Compliance & Security Framework
(Chapter -2 : DISSA Course)

Arijit Chakraborty

Jan 16, 2022

Coverage & session plan

- NIST
- SSAE 16, AT 101
- FEDRAMP
- HIPPA, DISHA
- HITECH Act
- GDPR
- PDP Bill
- **Case studies**

NIST Cybersecurity Framework (CSF)

- NIST CSF = risk-based framework developed for critical infrastructure sectors , has been adapted by organisations across all industry sectors.
- NIST does not provide a certification process, rather a well-designed framework to assist in establishing its Cyber Security maturity posture over 5 business-critical functions:
  Identify, Protect, Detect, Respond and Recover

- Each of the core NIST CSF functions is graded on a scale of 0-4, their higher scores outlining higher levels and degrees of Cyber Security maturity.
- This ability to provide an overall rating for an organisation's cyber security posture makes it attractive.
- Senior Management can quickly understand and appreciate positive developments in a risk improvement programme.
- NIST CSF will identify current Cyber Security maturity levels and set out a clear plan to mitigate the risks by order of priority

SSAE-16

- **Statement on Standards for Attestation Engagements** No. 16 (SSAE-16) monitors & enforces controls around applications and application infrastructure that impact financial reporting.

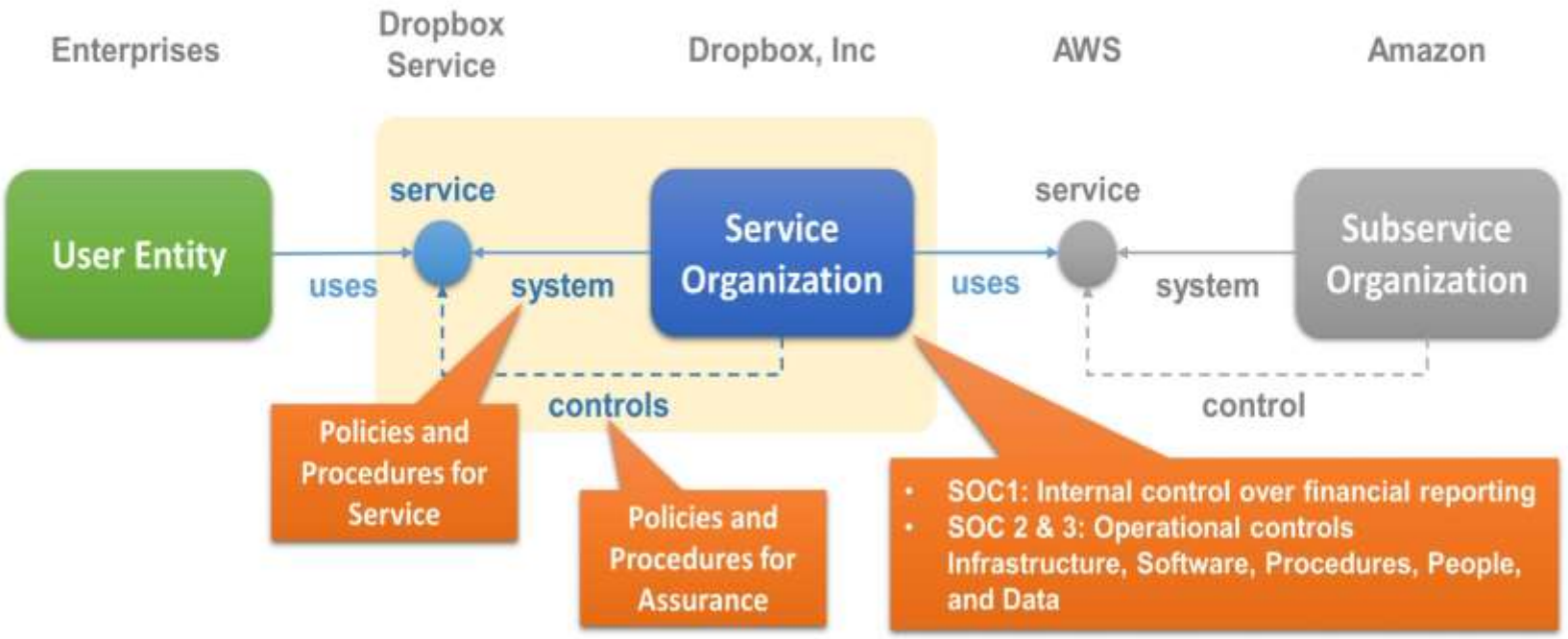
✓ covers business process controls & ITGC .

