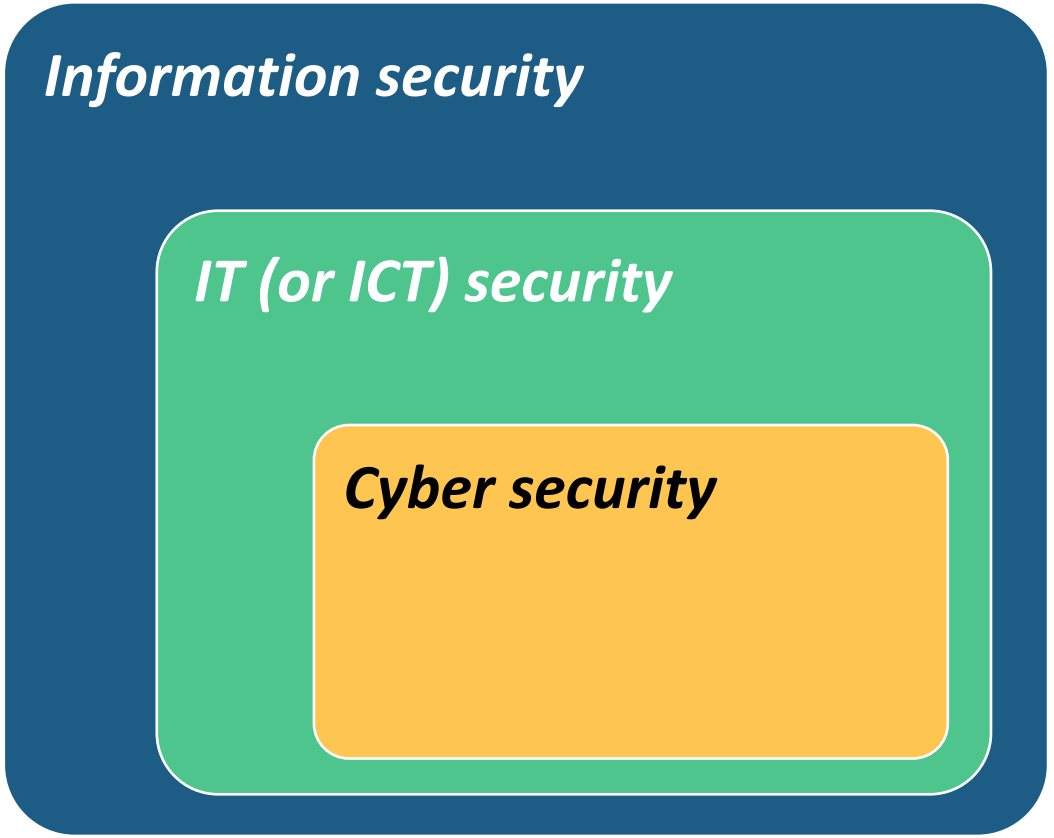
Cyber security

[Part 1. Intent]

Cyber security is the practice of protecting critical systems and sensitive information from digital attacks.

It is often synonymously referred as IT (or ICT) security and Information security.

- Information security deals at ***org-wide level***, in terms of CIA. e.g. ISO27001 establishes ISMS with 14 domains.
- IT (or ICT) security focusses on data and ***technology Infrastructure***. e.g. Servers, Endpoints, Dbs and Networks.
- Cyber security focusses on protection from ***digital attacks***. e.g. Malwares, DoS, SQL Injection, MitM



Impact of security violations

[Part 1. Intent]

Such '***Information***' if not secured, would lead to serious consequences!

- Financial... Non-Financial...
- Physical... Logical...
- Legal... Ethical/Moral...
- Short-Term... Long-Term...
- Serious... Non-Serious...
- To Organization / Employees / all...

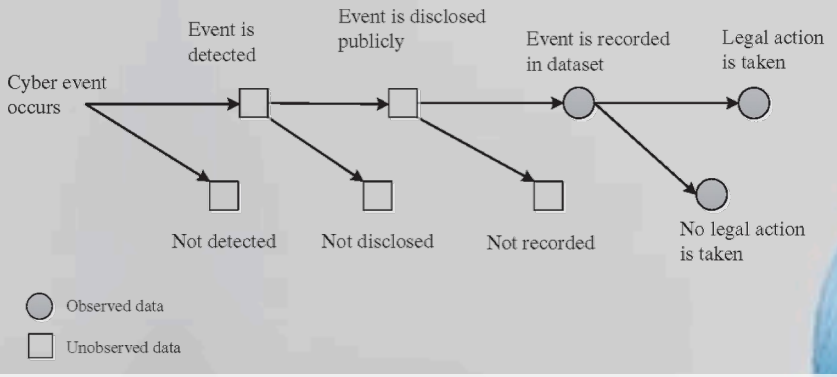
- Loss of Business
- Loss of operational continuity
- Loss of business information
- Loss of Customers
- Loss of Trusts of Employees, Customers, Public, Stakeholders
- Embarrassment
- Bad publicity
- Internal disciplinary action;
- Termination
- Penalties / Prosecution
- ... ...

