

# Data Security in E-Governance Projects in India

***Vinayak Godse***  
***Director- Data Protection***

**RISE Conference**

**Brussels– 9<sup>th</sup> Dec 2010**

# E-Governance : enhancing value through technology transformation

## E-Governance Objectives

- Exchange of information with citizens, businesses or other government departments
- Speedier and more efficient delivery of public services
- Improving internal efficiency
- Reducing costs or increasing revenue
- Re-structuring of administrative processes
- Ensuring participation of the people
- Transparency, limit leakage, targeted social benefits, etc.

## Stages of Adoption

**Stage I – WEB PRESENCE-** Marked by web presence of public institutions and dissemination of information.

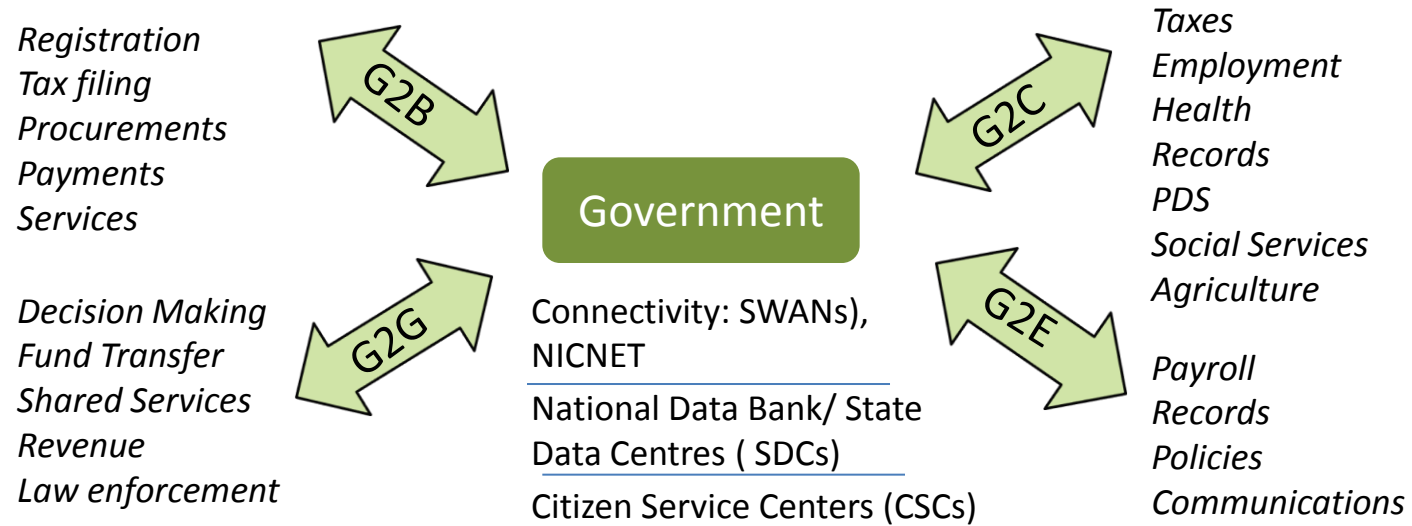
**Stage II – INTERACTIVE PRESENCE-** Marked by an interactive interface with stakeholders with proactive solutions to problem solving and electronic requests for services & financial transactions.

**Stage III – TRANSACTIONAL PRESENCE-** Completion of transactions on the internet and access to internet.

**Stage IV – NETWORKED PRESENCE AND E-PARTICIPATION-** Marked by a Government to Citizen (G2C) framework based on an integrated network of public agencies, process certification & participation in basic process design and political processes.

