Sudan University of Science and Technology

College of Graduate Studies

A Conceptual Framework of Digital Government for the Success of Whistleblowing in Public Organizations

إطار مفاهيمي للحكومة الرقمية لإنجاح "دق ناقوس الخطر" في المنظمات العامة

A PhD thesis submitted to the College of Graduate Studies in partial fulfillment of the Requirements of the Degree of

Doctor of Philosophy in Computer Science

By

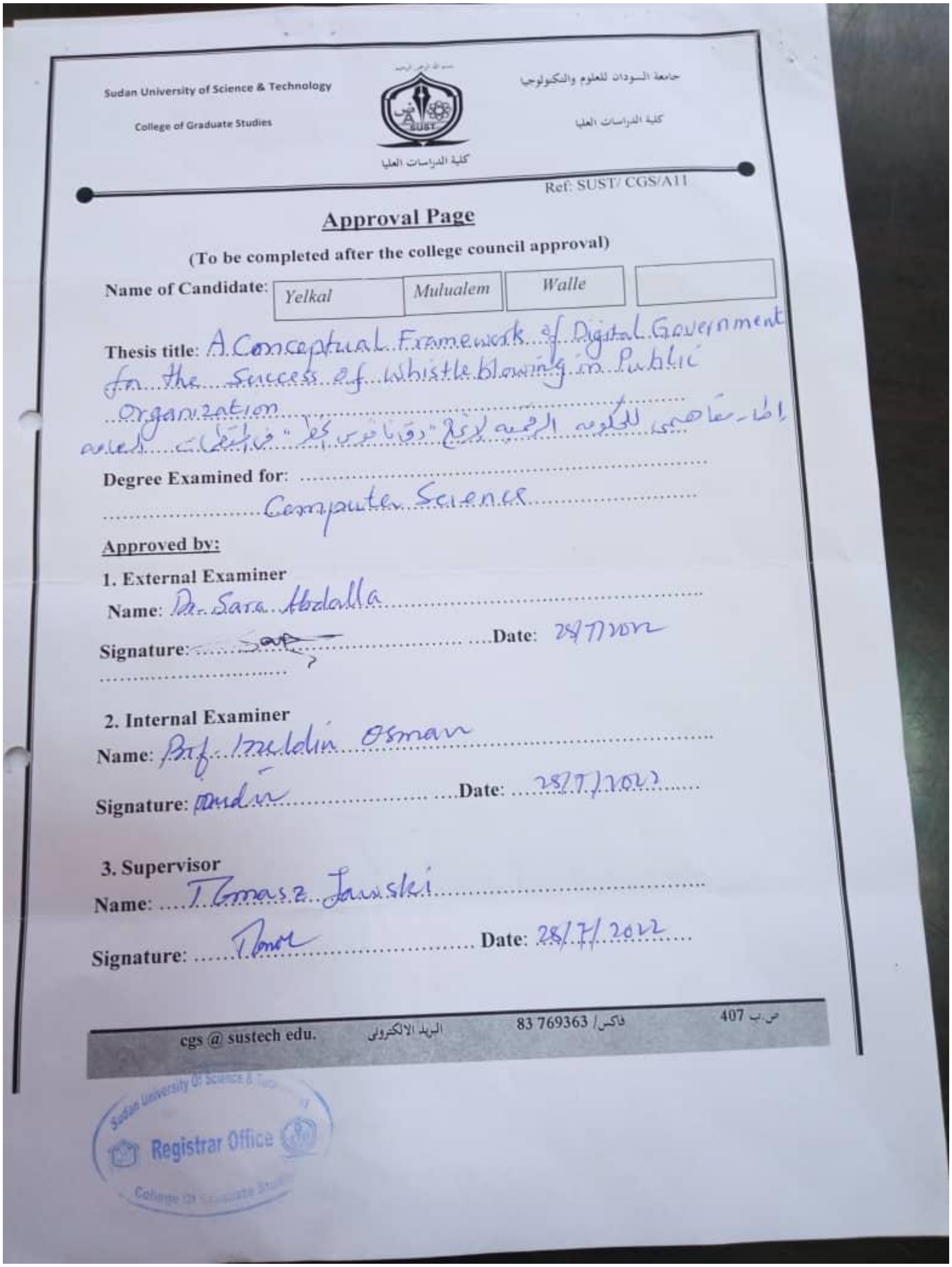
Yelkal Mulualem Walle

Supervisors:

Professor Tomasz Janowski

Professor Elsa Estevez

October, 2022



Sudan University of Science & Technology

College of Graduate Studies

بسم الله الرحمن الرحيم

SUST

كلية الدراسات العليا

جامعة السودان للعلوم والتكنولوجيا

كلية الدراسات العليا

Ref: SUST/ CGS/A11

Approval Page

(To be completed after the college council approval)

Name of Candidate:	*Yelkal*	*Mulualem*	*Walle*	

Thesis title: A Conceptual Framework of Digital Government for the Success of Whistle blowing in Public organization

اطار مفاهيمي للحكومة الرقمية لنجاح "دق ناقوس الخطر" في المنظمات العامة

Degree Examined for: Computer Science

Approved by:

1. External Examiner

Name: Dr. Sara Abdalla

Signature: .... Date: 28/7/2022

2. Internal Examiner

Name: Prof. Izzeldin Osman

Signature: Osman .... Date: 28/7/2022

3. Supervisor

Name: Tomasz Janski

Signature: .... Date: 28/7/2022

cgs @ sustech edu. البريد الالكتروني

فاكس/ 83 769363

ص.ب 407

DECLARATION

To the best of my knowledge and belief, this dissertation contains no material previously published by any other except where due acknowledgment has been made.

This dissertation contains no material which has been accepted for the award of any other degree or diploma in any university.

Yelkal Mulualem Walle ____________________

20 October, 2022

ASSIGNING COPYRIGHT DECLARATION

The Parties. This copyright Assignment Agreement made on October 20, 2022 (Effective date”) is by and between:

Assignor: Yelkal Mulualem Walle

Assignee: College of Graduate studies, with mailing address Sudan University of Science and Technology (SUST).

The assignor assigns to the Assignee (CGS) of all full copyright of this PhD thesis work.

Yelkal Mulualem Walle ________________ 20-10-2022

Assignor’s Name **Signature** **Date**

ACKNOWLEDGMENT

It has been an enjoyable and unforgettable experience to undertake my doctoral research program, which I hope will be a starting point of doing further research. However, this thesis would not have been possible without the guidance and help of several individuals who assisted in the preparation and completion of this study and some of whose names deserve special mention. Firstly, my sincere thanks and deep gratitude goes to both my supervisors, Professor Tomasz Janowski and Professor Elsa Estevez for their whole-hearted encouragement, support and guidance throughout the development of this thesis. Their wide knowledge, constructive comments and logical way of thinking have been of great value. Without their understanding, patience, and continuous support, this piece of work would never have been completed.

I would also like to express my gratitude to all staff at the College of Computer Science and Information Technology at Sudan University of Science and Technology for their guidance and considerable assistance in the completion of this research.

My sincere appreciation is extended to both of my parents, Mulualem Walle and Belaynesh Demewez. I also owe special thanks to my beloved brothers, Yabibal Mulualem and Solomon Mulualem, and my beloved sisters, Saba Mulualem and Zena Mulualem, for their love, encouragement, and moral support. Above all, my appreciation to God the Almighty for giving me the ability to undertake the endeavor of conducting this research and preparing this thesis.

Finally, my special thank goes to all my friends; thank you for your friendship and to my wife, Firehiwot Abebaw and my two lovely kids, Bisrta Yelkal and Bahiran Yelkal, thank you for giving me the encouragement, love and endless support to finish my thesis.

ABSTRACT

In recent years, there has been an increase in the development and adoption of Digital Government (DGOV) - the use of digital technology to transform public sector organizations and their interaction and engagement with citizens, businesses and each other - as such adoption causes major changes in the overall social, economic and political practice and processes carried out by governments. Whistleblowing (WB) - the disclosure by organization members (former or current) of illegal, immoral, or illegitimate practices under the control of their employers, to persons or organizations that may be able to effect action - is nowadays considered by many organization as the ultimate line of defense for safeguarding the public interest and a successful strategic approach to minimize workplace misconduct. While considerable efforts have been devoted to DGOV and WB separately, research work at the intersection of these two domains is very scarce; hence a systematic DGOV for WB (DGOV4WB) research framework has yet to emerge. This research aims to study the influence of Digital Government on whistleblowing. This study adopted mixed - qualitative and quantitative research methods. Qualitative methods, particularly the explanatory case study, extensive research literature review, policy literature review and whistleblowing legislation review, were used to explore the nature of whistleblowing, to conceptualize the performance measurement framework and the impact of digital technology and digital government on it and to develop Digital Government Innovation cause-effect framework for the whistleblowing domain based on Janowski. The DGOV4WB research framework is validated through the analyses of four case studies of existing DGOV initiatives that transform whistleblowing. Quantitative methods, were also used to develop a successful model of the Ethiopian Digital Government whistleblowing initiatives to assist Ethiopians with more efficient and cost-effective whistleblowing operations. Factors affecting the adoption and effective utilisation of Digital Government whistleblowing initiatives were identified through the literature. Following this, strategies were proposed which led to the development of a framework through TAM model that will assist to increase the adoption and effective use of Digital Government amongst public organizations whistleblowing initiatives in Ethiopia. This model was validated via a survey and analysed with the aid of SPSS software. Data was collected using a survey applied to a sample of 554 citizens (from public organizations) and data analysis involved linear regression statistical technique. The results showed that the core constructs of the TAM have strong influences on user intention towards Digital Government Whistleblowing System - a service that enables employees and third party suppliers to report malpractice, unlawful or unethical behaviour within the workplace. In addition, findings suggest that whistleblowing system quality is a factor that influences their behavior toward the use of Digital Government whistleblowing system in Ethiopia public organizations. This research offers recommendations that will assist the researchers and Ethiopian government /public organizations in resolving the problems in a fight against fraudulent and corruption activities through Digital Government whistleblowing systems.

الـمستخلص

في السنوات الأخيرة ، كانت هناك زيادة في تطوير واعتماد الحكومة الرقمية(استخدام التكنولوجيا الرقمية لتحويل مؤسسات القطاع العام وتفاعلها ومشاركتها مع المواطنين والشركات وبعضها البعض - حيث يؤدي هذا التبني إلى تغييرات كبيرة في الممارسات والعمليات الإجتماعية واالاقتصادية والسياسية الشاملة التي تقوم بها الحكومات. الإبلاغ عن المخالفات "دق ناقوس الخطر"هو إفشاء أعضاء المنظمة السابقين أو الحاليين عن الممارسات غير القانونية أو غير الأخلاقية اأو غير المشروعة الخاضعة لسيطرة أصحاب العمل، إلى الأشخاص أو المنظمات التي قد تكون قادرة على تنفيذ إجراءآت تجد منهذه الممارسات وفي القت الحاضر تعتبر كثير من المنظمات دق ناقوس الخطر بمثابة خط الدفاع النهائي عن حماية المصلحة العامة ونهج استراتيجي ناجح لتقليل سوء السلوك في مكان العمل. وعلى الرغم من انه تم تكريس جهود كبيرة بشكل منفصل، فإن العمل البحثي عند تقاطع هذين المجالين نادر للغاية؛ ومن ثم، لم يظهر بعد إطار عمل بحثي منتظم . يهدف هذا البحث إلى دراسة تأثير الحكومة الرقمية على الإبلاغ عن المخالفات عن طريق دق ناقوس الخطر وتأثير الحكومة الرقمية علي دق ناقوس الخطر.اعتمدت هذه الدراسة أساليب بحثية مختلطة - نوعيّة وكميّة. تم استخدام الأساليب النوعية ، ولاسيما دراسة الحالة التفسيرية ، والمراجعة الشاملة لأدبيات البحث ، ومراجعة الأدبيات المتعلقة بالسياسات ، ومراجعة تشريعات التبليغ عن المخالفات (دق ناقوس الخطر)، واستكشاف طبيعة التبليغ عن المخالفات ، ووضع تصور لاطار قياس أداء وتأثير التكنولوجيا الرقمية والحكومة الرقمية عليه. وتطوير إطار عمل مبني علي اليبب والنتيجة لابتكارات الحكومة الرقمية في مجال الإبلاغ عن المخالفات وفقا لددراسة جاونسكي (2015). يتم التحقق من صحة إطار بحث(الحكومة الألكترونية لاجل نجاح الإبلاغ عن المخالفات) من خلال تحليل أربع دراسات حالة لمبادرات حكومة رقمية حالية تعالج عملية الإبلاغ عن المخالفات . كما تم استخدام الأساليب الكمية لتطوير نموذج ناجح لمبادرات الإبلاغ عن المخالفات للحكومة الإثيوبية الرقمية لمساعدة الأثيوبين في عمليات الإبلاغ عن المخالفات بطريقة أكثر كفاءة وفعالية من حيث التكلفة. تم تحديد العوامل التي تؤثر على تبني مبادرات الإبلاغ عن المخالفات للحكومة الرقمية واستخدامها الفعال من خلال الأدبيات. بعد ذلك، تم اقتراح استراتيجيات أدت إلى تطوير إطار عمل من خالل نموذج " TAM"والذي سيساعد على زيادة اعتماد الحكومة الرقمية واستخدامها الفعال بين المنظمات العامة في مبادرات الإبلاغ عن المخالفات في إثيوبيا. تم التحقق من صحة هذا النموذج عبر مسح وتحليل بمساعدة برنامج. SPSS تم جمع البيانات باستخدام مسح تم تطبيقه على عينة من 555 مواطنًا (من المؤسسات العامة) وتحليل البيانات باستخدام تقنية الانحدار الخطي الإحصائية. أظهرت النتائج أن التركيبات الأساسية لـ " TAM"لها تأثيرات قوية على دوافع المستخدم تجاه نظام الحكومة الرقمية وهي خدمة تمّكن المبلغ عن المخالفات للحكومة الرقمية - و الموظفين وموردي الطرف الثالث من الإبلاغ عن سوء التصرف أو السلوك غير القانوني أو غير الأخلاقي داخل مكان العمل. وبالإضافة إلى ذلك ، تشير النتائج إلى أن جودة نظام الإبلاغ عن المخالفات هو عامل يؤثر على سلوكهم تجاه استخدام نظام الإبلاغ عن المخالفات للحكومة الرقمية في المؤسسات العامة في إثيوبيا .يقدم هذا البحث توصيات من شأنها مساعدة الباحثين والحكومة الإثيوبية / المنظمات العامة في حل المشكلات في مكافحة أنشطة الاحتيال والفساد من خلال أنظمة التبليغ عن المخالفات الحكومية الرقمية.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF SYMBOLS / ABBREVIATIONS

ATT	Attitude towards Behavior
BI	Behavioral Intention
DGOV	Digital Government
DGOV4WB	Digital Government for Whistleblowing
DT	Digital Technology
DT4WB	Digital Technology for Whistleblowing
ICT	Information Communication Technology
IQ	Information Quality
MoMP	Ethiopian Ministry of Mines and Petroleum
OECD	Organisation for Economic Co-Operation and Development
PEU	Perceived Ease of Use
PG	Public Governance
PG4WB	Public Governance for Whistleblowing
PU	Perceived Usefulness
SN	Subjective Norm
TAM	Technology Acceptance Model
TI	Transparency International
WSQ	Whistleblowing System Quality
WB	Whistleblowing

LIST OF APPENDICES

CHAPTER I

INTRODUCTION

1.0. Introduction

The first chapter presents the general overview of the research. It explains the background of the study and its aim, the rational of the study, the methodology adopted, significance of the study and the inadequacies of previous study from the literature reviewed. The chapter finishes off with an outline of the thesis structure. Chapter one thus serves as a general introduction to the whole thesis.

