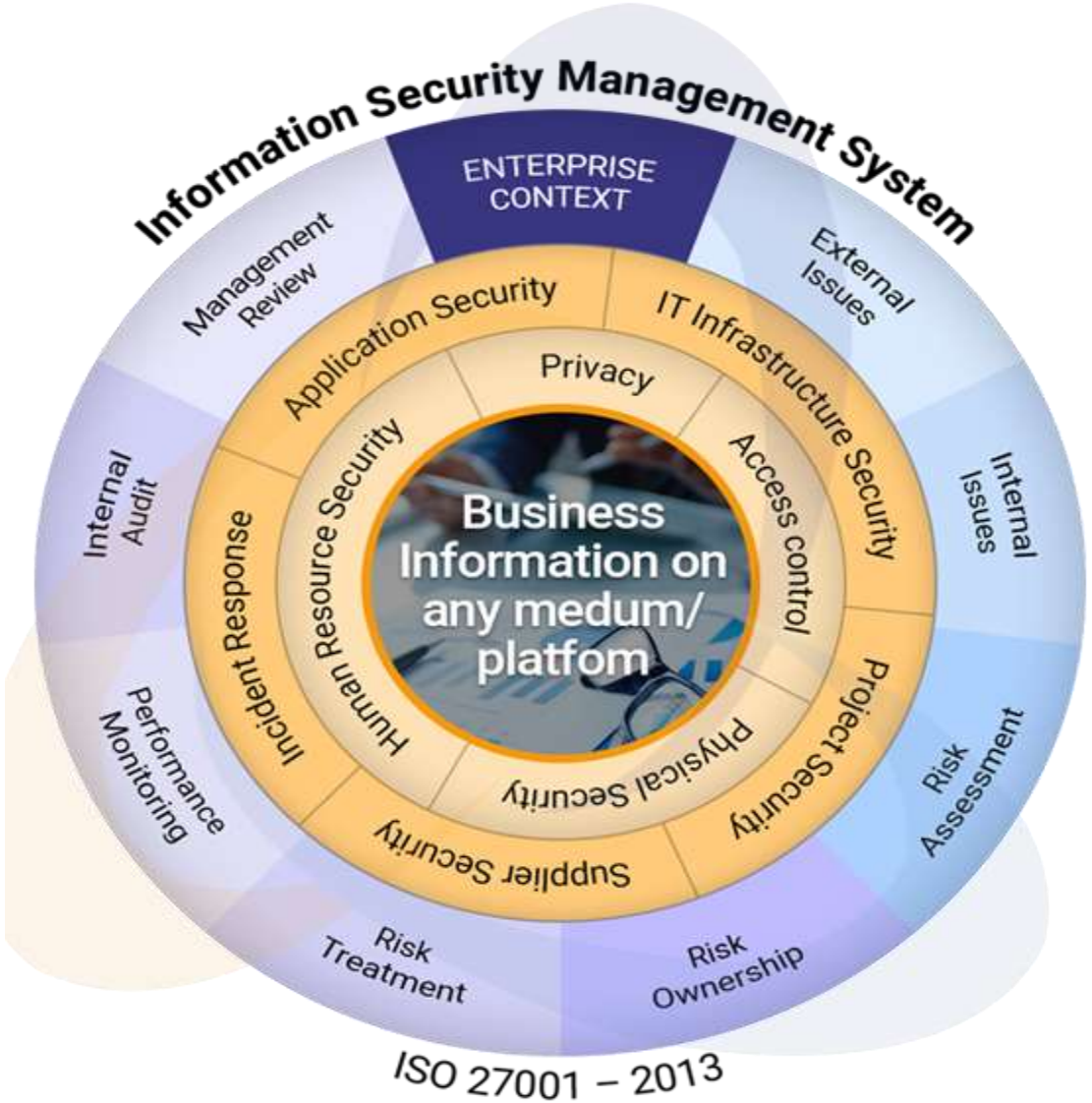
Compliance & Security Framework

(Chapter -2 : DISSA Course)

