Data Privacy Compliance Using COBIT 2019 and Development of MISAM Audit Caselet

Co-authored by

Aman Dev Singh Dharni

Bobby Swar

Shaun Aghili

Project Report

Submitted to the Faculty of Graduate Studies,
Concordia University of Edmonton

In Partial Fulfillment of the
Requirement for the Final
Research Project for the Degree

MASTER OF INFORMATION SYSTEMS ASSURANCE MANAGEMENT

Concordia University of Edmonton
FACULTY OF GRADUATE STUDIES

Edmonton, Alberta

April 2020

Data Privacy Compliance Using COBIT 2019 and Development of MISAM Audit Caselet

Aman Dev Singh Dharni

Approved:

Bobby Swar (Approval on File) April 13, 2020

Chair of MISSM/MISAM Research Committee Date

Edgar Schmidt (Approval on File) April 20, 2020

Dean of Graduate Studies Date

ABSTRACT

In recent times, ensuring data and user privacy has been one of the biggest impediments in information technology. With the advent of high penalties for privacy breaches and the high risk of reputation loss for a corporation, the need to comply with privacy regulations have never been greater. This paper talks about the growing importance of data privacy and penalties imposed on organizations due to recent data breaches that compromised the confidentiality of users. Additionally, privacy regulations PIPEDA and GDPR are discussed along with leveraging COBIT 2019 framework to ensure PIPEDA and GDPR compliance. Finally, an audit caselet is developed to help aspiring auditors design a PIPEDA and GDPR compliant audit checklist under the COBIT 2019 framework.

Keywords: Data privacy, PIPEDA, GDPR, COBIT 2019, Compliance.

1. INTRODUCTION

1.1 Background

In order to gain competitive edge, create value to corporations and personalise user experience, data driven businesses have become highly dependent on the application of personal information. Today, organizations leverage consented personal information and preferences of customers to improve business growth via targeted advertising and marketing. Private user data has thus become an integral part of operations and business decision-making processes of enterprises worldwide. But, with greater adoption and even greater development and integration of user data in business operations, comes the need for governance structures, regulations and processes that can help ensure protection of private user information from unconsented misuse. For instance, on 23 October 2020, the Austrian Data Protection Authority fined Austrian Post €18,000,000 for processing user data without having the sufficient legal basis to do so. The Austrian data protection authority found out in its investigation that Austrian Post created profiles on Austrian citizens that included personal information like political party affiliations, house address, personal predilections, etc. and resold this confidential information to political parties and companies for targeted advertising. Hence, we can say that compliance to stricter laws and regulations on gathering, exploiting, and distributing private data should not be taken lightly since non-compliance could lead to hefty fines.

In addition to this, for aspiring auditors, a real time privacy audit of an enterprise is not only nonviable, oftentimes, due to lack of experience, many auditors do not receive

a chance to get hands on experience on performing an audit early in their careers. Moreover, the recent release of COBIT 2019 means, not many security experts have yet implemented the framework in their organizations. Therefore, designing a caselet for adopting COBIT 2019 framework in privacy compliance can greatly help aspiring auditors to improve their auditing skills and get an up to date knowledge of widely accepted and implemented security and privacy regulations like GDPR and PIPEDA.

The rationale behind developing the caselet is to help would-be auditors to use COBIT 2019 framework for steering privacy compliance for PIPEDA and GDPR regulations. *Table 1* shows the list of recent white papers published by global consulting firms and international professional associations that weigh upon the changing compliance environment. And from *Table 1* given below, we can infer that most audit functions are either planning or are already adopting innovative and up-to-date standards and frameworks to tackle privacy risks.

Organization	**Insight**
Gartner, 2019	In Gartner's 2019 Audit Plan Hot Spots series, key risk areas that audit departments anticipate focusing on 2019 have been identified. Here, data privacy is amongst the top 5 concerns as companies face more advanced security breaches. The costs and risks of inadequately managing and protecting data have exponentially increased after the introduction of GDPR.

IIA, 2018	Out of 636 Chief Audit Executives (CAEs), Directors, and Senior Managers surveyed, for allocation of audit effort by risk area, 16% (second highest) of the anticipated allocation of resources was expected towards privacy compliance and regulatory requirements, which was not related to financial reporting.
Deloitte, 2019	In Deloitte's internal audit insights for 2019, GDPR assurance and advice has been considered in the top ten high-impact areas of focus. Deloitte states that "GDPR-related audits should now be considered in the annual risk assessment and internal audit planning processes", just like SOX compliance. Internal Audit needs to help the corporation with measuring the risks, data requirements, processes and courses needed for privacy regulation fulfilment.
Protiviti	Protiviti, a global consulting firm conducted a survey with 1113 respondents consisting of CAEs, Digital leaders/Experts, and Audit staff. In their research, they found that for 76% of the respondents, the internal audit department was currently undertaking or expected to undertake transformation or innovation initiatives. But presently, only 25% were currently undertaking next-generation governance competencies. And 56% were planning to transform their audit process within the next one to two years.

KPMG, 2019	In KPMG's report of "Top 20 Key Risks to Consider by Internal Audit Before 2020", GDPR compliance holds the 3rd position. The report emphasizes on GDPR being a major and highly influencing change in information protection and user data privacy in recent history. And due to GDPR's highly time dependent requirements like the duty to inform regulation authorities about private information breaches within 72 hours, organizations must have a nimble and continuous data protection and incidence response control in place.

Table 1: Global Insight for Increasing Privacy Concerns

Harmonising between regulations periodically updated by the government to supervise industrial advancements in information technology and the aim of defending private information requires adoption of latest frameworks and being up to date with latest security laws. Since a high amount of audit resource allocation is anticipated towards privacy fulfilment and regulatory requirements, it would be of great use to adopt recently updated COBIT 2019 framework to ensure privacy compliance by creating a privacy audit checklist. In addition to this, creating a caselet to use COBIT 2019 to ensure GDPR and PIPEDA compliance in an enterprise will greatly assist aspiring auditors in gaining privacy audit experience.

1.2 Problem Statement

Data privacy (Gartner, 2018) and data governance (IIA, 2018) are one of the top five key risk areas that Audit departments anticipate focusing on in 2019. Out of more than 200 respondents surveyed in 2019 across Gartner's global network of client organizations, 42% are not fully confident in Audit's ability to provide assurance over data privacy risks. For example, non-compliance to GDPR, a privacy regulation, can result in a penalty of 4 percent of global annual turnover of the preceding financial year or €20 million (GDPR, 2018). Thus, complying to privacy regulations is of paramount importance to an enterprise. Additionally, aspiring auditors do not have the benefit of implementing COBIT 2019 for privacy audit in a live environment, and there are no COBIT 2019 caselet available for privacy compliance implementation. Would-be auditors need to gain competency through case studies. Therefore, there is a need to develop COBIT 2019 caselet focusing on privacy compliance.