1.1. Background of the Study

In recent years, the increase use of Digital Government - the use of digital technologies, such as mobility, social media, big data, analytics and cloud in public governance of an organization - helps to drive deep reform of services, processes, and technologies; and to embrace good government principles and achieve policy goals (OECD, 2016a). From a technical perspective, the Digital Government is a government of new digital technologies to enable the business to flourish, increase citizen engagement, and drive economic growth and to make public institutions more inclusive, effective, accountable, and transparent (Huawei. 2019). Most specifically, Jaeger (2003) states that digital technology transforms government information and services' one-way street into a two-way relationship in which individuals, enterprises, and governments are actively engaged with each other (Jaeger, 2003).

Accenture (2015) states that Digital Government is a profound element in the modernization of any government, acting as a means of improving transparency, accountability, and good governance; engage citizens and make public services more as efficient and as effective as possible through the use of digital technologies. OECD (2016a) further states that the use of digital technologies in government is transforming today’s societies and economies. It offers a great opportunity for governments to engage much more deeply with citizens and significantly enhance the quality of service delivery.

Effective and operational Digital Government facilitates better and more responsive, efficient, effective and equitable delivery of public service to all people, promotes productivity among public servants, building public trust and ensuring a greater public sector transparency and accountability, encourages the participation of citizens in government, and empowers all citizens (UNDESA, 2019). Furthermore, UNDESA (2019) also added Digital Government can play a significant role in building efficient, inclusive and transparent institutions to support policymaking and service delivery. It helps to enhance economic competitiveness, economic growth and job creation, forge new levels of engagement and trust, and greater efficiency and productivity for public and private sector organisations (OECD, 2016a).

Whistleblowing, disclosure of information by an employee or contractor alleging willful misconduct by an individual or individuals within an organization, is an important means of improving government transparency and accountability (Figg, 2000; Carmen & Chang, 2011). Near and Miceli (1995) stated that whistleblowing is considered to be among the most effective means of exposing and remedying corruption, fraud and other types of wrongdoing in the public and private sectors (Near & Miceli, 1995).

In the digital world, Digital Government is recognized as a tool to help reinvent the public sectors by transforming internal government processes and structure, as well as external relationships with citizens and businesses (Accenture, 2015). In addition, research and experience shows that the use of digital technology reduces opportunities for corruption and discretion, e.g. by disintermediating services and allowing citizens to conduct transactions themselves (Pathak et al., 2009).

Digitally enabled whistleblowing system - a service that enables employees and third party suppliers to report malpractice, unlawful or unethical behaviour within the workplace - enables employees, third party suppliers, and citizens to report malpractice and unlawful or unethical behavior within the workplace (Libit, Freier & Draney, 2014; Brevini, 2017). Digital technologies offer a great opportunity to the government to design a scalable and flexible whistleblowing system and future-proof whistleblowing service to the customers - enabling citizens and businesses to access whistleblowing services and information as efficiently and as effectively through digital technologies. However, the widespread failure of Digital Government whistleblowing projects suggests that Digital Government also creates delusional hope. Developed countries such as Denmark, Australia, Republic of Korea, US and UK are still leading the world in the field of Digital Government (UNEGOV, 2018) and whistleblowing systems. The digital age holds the promise of new and powerful weapons in the arsenals of developing countries wrestling against fraud and corruption challenges. According to The UN Educational, Scientific and Cultural Organization (UNESCO), the literacy rates on the Sub Sharan African are still below 65% in 2018 and 27 % of the world’s illiterate people live in sub-Saharan with 17 countries in Africa still have literacy rates of 50 % and below (UNESCO, 2018). At the same time digital technology penetration is the lowest in the world. Considering the above context, Digital Government whistleblowing platforms that offers an outlet for more active governance to citizen and business involvement in government whistleblowing process would have much less cultural impact than they would in developed countries. Therefore, the impact and implications of Digital Government whistleblowing initiatives in developing countries need to be examined.

Technology Acceptance Model (TAM) explains how users adopt and use new technology by evaluating the factors that influenced the decision to accept a new technology (Davis, 1989). TAM is probably one of the most widely cited models in the field of technology acceptance. Table 2.2 shows the TAM application in different areas of technology, especially in developing countries. Despite a large amount of research in this area, few studies have applied the TAM to Digital Government implementation in African countries (Bwalya, 2009; Petersen et, al, 2019; Chemisto & Rivett, 2018; Mensah & Mi, 2017). However, there is no study uses the TAM model to explain and predict user acceptance on whistleblowing systems in Sub-Saharan African Countries. It is necessary to develop and establish empirical support for the TAM in explaining citizens.

The purposes of this study are five-fold. First, is to explore the benefits, challenges and possible routes to transform whistleblowing and whistleblower protection through digital technology, considering political, institutional, cultural and other environmental factors. i.e. The contribution of Digital Government for whistleblowing and whistleblower protection. Second, is to explore how to measure whistleblowing performance (to develop performance measurement framework) and how Digital Government can enhance the performance of whistleblowing and whistleblower protection. Third, to develop Digital Government innovation cause-effect framework for whistleblowing domain. Fourth, while prior research on the TAM and Digital Government focuses on developed countries, this study focuses on Digital Government whistleblowing systems in developing countries like Ethiopia, and how TAMs' impacts Digital Government whistleblowing systems success and the country's developmental aspiration. The researcher examine whether the environment influences the impacts that the TAM model can have for Digital Government whistleblowing initiatives, despite cultural differences. Fifth, to examines the various factors affecting the intentions of Ethiopian citizens to use Digital Government whistleblowing systems and surveys a sample of citizens in Ethiopia. The findings of this study can be repeated and extended to other sub-Saharan African countries to build a comprehensive picture of critical factors affecting citizen acceptance of Digital Government whistleblowing systems.

1.2. Definition of Terms

The key terms in this research are defined in sections 1.2.1 and 1.2.2 below.

1.2.1. Definition of Whistleblowing

There is no common legal definition of what constitutes whistleblowing. The International Labour Organization (ILO) defines it as “the reporting by employees or former employees of illegal, irregular, dangerous or unethical practices by employers” (ILO, 2005). Near & Miceli (1985) defines Whistleblowing as “the disclosure by organization members (former or current) of illegal, immoral, or illegitimate practices under the control of their employers, to persons or organizations that may be able to effect action”. Whistleblowing can act as an early warning to prevent damage as well as detect wrongdoing that may otherwise remain hidden. Council of Europe refers to whistleblowing as the act of someone reporting a concern or disclosing information on acts and omissions that represent a threat or harm to the public interest that they have come across in the course of their work; for example, harm to the users of a service, the wider public or the organization itself, or a breach of the law (CM, 2014).

1.2.2. Definition of Digital Government

Digital Government defined as the optimal use of electronic channels of communication and engagement to improve citizen satisfaction in service delivery, enhance economic competitiveness, forge new levels of engagement and trust, and increase productivity of public services (Accenture, 2015). Accenture (2015) states that Digital Government encompasses the full range of digitalization—from the core digitalization of public services to the digital infrastructure, governance and processes, including both front- and back-office transformation needed to deliver the new service paradigm. The Organisation for Economic Co-operation and Development (OECD, 2014b) defines Digital Government as "the use of digital technologies, as an integrated part of governments' modernization strategies, to create public value". It relies on a Digital Government ecosystem composed of government actors, nongovernmental organizations, businesses, citizens' associations and individuals, which supports the production of and access to data, services and content through interactions with the government. Organizations improves how to operate, how to deliver services, and how to engage their stakeholders.

Further Smart Nation Digital Government Group (SNDGG) describes Digital Government through a six-fold strategy to build Digital Government. This entails: Integrating services around citizen and business needs; Strengthening integration between policy, operations and technology; Building common digital and data platforms; Operating reliable, resilient and secure systems; Raising our digital capabilities to pursue innovation; and Co-creating with citizens and businesses, and facilitating adoption of technology (SNDGG, 2018).

Corydon, Ganesan & Lundqvist (2016) analysis described a Digital Government has core capabilities supported by organizational enablers. This Capabilities involves the citizen and business facing innovations includes Services, Processes, Decisions, and Data sharing while organizational enablers involves innovations across government systems includes – Strategy; Governance and organization; Leadership, talent, and culture; and Technology.

According to Katsonis & Botros (2015) and Deloitte (2015), Digital Government enables governments to create more public value and public sector transformation - greater openness, transparency, engagement with and trust in government - through the integration of digital technologies and user preferences in service design and delivery of direct personal services and in shaping public policy outcomes.

1.3. Research Scope

The scope of this research focuses on the application of Digital Government (DGOV) on whistleblowing (WB) and whistleblower protection in particular in case of Ethiopia. I.e. A systematic DGOV for WB (DGOV4WB) research framework - the use of digital technology to foster governance of Whistleblowing and Whistleblowing Protection. The research investigates / identify the potential issues in whistleblowing domain and explore how Digital Government has been used to address these issues and further determines the impact of digital technology on public governance in the whistleblowing domain.

The research also determines the main contributing stakeholders in the whistleblowing domain, identify and model the relation of stakeholders with respect to the whistleblower; and examines the usage of digital technology by public authorities and other stakeholders as part of governance processes within the whistleblowing domain. This study developed a successful TAM model of the Ethiopian Digital Government whistleblower initiatives to assist Ethiopians with more efficient and cost-effective whistleblowing operations. This research concentrates on whistleblowing since it plays a vital role in the fight against corruption around the world in particular in Ethiopia.

1.4. Statement of Research Problem

Many organizations around the world are vulnerable to problems such as fraud, bribery and abuse, negligence, bullying, harassment and unethical behaviour that may cause financial and reputational harm to organizations if left unobserved and undetected (GFIR, 2018). The 2015/2016 Annual Global Fraud Survey shows that from the 2012/2013 survey, fraud cases increased by 14 percentage points (GFR, 2016). Researchers (Barkemeyer, Preussb & Lee, 2015; Alleyne & Watkins, 2017) suggest that by developing a proactive approach and including stakeholders in fostering an ethical workplace, an organization can significantly reduce financial liability and loss and preserve its strong corporate image on the marketplace. Global Fraud Study of the Associations of Certified Fraud Examiners (ACFE) states that the most common method of detecting fraud was through whistleblowers disclosure---about 39.1 percent of the (ACFE, 2016).

Different international organizations (OECD, 2016c; TI, 2013) and researchers (Figg, 2000; Apaza & Chang, 2011) indicate the importance of whistleblowing --- disclosure of information by an employee or contractor alleging wilful misconduct by an individual or individuals within an organization (Near & Miceli, 1985) --- in the fighting against fraudulent activities within the organization (EY, 2016). However, whistleblowing suffer from wide range of problems including anonymous and confidential reporting mechanism, monitoring of the whistleblowing process, and ways of confidential communication between different whistleblowing stakeholders including direct communication and training with all involved stakeholders (Apaza & Chang, 2011; Near & Miceli, 1985). This indicates that whistleblowers need strong legal protections to protect them from retaliation and enable them to report offences safely and freely (TI, 2013; Rothschild & Miethe, 1999).

To deal with some of the issues of the whistleblowers and whistleblowing, government and organizations around the world work intensively through developing a comprehensive whistleblowing polices with the aim i) to provide accessible and reliable channels to report wrongdoing and to encourage whistleblowers to report wrongdoing internally; and ii) to provide strong protection for whistleblowers from any types of retaliation within the organization (TI, 2013; Apaza & Chang, 2011). A key question for governments and organizations is how to make the whistleblowing program effective. As per (TI-NL, 2017), effective whistleblowing program needs to i) provide secured whistleblowing channel which can be accessible 7/24/365; ii) promote whistleblowing programs; iii) build free and transparent whistleblowing organizational culture and iv) protect whistleblowers in their administration.

In order to address some of the whistleblowing and government challenges stated above, governments and organizations have started to develop and use different types of whistleblowing programs strategically relying on the use of digital technologies. Underpinning such responses is an assumption that Digital Government could help in providing secured whistleblowing reporting channel. Such a channel could substantially transform the whistleblowing process by reducing victimization (retaliation) for whistleblowers. This assumption is based on the basic features of Digital Government developed by international organizations (OECD, 2003; TI, 2016; Accenture, 2015; Corydon, Ganesan & Lundqvist, 2016), and researchers (Kraemer & King, 2006; Hoetker, 2002; Bertot, Jaeger & Grimes, 2010; Intuit, 2017). Digital Government enables more effective and responsive delivery of public services, increases citizen participation, allows submitting reports anonymously (Emura et al., 2017), and provides greater access to information about whistleblowing laws, cases and decisions.