Arijit Chakraborty

May 30, 2021

ISO 27001

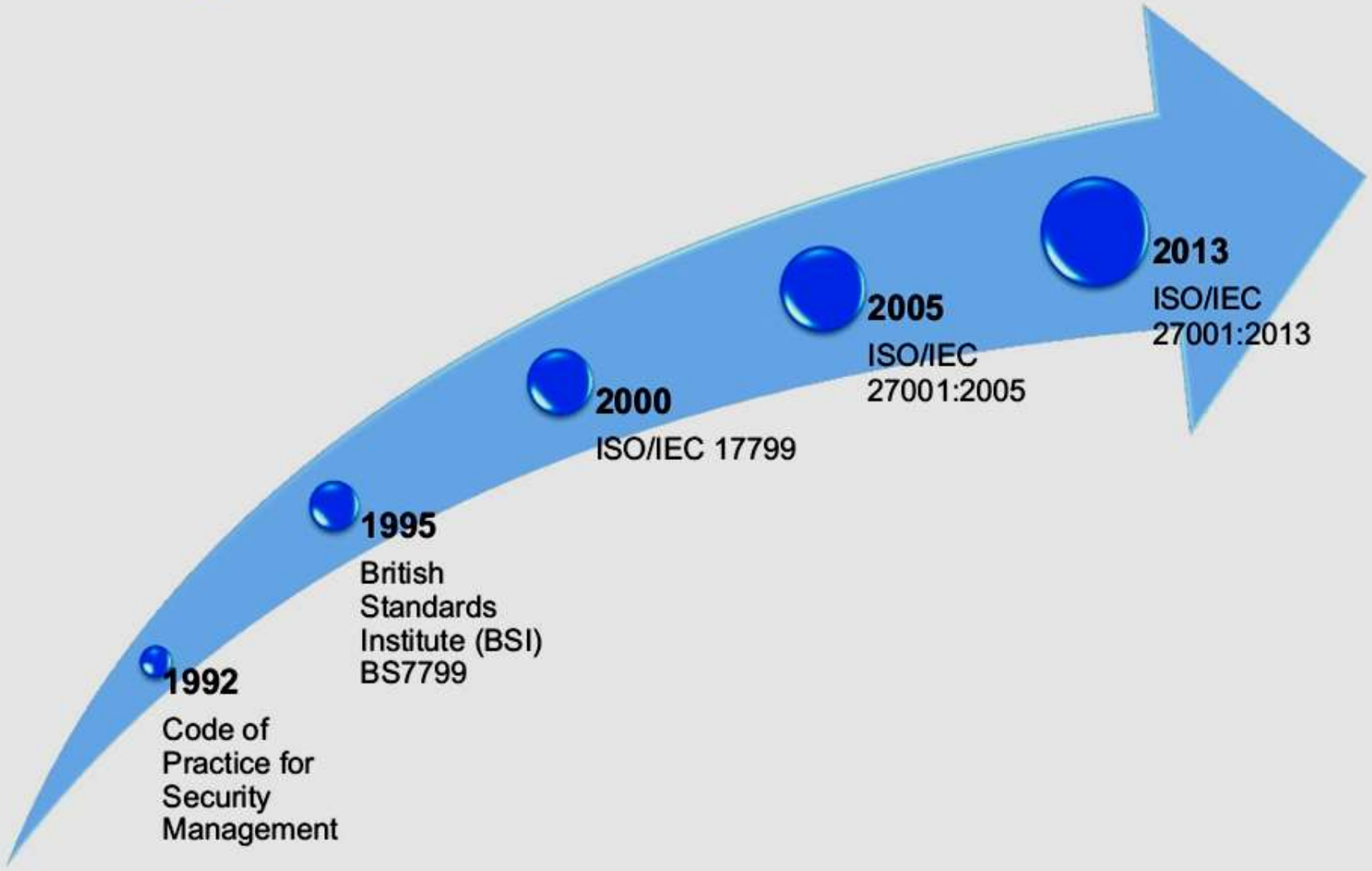

Information Security Management System
ENTERPRISE CONTEXT
External Issues
Internal Issues
Risk Assessment
Project Security
Physical Security
Supplier Security
Human Resource Security
Incident Response
Application Security
IT Infrastructure Security
Privacy
Access control
Business Information on any medum/ platfom
Risk Ownership
Risk Treatment
Performance Monitoring
Internal Audit
Management Review
ISO 27001 – 2013

Purpose & importance

The goal of ISO 27001

- to provide a **framework of standards for how a modern organization should manage their information and data.**
- Risk management is a key part of ISO 27001
- ***Benefits include:***
- Increased reliability and security of systems and information.
- Improved customer and business partner confidence.

History of ISO/IEC 27001



Needs of ISO 27001

- *Comply with Legal Requirements*
- *Achieve Competitive Edge*
- *Lower Cost*
- *Better Organization*


Reduce the chances of security breaches within your IT environment
Control of IT risks
Confidentiality of the information
Lower costs
Minimization of IT risks, possible damage and consequential costs
BENEFITS OF ISO 27001
Systematic detection of vulnerabilities
Competitive edge due to recognized standard
Fulfillment of internationally recognized requirements
Increase in trust with respect to partners, customers and the public
A structured method to address compliance requirements

IMPLIMENTATION PROCESS

- Step 1: Assemble an implementation team
- Step2: Develop the implementation plan
- Step 3: Initiate the ISMS
- Step 4: Define the ISMS scope
- Step 5: Identify your security baseline
- Step 6: Establish a risk management process
- Step 7: Implement a risk treatment plan
- Step 8: Measure, monitor and review
- Step 9: Certify your ISMS