Ref: E-Governance and best practices, NISG

# E-Governance: structure, stories & enablers



**Reaching to critical mass:** Common Services Centers (CSC) 100,000 in 600,000 villages, planned to have 250,000 by 2012

**Breadth and coverage of services:** 1,100 citizen and business-centric services by 2014, 600 of which are operational

**Integration of one of the largest retail system:** Public Distribution System (PDS) with a network of 4.78 Lakh Fair Price Shops (FPS)

**Bhumi, Choupal, MCA 21, ePassport, RACE, eSeva, eMitra, FRIENDS, Gynadoot:** Many success stories with millions of people connected

**National eGovernance Plan:** investment > \$ 10 billion, mission mode projects, many more to add

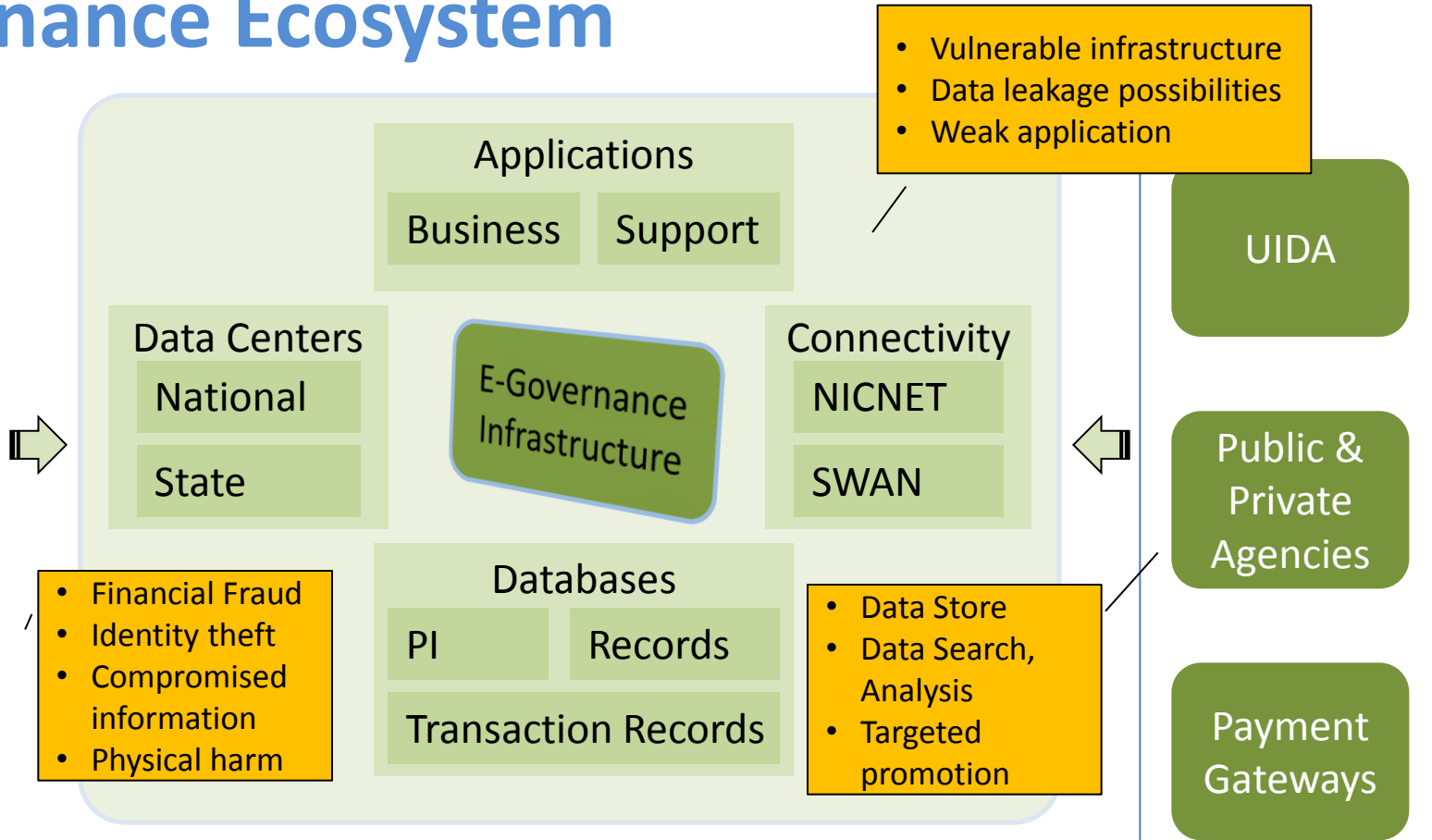
By 2015, 600 million will have **UID**  
 By 2015, 275 million **broadband Users**  
 By 2012, **domestic IT market** to reach \$ 112 Billion



