PCI DSS IMPLEMENTATION GUIDELINES FOR SMALL AND MEDIUM ENTERPRISES USING COBIT BASED IMPLEMENTATION APPROACH

Rajmeet Kaur

Research Project

Submitted to the Faculty of Graduate Studies

Concordia University of Edmonton

in Partial Fulfillment of

Requirements for the Final

Research Project for the Degree

Master of Information Systems Assurance Management

Concordia University of Edmonton

FACULTY OF GRADUATE STUDIES

Edmonton, Alberta

December 2020

PCI DSS IMPLEMENTATION GUIDELINES FOR SMALL AND MEDIUM ENTERPRISES USING COBIT BASED IMPLEMENTATION APPROACH

Rajmeet Kaur

Approved:

Bobby Swar [Original Approval on File]

Bobby Swar Date: December 14, 2020

Primary Supervisor

Edgar Schmidt [Original Approval on File]

Edgar Schmidt, DSocSci Date: December 16, 2020

Dean, Faculty of Graduate Studies

Abstract

PCI DSS is a data security standard for companies that process, transmit, or store cardholder data to protect cardholder's data against data theft and fraud. Companies must comply with PCI DSS requirements to maintain a secure environment while dealing, accepting, or processing credit or debit cards. The main benefit of PCI DSS implementation is protecting cardholder's data, preventing data breaches, and building customer trust. Organizations find the implementation of PCI DSS a time-consuming and costly process. Small and Medium Enterprises (SMEs) lack resources in comparison to large organizations. Non-compliance can result in such heavy fines, penalties, customer, and reputational loss, leading to the business closing. PCI DSS non-compliance also results in a lack of security measures for critical information and data protection. This paper identifies SME's challenges to implement and comply with PCI DSS as a data security standard. This paper proposes PCI DSS implementation guidelines for SMEs using the COBIT based implementation approach based on the identified challenges. Guidelines are introduced in seven phases of the COBIT 2019 implementation guide.

Keywords: PCI DSS, PCI DSS implementation, PCI DSS compliance, small & medium enterprises, PCI DSS implementation and compliance challenges, COBIT based implementation approach, PCI DSS implementation guidelines

Table of Contents

List of Tables

Table

List of figures

Figures

Introduction

Payment Card Industry Data Security Standard (PCI DSS) is a data security standard provided by the Payment Card Industry Security Standards Council (PCI SSC) for every organization dealing or taking card payments. PCI SSC mandates every organization accepting, storing, processing, or transmitting card payments or data to comply with PCI DSS (Chuvakin & Williams, 2010). Aligning business to PCI DSS controls aids in enhancing protection around payment card data operations, which improves an organization's ability to maintain confidentiality and integrity of cardholder data (Seaman, 2020).

PCI DSS helps organizations mitigate data breach events resulting in reputational, financial, and customer losses (Seaman, 2020). PCI DSS Compliance also saves the business from heavy fines and penalties in case of a data breach. As a data security standard, it helps to safeguard the digital identity of customers, clients, and related parties. Businesses can gain the trust of their customers by assuring commitment to protect cardholder data. Gaining trust results in increasing business profits by building customer relations (Seaman, 2020). PCI DSS aids organizations to face IT challenges like attacks, outdated software, or viruses.

PCI DSS non-compliance results in data breach events, heavy fines, penalties, and other associated costs. Data breach costs can vary from thousands to millions of dollars. Card reissue costs can be $2 - $5 or more per card affected in a data breach that needs to be reissued (Seaman, 2020). Seaman (2020) mentioned that the average number of cards affected in a data breach is typically in the thousands for small businesses and hundreds to millions for larger businesses. Non-compliance costs includes $500 - $1,000 per month

for organizations, resulting amount of $60,000 – $120,000 annually (Seaman, 2020). Other associated costs include fraud detection services costs and fraud monitoring programs and technologies (Seaman, 2020).

Organizations face some PCI DSS implementation and compliance challenges to enjoy benefits offered by PCI DSS. PCI DSS is a mandatory standard, which requires the implementation of all the requirements to become a PCI DSS compliant. Boese IV (2020) argues that PCI DSS requirements are time-consuming and expensive due to their technical nature. Businesses need to hire specialized staff and equipment to work on technical aspects, including firewalls, encryption for data in transit and at rest, tokenization, implementing access controls for PCI DSS compliance (Boese IV, 2020).

As per the 2019 Data breach incident report, a total of 41,686 security incidents and 2,013 data breaches were recorded worldwide, out of which 43% of victims are small and medium businesses (Verizon, 2019a). The organizations that faced data breaches were not complying with all 12 requirements of PCI DSS (Verizon, 2019b). Implementing PCI DSS is challenging for Small and Medium Enterprises (SMEs) due to limited resources (Boese IV, 2020). SMEs lack resources in terms of money, human resources, knowledge, staff, and equipment to implement PCI DSS, which draws cyber criminal's attraction. On the contrary, PCI DSS non-compliance necessitates organizations to face heavy fines & penalties, reputational and business loss.

Other researchers also provided guidelines for PCI DSS compliance by diverging PCI DSS with different information security standards and frameworks such as ISO/IEC 27001 and COBIT, ITIL, and ISO 27002 as general solutions for every organization. This research paper identified the need to propose PCI DSS implementation guidelines

considering challenges faced by SMEs. This research paper identifies problems faced by SMEs in PCI DSS implementation and compliance through literature review. Based on identified problems, the paper offers guidelines for PCI DSS implementation for SMEs using the COBIT based implementation approach.