ISO 27001 CERTIFICATION PROCESS

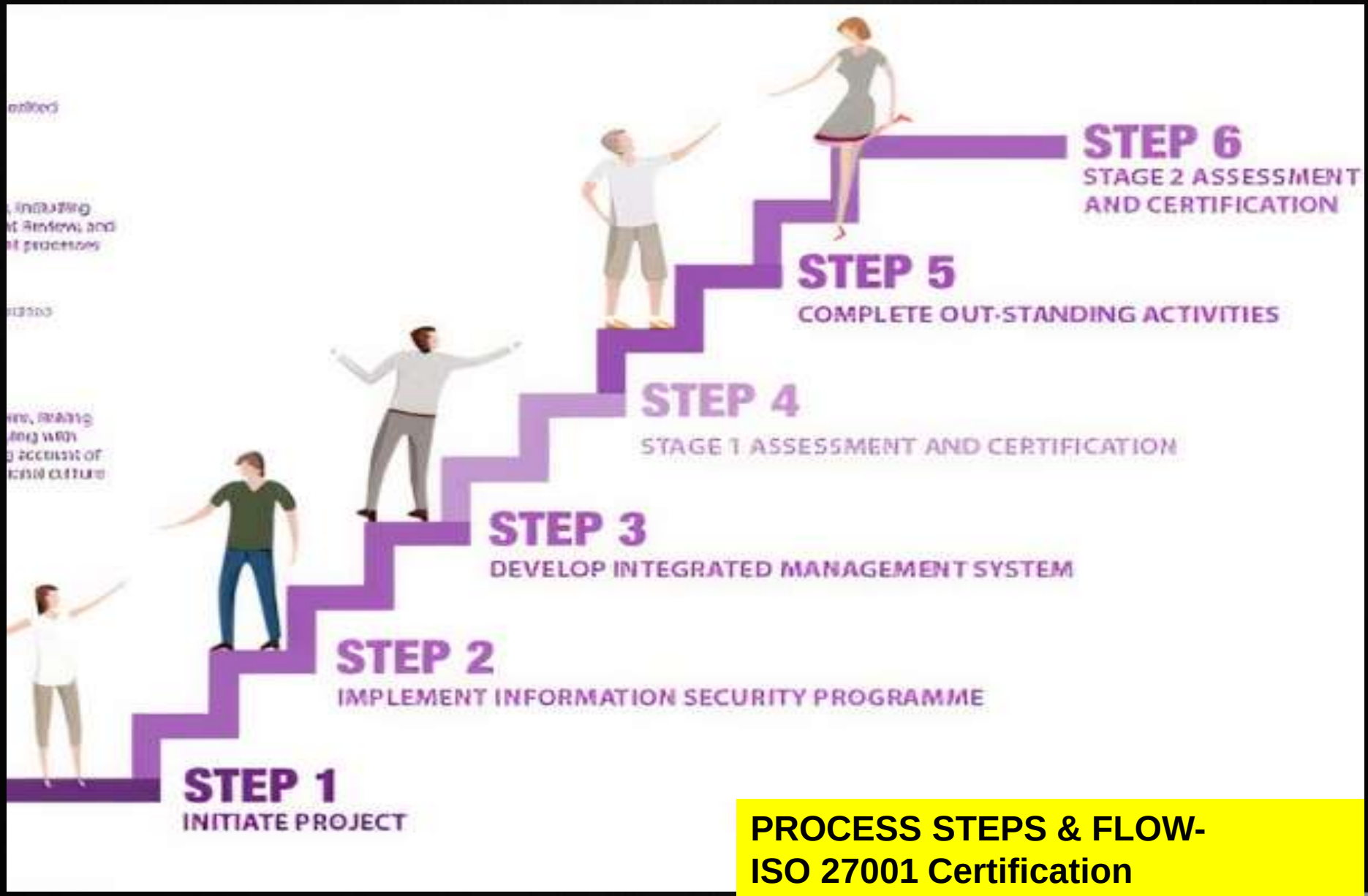
1. **A certification body is hired** to conduct a basic review of the ISMS to look for the main forms of documentation.

2. **An in-depth audit** is then performed by the certification body where the components of ISO 27001 are checked against the organization's ISMS.

3. **Follow-up audits** are scheduled between the certification body and the organization to ensure compliance is kept in check.

PROCESS FLOW- ISO 27001

CERTIFICATION PROCESS



PROCESS STEPS & FLOW-
ISO 27001 Certification

- ***Testimonial - Apolo Gleneagles***

"The trainings and audits were comprehensive enough covering all business areas. This has led to building good understanding amongst all the employees and continual improvement in our systems."