# E-Governance: Goals for 2015 ?

- **Wireless Broadband and Mobile Access** in all towns and villages
- Common Service Centres (**CSCs**) in all villages
- All major **public services available online**
- All **major public services** available through call centres
- Individual **ID scheme fully operational**
- Integrate **Financial Services and Mobile** telephony
- Integrate **ID services with mobile** telephony
- Create complete range of high quality **educational programmes** for school and college level available online and integrated into the regular curriculum
- Major **agriculture sector services** including consultancy, credit and insurance available online
- High quality **medical services available in villages** through telemedicine
- Provision of **Insurance services** (crop, health, life, etc.)
- Create an **open technology generic integrated platform** for e-governance **that can be used by governments worldwide** backed by strong support services by Indian IT industry and manpower
- Position **India as a hub** for a number of ICT-related technologies **relevant for developing/ multi-lingual countries**
- Draw up and implement a national programme to position **India as a global centre for IT security services** which also support a secure cyber space in the country
- Adopt an **E-Governance Law**

# E-Governance Ecosystem



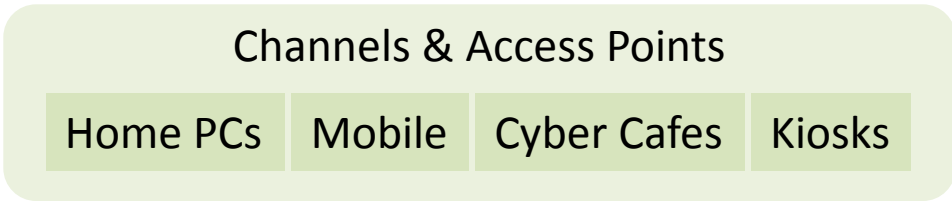
- Vulnerable infrastructure
- Data leakage possibilities
- Weak application

- Financial Fraud
- Identity theft
- Compromised information
- Physical harm

- Data Store
- Data Search, Analysis
- Targeted promotion

- Non transparent Information practices
- Data mining
- Limitless collection & usage
- Sharing to unintended purpose (Security)
- Unauthorized access

- Insecure transmission
- Vulnerable comm
- Compromised endpoint



- Insecure endpoints
- Illiterate citizens
- Less awareness

# Data Security and Privacy issues

## **Construct a detailed profile of individual ?**

using only publicly available, individually identifiable information from government records.

**Use of sensitive information for commercial gain or cause harm?** medical records, personal shopping habits and financial data

**Secondary use the government bodies or authorities ?** Using information for political gain, communal advantages, etc

**Central storage of information invites risk of compromise and abuse?** Gives higher pay off

**Scale and complexity of data transactions creates more possibilities of data leakage?**  
Multiple entities dealing with data

**Public databases provide significant target to cross border cyber threats ?** Rising instances of cyber threats

Society which recognized with diverse culture and perceptions

Society where illiteracy is one of the significant challenge

Society where communal politics still prevails

Society where practice of renting creates huge problem in public services delivery

Country which is situated in one of the most challenging geopolitical area leading to strong focus on national security against privacy