1.3 Summary Research Statement

This research contains an audit checklist for PIPEDA and GDPR compliance using COBIT 2019 framework. Moreover, a comprehensive case study is designed enabling aspiring auditors to identify various GDPR and PIPEDA related privacy considerations in an enterprise. The case study will be used to create a privacy checklist for an organization using COBIT 2019 framework and mapping the identified privacy gaps corresponding to PIPEDA and GDPR requirements.

1.4 Organization of the Research Paper

The aim of this paper is to introduce the reader to the importance of user data privacy, give an outline on Personal Information Protection and Electronic Documents Act (PIPEDA), General Data Protection Regulation (GDPR) and deliver a brief overview of COBIT 2019. The methodology section of this paper discusses the scope and limitations of this research along with the research question that is raised. Finally, this paper discusses the case study designed to help aspiring auditors perform a privacy audit and presents a user data privacy compliance checklist devised in accordance with the COBIT 2019 framework.

2. LITERATURE REVIEW

This section discusses the industry's growing concerns with increasing cyber-attacks resulting in the loss of data privacy and affecting consumers' confidentiality, availability and integrity of information, along with handling information security programs for user awareness. Then later in this section, COBIT framework is discussed along with privacy regulations Personal Information Protection and Electronic Documents Act (PIPEDA) and General Data Protection Regulation (GDPR).

2.1 Data Privacy and Cyber-Attacks

Cyber-attacks are rising rapidly day by day, and they are no longer exclusively targeted towards big corporations. According to Zarka, Moin, and Karuna (2016), with the growth and availability of new tools and practices, cyber-crime is increasing rapidly. The has led to an increased amount of cyber-attacks and the level of damage instigated to

the targeted individual. As per Navjeet (2015) and Andreea (2015), cyber criminals use various methods like brute force attacks, phishing, social engineering, man in the middle attacks, etc., to damage the integrity, availability and confidentiality of data, with as much as 117,000 cyber-attacks being propagated every day. Successful execution of cyber-attacks allows criminals to gain access to name, date of births, house address, medical records, email address, insurance information, phone numbers, etc., of unsuspecting victims. Zarka, Moin and Karuna (2016) also found that bank related cyber-crimes are rapidly growing. Although banks highly prioritize the security and safety of their customers, yet conservative and predictable security measures are no longer optimal to prevent hackers from bypassing them. As per Maria (2015) banks are four times more likely to be targeted than regular businesses. The attacks include, but are not exclusive to online payment fraud, internet transactions, ATM cards and machines, etc. Also, apart from cyber-attacks, customer privacy can be violated by sharing their private information with third parties, letting external organizations access user-data for personalised and targeted advertising without user consent, giving insufficient information to customers regarding how their personal information will be processed, collecting more than necessary user data, etc. Banks need a continuous risk assessment policy in place. Banks need to keep a sharp eye on underlying system susceptibilities in banking networks and latest tools and techniques used by hackers to side-step security protocols and initiate attacks. With an estimated fifty billion devices to be linked to the internet by 2019, regulation authorities need to come up with a robust plan to secure the personal information, rights and confidentiality of consumers. And, financial institutions need to uninterruptedly employ safety nets to secure their customers' data and confidentiality.

As per Navjeet (2015), security of transmitted data and stored data are one of the chief concerns while using the internet. In her paper, she states that the customer is the most delicate link in a bank's security architecture, and even a small-scale attack, if carried out successfully, can bring down an entire corporation and cause massive reputation loss. Consequently, the majority of the attacks targeting net banking systems are directed at the unsuspecting user by using social engineering methods to lure them into giving their identification and authentication information which in turn compromises the user's net-banking services to perform unauthorised banking transactions. Stephan and Edward (2017) also identified users as the principal underlying limitation in an organization's information security infrastructure. User behaviour should be taken into consideration when creating the information security policy (ISP). Carrying out information security awareness programs and allowing all the employees to understand the ISP policy is considered to be the most economical way of reducing data security risks. Stephen and Edward proposed a research model (*Figure 1*) which states that user awareness received via internal channels (awareness programs and trainings provided by the organization like e-learning, internal newspapers, posters, etc.) and external channels (self-regulated research and learning, newspapers, T.V., YouTube, etc. and prior knowledge on the topic) both translating to improved information security awareness and enhanced positive outlook towards information security behaviours in the organization. In addition to this, the user's attitude, and perceived social norms along with low level of neutralization techniques (individuals convincing themselves and others that their non-standard actions are justifiable, pardonable or forgivable) give rise to a greater intent of being ISA program compliant. The proposed model was evaluated based on an employee

survey whose findings supported the case that carrying out information security awareness programs raises user ISA and security compliance and positively influences user's information security conduct.

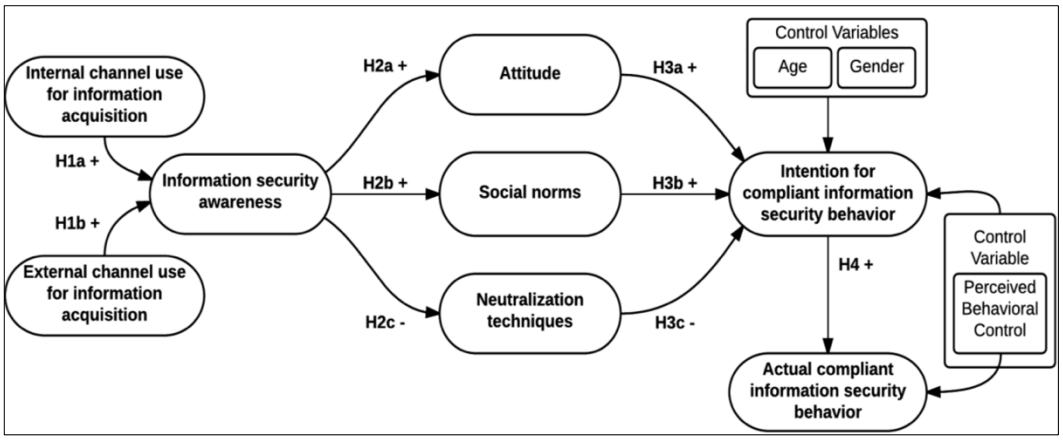


Figure 1: Information Security Awareness Retention Model (Stephan and Edward, 2017)

Given below (*Table 2*) is a table of one of the most well-known data violations in recent history, along with the resulting financial repercussions:

Organization	**Data Breach**	**Financial Repercussions**
Equifax	In 2017, Equifax lost the financial and private information of nearly 150 million users due to an unpatched framework in the	The company is now liable to pay $575 million in a disbursement with the Federal Trade Commission.

	database. The company failed to fix a critical vulnerability months after a patch had been issued and then failed to inform the public regarding the breach for weeks after it was discovered.	Equifax had already been fined £500,000 in the United Kingdom the privacy breach.
British Airways	In 2018, British Airways used card skimming scripts to harvest the private information and credit card data of up to five hundred customers.	On 8th July 2019, British Airways was fined £204.6 million by the UK's data protection authority under the GDPR regulation (Article 32).
Uber	In 2016 Uber had six hundred thousand drivers and fifty-seven million user accounts compromised. Uber also tried to bribe the culprit $100,000 to keep the hack away from	Uber was penalised the largest information-breach fine in history in 2018 for $148 million for violating data breach notification regulations.

	public's notice and failed to notify the regulating authorities regarding the data breach.	
Marriott International Inc.	UK's data protection authority delivered a huge penalty over an information leak when payment info, and personal user information of 500 million clientele was compromised.	Due to insufficient technical and organisational measures to ensure information security. On 9th July 2019, under GDPR law, Marriot International Inc. was ordered to pay £110,390,200 (Article 32)
Google Inc.	In January 2019, the CNIL committee enforced a fine against Google Inc., for giving inadequate information to its user regarding consent over personalized advertisement	Under Article 5, 6, 13, 14 of GDPR, Google was fined £50,000,000 on 21st January 2019.

	and for the lack of transparency over user consent policies.	

Table 2: Recent Data Breaches and Regulation Fines. Source: GDPR Enforcement tracker https://www.enforcementtracker.com/

Therefore, data privacy is becoming one of the biggest consideration factors that can affect the financial and reputational stability of any enterprise.

2.2 COBIT

COBIT is an industry leading framework that has been developed by a non-profit organization called ISACA. It pertains to information technology (IT) management and IT governance. It was built in 1996 to suit the requirements of both business executives and IT professionals. Over the years, COBIT went through several iterations with the current version being updated from COBIT 5 to COBIT 2019 (see *Figure 2*). To put it simply, COBIT helps enterprises produce optimum usefulness from IT by maintaining a fine balance between benefit realization, resource utilization and risk level optimization. COBIT assists information technology to be administered in an all-inclusive way for the whole organization. This is done by taking into account the external and internal stakeholders' IT-related interests and keeping in mind the entire functional and organizational areas of accountability affected by information technology.

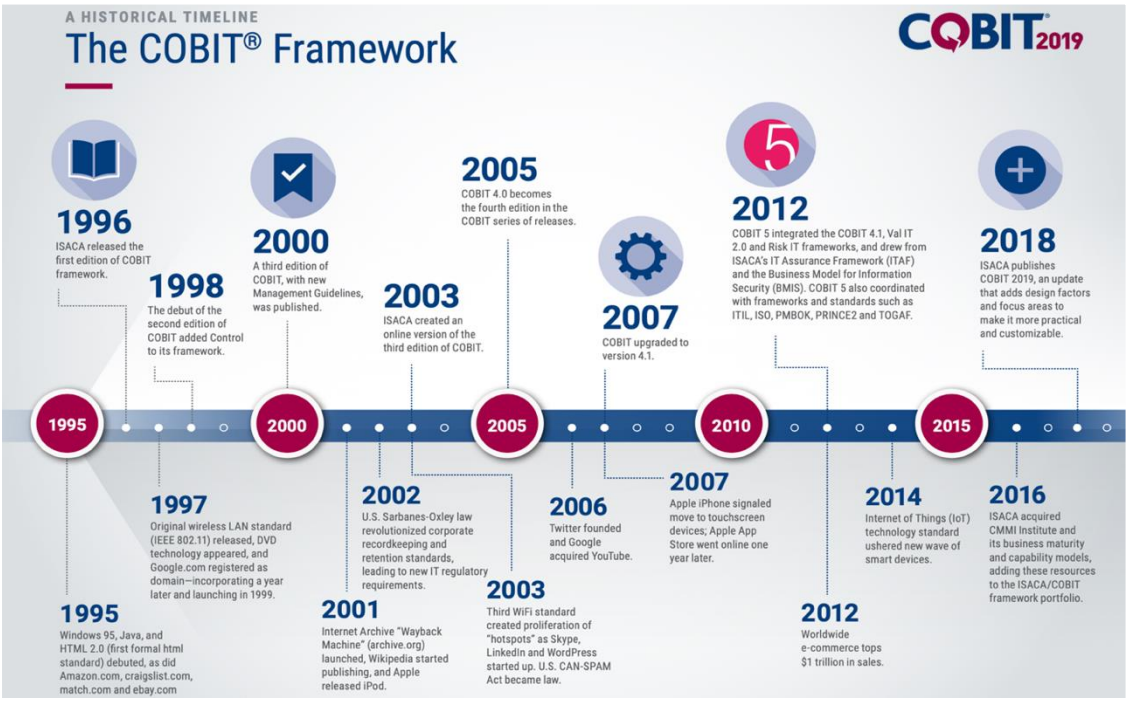


Figure 2: A Historical Timeline for COBIT (ISACA, 2019)

2.2.1 COBIT 2019 – New Features

In December 2018, ISACA released COBIT 2019. It became the successor to COBIT 5 which was released in 2012. ISACA came up with four titles that were a part of the COBIT 2019 product family, namely:

1. COBIT 2019 Framework: Introduction and Methodology - an outline to the main ideas of COBIT 2019.
2. COBIT 2019 Framework: Governance and Management Objectives – This title comprehensively describes the forty fundamental governance and management objectives. They are then corresponded with the interrelated process, enterprise goals, and governance and management practices.

3. COBIT 2019 Design Guide: Designing an Information and Technology Governance Solution – This title investigates design factors that can affect governance and it comes with a workflow planning tool that can be used to customize the organization's governance system.
4. COBIT 2019 Implementation Guide: Implementing and Optimizing an Information and Technology Governance Solution - This title helps develop a road map for uninterrupted governance expansion and upgradation.

The new features and terminologies that have been added or changed in COBIT 2019 as compared to its predecessor can be detailed as follows:

1. Enablers are now called components. And, there is a performance management process for all 7 components.
2. Managed Program and Managed Projects are 2 different objectives in BIA (Build, Acquire and Implement).
3. BIA's Managed Change process is now called Managed IT changes objective.
4. The Governance System has 6 principles and the Governance Framework has 3 principles.
5. As compared to 17 Enterprise Goals and IT Goals each earlier, now there are only 13 Enterprise Goals and 13 IT Goals.
6. Capability assessment based on Capability Maturity Model Integration version 2.0.
7. 11 design factors have been introduced and ISACA has created an Excel-based toolkit for a greater understanding of the factors.