-- Sambit Prakash, CISO & Head on ISO 27001 *assessment and training services.*

- ***Testimonial - Reliance Nippon Life Insurance***

"*ISO Auditor's contribution in terms of audit findings & feedback has helped RNLIC to strengthen its process and systems.*"

- *-- Kapil Punwani, AVP - Risk Management on* ISO 22301 *&* ISO 27001 *assessment services.*

ISO 27001 Case Study - HP

ISO/IEC 27001 is the only auditable international standard which defines the requirements for an Information Security Management System (ISMS). The standard is designed to ensure the selection of adequate and proportionate security controls.

Onsite Information Security Controls

Controls that were considered essential for the onsite team from HP software Professional Service Global Delivery INDIA Centre were:

- **Controls considered in-scope by HP**
- ✓ HR Security
- ✓ Communication & Ops management
- ✓ Access control
- ✓ IS Incident management
- ✓ BCP Management
- ✓ Compliance

HP Software Professional Services Global Delivery India Center

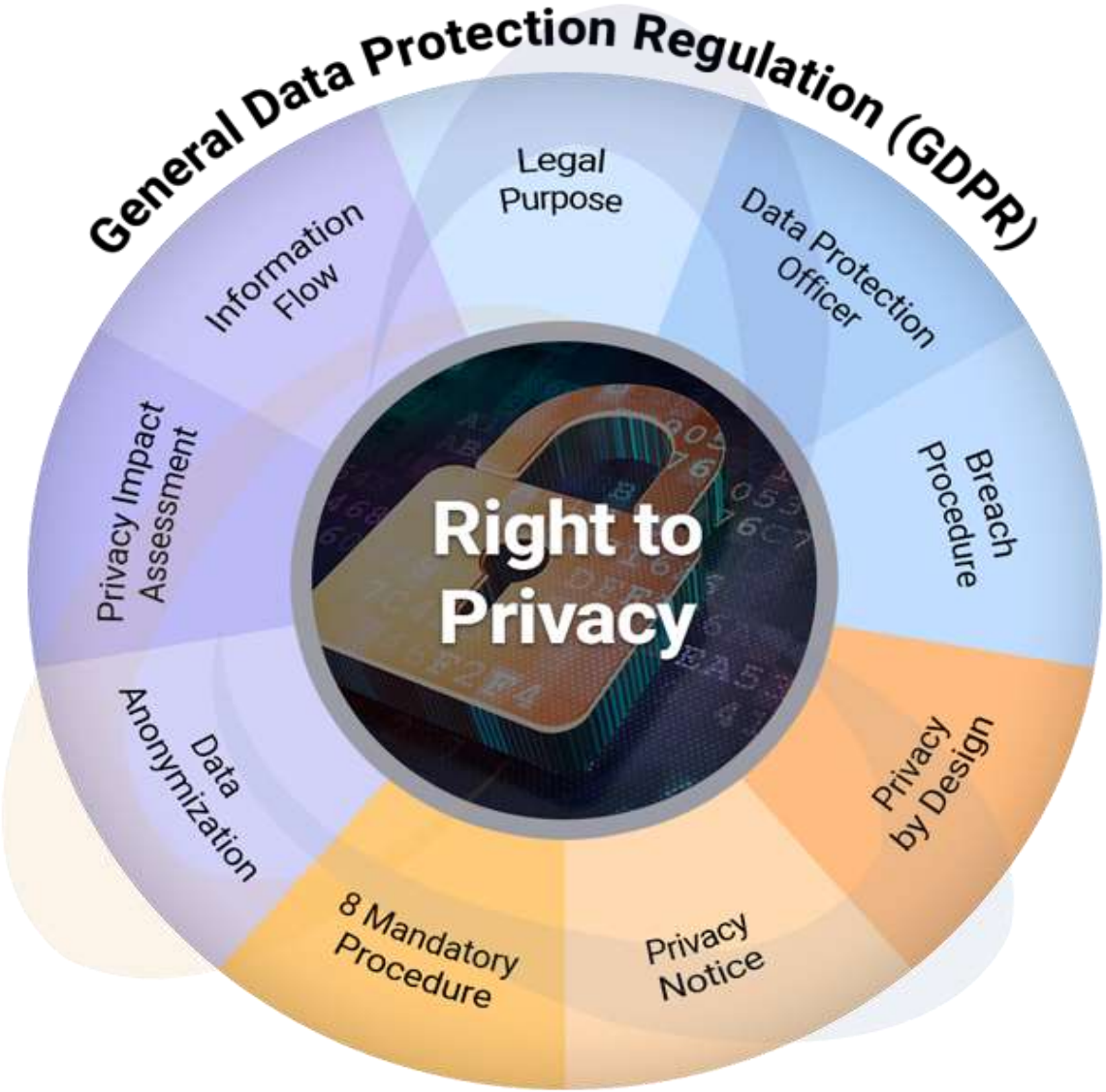
Professional Services Global Delivery Center, India is part of the HP Software Professional Services Business Unit. PS–GDC India operates from Bangalore and Chennai locations with staff strength of approximately 271.

