International Journal of
INTELLIGENT SYSTEMS AND APPLICATIONS IN ENGINEERING
ISSN:2147-6799 www.ijisae.org Original Research Paper

Securing the Supply Chain: Addressing CMMC 2.0 Implementation Barriers Through the BDSLCCI Framework

Shekhar Pawar*[1], Hemant Palivela[2]

Submitted:05/11/2025 **Accepted:**16/12/2025 **Published:**26/12/2025

Abstract: Implementing Cybersecurity Maturity Model Certification (CMMC) 2.0 is facing a few challenges for organizations all over the world, especially those involved in supply chains for critical infrastructure and defense. Many small and medium-sized businesses (SMBs) find it difficult to achieve the intricate, resource-intensive criteria of CMMC 2.0 as cybersecurity threats increase and regulatory expectations change. This study examines the systemic obstacles to adoption, such as audit preparedness, ongoing compliance, and third-party monitoring, and suggests the BDSLCCI Framework as a multilingual, scalable, and governance-integrated substitute. The study shows how global stakeholders can improve cybersecurity maturity, lessen compliance fatigue, and promote resilient supply ecosystems by mapping CMMC 2.0 criteria to BDSLCCI's layered architecture. In order to democratize cybersecurity and promote inclusive, cross-border compliance tactics, the findings urge the wider worldwide adoption of flexible frameworks such as BDSLCCI.

Keywords: *CMMC 2.0, BDSLCCI, Supply Chain Security, Small and Medium Business (SMB), Cybersecurity*

1. Introduction

A Small and Medium Business (SMB) is classified differently in each country, usually according to factors like the number of employees and/or a specific range of yearly revenue. While few countries refer to these organizations as Small and Medium Enterprises (SMEs), others use the more general term Micro, Small, and Medium Enterprises (MSMEs), which reflects more specificity in terms of size and scope. Approximately 90% of all businesses worldwide are SMBs, numbering over 400 million. According to a 2016 World Trade Organization (WTO) report, these businesses contribute to approximately 70% of worldwide employment and account for 55% of the GDP in developed countries, demonstrating their critical role in economic development [17, 22]. The comparable numbers in the United States are especially striking, with some 31 million small firms and only 20,000 large enterprises. Nearly half of the private sector workforce is employed by small firms, which make up over 99% of all company organizations and account for over 44% of the country's total economic activity [29].

SMBs account for 95% of global manufacturing's total volume and are essential to the creation of value across supply chains, making them a powerful force in the industry. SMBs are essential at every stage of these networks, even though big businesses frequently take the lead. However, their capacity to maintain strong cybersecurity is hampered by their constrained resources and conflicting priorities. Many SMBs underestimate their susceptibility to cyber threats, even when they think they are well-prepared. According to recent study, SMBs are potential entry points for cybercriminals due to staffing and financial limitations that result in insufficient IT security measures, particularly in digitally connected ecosystems like Industry 4.0. Even bigger enterprises with robust security systems are at risk from this. Unfortunately, more than half of all companies have been the target of a cyberattack. Supply chains are implementing risk-reduction techniques, but they frequently ignore potential risks associated with SMBs. Blockchain and other emerging technologies provide new ways to improve data integrity, security, and resilience, but they are unable to address the systemic threats that under protected SMBs inside interconnected supply networks face [11, 12, 13, 23].

SMBs are at significant risk from cybercrime, which can have a variety of adverse effects, from direct financial losses and operational disruptions to brand harm and an overall decrease in customer trust. Limited resources are further strained by legal penalties and regulatory hurdles, while the psychological toll on employees and business owners or top management - manifesting as concern and anxiety - compounds the burden. Better cybersecurity preparedness among SMBs is necessary because the severity of these implications frequently corresponds with the magnitude of the attack. Since these companies make up the bulk of players in global supply chains, any weakness or interruption that affects them has a domino effect on the larger ecosystem. When an SMB suffers a cyberattack, it may lose access to critical data or systems. This disruption leads to missed client delivery deadlines, triggering contract cancellations and damaging market reputation. As revenue declines, layoffs may follow, causing employee morale to plummet. The initial breach sets off a chain reaction - each consequence toppling the next like falling dominoes. Their operational health, particularly in areas like

1 DBA, Swiss School of Business and Management School Geneva, Geneva Business Center, Avenue des Morgines 12, Genève, 1213, Switzerland
ORCID ID: 0000-0001-7091-4113
2 Visiting Professor, Swiss School of Business and Management School Geneva, Geneva Business Center, Avenue des Morgines 12, Genève, 1213, Switzerland
ORCID ID: 0000-0002-5040-6979
** Corresponding Author Email: shekhar@ssbm.ch*

cybersecurity and resource management, strongly effects the resilience and integrity of interrelated industries and partners [15].

According to current United States survey statistics, almost 41% of SMEs have been the victim of a cyberattack in recent years. The average reported ransom payment among those impacted was $16,000. Remarkably, after paying the ransom, only roughly 50% of SMEs were able to fully restore their data. Additionally, following the initial incident, 27% of these organizations were having repeat attacks, and an equal percentage experienced further ransom requests. SMEs were forced to conduct significant system rebuilds as part of their recovery efforts in almost half of the situations [28].

The authors will explain how the BDSLCCI framework can assist with the mapping of customized controls within the CMMC 2.0 model in the following parts and their corresponding subsections.

2. SMB Barriers: Cost, Capacity, and Irrelevance to Business Goals

SMBs frequently have limited financial resources, which makes it difficult for them to hire specialized IT security staff or invest in complete cybersecurity solutions. Employee exposure to cyber threats, including phishing and other social engineering assaults, is made worse by a widespread lack of understanding and formal training. Additionally, the continued reliance on outdated hardware and software systems renders many SMBs vulnerable to exploitation through unpatched security flaws. From a regulatory standpoint, SMBs are required to navigate increasingly complex legal frameworks and ensure compliance with data protection regulations - an undertaking that proves challenging in the absence of robust cybersecurity infrastructure and expertise [28, 31]. Previous research investigations have identified a number of challenges that SMBs face while putting in place efficient cybersecurity measures. The most urgent issues, according to a few recent studies, are a general lack of specialized cybersecurity expertise, obstacles in managing complicated regulatory compliance requirements, and limited financial resources to attract and retain highly qualified individuals [1, 12, 13, 17, 18, 19, 20, 21, 22].

The 2018 State of Cybersecurity in SMBs survey states that handling cyber hazards presents a number of ongoing difficulties for SMBs. The few obstacles that have been identified include: (i) a lack of in-house expertise to effectively mitigate cybersecurity threats; (ii) limited IT budgets that limit the implementation of strong security measures; (iii) a general lack of awareness and understanding regarding appropriate cyber-attack prevention strategies; (iv) the rapid pace of technological advancement, which frequently delays SMBs' ability to adapt; (v) an overwhelming and often contradictory volume of cybersecurity-related information; and (vi) a lack of continuing commitment to upholding cybersecurity practices [24].

SMBs have a variety of operational and capacity-related difficulties in strengthening their cybersecurity posture, in addition to budgetary limitations. These include inadequate support for change management procedures, a lack of system integration knowledge, restricted access to advanced consulting services, and inadequate staff training in cybersecurity fundamentals. Furthermore, a lot of SMBs have trouble finding and using freely available resources, and they frequently have trouble implementing scalable, user-friendly security tools [4].