The research paper begins with the introduction section, which includes research objectives explaining PCI DSS, its benefits, implementation challenges, and non-compliance consequences. The next section is the literature review. It has PCI DSS and its background, COBIT 2019 implementation guide introduction, and related works, including Data breach cases and PCI DSS compliance challenges faced by SMEs. The methodology is the third section of the research paper. It highlights research objectives, scope, limitations, questions addressed, and methods employed to develop implementation guidelines. The fourth section is a crucial section of this paper: the presentation and discussion of results. Results are the PCI DSS implementation guidelines developed for SMEs using the COBIT implementation approach. This research paper presents PCI DSS implementation guidelines by mapping challenges faced by SMEs with affected PCI DSS requirements. The last section is about the paper's conclusions and suggested future research for SMEs related to PCI DSS implementation.

Literature Review

Recent Data Breaches

Cybercriminals can breach any organization's data effortlessly in the absence of proper security measures. Criminals can use many methods like phishing, malware, and spoofing to access other person's data. Cybercriminals have the main motive of financial

gain. Nanda, Popat, and Vimalkumar (2018) studied some high-profile data breaches involving credit cards. Data breached companies include Home Depot, Michaels, Global Payment, Target, Goodwill, Staples, and Adobe Systems. Paper found that among every seven breaches, five breaches happened due to vulnerable Point-of-Sale systems. Researchers emphasized the importance of two-factor authentication, strong and complex passwords.

GoAnywhere (2017) highlighted three organizations that suffered the loss due to PCI non-compliance. The report emphasized the need to take PCI DSS compliance seriously to avoid any shocking consequences. At the time of the breach, None of the three organizations was fully compliant with PCI DSS. Organizations had achieved full compliance once but were not able to sustain it. Three high-profile data breaches are:

Home Depot. It is one of the worst data breaches in the retail industry, as hackers successfully compromised 56 million credit cards. The reason behind the data breach is malware-infected point-of-sale devices. “In Home Depot’s case, investing in security software with the ability to audit security infrastructure for PCI DSS compliance, may have been the difference between a $19.5 million data breach settlement, and business as usual” (GoAnywhere, 2017).

Office of Personnel Management, US. Hackers were able to steal 4.2 million personal files of employees, including former and current employees, and background investigation information for security clearance. The reason behind this data breach was the lack of two-factor authentication to access sensitive data for employees. The article emphasized that encrypting and protecting files during transfer is not enough; organizations need to monitor internal actors (GoAnywhere, 2017).

TJX Companies. GoAnywhere stated that the TJX company faced a data breach due to PCI DSS non-compliance. The cybercriminals stole more than 80 GB of cardholder data over 18 months. Before the company could identify and stop the violation, attackers had already stolen 45.6 million records. Court filings say that TJX was not complying with 9 out of 12 requirements of PCI DSS. Reasons that contributed to this data breach are wireless network, network segmentation failure, and prohibited data storage (GoAnywhere, 2017).

SMEs Data Breaches. SMEs means businesses that maintain their revenues, employees, and assets below a defined threshold. Each country has a different threshold for SMEs. This proposal document focuses on the Canadian threshold for SMEs, which is 1 to 99 employees of small businesses and 100 to 499 for medium-sized enterprises (Government of Canada, 2019).

Ydstie (2015) mentioned three SMEs cyberattacks, which resulted in the loss of thousands to millions. Wright Hotels lost about over $ 1 million when cybercriminals stole their bank funds through a hacked email account. The attackers gained access to the owner's outlook calendar, which helped them plan money transactions while he was busy in meetings. Outlook calendar access offered the attackers enough time to stole money and deleted all communications without leaving evidence (Ydstie, 2015). PATCO Construction lost $588,000 in a cyberattack. The attacker successfully employed trojan in the company's systems, which granted access to online banking credentials. The attacker stole money in just seven days (Ydstie, 2015). In another data breach event, the attacker stole the card number and emptied the bank account of the owner of Volunteer Voyages.

Volunteer Voyages SME lost over $14,000 through fraudulent withdrawals from the business account (Ydstie, 2015).

These data breaches point out imperatively that no organization can escape PCI DSS compliance. Organizations should consider PCI DSS implementation and compliance maintenance seriously to avoid any destructive outcomes (GoAnywhere, 2017).

PCI-DSS

PCI DSS is a data security standard provided by the PCI SSC for securing and protecting cardholder's data. Every organization accepting, dealing, processing cards needs to comply with this standard to safeguard data from criminal minds (Payment Card Industry Security Standards Card [PCI SSC], 2018). PCI DSS provides 12 operational and technical requirements to all organizations that store, transmit, and process cardholder data (PCI SSC, 2018). Unlike Federal or Provincial laws, this standard is not a regulatory or statutory requirement in any state or country (Chuvakin & Williams, 2010). It is still a standard mandated by PCI SSC for merchants to protect cardholders's data and identity. Data breaches result in heavy fines and penalties in case of non-compliance.