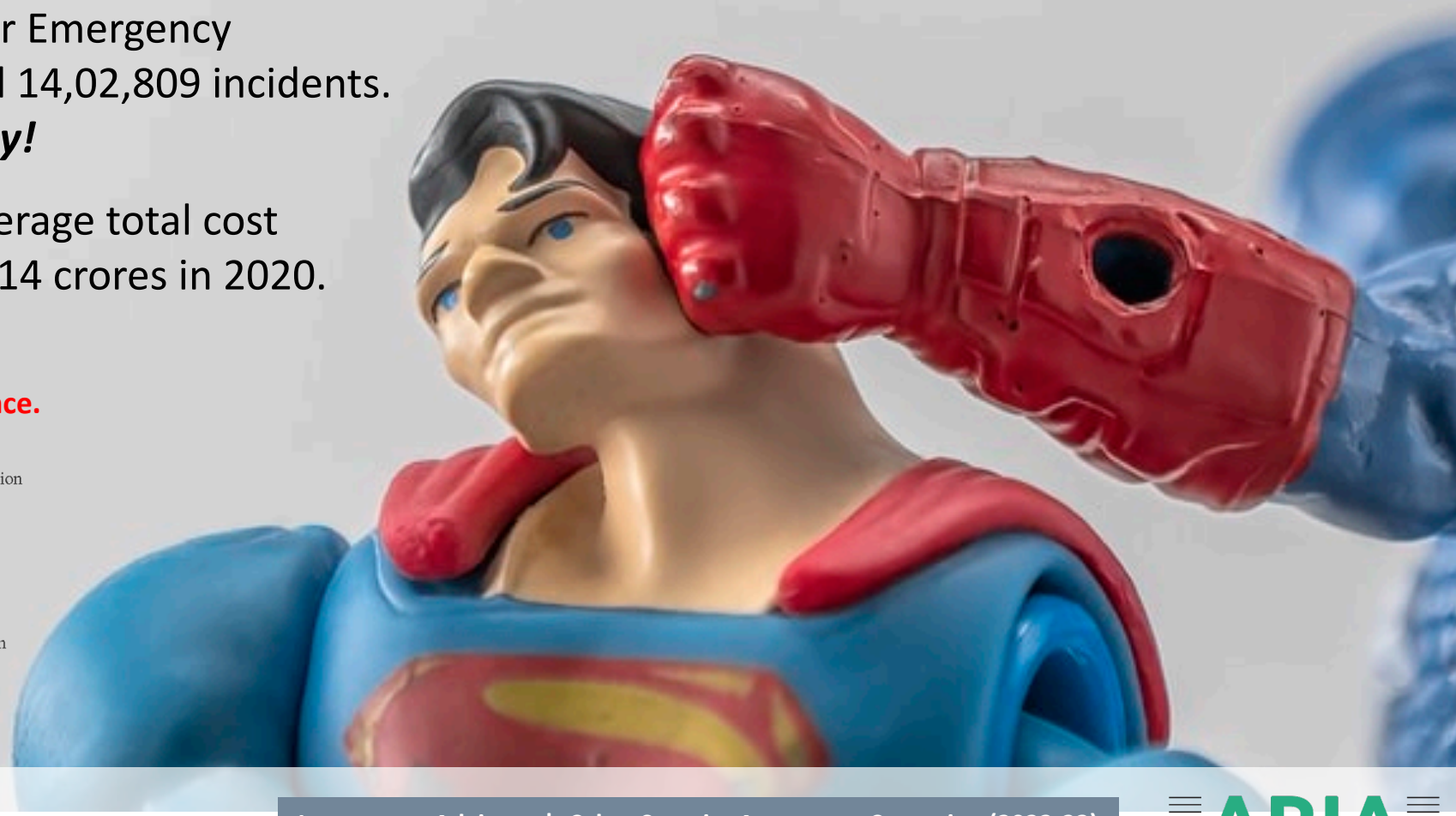
Extent of Impact

[Part 1. Intent]

- In the year 2021, Indian Computer Emergency Response Team (CERT-In) handled 14,02,809 incidents. ***Almost 4,000 incidents every day!***
- According to IBM Security, the average total cost of a data breach in India was INR 14 crores in 2020. ***Almost INR 4,00,000 every day!***

Note: This number is far-lesser than actual occurrence.





★★★★★

Cyber security Incidents

[Part 1. Intent]

Oct. 2020

| Mumbai, was hit by a massive power outage prompting the cancellation of train services which brought the whole city to its knees.

Feb. 2021

| Hackers stole the personal data of 4.5 Mn Air India passengers

Sep. 2021

| Indian SMEs lost yearly INR 7 Cr in cyber attacks

Nov. 2021

| Personal and financial information of nearly 180 Mn PNB customers was left exposed for 7 months.

★★★★★

Cyber security Incidents

[Part 1. Intent]

- July 2022 | SEBI faced Cyber ***security incident*** involving its email system.
  As per SEBI, no sensitive data was lost. Further, FIR is lodged and CERT-In is looped in.
- July 2022 | Hacker groups from Malaysia and Indonesia initiated a ***cyber war*** against India, following Nupur Sharma's recent controversial comments.
  The hacker groups targeted more than 2,000 websites and leaked the database of Andhra Pradesh police as well as PAN card and Aadhaar details of many Indians.

and it continues...

The need

[Part 1. Intent]

Hence, considering the importance of information as an asset, its security, and the potential / extent of impact, if it is not secured,

logical & obvious

there is a need to establish awareness of Cyber security and related practices with all stakeholders!

You! are RESPONSIBLE for your *action* and *inaction*.

You may affect others! and may be affected by others!

★★★★★

The commitment

[Part 1. Intent]

Cyber Security Pledge to build safe digital environment

Let's commit ourselves, to be cyber aware and alert in safeguarding self, organisation and others, against all possible cyber attacks, by implementing secured infrastructure and following secured practices.

Organisations may consider establishing Information security policy and guidelines.

Part 2. Infrastructure

Awareness ➔ ICT Infrastructure Environment & Controls related

Go to Index page

ICT Infrastructure

[Part 2. Infrastructure]

- ***ICT*** refers to Information and Communication Technology
- ***ICT Infrastructure Environment*** comprises of the Servers / Endpoints (Desktop / Laptop), Equipments, Printers, Mobile devices, Software / Applications, databases and Network, Internet, Email and other online services including cloud services.
- Such ICT Infrastructure, which is the vital centre of productivity and operations need to be secured.