3. Federal Contract Information (FCI) And Controlled Unclassified Information (CUI)

Information produced by the United States government or created by a contractor while carrying out a federal contract that is not meant for public distribution is referred to as Federal Contract Information (FCI). According to 48 Code of Federal Regulation (CFR) 52.204-21, FCI does not include routine administrative information like payment processing records or publicly accessible data. Rather, it usually consists of technical specifications, timelines for projects, internal communications, and other confidential contractual data. FCI nevertheless needs a minimum level of protection to avoid unwanted access or disclosure, even if it is not as sensitive as Controlled Unclassified Information (CUI). The Federal Acquisition Regulation (FAR) clause 52.204-21, which requires the deployment of 15 fundamental cybersecurity measures, outlines the protecting criteria for FCI. The Cybersecurity Maturity Model Certification (CMMC) 2.0 framework's Level 1 is based on these controls. Access control, physical security, and incident response procedures are among the minimal standards that contractors managing FCI must make sure their staff and systems follow. In addition to preserving contractual eligibility, adherence to these rules is crucial for upholding the secrecy and integrity of government procurement procedures [26].

The long-standing disparity in the way U.S. federal agencies handled sensitive but unclassified data led to the introduction of the idea of CUI. Agencies employed confusing names like "For Official Use Only (FOUO)" and "Sensitive But Unclassified (SBU)" prior to the creation of the CUI program, which resulted in inconsistent protection requirements. As a result, Executive Order 13556 required the development of a single framework to ensure that such data is handled, marked, and protected uniformly throughout the federal organization.

CUI includes a wide range of data that must be protected because of legal, regulatory, or policy-based requirements even though it is not covered by Executive Order 13526 or the Atomic Energy Act. Examples include documents that are sensitive to law enforcement, export-controlled technical information, confidential corporate data, and personally identifiable information (PII). Preventing illegal access, misuse, or disclosure that might jeopardize public trust, national security, or privacy is the aim.

32 CFR Part 2002, which describes the duties of federal agencies in identifying, marking, disseminating, and decontrolling CUI, governs the operation of the CUI program. DoD Instruction 5200.48, which offers operational guidelines for handling CUI in defense contexts, goes into additional depth about this framework inside the Department of Defense (DoD). DFARS clauses 252.204-7008 and 252.204-7012, which require the reporting of cybersecurity incidents and the preservation of CUI in non-federal systems, also impose compliance requirements on defense contractors.

The National Institute of Standards and Technology (NIST) has created a series of publications to support these requirements, such as SP 800-171 for safeguarding CUI in non-federal systems, SP 800-172 for improved security in critical programs, and SP 800-53 for more general federal information systems. In order to ensure the confidentiality, integrity, and availability of CUI, these

standards specify technical, administrative, and physical measures that organizations must put in place.

The U.S. government's approach to information protection has fundamentally changed as a result of the CUI initiative. The effort improves collaboration between agencies and national security by standardizing divergent procedures and bringing them into compliance with contemporary cybersecurity requirements. Understanding and following CUI regulations is not only a matter of compliance but also a strategic necessity for protecting sensitive information assets for firms that operate inside or alongside the federal ecosystem [2, 25].

4. Overview of CMMC 2.0: Structure and Intent

A systematic framework called the Cybersecurity Capability Maturity Model (C2M2) was created to direct the use and administration of cybersecurity procedures in information technology (IT), operational technology (OT), and related information assets. It helps businesses to prioritize cybersecurity investments, discuss best practices, benchmark and assess their maturity levels, and improve their cybersecurity capabilities. C2M2 was created under the Electricity Subsector Cybersecurity Risk Management Maturity Initiative, a White House-led initiative involving the DOE, Department of Homeland Security (DHS), and stakeholders from both the public and private sectors. It was first published by the U.S. Department of Energy (DOE) in 2012 and revised in 2014. The program promoted public-private cooperation by utilizing the National Infrastructure Protection Plan framework.

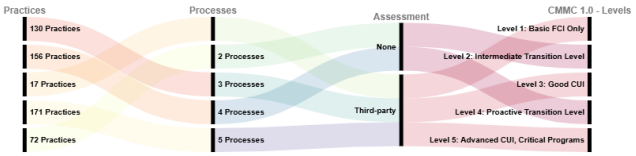

Fig. 1. CMMC 1.0 Levels – Practices, Processes, and Assessment Type.

Complementing this, the Cybersecurity Maturity Model Certification (CMMC) is a Department of Defense (DoD) effort targeted at bolstering cyber resilience across the Defense Industrial Base (DIB). As shown in Figure 1, the CMMC 1.0 version is illustrated. This strategy establishes uniform evaluation criteria and integrates cybersecurity compliance into the procurement procedures of the U.S. DoD. Figure 2 illustrates the current version, CMMC 2.0, which was announced in November 2021 and is principally grounded in NIST SP 800-171, with NIST SP 800-172 applicable to select programs. The Department of Defense (DoD) promotes early adoption of CMMC while it is undergoing rulemaking under the Federal Acquisition Regulation (FAR) and Defense Federal Acquisition Regulation Supplement (DFARS).

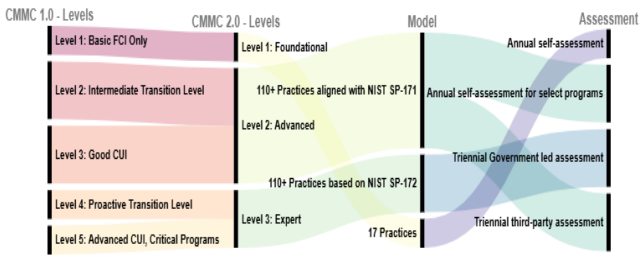

Fig. 2. CMMC 2.0 Levels Migrated from CMMC 1.0 - Model and Assessment Type.

There are three developmental levels in CMMC 2.0:

Level 1 (Foundational): Contains 17 fundamental procedures with an emphasis on protecting Federal Contract Information (FCI). Every year, contractors are required to self-attest; third-party evaluations are not permitted.

Level 2 (Advanced): Protects Controlled Unclassified Information (CUI) by implementing all 110 controls from NIST SP 800-171. Depending on the terms of the contract, certification may be necessary or self-attested. It is carried out by qualified third-party assessors.

Level 3 (Expert): Protects CUI with implications for national security by using further controls from NIST SP 800-172. Government representatives perform assessments, and Level 2 certification is a requirement.

DIB contractors must abide by the current DFARS rules, even if CMMC has long been optional:

(i) DFARS 252.204-7012: It has been in place since 2017 and requires the creation of a System Security Plan (SSP) and a Plan of Actions and Milestones (POAM), as well as self-evaluation per NIST SP 800-171.

(ii) DFARS 252.204-7019/7020: These clauses, which were introduced in 2020, mandate that the SSP and POAM be scored using a DoD methodology and that the findings be sent to the Supplier Performance Risk System (SPRS). Evaluations can be carried out independently or by the DIB Cybersecurity Assessment Center (DIBCAC).

Stricter deadlines for closing POAM items (within 180 days), the introduction of minimum passing scores, the formal role of CMMC Third-Party Assessment Organization (C3PAO) for Level 2 and government-led assessments for Level 3 are some of the main differences between DFARS and CMMC [16].

By 2024, the U.S. The Department of Defense confirmed its intention to enforce the related cybersecurity standards by the end of 2025 by finalizing regulatory modifications that legally codified the Cybersecurity Maturity Model Certification (CMMC) 2.0 into federal law. According to the official document, the final rule amending the Defense Federal Acquisition Regulation Supplement (DFARS) was expected to go into effect on November 10, 2025, and it was published in the Federal Register for public inspection on September 9, 2025.

This release represents the end of a multi-year effort to apply improved cybersecurity criteria under the CMMC program for defense contractors, as described below.

(i) On November 10, 2025, this regulatory amendment took effect, initiating Phase-1 of a planned three-year rollout plan for CMMC adoption. In order to prove compliance with CMMC Level 1 and Level 2 requirements, contractors must perform self-assessments during Phase-1.

(ii) Third-party certification of Level 2 compliance through approved C3PAOs will be required for Phase-2, which is set to start in November 2026.