# Agenda for Data security and Privacy

**Trust Relationship in Technology Transformation**

**Policy responding to cultural Change**

**Assuring Personal Rights in the Age of E-Governance & E-Commerce**

**Securing interest of Weaker Section of the Society**

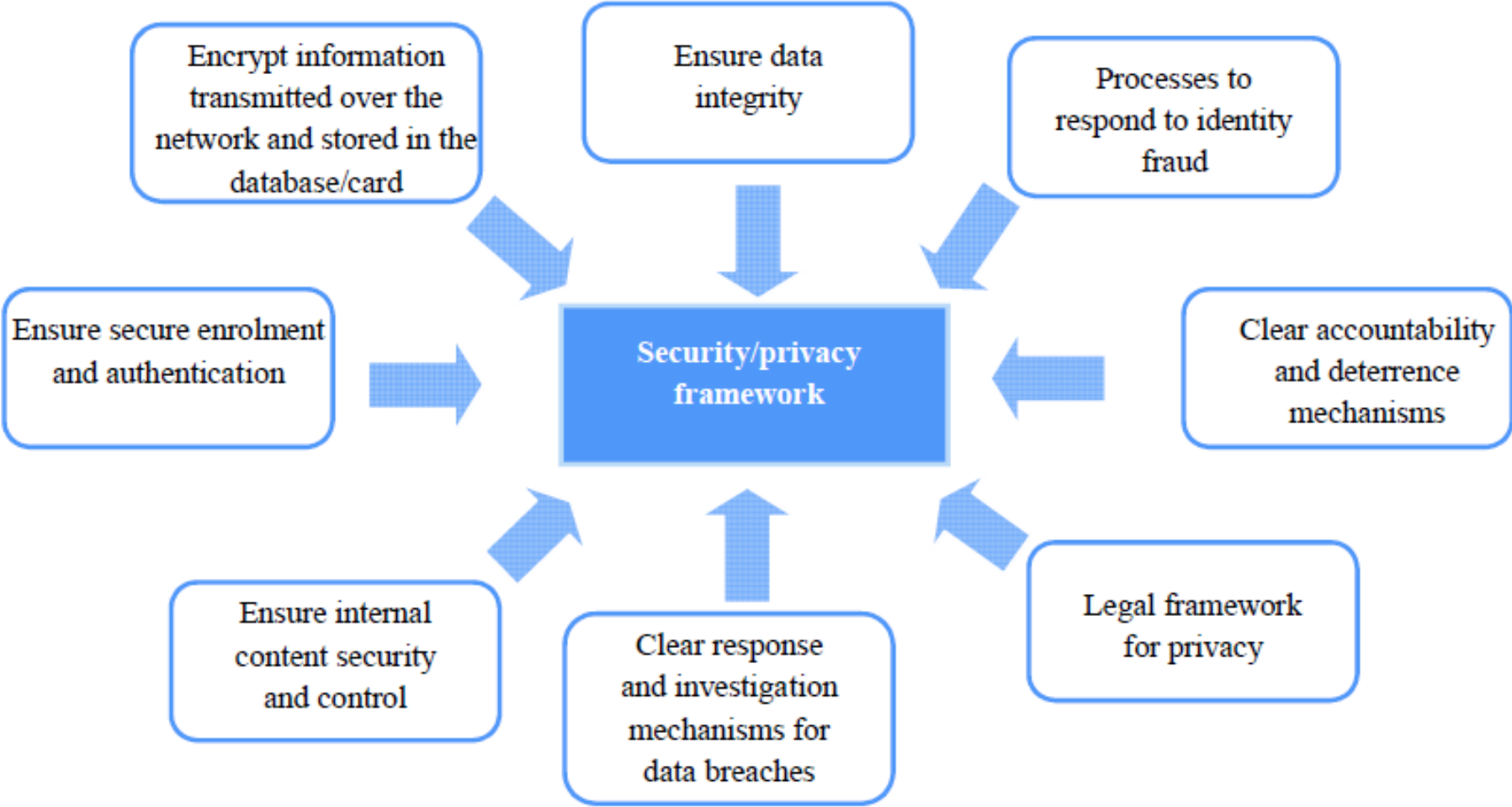
**Privacy in New Age Transactions and Service Deliveries**