- HP Implemented on-site controls ***after ISO Auditor insisted***
- On-site project professionals to comply with HP IS Security Policy & Customer standards
- Awareness workshops
- Received +ve feedback
- Better CIA of data

Benefits received by HP India

1. Winning customer confidence
2. Market USP
3. Compliance with ISO / IEC 27001
4. Reduced cost of risk of single / multiple data security breaches
5. Improved employee awareness
6. Regular ISMS Audit secures IS Risk management process
7. Ensured compliance with HP'S Global Standard of Business Conduct (SBC)

GDPR & PDP Bill



Evolution of Data Protection Regulations

- EU enacted **General Data Protection Regulation** (GDPR) -- right to privacy as one of the fundamental rights.
- GDPR - effective May 25, 2018
- Requires **explicit consent from consumers** for usage of their data.
- July 27, 2018 : Justice BN Srikrishna committee submitted draft PDP Bill 2018 to Central Government.
- PDP Bill 2018 in India follows implementation of GDPR (with certain carve-outs)
- PDP Bill -- **112 sections** ,similar to EU's GDPR

PDP Bill - Draft

- **PDP** : Will form **framework for India's data protection laws**
- **PDP : Companies to adopt certain practices to :**

✓ collect,

✓ process and

✓ store consumers' data, and

✓ recommends a range of penalties including jail term for privacy violations.

- Once introduced in parliament, it will be subject to **further review**
- Essentially makes **explicit individual consent** central to data sharing.

PDP : Ecosystem

Data Fiduciary - Any person, including State, a company, any juristic entity or any individual **who determines purpose and means of processing** of Personal Data

Data Processor - Any person, including the State, a company, any juristic entity or any individual **who processes Personal Data on behalf of a Data Fiduciary but does not include an employee** of Data Fiduciary.

Data principal - A natural person to whom the Personal Data relates.

Personal data - Data about or relating to a natural person in relation to any **characteristic, trait, attribute** or any other feature of the identity of such natural person, or **any combination** of such features.

Sensitive Personal data & Info (SPDI)

- ✓ Passwords,
- ✓ Financial data, Bank accounts, credit card or debit card or other payment instrument details
- ✓ Biometric data
- ✓ Health data, medical records and history
- ✓ Genetic data
- ✓ sexual orientation, transgender status,
- ✓ Caste or tribe,
- ✓ Religious political belief or affiliation, or
- ✓ Any other category as may be specified by **Data Protection Authority of India.**
- [Section 3(35) of the bill]

Highlights of Personal Data Protection Bill, 2018

- 1. **Change in terminology**: "Data Subject" and "Data Controller", reformulated as "Data Principal" and Data Fiduciary", to emphasize greater accountability and trust between the two. [Section 3(13), Section (14)]
- 2. **Horizontal Application**: The proposed bill applies to **both government and private entities**. [Section 2(1)(b)]
- 3. **Extra-territorial Application**:
- The applicability of the law **will extend to data fiduciaries or data processors <u>not present within the territory</u> of India,** if they carry out processing of personal data in connection with
- (a) any business carried **on in India,**
- (b) systematic offering of goods & services to **data principles in India**,
- (c) any activity which involves **profiling of data principals** within the **territory of India**. [Section 2 of the Bill]

- 4. **Grounds for Processing Personal & SPD** : The legal ground for processing under the bill include:
- (a) consent,
- (b) functions of state,
- (c) compliance with law or order of court/tribunal,
- (d) for prompt action in case of emergencies,
- (e) purposes related to employment and
- (f) reasonable purposes of the data fiduciary.

- 5. **Personal and Sensitive Personal Data of Children**: Processing of personal & SPD of children by data fiduciaries should be done in a manner that **protects and advances the rights and best interests** of the child.
- Data fiduciaries are required **to establish mechanisms for age verification and parental consent**.
- 6. **Data Principal Rights**: The bill provides the data principal with
- a) right to confirmation and access,
- (b) correction,
- (c) **data portability -** fundamental right of **data** principal to move their information from one controller to another controller (in structured & machine –readable format)
- (d) right to be forgotten.
- [Section 24, Section 25, Section 26, Section 27 of the Bill]

- 7. **Transfer of Personal Data Outside India**: Section 40 places restrictions on cross-border data flows.
- Section 40 (1) : mandates storing **one serving copy of all personal data within the territory of India**.
- section 40 (2) **empowers central government to classify any sensitive personal data as critical personal data** and mandate its storage and processing exclusively within India
- 8. **Conditions for Transfer of Personal Data Outside India**: subject to standard contractual clauses or intra-group schemes that have been approved by DP Authority