2.2.2 COBIT 2019 for Privacy

COBIT 2019's six underlying principles help us understand the fundamental notions behind the framework but how do these principles align with privacy risks? ISACA's privacy principles work hand in hand with the COBIT framework, providing safeguards for an organization and ultimately giving value to its stakeholders (ISACA, 2017). It can be briefly explained as follows:

1. Provide Stakeholder Value:
   1.1. Recognizing and understanding stakeholders' need for privacy.
   1.2. Building customer, employee and stakeholders' trust by safeguarding their privacy.
   1.3. Giving value to stakeholders by providing protection from and reducing the risk of identity fraud and other harms.
2. Holistic Approach:
   2.1. Identifying privacy risks based on already defined processes, information data types, organizational structure, behaviors and cultures.
   2.2. Providing enterprises with privacy protection guidelines to be implemented alongside COBIT 2019 components, thus minimizing privacy risks to acceptable levels when the business implements actions to meet enterprise goals.
3. Dynamic Governance System:
   3.1. Applying an integrated framework aligning enterprise IT, information security and privacy through COBIT 2019's alignment with generally accepted privacy standards and governance models.
4. Governance Distinct from Management:

4.1. Promoting responsible privacy behavior to protect the privacy of all individuals associated with the business by fostering a privacy-positive culture to deliver an optimistic privacy-protection influence on the behavior of all personnel.

4.2. Ensuring privacy controls are integrated into business activities that involves any kind of personal information.

5. Tailored to Enterprise Needs

5.1. Adopting a risk-based approach to ensure that privacy risk is mitigated in a consistent and effective manner and concentrating on critical business applications in which a privacy breach would have the greatest business impact.

6. End-to End Governance System

6.1. Identifying where personal data exists within the organizational environment and how it flows throughout the enterprise.

6.2. Defining and implementing privacy protection controls within all processes that impact privacy inside the enterprise.

2.3 PIPEDA

The Personal Information Protection and Electronic Documents Act is a privacy regulation originating from Canada. PIPEDA became a regulation on 13 April 2000. For private-sector organizations in Canada, PIPEDA is the federal privacy law. The purpose of the law is to “govern the collection, use and disclosure of personal information while maintaining the right to privacy of individuals with respect to their personal information and the need of organizations to collect, use or disclose personal information for purposes

that would considered appropriate by a reasonable person under the circumstances" (PIPEDA, 2019).

According to this act "all businesses that operate in Canada and handle personal information that crosses provincial or national borders are subject to PIPEDA, regardless of the province or territory in which they are based". Any information that can help successfully identify a person and acquired in the course a profitable activity is considered as personal information under PIPEDA regulation. Listed below are the components considered as personal information.

1. Name and age of the person.
2. A person's income
3. A person's ethnicity, nationality or race.
4. Whether he/she is married/single.
5. Employment history.
6. Educational history.
7. DNA and medical history.
8. Social insurance number.
9. Driver's license number, among many other things.

As of first November 2018, institutes under the PIPEDA regulation need to evaluate the loss of private data that can cause substantial harm to the subject, when they experience a data breach. In order to be PIPEDA compliant, businesses need to:

1. Report to the Privacy Commissioner of Canada breaches of security safeguards involving personal information that pose a real risk of significant harm to individuals.
2. Notify affected individuals about those breaches.
3. Notify any other organization that may be able to mitigate harm to affected individuals.
4. Track and keep records of all breaches for at least 24 months following the date it determined that a breach occurred.

The federal Privacy Commissioner governs PIPEDA. The power to address the public regarding encroachments of the regulation and referring severe cases to Federal Court lies with the Privacy Commissioner. The five phases of PIPEDA act enforcement are:

1. Complaint – Written by an individual to the Privacy Commissioner or initiated by the Commissioner's own accord.
2. Investigation – The Commissioner carries out investigation and has the power to obtain oral or written evidence on oath, access organizational premises and conduct physical checks.
3. Report – The report contains summary from both the complainant and the defendant, and then comes up to a common conclusion or agreement, within a year of complaint submission date.
4. Compliance Agreement – The agreement contains terms necessary for compliance with PIPEDA, and the federal court has the power to enforce the term of the compliance agreement in case of non-obedience.

5. Hearing – The hearing is conducted at the federal court. Here, damages are awarded to the complainant if proven guilty and the court can order the business to issue a notice of any measure(s) taken to rectify the business practice/process.

2.4 GDPR

As per EU's GDPR website, "the General Data Protection Regulation 2016/679 (GDPR) is a regulation in EU law on data protection and privacy for all individual citizens of the European Union (EU) and the European Economic Area (EEA). It also addresses the transfer of personal data outside the EU and EEA areas. In 2016, GDPR (effective on 25 May 2018) was adopted to replace the Directive 95/46/EC to implement a legally binding regulation that will be considered the EU data protection law. GDPR gives EU residents control over their personal data wherever in the world the data may reside."

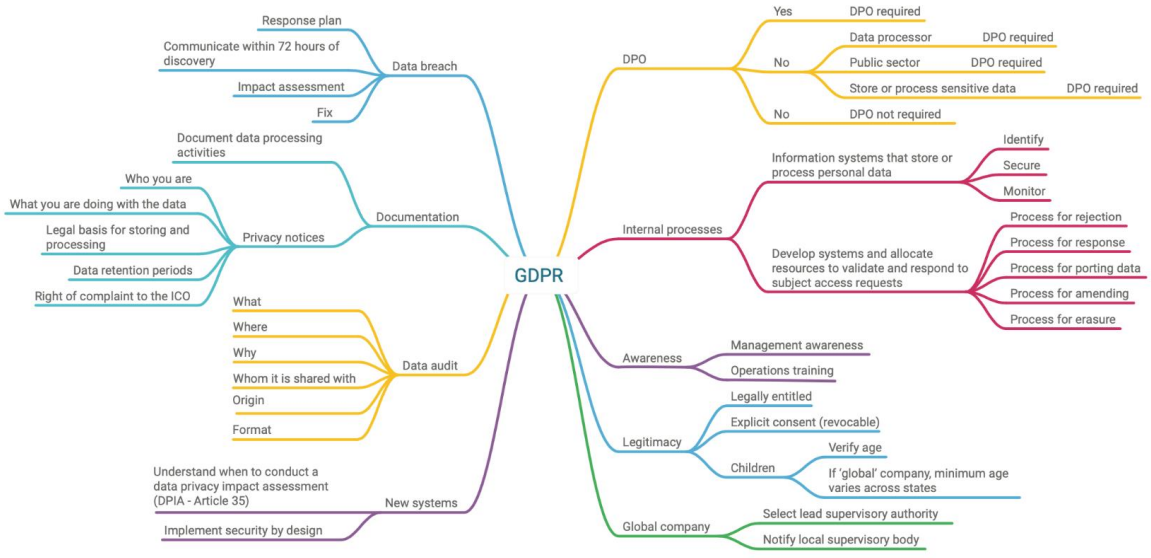


Figure 3: Key GDPR Domains (ISACA, 2018)