PCI DSS classifies critical information and data into two parts i.e., Cardholder Data (Primary Account Number [PAN]), Expiration Date, Service Code) and Sensitive Authentication Data {Magnetic Stripe data or chip or equivalent}, (Customer Verification Value [CVV])/(Card Identification Number[CID])/ (Card Authentication Value[CAV]), (Personal Identification Number [PIN])} (PCI SSC, 2018).

PCI SSC developed PCI DSS as a data security standard for protecting cardholder data in 2004. Major card brands, including American Express, Visa, MasterCard, JCB

International, and Discover Financial Services, collaborated to form an administrative council named PCI SSC, which maintains, updates, and promotes PCI DSS (Rahaman, Wang, & Yao, 2019).

The PCI council's responsibility is to evaluate organizations based on standard benchmarks as compliant and & certification. PCI SSC assesses organizations through two different methods, SAQ or QSA, based on the number of transactions annually processed (Olajide, Zavarsky, Ruhl, & Lindskog, 2015). Organizations need to implement all requirements and report to the council depending on merchant levels annually. PCI DSS implementation is not a one-time process; merchants need to maintain their PCI compliant status every year and regularly. For small merchants, the Self-assessment Questionnaire (SAQ) is recommended as a questionnaire checklist of conditions with yes or no to submit a PCI DSS report on compliance (PCI SSC, 2018).

Table 1

Merchant Levels based on annual transactions (Olajide, Zavarsky, Ruhl, & Lindskog, 2015)

Merchant Level	Number of transactions (annually)
Level 1	6 million
Level 2	1-6 million
Level 3	20,000-1 million
Level 4	Less than 20,000

Table 1 highlights the different merchant levels provided by PCI SSC based on the number of transactions annually involved by an organization. PCI SSC assesses merchants to charge fines and penalties monthly for non-compliance based on merchant levels. These fines can vary from $5,000 to 100,000 per month, depending on the number of months of non-compliance (Miteva, 2017). Non-compliance with PCI DSS can affect organizations in different ways, such as:

1) Reputational damage
2) Money and revenue Loss
3) Data breaches
4) Fines and Penalties
5) Legal Action (Miteva, 2017).

If an organization experiences a data breach while being compliant with the standard, it must still pay fines and penalties. Fines and penalties are not just for organizations that are not complying with all PCI requirements. Fines and penalties are imposed on those parties as well, who are assessed as PCI compliant but had any data breach or data theft. Table 2 highlights PCI objectives and requirements required to implement and set by PCI SSC to validate an organization's PCI compliant status. All requirements are distributed into six different control objectives of PCI DSS. Organizations need to fulfill all six objectives to implement as a data security standard. Control objectives are focused on protecting and securing cardholder data from cyber criminals (PCI DSS, 2018).

Table 2

PCI-DSS Compliance requirements (PCI SSC, 2018)

Requirement number	Control Objective	Requirement Description
Requirement 1	Build and Maintain a Secure Network and Systems	Install and maintain a firewall configuration to protect cardholder data
Requirement 2	Build and Maintain a Secure Network and Systems	Do not use vendor-supplied defaults for system passwords and other security parameters
Requirement 3	Protect Cardholder Data	Protect stored cardholder data
Requirement 4	Protect Cardholder Data	Encrypted cardholder data while transmission across open, public networks
Requirement 5	Maintain a Vulnerability Management Program	Protect all systems against malware and regularly update anti-virus software or programs
Requirement 6	Implement Strong Access Control Measures	Develop and maintain secure systems and applications
Requirement 7	Implement Strong Access Control Measures	Restrict access to cardholder data by business need-to-know
Requirement 8	Implement Strong Access Control Measures	Identify and authenticate access to system components
Requirement 9	Monitor and Test Networks regularly	Restrict physical access to cardholder data
Requirement 10	Monitor and Test Networks regularly	Track and monitor all access to network resources and cardholder data

Requirement number	Control Objective	Requirement Description
Requirement 11	Maintain an Information Security Policy	Regularly test security systems and processes
Requirement 12	Maintain an Information Security Policy	Maintain a policy that addresses information security for all personnel

PCI DSS Implementation and Compliance Challenges

Rees (2010) outlines some organization's challenges in implementing PCI DSS as a standard and maintaining compliance status, as all requirements are mandatory and technical. Thus, the standard is not simple for businesses to understand and implement as a simple operation of the company. Standard scoping has a different meaning for different organizations. For example, project managers define scoping as what to do and how to deliver the project (Rees, 2010). Nanda, Popat, & Vimalkumar (2018) listed some challenges that organizations face to be PCI compliant are expensive, strict guidelines, confusing scope, and casual treatment. The paper recognized that SMEs have few resources, so it is expensive to complete all necessary activities to achieve compliance Nanda, Popat, & Vimalkumar, 2018). On the other hand, fines and penalties are too high amounts. Another major challenge identified in this paper is that the organization believes that they need to accept only those parts of PCI DSS with which their companies are concerned (Nanda, Popat & Vimalkumar, 2018).

Fernande (2015) focused on requirements that organizations find the most challenging to implement. Requirement 10 of PCI DSS requires organizations to track and monitor all access to network resources and cardholder data. Requirement 11.5

requires testing security systems and processes regularly (Fernande, 2015). Verizon (2019b) provides data about the rate of PCI fully compliant organizations, which decreased in the last three years (2016-2018). The global compliance rate fell to 36.7% in 2018 as compared to 2016 was 55.4%. Verizon (2019b) stated that requirement six has the most extensive compliance drop by organizations because they find it difficult to maintain effective vulnerability management. Most organizations had difficulty meeting requirement 10 - reconstruct events by implementing proper audit trails (Verizon, 2019b).