(iii) Phase-3, which will begin in November 2027, will implement Level 3 regulations, which call for companies handling the Department's most sensitive data to obtain official certification from the DIBCAC [7].

The "NIST SP 800-171" standards are mapped in detail to the "CMMC 1.0" and "CMMC 2.0" frameworks in Appendix A [8, 32].

5. Audit Risks and Oversight Gaps in CMMC Implementation

Numerous dangers and inadequacies related to CMMC have been recognized and reported in numerous research papers since its debut. The dependence on vendor self-evaluations raises significant problems, especially in the field of cybersecurity, according to recent research. There may be gaps in risk assessment and assurance if vendors fail to regularly report the full scope or efficacy of their security controls [14].

Systemic problems could occur in the absence of a strong and well-regulated authorization structure for third-party evaluation firms. The Department of Defense may unintentionally award contracts to vendors whose security controls are inadequate for safeguarding CUI and other sensitive data if these entities lack the requisite credentials or rigor to conduct cybersecurity evaluations. Such oversights expose national security interests to preventable vulnerabilities and jeopardize the integrity of the CMMC 2.0 framework [6, 10].

Because of its quite complicated compliance architecture and frequent updates, the CMMC has had little acceptance. Depending on the size and operational complexity of the company, implementation expenses for firms aiming for Level 2 certification are projected to be between $100,000 and $250,000 [27, 33]. Adoption obstacles still exist, especially for SMBs. The development of mechanisms for sustained compliance, careful preparation for formal evaluations, and the nuanced interpretation and integration of level-specific standards are just a few of the issues associated with implementing CMMC 2.0. Smaller organizations may have resource limitations that make implementation difficult. Additionally, since cybersecurity standards and regulatory requirements continue to change, all firms need to be alert and flexible [30, 34, 35]. The integrity of the supply chain is at danger because prime contractors could have to replace non-compliant SMBs, which could impede access to specialized capabilities. Furthermore, contractors may face legal repercussions under the False Claims Act if they misrepresent their cybersecurity posture. Despite these difficulties, the Department of barrier (DoD) views CMMC as a vital barrier against sensitive intellectual property exfiltration and a pillar for protecting the defense industrial base [3, 5].

According to the research survey published by Redspin on CMMC 2.0 problems, defense contractors' readiness and governance are seriously lacking. Important conclusions show that 57% have not finished a gap analysis against NIST SP 800-171 standards, 56% have not implemented the required end-to-end encryption, and 62% lack sufficient governance controls for certification. Furthermore, 36% and 31% of respondents list financial constraints and technical complexity as obstacles, respectively, and 44% do not have continuous monitoring in place. These results support a balanced approach to security investments and governance maturity by highlighting the necessity of improved governance, encryption, and compliance to properly meet CMMC 2.0 objectives [36].

With more than half of respondents concentrating just on obtaining a self-assessment score, there is a large CMMC readiness gap. Many strive for CMMC Level 2 accreditation, which requires 110 practices to be evaluated by third parties. 50% of respondents say they are only Moderately, Slightly, or Not at All Prepared, while 16.3% claim minimum or no readiness. Furthermore, 13% have not made any preparations [36].

Subcontractors are not the only ones who are concerned about costs when it comes to CMMC preparation and certification; prime or dual-role businesses were cited by 52% of respondents as their primary obstacle. Interestingly, 35% of these respondents say they have not spent any money or less than 1% of their budgets on CMMC preparedness [36].

According to 75% of respondents, their mandatory cyber defenses are outlined in a System Security Plan (SSP), which is mandated by the CMMC. Despite a requirement in the Defense Federal Acquisition Regulations (DFARS) 252.204-7012 for contractors handling CUI since late 2017, just 47% of contractors have completed their System Security Plan (SSP). Furthermore, 54% of respondents continue to self-evaluate, suggesting that military industrial base security might be improved by third-party validation of CMMC by a C3PAO [36].

Organizations are not making enough progress in upholding and modernizing their compliance procedures. There is a considerable delay in maintaining and upgrading efforts, despite the fact that many have begun compliance activities. Due to out-of-date plans, two-thirds of people who have a SSP only update it once a year, increasing vulnerability. Furthermore, only 58% have a Plan of Action & Milestones (POA&M), and even fewer update it frequently, indicating significant deficiencies in the management of persistent security threats [36].

Only 23.5% of surveyed respondents had an actively monitored mechanism to flow down CMMC requirements to all subcontractors handling FCI or CUI, making the supply chain susceptible. In addition to not meeting CMMC requirements, this gap keeps supply chain vulnerabilities active [36].

Partnerships with service providers are important, as evidenced by the fact that more than half of respondents had worked with an External Service Provider (ESP). 57% of organizations seeking certification (OSCs), who presently use an ESP want to stick with their current compliance practices after obtaining CMMC accreditation. Furthermore, 18% plan to recruit an ESP for the first time, demonstrating the firms' perceived worth in relation to the Supplier Performance Risk System (SPRS) scores rather than merely keeping CMMC accreditation [36].

In summary, the complex architecture needed for control implementation, relatively high compliance costs, and the lack of a well-regulated ecosystem of accredited assessment organizations to support consistent and accessible certification are just a few of the difficulties SMBs face when implementing the CMMC.

6. Introducing the BDSLCCI Framework: Principles and Architecture

The term "Mission Critical Asset" (MCA) in the Business Domain-Specific Least Cybersecurity Controls Implementation (BDSLCCI) framework refers to any digital or physical resource whose compromise could result in a major disruption of critical business operations, non-compliance with regulations, or a decline in stakeholder trust. MCAs include a variety of assets, such as customer-facing platforms, operational control systems,

proprietary databases, and documents pertaining to compliance. A contextualized approach to cybersecurity control implementation is required because the identification and prioritization of MCAs are intrinsically based on the particular business area of the firm.

As shown in Figure 3, by giving cybersecurity measures that support the fundamental values of confidentiality, integrity, and availability (CIA) top priority, BDSLCCI highlights the protection of MCAs. However, depending on the operational situation and the type of MCA, each CIA component has a different proportional value. For instance, a Computer Numeric Control (CNC) machine may be categorized as an MCA in a small or medium-sized business (SMB) focused on manufacturing. Availability is crucial in this situation since a cyberattack that interferes with CNC operations could stop production and result in significant operational and financial losses.

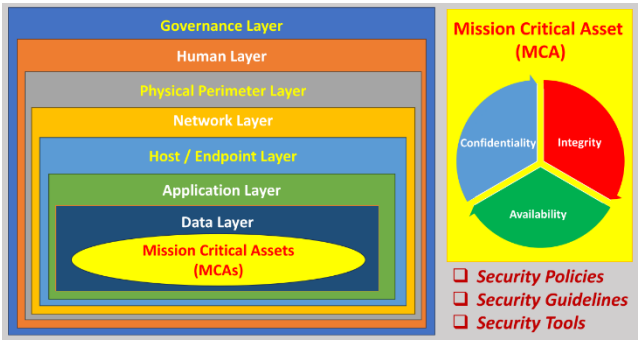

Fig. 3. BDSLCCI Defense in Depth (DiD) and Mission Critical Asset (MCA) Security Layers.

As a result, later stages of the BDSLCCI deployment deal with controls pertaining to the integrity and confidentiality of the CNC system.

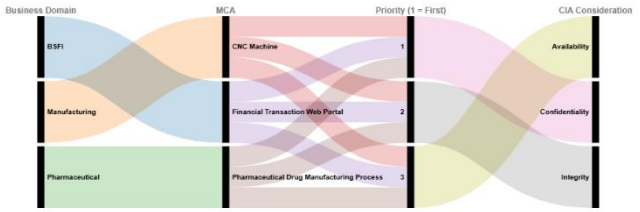

Fig. 4. BDSLCCI MCA Mapping with Prioritized Consideration of CIA.