- 9. **Data Protection Authority of India**: independent authority empowered to oversee the enforcement & adjudication [Chapter X. Section 60]
- 10. **Penalties, Remedies and Offences**: penalties under chapter XI, ranging from **INR 5 crore or 2 % of total worldwide turnover to INR 15 crore or 4% of the total worldwide turnover, whichever is higher**.
- Data principal under section 75 **has remedy to claim compensation for harm suffered as a result of any violation of any provision in the bill from the data fiduciary or the data processors**.
- Non-bailable , cognisable : certain offences under chapter XIII which are **punishable with imprisonment**
- 11. **Transition Provisions**: Section 97 - The enforcement duration is 18 months from the date of enactment

PDP Bill vs GDPR of EU

- PDP : any company that fails to comply with PDP will be fined Rs 5 crore or 2% of its turnover, whichever is higher.
- The severity of this punishment mirrors that of GDPR, which fines companies €20 million or 4% of turnover.
- The “right to be forgotten” suggested in the bill **only allows individuals to restrict companies from using their data.**
- It **does not allow Indians** to ask companies **to completely delete data they have shared**, an accepted practice in the EU.

Differences

- Please note that:
- 1. the **citizens whose personal data** is being processed are called **'data subjects' in GDPR** terminology **and 'data principals' by Indian draft bill.**
- 2. Similarly, **entities that process the personal data** are called '**data controllers' by GDPR** while being referred to as **'data fiduciaries' by the Indian draft bill.**

IS Auditor role : review Key Compliances for Corporate Sector

- Personal Data Protection Policy
- Impact assessment
- Record keeping & data audits
- Data Protection officer
- Security Safeguards
- Breach notification
- Transparency
- Grievance redressal

IT Act 2000

- Enacted on 17th May 2000-
- India is **12th nation** in the world to adopt cyber laws
- Introduced by - Pramod Mahajan, Minister of Communications and Information Technology
- Amended by - IT (Amendment) Act 2008

IT Amendment Act (ITA2008)

- An Act to provide **legal recognition for transactions** carried by means EDI
- Act is administered by **Indian Computer Emergency Response Team** (CERT-In).
- Amended by IT Amendment Bill passed in Lok Sabha on Dec 22nd and in Rajya Sabha on Dec 23rd of 2008.

- Facilitate **e- filing of documents**
- Facilitate **electronic storage of data**
- Give **legal sanction & facilitate electronic transfer of funds** between banks & FI

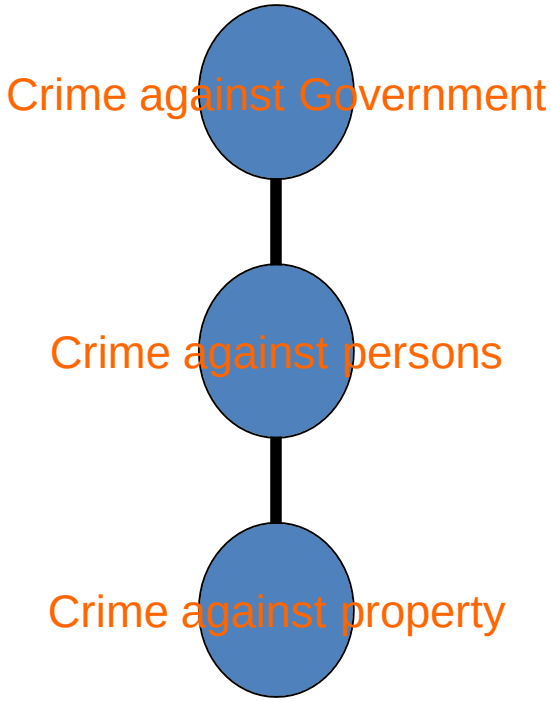
Civil offences under IT Act

- Chapter IX of IT Act, Section 43
- Whoever without permission of owner of computer
  - Secures access
  - Downloads, copies, extracts any data
  - Introduces or causes to be introduced any viruses or contaminant
  - Damages or causes to be damaged any computer resource
    - Destroy, alter, delete, add, modify or rearrange
    - change the format of a file
    - Disrupts or causes disruption of any computer resource
    - Preventing normal continuance of computer

- Denies or causes denial of access by any means
- Denial of service attacks
- Assists any person to do any thing above
- Rogue Websites, Search Engines, Insiders providing vulnerabilities
- Charges the services availed by a person to the account of another person by tampering or manipulating any computer resource
- Credit card frauds, Internet time thefts
- Liable to pay damages not exceeding Rs. One crore to the affected party
- Investigation by ADJUDICATING OFFICER

