Published by :
http://www.ijert.org

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 14 Issue 03, March-2025

How BDSLCCI can Help SMEs to Achieve Data Protection Compliance, Such as EU GDPR and the DPDP Act of India

Shekhar PAWAR
Doctor of Business Administrator (DBA), Swiss School of Business and Management School Geneva, Geneva Business Center, Avenue des Morgines 12, Genève, 1213, Switzerland

Abstract **- Data protection acts in many countries are playing an essential role in maintaining privacy, security, and trust in the digital age. Typically, data protection acts cover a wide range of personal data, which is not limited to personally identifiable information (PII), sensitive personal data, behavioral data, biometric data, and location data. It is not only the responsibility of an individual person but also of entities that are involved in such data's life cycle. These entities can be government, small, or even large organizations. The digitization of small and medium enterprises (SMEs) has increased cyber threats according to the latest global statistics. Despite the numerous cybersecurity standards available in the global market, SMEs face challenges in implementing cybersecurity measures and are mostly on the radar of cybercriminals. To address those along with the growing need to adhere to data protection acts, the Business Domain Specific Least Cybersecurity Controls Implementation (BDSLCCI) is providing a new framework, considering the Confidentiality, Integrity, and Availability (CIA) Triad and Defense in Depth (DiD) concepts. The author will share how BDSLCCI is mapped with the requirements of key data protection acts.**

Keywords: **SME; MSME; SMB; DPDP Act India; GDPR EU; cybersecurity; BDSLCCI; Data Protection Act**

1. INTRODUCTION

Data, including all computer-processable information, is a broad term that includes all types of information. Information is the contextualization by making data useful, and using them, for specific tasks [1]. Personally Identifiable Information (PII) refers to data that can be used to identify individuals and requires special handling due to privacy concerns. Examples of PII include names, addresses, phone numbers, emails, and other identifying information. Sensitive personal information like financial information, health records, political views, religious convictions, sexual orientation, and racial or ethnic origin may be included. Additionally, PII can include internet browsing history, purchase records, online activities, and biometric data like fingerprints, facial recognition details, and other biometric identifiers. Location data, such as GPS coordinates or any other location-tracking information, is also considered PII [2]. PII data is subject to stricter regulations and protection measures due to its potential impact on individual privacy. While general data can be used for analysis, reporting, and decision-making, PII data must be handled carefully to ensure privacy laws and protect identities [3]. Data leakage presents a major risk to enterprises, leading to reputational and financial harm. Common types of leaked data include employee and customer information, intellectual property, and medical records. The rapid expansion of the digital age and Industry 4.0 has increased the frequency of data breaches [4].

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 14 Issue 03, March-2025

Cybercriminals are placing high importance on PII data breaches, as it is helping them to do more sophisticated cybercrimes [5]. A ConsumerAffairs analysis of Maine Attorney General's data breach notifications shows over 100 million victims in 2024, with conservative estimates due to multiple filings and difficulty in tallying annual totals due to companies frequently revising the number of victims [6]. In January 2024, the Mother of All Breaches (MOAB) incident exposed 26 billion records, revealing 12 TB of data from platforms such as LinkedIn, Twitter, Weibo, and Tencent. This breach underscores the critical need for enterprises to prevent unauthorized information disclosure [7]. In the first four months of 2024, the Indian Cyber Crime Coordination Centre (I4C) received reports of over 740,000 cybercrime incidents. Online financial fraud made up approximately 85% of these cases, highlighting the significant challenges faced [8]. Research indicates that PII records were extensively compromised in countries such as France, Thailand, the United States, and Turkey. Due to the Aadhaar data breach, India experienced the highest loss of personal and health records [9].

Data protection safeguards PII and other sensitive data not limited to unauthorized access, confidentiality, integrity, and availability. On the other hand, cybersecurity protects an organization's digital infrastructure, which is via different defense-in-depth layers, including physical, networks, systems, applications, and data. BDSLCCI is one of the cybersecurity frameworks helping small and medium-sized companies; depending on the region, turnover, and other parameters, these companies are also known as micro, small, and medium enterprises (MSMEs), small and medium businesses (SMBs), or small and medium enterprises (SMEs). According to research studies, SMEs are facing three major challenges while deciding and implementing cybersecurity standards available in the market. Firstly, these organizations not having enough funds to invest, and secondly, SMEs not having knowledgeable employees to implement or maintain cybersecurity standard requirements. Thirdly, these organizations are not able to forecast return on investment (RoI) for investment of time and funds for the cybersecurity, as those are generic for any kind of business domain. The purpose of the BDSLCCI framework is to resolve all these challenges faced by SMEs. As shown in Figure 1, it covers defense in depth (DiD) controls and mission-critical assets (MCAs). The BDSLCCI framework is also designed to address the requirement fulfillment of data protection compliance [10, 11]. The BDSLCCI framework changes its version every year to address the latest cyber attack statistics. To make it easy to assist SMEs to adopt the needs of cybersecurity and data protection, BDSLCCI is available as a web platform having various policy and guideline documents and tools [12].

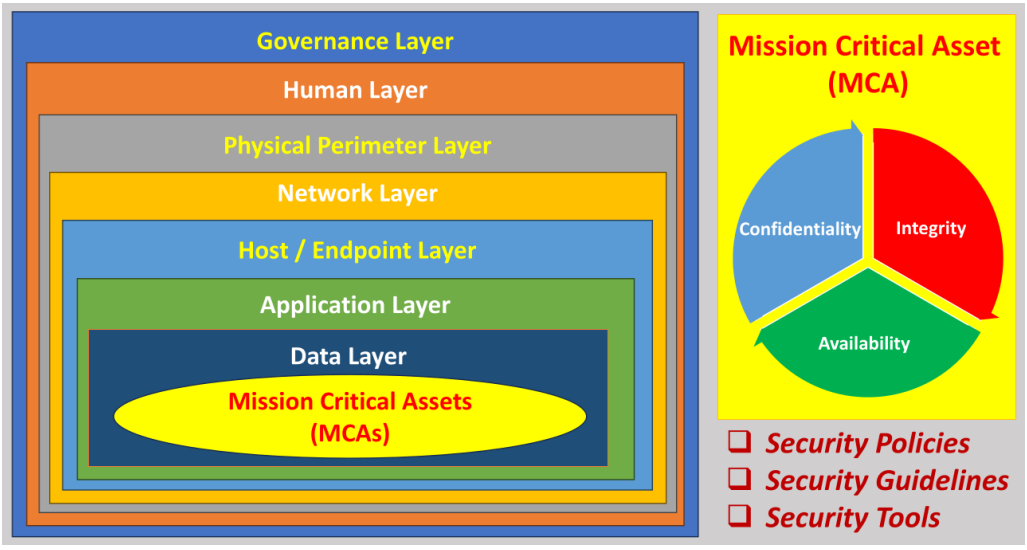

Figure 1: BDSLCCI Framework covering Defense in Depth (DiD) and MCA Cybersecurity Controls

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 14 Issue 03, March-2025

In the following sections, the authors will explain how they concluded that SMEs need to implement cybersecurity controls differently from the BDSLCCI framework to meet data protection requirements.