On the other hand, financial transactions and related systems - usually administered via online portals or mobile applications - make up MCAs in a banking-focused SMB. Given the sensitivity of financial data and the legal ramifications of data breaches, confidentiality is of utmost importance in this situation. Although availability and integrity are still crucial, the major goal of the control strategy is to stop illegal access and data leaks. The stability of computerized systems is crucial in the pharmaceutical industry since SMBs may depend on them to manufacture medications. A breach that modifies the specifications of medicinal components could put customers' health at grave danger. Because of the strategic importance of these assets, integrity-focused controls are put in place as a first line of defense, followed by further layers of security. Refer Figure 4 for the diagrammatic representation of MCA's mappings with CIA traid prioritization.

BDSLCCI uses a Defense in Depth (DiD) approach to enable organization-wide cybersecurity maturity and ensure comprehensive defense of MCAs. This method combines several levels of security measures from the administrative, technical, and physical domains. Data security, application security, host or endpoint security, network security, physical perimeter security, human security, and overall governance represent the sequential hierarchy of control layers that make up the DiD architecture. Because of this tiered setup, threats can be detected, prevented, or mitigated even in the case that one control fails. The level-wise mapping of the DiD strategy within the BDSLCCI framework to the associated minimal number of suggested cybersecurity controls is shown in Figure 5.

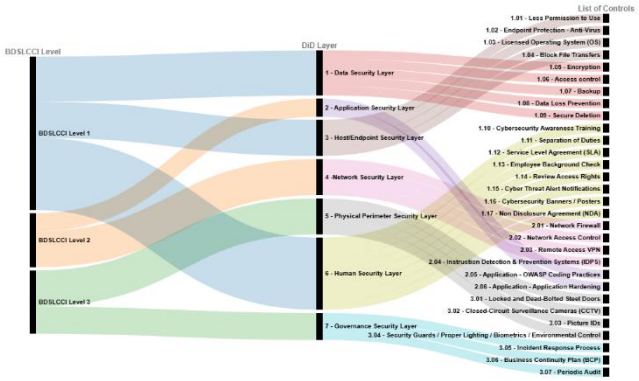

Fig. 5. BDSLCCI Defense in Depth (DiD) Levels and Controls Mapping.

BDSLCCI promotes organizational resilience, lowers single points of failure, and permits scalable cybersecurity implementation across various business contexts by matching asset criticality with customized control layers. SMBs and industry-specific ecosystems, where resource limitations frequently call for a practical and risk-based approach to cybersecurity, will especially benefit from this.

Additionally, an end-to-end web-based platform that enables the full lifecycle - from gap analysis to accreditation - will be used to operationalize BDSLCCI. The BDSLCCI framework greatly reduces implementation time and effort by providing customizable policies, guidelines, and template documentation that are intended to function as ready-to-use tools. By lowering the total cost, consultancy overhead, and time needed for cybersecurity adoption, this digital implementation seeks to make strong security practices more affordable and long-lasting for businesses of all sizes and industries.

7. Comparative Mapping: CMMC 2.0 Vs BDSLCCI

The primary goal of both the BDSLCCI framework and CMMC 2.0 is to meet the cybersecurity needs of small and medium-sized businesses (SMBs) by providing scalable and context-sensitive controls that are customized to their operating contexts.

As shown in Figure 6 and explained in Annexure A, which provides a mapping of NIST SP 800-171 requirements to CMMC 2.0 and the corresponding BDSLCCI control domains, the BDSLCCI framework effectively covers a significant portion of the controls required by CMMC 2.0, even though it advocates for a minimal set of cybersecurity controls.

Significantly, the BDSLCCI framework uses DiD controls that show either substantial or partial alignment across many mapped control areas and views information as a critical asset. Additional rules that are especially suggested for SMBs can cover a number of CMMC 2.0 standards. The following referenced components - ARCSIK Matrix (501), Password Guidelines (502), Asset Tracker

(503), Cloud Computing Security Guidelines (504), Data Center Security Guidelines (505), Digital Media Transport Guidelines (506), IT Usage and Cybersecurity Policy (507), and Additional Guidelines Needed (508) - provide additional clarification, as shown in the mapping shown in Figure 6. As shown in the accompanying graphic, these elements fall under the BDSLCCI Control Areas.

Figure 6 also illustrates that the degree of association among certain domains varies significantly. In this research, "limited coverage" refers to less than sixty percent, "partial coverage" to more than sixty percent, and "maximum coverage" to ninety percent or greater alignment. In general, the BDSLCCI DiD controls can meet around seventy-five to eighty percent of the CMMC 2.0 control requirements.

Further, additional controls that consider FCI and CUI as separate mission-critical assets might be incorporated to meet CMMC 2.0 standards. Dedicated confidentiality, integrity, and availability (CIA) controls would then oversee these assets, creating a thorough bridge to satisfy the entire range of CMMC 2.0 standards. To achieve alignment with the control objectives of CMMC 2.0, another feasible solution is to improve the DiD strategy itself, either by adding new security layers or by upgrading current mechanisms with extra policies and standards.

8. Conclusion: Toward Scalable and Inclusive Cybersecurity Compliance

In conclusion, obtaining CMMC 2.0 compliance can be benefited by the BDSLCCI architecture.

Additionally, by extending its usefulness to other vital corporate assets, it promotes organizational growth and resilience by putting strong cybersecurity procedures into place.

The correlation between the BDSLCCI cybersecurity framework and the CMMC 2.0 compliance standards is shown in Figure 7. The BDSLCCI framework takes a business-centric approach that is adapted to the mission-critical assets and operational realities of SMBs.

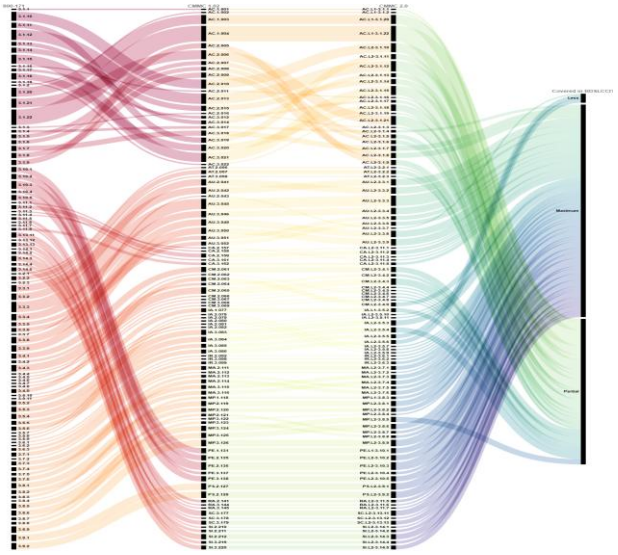

Fig. 6. BDSLCCI Controls Mapping with CMMC 2.0.

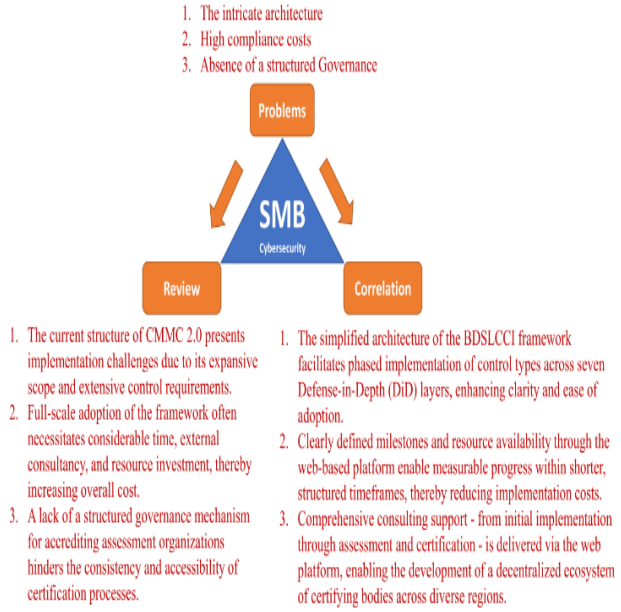

Fig. 7. The Correlation of BDSLCCI in Cybersecurity Deployment Strategies for CMMC 2.0.