**Securing the Transformation Economy into E-economy**

**Balancing Privacy with National Security concerns**

**Ensuring the growth Industry**

# UIDA Security and Privacy Framework



# eSAFE: e-Governance Security Assurance Framework

*Initiative of Standardization Testing and Quality Certification Directorate (STQC), DIT, MICT, Government of India*

## Approach

- ISO 27001: the international standard for an Information Security Management System (ISMS)
- In line with Information Security Program for Federal Information Systems in USA -

Document No.	Document Title
ISF 01	Information Security Assessment Framework
GD 100	Guidelines for Security Categorization of eGovernance Information Systems
GD 200	Catalog of Security Controls
GD 201	Baseline Security Controls for LOW IMPACT INFORMATION SYSTEMS
GD 202	Baseline Security Controls for MEDIUM IMPACT INFORMATION SYSTEMS
GD 203	Baseline Security Controls for HIGH IMPACT INFORMATION SYSTEMS
GD 210	Guidelines for Implementation Security Controls
GD 220	Guidelines for Assessment of Effectiveness of Security Controls
GD 300	Guidelines for Information Security Risk Assessment and Management

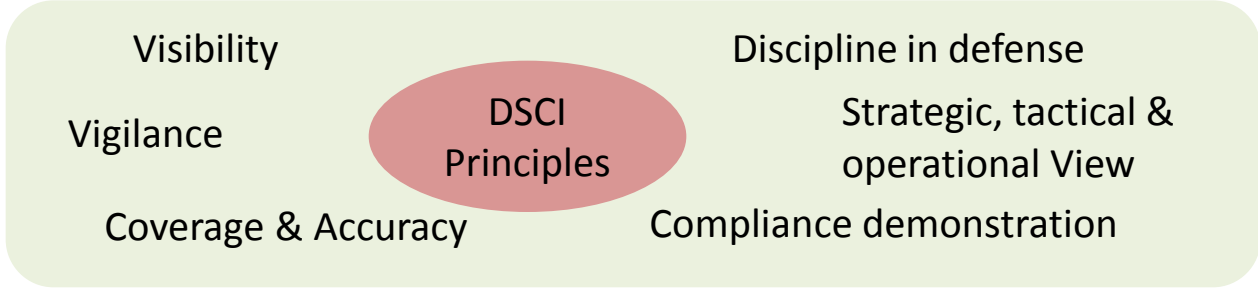
Categorization of e-Governance information systems according to risk levels: High, Medium, Low