GDPR not only standardizes regulation across the EU and EEA, it also affects all enterprises that process data from EU/EEA countries. *Figure 3* represents key domains and associated requirements under GDPR. As per Information Commissioner's Office (ICO), they are seven fundamental philosophies that GDPR sets out:

1. Transparency, equality & lawfulness – Auditors must ensure that enterprises have the systems and processes in place to ensure that consent rights and contract obligations are not breached.
2. Purpose limitation – When undertaking user consent to process data for a specific purpose, the same data cannot be used again for another purpose.
3. Data minimisation – "Enterprises must limit personal data collection, storage and usage to what is relevant and necessary for processing". This means that companies should not collect and store private information just in case they might become useful in future. Therefore, data collected should only pertain to accomplishing a specific task.
4. Accuracy – Personal information should reflect the most recent status of the entity. Additionally, enterprises should not replicate user data.
5. Storage limitation – Personal information shall not be stored for longer than what is essential for administration. Data storage can be extended exclusively for archiving purposes in "public interest, scientific or historical research purposes or statistical purposes".
6. Confidentiality, Integrity and Availability - Personal data must be processed using fitting organizational and technical safety procedures and include protection against illegal access to maintain the CIA triad.

7. Accountability - Under GDPR, a data controller is the lawful individual or agency which regulates the means and reasons for computing private user information. Therefore, the controller is accountable for ensuring compliance with the six key principles mentioned earlier.

Ideally, the seven fundamental principles should be obeyed when crafting a decent information protection policy. For GDPR non-compliance, an organization is liable to be fined the higher of either 20 million European pounds, or 4% of the company's entire global yearly turnover.

3. METHODOLOGY

3.1 Research Scope

Under the research's scope, we use COBIT 2019 framework to help perform a PIPEDA and GDPR compliant audit by creating a privacy audit checklist. A caselet is developed, based on which a data privacy compliance checklist is designed. A hypothetical organization (GreatTrust bank) is created where privacy risks are identified and then mapped in line with PIPEDA and GDPR compliance regulation requirements while being in line with the COBIT 2019 framework.

3.2 Research Limitations

The limitation of the proposed research paper will be:

1. Not being able to test the feasibility of the created audit checklist in a real organization.
2. The audit checklist will primarily focus on the data privacy compliance for PIPEDA and GDPR requirements only.

3.3 Research Question

How can the COBIT 2019 framework be implemented to provide greater audit assurance pertaining to privacy of users?

How can an aspiring auditor gain competency of conducting a data privacy compliance audit in line with the COBIT 2019 framework?

3.4 Procedural Methodology

The procedural methodology followed in the research is as follows:

1. Reviewed and analyzed PIPEDA and GDPR regulatory documents. Created a list of governing requirements that are necessary for an organization to be PIPEDA and GDPR compliant.
2. Analyzed COBIT 2019 Framework. Identified how the regulatory requirements of PIPEDA and GDPR could be mapped to COBIT's Governance and Management Objectives.
3. Determined the essential privacy policy objectives that hold true for all organizations.

4. Combined steps 1., 2. and 3. to create a user data privacy audit checklist in MS EXCEL which is PIPEDA and GDPR compliant and aligned with COBIT 2019 framework.
5. Utilized the literature review and analysis done so far to create a "Study Guide". This guide contains a brief overview of COBIT framework, PIPEDA regulation and GDPR regulation.
6. Created a case study for a hypothetical organization (GreatTrust Bank). The case study contains deliverable instructions, learning objectives, company background, organizational structure of the bank, CEO's interview and the bank's privacy objectives. This information is then to be used by the reader as a base to create the privacy compliance audit checklist.
7. Created teaching material in PowerPoint presentation which includes the study guide and acts as an introduction to the case study.
8. Created a "Test Bank" with multiple choice questions and short answer questions, to ensure that the reader is able to grasp the concepts involved in the case study.

4. ANALYSIS & DISCUSSION OF RESULTS

The research result (or deliverable) consists of four parts:

1. "The Case-Study Narrative" document introduces the reader to a hypothetical GreatTrust bank. The bank is planning to completely revamp its privacy policies and controls to be in line with GDPR and PIPEDA privacy regulation. And, to achieve that the reader will be acting as the Chief Risk Officer, who is a COBIT framework veteran and in charge of spearheading the initiative.

2. “The Study Guide” acts as a starter kit to privacy regulation concepts of GDPR and PIPEDA. The Study Guide also introduces the reader to the COBIT 2019 framework. At the end of the document, the reader can further improve his knowledge by following the links given in the “for further reading” section.
3. The “Test Bank” consists of 42 multiple choice questions and 6 short answer questions to test the reader’s knowledge and to ensure that the reader was able to grasp all the important concepts.
4. The “Data Privacy Compliance Checklist”, which contains five spreadsheets is described below:
    i. COBIT 2019 Privacy Checklist: It includes all the GDPR and PIPEDA compliance requirements and maps them to the privacy policy objectives of the GreatTrust Bank under the COBIT 2019 governance and management objectives.
    ii. COBIT 2019 Objectives: This sheet lists all 40 management and governance objectives of COBIT 2019.
    iii. COBIT 2019 Activities: This sheet lists all 1202 activities associated with each of the governance and management practices in COBIT 2019.
    iv. GDPR: This sheet contains 91 GDPR control activities under 8 principles.
    v. PIPEDA: This sheet contains 90 PIPEDA control activities under 10 principles.

Each of the columns for the COBIT 2019 Privacy Checklist spreadsheet are explained in detail below, see *Figure 4., 5.* and *6.* (and appendix for the complete spreadsheet):

1. COLUMN B: Company Privacy Policy

Column B contains 6 essential privacy policy directives. These directives have been identified by ISACA as crucial mandates for privacy compliance in any organization collecting and storing user information. Some tweaks have been made to ensure that PIPEDA and GDPR regulatory requirements are mapped with each of the directives.

2. COLUMN C: Policy's Purpose Statement

The purpose statement of privacy policy directives listed in column B are explained in column C.