2. RELATED WORK

On May 25, 2018, the European Union (EU) enacted the General Data Protection Regulation (GDPR) to enhance privacy rights and influence how organizations manage data privacy. This significant overhaul of data protection laws affects any organization that processes the data of EU citizens, irrespective of its location. Table 1 outlines the key areas of the GDPR [13].

TABLE 1. OVERVIEW OF EU GDPR

Area	Description
Objective	Empowering individuals to manage their personal data more effectively while guaranteeing strong safeguards across various industries.
Technology Adaptation	The GDPR was established to keep pace with the latest technological advancements. It encompasses contemporary data management practices such as online behavior tracking, cookie usage, and other monitoring technologies to maintain the effectiveness of data protection measures as technology evolves.
Key Entities in GDPR	• Data Subjects: Primarily EU citizens or residents whose data is processed. Their GDPR rights now include access, correction, deletion, restriction, objection to processing, and data portability. • Data Controllers: Entities that determine the purposes and means of processing personal data. • Data Processors: Entities that process data on behalf of data controllers.
Key Data Processing Principles	Principles such as confidentiality, integrity, lawfulness, fairness, transparency, purpose limitation, accuracy, data minimization, and storage limitation must be adhered to when processing data under GDPR. • Lawfulness, Fairness, and Transparency: Data processing must be transparent to data subjects, fair, and lawful. • Purpose Limitation: Data should only be collected for specific, legitimate purposes and not used in ways that are incompatible with those purposes. • Data Minimization: Only the data that is strictly necessary should be collected. • Accuracy: Data must be kept accurate and up to date. • Storage Restrictions: Data should not be stored longer than necessary. • Integrity and Confidentiality: Data must be processed securely to prevent loss, damage, or unauthorized access. • Data Localization: Personal data of EU citizens must be stored within the European Economic Area (EEA) unless certain conditions are met. Data can only be transferred outside the EEA if the receiving country ensures an adequate level of data protection or if appropriate safeguards, such as binding corporate rules or standard contractual clauses, are in place.
Key Operational Requirements	• Breach Notification: Organizations are required to notify the relevant authorities and affected individuals within 72 hours of a data breach. • Expertise: Appointing a Data Protection Officer (DPO) is a key component of an organization's data protection expertise. • Accountability and Governance: Organizations must implement governance procedures and demonstrate compliance to ensure data protection.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 14 Issue 03, March-2025

Special Categories of Data	• The GDPR identifies and imposes strict limitations on the processing of certain categories of sensitive data, including racial or ethnic origin, political opinions, religious beliefs, and genetic information. • The GDPR sets the legal age of consent for data processing at 16. However, EU member states can lower this age to as young as 13. Data processing for children below the age of consent is only allowed if a parent or guardian has given or authorized consent. When obtaining consent from children, organizations must ensure it is clear and verifiable. The GDPR includes specific provisions to protect children's data, especially in online environments such as social media, games, and educational applications.
Implementation and Challenges	Implementing GDPR in practice presents several challenges, such as incorporating its requirements into existing data management processes, maintaining ongoing compliance, and adjusting to changing interpretations of privacy laws. Additionally, organizations must ensure strong data security and effective breach response protocols, as well as fully comprehend the extent of data collected, processed, and stored. Employers also need to educate their staff about GDPR compliance and the rights of data subjects.
Comparative Analysis	Since GDPR applies to any organization dealing with the data of EU citizens, it has a broader global scope compared to laws that are specific to certain industries (such as HIPAA for healthcare) or have a more restricted geographic focus. Additionally, GDPR offers a more comprehensive approach to data protection, setting higher standards for consent and the rights of data subjects than many other frameworks.
Impact of Noncompliance	Violating the GDPR can lead to serious consequences, including hefty financial penalties, legal actions, and damage to reputation. With fines reaching up to €20 million or 4% of the annual global turnover, whichever is higher, the financial risk is significant. Beyond monetary penalties, noncompliance can result in long-term operational disruptions, harm to a brand's reputation, and a decline in consumer trust.

The Digital Personal Data Protection (DPDP) Act, enacted in India in 2023, marks a crucial development in the nation's data protection framework. In January 2025, the Government of India released the Draft Digital Personal Data Protection Rules, 2025. For detailed information on the key areas of the DPDP Act 2023, please refer to Table 2 [14].

TABLE 2. OVERVIEW OF INDIA'S DPDP ACT

Area	Description
Objective	The Digital Personal Data Protection (DPDP) Act, 2023 of India seeks to protect individuals' personal data while ensuring that data processing for legitimate purposes is balanced.
Technology Adaptation	The DPDP Act embraces a digital-first strategy, prioritizing digital consent mechanisms, grievance resolution, and the operation of the Data Protection Board as a digital entity.
Key Entities in GDPR	• Data Principals: Individuals whose personal data is being processed. • Data Fiduciaries: Organizations that process personal data. • Significant Data Fiduciaries (SDFs): Organizations with additional responsibilities due to the volume and sensitivity of the data they manage. • Data Processors: Individuals or organizations that handle personal data on behalf of a data fiduciary without deciding the purpose or method of processing.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 14 Issue 03, March-2025

Key Data Processing Principles	• The act requires explicit consent for data processing, data minimization, purpose limitation, and data security. It also highlights individuals' rights to access, correct, and delete their data. • The DPDP Act, 2023 has significantly altered data localization in India. While it does not enforce strict data localization, it allows the government to restrict data transfers to certain countries based on national security concerns. Consequently, companies handling Indian citizens' data must be cautious about where they store and process this data.
Key Operational Requirements	• Data fiduciaries must implement robust security measures, provide clear consent notices, and promptly inform parties of data breaches. For high-risk processing, they are also required to conduct Data Protection Impact Assessments (DPIAs). • Upon discovering a personal data breach, data fiduciaries must notify the Data Protection Board (DPB) and the affected data principals immediately. • Within 72 hours of becoming aware of the breach, data fiduciaries must submit a detailed report to the DPB, including the nature, scope, timing, and location of the breach, as well as the actions taken to mitigate the risk. • Notifications to affected parties must detail the type and scope of the breach, potential consequences, mitigation measures being taken, and contact information for inquiries. • Unlike some other data protection laws, the DPDP Act mandates reporting of all breaches, regardless of their severity or potential impact. • Organizations face substantial penalties for failing to report breaches or for not implementing adequate security measures.
Special Categories of Data	• The DPDP Act considers any personal information that can identify an individual, either directly or indirectly, such as names, addresses, phone numbers, email addresses, and other identifiers. • Sensitive personal data includes financial, health, biometric, genetic, sexual orientation information, and details about political or religious beliefs. • The act has specific rules for managing children's data, requiring age verification and parental consent, and it also limits the processing of sensitive personal data.
Implementation and Challenges	Implementation challenges involve adhering to detailed consent requirements, handling cross-border data transfers, and dealing with the absence of specific security guidelines.
Comparative Analysis	The DPDP Act and the EU's GDPR share similarities in user rights and data protection principles. However, they differ in aspects such as data localization and government access to data.
Impact of Noncompliance	Failure to comply can lead to hefty fines, ranging from INR 50 crore to INR 250 crore, based on the severity of the breach. This highlights the importance of adhering to the act's regulations.