ICT Systems & Software

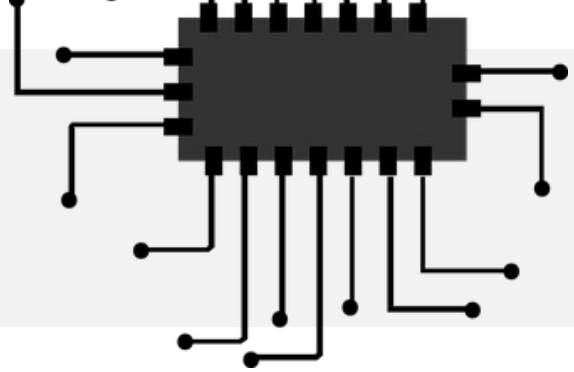
[Part 2. Infrastructure]

Security of the ICT Systems & Software comprise of the following areas / operations process:

1. IT Assets / Infrastructure Management
2. Software Management
3. Access Management
4. Network Management
5. Cloud services
6. Patch Management
7. Service Management (including Change management, ICT services and Backup management)

1. IT Assets / Infrastructure Management

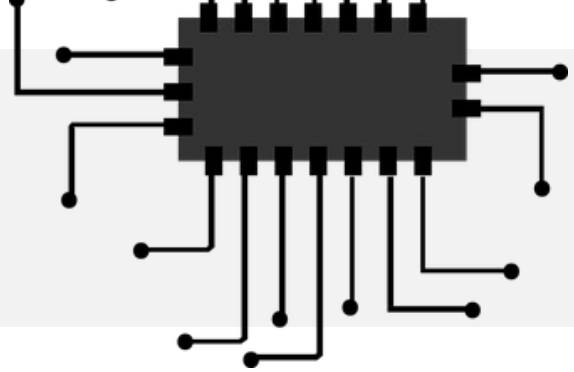
[Part 2. Infrastructure]



- ***Inventory*** of critical ICT assets need to be maintained along with CIA importance and ownership / custody details.
- ***Acceptable use*** of the ICT systems & software shall be as allocated & approved, and communicated.
- At the time of exit of employees / contractors / third party, proper ***return of assets*** has to be ensured.
- ***Information classification*** and ***labelling***, shall be ensured. e.g. Sensitive, Confidential, Internal, Public.
- ***Handling of assets*** shall be ensured sensitively for secure processing, copying, storage, transmission, declassification and destruction.
- Storage of data has to be restricted and controlled in authorised devices and by approved personnel only.
- There should be secure management (CIA) of ***removable media***. e.g. Hard disks (including SSDs), USB drives, Memory cards in devices like Digital Camera, Mobile devices

1. IT Assets / Infrastructure Management (contd.)

[Part 2. Infrastructure]

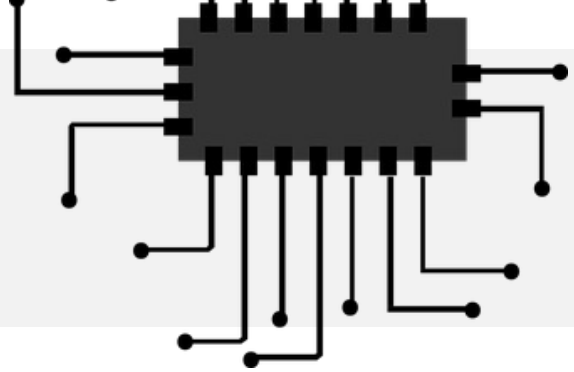


- ***Transit*** of any information, software or media should be approved and marked for 'information sensitivity'.
- Protect the data from unauthorised access, misuse, or corruption. Apply controls like data encryption, restricted access, etc.
- Careful and secured process shall be followed for ***disposal of media*** containing sensitive information. e.g. complete erase of hard disks, secure destruction of media.

- Purchase only from properly evaluated vendors. Maintain an approved vendors list for IT Infrastructure related procurements.
- Plan, provision and monitor the capacity and availability of IT Assets / Infrastructure.
- Perform regular maintenance of the IT Assets including preventive maintenance.

1. IT Assets / Infrastructure Management (contd.)

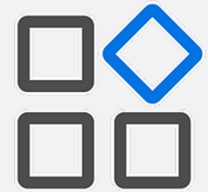
[Part 2. Infrastructure]



- All new information processing systems, upgrades and new versions shall be adequately tested, based on acceptance criteria including security requirements, before acceptance and implementation across the organization.
- Ensure all the critical systems e.g. servers, network equipment, printers, etc. in secure areas and securely mounted.
- Ensure protection from physical damage, spoilage, theft or data loss.
- Ensure hardening of servers, desktops/laptops and network devices based on best practices.
- Enable ***audit trails and logs*** based on need and sensitivity, and ensure they are secured.
- Ensure appropriate ***temperatures*** in the server room and UPS rooms and maintain record.
- Ensure all the critical IT facilities have been connected to backup power (UPS).

2. Software Management

[Part 2. Infrastructure]



- All the operating systems and software / applications shall be procured, installed and used – only as ***required, authorised and approved!***
- ***Software licenses*** shall be tracked and maintained. Over-use of license shall be monitored. Pirated software shall be strictly prohibited!
- Installation of any software shall be strictly admin controlled and approved.
- Prior to installing any ***COTS tools and Open Source tools***, conduct risk assessment. Based on the associated risks, take decision to go ahead or not.
- ***Beware of freeware!***
  Whilst they may come from reputable sources, some freeware contains malware such as viruses, adware and spyware which pose a significant security threat.
  Freeware installation and use should be approved! – It shall not be taken for granted, just because it is use.