It simplifies the entire cybersecurity implementation, evaluation, and certification process and is backed by a sophisticated web-based platform. SMBs can more easily and affordably achieve significant alignment with most CMMC 2.0 control standards with this integrated strategy.

Acknowledgements

Not applicable.

Author contributions

Shekhar Pawar: Conceptualization, Methodology, Software, Field study, Data curation, Writing-Original draft preparation, Software, Validation, Visualization, Investigation Hemant Palivela: Writing-Reviewing and Editing.

Conflicts of interest

The authors declare no conflicts of interest.

Appendix A

The table below presents the mapping between "NIST SP 800-171" requirements, "CMMC 1.0", and "CMMC 2.0" [8, 32].

Table 1. Control areas mapping between "NIST SP 800-171" requirements, "CMMC 1.0", and "CMMC 2.0".

The table below presents the mapping between "NIST SP 800-171" requirements, "CMMC 1.0", and "CMMC 2.0".

Table 1. Control areas mapping between "NIST SP 800-171" requirements, "CMMC 1.0", and "CMMC 2.0".

800-171	*800-171 Requirement as Recommended Policy*	*CMMC 1.02*	*CMMC 2.0*
3.1.1	Make sure that system resources are only accessible by authenticated users, their assigned processes, and trusted devices.	AC.1.001	AC.L1-3.1.1
3.1.2	According to each authorized user's role and privilege level, system access must be limited to the particular transactions and functions that are given to them.	AC.1.002	AC.L1-3.1.2
3.1.3	Documented and approved authorizations will carefully regulate the flow of CUI, ensuring that transmission, access, and dissemination comply with established control standards.	AC.2.016	AC.L2-3.1.3
3.1.4	Assign diverse roles to individuals in a manner that minimizes the opportunity for malevolent activities, ensuring that no single person has control over all important functions without monitoring or collaboration.	AC.3.017	AC.L2-3.1.4
3.1.5	In accordance with the least privilege concept, make sure that each user, regardless of position or clearance level, only has the minimal access required to complete their assigned responsibilities.	AC.2.007	AC.L2-3.1.5
3.1.6	In order to minimize needless exposure to elevated permissions and lower the danger of privilege misuse, access to non-security-related system functions must be made through non-privileged accounts or roles.	AC.2.008	AC.L2-3.1.6
3.1.7	Keep thorough audit records to aid in oversight and forensic analysis, and restrict the use of privileged operations to authorized users.	AC.3.018	AC.L2-3.1.7
3.1.8	To improve access security and stop brute-force exploitation, implement measures to limit the number of consecutive unsuccessful authentication attempts.	AC.2.009	AC.L2-3.1.8

800-171	*800-171 Requirement as Recommended Policy*	*CMMC 1.02*	*CMMC 2.0*
3.1.9	Ensure that any displayed privacy and security notices meet with relevant CUI standards, clearly expressing user obligations and data management processes.	AC.2.005	AC.L2-3.1.9
3.1.10	After a predetermined amount of user idleness, turn on session lock mechanisms with pattern-obscuring displays to automatically limit access and hide sensitive info.	AC.2.010	AC.L2-3.1.10
3.1.11	Configure systems to automatically terminate user sessions upon the occurrence of predefined conditions - such as periods of inactivity, session time limits, or completion of specific transactions to mitigate unauthorized access risks.	AC.3.019	AC.L2-3.1.11
3.1.12	Create systems to actively monitor and control remote access sessions, making sure that all connections are secure, authorized, and under constant supervision.	AC.2.013	AC.L2-3.1.12
3.1.13	To safeguard remote access connections and stop unwanted data exposure during transmission, use verified encryption standards.	AC.3.014	AC.L2-3.1.13
3.1.14	To enable centralized monitoring, enforce access regulations, and safeguard system entrance, all remote connections should only be routed via approved access control mechanisms.	AC.2.015	AC.L2-3.1.14
3.1.15	Make sure that only competent individuals are allowed to remotely execute high-risk instructions and retrieve vital security data after formal authorization and strict access control procedures.	AC.3.021	AC.L2-3.1.15
3.1.16	Before establishing connectivity, all access points and devices must adhere to defined security regulations. Wireless connections will only be allowed with express consent.	AC.2.011	AC.L2-3.1.16
3.1.17	To avoid unwanted access and data breach, all wireless interfaces and communications must be protected using robust authentication techniques and authorized encryption algorithms.	AC.3.012	AC.L2-3.1.17
3.1.18	Employ validated controls to limit mobile device access to enterprise systems, making sure that only authorized and compliant endpoints are connected to the network.	AC.3.020	AC.L2-3.1.18
3.1.19	In order to maintain confidentiality and fulfill legal requirements, make sure that all CUI sent to or stored on mobile devices is secured using acceptable encryption technologies.	AC.3.022	AC.L2-3.1.19
3.1.20	To regulate connections to external systems and ensure that access and usage are restricted to allowed reasons and adhere to corporate security policies, establish verification methods and implement controls.	AC.1.003	AC.L1-3.1.20
3.1.21	To protect sensitive data and adhere to established security rules, the use of portable storage devices on external platforms must be strictly regulated.	AC.2.006	AC.L2-3.1.21
3.1.22	Establish stringent controls to regulate the posting and processing of CUI on systems that are available to the public, making sure that such actions are specifically permitted, tracked, and compatible with relevant data protection laws.	AC.1.004	AC.L1-3.1.22
3.2.1	Educate system administrators and users on the formal procedures in place to protect organizational systems and the security consequences of their actions.	AT.2.056	AT.L2-3.2.1
3.2.2	Make certain that employees receive pertinent and sufficient cybersecurity training that is in line with their responsibilities, company policies, and legal compliance requirements.	AT.2.057	AT.L2-3.2.2
3.2.3	In compliance with established risk mitigation and response policies, make sure staff members receive focused training on identifying and reporting any insider threats.	AT.3.058	AT.L2-3.2.3
3.3.1	Establish procedures for creating and maintaining audit trails that provide post-event diagnostics, real-time oversight, and regulatory reporting of security breaches.	AU.2.042	AU.L2-3.3.1
3.3.2	Ensure that each system interaction is recorded in a way that clearly associates activities with the accountable user.	AU.2.041	AU.L2-3.3.2
3.3.3	Ensure that audit log configurations reflect changing risk profiles and compliance requirements by reviewing them on a regular basis.	AU.3.045	AU.L2-3.3.3
3.3.4	Establish automated warning systems to inform security staff of any interruptions or malfunctions in the creation of audit logs, ensuring ongoing visibility and prompt incident response.	AU.3.046	AU.L2-3.3.4
3.3.5	Ensure that forensic investigations and organizational response procedures are supported by audit review, analytical insights, and reporting outputs.	AU.3.051	AU.L2-3.3.5
3.3.6	To support forensic investigations and incident response, make sure that audit review, analytical insights, and reporting outputs are methodically connected.	AU.3.052	AU.L2-3.3.6
3.3.7	To provide consistent timestamp accuracy across systems for efficient audit record creation and incident analysis, implement time synchronization methods (such as NTP).	AU.2.043	AU.L2-3.3.7