✓ Service Organization Controls (SOC) 1 reports, formerly known as SAS 70 reports, leverage the SSAE-16 framework.

✓ The SSAE-16 framework = best practices,

✓ mandatory part of SOX compliance process.

Service Organization Control (SOC)



SOC 1 & SOC 2

AT-101 Audit standard

- SOC 2 reports based on the AT-101 auditing standard. SOC 2 reports test the design or operating effectiveness of security, availability, processing integrity, confidentiality, and/or privacy controls.
- All SOC 2 reports need to cover security controls. Availability, processing integrity, confidentiality, and/or privacy controls
- **IS Auditor**
- To Review SOC 2 reports from other organizations can reveal how partnering with them could introduce risk into Organisation environment.
- **Organizations using AT 101 framework**
- Software as a Service (SaaS) providers,
- Cloud computing companies, and other technology-related services

FedRAMP

- FedRAMP = standardized way for government agencies to evaluate the risks of cloudbased solutions.
- ❑ It follows a “do it once, use it many times” approach, allowing existing security assessments and packages to be reused across multiple agencies.
- ❑ can improve real-time security visibility for organizations.
- In government agency, IS Auditor will use FedRAMP packages to decide whether it makes sense to leverage specific cloud-based solutions.

- Cloud solution providers interested in selling to federal government agencies will go through the FedRAMP certification process.

HIPAA / HITECH

- A. Health Insurance Portability and Accountability Act (HIPAA) signed into law in August 1996, updated by HIPAA Privacy Rule in 2003 & HIPAA Security Rule in 2005, amended - 2009
- HIPAA encompasses:

✓ Technical Safeguards
✓ Physical Safeguards
✓ Administrative Safeguards
✓ Privacy Rule
✓ Breach Notification Rule
✓ Enforcement Rule
✓ Data Encryption

- B. Health Information Technology for Economic and Clinical Health (HITECH) Act
- **HITECH** enforces **security to protect Personal Health Information (PHI).**
- **Applicability :** who is **collecting, storing or processing personal health information (PHI), including hospitals, medical providers, and insurance companies.**
- HITECH Act is to improve the quality, safety, and efficiency of healthcare by expanding the adoption of health information technology.

HIPAA – India’s response

- **DISHA** – India's Probable Response To The Law On Protection Of Digital Health Data
- proposed **Digital Information Security in Healthcare Act** ("**DISHA**"), which seeks to:
- provide for electronic health data privacy;
- confidentiality, security and standardization; and
- establishment of National Digital Health Authority and Health Information Exchanges.
- DISHA = Indian counterpart to HIPAA

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

EU GDPR

- The European General Data Protection Regulation (GDPR) has almost become a common noun for personal data protection regulation,
- for the stringent provisions that it contains but also for comprehensiveness of the issues that it addresses.
- The Indian panel created to draft a data protection legislation, under Justice BN Srikrishna has referred to GDPR repeatedly in a whitepaper, along with the draft Personal Data Protection Bill 2018.

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.

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.