TYPES OF CYBER CRIMES

- Cyber terrorism
- Cyber pornography
- Defamation
- Cyber stalking (section 509 IPC)
- Sale of illegal articles-narcotics, weapons, wildlife
- Online gambling
- Intellectual Property crimes- software piracy, copyright infringement, trademarks violations, theft of computer source code
- Email spoofing
- Forgery
- Phising
- Credit card frauds



Offences

- Section 65 - Tampering with computer source documents
- Section 66 - Hacking with computer system
- Section 67C - Failure to maintain records
- Section 68 - Failure/refusal to comply with orders
- Section 69 - Failure/refusal to decrypt data
- Section 70 - Securing access to a protected system
- Section 71 - Misrepresentation

Sec 69: Decryption of information

- **Ingredients**
- Controller issues order to Government agency **to intercept any information transmitted through any computer resource.**
- Order is issued in the interest of the:
- sovereignty or integrity of India,
- the security of the State,
    - friendly relations with foreign States,
    - public order or
    - preventing incitement for commission of a cognizable offence
    - Person in charge of the computer resource **fails to extend all facilities and technical assistance to decrypt information**- punishment up to 7 years.

Forgery

Andhra Pradesh Tax Case

In the explanation of **Rs. 22 Crore recovered** from house of owner of a plastic firm by vigilance department,

accused person submitted 6000 vouchers to legitimize the amount recovered,

but after **careful scrutiny of vouchers and contents of his computers** it revealed that

all of them were made **after the raids were conducted** .

All vouchers were **fake computerized vouchers.**

Comparison of IT Act 2000 with 2008

1. Corporate Responsibility Introduced in S. 43A.
2. Important Definitions Added : Section 2(ha)- “Communication device “ and Section 2 (w) – “intermediary”
3. Legal Validity of Electronic Documents Re-emphasized
4. The Role of Adjudicating Officers under Amended Act

Essence

- Information Technology Act 2008 = **suitable case for analytical study of cyber crime issues.**
- **Comprehensive, clear framework.**
- Legal recognition to the Virtual electronic medium.

Recent whatsapp forwards

- The new communication rules for WhatsApp and WhatsApp Calls (Voice and Video Calls) will be implemented from tomorrow: -
- 01. All calls will be recorded.
- 02. All call recordings will be saved. 03. WhatsApp, FaceBook, Twitter, Instagram and all social media will be monitored.
- 04. Your devices will connect to the Ministry system. 05. Take care not to send the wrong message to anyone.
- 06. Tell your children, siblings, relatives, friends, acquaintances that you should take care of them and rarely run social sites.
- 07. Do not send any bad post or video against the government or the Prime Minister regarding politics or the current situation.
- 08. It is currently a crime to write or send a bad message on any political or religious issue, doing so can lead to arrest without a warrant.
- 09. The police will issue a notification, then be prosecuted by Cyber Crime, which is very serious. 10. All you group members, moderators please consider this issue.
- 11. Be careful not to send the wrong message and let everyone know and take care of the subject. Be more aware of all in the group ...
- ***"Two blue ticks, and one red tick means the government can take action against, while three red ticks will mean that the government has started court proceedings against you"***

Overview – IT Rules 2021

- The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 notified on February 25, 2021. under IT Act, 2000- - 3 months to comply : social media
- 2021 Rules replace IT (Intermediaries Guidelines) Rules, 2011.
- All significant social media platforms with more than 50 lakh (5 million) users, which means Facebook, Twitter, Instagram , - very much categorized as large social media platforms.
- March 2021 = WhatsApp - more than 390 million users in India.
- Facebook has 320 million users in India, - January 2021
- Twitter = more than 17.5 million users in India, January 2021
- The IT Rules = digital media regulation

1. robust complaint mechanism for users of social media & OTT platforms to address their grievances.
2. emphasis on protection of women & children from sexual offences on social media.
3. online content publishers & social media intermediaries should follow Constitution of the country & subject themselves to domestic laws.

Due diligence by intermediaries

- Intermediaries : entities that store or transmit data on behalf of other persons.
- Intermediaries : internet or telecom service providers, online marketplaces, & social media platforms.
- DD includes:
- (i) informing users about rules and regulations, privacy policy, and terms and conditions for usage of its services,
- (ii) blocking access to unlawful information within 36 hours upon an order from the Court, or the government,
- (iii) retaining information collected for the registration of a user for 180 days after cancellation or withdrawal of registration.
- (iv) Intermediaries required to report cybersecurity incidents and share related information with Indian Computer Emergency Response Team

Significant social media intermediaries:

- Social media intermediary with **registered users in India above a threshold** – say, 5 Million (to be notified) classified as **Significant Social Media Intermediaries**.
- Additional due diligence to be observed by them:
- (i) appointing a **chief compliance officer** to ensure compliance with IT Act & Rules,
- (ii) appointing a **grievance officer residing in India**, and
- (iii) publishing a **monthly compliance report.**

Non-compliance & consequence

- **Invoking of section 79 of the IT Act**
- Clearly mentioned in new IT Rules 2021.
- "When an intermediary fails to observe these rules, the provisions of sub-section (1) of section 79 of Act shall not be applicable for such intermediary and the intermediary shall be liable for punishment under any law including the provisions of the Act & Indian Penal Code".
- Section 79 specifically gives digital media platforms such as Facebook, Twitter, YouTube & WhatsApp legal immunity in a way against liability for posts made on their networks, third party information or data.
- That legal immunity will be withdrawn if non-compliance becomes an issue.