3.3.8	Protect audit logs and logging tools from manipulation, illegal access, and data loss by putting in place administrative and technical safeguards. This will enable trustworthy security monitoring and forensic analysis.	AU.3.049	AU.L2-3.3.8
3.3.9	Reduce the possibility of illegal changes by enforcing role-based access controls, which ensure that only authorized privileged users can manage or modify audit logging setups.	AU.3.050	AU.L2-3.3.9
3.4.1	As security controls and operational requirements change, make sure that all organizational systems are cataloged and that baseline settings are recorded and updated on a regular basis.	CM.2.061	CM.L2-3.4.1
3.4.2	All deployed IT solutions must have standardized security settings that minimize exposure to threats and are in line with organizational baselines.	CM.2.064	CM.L2-3.4.2
3.4.3	To ensure accountability and compliance with organizational change management rules, all system modifications must go through documented review, approval, and logging procedures.	CM.2.065	CM.L2-3.4.3
3.4.4	Do a formal security impact analysis before making system changes to make that possible risks are evaluated and dealt with in compliance with organizational risk management and change governance frameworks.	CM.2.066	CM.L2-3.4.4
3.4.5	Create and uphold documented access control policies that restrict system modification rights to specific persons, ensuring compliance with security governance and change management regulations.	CM.3.067	CM.L2-3.4.5

800-171	*800-171 Requirement as Recommended Policy*	*CMMC 1.02*	*CMMC 2.0*
3.4.6	In compliance with authorized baseline configurations, make sure that all deployed systems are hardened by turning on just those features specifically needed for business and security functions.	CM.2.062	CM.L2-3.4.6
3.4.7	To reduce system exposure and maintain the least functionality concept across organizational contexts, restrict or disable any non-essential programs, functions, ports, protocols, and services.	CM.3.068	CM.L2-3.4.7
3.4.8	Use a permit-by-exception or deny-by-default policy to manage software execution and make sure that only programs that have been specifically approved are allowed to operate on company systems. This method considerably lowers the possibility of harmful or unauthorized code execution.	CM.3.069	CM.L2-3.4.8
3.4.9	In order to ensure adherence to allowed settings and prevent unauthorized or potentially dangerous applications from jeopardizing system integrity, establish controls to monitor, restrict, and manage user-installed software on organizational systems.	CM.2.063	CM.L2-3.4.9
3.5.2	Ensure that only trusted entities can interact with protected resources by requiring authentication or verification of user, process, and device identities before allowing access to organizational systems.	IA.1.077	IA.L1-3.5.2
3.5.3	Enforce multifactor authentication (MFA) for non-privileged accounts during network access and for all privileged accounts during local and network access. This reduces the possibility of unwanted system access and ensures more robust identity verification.	IA.3.083	IA.L2-3.5.3
3.5.4	Use replay-resistant authentication methods to prevent unauthorized parties from intercepting, replaying, or reusing credentials during authentication attempts for both privileged and non-privileged accounts on the network.	IA.3.084	IA.L2-3.5.4
3.5.5	To reduce the risks of identity ambiguity, illegal access, and audit trail manipulation, implement restrictions that forbid the reuse of user, device, or process IDs within a specified retention period.	IA.3.085	IA.L2-3.5.5
3.5.6	To prevent unwanted access and maintain the integrity of organizational environments, configure systems to automatically deactivate user, device, or process identifiers after a predetermined amount of inactivity.	IA.3.086	IA.L2-3.5.6
3.5.7	To improve resistance against brute-force and dictionary-based attacks and strengthen secure authentication procedures, mandate minimum password complexity criteria and demand character variation during password formation.	IA.2.078	IA.L2-3.5.7
3.5.8	To stop credential recycling and bolster protections against unwanted access attempts, prohibit password reuse across a predetermined number of prior iterations.	IA.2.079	IA.L2-3.5.8
3.5.9	Permit temporary passwords for first system logons, but require that they be changed right away to a permanent, policy-compliant credential after the first use. This ensures strong identity verification and safe onboarding.	IA.2.080	IA.L2-3.5.9

3.5.10	To secure credentials from unwanted access, interception, and alteration, make sure that all passwords are stored and sent using cryptographic protection measures that adhere to accepted security standards.	IA.2.081	IA.L2-3.5.10
3.5.11	By ensuring that system answers do not disclose information about authentication success, failure causes, or credential validity, obscure authentication feedback helps reduce the risk of enumeration and brute-force attacks.	IA.2.082	IA.L2-3.5.11
3.6.1	To ensure prompt and efficient mitigation of cybersecurity threats across organizational systems, establish and maintain an incident-handling capability that includes preparation, detection, analysis, containment, recovery, and user response.	IR.2.092	IR.L2-3.6.1
3.6.2	To ensure accountability, regulatory compliance, and coordinated incident response, promptly and systematically track, document, and escalate security incidents to appropriate external authorities and designated internal stakeholders.	IR.3.098	IR.L2-3.6.2
3.6.3	To verify readiness, find weaknesses, and ensure efficient implementation of detection, containment, recovery, and communication protocols during cybersecurity incidents, test the organization's incident response capability on a regular basis.	IR.3.099	IR.L2-3.6.3
3.7.1	Maintain organizational systems on a regular and approved basis while following established protocols and access control criteria to ensure operational integrity, security compliance, and peak performance.	MA.2.111	MA.L2-3.7.1
3.7.2	Establish stringent controls over the equipment, methods, procedures, and staff members permitted to do system maintenance, making sure that all operations are safe, auditable, and in line with company guidelines and risk management goals.	MA.2.112	MA.L2-3.7.2
3.7.3	Prior to removal, make sure that any equipment assigned for off-site maintenance has been thoroughly sanitized to remove CUI, strictly adhering to organizational security rules and approved data sanitization processes.	MA.3.115	MA.L2-3.7.3
3.7.4	Make sure that only validated and secure tools are brought into the operational environment by scanning all media containing diagnostic and test programs for harmful code prior to deployment on organizational systems.	MA.3.116	MA.L2-3.7.4
3.7.5	To prevent unwanted remote access and preserve system integrity, mandate multifactor authentication (MFA) for starting nonlocal maintenance sessions over external network connections and enforce prompt disconnection following conclusion of such activities.	MA.2.113	MA.L2-3.7.5
3.7.6	In order to protect sensitive systems and data during maintenance operations and to enforce responsibility, make sure that individuals doing maintenance tasks without the necessary access authorizations are directly supervised.	MA.2.114	MA.L2-3.7.6
3.8.1	In accordance with company data protection standards, make sure that any system media containing CUI - in both paper and digital formats - are physically controlled and stored securely to prevent unauthorized access, loss, or compromise.	MP.2.119	MP.L2-3.8.1
800-171	***800-171 Requirement as Recommended Policy***	***CMMC 1.02***	***CMMC 2.0***
3.8.2	Ensure that only authorized workers handle sensitive data in accordance with organizational access control procedures by restricting access to CUI stored on system media to those who have been vetted.	MP.2.120	MP.L2-3.8.2
3.8.3	Sanitize or destroy system media containing CUI using approved techniques that ensure total data eradication and prohibit unauthorized recovery or disclosure before disposing of or reusing it.	MP.1.118	MP.L1-3.8.3
3.8.4	To ensure correct handling, access control, and distribution, label any system media containing CUI with the proper CUI markings and any applicable distribution constraints in compliance with organizational and legal requirements.	MP.3.122	MP.L2-3.8.4
3.8.5	Strictly restrict authorized personnel's access to media containing CUI, and use systematic tracking, comprehensive documentation, and safe handling procedures to impose strict accountability throughout transportation outside of regulated locations.	MP.3.124	MP.L2-3.8.5
3.8.6	Unless equivalent protection is offered by authorized physical security measures, use cryptographic safeguards to ensure the confidentiality of CUI held on digital media during transportation.	MP.3.125	MP.L2-3.8.6
3.8.7	In accordance with corporate security policies and risk mitigation strategies, implement controls to limit the usage of removable media on system components, ensuring that only authorized devices and users can access or transfer data via such media.	MP.2.121	MP.L2-3.8.7