3. Access Management

[Part 2. Infrastructure]

- ***Access provisions should be controlled and regulated – and documented! (recorded)***
- Provide only ***need-based access*** (when required) by a ***user registration*** process – not all time or any time
- Provide restricted access to ***relevant personnel*** (who require access) – not to everyone
- Provide role-based ***extent of access*** (selective data) and type of access (read/write/copy/share)
- ***Review and Reconcile*** access privileges on regular basis and disable / update the access details and restrictions. e.g. AD users, Email users, Cloud service users
- For ***exit employees***, ensure the access provisions (to systems, software and services like email, cloud services) are ***disabled*** and ***shared passwords*** are immediately ***changed!***
- As far as possible, always have access-mechanism for each user, and ***name-based users*** (accountable) – not un-accountable users like "team", "admin", "mypc", "server", "hr"

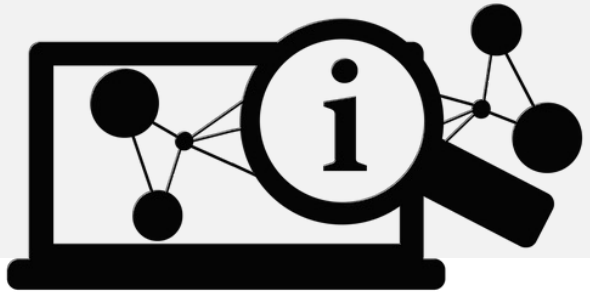
3. Access Management (contd.)

[Part 2. Infrastructure]

- All access should be password-protected and MFA, if possible along with strong password policy
- Enforcing the principle of ***least privilege*** significantly reduces your ***attack surface*** by eliminating unnecessary access rights, which can cause a variety of compromises.

4. Network Management

[Part 2. Infrastructure]



- Network security resources shall protect the business data and related systems from ***unauthorized*** or ***illegal access***.
- Manage the network based on the ***security*** requirements, ***management*** requirements and ***SLAs***.
- Establish and maintain ***Network Diagram*** and System Layouts – starting from Internet reception, LAN or VLAN or MPLS segmentation, Servers, Firewalls, Routers, switches, etc.
- Maintain the ***configurations*** of router, firewall (Policies, ACL), switch, if any, end-point protection, internet restrictions, *content* filtering, UTM, Anti-virus, IDS, IPS, etc. based on the respective policies.
- Ensure optimum ***bandwidth*** and optimum network ***uptime*** at optimum ***speed*** across the organization.
- Ensure adequate ***redundancy*** for critical IT equipment viz. router, firewall, etc.
- Conduct ***VA*** (Vulnerability assessment) / ***PT*** (Penetration testing), if necessary and feasible.

5. Cloud services

[Part 2. Infrastructure]

- The Organization Is Ultimately Responsible for the Security of the Data and Transactions
- Deploy Multi-Factor Authentication (MFA) to the extent possible
- Manage Your User Access to Improve Cloud Computing Security (Refer Access management practices)
  Streamline Identity and Access Credentials Management (IAM)
- Monitor End User Activities With Automated Solutions to Detect Intruders (Cloud IDS, IPS, VA, PT, Endpoint detections and response)
- Ensure data localisation – as per regulations for GRC data – It should be in ***Indian servers only!***
- Provide Anti-Phishing Training for Employees on a Regular Basis
- Consider Cloud-to-Cloud Back Up Solutions.
  Take Advantage of Better Uptime & Redundancy
- Consider Security as Service - under many cloud instances.

Rules of the game are same! field is different.

6. Patch Management

[Part 2. Infrastructure]

- Patch management shall be followed for all Servers / Endpoints (Desktop / Laptop), Equipments, Mobile devices, databases and Network devices.
- OS patches should be downloaded, tested and approved before pushing on to the relevant systems.
- Certain devices may need firmware upgrade, have to be ensured.
- Antivirus (including endpoint protection modules like antimalware, etc.) shall be configured on all systems and enabled. Real-time protection should be enabled.
- It shall be configured appropriately and secured (restricted) to ensure that users do not change the configuration or disable it.
- Regular updates of Antivirus definitions (endpoint definitions) shall be ensured, for up-to date protection.
- Users shall run the need-based scans of devices / media, when required.

7. Service Management

[Part 2. Infrastructure]

(Service management including Change management, ICT services and Backup management)

- Any proposed changes to the baseline IT environment, shall follow ***change management*** process (logged, impact analysis conducted, risk assessment done, and approved).
- Handle ***IT related issues*** and service requests promptly and appropriately.
- Ensure uptime & availability of all IT facilities.
- Conduct ***periodic reviews/checks*** regularly covering ICT Infrastructure Environment and related controls.
- Personnel assigned for IT (or ICT) Operations should be periodically ***trained in technology / security*** aspects and updated with latest developments.
- ICT operations shall ensure ***backups*** are taken (with appropriate methodology), kept at secure place (onsite, offsite or cloud), safely maintained (encryption at rest) and tested for restoration regularly.

Part 3. Practices

Awareness ➔ Secured Practices / Process related

Secured Practices / Process

[Part 3. Practices]

Information Security is an IT Problem?

- 10% of security safeguards are Technical.
- Whereas 90% rely on users (You) to adhere to secured practices / best practices / process.

The lock on the door..... is 10%

Remembering to lock – checking to see if it is closed – Ensuring others do not prop the door open – Keeping control of keys..... is the 90%

Secured Practices / Process

[Part 3. Practices]

Adopting best practices and technologies can help you and your organization implement strong cybersecurity that reduces vulnerability to cyber attacks and protects critical information systems.

Certain areas of Secured Practices / Process are as follows:

1. Password practices
2. Workstation security
3. Laptop security
4. Mobiles security
5. Mobile App practices
6. Email practices
7. Internet use practices
8. Antivirus use practices
9. Backup practices
10. Security Incidents reporting practices
11. Social media practices
12. Financial Transactions practices
13. Social Engineering safeguard practices

★★★★★

1. Password practices

[Part 3. Practices]

Framing Passwords

- Don’t use a word that can be found in a dictionary
- Use min. atleast 8 characters length
- Passwords should include alphabets + numerics + special chars
- Don’t frame same passwords for all applications
- Don’t make it easily guessable based on your public infos
- Don’t make it guessable based on your user id
- Don’t repeat the passwords on change
- When framing Passwords, also ensure that the Hints, the Secret questions and answers meet the strength and complexities
- Don’t use sequences of keys in keyboards or order of alphabets

1. Password practices (contd.)

[Part 3. Practices]