PCI DSS implementation and compliance challenges faced by SMEs

According to Verizon (2018a), out of a total of 41,686 security incidents and 2,013 data breaches, 43% of victims are SMEs. The reason behind these cybersecurity events is non-compliance (inability to sustain) with all the PCI DSS requirements (Verizon, 2019b). Rees (2012) stated in a study about small firms that if a firm, whether small or large, accept card payments from clients just a few or millions, they need to comply with PCI DSS. There are no differences in PCI DSS compliance procedures for large companies or small companies (Rees, 2012). Achieving PCI compliance for SMEs is difficult for organizations and is affected by awareness, normative beliefs, peer-behaviour, self-efficacy, value, and compliance costs (Clapper & Richmond, 2016). Boese IV (2020) highlighted the constraints of small and medium merchants due to a lack of adequate resources as large organizations. Due to its technical nature, the small business found PCI DSS implementation a time-consuming and costly process. These organizations need to hire specialized staff and equipment to meet standard benchmarks and become PCI compliant (Boese IV, 2020). These challenges increase the likelihood and cost of a data breach higher for SMEs, and this cost can range from fees lawsuits to

fines and penalties and can turn results in business closing. The primary reason merchants fail PCI SSC audit is the failure to safeguard cardholder data (Boese IV, 2020).

SMEs lack the required security measures to protect their data and critical information from evil eyes. The bookkeeping and accounting processes of enterprises are mostly manually or obsolete, making business houses more vulnerable both inside and outside and increases the risks of losing data and information (Lingor & Ruesch, 2020. Eva Velasquez, president of Identity Theft Center, said 1,244 data breaches were reported last year (2018); however, most of these breaches targeted small businesses (Rafter, 2019). She emphasized that data breaches at smaller firms are ubiquitous, but most do not hit the headlines due to insufficient resources. SMEs need to be careful when handling customer information and must take the necessary steps to protect themselves (Rafter, 2019).

Friedman (2020) highlighted a cyber attack event in Forbes of '*Barbara Corcoran,*' the real estate guru, and ABC's Shark Tank's co-star lost almost $400,000 in an email phishing scam. The fraudsters misled her bookkeeper by sending a bill that appeared from her assistant (Friedman, 2020). Ydstie (2015) mentioned three SMEs cyberattacks, which resulted in the loss of thousands to millions. Wright Hotels lost about over $ 1 million when cybercriminals stole their bank funds through a hacked email account. The attackers accessed the owner's outlook calendar to make money transactions while he was engaged in meetings and deleted all communications, which could track ongoing transactions. PATCO Construction lost $588,000 in a cyberattack when the attacker successfully employed trojan in the company's systems to access online banking credentials (Ydstie, 2015). In another data breach event, the attacker stole the card

number and emptied the bank account of the owner of Volunteer Voyages. Volunteer Voyages SME lost over $14,000 through fraudulent withdrawals from the business account (Ydstie, 2015). All these email and banking related data breach events point out poor management and flawed communication in SMEs related to critical data.

Related works by Other Researchers

Yulianto, Lim & Soewito (2016) developed an Information Security Model for PCI DSS (ISSM-PCI) in their paper. This paper comprises four maturity levels- 1) None, 2) Initial, 3) Basic, and 4) Capable. The ISMM-PCI mapped PCI DSS and ISO/IEC 27001 by using both qualitative and quantitative analysis. The focus of this model is to enhance the quality of people, process, and technology. Yulianto, Lim & Soewito (2016) describe the model's importance by assisting organizations in identifying critical success factors and gaps quickly. This model focuses on choosing the best security controls to improve information security management and protect information assets while achieving PCI DSS compliance status. The main benefit of ISMM-PCI, as compared to other ISMMs, is its ease of use. Researchers affirm that organizations can use the ISSM-PCI model, regardless of its size (Yulianto, Lim & Soewito, 2016).

Nicho & Fakhry (2011) identified a requirement for integrating PCI controls into other information security standards and frameworks to increase security levels. This paper developed an integrated security governance framework for implementing PCI DSS by incorporating Control Objectives for Information and related Technology (COBIT), Information Technology Infrastructure Library (ITIL), and ISO 27002. The Paper focused on an integrated governance framework that will help merchants comply

with PCI DSS effectively and ensure audit and control (Nicho & Fakhry, 2011). Integrating PCI DSS with other information system standards and frameworks provides an additional security level rather than isolated PCI DSS. Paper established a need to map the COBIT controls with PCI DSS to guide practitioners and academics (Nicho & Fakhry, 2011).

PCI SSC mandated for every merchant or business, taking cards from their clients and customers, to implement and comply with PCI DSS requirements. PCI SSC provided some helpful resources for SMEs on its website under the title "Resources for Small Merchants." This resource is an educational resource, including knowledge about guide to safe payments and payment systems. It does not guide how to ease PCI DSS implementation as a small merchant (Official PCI Security Standards Council Site, n.d.).