Comparison

- In case of a breach, there's no requirement by Indian draft bill to share it with the data principal;
- rather, the data protection Authority shall determine whether such breach should be reported to the data principal.
- This is also in contrast to GDPR provisions.
- Concept of GDPR = premise that the ownership of data must belong to the data subject, Indian bill does not provide that
- Overall, Indian bill is a diluted version of GDPR, with lesser power for the citizens

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

PwC SDC Kolkata Data Protection and Privacy Policy

Contents

DEFINITIONS

- **Agent**: Any individual or entity which has a contractual relationship with IOCL, where IOCL is the principal and the other individual or entity is the agent, shall hereinafter be referred to as an "Agent". For instance, IOCL's distributors, dealers, CFA, contractors, etc. shall be considered Agents.
- **Data Subject:** All individuals whose personal information is either collected, received, processed, stored, dealt or handled by IOCL shall be referred to as "Data Subject".
- **Information:** Personal Information of a Data Subject collected by IOCL under this Policy shall hereinafter be referred to as "Information".
- Such Information includes, interalia, Sensitive Personal Data or Information as defined under the Indian Information Technology Act, 2000 and the **Aadhaar number** and/or the **biometric information** associated with an Aadhaar number.
- **GOVERNING LAW**
- IOCL is an organisation based and existing in India and is thus bound by the laws of the Republic of India. This Privacy Policy has been prepared in accordance with applicable Indian laws, including the Indian Information Technology Act, 2000
- **APPLICABILITY**
- This Policy applies to all individuals whose Information is either collected, received, processed, stored, dealt or handled by **IOCL.**

- **OBJECTIVE**
- This Privacy Policy is intended to inform the **Data Subject** on how **IOCL** collects, processes, stores, and uses personal information that a **Data Subject** provides to **IOCL** either directly or indirectly**.** This Privacy Policy also covers **IOCL's** treatment of any personal information that Third Parties share with **IOCL**.

- **HOW IOCL COLLECTS DATA SUBJECT'S INFORMATION**
- **IOCL** collects **Data Subject's** Information during their visit to the IOCL Websites. This also includes instances where a third-party may provide such Information on the IOCL Websites on behalf of the Data Subject.
- Data where the identity has been removed [anonymous data] such as cookies, web beacons and other browsing information do not come under the ambit of **Data Subject's Information**.
- Such browsing information is collected through cookies and web beacons to track what features or web-pages the **Data Subject** has viewed on the IOCL Websites, and other information about **Data Subject's** browser and browsing behavior. IOCL uses browsing information to improve the design and content of the IOCL Websites, to suggest content and products that **IOCL** thinks may be relevant to the **Data Subject**, and other related purposes. Most browsers accept cookies automatically

- **WHY IOCL COLLECTS DATA SUBJECT'S INFORMATION [PURPOSE]**
- **IOCL** uses the **Information** to conduct its business and to provide **Data Subject** with the best possible services/products. **IOCL** will only use the **Information** based on this Privacy Policy, its understanding with the **Data Subject**, or as required by law.
- **IOCL** will collect adequate, relevant and necessary **Information** and will process such Information fairly and lawfully for the purpose it is collected . Most commonly, **IOCL** will use the **Information** in the following circumstances:
- (a) Where **IOCL** needs to perform the obligations it has promised the **Data Subject,** such as to provide a service or product to the **Data Subject** and to enable the **Data Subject's** use of **IOCL's** products/services, including but not limited to dealing with enquiries and complaints made by or about the **Data Subject** relating to services/products provided by **IOCL** and to improve and customise **IOCL's** services/products in accordance with the **Data Subject's** preferences;
- (b) Where **IOCL** needs to comply with a legal, accounting, business or reporting obligation, including compliance with requests from the Government of India or any Governmental Agency;

- (c) To send marketing as well as non-marketing commercial communications to the **Data Subject**;
- (d) To send the **Data Subject** notifications that the **Data Subject** has specifically requested for as well as to send statements, invoices and payment reminders to the **Data Subject**, and to collect payments from the **Data Subject**;
- (e) To provide Third Parties with statistical information about its customers but those Third Parties will not be able to identify any individual from that information;
- (f) To keep **IOCL's** website, mobile applications and other systems secure and to prevent fraud;
- (g) To promote the mission and objectives of Skill Development in India and/or to provide and disseminate information about relevant programmes under the Skill Development Mission.
- (h) To manage the employment of the data subject with IOCL.