3. COLUMN D: COBIT 2019 Area

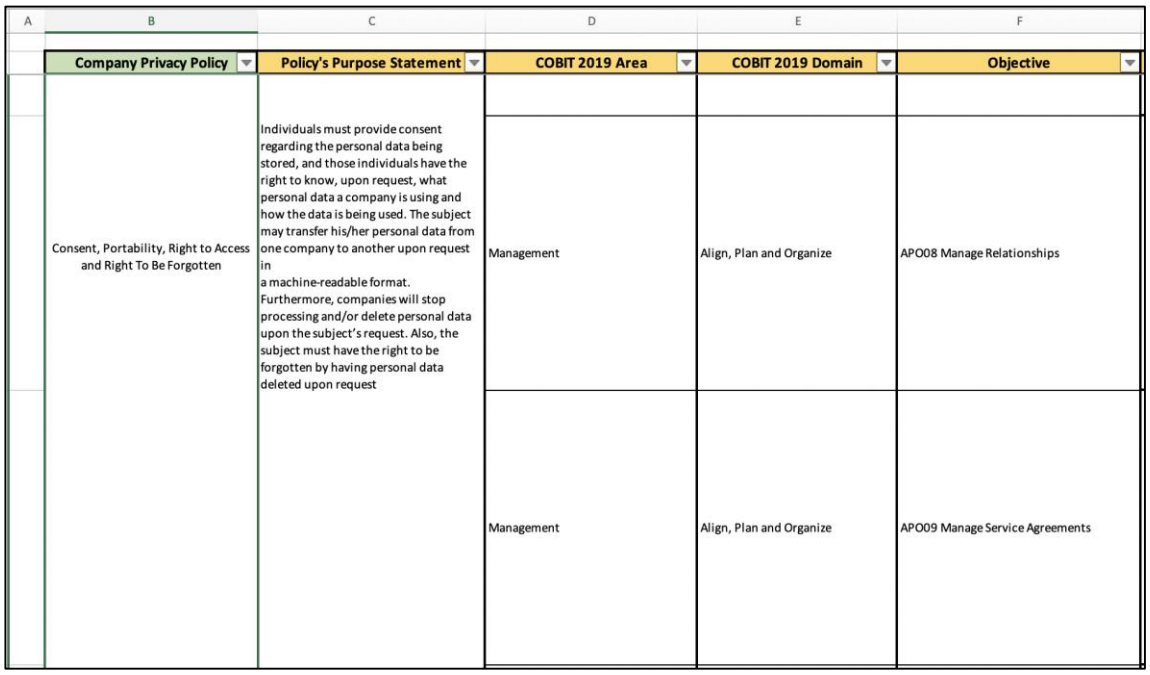
With respect to the company privacy policy, column D identifies whether the responsibility lies with the Management or the Governance body for the privacy objective.

4. COLUMN E: COBIT 2019 Domain

In line with the company privacy policy, one (or more) of the five COBIT 2019 domains are listed in column E, that best suit the policy's purpose (from COBIT 2019 Objectives spreadsheet).

5. COLUMN F: Objective

In column F, one of the forty COBIT 2019 objective is identified, with respect to the COBIT 2019 domain mentioned in column E (from COBIT 2019 Objectives spreadsheet).



Company Privacy Policy	Policy's Purpose Statement	COBIT 2019 Area	COBIT 2019 Domain	Objective
Consent, Portability, Right to Access and Right To Be Forgotten	Individuals must provide consent regarding the personal data being stored, and those individuals have the right to know, upon request, what personal data a company is using and how the data is being used. The subject may transfer his/her personal data from one company to another upon request in a machine-readable format. Furthermore, companies will stop processing and/or delete personal data upon the subject's request. Also, the subject must have the right to be forgotten by having personal data deleted upon request	Management	Align, Plan and Organize	APO08 Manage Relationships
		Management	Align, Plan and Organize	APO09 Manage Service Agreements

Figure 4: Column B-F of Data Privacy Compliance Checklist

6. COLUMN G: Objective Description

Column G contains the COBIT 2019 objective's description as per "COBIT 2019 Framework Governance and Management guide" (from COBIT 2019 Objectives spreadsheet).

7. COLUMN H: Objective Purpose Statement

Column H contains the COBIT 2019 objective's purpose statement as per "COBIT 2019 Framework Governance and Management guide" (from COBIT 2019 Objectives spreadsheet).

8. COLUMN I: Practice ID

Column I contain the specific Practice ID(s) identified with respect to the corresponding COBIT 2019 objective in column F (from COBIT 2019 Activities spreadsheet).

9. COLUMN J: Practice Name

Column J contains the specific Practice Name(s) identified with respect to the corresponding COBIT 2019 objective in column F (from COBIT 2019 Activities spreadsheet).

10. COLUMN K: COBIT 2019 Activities

In column K, the COBIT 2019 activities are defined as per "COBIT 2019 Framework Governance and Management guide" (from COBIT 2019 Activities spreadsheet).

F	G	H	I	J	K
Objective	**Objective Description**	**Objective Purpose Statement**	**Practice ID**	**Practice Name**	**COBIT 2019 Activities**
APO08 Manage Relationships	Manage relationships with business stakeholders in a formalized and transparent way that ensures mutual trust and a combined focus on achieving the strategic goals within the constraints of budgets and risk tolerance. Base relationships on open and transparent communication, a common language, and the willingness to take ownership and accountability for key decisions on both sides. Business and IT must work together to create successful enterprise outcomes in support of the enterprise objectives.	Enable the right knowledge, skills and behaviors to create improved outcomes, increased confidence, mutual trust and effective use of resources that stimulate a productive relationship with business stakeholders.	APO08.01 APO08.03	Understand business expectations. Manage the business relationship.	(*) Identify business stakeholders, their interests and their areas of responsibilities. (*) Manage the relationship in a formalized and transparent way that ensures a focus on achieving a common and shared goal of successful enterprise outcomes in support of strategic goals and within the constraint of budgets and risk tolerance. (*) Clarify business expectations for I&T-enabled services and solutions. Ensure that requirements are defined with associated business acceptance criteria and metrics.
APO09 Manage Service Agreements	Align I&T-enabled products and services and service levels with enterprise needs and expectations, including identification, specification, design, publishing, agreement, and monitoring of I&T products and services, service levels and performance indicators.	Ensure that I&T products, services and service levels meet current and future enterprise needs.	APO09.04 APO09.05	Monitor and report service levels. Review service agreements and contracts.	(*) Establish and maintain measures to monitor and collect service level data. (*) Regularly review service agreements according to the agreed terms to ensure that they are effective and up to date. When appropriate, take into account changes in requirements, I&T-enabled services, service packages or service level options.

Figure 5: Column G-K of Data Privacy Compliance Checklist

11. COLUMN L, M, N & O: RACI

These columns identify key employees who are Responsible, Accountable, Consulted and/or Informed corresponding to the COBIT 2019 activities mentioned in column K. They have been identified as per COBIT 2019 Framework's suggestions.