3.8.8	To avoid unauthorized data access, minimize malware exposure, and uphold organizational data security requirements, prohibit the usage of portable storage devices without a clearly recognized and authorized owner.	MP.3.123	MP.L2-3.8.8
3.8.9	By putting together suitable encryption, imposing access controls, and establishing physical security measures in accordance with corporate data protection rules, organization may secure the confidentiality of backup media holding CUI across all storage sites.	MP.3.126	MP.L2-3.8.9
3.9.1	Before granting access to organizational systems that include CUI, thoroughly screen individuals to make sure that only verified and reliable employees are given access in compliance with established security clearance and risk management procedures.	PS.2.127	PS.L2-3.9.1
3.9.2	Revoke access as soon as possible, retrieve any CUI-bearing assets, and update access control records to prevent unlawful data exposure in order to protect CUI during personnel activities like terminations and transfers.	PS.2.128	PS.L2-3.9.2
3.10.1	To avoid unwanted intrusion and safeguard vital assets, strictly restrict physical access to organizational systems, equipment, and operational environments to those who are permitted. Use access control techniques including identity verification, surveillance, and secure entry points.	PE.1.131	PE.L1-3.10.1
3.10.2	To ensure operational integrity, identify abnormalities, and stop unwanted entry or interruption, establish protective controls and ongoing monitoring for the physical facilities and supporting infrastructure - such as power, cooling, and environmental systems - that house organizational systems.	PE.2.135	PE.L2-3.10.2
3.10.3	While keeping thorough visitor logs and upholding established physical security procedures, escort all guests into the organization's facilities and continuously monitor their activities to prevent access to unapproved places or information.	PE.2.136	PE.L2-3.10.3
3.10.4	To assist accountability, incident investigation, and compliance verification, keep thorough audit logs of physical access to organizational buildings and systems. These logs should include entrance and exit events, personnel names, timestamps, and access points.	PE.3.137	PE.L2-3.10.4
3.10.5	Maintain inventories, use logs, and tamper detection systems to enable accountability and incident response. Control and manage physical access devices, including as locks, keycards, and biometric scanners, to ensure that only authorized people can enter secure areas.	PE.3.138	PE.L2-3.10.5
3.11.1	Assess the efficacy of security controls put in place in organizational systems on a regular basis to find weaknesses and make sure they are in line with operational needs, risk tolerance, and legal requirements. When required, take corrective action and record findings.	CA.2.158	CA.L2-3.11.1
3.11.2	Create and carry out workable plans to address found flaws and reduce organizational system vulnerabilities. To ensure ongoing progress and regulatory compliance, every plan must specify the most important remedial tasks, designate accountable staff, establish deadlines, and include verification procedures.	CA.2.159	CA.L2-3.11.2
3.11.3	Maintain compliance and proactive risk mitigation by continuously evaluating and monitoring the security measures implemented throughout corporate systems to confirm their continued efficacy, spot deviations or failures, and enable quick remedy.	CA.3.161	CA.L2-3.11.3
3.11.4	System Security Plans (SSPs) that precisely define system boundaries, operational environments, applied security measures, and linkages or dependencies with other systems should be created, maintained, and updated on a regular basis. These plans must support ongoing risk management and compliance initiatives, appropriately reflect current configurations, and go through planned evaluations.	CA.2.157	CA.L2-3.11.4
3.11.5	To determine how organizational system operations - including the processing, storing, or transmission of CUI - affect mission functions, organizational assets, personnel, and the organization's image or reputation, conduct regular risk assessments. In order to inform mitigation methods and ensure robust operations, assessments must identify threats, vulnerabilities, and potential repercussions.	RA.2.141	RA.L2-3.11.5
3.11.6	Conduct routine vulnerability scans on company systems and apps, and start scans right away if new or emerging threats are found. Make sure that vulnerabilities are evaluated, prioritized, and fixed in conformance with the organization's risk management strategy.	RA.3.144	RA.L2-3.11.6
3.11.7	To ensure successful risk reduction and ongoing regulatory compliance, address vulnerabilities found in organizational systems based on formal risk assessment results. Prioritize corrective activities based on potential impact, exploitability, and mission-criticality.	RA.3.145	RA.L2-3.11.7

800-171	***800-171 Requirement as Recommended Policy***	***CMMC 1.02***	***CMMC 2.0***

3.11.8	To improve the organization's overall security posture, create and maintain open lines of communication with outside security service providers. Coordinate on issues like threat intelligence, incident response, vulnerability management, and compliance assistance.	CA.3.162	CA.L2-3.11.8
3.13.11	Implement cryptographic methods to protect CUI's confidentiality while it's in transit and at rest. Encryption standards should be in line with organizational risk tolerance and legal requirements to avoid unwanted access or disclosure.	SC.3.177	SC.L2-3.13.11
3.13.12	Implement and maintain Domain Name System (DNS) filtering services to limit access to known harmful, unauthorized, or non-compliant domains - thereby lowering risks linked to phishing, malware, and data exfiltration. Update filtering policies frequently in light of new business needs including threat intelligence.	SC.3.178	SC.L2-3.13.12
3.13.13	Use email authentication tools like SPF (Sender Policy Framework), DKIM (DomainKeys Identified Mail), and DMARC (Domain-based Message Authentication, Reporting & Conformance) to verify email sources, stop spoofing, and maintain the reliability and integrity of company communications. To handle changing threat landscapes, keep an eye on these setups and make necessary updates.	SC.3.179	SC.L2-3.13.13
3.14.1	Establish protocols for quickly locating, reporting, and fixing information and system defects in all organizational settings. Maintain system integrity and regulatory compliance by ensuring prompt detection through automated tools, staff reporting, and audits; documenting all findings; and putting corrective measures into place in order of severity and risk effect.	SI.2.210	SI.L2-3.14.1
3.14.2	Install and maintain anti-malware, antivirus, and endpoint detection software at key points in organizational systems, such as email gateways, servers, network boundaries, and endpoints. For real-time threat detection, quarantine, and remediation, make sure these tools are often updated and monitored.	SI.2.211	SI.L2-3.14.2
3.14.3	To reduce identified risks and maintain system resilience and regulatory compliance, keep an eye out for system security warnings and advisories from reliable internal and external sources. Then, take prompt action, such as patching, configuration updates, or incident response.	SI.2.212	SI.L2-3.14.3
3.14.4	When new releases, signature definitions, or patches become available, make sure that all malicious code protection mechanisms - such as antivirus, anti-malware, and endpoint detection systems - are updated on time. To maintain the best security against changing threats, automate updates wherever possible and confirm successful deployment.	SI.3.219	SI.L2-3.14.4
3.14.5	Enforce real-time scanning of files from external sources, including downloads, email attachments, and removable media, at the point of access, including during download, opening, or execution. Conduct regular vulnerability and malicious code scans across organizational systems. Make sure scanning tools are appropriately configured and updated on a regular basis so they can react quickly to new threats.	SI.3.220	SI.L2-3.14.5

References

[1] A. Asti, Cyber defense challenges from the small and medium sized business perspective, GIAC Certi cations, SANS Inst., 2017, p. 16, Art. no. 38160. [Online], Available: https://www.giac.org/researchpapers/38160/

[2] Chief Information Officer U.S. Department of War. "CMMC Resources & Documentation." Defense.gov, 2021, dodcio.defense.gov/cmmc/Resources-Documentation/.

[3] Cummings, Jarret. "CMMC Program Rule Finalized." Proquest.com, 11 Dec. 2024, www.proquest.com/docview/3225403625.

[4] De Queiroz, H., Malka, S.C. and Sahoo, S., 2025. Small Business and Cybersecurity Readiness: Unpacking Action Driven Framework and Model. Available at SSRN 5381511.