- **INFORMATION SHARING AND DISCLOSURE**
- **IOCL** may disclose the **Information** to any of its Agents or Third Parties insofar as reasonably necessary for the purposes set out in this Policy and for the purpose of providing services/products to the **Data Subject**.
- Such Agents and Third Parties are expected to provide a similar level of protection to the **Information** as is adhered to by **IOCL**.
- In addition to this, **IOCL** may disclose the **Information** where it is required to do so by law or to Governmental Agencies.
- **TRANSFER OF INFORMATION OUTSIDE INDIA**
- Unless stated otherwise, **IOCL** stores and processes the **Information** in India. There may, however, be occasions when **IOCL** needs to transfer the **Information** outside India for its business requirements. In such instances, **IOCL** will exercise the same level of care in handling the Information as it does in India.
- **DATA SECURITY**
- The **Information** is processed by **IOCL** in strict accordance with the Indian Information Technology Act, 2000, and the rules notified thereunder. **IOCL** implements and maintain 'Reasonable Security Practices and Procedures' as stated in the Indian Information Technology Act, 2000 and the Information Technology [Reasonable Security Practices and Procedures and Sensitive Personal Data or Information] Rules, 2011, while processing, collecting, storing or handling any **Information.**

- **DATA RETENTION**
- **IOCL** will only retain the **Information** for as long as necessary to fulfil the purposes **IOCL** collected it for, including for the purposes of satisfying any legal, business, accounting, or reporting requirements.
- In some circumstances, **IOCL** may anonymise the **Information** so that it can no longer be associated with the **Data Subject**, in which case **IOCL** may use such information without a further reference to **Data Subject**.
- **REVIEW OF INFORMATION**
- **CHANGES TO THIS PRIVACY POLICY**
- **GRIEVANCE OFFICER**

Privacy Policy : Maruti Suzuki India

- **Privacy Policy**
- Maruti Statement of Privacy At Maruti we take your privacy seriously. Please read the following to learn more about our terms and conditions.
- **What the terms and conditions cover**
- This covers Maruti's treatment of personally identifiable information that Maruti collects when you are on Maruti Suzuki site and when you use our services.
- This policy also covers Maruti's treatment of any Personally identifiable information that Maruti shares with you. This policy does not apply to the practices of companies that Maruti does not own or control or Maruti does not own or employ or manage.
- **Information Collection and Use**
- Maruti collects personally identifiable information when you register for a Maruti account. When you choose the services and promotions. Maruti may also receive personally identifiable information from our business partners.
- When you register with Maruti, we ask for your name, e-mail address, birth date, gender, occupation, industry and personal interest.
- Once you register with Maruti and sign in to our services, **you are not anonymous to us.** Maruti uses information for **three general purpose**: to fulfill your requests for certain products and services and to contact you about specials and new products.

- **Information Sharing and Disclosure**
- Maruti will not sell or rent your Personally Identifiable Information to anyone. Maruti will send Personally Identifiable Information about you when:
- 1. We have consent to share the information
- 2. We need to share your information to provide the product or service you have requested
- 3. We respond to court orders or legal process.
- 4. When we find your action on the web site violates the Maruti terms and condition or any of your usage guidelines for specific products or services.
- **Security**
- Your Maruti account information is password-protected for your privacy and security We have taken adequate measures to secure access to your personal data

- **Changes to this Policy**
- Maruti may edit this policy from time to time. If we make any substantial changes ,we will notify you by posting a prominent announcement on our pages.
- **Email Disclaimer**
- This electronic transmission contains information from Maruti Suzuki India Limited (MSIL) which is confidential and proprietary, and is intended for use only by the person named herein.
- In case, you are not the intended recipient, pls. don't use this information in any manner, whatsoever, and immediately return it to Sender.