The BDSLCCI framework takes into account the CIA triad controls mapped by MCA and the prioritized controls of DiD. Each MCA assigns different levels of importance to confidentiality, integrity, and availability based on the potential business loss from cyber threats. For instance, a small or medium-sized enterprise (SME) in the manufacturing sector might have computer numeric control (CNC) machines on their shop floor. The biggest loss for that SME's business will be if CNC machines are disrupted by cyberattacks like ransomware or malware, which will stop production on the shop floor. The organization must address availability-related cybersecurity controls for MCA, a CNC machine, in order to meet Level 1 of the BDSLCCI. This SME can prioritize confidentiality and integrity-related CNC machine controls in later levels of BDSLCCI. Apart from this MCA’s

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 14 Issue 03, March-2025

cybersecurity, SMEs need to achieve controls for human layer security, data layer security, and host/endpoint security to achieve BDSLCCI level 1. These controls are essential to ensure that both operational efficiency and sensitive information are protected from potential threats. By implementing a robust cybersecurity framework, the organization can not only safeguard its CNC machines but also enhance overall resilience against future cyber incidents. On the other hand, for an SME working in the financial business domain where it is managing financial transactions via a web portal, confidentiality followed by integrity will be more important than availability. For the pharmaceutical domain's SME, if it is manufacturing medicines using computerized systems, the integrity of these systems is more important. This manipulation may result in the administration of incorrect dosages, which could have serious side effects or even be deadly. In this kind of SME, integrity-related cybersecurity controls for its MCA will be a high priority. Table 3 shows the BDSLCCI recommended list of cybersecurity controls for its qualification for the level 1, level 2, and level 3 [10. 11, 12, 28].

TABLE 3. BDSLCCI CYBERSECURITY MATURITY LEVELS FOR PARTICULAR SME

MCA's CIA Implementation Level for Particular SME	**Implementation of DiD Prioritised Controls for SME**	**SME's BDSLCCI Maturity Level**
Either Confidentiality, Availability or Integrity	Human Security Layer + Data Security Layer + Host/Endpoint Security Layer	Level - 1
Either Integrity and Availability, Confidentiality and Integrity, or Confidentiality and Availability	All controls of Level 1 + Network Security Layer + Application Security Layer	Level - 2
All Integrity, Confidentiality and Availability	All controls of Level 2 + Physical Perimeter Security Layer + Governance Security Layer	Level - 3

Table 4 shows the BDSLCCI recommended list of DiD cybersecurity controls for its level 1, level 2, and level 3 [10. 11, 12, 28].

TABLE 4. PRIORITIZATION OF DID CONTROLS ACCORDING TO BDSLCCI LEVELS

Priority Sequence	**Layer Name**	**Maturity Level**	**BDSLCCI Controls' Policies**
1	Host/Endpoint Security Layer	**BDSLCCI Level 1**	1.1 - Host/Endpoint Security Layer - Less Permission to User 1.2 - Host/Endpoint Security Layer - Endpoint Protection - Anti-Virus 1.3 - Host/Endpoint Security Layer - Licensed Operating System (OS) 1.4 - Host/Endpoint Security Layer - Block File Transfers
2	Data Security Layer		1.5 - Data Security Layer - Encryption 1.6 - Data Security Layer - Access control 1.7 - Data Security Layer – Secured Backup and Restoration 1.8 - Data Security Layer - Data Loss Prevention (DLP) 1.9 - Data Security Layer - Secure Deletion
3	Human Security Layer		1.10 - Human Security Layer - Cybersecurity Awareness Training 1.11 - Human Security Layer - Separation of Duties 1.12 - Human Security Layer - Service Level Agreement (SLA) 1.13 - Human Security Layer - Employee Background Check 1.14 - Human Security Layer - Review Access Rights 1.15 - Human Security Layer - Cyber Threat Alert Notifications 1.16 - Human Security Layer - Cybersecurity Banners / Posters 1.17 - Human Security Layer - Non-Disclosure Agreement (NDA)

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 14 Issue 03, March-2025

4	Network Security Layer	**BDSLCCI Level 2**	2.1 - Network Security Layer - Network Firewall 2.2 - Network Security Layer - Network Access Control 2.3 - Network Security Layer - Remote Access Virtual Private Network (VPN) 2.4 - Network Security Layer - Instruction Detection & Prevention Systems (IDPS) 2.5 - Application Security Layer - The Open Worldwide Application Security Project (OWASP) Coding Practices 2.6 - Application Security Layer - Application Hardening
5	Application Security Layer		
6	Physical Perimeter Security Layer	**BDSLCCI Level 3**	3.1 - Physical Perimeter Security Layer - Locked and Dead-Bolted Steel Doors 3.2 - Physical Perimeter Security Layer - Closed-Circuit Surveillance Cameras (CCTV) 3.3 - Physical Perimeter Security Layer - Picture IDs 3.4 - Physical Perimeter Security Layer - Security Guards / Proper Lighting / Biometrics / Environmental Control 3.5 - Governance Security Layer - Incident Response (IR) Process 3.6 - Governance Security Layer - Business Continuity Plan (BCP) 3.7 - Governance Security Layer – Periodic Security Audit
7	Governance Security Layer		

In addition to policy areas, BDSLCCI suggests using the ARCSIK matrix to assign various organizational roles as follows:

A - Accountable: This role is held accountable if risks occur, often due to failed preventative controls. This person has the final authority over the successful completion of specific tasks or deliverables.

R - Responsible: This role is primarily responsible for completing tasks in this area. It can be a manager or team member directly responsible for successfully completing a project task.

C - Consulted: This role provides guidance and support to those more actively involved. It is a hands-off role, typically filled by someone with unique insights the team will consult.

S - Supportive: This role actively contributes to planning, executing, or managing tasks in this section. Team members in this role perform various activities or deliverables to benefit the process or project and provide support.

I - Informed: This role should be kept updated on the status of risks in this area as it is in their best interest. It can be a client or executive who isn't directly involved but should be kept informed.

K - Knowledgeable: Tasks not yet assigned to specific colleagues can be completed by anyone with the necessary expertise and knowledge if roles are not assigned.