12. COLUMN P: Corresponding GDPR Principle

With respect to the privacy policy directive, matching GDPR compliance principles are identified here (from GDPR spreadsheet).

13. COLUMN Q: Applicable GDPR Control Activity

With respect to the GDPR Principle in column P, applicable GDPR control activities are identified here (from GDPR spreadsheet).

14. COLUMN R: Yes/No

Here the auditor inputs Yes or No to whether the GDPR checklist requirement is being fulfilled or not.

15. COLUMN S: Corresponding PIPEDA Principle

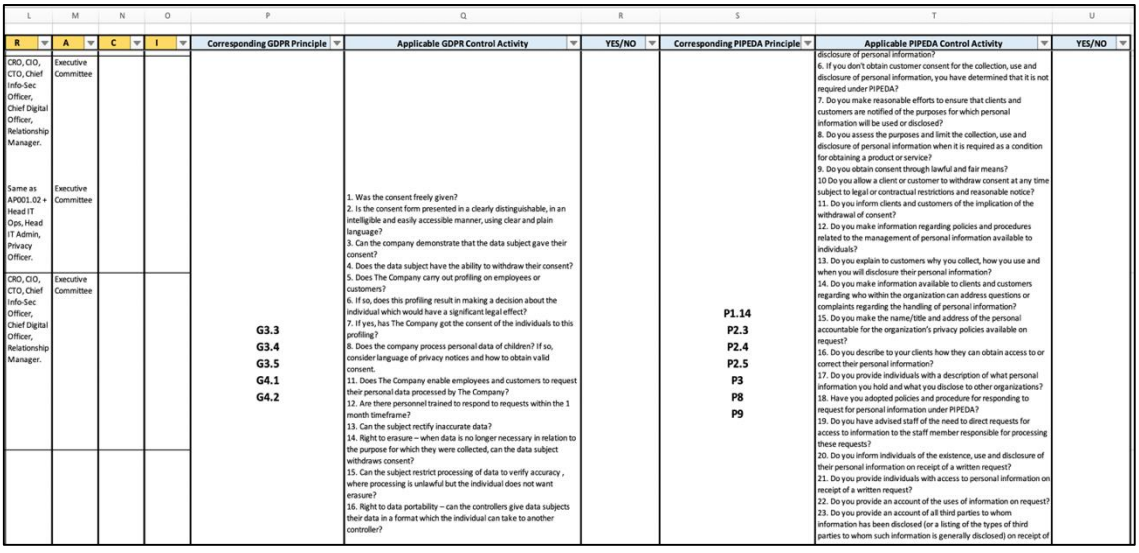
With respect to the privacy policy directive, matching PIPEDA compliance principles are identified here (from PIPEDA spreadsheet).

16. COLUMN T: Applicable PIPEDA Control Activity

With respect to the PIPEDA Principle in column S, applicable PIPEDA control activities are identified here (from GDPR spreadsheet).

17. COLUMN U: Yes/No

Here the auditor inputs Yes or No to whether the PIPEDA checklist requirement is being fulfilled or not.



L	M	N	O	P	Q	R	S	T	U
R	A	C	I	Corresponding GDPR Principle	Applicable GDPR Control Activity	YES/NO	Corresponding PIPEDA Principle	Applicable PIPEDA Control Activity	YES/NO
CRO, CIO, CTO, Chief Info-Sec Officer, Chief Digital Officer, Relationship Manager.	Executive Committee							disclosure of personal information? 6. If you don't obtain customer consent for the collection, use and disclosure of personal information, you have determined that it is not required under PIPEDA? 7. Do you make reasonable efforts to ensure that clients and customers are notified of the purposes for which personal information will be used or disclosed? 8. Do you assess the purposes and limit the collection, use and disclosure of personal information when it is required as a condition for obtaining a product or service? 9. Do you obtain consent through lawful and fair means? 10 Do you allow a client or customer to withdraw consent at any time subject to legal or contractual restrictions and reasonable notice? 11. Do you inform clients and customers of the implication of the withdrawal of consent? 12. Do you make information regarding policies and procedures related to the management of personal information available to individuals? 13. Do you explain to customers why you collect, how you use and when you will disclosure their personal information? 14. Do you make information available to clients and customers regarding who within the organization can address questions or complaints regarding the handling of personal information? 15. Do you make the name/title and address of the personal accountable for the organization's privacy policies available on request? 16. Do you describe to your clients how they can obtain access to or correct their personal information? 17. Do you provide individuals with a description of what personal information you hold and what you disclose to other organizations? 18. Have you adopted policies and procedure for responding to request for personal information under PIPEDA? 19. Do you have advised staff of the need to direct requests for access to information to the staff member responsible for processing these requests? 20. Do you inform individuals of the existence, use and disclosure of their personal information on receipt of a written request? 21. Do you provide individuals with access to personal information on receipt of a written request? 22. Do you provide an account of the uses of information on request? 23. Do you provide an account of all third parties to whom information has been disclosed (or a listing of the types of third parties to whom such information is generally disclosed) on receipt of	
Same as AP001.02 + Head IT Ops, Head IT Admin, Privacy Officer.	Executive Committee				1. Was the consent freely given? 2. Is the consent form presented in a clearly distinguishable, in an intelligible and easily accessible manner, using clear and plain language? 3. Can the company demonstrate that the data subject gave their consent? 4. Does the data subject have the ability to withdraw their consent? 5. Does The Company carry out profiling on employees or customers? 6. If so, does this profiling result in making a decision about the individual which would have a significant legal effect? 7. If yes, has The Company got the consent of the individuals to this profiling? 8. Does the company process personal data of children? If so, consider language of privacy notices and how to obtain valid consent. 11. Does The Company enable employees and customers to request their personal data processed by The Company? 12. Are there personnel trained to respond to requests within the 1 month timeframe? 13. Can the subject rectify inaccurate data? 14. Right to erasure – when data is no longer necessary in relation to the purpose for which they were collected, can the data subject withdraws consent? 15. Can the subject restrict processing of data to verify accuracy , where processing is unlawful but the individual does not want erasure? 16. Right to data portability – can the controllers give data subjects their data in a format which the individual can take to another controller?				
CRO, CIO, CTO, Chief Info-Sec Officer, Chief Digital Officer, Relationship Manager.	Executive Committee			G3.3 G3.4 G3.5 G4.1 G4.2			P1.14 P2.3 P2.4 P2.5 P3 P8 P9		

Figure 6: Column L-U of Data Privacy Compliance Checklist

5. CONCLUSIONS & RECOMMENDATIONS

The primary aim for this research was to create a data privacy compliance checklist under the COBIT 2019 framework that fulfilled GDPR and PIPEDA privacy regulation requirements. Additionally, an audit caselet was designed to help aspiring auditors hone their auditing skills by helping them develop the above-mentioned checklist. The government of Canada and the European Union periodically updates its privacy regulations to meet the ever-progressing field of Information Technology. Initially, a requirement list containing activities to be PIPEDA and GDPR compliant was created. Then, following ISACA's guidelines for an enterprise, essential data privacy objectives were designed. These data privacy objectives were subsequently mapped to COBIT 2019 Governance and Management Objectives. After doing that, all the PIPEDA and GDPR compliance list items identified earlier were matched to the data privacy objectives. By following this methodology, the data privacy compliance checklist was created.