This paper focuses on specific challenges faced by SMEs associated with PCI DSS implementation and maintaining compliance status. Some challenges are shared between two or more requirements from the literature review, whereas some are specific to a particular requirement. PCI DSS is a complex standard, including strict guidelines. PCI DSS scoping is confusing for smaller organizations due to the different nature and size (Rees, 2010). Verizon (2019b) states that most SMEs face data breach events because they cannot sustain all PCI DSS requirements compliance. Clapper & Richmond (2016) highlighted some reasons that cause difficulty for smaller businesses to be PCI compliant, including lack of awareness, peer-behaviour, self-efficacy, and compliance cost. Boese IV (2020) reflected several problems faced by SMEs to become PCI compliant. PCI DSS is a technical standard, so it is a time-consuming process to implement and comply with PCI DSS regularly for SMEs. SMEs lack resources

compared to large organizations that result in an expensive matter to implement and maintain PCI DSS regularly. Non-compliance can result in such heavy fines and penalties that could lead to business closing for SMEs (Boese IV, 2020). Friedman (2020) and Ydstie (2015) highlighted data breach events that point out some challenges faced by SMEs in implementing PCI DSS. These challenges include lack of proper security measures, adequate access controls, two-factor authentications, poor management and flawed communication to protect critical data.

COBIT 2019 Implementation Guide

COBIT 2019 is a framework provided by ISACA for IT governance and management. This framework considers IT's role in the enterprise's sustainability and growth and emphasizes risk mitigation in the digital world (ISACA, 2018a). Enterprise Governance of Information and Technology (EGIT) is a fundamental part of the board's corporate governance. EGIT is flexible and can be implemented in any organization, regardless of size. Board members govern processes and mechanisms that aid organizations in aligning business and IT for value creation. COBIT 2019 specified three outcomes after adopting EGIT, including benefits realization, risk optimization, and resource optimization (COBIT, 2018a). COBIT framework differentiates between governance and management. Governance is the board's responsibility, whereas management is the responsibility of executive management (Information Systems Audit and Control Association [ISACA], 2018a).

COBIT 2019 Implementation guide focuses on enterprise-wide IT governance. This guide identifies IT as ubiquitous in the enterprise. Separating IT from business

activities is neither possible nor good practice. Governance and IT management should be implemented as a vital part of enterprise governance (ISACA, 2018a). COBIT implementation approach can be used for easing the PCI DSS implementation process. PCI DSS itself is a technical standard that needs to be implemented as part of organizational processes. There are seven phases of the COBIT implementation approach as under:

1) What are the drivers? – Phase 1 of the implementation approach identifies drivers that create a desire to change at the executive level. Drivers can be internal or external events, conditions, or issues that serve as stimuli for change (ISACA, 2018b).
2) Where are we now? – Phase 2 aligns IT objectives with business strategies and risks. IT prioritizes the most critical goals, alignment goals, and processes of an enterprise. Based on prioritized factors, management can know the business's current capabilities and deficiencies (ISACA, 2018b).
3) Where do we want to be? – Phase 3 sets a target for improvement. Gap analysis identifies potential solutions, some of them can be easy to implement, and others can be challenging (ISACA, 2018b).
4) What needs to be done? - Phase 4 helps plant feasible and practical solutions that define projects supported by justifiably been business cases and a change plan for implementation (ISACA, 2018b).
5) How do we get there? – Phase 5 provides the implementation of proposed solutions through daily practices and establishing measures and monitoring

systems to ensure achievement of business alignment and performance can be measured (ISACA, 2018b).

6) Did we get there? – Phase 6 focuses on the sustainable transition of improved governance and management practices into everyday business operations (ISACA, 2018b).
7) How do we keep the momentum going? - Phase 7 identifies governance and management requirements to assess overall initiative success and reinforces the continual improvement need. It also prioritized additional opportunities to improve the governance system (ISACA, 2018b).

Implementing EGIT improvements is a step by step process to ensure that initiative is governed and adequately guided and supported by management. Major IT Projects fail due to a lack of proper management direction, support, and oversight (ISACA, 2018b). The first step towards EGIT implementation is to create an appropriate environment. A suitable environment should be created and maintained to ensure that EGIT is implemented as an integral part of the enterprise's overall governance approach. The objective is to develop sufficient commitment, direction, and control of activities to align with enterprise objectives and ensure appropriate implementation support from the board and executive management (ISACA, 2018b).

The next step is to apply a continuous improvement lifecycle approach. This approach allows the enterprise to address the complexity and challenges typically faced during EGIT implementation. There are three interrelated components to the life cycle, including:

1) Program Management,

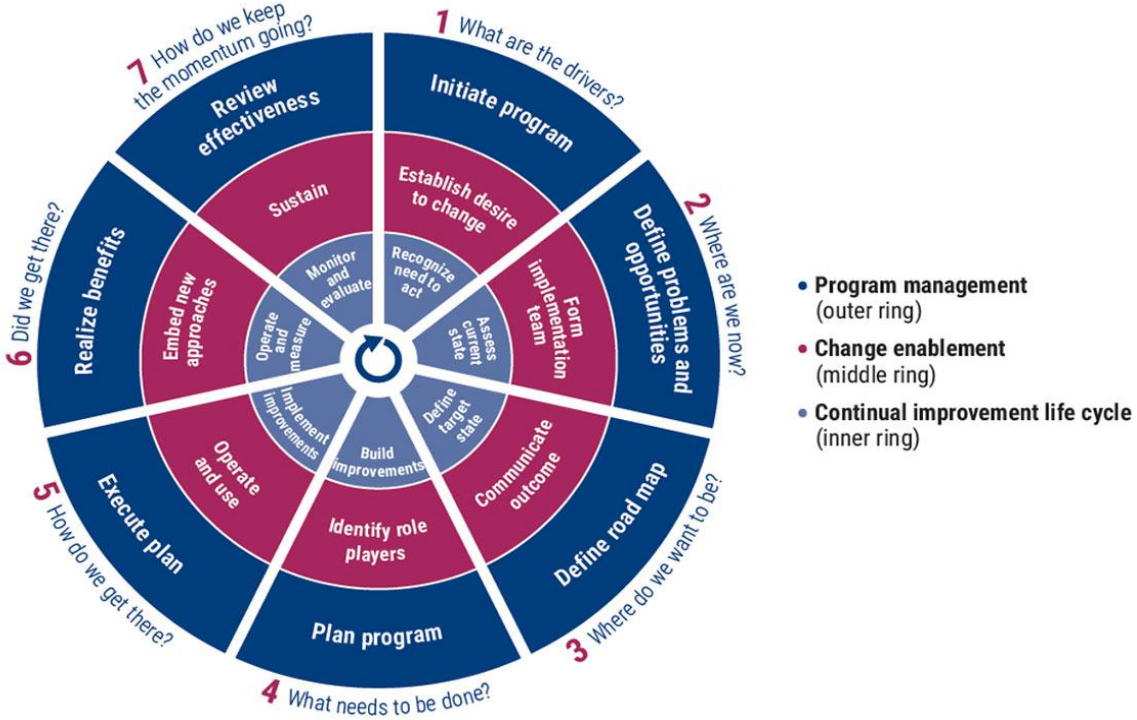
2) Change Enablement and

3) Continuous Improvement Cycle.

The figure illustrates that initiatives as continual lifecycles emphasize that they are an ongoing process of implementation and improvement (ISACA, 2018b).

Figure 1

Components of the Life cycle (ISACA, 2018b)



Methodology

Many SMEs erroneously believe that they will not be targets for cybersecurity attacks. However, every organization accepting, processing, transmitting, or storing cardholder data needs to implement PCI DSS as a security standard and sustain

compliance status annually. Due to its small size, SMEs lack resources compared to large organizations, making PCI DSS compliance difficult for SMEs. This research paper identifies challenges faced by SMEs in PCI DSS implementation. The paper proposes guidelines for PCI DSS implementation and maintaining compliance for SMEs using COBIT 2019 implementation approach based on identified challenges.

This research aims to develop guidelines that focus on SMEs only, considering difficulties to fulfill data security benchmarks provided in standard due to inadequate resources in terms of money, specialized staff, knowledge, IT equipment, and many more. This research is based on version 3.2.1 of PCI DSS.

PCI DSS standard plays a prominent role in organizations to protect and secure cardholder data. This study focuses on solving the following questions:

1) What are the challenges faced by SMEs in PCI DSS implementation and maintaining compliance?
2) How can SMEs implement PCI DSS as a data security standard using COBIT 2019 Implementation guide?
3) How can SMEs maintain PCI complaint status regularly using COBIT 2019 Implementation guide?

The following methodology is employed to develop an implementation guide:

a. A literature review is conducted to identify SME's challenges related to PCI-DSS implementation and maintain compliance status.
b. Identified challenges in step a are mapped to the PCI DSS requirements.

c. PCI DSS implementation guidelines are proposed by dividing them into seven phases of the COBIT 2019 implementation guide for PCI DSS implementation. PCI DSS implementation guidelines are stated under the program management tasks, while the continual improvement life cycle provides guidelines required to work continuously to maintain PCI DSS compliance.

Presentation and Discussion of Results

The first part of the results section presents PCI DSS implementation and compliance challenges that SMEs face through literature review. Table 3 maps each identified challenge to the PCI DSS requirement(s) that is affected. Mapping helps to identify difficulties encountered to fulfill each requirement to become PCI DSS compliant. This table substitutes SME's challenges into implementation and maintaining compliance challenges.

Table 3

PCI DSS Implementation and Compliance Challenges mapped to PCI DSS requirements

Challenges faced by SMEs	**Implementation Challenge**	**Compliance Challenge**	**PCI DSS requirements**
Maintaining compliance with all requirements annually (Verizon, 2019b)	x	x	R1, R2, R3, R4, R5, R6, R7, R8, R9, R10, R11, R12
Inadequate security measures to protect cardholder data (Lingor & Ruesch, 2020)	x	x	R1, R2, R3, R4, R5, R7, R8, R9

Challenges faced by SMEs	Implementation Challenge	Compliance Challenge	PCI DSS requirements
Improper access controls (Friedman, 2020)	x		R3, R4, R7, R8, R9
Lack of proper authentication systems to protect critical data and information (Friedman, 2020)	x		R7, R8, R9
Manual and Obsolete processes, program, and systems (Lingor & Ruesch, 2020)	x	x	R6
Doubtful and confusing scope (Nanda, Popat & Vimalkumar, 2018)	x	x	R12
Lack of awareness, reluctant peer-behaviour (Clapper & Richmond, 2016)	x	x	R12
Insufficient technical resources and expertise (Boese IV, 2020)	x	x	R10, R11
PCI SSC Audit Failures due to insufficient audit trails (physical and non-physical) (Boese IV, 2020).		x	R9, R10