Increasingly, the use of digital technology to transform public administration organizations and their relationships with citizens, businesses and each other (i.e., Digital Government) (OECD, 2019) is recognized as a tool to help reinvent the public sector by transforming internal processes and systems of governments as well as their external ties with citizens and businesses (Fang, 2002; Seifert & Chung, 2008). This allows governments to provide services that meet the evolving expectations of citizens and businesses, and to be more accountable and transparent at global and national levels. It also provides secure online communications (Emura et al., 2017) that can have an impact on the protection of sources and whistleblowers.

While considerable efforts have been devoted to studying Digital Government (DGOV) and whistleblowing (WB) separately, research work at the intersection of these domains is very scarce as depicted in Table 1.1. Only a very few scholars investigated the possible contribution of technologies in whistleblowing and its side effects (Lam & Harcourt, 2019; Brevini, 2017; Heemsbergen, 2013) and a systematic DGOV4WB research framework is yet to emerge. Therefore, it is imperative to investigate the possible contribution of Digital Government as key implementation means for whistleblowing and whistleblower protection and examine the present situation of Digital Government whistleblowing initiatives in Ethiopia and give recommendations based on the findings of the research. In addition, the research conceptualizing whistleblowing performance and presents the performance measurement framework for whistleblowing and then explores the impacts of Digital Government on the framework by empirically analyzing four Digital Government whistleblowing initiative case studies.

Table 1. 1: Scopus Databases Search Publications Result

	Publication Year														
Key words	**< 2000**	**2004**	**2005**	**2006**	**2009**	**2010**	**2011**	**2012**	**2013**	**2014**	**2015**	**2016**	**2017**	**2018**	**Total**
Digital Government & Whistleblower	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Digital Government & Whistleblowing	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
E-government & Whistleblowing	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
E-government & Whistleblower	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Digital Technologies & Whistleblower	0	0	1	0	0	0	0	0	0	0	0	0	1	0	2
Digital Technologies & Whistleblowing	0	2	1	0	0	0	0	0	0	0	0	0	0	0	3
Technology & Whistleblowing	13	2	1	1	1	4	1	2	5	3	1	3	2	3	42
Technology & Whistleblower	2	0	2	1	0	1	1	1	2	1	5	3	1	2	22
ICT & Whistleblowing	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
ICT & Whistleblower	0	0	0	0	0	0	0	0	0	0	2	1	0	0	3

1.5. Research Aim

As a result of the issues identified in section 1.4, the primary aim of this research is to identify the contribution of Digital Government to whistleblowing and to recommend strategies that would assist in stimulating or increasing the adoption and utilisation of Digital Government in Whistleblowing process, particularly in Ethiopian context. The research loos at the current state of the art of the two domain areas (Digital Government and Whistleblowing) in the literature and develop a conceptual framework for integrating the two domains. The research also looks at the current level of Digital Government utilisation in government/ public organization whistleblowing process in Ethiopia. Likewise, it is important to determine the impact of Digital Government on the organisational whistleblowing performance.

Increasingly, the use of digital technology to transform public administration organizations and their relationships with citizens, businesses and each other (i.e., Digital Government) (OECD, 2019) is recognized as a tool to help reinvent the public sector by transforming internal processes and systems of governments as well as their external ties with citizens and businesses (Fang, 2002; Seifert & Chung, 2008). This allows governments to provide services that meet the evolving expectations of citizens and businesses, and to be more accountable and transparent at global and national levels. It also provides secure online communications (Emura et al., 2017) that can have an impact on the protection of sources and whistleblowers. An understanding of these concepts can provide an avenue for policy-makers, stakeholders and practitioners to stimulate the rate of Digital Government and utilisation within whistleblowing process.

1.6. Research Questions

Despite the presence of research findings and policy frameworks on whistleblowing and whistleblower protection, digital technology alone doesn’t address issues related to whistleblower protection. As stipulated in statement of the problem section, there is a research gap on the influence of the Digital Government on whistleblowing and whistleblower protection.

To achieve the research aim stated in Section 1.5, the following research questions have been formulated to guide this research which are comprised of the main research question as well as sub-research questions.

What is the influence of Digital Government on whistleblowing and whistleblower protection?

The main research question is expanded into four sub-questions:

i. How to conceptualize whistleblowing?
ii. How to measure the performance of whistleblowing?
iii. How can Digital Government enhance the performance of whistleblowing?
iv. What are the contributing factors affecting the intentions of Ethiopian citizens to use Digital Government whistleblowing systems?

1.7. Research Methodology

This section presents an overview of the research methodology applied in this research. The research used a mixed approach (qualitative and quantitative) where exploratory and descriptive nature of the research, a qualitative research approach, adopts to explore the interaction between Digital Government and whistleblowing domains. Nonetheless, a survey has been used to assess citizen adoption of Digital Government whistleblowing initiatives in Ethiopia. The research also employs a case study strategy which is appropriate for investigating a contemporary research phenomenon. Denzin and Lincoln (2011) stress that qualitative researchers study things in their natural settings, attempting to make sense of phenomena in terms of the meanings people bring to them.

A triangulated data collection method also adopted after conducting an extensive review of literature relevant to the topic under study. This involved the collection of data in two phases. In the first phase of the research, a survey utilising self-administered questionnaires was conducted to identify organizations to be interviewed and questioned and used as case studies. A five point Likert scale questionaries' with anchors of strongly disagree to strongly agree was used to measure each item of the other constructs in this study. The research seeks to understand the level of adoption and use of digital enabled whistleblowing initiatives by public organizations in Ethiopia.

Data analysis for the first phase of the research was undertaken using descriptive statistics as well as content analysis. Content analysis involves the numerical description of the features of a given text or series of images. According to Neuendorf (2019), content analysis offers a model for systematic qualitative analysis.

Generally, the methodology to be applied in this research comprises six main activities:

- Research Literature Review to identify and document the most significant research literature that shapes the whistleblowing and Digital Government domains, including quantitative and qualitative analysis based on narrative reviews of scientific publications;
- Policy Literature Review to identify and document the most significant policy literature in the area including recommendations, initiatives and experiences produced by major international organizations likes the UN or OECD;
- Case Study Development to document case studies of whistleblowing and whistleblower protection initiatives from around the world, including experiences of practitioners that implemented such initiatives;
- A conceptual framework to guide the process of planning, development and evaluation of technology-enabled whistleblower protection based on the inputs obtained from research literature review, policy literature review and case study development;
- Digital Government case-effect framework to identify pressures on organizational authorities on whistleblowing domain and determined how the public authorities respond to such pressures by innovation in their policies, processes, services and structures using existing digital technologies;
- Whistleblowing system performance measurement framework to measure the contribution Digital Government on the performance of whistleblowing system; and
- Developing TAM model for whistleblowing initiatives and assessing the use and adoption of digital enabled whistleblowing initiatives in Ethiopia.

1.8. Significance of the Study

In 2013, Gold stats that “Despite the undeniably important role that whistleblowers play in the service of promoting justice and accountability, the legal protections that exist to support employees of conscience largely fail to either encourage employees to serve as enforcement mechanisms for existing laws or to protect them if they suffer retaliation for raising concerns.” (Gold, 2013).

Increasingly, governance processes are supported by digital technology, with new governance paradigms emerging due to digitization, globalization and increasing influence of non-governmental organizations. These include enhanced mechanisms for government wide coordination in policy and information exchange (OECD, 2003).

Digital Government, i.e. the use of digital technology by the government for the provision of information and public services to the people, is being implemented in more areas of government administration at local and national levels worldwide. While it was initially promoted as a means of improving internal management efficiency in public administration, Digital Government is increasingly considered an important measure for enhancing citizen access to government services and expediting the delivery of services to citizens (Grönlund & Horan, 2005; OECD, 2003). Even though Digital Government's potential to increase transparency and combat corruption in government administration is gaining popularity among practitioners and researchers, the impact of digital technology on whistleblower protection is still under-researched. Thus, this research can generate an empirically-grounded understanding of how Digital Government interventions can be used to enable whistleblower protection mechanisms.

The results will have significant implications for practitioners, especially in the area of technology-enabled whistleblowing and whistleblower protection. It is intended that the quantitative phase of the study will contribute to understand various factors affecting the intentions of Ethiopian citizens to use Digital Government whistleblowing systems to fight administrative corruption whilst the qualitative study will add to the body of literature.

1.9. Contribution

The OECD policy recommendations show that whistleblowing legislation need to refer to channels by which protected disclosures can be made. These includes internal disclosures, external disclosures to a designated body, and external disclosures to the public. It is also recommended to encourage protected reporting mechanisms and to raise awareness through training, newsletters, and information sessions about reporting channels and procedures to facilitate disclosures (OECD, 2016a) through which digital technology and Digital Government can play a crucial role in anonymity and information dissemination to raise awareness.

A number of significant contributions that advance the state of the art in technology-enabled whistleblowing process are also expected:

- The findings from the quantitative analysis of technology-enabled whistleblowing research;
- Identification of policy instruments and tools for whistleblower protection and a repository of legislative instruments for whistleblower protection enacted by governments and international organizations from around the world;
- Performance measurement framework for whistleblowing process and identifying where Digital Government can enhance the performance of whistleblowing process.
- A conceptual framework of Digital Government enabled whistleblowing and whistleblower protection including instances for each theoretical construct (problem to solution mapping);
- Empirical research that shows the level of technology adoption for whistleblowing around the world and particularly in Ethiopia and identifies factors affecting the intentions of Ethiopian citizens to use Digital Government whistleblowing systems.
- A framework for defining a research agenda for technology-enabled whistleblowing process and populating this agenda with illustrative research problems.

Generally, the contribution of this research will be three-fold: contributions to the general body of knowledge, practical contributions and methodological contributions. In terms of contributions to the general body of knowledge, this research will have significant implications for Digital Government research which seeks to understand and explain the issues surrounding whistleblowing in terms of their adoption and effective use of digital technology (Fedorowicz & Dias, 2010). Since this research sets out to investigate the impact of digitization within organizational contexts, its findings will be aimed at providing a deeper understanding of the issues associated with the adoption and utilization of digital technology for performance improvement in whistleblowing and whistleblower protection. In order words, the research will contribute to knowledge by developing an evidence-based report that describes the level of technology adoption for whistleblowing and whistleblower protection mechanism in general and for Ethiopia in particular. Full description discussed in final chapter.

1.10. Structure of the Thesis

Chapter 2 focuses on a review of the literature in order to define the scope of the research. It considers previous research on Whistleblowing Domain and Digital Government Domain, and provides background information on the use of Digital Government by organizations in their whistleblowing process.

Chapter 3 discusses on the conceptual framework of the research and its research hypotheses. The chapter presents the proposed model of using Digital Government in whistleblowing, with an overview of the use of Digital Government for effective whistleblowing program is presented.

Chapter 4 discusses the research methodology and evaluates the selection of the research method adopted that are relevant to this study. The chapter also outlines the underlying research assumptions that guide Digital Government research and justifies the choice of a mixed (qualitative and quantitative) research methodology. In addition, the research design, rationale for the chosen approach and its suitability for the research are discussed. The design of the research process is presented in a diagrammatical form (flowchart) which shows the development of the thesis.

Chapter 5 presents the analysis and findings of the first phase (multiple case studies) and the second phase systematic literature reviews of the research. The chapter includes background and objective information on the cases that participated in the study. In addition, emerging themes from the case studies and results of the findings are presented.

Chapter 6 discusses the research findings and relates them to the existing literature. Whistleblowing system performance measurement framework and Digital Government contribution on the performance of whistleblowing system, Digital Government cause-effect framework is proposed in this chapter.

Chapter 7 summarizes the overall findings of the research. The chapter presents the research outcomes including the achievement of the research questions. Subsequently, the chapter provides the contributions made by the research, specifically focusing on Digital Government contribution in whistleblowing system and utilisation amongst public organizations within Ethiopia. The limitations of the research are also presented and finally some areas for further research were identified.

1.11. Summary

Chapter one describes the background of the research and presented the aim of the research. The chapter has also reviewed research literatures that provides a background to the research and has put forward the research questions. The research literature review shows that there is an increasing demand for research on investigating the impact of Digital Government for whistleblowing and whistleblower protection and assessing the use and adoption of digital enabled whistleblowing initiatives in developing countries, Ethiopia in particular. The definition of key terms (Digital Government and whistleblowing) were presented and the statement of the problem for the research was presented in this chapter. Furthermore, the chapter has briefly presented an overview of the research methodology. In addition, the significance of the research was discussed which highlighted the proposed contributions of the study.

CHAPTER II

LITERATURE REVIEW

2.0. Introduction

This section contains an in depth analysis of the literature that shapes this research. The literature covered includes the definition of whistleblowing and whistleblower, a discussion on whistleblower protection, and a review of international conventions on whistleblower protection. Finally, the later part of the section reviews the effect of digital technology on whistleblowing followed by how Digital Government can strengthen whistleblowing and whistleblower protection.

2.1. Whistleblower and Whistleblowing

In strengthening internal governance controls, organizations are encouraged to facilitate organizational citizenship behaviors such as whistleblowing, by influencing development of an organizational culture that facilitates employee communication, questioning, and reporting of corporate misconduct (Lachman, 2008). Berry (2004) pointed out that enhancing employee reporting builds trust, enables early detection of organizational wrongdoing, and facilitates development of an ethical work environment (Berry, 2004). Mesmer-Magnus & Viswesvaran (2005) also state that organizational employees have three options to address unsatisfactory situations faced within an organization: i) to exit the organization, ii) to voice discontent including to blow the whistle, or iii) to remain silent (Mesmer-Magnus & Viswesvaran, 2005).