Using Passwords

- Don’t visibly type in front of others
- Use virtual keyboard, if available
- Don’t let browsers or softwares or websites remember the password
- Don’t use on un-official or friend’s or public computers
- Don’t share with others and change immediately, if shared
- Don’t use passwords on suspicious websites

1. Password practices (contd.)

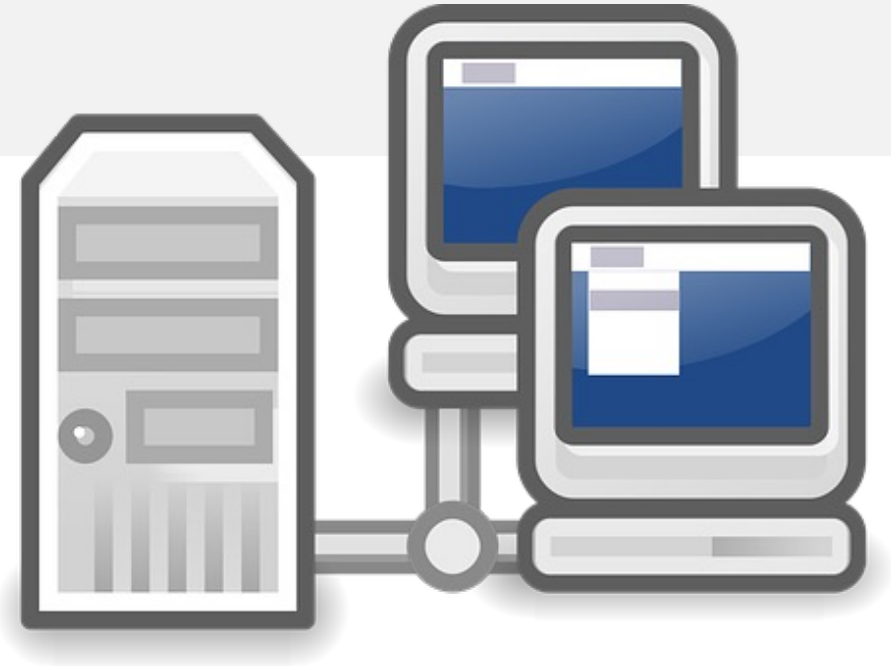
[Part 3. Practices]

Maintaining Passwords

- Don’t store / note passwords in clear text.
- Don’t write down as to be easily accessible or visible to others
- Don’t make post-it notes of your passwords
- Change them immediately upon first receipt
- Change the default passwords immediately in new h/w or s/w
- Change them frequently – 45 days
- Change them immediately upon suspicion
- Ensure strength of the password of passwords
- Don’t share the secret questions or answers with anyone
- Don’t store passwords in (mostly untrusted) mobile apps or s/ws

2. Workstation security

[Part 3. Practices]



Controls for the period when it's attended by You

- Sharing – Share folders /files only if necessary
- Sharing – Cancel sharing once requirement is met
- Sharing – Provide only required permissions (read / write)
- Ensure non-visibility by people around

Controls for the period when it's un-attended

- Log-off before leaving the device
- Set a 5-minute screen-saver with password protection
- Have a boot password / power-on password
- Have a operating system logon password
- Encrypt & Password Protect it

3. Laptop security

[Part 3. Practices]

In addition to Workstation controls...

Controls for the period when it's attended by You

- Have a personal firewall for the Laptops
- Ensure proper ergonomics and house-keeping around else it might be dropped / damaged
- Ensure non-visibility by people around

Controls for the period when it's un-attended

- Never leave it un-attended at places other than home/office
- Physically secure it to the desk / grill-window with a lock-down cable
- Have the name and address of the user labelled, to facilitate its return in the event of a loss

4. Mobiles security

[Part 3. Practices]

Controls for the period when it's attended by You

- Ensure non-visibility by people around
- Ensure proper ergonomics and house-keeping around else it might be dropped / damaged
- Turn off wireless interfaces when not necessary
- Install anti-virus software
- Do not share phone-device with kids, naive users and others
- Lock keypad / touch when not required to avoid accidental calls or deletion of data

4. Mobiles security (contd.)

[Part 3. Practices]

Controls for the period when it's un-attended

- Never leave it un-attended at any place
- Have the name and address of the user labelled, to facilitate its return in the event of a loss
- Enable mobile tracking facility, Remote-wipe facility
- Lock Keypad / touch before leaving the device
- Set auto lock every 2-minutes with password protection
- Have a power-on password
- Encrypt & Password Protect it