**.... Privacy is not on agenda**



# DSCI Security Framework (DSF)

## Articulates DSCI Principles



## Each of the 16 Disciplines of DSF

### Strategy *| For Security Leaders, Consultants, Reviewer*

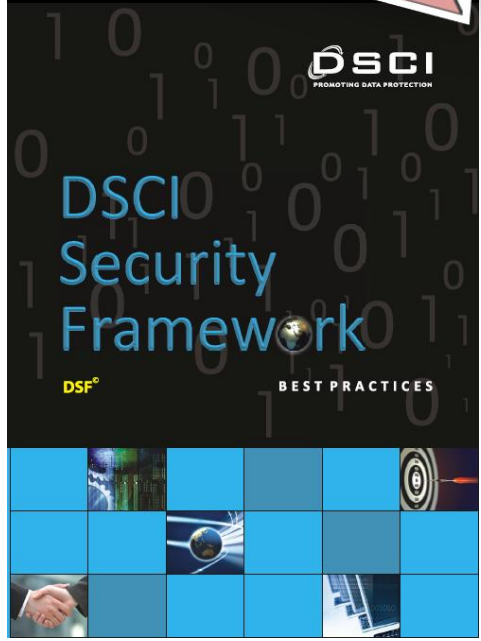
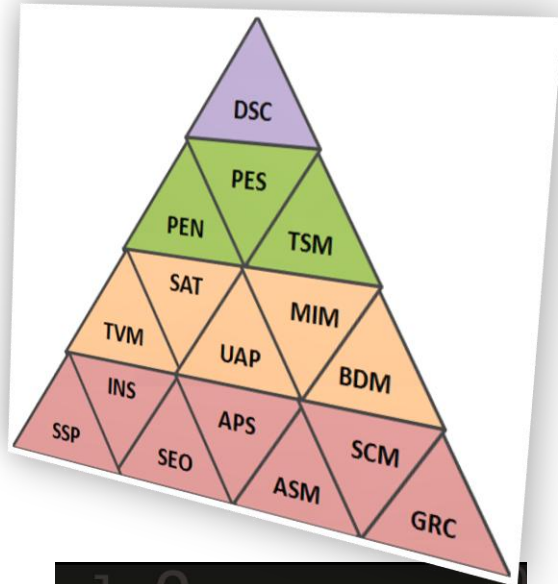
- Means to evaluate an organization's strategy in the discipline
- Guidance to evolve strategy for the discipline

### Practices *| For Implementer*

- Compilation of practices that provide detailed guidelines achieving excellence in the discipline

### Maturity Metrics *| For Security Leaders, Executive Management*

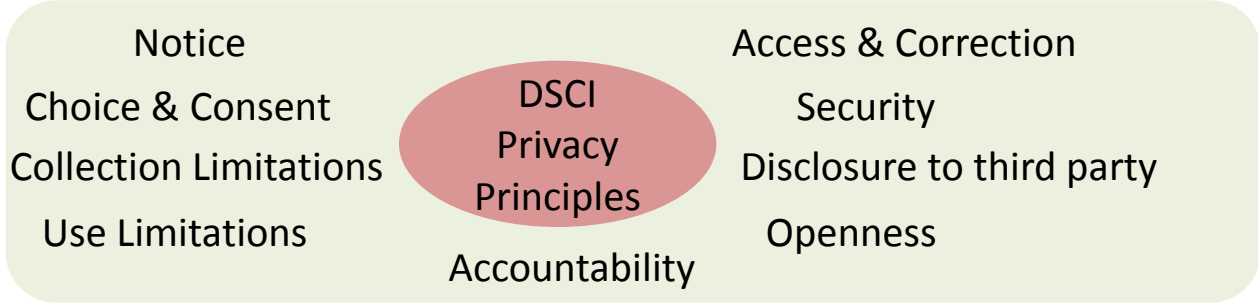
- A comprehensive set of Metrics for the discipline



A **NASSCOM**® Initiative

# DSCI Privacy Framework (DPF)

## DSCI Privacy Principles



## Privacy in Digital Age

- Discussion on privacy

## Data Protection: Organization Roles

- Applicability of the privacy principles for roles 'Controller', 'Processor'