The term whistleblowing is derived from the sporting events where a referee blows the whistle to stop an illegal or foul play (Qusqas & Kleiner, 2001). Even though researchers from different disciplines define whistleblowing in various ways, the more widely accepted and most frequently used definition of whistleblowing in accounting research is by Near and Miceli (1985). They define whistleblowing as “the disclosure by organization members (former or current) of illegal, immoral, or illegitimate practices under the control of their employers, to persons or organizations that may be able to effect action" (Near & Miceli 1985, Figg 2000). Whistleblowing is considered as an avenue for maintaining integrity by speaking one's truth about what is right and what is wrong in an organization. It is a strategy for asserting rights, protecting interests, influencing justice, and righting wrongs (Berry, 2004).

Whistleblowers can generally be defined as employees who have and report insider knowledge of illegal or unethical activities occurring in an organization (Cohen, 2017). Whistleblowers can be also suppliers, contractors, clients or any individuals who somehow becomes aware of illegal or unethical activities taking place in a business either through witnessing the behavior or being told about it, and they might disclose this internally or externally (Gold 2013, Devine & Maassarani, 2011).

Cohen (2017) generally classified whistleblowers into two categories. First, a whistleblower may be a person that has information about wrongdoing that is being committed by an employees or management in an organization. In this case, a person blows the whistle because: i) they personally believe that the wrongdoing is unethical and/or ii) they are incentivized by the prospect of receiving a financial reward. Secondly, a whistleblower might also be a person who is personally engaged in the wrongdoing with other colleagues and/or with the prior knowledge or direction of management. In this case, a person may blow the whistle for other reasons: i) they may have been unfairly pressured to engage in the wrongdoing; ii) they personally believe that the wrongdoing is unethical; iii) they fear the repercussions of being caught by law enforcement agencies; or iv) they seek to obtain a personal benefit such as a reward or a reduction in penalties for violating the law, e.g. a reduced prison sentence or fine.

Whistleblowers enhances corporate and government accountability by being the first line of defense against wrongdoing, and it is recognizes as one of the most effective and powerful tools for protecting the public interest (OECD, 2016c & 2012). As insiders, whistleblowers are the source of valuable information that neither the government nor the public can get from the oversight systems. They are knowledgeable people who know precisely what their organizations are doing. Therefore, whistleblowing is an important means of improving government transparency and accountability (Jos, 1991; Rosen, 1998; Rosenbloom, 2003).

2.2. Types of Whistleblowing

While whistleblowing includes disclosures which are both internal or external to the organization, Miceli and Near (1987) pointed out that organizations benefits when employees choose to report internally since it facilitates early detection of misconduct and creates opportunities for timely investigation and corrective action which helps an organization to proactively manage, or even avoid public embarrassment, government scrutiny, costly fines, or litigation. However, an employee's decision to report individual or organizational misconduct is a complex phenomenon that is based upon organizational, situational or personal factors (Miceli et al., 1987). Research suggests that nearly all whistleblowers initially attempt to report wrongdoing via internal channels before utilizing external channels (Miceli & Near, 1992, 2002). Even though whistleblowing via internal channels is less threatening to an organization as compared with external channels which threatens public scrutiny or legal intervention, whistleblowing within an organization is often unwelcome (Miceli et al., 1991a). Rather, whistleblower reports of wrongdoing are frequently buried or ignored (Miceli et al., 1991b).

In their detailed literature analysis Near and Miceli (1992) identified four characteristics of whistleblowers. 1) Whistleblower should be a member of the organization to which wrongdoing is attributed at some point in time and blowing the whistle can be made after may leaving the organization (Elliston 1982). 2) Whistle-blower can be an individual who does not have an authority to stop illegal activities within the organization and it led to blow the whistle to change the wrong activities through other informal bases of power (Elliston 1982a; Weinstein 1979). 3) Sometimes whistleblower want to be anonymous through the immergence of anonymous hotlines and this could affect the credibility with which it received. 4) Some whistleblowers may occupy roles where such wrongful activity is prescribed.

The impact assessment for European commission staff working document explores the distinction between whistleblowers and complainants based on public and privet interest –"*Whistleblowers are individuals who report violations which affect the public interest and complainants could include aggrieved workers, whose reports relate to personal grievances or breaches of individual working conditions*" (EU, 2018). Whistleblowers are also to be distinguished from complainants who might be clients or citizen bystanders and who do not fear retaliation in relation to their complaint. The key distinguishing criterion is the lack of work-based connection between the latter and the reported person (EU, 2018). It is because of their work-based relationship and the related risk of sanctions – for example, for breaching the duty of confidentiality – that whistleblowers require specific legal protection, so that they can feel safe to "raise the alarm". When there is no a power imbalance between the reporting and the reported person, there is no need for protection against retaliation. Figure 2.1 shows the Relationship of individual to the institution responsible for/involved in the wrongdoing.

A number of researcher's have discussed on the difference between internal versus external whistleblowing approaches, and identified versus anonymous whistleblowing (Dworkin and Baucus, 1998; Grant, 2002; Park et al., 2005). According to Park et al., whistleblowers have different attitudes toward how to blow the whistle and they need to consider three basic whistleblowing route (dimensions) concerns before blowing the whistle.

1) Formal whistleblowing versus informal whistleblowing

Whistleblower in an organization could use either of the two whistleblowing communication types (Park et al., 2005). It involves the communication channel or procedure used for reporting wrongdoing activities in an organization. Formal whistleblowing is an institutional form of reporting wrongdoing and the communication is through pre-defined channels set by organizations (Mehrotra, 2019; EU, 2018). The whistleblower should following the standard lines of communication or a formal organizational protocol for reporting unlawful activities. It is backed by organizational procedure, and it is necessary to fulfill the goals of the organization. In Informal whistleblowing, the whistleblower could disseminate the information (unlawful activities) in any direction or speak up the wrongful activities to colleagues or for anyone who has a trust without following the organization communication standard.

Types of wrongdoing

	Internal Insiders to the institution (employees, contractors, volunteers, board members, members, recent former insiders, existing insiders).	**External** Clients, consumers and citizens bystanders with no particular work dependence or vulnerability to the institutions
Violations or wrongdoing affecting one individual only	***Aggrieved Workers***	***Complaints***
Violations or wrongdoing affecting group of individual **(Public interest)**	***Whistleblowers***	
Violations or wrongdoing affecting most or all the society **(Public interest)**		

Figure 2. 1: Relationship of individual to the institution (EU, 2018)

2) Anonymous vs Identified whistleblowing

This classification is based on whether the whistleblower provides his/her identities when they report the wrongdoing activities (Park et al., 2005). Anonymous whistleblowing is reporting wrongdoing activities without exposing whistleblower personal information or identities, whereas in Identified whistleblowing the whistleblower provides real name other personal information's that could help to identify the whistleblower in reporting of a wrongdoing (Mehrotra, 2019; EU, 2018).

3) Internal vs External whistleblowing

Internal whistleblowing is reporting misconduct in their organization to appropriate persons or other employees within the workplace or organization who they believes can correct the wrongdoing activities (Park et al., 2005). This can includes either or not the person has formal responsibility for correcting the wrongdoing. Externally whistleblowing is reporting the wrongdoing activities to outside stakeholders or agencies believed to have the necessary power to correct the wrongdoing such as the media, government agencies, and consumer groups. External whistleblowers report misconduct of an organization to outside persons and agencies like lawyers, mass media, law enforcement, or watchdog agencies (Mehrotra, 2019; EU, 2018).

Based on the above three basic whistleblowing route (dimensions), it leads eight conceptually distinct ways to blow the whistle as shown in the Figure 2.2 and their specific types of whistlblowing and their definitions is shown in table 2.1.

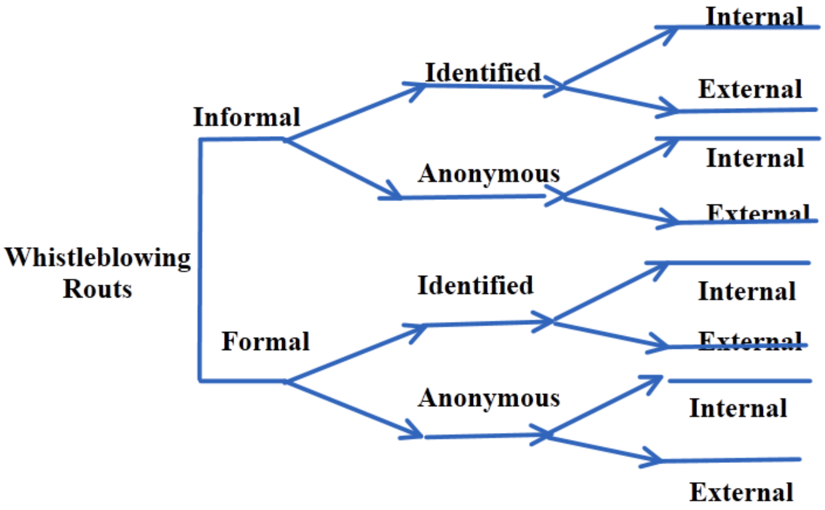


Figure 2. 2: Whistleblowing Routs (Park et al., 2005)

Table 2. 1: Types of whistleblowing and their definitions

No	Types of whistleblowing	Description
1	Formal, Anonymous, internal	Reporting concerns / wrongdoings anonymously without identifying the identity to the appropriate persons within the workplace or organization through organizational official reporting channels (Mehrotra, 2019; EU, 2018; Park et al., 2005). E.g Leaving message through organization hotlines
2	Formal, Anonymous, External	Reporting concerns / wrongdoings anonymously without identifying the identity to outside stakeholders such as the media, government agencies, and consumer groups through their official reporting channels (Mehrotra, 2019; EU, 2018; Park et al., 2005). E.g. Reporting Fraudulent activities to Media through their reporting channels email, hotline
3	Formal, Identified, internal	Reports concerns / wrongdoing by giving detailed information about himself to the appropriate persons within the workplace or organization through organizational official reporting channels (Mehrotra, 2019; EU, 2018; Park et al., 2005). E.g. Raising concerns to the top managers of organization in regular Meeting.
4	Formal, Identified, external	Reporting concerns / wrongdoings by giving detailed information about himself to outside stakeholders such as the media, government agencies, and consumer groups through their official reporting channels (Mehrotra, 2019; EU, 2018; Park et al., 2005). E.g. Raising concerns to the controllers; approaching a MP; speaking to a journalist and media outlets when they got a chance to speak up following the organizational norm.
5	Informal, Anonymous, internal	Reporting concerns / wrongdoings anonymously without identifying the identity to the appropriate persons within the workplace or organization through informal communication –

		without using organizational official reporting channels (Mehrotra, 2019; EU, 2018; Park et al., 2005). E.g. Unidentified email sent to organization Top managers personal email.
6	Informal, Anonymous, External	Reporting concerns / wrongdoings anonymously without identifying the identity to outside stakeholders such as the media, government agencies, and consumer groups through informal communication – without using organizational official reporting channels (Mehrotra, 2019; EU, 2018; Park et al., 2005). E.g. Reporting Fraudulent activities - secret information - to outsider's likes of Media outlets and low enforcement body through the use secured reporting channels like anonymous web postings, email, hotline without giving detail personal information's.
7	Informal, Identified, internal	Reports concerns / wrongdoing by giving detailed information about himself /herself to the appropriate persons within the workplace or organization through informal communication – without using organizational official reporting channels (Mehrotra, 2019; EU, 2018; Park et al., 2005). E.g. Raising and discuss concerns with a colleague.
8	Informal, Identified, external	Reporting concerns / wrongdoings by giving detailed information about himself to outside stakeholders such as the media, government agencies, and consumer groups through informal communication – without using organizational official reporting channels (Mehrotra, 2019; EU, 2018; Park et al., 2005). E.g. Speak up wrongful activities to social media or exposing and criticizing the activities in social media.

When to blow the whistle?

The idea of wrongdoing, which goes beyond criminal behaviour and financial irregularity, has been the core part of whistleblowing research. It varies in each organization perspective and its policy (Mehrotra, 2019; Park et al., 2005).. Within any given organisation, there are various types of wrongdoing on which an employees might feel that it necessary to blow the whistle. Wrongdoing can be clear or ambiguous and formal or informal, operating at organisational or personal levels with or without support from the workplace, with outcomes for individuals or groups. E.g. sexual harassment and badly manufactured drugs and food is an ambiguous wrongdoing which is difficult to detect (Mathews, 1987). Informal wrongdoing can includes neglect and ostracism and formal wrongdoing can include systematical rejection of job applicants from certain countries or clan (Bjørkelo, 2014). Wrongdoings is not always only individual phenomena but also could represent class interests, being engaged in regardless of social position in the quest to retain, protect or improve one's standing (Kumar, 2002). Occupational wrongdoing at the personal level could involve misstating individual accounts or wilfully concealing information from colleagues.

According whistleblowing policy for *The Global Fund (2019) to Fight AIDS, Tuberculosis and Malaria,* whistleblowers could report on four types of misconduct: 1) Illegal or unlawful conduct such as theft, fraud, bribery, or money laundering. 2) Un-procedural conduct occurs when policies, rules, or regulations in an organization are violated. 3) Unethical conduct undermines universal, core ethical values such as integrity, respect, honesty, responsibility, accountability, and fairness. 4) Wasteful conduct occurs when resources are spent in a wasteful manner (TheGlobalFund, 2019).

2.3. Whistleblowing Processes

According to Miceli and Near (1992) blowing the whistle: the organizational and legal implications for companies and employees Lexington Books, whistleblowing process has been described through four steps that needs a decision by both whistle-blower (step1 and 2) and the organization (step 3 and 4) (Miceli and Near, 1992). It should be noted that this whole cycle may be repeated in various forms The Steps and their detail description is shown in table 2.2.