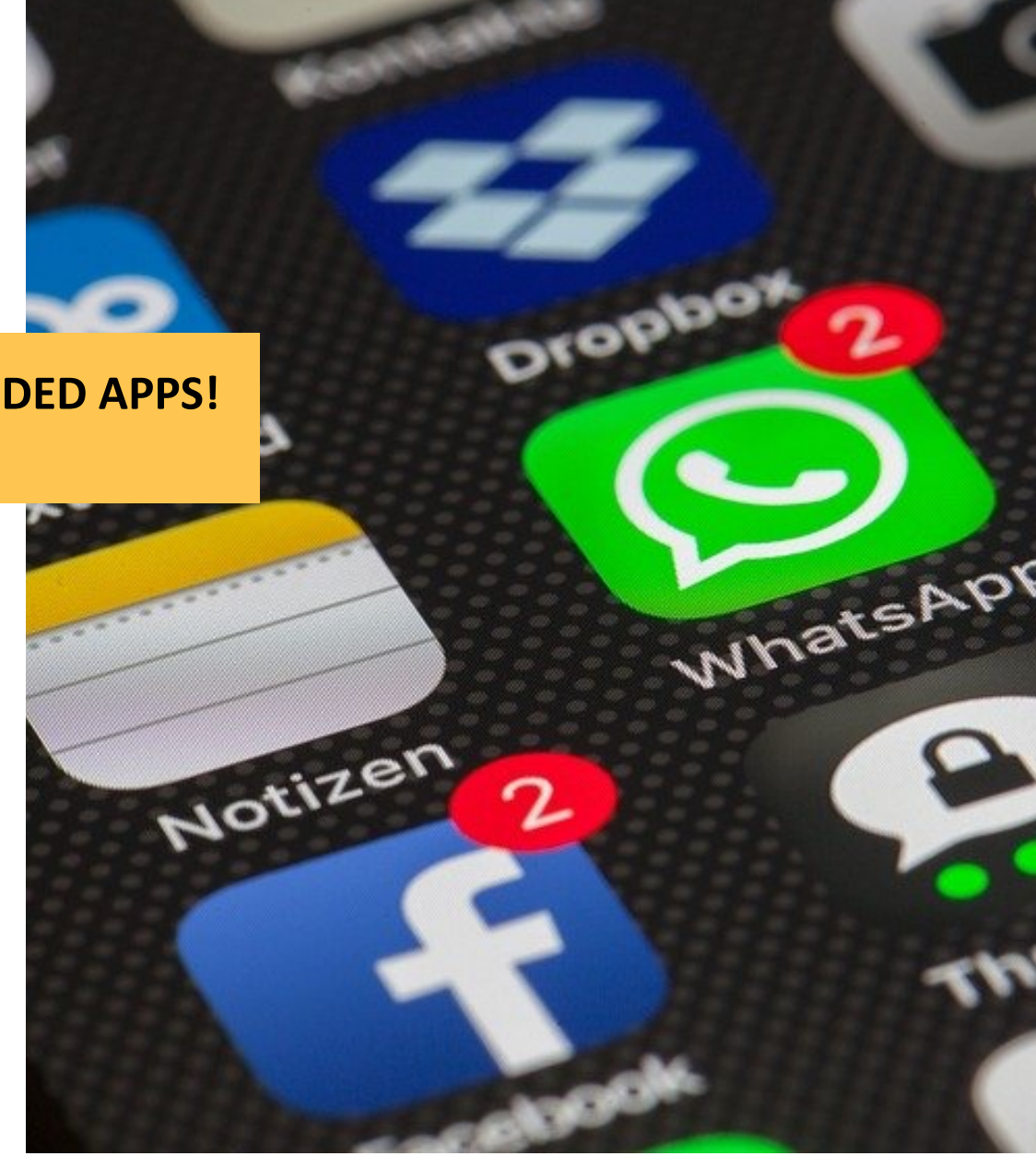
5. Mobile App Practices

[Part 3. Practices]

First and Last Rule: Install only needed apps! ABSOLUTELY NEEDED APPS! Which app to use! Which to not! Decide that first.

- Install only trusted apps!
- Don't give access to apps to access for everything.
  Be selective. Be careful.
- Secure access to – Microphone / Camera / Phone book.
- Secure access to – Photos / Message logs / Root.
- Apply MFA
- Don't allow to store card info.
- Keep apps updated.
- Change app login credentials atleast 45 days once.

Many more.. stay vigilant.



6. Email practices

[Part 3. Practices]

Controls related to Receiving

- Do not open or reply to spam messages.
- Do not open or reply to suspicious e-mails.
- Do not open un-solicited emails from strangers whatever subject line may read.
- Do not open attachments with macros or executable files unless it is from very very very trusted source
- Do not read or waste time on un-official messages during official time (vice versa is encouraged though!)
- Do check personally or through other modes of communication, in cases where an email requires critical action
- Beware of Phishing Emails, Spoofed emails

6. Email practices (contd.)

[Part 3. Practices]

Controls related to Sending

- Use the mailing system for official purposes only
- Send file attachments only if absolutely necessary
- Do not reply / forward spam messages.
- Do not forward chain letters. It's the same as spamming!
- Do not send confidential / critical business information without encryption & password
- Double-check the Email Address of Recipients before sending
- Check whether you have attached the proper files and not those belonging to others or those infected with virus
- Do not send 'very-large' attachments. Use hyperlinks instead.
- Use Official Disclaimers with Email-signatures

6. Email practices (contd.)

[Part 3. Practices]

Controls related to Maintenance / Usage

- Periodically backup your email folder
- Password Protect the Email-Client and Email-Client-Folder
- Do not treat Emails as a data storage but only as communication tool. Take out necessary attachments and store in usual file-structure of organization.
- When using web-mail on un-official devices, be sure to log off after use
- Use Emails on Mobiles and other Mobile devices only upon authorisation from the organization

7. Internet use practices

[Part 3. Practices]

- Visit only trusted websites
- While surfing beware of bad-waters!
- Use internet for official purpose only during official time
- Pay attention to warnings from your browser – read in your interest!
- Employees may be monitored for any internet activities
- Not everything on Internet is authenticated information and hence, double-check before using such information
- There's no free lunch in the world and hence, beware of free softwares, songs, videos, images and other information.
- Use Internet security and firewalls and do not open infected webpages
- Beware of real-looking fake web pages

8. Antivirus use practices

[Part 3. Practices]

- Use only approved Anti-virus software
- Do not turn off or disable scheduled & real-time virus-scan
- Run full scan of your system once in 7 days
- Run anti-virus updates if not automatically set and running
- User possession or development of viruses or other malicious software is prohibited and punishable as per IT Laws.
- Inform / Report the Virus or Infection warnings
- Do not use USB drives, external media without scanning

9. Backup practices

[Part 3. Practices]

- Desktop backup is the responsibility of the end-user
- End user to identify critical data that needs to backed & frequency
- Include email files in your list of critical files for backup
- Ensure before Backup that the data is virus-free
- Ensure encryption / password for backup media
- Ensure safe custody of backup media
- Ensure off-site backup as per ISMS at your organization
- Test Backup restoration at regular intervals
- Ensure Backup logs are maintained in system or manually
- Ensure approved methodology for backup and authority for backup
- While Disposal – ensure shredding, destruction, erasure

10. Security Incidents reporting practices

[Part 3. Practices]

- Report security incidents & breaches to HoD or IS Manager
- Report & respond to security incidents & security breaches