Challenges faced by SMEs	Implementation Challenge	Compliance Challenge	PCI DSS requirements
Poor management and flawed communication to protect critical data (Friedman, 2020; Ydstie, 2015)	x	x	R3, R4, R7, R8, R9, R12

The next part of the results presents PCI DSS implementation guidelines for SMEs using the COBIT based implementation approach. PCI DSS implementation guidelines are developed by applying the Continual Improvement Life Cycle (CIC) implementation approach of COBIT 2019. PCI DSS implementation is not just a one-time process. Instead, it is an ongoing implementation and improvement process followed annually to be PCI DSS compliant for organizations. CIC implementation approach of COBIT 2019 also forms an ongoing implementation and improvement process that ultimately becomes usual business activity. Thus, COBIT 2019 CIC implementation approach is the best recommendation for a practical PCI DSS implementation approach.

Proposed PCI DSS implementation Guidelines are divided into seven phases of the COBIT 2019 implementation guide. The identified PCI DSS implementation challenges are listed in each phase, comprising COBIT challenges, root causes and success factors. Root cause and success factors provide a significant influence by pointing specific pain points and favourable outcomes for PCI DSS implementation. Program management tasks provide guidelines for implementing PCI DSS for SMEs, whereas the Continual improvement lifecycle tasks provide guidelines to maintain PCI

DSS compliance regularly. Different guidelines for implementation and maintaining compliance are proposed considering challenges faced by SMEs to maintain PCI DSS compliance annually after implementing PCI DSS once. Every SME should develop and focus on a change enablement strategy depending on the organizational environment based on COBIT 2019 implementation guide. SMEs need a change enablement strategy to identify the need for change and initiate actions to fulfill requirements regularly considering behavioural and cultural tasks. Table 4 is a glimpse of the proposed guidelines. The entire proposed guidelines can be accessed through the provided link: https://drive.google.com/file/d/1zxeAkHRTsnb3cxnYH1qT_8YRwLxL5V16/view?usp=sharing

Table 4

Guidelines for PCI DSS implementation and compliance for SMEs

Phase 1: What are the drivers? - Obtain an understanding of the program background and objectives, i.e. PCI DSS implementation. This phase articulates the compelling reasons to act within the organizational context. The buy-in and commitment of all key stakeholders are obtained.					
PCI DSS Implementation and maintaining Compliance Challenges	COBIT Challenges	Root Causes	Success Factors	Continual Improvement Lifecycle Tasks	Change Enablement Tasks
Doubtful and confusing scope (Nanda, Popat & Vimalkumar, 2018)	Lack of senior management buy-in, commitment and support	Lack of understanding of the importance, urgency, and value of PCI DSS implementation to the enterprise	Make a committee or leverage an existing committee to provide a mandate and accountability for action	• Committee or higher management should create and establish information security policy to educate employees and management about PCI DSS scope, its importance, urgency and value or benefit of its implementation to the organization	• Update information security policy, as required, if there is any change by management or PCI DSS requirements by PCI SSC or any other reason.

This study is a limited theoretical approach and not tested in a real business environment for SMEs. Researchers can validate the research paper results by following and examining guidelines in SME's real business world. For future works, the researcher can identify some more challenges related to PCI DSS implementation and compliance and propose solutions for SMEs

Conclusions

PCI DSS compliance is mandatory for organizations that store, transmit, and process cardholder data. Due to its technical nature, this standard is difficult to implement and comply with for businesses with limited resources and knowledge. This research paper studied challenges faced by SMEs to comply with PCI DSS. Challenges are identified by looking at the literature review, including lack of access controls, authentication systems, awareness, technical resources, and knowledge. PCI DSS implementation guidelines are developed for SMEs considering COBIT 2019 implementation guide phases. These guidelines are provided by mapping identified challenges with affected PCI DSS requirements, meaning which problems SMEs face complying with a PCI DSS requirement. Challenges are either related to one requirement or common to more than one requirement. Guidelines are some possible courses of action that SMEs can execute to make the PCI DSS compliance process more manageable.

Implementing PCI DSS and maintaining compliance could be a costly and time-consuming process. However, it offers numerous benefits to a business, including protection and security to cardholder data as well as critical and sensitive information of the organization. PCI DSS also means free from data breaches, heavy fines, and penalties due to non-compliance. The proposed guideline's main motive is to make the PCI DSS

implementation process more manageable and achievable for SMEs. Identified challenges and proposed guidelines in this research paper are limited to the literature review section's study. Provided guidelines are not validated in SME's real business environment. In future, researchers can prove the validity of these guidelines by testing in a real business environment of environment.

References

Boese IV, RF. (2020). *PCI DSS Compliance Challenges for Small Businesses* (Publication No. 27672228) [Master's capstone project, Utica College]. ProQuest Dissertations & Theses.

Chuvakin, A. A., & Williams, B. R. (2010). *PCI Compliance: Understand and implement effective PCI data security standard compliance* (2nd ed.). Syngress Publications.