Table 2. 2: Whistleblowing Processes and Descriptions (Miceli and Near, 1992)

Stages of the Whistleblowing Process	Description
Stage 1:- - Is the observed activity actually wrongdoing - illegal, immoral or illegitimate? (Whistleblower decision)	A triggering event occurs due to the observed activity is, involving questionable, unethical, or illegal which leads to the potential whistleblower or employee to consider blowing the whistle. They will consider the observed activities - Whistleblower values conflicts with the observed activities - Observed activities against organizational norm values and standards - Unambiguous evidence
Stage 2:- - Should the observed activity be reported? (Whistleblower decision)	A whistleblower or an employee engages in decision making on himself/herself, assessing the observed activity in detail through looking organizational whistleblowing policy whether it involves wrongdoing and gathering additional information, and discussing the situation with colleagues or low enforcement bodies. They will decide based on cases - If he/she believes the activities has serious impact - If she/he knows where to report it (knowledge of Reporting Channels). - Whistleblowers' Personal Situations like individual characteristics and alternative sources of financial and emotional support - No other alternative action - Whistleblowers' believes reporting it will be efficacious In General, it is the decision-making process that takes place after an event of potential wrongdoing is witnessed. The whistleblower /employees has many options /alternatives to take. 1) They could exercises voice by blowing the whistle; 2) They could exit the organization, or remain silent either due to loyalty or neglect.

Stage 3:- - Should the action to be halted? (an organization decision)	Once the whistleblower decided to blow the whistle the organization must respond in some way. It is also possible that it could do nothing or the organization could take some action. It about takes action or decision as to whether it should continue the allegedly wrongful action or not. Organization decision will consider - Other means to question the reported activities - If inaction could cost organization reputability
Stage 4: - - Should the whistleblower be punished? (an organization decision)	Organization members react to, and possibly ignore the whistle-blower or to take actions to silence the whistleblower through different ways. E.g. Retaliate the whistleblower. The organization decision could consider - Low dependence (If the organization have relatively greater power over the whistleblower) - Invalid charge (if top management believes the charge is invalid). - No other alternatives to question the reported activities

Loads of researchers studying whistleblowing have focused on different factors that affect the at each stages whistleblowing process. The factors includes institutional / organizational framework, local and international influences, workplace ethos and individual orientation operate in conjunction with sociocultural dynamics. For example, the observed wrongful activities in stage, types and seriousness of wrongdoing, could have an impact on whether the whistleblower /employee blowing the whistle in stage two of the process (Miceli and Near, 1985), and this intern have a direct impact on organization’s decision to the activities and whistleblower in stage three and four respectively. Additionally, features of the organization including shared values, norms and beliefs, whistleblower attitude, and the knowledge of the employees have about whistleblowing channels can affect the probability of whistleblowing (Near, Baucus and Miceli, 1993), and organization members’ reactions to the whistleblower. The cycle of whistleblowing is shown in Figure 2.3.

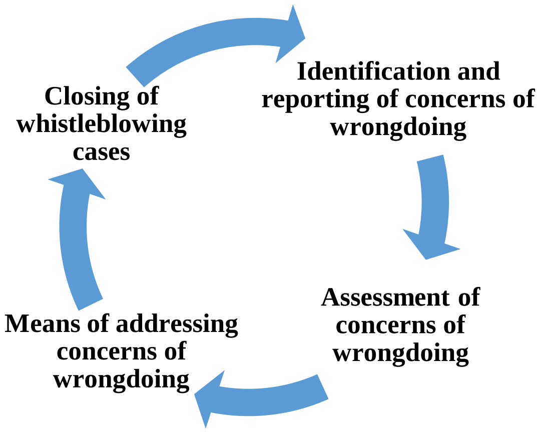

Identification and reporting of concerns of wrongdoing
Assessment of concerns of wrongdoing
Means of addressing concerns of wrongdoing
Closing of whistleblowing cases

Figure 2. 3: Full Cycle of Whistleblowing (Miceli and Near, 1992)

Although studies in the rea of whistleblowing system is very rear, whistleblowing can be expressed through different variables (Miceli et al., 2008; Hedin & Månsson, 2012; Miceli & Near, 1994; Mesmer-Magnus & Viswesvaran, 2005). After reviewing extensive literatures, the general whistleblower systems components and their relationship is shown in Figure 2.4.

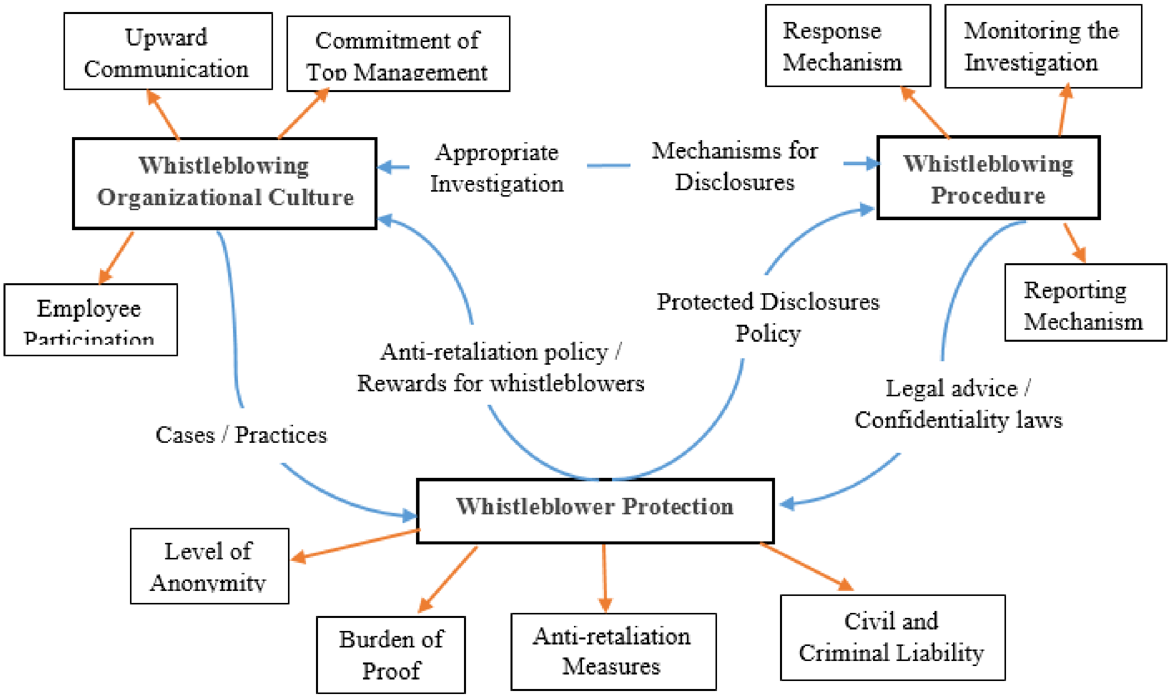

Upward Communication
Commitment of Top Management
Response Mechanism
Monitoring the Investigation
Whistleblowing Organizational Culture
Appropriate Investigation
Mechanisms for Disclosures
Whistleblowing Procedure
Employee Participation
Protected Disclosures Policy
Reporting Mechanism
Anti-retaliation policy / Rewards for whistleblowers
Legal advice / Confidentiality laws
Cases / Practices
Whistleblower Protection
Level of Anonymity
Burden of Proof
Anti-retaliation Measures
Civil and Criminal Liability

Figure 2. 4: Whistleblower Systems Components and their relationship

2.4. Whistleblower Characteristics

Employees with greater tenure are more invested in the organization and may prefer voice to exit. This is also congruent with predictions from theories of power in organizations, where employees with greater tenure may have greater power to effect change, and therefore may prefer voice to exit or silence (e.g., French & Raven, 2004). Individuals demonstrating higher organizational commitment are more invested in staying with the organization, therefore are more likely to blow the whistle rather than exit the organization, particularly when the prospect of continued wrongdoing is uncomfortable or unacceptable.

The first determinant of effective whistleblowing identified by Near and Miceli (1995) is categorization of whistleblowers. Three characteristics of whistleblowers are described by Miceli et al. (2008): personality characteristics, moral judgment, and demographic characteristics. Personality characteristics or dispositional characteristics are internal factors that cause an event or behavior. Moral judgment refers to the ability to judge one's own and others' behavior as right or wrong (Li, Zhu, & Gummerum, 2014). Demographic characteristics involve factors such as age, race, sex, and working experience. Whistleblowers' decision-making processes may be heavily influenced by all three of these characteristics (Bartels et al., 2014; Miceli et al., 2008).

Whistleblowing is carried out by people who are strongly committed and feel a moral responsibility for the operation of an organization (Miceli & Near, 1992; Rehg et al., 2004). It is usually experienced, well-educated and competent employees with a reservoir of trust in the organization who become whistleblowers (Miceli & Near, 1992, Hedin & Månsson, 2012). Usually, they also are personally affected by the problems and want to change the conditions of their work and performance (King III, 1997).

As per the study of Mesmer-Magnus & Viswesvaran (2005), whistleblowers tend to have good job performance, to be more highly educated, to hold higher-level or supervisory positions, to score higher on tests of moral reasoning, and to value whistleblowing in the face of unethical behavior. Also, it appears that whistleblowers are more likely than inactive observers to report a role-related responsibility or obligation to blow the whistle. However, age and organizational tenure as predictors of whistleblowing have yielded mixed results. Research outcomes indicate that older employees are more likely to blow the whistle than are younger employees. Females and more tenured employees appear to be slightly more likely to actually blow the whistle. These results support the contention that older employees with greater tenure and at higher levels are more likely to have the commitment and power to employ voice rather than exit mechanisms (Mesmer-Magnus & Viswesvaran, 2005).

Characteristics of whistleblowers in relation to retaliatory actions include age, education level, job level, role responsibility, and value congruence with the organization. While demographic characteristics of whistleblowers are thought to be less predictive of retaliation than are contextual variables (Miceli & Near, 2002), research suggests that individuals who blow the whistle because it is their job to do so (e.g., audit or role responsibility) are less likely to be retaliated against and are more likely to be successful in stopping the transgression (e.g., Casal & Zalkind, 1995; Miceli and Near, 2002). Further, Parmerlee and his colleagues (1982) found preliminary evidence that older whistleblowers are more likely to be retaliated against than are younger whistleblowers. Interestingly, their results also suggest that whistleblowers that are valuable to their organization (e.g., due to age, experience, education, job level) are more likely to be retaliated against as compared to less valuable whistleblowers (Parmerlee, Near & Jensen, 1982).

Perhaps, for older individuals and those at higher job levels and with more experience, greater organizational loyalty is expected. When such individuals blow the whistle, other organizational members may feel a greater sense of betrayal, thus paving the way for more retaliatory behaviors. This is especially true when external channels are employed to report violations. Norms of reciprocity and notions of perceived justice violations (however misguided) appear to predict retaliation (Mesmer-Magnus & Viswesvaran, 2005). Theories of power also suggest that whistleblowers at higher job levels, who are expected to enforce the power structure, upon violating this mandate are more likely to suffer retaliation. On the other hand, individuals at lower levels of the organizational structure may have lesser power, thus being easy targets for retaliation. Finally, evidence suggests that whistleblowers whose values regarding right and wrong are not congruent with those of the organization, are more likely to be retaliated against (Miceli & Near, 1994), presumably because top management does not deem the wrongdoing to be as severe as is perceived by the whistleblower, thus casting doubt on the merit of the whistleblower's complaint.

2.5. The Risk of whistleblowing

There are several disadvantages for a person that blows the whistle in organizations without a whistleblower protection policy and in countries without whistleblower protection laws (Cohen, 2017): i) a person who blows the whistle may have their employment contract terminated, especially in cases where senior management are involved in the wrongdoing; ii) a whistleblower may not be able to find another job in the same industry if they are placed "on a blacklist of unemployable potential re-offenders"; and iii) the employees and managers may retaliate against the whistleblower and their family members in the form of physical, psychological or verbal harassment, threats, demotions, denied promotions, reduction in salary, denied salary raises, public humiliation and attacks on their credibility. According to Banisar (2011) those who report wrongdoings may be subject to retaliation, such as intimidation, harassment, dismissal or violence by their fellow colleagues or superiors. In many countries, whistleblowing is even associated with treachery or spying.

Even in countries or organizations with whistleblower protection legislations, whistleblowers can be subjected to retaliation. Example Article 32 of UNCAC (2005) provides protection of witnesses, experts, and victims: it dictates that states

"shall take appropriate measures… to provide effective protection from potential retaliation or intimidation for witnesses and experts who give testimony concerning offences established in accordance with this Convention and, as appropriate, for their relatives and other persons."

However, this protection will apply only for witnesses and victims to the wrongdoing and this protection does not protect whistleblowers from retaliation unless they are "witnesses or victims".

Ethics Resource Center (ERC, 2012) 2011 National Business Ethics Survey report shows that employees who raise serious concerns about institutional wrongdoing do not typically receive bonuses, promotions, or other expressions of gratitude for bringing issues to light (Devine & Maassarani, 2011). Instead, whistleblowers disclose issues at a great risk to their professional and personal lives. Miceli and Near (1994) pointed out that retaliation against whistleblower may take many forms, ranging from attempted coercion of the whistleblower to withdraw accusations of wrongdoing to the outright exclusion of the whistleblower from the organization. Other retaliatory acts may include organizational steps taken to undermine the complaint process, isolation of the whistleblower, character defamation, imposition of hardship or disgrace upon the whistleblower, exclusion from meetings, elimination of perquisites, and other forms of discrimination or harassment. Retaliatory acts may be motivated by the organization's desire to: 1) silence the whistleblower completely, 2) prevent a full public knowledge of the complaint, 3) discredit the whistleblower, or 4) discourage other potential whistleblowers from taking action (Miceli & Near, 1994).

There are studies and cases demonstrating the retaliation experienced by whistleblowers. A study conducted in 1990 of 233 whistleblowers in the US found that 90% had lost their jobs or were demoted (Grace & Cohen, 1998), 27% faced lawsuits and 26% had psychiatric or medical referrals after blowing the whistle. Furthermore, a survey conducted of 761 whistleblowers in the US found that 69% lost their job or were forced to retire, 64% received negative performance evaluations, 68% had their work closely monitored by their supervisors, 69% were criticized or avoided by their colleagues, and 64% were blacklisted from getting another job in the same industry (Rothschild & Miethe, 1999).