OTT Platform, News Publishers & Digital Media = Code of Ethics for Digital Media Publishers:

- **Over-the-top (OTT) Platforms- (like Netflix and Amazon Prime Video)**
- The new rules call OTT platforms **'publishers of online curated content'.**
- They would have to **self-classify the content** into **5 categories** based on age.
  - U (Universal)
  - U/A 7+
  - U/A 13+
  - U/A 16+
  - A (Adult)
- OTT platforms **required to provide parental lock systems** for content classified U/A 13+ or higher, & **have age verification mechanism f**or content classified as 'Adult'.
- The **rating for content & content's description with viewer discretion message should be prominently displayed before programme starts** so that users can make informed decisions based on suitability.
- **News Publishers**
- **Publishers of news on digital media** should observe **Norms of Journalistic Conduct of the Press Council of India** & **Programme Code under the Cable Television Networks Regulation Act 1995** to provide a level playing field between the offline (Print, TV) and digital media.

GST Network's IT and security Controls

- *India's GST Network (GSTN) : well crafted IT and security mechanism based on an advance security architecture*
- *built around threats and risk mitigating principles*
- *covering both physical & software security*
- ***Comments of CISO, GSTN***
- *'' The GST Network's IT infrastructure and security structure is well -designed and implemented in such a way that it is highly resilient and advance enough to mitigate evolving threats and risks"*
- *"Information security is one of the major focused areas and it is embedded in GST System,"*
- \- Anand Pande, Senior Vice President – CISO, GSTN.

GSTN – Platform Approach

- **Platform approach**, enabled to integrate
- banks,
- RBI,
- GST Suvidha Providers
- other functional & technical stakeholders.

- **Agile methodology** of software development used (DevOps)
- RBAC = role-based data access system
- Sensitive data sets within GST data system are **encrypted at rest as well as in flight.**

GSTN – Threat Mitigation

- GSTN followed & embedded major threats mitigating principles for internal and external threats.
- **Risks considered :**

1. data tampering attempts for commercial benefit by individuals or groups,
2. industrial espionage,
3. insider and external attacks to steal or tamper data,
4. cyber attacks on GST system and
5. unauthorized data and system access.

Limited Exposure to Internet

- Core GST system **not directly exposed** to internet.
- It has **multi-layered security architecture** built with advanced technologies
- The system access is **role based through secured channels**
- Any data transfer from GST System to State or other systems **is in encrypted format**

Data Center

- Data center stores & shares applications and data.
- It comprises : **switches, storage systems, servers, routers, & security devices.**
- Data center infrastructure housed in **secure facilities organized by halls, rows and racks**, supported by **power & cooling systems, backup generators & cabling plants**.
- GSTN : innovative concept of DC/NDC and DR/NDR **across 2 distinct geographies** ensures continuity in business should a disaster strike.
- Introduction of **Near DC (NDC) & Near DR (NDR)** ensures zero data loss, should the disaster strike is sudden & does not offer any recovery from main data centre.

GSTN : Tier 3 type DC

- A **Tier 3 data centre** : multiple paths for power & cooling
- systems in place to update & maintain without taking it offline.
- **Expected uptime** of 99.982% (1.6 hours of downtime annually) = Maintenance, emergency
- Can perform repairs **without any notable service disruption**
- Tier 4 data centers : “fault tolerant.”
- Unplanned maintenance **does not stop data** flow to DC Tier IV

Advanced threat protection (ATP)

- Advanced threat protection (ATP)
- security solutions that defend against sophisticated malware or hacking-based attacks targeting sensitive data.
- Capabilities of ATP :

1. Halting attacks in progress or mitigating threats before they breach systems
2. Disrupting activity in progress or countering actions that have already occurred as a result of a breach
3. Interrupting the lifecycle of attack to ensure that threat is unable to progress or proceed

CISO Comments on cyber attack @ GSTN

- *“GSTN network is under continuous cyberattack but we have our own security operations command and control centre.*
- *We have optimised our monitoring framework in such a way that none of the attacks was able to surpass even the first layer of security so far.*
- *You cannot stop the security attacks but you can mix the security control at your end in such a way that it should not pass the security gates,“*
- *---- - Anand Pande, Senior Vice President – CISO, GSTN.*

Thank You

Arijit Chakraborty