Clapper, D. & Richmond, W. (2016). SMALL BUSINESS COMPLIANCE WITH PCI DSS. *Journal of Management Information and Decision Sciences*, 19(1), 54-67. Retrieved from https://search.proquest.com/docview/1804900242?accountid=10243

Fernandes, J. J. (2015). Get ready for PCI DSS 3.0 with real-time monitoring. *Computer Fraud and Security*, 2015(2), 17–18. https://doi.org/10.1016/S1361-3723(15)30009-9

Friedman, Z. (2020, February 28). *'Shark Tank' Star Loses $400,000 In Email Scam*. https://www.forbes.com/sites/zackfriedman/2020/02/28/shark-tank-financial-scam/.

GoAnywhere. *3 Data Breaches That May Have Been Avoided through PCI DSS Compliance*. (2017, February 2). Retrieved from https://www.goanywhere.com/blog/2017/02/02/3-data-breaches-pci-compliance

Government of Canada (GC). (2019). *Key Small Business Statistics - January 2019.* Retrieved from the Government of Canada website: https://www.ic.gc.ca/eic/site/061.nsf/eng/h_03090.html

Information Systems Audit and Control Association. (2018a). *COBIT 2019 Framework: Introduction and Methodology.* Retrieved from https://www.isaca.org/bookstore/bookstore-cobit_19-digital/wcb19fim

Information Systems Audit and Control Association. (2018b). *COBIT 2019 Implementation Guide: Implementing and Optimizing an Information and Technology Governance Solution.* Retrieved from https://www.isaca.org/bookstore/bookstore-cobit_19-print/cb19igio

Lingor, S., & Ruesch, J. (2020, August 13). *Protecting Small Businesses from Fraud*. Retrieved from https://www.cpapracticeadvisor.com/small business/news/21150163/protecting-small-businesses-from-fraud.

Miteva, Ani. (2017, September 19). *PCI Non-Compliance: 7 Negative Consequences for Businesses.* Mymoid. Retrieved from https://www.mymoid.com/pci-non-compliance-consequences

Nanda, A., Popat, P., & Vimalkumar, D. (2018). *Navigating Through Choppy Waters of PCI DSS Compliance*. Advances in Information Security, Privacy, and Ethics, 99–140. Retrieved from https://doi.org/10.4018/978-1-5225-2604-9.ch005

Nicho, M., Fakhry, H., & Haiber, C. (2011). *An Integrated Security Governance Framework for Effective PCI DSS Implementation.* International Journal of

Information Security and Privacy, 5(3), 50–67. Retrieved from https://doi.org/10.4018/jisp.2011070104

Official PCI Security Standards Council Site - Verify PCI Compliance, Download Data Security, and Credit Card Security Standards. (n.d.). Retrieved October 19, 2020, from https://www.pcisecuritystandards.org/merchants/

Olajide. P., Zavarsky. P., Ruhl. R., & Lindskog. D. (2015). *PCI DSS Compliance Validation of Different Levels of Merchants in a Multi-tenant Private Cloud*. Retrieved from https://concordia.ab.ca/wp-content/uploads/2017/04/OlajideP.pdf

Payment Card Industry Security Standards Council. (2018). *Payment Card Industry (PCI) Data Security Standard Requirements and Security Assessment Procedures*. (Version 3.2.1). Retrieved from https://www.pcisecuritystandards.org/document_library

Rafter, D. (2019, May 24). *How to Protect your small business from a data breach*. CreditCards.com. Retrieved from https://www.creditcards.com/credit-card-news/small-business-data-breaches-safety-tips/

Rahaman, S., Wang, G., & Yao, D. (Daphne). (2019). *Security Certification in Payment Card Industry.* Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security, 481–498. Retrieved from https://doi.org/10.1145/3319535.3363195

Rees, J. (2010). *The challenges of PCI DSS compliance*. Computer Fraud & Security, 2010(12), 14–16. Retrieved from https://doi.org/10.1016/s1361-3723(10)70156-1

Rees, J. (2012). *Tackling the PCI DSS challenges*. Computer Fraud & Security, 2012(1), 15-17. Retrieved from https://doi.org/10.1016/S1361-3723(12)70009-X

Seaman, J. (2020). *PCI DSS: An integrated data security standard guide*. Apress. Retrieved from https://doi.org/10.1007/978-1-4842-5808-8

Verizon. (2019a). *2019 Data Breach Investigations Report.* Retrieved from https://enterprise.verizon.com/resources/executivebriefs/2019-dbir-executive-brief.pdf

Verizon. (2019b). *2019 Payment Security Report*. Retrieved from https://enterprise.verizon.com/resources/reports/2019-payment-security-fullreport-bl.pdf

Ydstie, J. (2015, September 15). *When Cyberfraud Hits Businesses, Banks May Not Offer Protection.* Retrieved November 10, 2020, from https://www.npr.org/sections/alltechconsidered/2015/09/15/440252972/when-cyber-fraud-hits-businesses-banks-may-not-offer-protection

Yulianto, S., Lim, C., & Soewito, B. (2016). *Information security maturity model: A best practice-driven approach to PCI DSS compliance.* 2016 IEEE Region 10 Symposium (TENSYMP), 65–70. Retrieved from https://doi.org/10.1109/tenconspring.2016.7519379