The severity of retaliation varies across organizations. The whistleblower frequently pays the price both professionally and socially. The notable examples of retaliation includes character defamation, ostracism, harassment, demotion, poor performance appraisals, work overload, denial of promotion, disciplinary actions, transfers, and termination (Mesmer-Magnus & Viswesvaran, 2005; Ghana, 2016).

The type of whistleblowing and the context of the wrongdoing also determine whether retaliation will occur. For instance, external whistleblowers are more likely to face retaliation when their disclosures are very harmful to the organization and when they are reporting severely engrained wrongdoing (Miceli et al., 2008). In recent years, legislation across the countries including USA, UK, South Africa, Ghana, Canada, and others many countries in the world have required multinational public organizations to establish channels through which whistle-blowers can anonymously report abuses (EY, 2016). Transparency International (2013) defines the whistleblowing domain in three dimensions: i) whistleblowing procedure; ii) whistleblowing organizational culture, and iii) whistleblower protection.

2.6. Whistleblowing Procedure

In an organization, whistleblowing procedures are formulated to facilitate reporting of unlawful incidents in good faith which can afford the utmost confidentiality and effective protection against any retaliation or reprisals as a result of whistleblowing (OECD, 2014). A clear and easy-to-follow procedure is crucial for encouraging employees to report wrongdoing. Employees should be guaranteed a sufficient level of information, security, and objectivity throughout all stages of the process. These procedures are a key element for organizational integrity and facilitate combating practices that might damage its activities and reputation. TI (2016) indicates that the effectiveness of the internal reporting procedures includes reporting mechanisms (making disclosure) - accessibility of whistleblowing reporting channels; response mechanism (reporting and managing investigation outcome) - clear procedures to ensure thorough, timely and independent investigations of reports of misconduct. I.e. Receiving and assessing a disclosure and managing protected disclosures; and Monitoring the investigation result - the key statistics on whistleblowing cases collected and reviewed on a regular basis (TI, 2016).

2.7. Whistleblowing Organizational Culture

The organizational culture is one of the most significant components that is always being developed in the corporate environment. According to Luthans in Lako (2004), organizational culture is the norms and values that direct the behavior of organizational members. Limaj & Bernroider (2019) also defines Organizational culture as a set of underlying assumptions and beliefs held by the organization's employees, then developed and passed down to overcome external adaptation and internal integration problems.Every member will behave in accordance with the prevailing culture in order to be accepted by his environment. The organizational culture functions as a differentiator between one organization and another, builds a sense of identity for members, facilitates the growth of commitment, and enhances social system stability as a social unifier towards organizational integrity.

According to Schwartz (2013), there are three elements that must be present for an organizational ethical culture to be sustained in order to reduce unlawful or unethical behaviors carried out within or on behalf of the company. The three principal elements entail (1) the existence of core ethical values embedded throughout the corporation such as ‘integrity’; (2) the establishment of a formal ethics program such as ‘ethics training’; (3) the continuous presence of ‘ethical leadership,’ which is an appropriate ‘tone at the top’ as reflected by the board of directors, senior executives, and managers.

The three key components are (1) the presence of fundamental ethical principles that permeate the entire organization, such as "integrity," (2) the development of a formal ethics program, such as "ethics training," and (3) the ongoing presence of "ethical leadership," which is an appropriate "tone at the top" as demonstrated by the board of directors, senior executives, and managers.

Organizations are hard-pressed to come up with varied policies, procedures and practices that promote integrity-in-action and not just talk. Whistleblowers need to be supported and encouraged to act as monitors of corporate behaviors and discourage wrongdoers to the extent of eliminating them. One of the primary concerns of many organizations is to develop an ethical corporate culture through which it aims to control, minimize and ultimately try to eliminate wrongdoings and wrongdoers from the organization that are creating obstacles in the way of progression; by taking action against the wrongdoers and promoting whistleblowing which helps in drawing attention of the management toward wrongdoings and the wrongdoers. In other words, cultural rationalizations, such as fraud-tolerant attitudes in a corporation can increase the likelihood of fraud occurrence. Cultivating an ethical culture is stressed as the first line of defense for fraud mitigation (Suh et al., 2018). According to Sulistyowati (2007), a good organizational culture will not open the slightest opportunity for employees to commit fraud because a good organizational culture will shape employees to have a sense of belonging and pride as employees of the company. So, the stronger the organizational culture of a company, the less fraud that employees might commit.

Organisation's corporate culture determines to what extent potential whistleblowers feel safe and comfortable to report wrongdoing internally (Lachman, 2008). This has a direct influence on how whistleblowers react toward observed wrongdoings. Whistleblowers need to be supported and encouraged to act as monitors of corporate behaviors and report illegal acts and/or misconducts to the extent of eliminating them. The goodwill for internal reporting of wrongdoing is embedded in the corporate culture (Berry, 2004). Transparency international (2013) indicates the contributing factors in organizational culture includes i) commitment of organizations top management towards the whistleblowing - direct involvement of top officials and their strong engagement in the whistleblowing process; and ii) upward communication where information comes from the upper management - clear support of organizational higher officials for its employees and customers based on the existing whistleblowing frameworks and encourage internal reporting of wrongdoing.

2.8. Whistleblower Protection

As whistleblowing has immense social value but usually comes at a very high professional or personal cost, one of the most important protections relates to conditions of employment. Whistleblowers should be protected from dismissals, suspensions, disciplinary sanctions and other forms of workplace sanctions or discriminations (Chêne, 2009). Protection should be broad enough to cover any retaliatory measures, including subtle forms of discriminations and petty harassment. The risk of corruption is significantly heightened in environments where the reporting of wrongdoing is not supported or protected. Public and private sector employees have access to up-to-date information concerning their workplace practices, and are usually the first to recognize wrongdoings (UNODC, 2004).

According to the Organisation for Economic Co-Operation and Development (OECD) convention on Effective Whistleblower Protection "Whistleblower protection is integral to fostering transparency, promoting integrity" (OECD, 2016c). Whistleblower protection is nowadays considered as the ultimate line of defense for safeguarding the public interest. Protecting whistleblowers promotes a culture of accountability and integrity in both public and private institutions, and encourages the reporting of misconduct, fraud and corruption. "Effective whistleblower protection supports employees in "blowing the whistle" on corruption, fraud or wrongdoing "(OECD, 2016). Whistleblower protection is essential to encourage the reporting of misconduct, fraud and corruption. According to the United Nations Office on Drugs and Crime (2004), the risk of corruption is significantly heightened in environments where the reporting of wrongdoing is not supported or protected. This applies to both public and private sector environments, especially in the cases of bribery: protecting public sector whistleblowers facilitates the reporting of passive bribery, as well as the misuse of public funds, waste, fraud and other forms of corruption (UNODC, 2004).

Encouraging and facilitating whistleblowing, in particular by providing effective legal protection and clear guidance on reporting procedures, can also help authorities monitor compliance and detect violations of anti-corruption laws (OECD, 2012). Providing effective protection for whistleblowers supports an open organizational culture where employees are not only aware of how to report but also have confidence in the reporting procedures. It also helps businesses prevent and detect bribery in commercial transactions. The protection of both public and private sector whistleblowers from retaliation for reporting in good faith suspected acts of corruption and other wrongdoing is therefore integral to the efforts to combat corruption, promote public sector integrity and accountability, and support a clean business environment (OECD, 2016).

2.9. Whistleblower Protection Mechanisms

The OECD Anti-Bribery Convention and Recommendation Convention (2009) itself does not specifically include provisions on whistleblowing. Nevertheless, subsequent OECD instruments encourage the adoption of whistleblower protection. In 2012, OECD prepared a compendium of best practices and guidelines for legislation on the protection of whistleblowers in G20 countries (OECD, 2014a). This compendium identifies four specific whistleblower protection mechanisms: i) protection from retaliation, ii) anonymity and confidentiality, iii) burden of proof, and iv) criminal and civil liability. These mechanisms are described in the following sections.

2.9.1. Protection from Retaliation

Protection against retaliation is considered to be one of the cornerstones of effective whistleblower protection legislations (TI, 2016). Effective protection of whistleblowers from reprisal is required, Devine and Walden, described what reprisals might entail: "The law should cover all common scenarios that could have a chilling effect on responsible exercise of free expression rights." (Devine & Walden, 2013). The crucial element in ensuring the protection of whistleblowers is educating public employees on their rights and protections under whistleblower legislation, because "whistleblowers are not protected by any law if they do not know it exists." (Banisar, 2011).

Individuals shall be protected from all forms of retaliation, disadvantage or discrimination at the workplace linked to or resulting from whistleblowing. This includes all types of harm, including dismissal, probation and other job sanctions; punitive transfers; harassment; reduced duties or hours; withholding of promotions or training; loss of status and benefits; and threats of such actions (TI, 2013).

Whistleblower protection laws should provide a whistleblower with adequate and comprehensive protection against discriminatory or retaliatory personnel action from retaliation by their employer or fellow employees. This should include protection from discrimination, physical or psychological abuse, intimidation, threat of demotion, reduction in pay, and other financial reprisals, e.g. loss of perks or bonuses. The law should specify that an employer cannot terminate an employee's employment contract because the employee blew the whistle (Cohen, 2017).

Different countries around the world have adopted whistleblower protection laws against retaliation. For example, the French Sapin II Law on Transparency, Anti-corruption and Economic Modernization (Sapin, 2016), sets out broad employment protections for whistleblowers including direct or indirect disciplinary actions, dismissal or discrimination, particularly with regard to remuneration, training, classification and reclassification, assignment, qualification, professional promotion, transfer or contract renewals, as well as exclusion from recruitment or access to internships or training. Similar provisions protecting whistleblowers against employment-related reprisals are expressly listed in detail under South Africa's protected disclosure Act 26 of 2000 (SAPDA, 2000). Korea's Anti-Corruption and Civil Rights Commission (ACRC) Act also provides protection against financial or administrative disadvantages, such as the cancellation of a permit or license, or the revocation of a contract (SKA, 2008).

2.9.2. Anonymity and Confidentiality

As confidentiality agreements are common in employment contracts, whistleblower legislation must state that a confidentiality agreement in employment contracts cannot prevent an employee from reporting to the regulator any sensitive information that they learned during their employment at organization (Bowden, 2006). Otherwise, employers could always prevent their employees (e.g. through a court ordered injunction) from reporting wrongdoing by inserting a broad confidentiality agreement in the employment contract. In 2013, Transparency International publication on whistleblower protection and the UN Convention Against Corruption stated on anonymity for whistleblowers: "full protection shall be granted to whistleblowers who have disclosed information anonymously and who subsequently have been identified without their explicit consent" (TI, 2013).

One essential ingredient of an effective system is to assure whistleblowers who do not wish to be identified that their confidentiality will be respected (TI, 2013). That means that their identity will not be disclosed outside the organization they report to without their consent. Some countries like e.g. South Korea require whistleblowers to give their names to the authorities, but ensure confidentiality by making strict requirements that employees of these authorities will not release any personal details without the whistleblower's consent (SKA, 2008).

Most whistleblower laws provide for the protection of the identity of the whistleblowers, which is kept confidential unless a whistleblower provides his/her consent to disclose it (Banisar, 2011). The U.S. law on whistleblower protection of 1989, for example, prohibits the disclosure of the identity of a whistleblower without consent, unless the Office of the Special Counsel "determines that the disclosure of the individual's identity is necessary because of an imminent danger to public health or safety or imminent violation of any criminal law" (USWPC, 1989). Some countries also impose sanctions for disclosing the identity of the whistleblower; for example, India's Public Interest Disclosure and Protection to Persons Making the Disclosures bill imposes a penalty of imprisonment and fine for revealing the identity of the whistleblower (IPB, 2010).

Although anonymity can provide a strong incentive for whistleblowers to come forward, a number of whistleblower protection laws exclude anonymous disclosures. For instance, The Supreme Court of Brazil has discussed the investigative challenges resulting from secret reporting and has ruled that the opening of a criminal investigation cannot be justified by an anonymous tip itself (SCB, 2005). other barriers to protecting anonymous whistleblowers can also be cultural, so whistleblowers can be seen negatively in some ways (OECD, 2014a).

Anonymous channels are critical to get those who know about the wrongdoing in the door to auditors or regulators, in the first instance. Without them, a government institution or a corporation may never know about the wrongdoing. At present, however, whistleblower protection rules may actually deter whistleblowing by providing no protection unless employees first identify themselves. Research and experience shows that whistleblowers will often identify themselves, and provide invaluable information, if first afforded the facility to make an anonymous disclosure or enquiry, in the knowledge that, if later identified, protection will extend to their original disclosure (OECD, 2014a). The identity of the whistleblower can often be deduced from circumstances, and the fact that a disclosure is anonymous can focus attention on the identity of the person who made it (rather than on the message). Moreover, anonymous allegations are difficult for law enforcers to pursue, and a culture of anonymous disclosures is unhealthy.

2.9.3. Burden of Proof

In order to avoid sanctions or penalties, an employer must clearly and convincingly demonstrate that any measures taken against an employee were in no sense connected with, or motivated by, a whistleblower's disclosure (TI, 2013). An important issue in WPL relates to the burden of proof. It is obviously very difficult for an employee to prove the fact that retaliation was a result of making the disclosure, especially as many forms of reprisals may be very subtle and difficult to establish (Chêne, 2009). Best practice in this regard involves reversing the burden of proof for claims of retaliation. It should be assumed that retaliation has occurred where disciplinary action cannot clearly be justified on management grounds unrelated to the fact of disclosure. The South African legislation stipulates that dismissal after whistleblowing is deemed to be "automatically unfair dismissal" (SAPDA, 2000). It is however important to note that the employer's rights should be protected as much as the whistleblower's with regard to the right to defense and to fair trial.