Figure 2 shows the snapshot of the sample ARCSIK matrix that explains how the personal data privacy act's requirements are mapped with key roles such as DPO and top management. BDSLCCI recommends using such a kind of mechanism to keep track of roles mapped with areas in cybersecurity or data protection.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 14 Issue 03, March-2025

BDSLCCI Controls Categories A = Accountable, R = Responsible, C = Consulted, S = Supportive, I = Informed, K = Knowledgeable		Data Protection Officer (DPO)	Managing Director/CEO	Security Manager	Head of IT/CIO
4.1 Personal Data Privacy (GDPR EU / DPDPA India)					
4.1.1	Monitoring Compliance - Regular Audits	A	A	C	C
4.1.2	Monitoring Compliance - Training	A	A	C	C
4.1.3	Monitoring Compliance - Data Protection Impact Assessments (DPIAs) Advisory Role	A	A	C	C
4.1.4	Liaison with Supervisory Authorities - Point of Contact	A	A	C	C
4.1.5	Liaison with Supervisory Authorities - Cooperation	A	A	C	C
4.1.6	Handling Data Subject Requests - Access Requests	A	A	C	C
4.1.7	Handling Data Subject Requests - Rectification and Erasure	A	A	C	C
4.1.8	Advising on Data Protection Matters - Policy Development	A	A	C	C
4.1.9	Advising on Data Protection Matters - Risk Management	A	A	C	C
4.1.10	Record Keeping - Maintaining Records Documentation	A	A	C	C
4.1.11	Record Keeping - Reporting	A	A	C	C
4.1.12	Incident Response - Data Breach Notification	A	A	C	C

Figure 2: BDSLCCI Personal Data Privacy Role Mapping

The BDSLCCI framework is assisting many SMEs, SMBs, MSMEs, and even startup companies in their initial stages. To facilitate deployment for many SMEs, this framework is available as an AI-ML-powered web portal with many facilities.

Refer to figure 3, explaining high-level BDSLCCI framework coverage. BDSLCCI's gap analysis helps SMEs to understand their current cybersecurity posture compared to the latest version of the BDSLCCI framework. The BDSLCCI web portal helps to identify recommended MCA and DiD controls for achieving BDSLCCI levels 1, 2, and 3. It also helps with sample documentation about policies and guidelines. It also provides sample documentation such as the Employee Consent Form for Data Privacy, which helps SMEs save time to adopt guidelines. Apart from that, BDSLCCI provides optional tools to check the vulnerabilities in endpoints. It also provides online cybersecurity awareness training for the employees. Once an SME implements recommended cybersecurity controls, it can undergo an online or offline BDSLCCI audit and assessment. If auditors approve satisfactory implementation of the BDSLCCI framework, the SME receives the BDSLCCI certificate, transcript, and detailed analytics report showing the effectiveness and coverage of the controls.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 14 Issue 03, March-2025

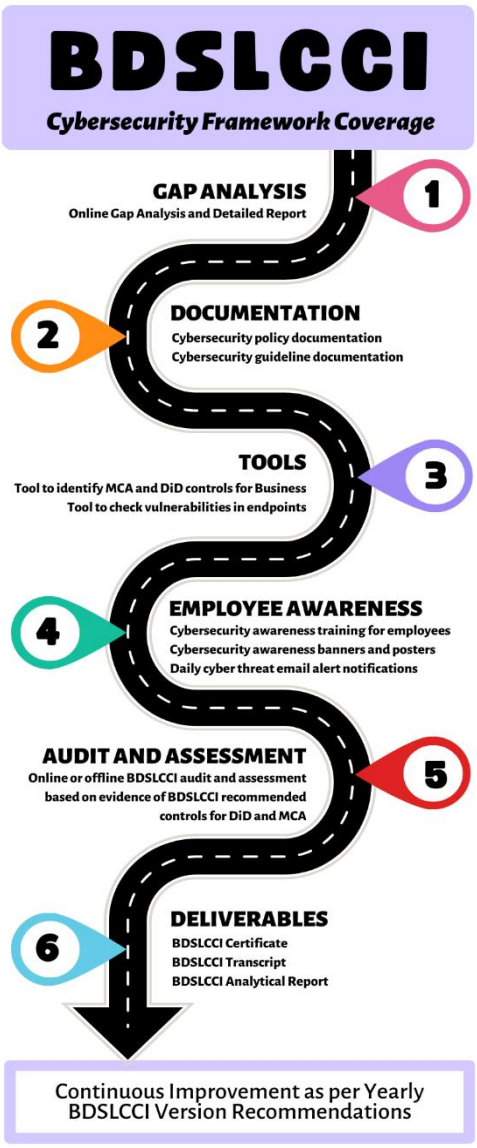

Figure 3: BDSLCCI Cybersecurity Framework Coverage

Table 5 shows key differences between BDSLCCI and GDPR [11, 12, 13]. The BDSLCCI framework is not only helping SMEs to implement cybersecurity controls tailored to their business domain but also helps in adhering to the requirements of data protection acts of different countries with additional guidelines [10, 11].

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 14 Issue 03, March-2025

TABLE 5. BDSLCCI VS GDPR

BDSLCCI	GDPR
Focuses on Defense in Depth (DiD) and Mission Critical Assets (MCAs)	Emphasizes safeguarding data
A risk-based strategy to safeguard personal information privacy involves implementing technical, physical, and administrative controls to ensure cybersecurity.	A right-based strategy to address more general threats to the liberties and privileges of data subjects.
Documentation is private, changes with the new version of BDSLCCI on a yearly basis to align with the latest cybersecurity needs, and is protected by strict copyrights.	Publicly and easily available
Focus on preventive controls, detective controls, deterrent controls, recovery controls, and corrective controls protecting many security layers of the organization, including data security.	Refers to both digital and physical media's unstructured data.
Helping organizations to adopt cybersecurity best practices, including protection of PII data.	Likelihood and gravity of the risks to the liberties and privileges of associated human beings.
A cybersecurity management system	A legal framework
Recommended policies and guidelines	Mandatory principles and requirements
Different terminologies for different guidelines of data protection acts	Terminologies Used: Data Subject, Data Controller, Data Processor
International with possible consideration of regional compliance needs via recommended guidelines	International
Certification of BDSLCCI level achieved	Certification Article 43
Incident management policy is recommending adherence to the requirement of breach notification as per the law of the land or relevant compliance requirements	Breach notification with 72-hour requirement

A few important personal data protection laws from various nations are displayed in Table 6. The European Union's GDPR is frequently regarded as one of the world's most extensive and strict data protection regulations. With stringent requirements for consent, data subject rights, data breach notifications, and severe penalties for non-compliance, it establishes a high bar for data privacy and security. This table illustrates how nearly all data protection laws in various countries or regions are in full conformity with GDPR.

The GDPR aims to protect the personal information and privacy of individuals in the European Union and the European Economic Area (EEA). Generally, SMEs with fewer than 250 employees are not required to maintain records of their processing activities unless the processing is routine, poses risks to individuals' rights and freedoms, or involves sensitive data or criminal records. SMEs are only required to appoint a Data Protection Officer (DPO) if their main activities include processing sensitive data, criminal records, or extensive monitoring of individuals. To help SMEs understand and comply with GDPR regulations, the European Data Protection Board (EDPB) has published a guide specifically for them [12, 17].