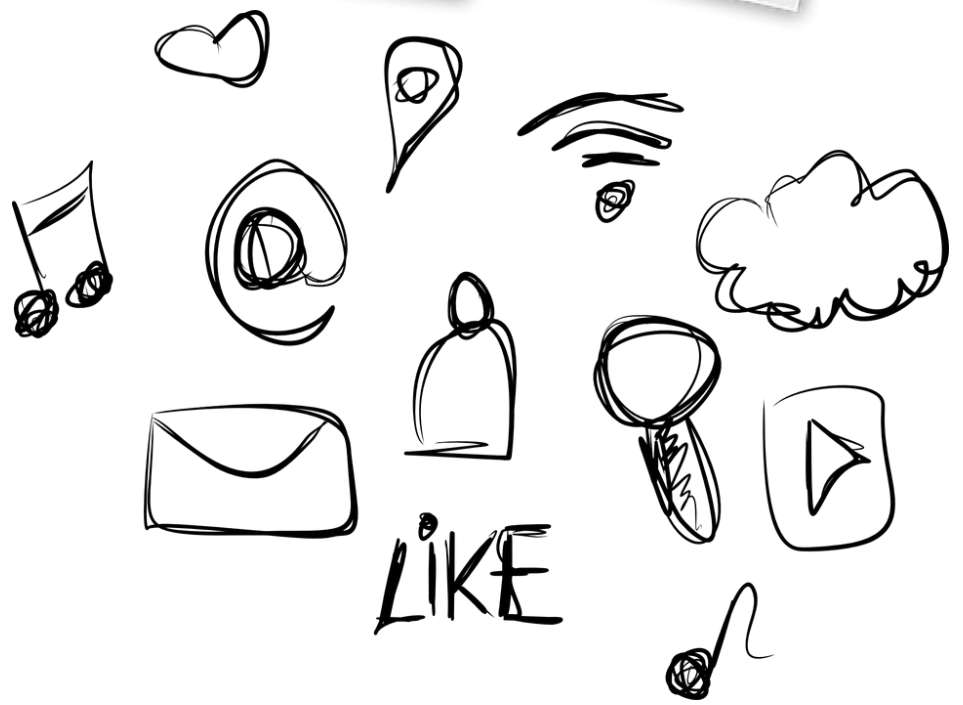
An incident may relate to –

- Suspected hacking attempts,
- Loss of information,
- Hardware resources and components,
- Virus incidents, Failure / crash of IT equipment,
- Power problems and
- Loss of data,
- Natural calamity or disaster,
- Software and Operational failure / errors

11. Social media practices

[Part 3. Practices]

- Don't reveal too much – photos, personal updates, etc. Be careful!
- Avoid "FOMO"
- Configure privacy settings properly
- Don't go friend-shopping. Not 'entire world' is your friend. Add friends who are really known to you..
- Don't interact too much. Block all – Allow some!
- Opt-out of targeted advertisements. Beware of ***adware-malware!***
- Don't scatter social media accounts on all devices unnecessarily
- ***Build a positive online reputation..***
- Think before you 'post'



12. Financial Transactions practices

[Part 3. Practices]

- Don't fall to urgent / phishing communication – call, sms, email, etc.
- Don't enable "remember password"
- Don't search for the financial platforms or services like banks, etc. through google. It will be phished!
- Don't store card information – while online purchases, etc.
- Don't enter password before your nearby people.
- Ensure https is enabled.
- Beware of keyloggers. Use virtual keyboard wherever available.
- Now-a-days 'Secure message' is very helpful. Enable that in the bank site.
- Don't keep common password for all financial transaction platform.
- Enable MFA.
- Configure daily transaction limits, wherever possible.
- Wherever using card details – ensure they are PCI-DSS certified.

13. Social Engineering safeguard practices

[Part 3. Practices]

“The Clever Manipulation of the natural human tendency to trust.”

- Social engineering is the practice of obtaining confidential information by manipulation of legitimate users.
- A social engineer will usually use the telephone / email / Internet / Social Networking Messaging / sometimes personal interaction....

  to trick people into revealing sensitive information, or getting them to do something that is against typical secured practices.

13. Social Engineering safeguard practices (contd.)

[Part 3. Practices]

Signs of social engineering attacks to recognize:

- Shoulder Surfing, Dumpster Diving, New house-keeping
- Sudden Trustworthiness, Charm, Attraction and Closeness
- Refusal to give contact information
- Rushing by the Social engineer
- Requesting forbidden information
- Name-dropping
- Intimidation / coercion / threatening
- Very high dreams and higher promises
- Asking for immediate action and rushing towards it
- Small mistakes (misspellings, misnomers, odd questions)

Go to Index page

Part 4. Continuity

Awareness ➔ Business continuity and Incident management related

Go to Index page

Business continuity

[Part 4. Continuity]

Business continuity planning (as a process) involves designing and implementing plans that protect against business disruption in case of crises and disasters.

e.g. Power failure, Failure of IT System, Natural disaster like earthquake, flood, cyclone, Fire, Accident, War and Terrorist attacks

It covers:

➔ Business Resumption Planning (Focus on Operations)
➔ Disaster Recovery Planning (Focus on Information Technology)
➔ Crisis Management (Coordination, Avoiding or minimising damage to Profitability, reputation or ability to operate)

- Organisation shall document the business continuity plans (BCP) and disaster recovery plans (DRP)
- Identify critical systems, processes and functions and conduct Business Impact Analysis (BIA)
- Establish Recovery time objective (RTO) and 'pain threshold' Maximum tolerable period of disruption (MTPOD)