Whistleblower protection laws may lower the burden of proof whereby the employer must prove that the conduct taken against the employee is unrelated to his or her whistleblowing. South Africa's PDA states that any dismissal in breach of the Act is deemed to be an automatically unfair dismissal (SAPDA, 2000). U.S. law (USWPC, 1989) applies a burden-shifting scheme pursuant to which a federal employee who is a purported whistleblower must first establish that he or she: i) disclosed conduct that meets a specific category of wrongdoing set forth in the law; ii) made the disclosure to the "right" type of party – depending on the nature of the disclosure, the employee may be limited regarding to whom the report can be made; iii) made a report that is either outside of the employee's course of duties or communicated outside of normal channels; iv) made a report to someone other than the wrongdoer; v) had a reasonable belief of wrongdoing – the employee does not have to be correct, but the belief must be reasonable to a disinterested observer; and vi) suffered a personnel action, the agency's failure to take a personnel action, or the threat to take or not to take a personnel action. If the employee establishes each of these elements, the burden shifts to the employer to establish by clear and convincing evidence that it would have taken the same action in the absence of the whistleblowing (USWPC, 1989).

2.10. Whistleblowing in International Conventions

A variety of international conventions have recognized the need for protection and support for whistleblowers (Loyens & Vandekerckhove, 2018). Whistleblower protection requirements have been introduced in Articles 8, 13 and 33 of the United Nations Convention against Corruption (UNCAC, 2005), the Council of Europe Civil and Criminal Law Conventions on Corruption (CETS174, 1999), the Article III (8) of Inter-American Convention against Corruption (IACAC, 1996), and the Article 5(6) of the African Union Convention on Preventing and Combating Corruption (ACUPCC, 2003).

The UN Convention against Corruption binds all its signatory countries to consider legal provisions to protect people who report corruption-related offences from retaliation. In Article 33 (Protection of reporting persons), it provides for whistleblower protection (UNCAC, 2005):

> *"Each State Party shall consider incorporating into its domestic legal system appropriate measures to provide protection against any unjustified treatment for any person who reports in good faith and on reasonable grounds to the competent authorities any facts concerning offences established in accordance with this Convention."*

The others includes

1. Article 9 of the Council of Europe Civil Law Convention on Corruption, having entered into force in 2002, provides for the protection of workers against any unjustified sanction for those who have reasonable grounds to suspect corruption and who report in good faith their suspicion to responsible persons or authorities (CETS174, 1999).

2. Article 22 of the Council of Europe Criminal Law Convention, which entered into force in 2002, stipulates protection for persons who report criminal offences in line with that convention (CETS174, 1999).
3. Article 33 of the United Nations Convention against Corruption (UNCAC), having entered into force in 2005, stipulates that all parties to the Convention shall consider incorporating whistleblower protection into their domestic legal systems and article 32 of the same convention stresses the need to protect witnesses, experts and victims (UNCAC, 2005).
4. In 2009, the Council of the OECD adopted the Recommendation for Further Combatting Bribery of Foreign Public Officials in International Business Transactions, requiring all parties to the Anti-Bribery Convention, including 23 of the 28 EU countries, to adopt whistleblower protection measures in both public and private sectors (OECD, 2014).
5. In 2014, the Council of Europe Committee (CoE) of Ministers adopted Recommendation CM/Rec (2014)7 on the protection of whistleblowers. It urges CoE member states to put in place comprehensive national frameworks for the protection of whistleblowers standing in a de-facto working relationship with a public or private organization, paid or unpaid, regardless of their legal status (CM/Rec, 2014).

Marie Chêne (2009) explains what a good practice whistleblower protection legislation (WPL) need to include comprehensive free standing laws that have a broad scope and coverage, providing adequate alternative channels of reporting both internally and externally, protecting as far as possible the whistleblower's confidentiality, and providing for legal remedies and compensation (Chêne, 2009). Whistleblower protection has been a priority element of the financial, economic and regulatory cooperation between G20 countries since November 2010 (OECD, 2014a).

2.11. Measuring Whistleblowing and Whistleblower Protection performance

OECD (2016c) recommended to "Encourage countries to develop review mechanisms to identify data, benchmarks, and indicators relative to whistleblower protection systems and the broader integrity framework in order to evaluate effectiveness and monitor performance". An effective whistleblowing process may have implications for organizational future and its long term performance (Mesmer-Magnus & Viswesvaran, 2005).

There are various definitions of the effectiveness of whistleblowing. Stra and Baker (1988) defines effectiveness as the win/loss ratio of the low suits entered by whistleblowers. Miceli and Near's (1995) define effectiveness as "the extent to which the questionable or wrongful practice (or omission) is terminated at least partly because of whistleblowing and within a reasonable time". St-Martin (2014) pointed out five factors that can affect the effectiveness of whistleblowing: i) type of whistleblowing, ii) role of mass media, iii) documentation of evidence, iv) retaliation, and v) legal protection. Ellison (1985) indicates that successful whistleblowing should have two aims: i) Did they achieve what they had in mind? ii) Did others, in some way, heed their warnings?

Other important benchmarks to measure the effectiveness of the whistleblower protection systems may include clear and effective communication and awareness-raising (OECD, 2016c). Providing information on the rights and responsibilities of both employers and employees is an important element in creating an environment of trust, professionalism and collegiality that supports the tenets of integrity in both the workplace and society. In addition, awareness-raising could help change the culture surrounding whistleblowing and dismantle the negative barriers and connotations concerning the act of disclosing the wrongdoing (OECD, 2016c & 2014). Even when the law generally protects an employee from retaliation for reporting illegal activity in an organization, if the employee acts improperly in making that report, the organization may have a legitimate, legal reason to take action against that employee.

2.12. Government and Whistleblowing

Researchers and Policy recommendations (DBIS, 2015; NAO, 2014) indicates that the government (organization) plays its crucial role in whistleblowing, including i) developing or adopting a comprehensive and strong clear whistleblowing legal and policy frameworks and appropriate written procedures in place for dealing with whistleblowing; ii) Promoting a policy or procedure and making sure the whistleblowing policy and procedures are easily accessible to all workers - actively promoting a policy shows the organisation is genuinely open to hearing concerns from its staff; iii) since written policies and procedures are not enough, training need to be provided to all staff on the key arrangements of the policy on how disclosures should be raised and how they will be acted upon – sometimes additional training could be provided to those with whistleblowing responsibilities, such as managers or designated contacts on how to deal with disclosures; iv) Create an understanding that all staff at all levels of the organisation should demonstrate that they support and encourage whistleblowing; v) Create an organisational culture where workers feel safe to raise a disclosure in the knowledge that they will not face any detriment from the organisation as a result of speaking up; vi) Make a commitment that all disclosures raised will be dealt with appropriately, consistently, fairly and professionally; vii) Undertake to protect the identity of the worker raising a disclosure, unless required by law to reveal it and to offer support throughout with access to mentoring, advice and counselling; viii) Provide feedback to the worker who raised the disclosure where possible and appropriate subject to other legal requirements. Feedback should include an indication of timings for any actions or next steps; and viiii) Assessing whistleblower program effectiveness (NAO, 2014).

2.13. Digital Technology and Whistleblower Protection

Developments in digital technology open up vast opportunities for organizations to create and distribute information in new ways. Concerning Digital Government strategies for transforming public services, OECD (2016a) states that “Technology has a major part to play in the solutions to each of three major challenges which globalization is setting modern governments – economic productivity, social justice and public service reform”. Digital technology have played a pivotal role in aiding whistleblowers and sources as well as in generally enabling more transparency. They also pose challenges to the protection of whistleblowers and sources. Vast amount of data is created ranging from Internet connection records to communications data and this information can tell interested parties everything about a reporter, the story they are pursuing, and the sources they are protecting.

The technology landscape involved in whistleblowing has changed drastically over time. At its most basic level, writing and verbal speech could be used to convey information about wrongdoings. The printing press and radio eased the spread of news (OECD, 2016). Copiers allowed whistleblowers to copy documents and give them to press. Computers and the Internet make it easy to disseminate information and upload leaked documents. Easy uploading means the rise of leaking, i.e. mass release of millions of documents the whistleblower might not have even read.

Whistleblowing plays a crucial role in providing a free, transparent and just social order by helping to monitor compliance and detect violations of laws (TI, 2016). It can help in eliminating the wrongdoings, arbitrariness, and corruption from a society. Whistleblower protection contributes to creating trust and tolerance and enhances the capacity for countries to respond to wrongdoing and matters of public concern. A number of countries around the world have laws protecting whistleblowers from retaliation for filing a claim or reporting a violation. International instruments on whistleblower protection recognized the importance of whistleblower protection laws as part of an effective anti-corruption framework including the United Nations Convention against Corruption (2003), the 2009 OECD Anti-Bribery Recommendation, the 1998 OECD Recommendation on Improving Ethical Conduct in Public Service , the Council of Europe Civil and Criminal Law Conventions on Corruption (1999), the 1996 Inter-American Convention against Corruption and the African Union Convention on Preventing and Combating Corruption (2003).

The development of digital technology has resulted in an increased capability for data collection, storage, processing and discovery, as well as the use and disclosure of information (OECD, 2019 & Ontanu, 2019). However, the integration of digital technology into public sector transformation and modernization efforts is a challenge. According to OECD (2014b), “Public sector capacities, workflows, business processes, operations, methodologies and frameworks need to be adapted to the rapidly evolving dynamics and relations between the stakeholders that are already enabled by the digital environment”.

2.13.1. Digital Technology and Anonymity

Digital technology has made it possible to track people in historically unprecedented ways. Peoples are targets of surveillance at just about every turn of our lives. In transactions with retailers, mail-order companies, medical caregivers, day-care providers, and even beauty parlors, information about us is collected, stored, analyzed, and sometimes shared (Nissenbaum, 1998). From these bits of information, public identities may be formed that are not only elaborate, but permanently accessible in an active electronic form for those who may need or want them.

The meaning of anonymity, as may be reflected in ordinary usage or a dictionary definition, is “not named or identified”, that is to say, conducting oneself without revealing one’s name. It broadly involves the availability or unavailability of various information that may be known or identified about a person. Concerning information about individuals, possible descriptive types include individual and shared identification (Marx, 2004; Korkea-Aho, 1999).

Anonymity is considered acceptable, even necessary, because it offers a safe way for people to act, transact, and participate without accountability, without others getting at them, tracking them down, or even punishing them. This includes a range of possibilities. Anonymity may encourage freedom of thought and expression by promising people a possibility to express opinions and develop arguments about positions that, for fear of reprisal or ridicule, they would not or dare not take otherwise. Anonymity may enable people to reach out for help, especially for socially stigmatized problems like domestic violence, HIV and other sexually transmitted infections, emotional problems, or suicidal thoughts (Nissenbaum, 1999). It supports socially valuable institutions like peer review, whistleblowing, and voting.

For reporting channels to work efficiently, another challenge to overcome is how to ensure that they provide the right degree of confidentiality or even anonymity to whistleblowers. The term ‘anonymous’ should be understood as relating to a disclosure made through a channel that assures no possible link to the person providing the information: a file of information sent without a return address, an untraceable telephone call to a hotline, an email sent from a blocked account, IT systems guaranteeing anonymity and preventing back contacts, etc. A ‘confidential’ disclosure is one where the identity of the whistleblower is known only by the recipient of the disclosure (e.g. an Ombudsman or the ethics advisor) who has an obligation to keep the name secret, both towards members of the concerned organization and towards the wider public (Dehn, Guy & Calland, 2004).

Extending this understanding into the electronic sphere, one might suppose that conducting one’ s affairs, communicating, or engaging in transactions anonymously in the electronic sphere is to do so without one’ s name being known. Specific cases that are regularly discussed include: i) sending electronic mail to an individual, or bulletin board, without one’s given name appearing in any part of the header, ii) participating in a chat group, electronic forum, or a game without one’s name being known by other participants, iii) buying something with the digital equivalent of cash, or iv) being able to visit any web site without having to divulge one’s identity (Nissenbaum, 1999; Reiter & Rubin, 1998).

Anonymity technologies enable Internet users to maintain a level of privacy that prevents the collection of identifying information such as, e.g. IP addresses. Understanding the deployment of anonymity technologies on the Internet is important for analyzing the current and future trends (Liaba & Erdin, 2013). Anonymity has always been a dichotomous issue in both social life and cyber space. On one side, anonymity technologies provide legitimate usage such as privacy, freedom of speech, anticensorship, anonymous tips for law enforcement, and surveys such as evaluation and feedback. On another side, anonymity technologies provide protection to criminals in facilitating on-line crimes such as piracy, information and identity theft, spam, cyber-stalking and even organizing terrorism (Kelly, 2009).

Anonymity systems send data packets over relays so that no single system has information about both the sender and the receiver (Diaz, 2005). Since many people utilize these intermediaries at the same time, the Internet connection of any one single person is hidden among the connections of all other users. Hence, no individual system, internal or external, can determine which connection belongs to which user. The degree of anonymity varies and depends on the utilized mechanisms, adversary capabilities, and operation environment (Liaba & Erdin, 2013).

2.13.2. Electronic Surveillance and Protection of Sources

With the proliferation of electronic surveillance over the previous decade, the safety of anonymous sources and whistleblowers no longer depends only on ethical and legal protections, but also on information security. Computer-based work monitoring has enabled employers to continually or intermittently monitor employees in real time or on a delayed basis, with or without their knowledge or permission, at levels and in a manner previously unattainable (Aiello, 1993). Even if ethical and legal protections are in place, mass surveillance risks rendering them meaningless. The Snowden revelations on NSA files in 2013 is a proof of why whistleblowing is important and it revealed the extent of electronic surveillance and the prevalence of such practices across all electronic communications platforms (Guardians, 2013).

A number of cases of violent incidents occurred due to authority over information and communications. According to the United Nations' Human Rights Council, journalists, whistleblowers, sociopolitical activists, opposition representatives and dissidents, non-governmental organizations, and even ordinary citizens, are submitted to a number of abuses as a result of surveillance (UNHRC, 2014). These abuses include intimidation, discrimination, and incarceration; espionage and smear campaigns; chilling effects; information blackouts; legislation approved in conditions of emergency or secrecy; and, brutal repression, torture, and murder.