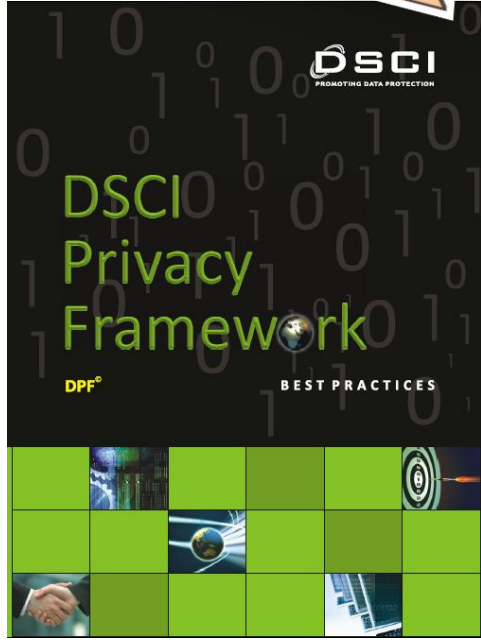
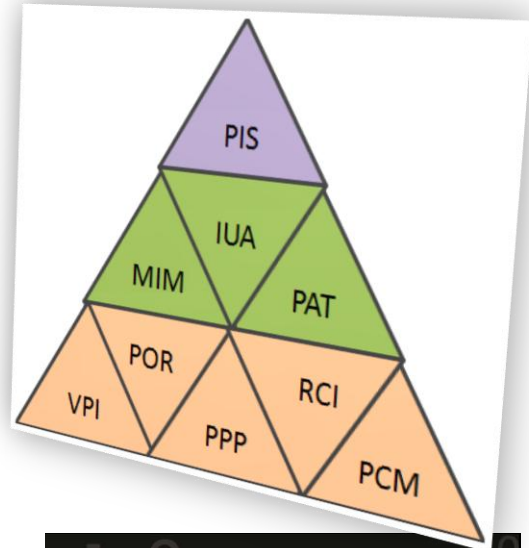
## DSCI Approach & Framework

- Approach & Evolution of DPF with 9 practice areas

## Practices

***| For Privacy Leaders, Consultants, Implementer***

- Compilation of practices that provide detailed guidelines for privacy implementation



A **NASSCOM**® Initiative

# Recommendations: RISE Policy Paper- Privacy in India

- **Revisit design, architecture, and deployment** of projects from data security and privacy perspective. Conduct routine privacy impact assessment
- Inculcate **data centric approach** in the security and privacy initiatives
- Ensure that project implementation and operations **adhere to the guidelines and standards** for privacy
- Ensure that **privacy in** ensured **in entire lifecycle of data** i.e. data collection, use, processing, and storage
- Adopt **privacy enhancing technologies, privacy design principles:**
- Implement **adequate measures** for security and **vulnerability management** of systems that engage in processing of personal information
- Build an **organization culture** that respect privacy of the end user.
- Ensure that **privacy policies and practices** are defined and implemented
- Ensure that significant effort is dedicated on **end user education** that enable them **to take trust decisions** while they are transacting online
- Establish **vigilant monitoring for privacy**; deploy a mechanism to address end user's grievances

# Privacy Technology for E-Governance

**Privacy Specification Language** (P3P policy, EPAL),

**Privacy-Preserving Data Mining** - Secure Multi-party Computation (SMC techniques),

**Privacy Preserving Databases:** Strong authentication, Granular Access control, Virtual Private Database , Label-Based Access Control, Secure Application Role, Encryption in the database:

**Anonymized Data Analysis:** Data Suppression, Cell Value Generalization

**Statistical Disclosure Control (SDC)** to guarantee **statistical confidentiality**: Query Restriction, Data/Output Perturbation, Tabular data protection, Dynamic databases, Microdata protection

**Privacy Broker for Privacy Preserving Transactions:** Privacy Specification, Privacy Rules, Authorization to data, ensures non-reputation

*Reference: Privacy Technology for E-Governance, Jaijit Bhattacharya*

# Data Protection: Legal Regime

## Framework for Privacy, Data Protection and Security

### PRIVACY ACT



**Proposed law:** applicable to both private & government bodies

### IT (Amendment) ACT, 2008

- Section 66-70: Cyber Security
- Section 69: Legal Interception and Monitoring Computer Resource
- Section 70: Critical Infrastructure Protection
- Section 84A: Encryption

### Other Laws

- Indian Penal Code
- Contract Acts
- Copyright Act
- Banking and Insurance Laws
- Telecom laws
- Consumer Laws
- Corporate Laws
- Intellectual Property Laws
- All other acts for e-governance
- etc.

Privacy provision in the Privacy Act may supersede all other privacy clauses which may be present in any other laws of the country

THANK YOU