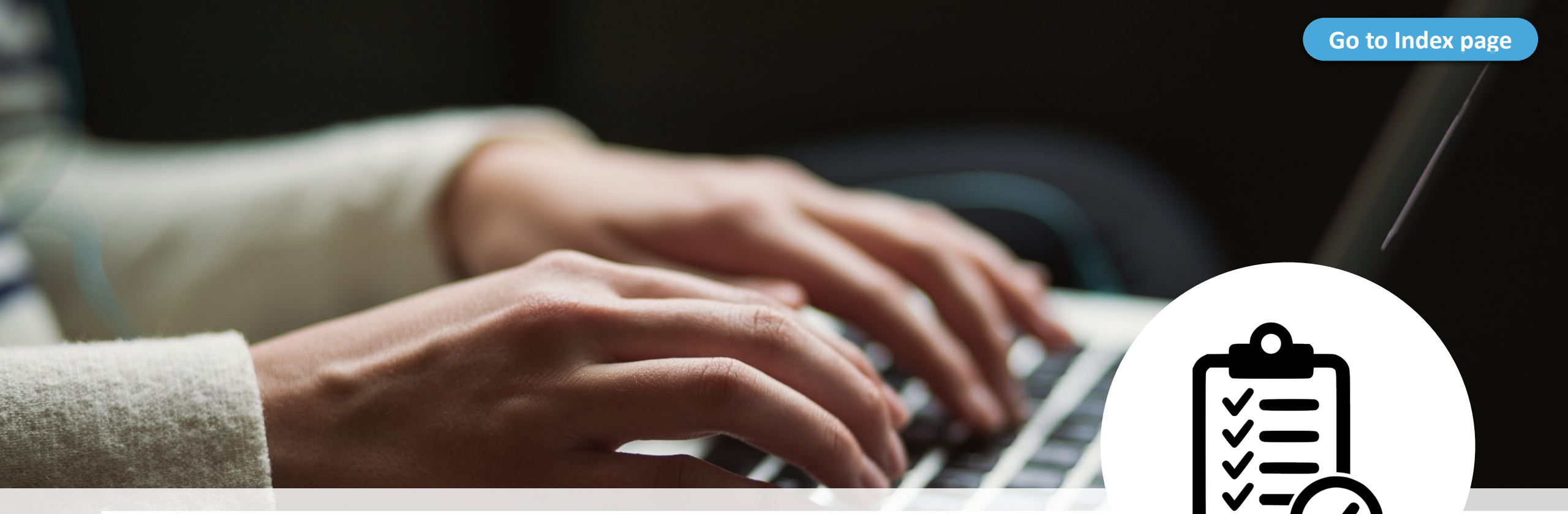
Incident management

[Part 4. Continuity]

- Proper cyber security Incident management system, should be established in the organisation.
- ***Cyber security Incident*** shall be defined.
- Establish processes for – reporting, handling, response, assessment and resolution.
- Evidences & Learnings be documented.

- Also refer - Security Incidents reporting practices

Go to Index page



Part 5. Compliance

Awareness ➔ Policies, Contractual, Legal & Regulatory related

Go to Index page

Compliance process

[Part 5. Compliance]

Identify relevant compliance requirements with Policies, Contractual obligations, Legal & Regulatory mandates.

- The specific safeguards, controls / practices and individual responsibilities shall be established to meet all types of compliance requirements.
- Ensure safeguards to ***protect IPR*** information / materials.
- Important records / data shall be ***protected in terms of CIA*** e.g. disclosure, loss, destruction and falsification.
- Ensure ***data privacy safeguards for PII***, in accordance with relevant legislation.
- Ensure the ***information processing facilities*** are used for organisational purposes only.
- The cyber security approach shall be ***reviewed*** at regular intervals.
- Ensure ***adherance*** to the cyber security policies, procedures, SLAs, NDAs, best practices and standards.

Caveat

[Part 5. Compliance]

The design of controls and extent of cyber security best practices, to be adopted for the organisation / user, should be based on business requirements (nature and size), risk assessment and feasibility (technical, financial and operational), and

compliance requirements! arising from policies, contractual obligations, legal & regulatory mandates.

Disclaimer

Terms of use of this presentation

- Information contained in the ***cyber security awareness campaign***, and related notes / documents / guidelines / interpretations / publication provided in connection to such awareness campaign, for RIA's compliance to cyber security awareness campaign, are intended for use, primarily by the relevant members of ARIA only, to the extent suitable to their situation / case. If you are not the intended audience of these publication or artefacts, an agent of the intended audience or a person responsible for delivering the information to the named entities, you are notified that any use, distribution, transmission, printing, copying or dissemination of this information in any way or in any manner is strictly prohibited.
- Every effort has been made to avoid errors or omissions in these publications and artefacts. In spite of this, errors may creep in. Any mistake, error or discrepancy noted may be brought to our notice at membership@aria.org.in (more contact details at https://aria.org.in) which shall be taken care of in the next update and release.
- Though, we may provide, to the best extent possible, a reasonably proper publication or artefact, there may be, alternative approaches / interpretations / improvisation possible.
- It is notified that neither ARIA nor the authors, including, members of Sanjay Kadel & Co. Chartered Accountants, or anyone connected herewith will be responsible for any damage or loss of action to any one, of any kind, in any manner, therefrom. It is suggested that to avoid any doubt the reader, receiver, or user of the information contained in these publications or artefacts, should cross-check all the facts, law and contents of the publication with original source, publication or notifications.

INVESTMENT ADVISER

CYBER SECURITY AWARENESS CAMPAIGN

Wishing you <secured> digital star! in work and life.

For Stakeholders of Investment Adviser (In pursuance of SEBI / BASL compliances initiative)

2022 - 23

SANJAY KADEL & CO.
chartered accountants

ARIA
Association of Registered Investment Advisers

ARIA Partners

Platinum *Partners..*

HDFC MUTUAL FUND
BHAROSA APNO KA

navi mutual fund

WHITEOAK CAPITAL MUTUAL FUND
THE ART AND SCIENCE OF INVESTING

Gold *Partners..*

Edelweiss | MUTUAL FUND

L&T Financial Services Mutual Fund

TATA MUTUAL FUND

Silver *Partners..*

MIRAE ASSET Mutual Fund

ICICI PRUDENTIAL MUTUAL FUND
TARAKKI KAREIN!