[5] DefenseScoop. "Pentagon Begins Enforcing CMMC Compliance, but Readiness Gaps Remain." DefenseScoop, 10 Nov. 2025, defensescoop.com/2025/11/10/cmmc-compliance-dod-enforcement-defense-industry-readiness-gaps/.

[6] Department of Defense Office of Inspector General. "Press Release: Audit of the DoD's Process for Authorizing Third Party Organizations to Per." DODIG, Department of Defense Office of Inspector General, 14 Jan. 2025, www.dodig.mil/In-the-Spotlight/Article/4028197/press-release-audit-of-the-dods-process-for-authorizing-third-party-organizatio/. Accessed 25 Oct. 2025.

[7] Department of Defense. Defense Federal Acquisition Regulation Supplement: Assessing Contractor Implementation of Cybersecurity Requirements (DFARS Case 2019–D041). 10 Sept. 2025, public-inspection.federalregister.gov/2025-17359.pdf.

[8] DoD CIO. Cybersecurity Maturity Model Certification (CMMC) Model Overview. Sept. 2024, dodcio.defense.gov/Portals/0/Documents/CMMC/ModelOverview.pdf.

[9] Garba, A.A., Siraj, M.M. and Othman, S.H., 2020. An explanatory review on cybersecurity capability maturity models. Adv. sci. technol. eng. syst. j, 5(4), pp.762-769.

[10] Igboko, U.A., 2025. Investigating The Factors and Impact of Cybercrime on Small-To Medium-Sized Business (SMBs): Analysing risks, factors, and solutions.

[11] Kaur, J., Kumar, S., Narkhede, B.E., Dabić, M., Rathore, A.P.S. and Joshi, R., 2024. Barriers to blockchain adoption for supply chain finance: the case of Indian SMEs: J. Kaur et al. Electronic Commerce Research, 24(1), pp.303-340.

[12] Kezron, I.E., 2024. A cybersecurity resilience framework for underserved rural SMEs in critical infrastructure supply chains: Strengthening operational continuity and threat response in digitally vulnerable sectors. World Journal of Advanced Research and Reviews, 24(3), pp.3464-3477.

[13] Kezron, I.E., 2024. Cybersecurity strategies for resource constrained SMEs and health providers. Iconic Research And Engineering Journals, 8(5), pp.1215-1224.

[14] Latsiou, Aikaterina C., et al. "Never Trust - Always Verify: Assessing the Cybersecurity Trustworthiness of Suppliers in the Digital Supply Chain." Procedia Computer Science, vol. 254, 5 Mar. 2025, pp. 98–107, www.sciencedirect.com/science/article/pii/S1877050925004181, https://doi.org/10.1016/j.procs.2025.02.068.

[15] Lee, C. S., & Wang, Y. (2022). Typology of Cybercrime Victimization in Europe: A Multilevel Latent Class Analysis. Crime & Delinquency, 70(4), 1196-1223. https://doi.org/10.1177/00111287221118880 (Original work published 2024).

[16] Office of Small Business Programs, Department of Defense. "CMMC 2.0 Details and Links to Key Resources." Business.defense.gov, 10 Sept. 2025, business.defense.gov/Programs/Cyber-Security-Resources/CMMC-20/.

[17] Abhishake Reddy Onteddu. (2021). AI and Deep Learning-Based Intelligent Drug Recommendation System for Patient Health Monitoring in IoT-Enabled Healthcare. Journal of Informatics Education and Research, 1(3).

[18] Pawar, S. and Palivela, H. (2025). NEED OF PARADIGM SHIFT IN CYBERSECURITY IMPLEMENTATION FOR SMALL AND MEDIUM ENTERPRISES (SMES). International Journal of Cybersecurity Intelligence & Cybercrime, [online] 8(1). doi:https://doi.org/10.52306/2578-3289.1184.

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

[20] 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.

[21] 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.

[22] Pawar, Shekhar, 2025, How BDSLCCI can Help SMEs to Achieve Data Protection Compliance, Such as EU GDPR and the DPDP Act of India, INTERNATIONAL JOURNAL OF ENGINEERING RESEARCH & TECHNOLOGY (IJERT) Volume 14, Issue 03 (March 2025). https://www.ijert.org/how-bdslcci-can-help-smes-to-achieve-data-protection-compliance-such-as-eu-gdpr-and-the-dpdp-act-of-india

[23] Pawar, Shekhar, and Dr. Hemant Palivela. "LCCI: A Framework for Least Cybersecurity Controls to Be Implemented for Small and Medium Enterprises (SMEs)." International Journal of Information Management Data Insights, vol. 2, no. 1, 1 Apr. 2022, p. 100080, www.sciencedirect.com/science/article/pii/S2667096822000234, https://doi.org/10.1016/j.jjimei.2022.100080.

[24] Pfeifer, M.R., 2021. IT security in SMEs—Threats and Chances for Supply Chains. J. Supply Chain. Cust. Relatsh. Manag, 2021, pp.1-8.

[25] Ponemon-Institute. (2018). State of Cybersecurity in Small & Medium Sized Businesses (SMB). [Online]. Available: https://www.keepersecurity.com/assets/pdf/Keeper-2018-Ponemon-Report.pdf

[26] Ross, R., Pillitteri, V. and Dempsey, K., 2022. Assessing enhanced security requirements for controlled unclassified information. NIST Special Publication, 800, p.172A.

[27] Strohmier, H., Stoker, G., Vanajakumari, M., Clark, U., Cummings, J. and Modaresnezhad, M., 2022. Cybersecurity maturity model certification initial impact on the defense industrial base. Journal of Information Systems Applied Research, 15(2), pp.17-29.

[28] Sundar, A., 2025. Adapting Cybersecurity Maturity Models for Online Startups and Small Businesses https://ajosr.org/wp-content/uploads/journal/published_paper/volume-3/issue-4/ajsr2025_sDMFWp5x.pdf.

[29] Tetteh, A.K., 2024. Cybersecurity needs for SMEs. Issues in Information Systems, 25(1).

[30] U.S. Small Business Administration. (2024). United States Small Business Administration, Office of Advocacy, Frequently Asked Questions. 2024. https://cdn.advocacy.sba.gov/wpcontent/uploads/2019/09/24154243/Frequently-Asked-Questions-Small-Business-2019-12.pdf.

[31] Wang, W., Sadjadi, S.M. and Rishe, N., 2024, May. A survey of major cybersecurity compliance frameworks. In 2024 IEEE 10th Conference on Big Data Security on Cloud (BigDataSecurity) (pp. 23-34). IEEE.

[32] Wong, L.W., Lee, V.H., Tan, G.W.H., Ooi, K.B. and Sohal, A., 2022. The role of cybersecurity and policy awareness in shifting employee compliance attitudes: Building supply chain capabilities. International Journal of Information Management, 66, p.102520.

[33] Ross R, Pillitteri V (2024) Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) NIST SP 800-171r3. https://doi.org/10.6028/NIST.SP.800-171r3.

[34] Wishart-Smith, Heather. "Cybersecurity Compliance: The Costs, Risks and Race to Certification." Forbes, 7 July 2025, www.forbes.com/sites/heatherwishartsmith/2025/07/07/cybersecurity-compliance-the-costs-risks-and-race-to-certification/.

[35] Sfoglia, P. (2023) 'CMMC 2.0:A Well-intentioned Misstep in Cybersecurity', National Defense, 108(837), 16+, available: https://link.gale.com/apps/doc/A762556446/AONE.

[36] Barnir N, Gandal N, Moore T, Scott V (2025;), "A cost–benefit approach to optimizing security precaution adoption". Information and Computer Security, Vol. ahead-of-print No. ahead-of-print. https://doi.org/10.1108/ICS-07-2024-0156.

[36] Redspin . "Aware but Not Prepared CMMC Research." Redspin, 14 Nov. 2025, redspin.com/aware-but-not-prepared-cmmc-research-report/.