In addition to this, a training package (caselet) was created which consisted of a case narrative, study guide, test bank and privacy audit checklist template. The purpose of this training package was to help aspiring auditors to get a brief overview of COBIT 2019, GDPR and PIPEDA privacy regulation. And, create an audit checklist that will map the regulations' requirements as per COBIT 2019 for a hypothetical organization. Since trainees or new auditors rarely get a chance to lead an audit project early in their careers, this caselet would serve as a perfect example to better prepare them for a future leadership role in auditing.

This research only focused on the GDPR and PIPEDA privacy regulation. PIPEDA being the most prominent privacy guideline in Canada was an obvious choice along with GDPR which has been adopted by organizations worldwide due to its global purview and massive financial implications for non-compliance. The data privacy audit checklist has been designed in a way that it incorporates most of the crucial data privacy requirements. The privacy policy directives are generalized enough to allow other researchers to incorporate privacy regulations local to their legislation and map the corresponding privacy requirements in the audit checklist. Additionally, it is recommended for future studies to update the GDPR, PIPEDA or local privacy requirements in the audit checklist with respect to the new revisions made periodically by the respective privacy regulation authorities.

6. REFERENCES

Andreea, B. (2015). Cyber-Attacks – Trends, Patterns and Security Countermeasures. Procedia Economics and Finance, vol. 28, 24-31. Available: https://core.ac.uk/download/pdf/82035298.pdf

Colin, B., Smith, O. (2018). GLOBAL Privacy Protection: Adequate Laws, Accountable Organizations and/or Data Localization? Association for Computing Machinery. Available: https://dl.acm.org/citation.cfm?doid=3267305.3274149

Dr. Bhavani, T. (2015). Big Data Security and Privacy. Association for Computing Machinery (ACM) 978-1-4503-3191-3/15/03. Available: http://dx.doi.org/10.1145/2699026.2699136

Deloitte (2018). Internal Audit Insights 2019. *Deloitte*. [Online]. Available: https://www2.deloitte.com/content/dam/Deloitte/us/Documents/risk/us-ia-high-impact-areas-of-focus.pdf

Govind, K. (2019, November). Transitioning an Enterprise from COBIT 5 to COBIT 2019. ISACA. Retrieved November 2019, from https://www.isaca.org/COBIT/focus/Pages/transitioning-an-enterprise-from-cobit-5-to-cobit-2019.aspx

Gartner (2018). 2019 Audit Plan Hot Spots Report Excerpt. *Gartner*. [Online]. Available: https://emtemp.gcom.cloud/ngw/globalassets/en/risk-audit/documents/audit-hot-spots.pdf

GDPR Enforcement Tracker. Available online: https://www.enforcementtracker.com

IIA (2018). GLOBAL PERSPECTIVES AND INSIGHTS. *IIA*. [Online]. Available: https://na.theiia.org/periodicals/Public%20Documents/GPI-2018-Top-Risks-Faced-by-CAES.pdf

IIA (2018). 2018 North American Pulse of Internal Audit. *IIA*. [Online]. Available: https://dl.theiia.org/AECPublic/2018-NA-Pulse-of-Internal-Audit-Report-NM.pdf

ISACA (2019). A Historical Timeline, The COBIT Framework. [Online]. Available: https://m.isaca.org/COBIT/Documents/COBIT-Timeline-2019_ifg_eng_1118.pdf

ISACA (2017). Connecting Privacy Activities with COBIT 5 Principles. [Online]. Available: https://www.isaca.org/COBIT/Documents/COBIT-Timeline 2019_ifg_eng_1118.pdf

ISACA (2018). COBIT 2019 Toolkit. [Online]. Available: http://www.isaca.org/COBIT/Documents/COBIT-2019-Toolkit_fmk_eng_1118.zip

ISACA (2018). How to Audit GDPR. [Online]. Available: http://www.isaca.org/Knowledge-Center/Research/ResearchDeliverables/Pages/How-to-Audit-GDPR.aspx

KPMG (2019). 20 Key Risks to Consider by Internal Audit Before 2020. *KPMG*. [Online]. Available: https://assets.kpmg/content/dam/kpmg/ch/pdf/key-risks-internal-audit-2018.pdf

Maria, K. (2015). Banks Get Attacked Four Times More Than Other Industries. Available: http://www.csoonline.com/article/2938767/advanced-persistent-threats/report-banks-get-attacked-four-times- more-than-other-industries.html

Navjeet, K. (2015). A Survey on Online Banking System Attacks and its Countermeasures. International Journal of Computer Science and Network Security, vol.15, no.3, 57-61.

Protiviti (2019). Embracing the Next Generation of Internal Auditing. *Protiviti*. [Online]. Available: https://www.protiviti.com/sites/default/files/united_states/insights/2019-ia-capabilities-and-needs-survey-protiviti.pdf

Soni, R.R, & Soni, N. (2013). An Investigative Study of Banking Cyber Frauds with Special Reference to Private and Public Sector Banks, Research Journal of Management Sciences, vol. 2,no.7, ISSN 2319–1171, 22-27. Available: http://paper.ijcsns.org/07_book/201503/20150310.pdf

Stefan, B., Edward, W. N. B. (2017). From Information Security Awareness to Reasoned Compliant Action: Analyzing Information Security Policy Compliance in a Large Banking Organization. The DATA BASE for Advances in Information Systems, VOLUME 48, NUMBER 3, 44-68.

Thomas, M. (2017). Adopting GDPR Using COBIT-5 (ISACA). [Online]. Available: https://www.isaca.org/bookstore/bookstore-wht_papers-digital/whpgdpr

Zarka, Z., Moin, U., & Karuna, S. (2016). Challenges in Privacy and Security in Banking Sector and Related Countermeasures. International Journal of Computer Applications (0975 – 8887), 24-35.

7. APPENDIX

Google drive link for all the deliverables:

https://drive.google.com/drive/folders/1KOPKYWBz3akMd3-LZThl00v9AXJzCTJs?usp=sharing