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 14 Issue 03, March-2025

The Privacy Act 1988 is a key Australian law that governs how government agencies, businesses, and private sector entities manage personal data. It sets out rules for collecting, using, storing, and sharing personal information to protect individuals' privacy. For SMEs, this law has specific implications. Most small businesses with annual revenues of $3 million or less are generally exempt from the Privacy Act. However, there are exceptions. For example, businesses must comply with the Act if they provide health services, trade in personal data, or are contractors under a Commonwealth contract. If a small business is subject to the Privacy Act, it must adhere to the 13 Australian Privacy Principles (APPs), which outline standards for handling personal data. The Office of the Australian Information Commissioner (OAIC) provides a Privacy Checklist for Small Businesses to determine if they need to comply with the Act. In response to rising data breaches and cyberattacks, the Privacy and Other Legislation Amendment Bill 2024 aims to strengthen privacy laws, including stricter requirements for companies handling personal information [15, 16].

Japan's Act on the Protection of Personal Information (APPI), established in 2003, is a comprehensive law governing how governments and businesses manage personal data. Any company, regardless of size, that handles the personal data of Japanese citizens must comply with the APPI. This includes both domestic and international businesses dealing with Japanese personal information. SMEs must adhere to the APPI's requirements, such as obtaining consent before data collection, ensuring data accuracy, and implementing security measures to protect personal information. Regular updates and audits of data protection policies are also recommended. The APPI was amended in 2020 to enforce stricter data security measures and impose harsher penalties for noncompliance, emphasizing the importance of security and transparency in handling personal data. The Japanese government provides guidelines and resources to help SMEs comply with the APPI, offering practical advice on implementing data protection practices and understanding legal obligations [18. 19].

The Protection of Personal Information Act (POPIA) in South Africa is a comprehensive data protection law designed to safeguard personal information processed by both public and private entities. Enacted in 2013, it became fully effective on July 1, 2020. POPIA applies to all businesses, including SMEs, that handle personal data. This means that any company, regardless of size, dealing with the personal information of South African citizens must comply with the Act. SMEs must adhere to eight requirements: accountability, processing limitation, purpose specification, further processing limitation, information quality, transparency, security measures, and data subject participation. Additionally, SMEs must appoint an information officer responsible for ensuring POPIA compliance, managing data subject requests, conducting impact assessments, and developing and implementing a compliance framework. The Information Regulator provides resources and guidelines, such as best practices, checklists, and templates, to help SMEs comply with POPIA [20, 21].

Thailand's Personal Data Protection Act (PDPA) is a thorough data protection law aimed at safeguarding personal information. Enacted in 2019, it became fully effective on June 1, 2022. The PDPA impacts all businesses, including SMEs [22, 23].

The California Consumer Privacy Act (CCPA) is a landmark privacy regulation that bolsters the privacy rights and protections for California residents. Enacted on June 28, 2018, and effective from January 1, 2020, the CCPA applies to businesses meeting any of these criteria: annual gross revenues over $25 million; handling personal information of 50,000 or more consumers, households, or devices annually; or earning at least 50% of annual revenue from selling consumer personal information. SMEs face unique challenges in complying with the CCPA, such as managing vendor relationships, limited privacy teams, and scarce resources for compliance. Under the CCPA, consumers have rights including data deletion requests, opting out of personal information sales, and knowing what personal data is collected. Even if not required by the CCPA, SMEs can benefit from good privacy practices, such as ensuring data security, being transparent about data collection, and respecting customer privacy preferences [24, 25].

In 2023, India enacted the Digital Personal Data Protection Act (DPDP Act), establishing a comprehensive framework for managing digital personal data. This legislation significantly impacts MSMEs, requiring even small businesses handling personal data to comply with its provisions.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 14 Issue 03, March-2025

Companies must obtain explicit and informed consent from individuals before collecting their personal information, implement strong security measures to prevent breaches and unauthorized access, and respect individuals' rights to access, update, and delete their data. To ease compliance, the Act provides certain exemptions for MSMEs, such as not needing to appoint a Data Protection Officer (DPO) or having less stringent reporting requirements unless they handle sensitive personal data. Despite these exemptions, MSMEs may struggle with compliance due to limited resources and expertise. To support MSMEs, the government and other organizations offer resources and guidelines to help them understand and implement the necessary measures [14, 26, 27].

TABLE 6. COMPARISON OF FEW DATA PROTECTION ACTS OF DIFFERENT COUNTRIES KEEPING GDPR AS BASE

Aspect	GDPR (EU)	Australia's Privacy Act	Japan's APPI	South Africa's POPIA	Thailand's PDPA	California's CCPA	India's DPDP Act
Scope	Personal data of EU residents	Personal information of individuals	Personal information of individuals	Personal information of individuals	Personal data of individuals	Personal information of California residents	Digital personal data of individuals
Consent	Explicit consent required	Implied or express consent	Explicit consent required	Explicit consent required	Explicit consent required	Explicit consent required	Explicit consent required
Data Subject Rights	Access, rectification, erasure, etc.	Access, correction	Access, correction, deletion	Access, correction, deletion	Access, correction, deletion	Access, correction, deletion	Access, correction, deletion
Data Breach Notification	Within 72 hours	As soon as practicable	Without delay	As soon as reasonably possible	Within a reasonable time	Within 72 hours	Within a reasonable time
Penalties	Up to €20 million or 4% of global turnover	Up to AUD 2.1 million	Up to JPY 100 million	Up to ZAR 10 million	Up to THB 5 million	Up to $7,500 per violation	Up to ₹250 crore or 4% of global turnover
Data Protection Officer (DPO)	Required for certain organizations	Not mandatory	Required for certain organizations	Required for certain organizations	Required for certain organizations	Required for certain organizations	Required for certain organizations

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 14 Issue 03, March-2025

3. BDSLCCI FRAMEWORK MAPPING WITH DATA PROTECTION COMPLIANCE

As explained in Table 4, there are key BDSLCCI policy' areas divided into multiple layers of the organization. Those can be mapped with relevant GDPR article requirement fulfilment as explained in Table 7 [13]. In addition to this, BDSLCCI offers separate documentation on the EU's GDPR Policy Guidelines, which SMEs can easily understand, along with additional precautionary measures that organizations should take.

TABLE 7. GDPR ARTICLES MAPPED WITH BDSLCCI POLICIES OR GUIDELINES

GDPR Article	Relevant BDSLCCI Policies / Guidelines
Article 6: This article outlines the legal grounds for processing personal data, specifying the conditions that must be met for such processing to be considered lawful.	It can be achieved by access control management and account management. BDSLCCI recommends to implement below cybersecurity control areas: 1.6, 1.8, 1.10, 1.11, 1.12, 1.14, 1.17, ARCSIK Matrix, Asset Management, and guidelines for consent form showing data subject has given explicit consent for their data to be processed for one or more specific purposes.
Article 7: Conditions for Consent - Consent must be given voluntarily, be specific, informed, and clear. Individuals have the right to revoke their consent at any time. **Article 10:** Processing of Personal Data Relating to Criminal Convictions and Offences - This article addresses the handling of personal data related to criminal convictions and offenses. **Article 15:** Right of Access by the Data Subject - Individuals have the right to access their personal data and obtain details on how it is being processed. **Article 29:** Processing Under the Authority of the Controller or Processor - Those handling personal data must do so under the direction of the controller or processor. **Article 22:** Automated Individual Decision-Making, Including Profiling - This article covers decisions made solely by automated means, including profiling.	It can be achieved by access control management and data protection. BDSLCCI recommends to implement below cybersecurity control areas: 1.1, 1.4, 1.5, 1.6, 1.8, 1.10, 1.11, 1.12, 1.13, 1.14, 1.17, 2.1, 2.2, 2.3, 2.4, ARCSIK Matrix, and guidelines for consent form.
Article 30: Documentation of Processing Activities - Controllers and processors must maintain records of their processing activities, detailing the categories of data subjects and the purposes for processing.	It can be achieved by audit log management and data protection. BDSLCCI recommends to implement below cybersecurity control areas: 1.5, 1.6, 1.8, 1.11, 1.12, 1.14, 1.17, 2.1, 2.2, 2.3, 2.4, 2.5, 2.6, and ARCSIK Matrix, and Asset Management.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 14 Issue 03, March-2025

Article 33: Notification of a Personal Data Breach to the Supervisory Authority - Controllers must inform the supervisory authority of any personal data breach within 72 hours.	It can be achieved by audit log management and incident response planning. BDSLCCI recommends to implement below cybersecurity control areas: 1.6, 1.11, 1.14, 2.1, 2.2, 2.4, 2.5, 2.6, 3.5, and ARCSIK Matrix.
Article 9: Handling certain categories of personal data, such as political opinions, racial or ethnic background, and health details. **Article 11:** Identification is not required for processing. **Article 44:** Personal data can only be transferred to foreign entities or countries under specific conditions. **Article 45:** Transfers are allowed if there is an adequacy decision. **Article 46:** Transfers are permissible with appropriate safeguards, like binding corporate rules or standard data protection clauses. **Article 48:** It is prohibited to transfer or disclose personal data if not allowed by Union law. **Article 49:** Data transfers may be allowed in certain situations, such as with explicit consent or significant public interest, even without standard protections.	It can be achieved by data minimization and data protection. BDSLCCI recommends to implement below cybersecurity control areas: 1.5, 1.6, 1.8, 1.11, 1.12, 1.14, 1.17, 2.1, 2.2, 2.3, 2.4, 2.5, 2.6, ARCSIK Matrix, and Asset Management.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 14 Issue 03, March-2025

Article 5: Personal data must be processed in a fair, lawful, and transparent manner. It should be collected for specific, legitimate purposes and not used in ways that are incompatible with those purposes. The data must be accurate, up-to-date, and retained only as long as necessary. **Article 8:** Conditions for obtaining consent from children to use information society services. **Article 12:** Clear communication, information, and procedures must be provided to data subjects to enable them to exercise their rights. **Article 13:** Information that must be provided when personal data is collected from the data subject. **Article 14:** Information that must be provided when personal data is not obtained directly from the data subject. **Article 16:** Right to Rectification - Data subjects have the right to request the correction of inaccurate personal data without undue delay. They also have the right to complete any incomplete personal data, including by providing a supplementary statement. **Article 17:** Right to Erasure (also known as the "right to be forgotten") - Individuals can request the deletion of their personal data in certain situations, such as when it is no longer needed for its original purpose. **Article 18:** Right to restrict processing - Data subjects can request limitations on the processing of their personal data under specific conditions. **Article 19:** Obligation to inform about the correction, deletion, or restriction of personal data processing. **Article 20:** Right to data portability - This right allows individuals to easily move, copy, or transfer their personal data across different IT environments, giving them greater control over their information. **Article 21:** Right to object - This right enables individuals to prevent the use of their personal data in certain circumstances, ensuring they have control over their information. **Article 25:** Data protection by design and default - This article requires controllers to implement appropriate organizational and technical measures to ensure data protection principles are integrated into processing activities.	It can be achieved by encryption and data protection. BDSLCCI recommends to implement below cybersecurity control areas: 1.1, 1.4, 1.5, 1.6, 1.8, 2.1, 2.2, 2.3, 2.4, ARCSIK Matrix, and guidelines for consent form.
Article 41: Monitoring of Approved Codes of Conduct - An accredited body must oversee the adherence to approved codes of conduct.	It can be achieved by secure configuration and data protection. BDSLCCI recommends to implement below cybersecurity control areas: 1.1, 1.4, 1.11, 1.14, 2.2, 2.4, 2.5, 2.6, 3.2, 3.4, ARCSIK Matrix, and Asset Management.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 14 Issue 03, March-2025

Article 24: Controllers must implement the necessary organizational and technical measures to ensure and demonstrate that data processing complies with the GDPR.	It can be achieved by secure configuration and data protection. BDSLCCI recommends to implement below cybersecurity control areas: 1.1, 1.4, 1.11, 1.14, 2.2, 2.4, 2.5, 2.6, 3.2, 3.4, 3.7, ARCSIK Matrix, and Asset Management.
Article 26: Joint controllers - When two or more entities collaboratively determine the purposes and means of processing personal data, they are considered joint controllers. **Article 47:** Binding Corporate Rules (BCRs) - These rules ensure that personal data transferred within a corporate group, including to countries outside the EU, is safeguarded in line with GDPR requirements.	1.1, 1.2, 1.4, 1.5, 1.6, 1.7, 1.8, 1.9, 1.11, 1.14, 1.15, 1.16, 1.17, 2.2, 2.4, 2.5, 2.6, 3.2, 3.4, ARCSIK Matrix, and Asset Management.
Article 31: Cooperation with the Supervisory Authority - Controllers and processors must work together with supervisory authorities.	It can be achieved by Governance and incident response planning. BDSLCCI recommends to implement below cybersecurity control areas: 1.1, 1.4, 1.11, 1.14, 2.2, 2.4, 2.5, 2.6, 3.2, 3.4, 3.5, and Asset Management.
Article 36: Prior Consultation - Prior to processing, the controller must consult with the supervisory authority if a data protection impact assessment indicates that the processing could present a high risk.	It can be achieved by Governance, and risk assessment and management. BDSLCCI recommends to implement below cybersecurity control areas: BDSLCCI Gap Analysis, 1.1, 1.4, 1.11, 1.14, 1.17, 2.2, 2.4, 2.5, 2.6, 3.2, 3.4, 3.5, 3.6, 3.7, ARCSIK Matrix, and Asset Management.
Article 27: Representatives of Controllers or Processors Outside the Union - This article mandates that controllers or processors not established within the EU must designate a representative in the Union.	It can be achieved by Governance, and secure configuration. BDSLCCI recommends to implement below cybersecurity control areas: 1.1, 1.4, 1.5, 1.6, 1.8, 1.9, 2.1, 2.2, 2.3, 2.4, 2.5, 2.6, ARCSIK Matrix, and Asset Management.
Article 37: Data Protection Officer Designation - This article outlines the criteria for appointing a data protection officer. **Article 38**: Position of the Data Protection Officer - This article details the role and resources allocated to the data protection officer within the organization.	It can be achieved by Governance, and training and awareness programs. BDSLCCI recommends to implement below cybersecurity control areas: 1.1, 1.4, 1.11, 1.14, 1.15, 1.16, 1.17, 2.2, 2.4, 2.5, 2.6, 3.2, 3.4, ARCSIK Matrix, and Asset Management.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 14 Issue 03, March-2025

Article 39: Data Protection Officer Duties - This article specifies the responsibilities of the data protection officer, including providing advice and monitoring compliance. **Article 40**: Codes of Conduct - Codes of conduct can be used as proof of compliance with GDPR. **Article 42**: Certification Procedures - Certification processes can be used to demonstrate adherence to GDPR standards.	
Article 34: Notifying the Data Subject of a Personal Data Breach - This article requires controllers to inform the data subject of a personal data breach if it significantly threatens their rights and freedoms.	It can be achieved by incident response planning and data protection. BDSLCCI recommends to implement below cybersecurity control areas: 1.1, 1.4, 1.11, 1.14, 2.2, 2.4, 2.5, 2.6, 3.2, 3.4, 3.5, 3.6, ARCSIK Matrix, and Asset Management.
Article 32: Security of Processing - Controllers and processors must ensure an appropriate level of security for the risk, including measures like encryption and pseudonymization.	It can be achieved by multifactor authentication (MFA), endpoint protection, and incident response planning. BDSLCCI recommends to implement below cybersecurity control areas: 1.1, 1.2, 1.4, 1.5, 1.6, 1.8, 2.1, 2.2, 2.4, 2.5, 2.6, and 3.5.
Article 35: Data Protection Impact Assessment - When processing operations present a high risk to individuals' rights and freedoms, a data protection impact assessment must be carried out.	It can be achieved by risk assessment and management, and continuous vulnerability management. BDSLCCI recommends to implement below cybersecurity control areas: BDSLCCI Gap Analysis, 3.5, 3.6, and 3.7.
Article 28: Engaging Processor - Controllers may only engage processors that provide sufficient guarantees to implement the required organizational and technical measures.	It can be achieved by vendor management and data protection. BDSLCCI recommends to implement below cybersecurity control areas: 1.1, 1.4, 1.5, 1.6, 1.8, 1.12, 1.17, 2.1, 2.2, and 2.3.

The draft regulations outline the specifics of "6. Reasonable security safeguards," which the Central Government plans to establish on or after the Act's effective date, under the authority provided by subsections (1) and (2) of section 40 of the Digital Personal Data Protection Act, 2023 (22 of 2023) [14].

(1) A Data Fiduciary must protect personal data under their control, including data processed by a Data Processor, by implementing the following security measures to prevent breaches:

(a) Implement appropriate data security procedures, such as encryption, obfuscation, masking, or using virtual tokens for personal data protection.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 14 Issue 03, March-2025

(b) Establish adequate controls to restrict access to the computer resources used by the data processor or data fiduciary.

(c) Ensure transparency in accessing personal data through logs, monitoring, and reviews to identify unauthorized access, investigate incidents, and prevent recurrence.

(d) Implement safeguards for ongoing data processing to maintain the confidentiality, availability, or integrity of personal data, such as data backups in case of data destruction or loss.

(e) Retain logs and personal data for one year, unless otherwise required by law, to detect unauthorized access, investigate incidents, and ensure continued processing in case of a compromise.

(f) Include a clause in agreements between the data processor and data fiduciary that mandates the implementation of appropriate security measures.

(g) Implement suitable organizational and technical measures to ensure effective adherence to security precautions.

(2) In this rule, the term "computer resource" is defined as per the Information Technology Act, 2000 (21 of 2000). This includes any computer, computer system, computer network, data, computer database, or software, encompassing all digital and electronic systems and devices used for data processing, storage, and transmission.

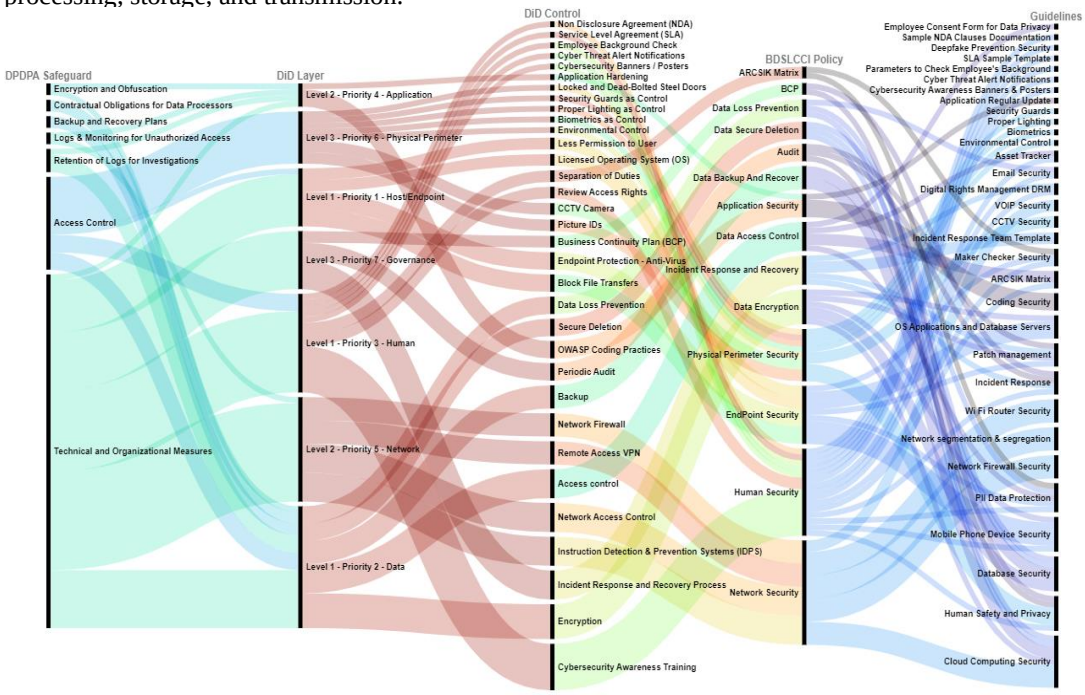

Figure 4: BDSLCCI Controls Mapped with Reasonable security safeguards of DPDP Act, India

As illustrated in Figure 4, the reasonable security safeguards of the DPDP Act can be aligned with BDSLCCI's DiD layer. This is followed by specific control areas within the DiD, along with BDSLCCI's recommended policies and guidelines. Additionally, BDSLCCI offers separate guideline documentation for India's Digital Personal Data Protection (DPDP) Act to help SMEs understand its requirements and adopt further precautionary measures [10, 11, 12, 14, 26, 27].

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 14 Issue 03, March-2025

4. CONCLUSION

It is evident that many SMEs are already facing various challenges in their journey and are not prioritizing investments in cybersecurity and hence increasing risks for not adhering compliance to the data protection acts. Proposed BDSLCCI cybersecurity framework is taken into consideration to resolve various barriers such SMEs facing to protect data and other critical assets.

To conclude the discussion, below are a couple of points:

- Apart from data security layer, each security layer in the SME plays important role to comply with cybersecurity followed by data protection compliance.
- The recommended BDSLCCI cybersecurity framework addresses numerous key issues for SMEs and aids in complying with most data protection act requirements.

In the future, this framework can be further developed to support enterprises beyond the SME category.

Funding

This research received no external funding.

Acknowledgments

This project received no external finance.

Declaration of Interest's Statement

The author declares that there are no conflicts of interest regarding the publication of this paper.

REFERENCES

[1] Dammann, O., 2019. Data, information, evidence, and knowledge: a proposal for health informatics and data science. Online journal of public health informatics, 10(3), p.e224.
[2] Nie, Z., 2024. Understanding how to identify and manage personal identifying information (PII) to further data interoperability. Journal of eScience Librarianship, 13(3).
[3] Olabanji, S.O., Oladoyinbo, O.B., Asonze, C.U., Oladoyinbo, T.O., Ajayi, S.A. and Olaniyi, O.O., 2024. Effect of adopting AI to explore big data on personally identifiable information (PII) for financial and economic data transformation. Available at SSRN 4739227.
[4] Rodrigues, G.A.P., Serrano, A.L.M., Vergara, G.F., Albuquerque, R.D.O. and Nze, G.D.A., 2024. Impact, Compliance, and Countermeasures in Relation to Data Breaches in Publicly Traded US Companies. Future Internet, 16(6), p.201.
[5] Zaeifi, M., Kalantari, F., Oest, A., Sun, Z., Ahn, G.J., Shoshitaishvili, Y., Bao, T., Wang, R. and Doupé, A., 2024, June. Nothing Personal: Understanding the Spread and Use of Personally Identifiable Information in the Financial Ecosystem. In Proceedings of the Fourteenth ACM Conference on Data and Application Security and Privacy (pp. 55-65).
[6] Dieter (2024). The biggest data breaches of 2024. [online] ConsumerAffairs. Available at: https://www.consumeraffairs.com/news/the-biggest-data-breaches-of-2024-121824.html.
[7] Cybernews (2025). Latest Security News | Cybernews. [online] Cybernews. Available at: https://cybernews.com/security/ (Accessed 13 Feb. 2025).
[8] Bharat P. and Jyotirmoy Banerjee, Strengthening the Legal Frameworks of Data Piracy and Cybersecurity in Digital Era, 4 IJHRLR 187-199 (2025). Available at www.humanrightlawreview.in/archives/
[9] Gracy, S.S., 2025. A global analysis of data breaches from 2004 to 2024. arXiv preprint arXiv:2502.05205.
[10] Pawar, S.A. and Palivela, H. (2023). Importance of Least Cybersecurity Controls for Small and Medium Enterprises (SMEs) for Better Global Digitalised Economy. Contemporary Studies in Economic and Financial Analysis, [online] 110B(978-1-83753-417-3), pp.21–53. Available at: https://ideas.repec.org/h/eme/csefzz/s1569-37592023000110b002.html.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 14 Issue 03, March-2025

[11] Pawar, S. and Pawar, P. (2024). BDSLCCI. [online] notionpress.com. Available at: https://notionpress.com/read/bdslcci.

[12] Pawar, S., & Palivela, Dr. H. (2022). LCCI: A framework for least cybersecurity controls to be implemented for small and medium enterprises (SMEs). International Journal of Information Management Data Insights, 2(1), 100080. https://doi.org/10.1016/j.jjimei.2022.100080.

[13] European Parliament and Council of the European Union, "General Data Protection Regulation," Official Journal of the European Union, L119, pp. 1-88, 2016.

[14] Government of India - Ministry of Electronics and Information Technology (2025). Data Protection Framework. [online] Available at: https://www.meity.gov.in/data-protection-framework.

[15] Gregorczuk, H., 2024. An Examination and Reconsideration of Fair Collection under the Australian Privacy Act in the Context of Retail Analytics and Big Data.

[16] Conde, J. and Svantesson, D.J.B., 2024. The five generations of facial recognition usage and the Australian privacy law. International Data Privacy Law, p.ipae007.

[17] Smirnova, Y. and Travieso-Morales, V., 2024. Understanding challenges of GDPR implementation in business enterprises: a systematic literature review. International Journal of Law and Management, 66(3), pp.326-344.

[18] Syed, H.I., 2024. The Impact of EU GDPR on EU SMEs Competitive Advantage.

[19] Yasuoka, H., 2023. Digital Transformation Strategies and Issues in Local SMEs: Issues of Strategy and Personal Data. Journal of Strategic Management Studies, 14(2), pp.25-31.

[20] Chimboza, T. and Smith, E., 2024. How Does Compliance with the Protection of Personal Information Act (POPI Act) Affect Organisations in South Africa.

[21] Bengu, S.P. and Beharry-Ramraj, A., 2024. Digitalisation For SME Integration Into Large Enterprises In South Africa: A Financial Services Framework. Available at SSRN 5023630.

[22] Tungtrakul, C., Thawornsujaritkul, T. and Silpcharu, T., 2024. The Guide for Information Technology Management Regarding Personal Data Protection of the Industrial Business Sector in Thailand. International Journal of Instructional Cases, 8(2), pp.196-210.

[23] Ketmaneechairat, H., Maliyaem, M. and Puttawattanakul, P., International Journal of Technology.

[24] Shehzadi, T., Privacy in the Digital Age: Balancing Innovation and Compliance in Marketing Strategies.

[25] Will, C. and Elly, B.B.B., 2024. Data Privacy by Design: A Business Analytics Perspective.

[26] Patil, A., 2024. Navigating the Digital Landscape: India's Evolving Legal Framework for E-commerce, Data Protection, and Cyber security. Data Protection, and Cyber security (May 29, 2024).

[27] Hardik, N., 2024. Digitalisation promotes adoption of soft information in SME credit evaluation: The case of Indian banks. Digital Finance, 6(1), pp.23-54.

[28] Pawar, S., & Palivela, H. (2025). Review and Design of Business Domain-Specific Cybersecurity Controls Framework for Micro, Small, and Medium Enterprises (MSMEs). Archives of Advanced Engineering Science, 1-19. https://doi.org/10.47852/bonviewAAES52024438.