However, the majority of journalists and civil society organizations still exchange confidential information over regular phone lines, text messages and unencrypted email. Journalists rely on source protection to gather and reveal information in the public interest from confidential sources (Mendel et al., 2012). Such sources may require anonymity to protect them from physical, economic or professional reprisals in response to their revelations. This is a significant challenge especially within the context of state or corporate surveillance, as the relevant actors can sidestep the legal protection of sources and whistleblowers, and identify their identities by other means. In 2015, the UNESCO study on access to information and knowledge, freedom of expression, privacy, and ethics on a global Internet indicated that (UNESCO, 2015):

"With respect to the role of privacy in protecting freedom of expression, whether the protection of the confidentiality of journalistic sources should be similar to, or dramatically different in the online digital media environment where it is possible to technically track networks of communication. In this light, should there be greater or different kinds of protections for journalists in protecting the confidentiality of their sources".

2.14. Digital Anonymous Whistleblowing Initiatives and Leak Platforms

The gaps in protection of whistleblowers, as well as the rise of digital technology and the ease of electronic transmission has given rise to new online platforms that enable whistleblowers to publish information anonymously. The global nature of the Internet has enabled this information to stay available online. One such platform is Wikileaks, which is a journalistic organization that provides a secure online "dropbox", enabling anonymous whistleblowers to deliver information without placing themselves at risk (APC, 2015).

This has inspired Internet activists to create similar platforms, such as Globaleaks and Associated Whistleblowing Press. Whilst not journalistic institution themselves, and not involved in publishing information, these platforms enable and support whistleblowing and investigative journalism. Globaleaks, for example, is an open source platform that enables institutions to install anonymous, and secure whistleblowing platforms. The platform has been implemented by over 24 institutions at the time of the writing of this report (GlobaLeaks, 2017). One notable implementation is AfriLeaks designed specifically to support investigative journalism in Africa (Afrileaks, 2019). These types of secure platforms have failed, however, to prevent significant reprisals against people who have leaked documents to them. In a more recent case of reprisals, email service provider Lavabit was forced to close down in 2013 after it was asked by the US government to compromise its entire privacy system for the sake of eavesdropping on a single customer, largely presumed to be Edward Snowden, a whistleblower that revealed mass surveillance and misconduct by the US National Security Agency.

2.15. Digital Government in the Whistleblowing Domain

Recent financial crises underline the importance of all economies of encouraging whistleblowers in all sectors to raise concerns before corruption hollows out and destroys economic, social, and political activity (ACFE, 2016). The 2019 annual report to congress on the Whistleblower Program of the United States Securities and Exchange Commission (SEC or Commission) states that "The whistleblower program continues to have a significant positive impact on the Commission's enforcement efforts and protection of investors and markets, including assisting the Commission . . . in the return of hundreds of millions of dollars to harmed investors, many being Main Street investors, as a result of whistleblower tips" (USSEC, 2019). The OECD (2014a) indicates that the most commonly reported categories include fraud, work place safety and health issues, and industrial relations and labor issues (OECD, 2014a; ACEF, 2016). The whistleblowing domain accounts for an important part of a country's overall development. The domain includes stakeholders from the public and private sectors who are administratively separated from each other and who sometimes have different or even partially contradictory objectives. While whistleblowing-related entities in the private sector pursue commercial objectives, mainly to increase the whistleblowing system user's number and generate profits by renting and selling their system, they may also exploit private data and other public goods even though protecting whistleblower confidentiality is an integral component of the whistleblower program.

Due to the dynamics of different stakeholders' interests, whistleblowing cases are challenging entities to manage. Although various stakeholders have numerous linkages and interdependencies, cooperation between them is extremely difficult, as the stakeholders typically have different interests and diverging visions for development (Kim & Wim, 2018; Richardson & Garner, 2019). In addition, the sustainability of whistleblowing program is both sensitive and critical (Benchekroun & Pierlot, 2012). In both respects – cooperation and sustainability – sectoral governance entails joint decision and action among public authorities, policymakers, the whistleblowing sectors and local communities to define and pursue common goals.

Whistleblowing represents the major context for the application of Digital Government. Already in 2018, a whistleblowing system a report of Bank Rakyat Indonesia (BRI) showed that obtaining whistleblowing information and reporting organizational misconducts was the most common service used by whistleblowers. The BRI report indicates that a total of 124 complaints were received in 2018 alone where 77 reports (62.1 %) through SMS and email accounts 43 (34.67 %) reports while in hand report through a letter were only 4 (3.23%).

However, the shortage of research and understanding needed to develop Digital Government practices in the whistleblowing domain sector has been recognized by several researchers (Kaye, 2017; Thorsen, 2016; Wisnewski, 2016; Brevini, 2017). In addition, despite the enormous potential of Digital Government to improve and advance interactions among citizens, businesses, and government, the full potential of Digital Government in the whistleblowing sector has yet to be determined (Kaye, 2017). One of the aims of this research is to assess the state of research on Digital Government in the whistleblowing domain by conducting a Digital Government stakeholder analysis for the whistleblowing domain and by interpreting the findings through the Digital Government evolution model (Janowski, 2015).

Table 2.3 describes the Digital Government Interactions in the whistleblowing stakeholders which includes six types of interaction between stakeholders which is created from government - public authority - to other 5 stakeholders and government itself. It includes government-to-government (G2G), government-to-employee (G2E), government-to-citizen/customer (G2C), Government-to-NGO (G2N), government-to-whistleblower (G2W) and government-to-media outlets (G2MO).

Table 2. 3: Digital Government Interactions in the whistleblowing stakeholders.

No	Interaction	Description
1	Government-to-Government (G2G)	G2G includes interaction between organizations' public authorities and law enforcement authorities (Hiller & Belanger, 2001) which involves whistleblowing and whistleblower protection. It helps to enhance cooperation and collaboration between governments of different levels. This can be at the country or at the different territorial levels of a country. The basic activities could be sharing of whistleblowing government databases as well as integrating separate whistleblowing systems/platforms.
2	Government-to-Employee (G2E)	G2E involves the relationships between the public authority and civil servants of the organization (Tang et al., 2011; Rao, 2017) and other employees of the public authority who can be able to involve in whistleblowing the wrongdoing activities within the organizations. It helps to improve the efficiency and effectiveness of the whistleblowing program within the government administration.
3	Government-to-Consumer / Citizen (G2C)	G2C involves the relationships between the public authority of an organization and citizens/ customer who lives in the territory under the jurisdiction of this authority (Hiller & Belanger 2001) and who are directly and indirectly affected by whistleblowing and whistleblower protection. Government-to-citizen services involve all the whistleblowing communications or transactions between government, at various levels, and citizens. The activities include whistleblowing information access, such as whistleblowing policies and whistleblowing training materials.

4	Government-to-NGOs (G2N)	G2N Involves interactions between the public authority and non-governmental organizations with interests combating fraud and corruption through encouraging whistleblowing and whistleblower protection under the jurisdiction of this authority. This relation includes government to Civil Society, Business Associations, and Professional associations. They can be able to educate the public about the importance of whistleblowers, provides whistleblowers with legal assistance, and advocates for policies that protect and reward whistleblowers.
5	Government-to-whistleblowers (G2W)	G2W involves the interaction between public authority and the whistleblowers who expose the unlawful activities within the organization and government itself.
6	Government-to-Media (G2M)	G2M involves the interaction between public authority and Media outlets. Media outlets include newspapers, magazines, radio, television, and the Web offering news about whistleblowing and whistleblower protection and presenting stories to the public via various channels of dissemination.

.

2.16. Digital Government and Whistleblower Protection

Despite digital technology playing a key role in enhancing whistleblowers information dissemination mechanisms, protecting reporting channels, anonymous technology and burden of proof through digital records, having a policy against secretly taping in the workplace is the whistleblowers best chance to effectively prohibit it (Ontanu, 2019). For example, in March 2014 The Irish Times media outlet published that Irish Minister for Justice Alan Shatter exposed the two whistleblowers in revelations of the widespread recording of telephone calls to and from Garda stations. Even though he "apologized to Garda whistleblowers Sgt Maurice McCabe and John Wilson over remarks, he made over the penalty points controversy, where the men had exposed the quashing of points by gardaí" (IRISH, 2014). This indicates that technology measures alone are not enough for whistleblower protection. It needs a shift on the use of technology to support government whistleblower operations to coordinating strategic decisions on digital technologies in the shaping of main strategies and agendas for whistleblower protection reform and modernization which needs strategic planning of whistleblower protection policies for digital technologies use in all areas and at all levels of the administration. In addition to protecting privacy rights and proprietary information, such a policy can help to maintain open communication between management, employees and co-workers.

In 2016, OECD in its publication on Digital Government strategies for transforming public services states that "Digital Government is digital technologies and user preference integrated in the design and receipt of services and broad public sector reform which is the integral part of government's modernization strategies to create public value". The advance of Digital Government boost governments' ability to manage many kinds of social affairs and obtain both good economic efficiency and social efficiency, as well as reduces management costs and enhances the working efficiency of the government (OECD, 2014b).

In many areas, digital technology have been an important enabling tool for reform. The pursuit of efficiency gains, effective delivery of program outcomes improving services, increasing accountability and transparency and facilitating consultation and engagement had been the main driver of technology use in government (OECD, 2003). According to OECD (2016a) “Digital Government enables governments to create increased public value and broad public sector modernization (with greater openness, transparency, engagement with and trust in government) through the integration of digital technologies and user preferences in service design and delivery of direct personal services and in shaping public policy outcomes, while also achieving efficiency and productivity gains”.

2.17. Digital Government Evolution Model

A few digital-government evolution models have been proposed. The evolution models were either developed by individual researchers (e.g. Siau & Long, 2005; Janowski, 2015) or proposed by institutions (e.g. UNDESA, 2014, 2016; Baum & Di Maio, 2001). Table 2.4 offers an overview of the strengths and weaknesses of each Digital Government model. However, considering the aim of this research, the theoretical foundation used for the analysis of this study is the Digital Government evolution model (Janowski, 2015) since this model helps to analyze sector-specific institutional transformations.

According to Janowski (2015), a Digital Government evolution model was defined comprising four stages: i) Digitization (Technology in Government) – digitizing government information, and automating operations and public service delivery systems to modernize the internal working of organizations by digitizing and automating them; ii) Transformation (Electronic Government) – improving the internal working and culture of government and facilitating institutional reform through digital technology to increase their efficiency, effectiveness and other relevant attributes; iii) Engagement (Electronic Governance) – engaging citizens and other nonstate actors in government decision making and building trust. It aims to transform relationships between government and citizens through the use of digital channels to build trust; iv) Contextualization (Policy-Driven Electronic Governance) – enabling sectors, territories, communities, citizens, etc. to pursue development action by themselves. It aims to create better conditions through digital technology in order to pursue public policy and development goals. Considering the above description, only the conceptualization stage of Digital Government explicitly considers sectorial applications.

Table 2. 4: Digital Government Stage Models

Model	Stages	Definition	Model Strength	Model Weakness
Gartner's four-stage model (Baum and Di Maio, 2000)	Web presence	Agencies provide a web site to post basic information to public	Concise and easy to follow	Ignores the potential benefits of political changes and institutional transformations
	Interaction	Users are able to contact agencies through web sites (e.g. e-mail) or do self-service (e.g. download document)		
	Transaction	Users (including customers and businesses) can complete entire transactions (e.g. license application and procurement) online		
	Transformation	Governments transform the current operational processes to provide more efficient, integrated, unified, and personalized service.		
UN's five-stage model (UNDESA, 2014, 2016)	Emerging presence	Offering basic information online - Channels: Basic website, Public kiosk	Focuses on web-based public service (front-office)	- Does not consider the building of back office - Ignores the potential benefits of political changes and institutional transformations
	Enhanced presence	Greater sources of information, and e-tools and e-services. Government websites deliver enhanced one-way or simple two-way e-communication between government and citizen. Channels: Web portal, SMS text, Mobile portal, Public kiosk		
	Transactional presence	Two-way interactive applications provide citizens with opportunities for online, financial and non-financial transactions Coordinated. Government websites engage in two-way communication with their citizens. Channels: Web portal, SMS text, Mobile app, Mobile portal, Public kiosk, PPPs		
	Connected presence	The way government operates fundamentally changes, and there is better coherence, integration and coordination of processes and systems within		

		and across government agencies. Government transforms itself into a connected entity. Integrated Channels: ALL		
Keng Siau and Yuan Long (Siau, K., & Long, Y., 2005)	web presence	Governments typically post simple and limited information through their web sites	This model presents a development trend rather than a must-go-path	Ignores the potential benefits of political changes and institutional transformations
	Interaction	Provides simple interaction between the governments and the users. This includes basic search engines, e-mail systems, as well as official form downloads.		
	Transaction	Enables users (including both individual citizens and business) to conduct complete online transactions.		
	Transformation	Transforming the way that governments provide services. The transformation involves both vertical (i.e. governments in different levels) and horizontal integration (i.e. different departments or governments in different locations).		
	e-democracy	It is a long-term goal for e-government development. By offering tools such as online voting, polling and surveys, governments attempt to improve political participation, citizen involvement, and politics transparencies.		
Janowski Digital Government Evolution Model	Digitization	Digitizing government information, and automating operations and public service delivery	- Concise and easy to follow - It follows institutional transformations	- It supports a must-go-path form each stages
	Transformation	Electronic Government - improving the internal working and culture of government and facilitating institutional reform through digital technology.		

(Janowski, 2015)	Engagement	Electronic Governance - Engaging citizens and other nonstate actors in government decision making and building trust.	(sector specific goals)	
	Contextualization	Enabling sectors, territories, communities, citizens, etc. to pursue development action by themselves.		

Table 2.5 illustrates the four phases of the Digital Government evolution model (Janowski, 2015) and their characterization depending on the three variables, including internal government transformation, Transformation that affects external relationships, and Transformation is context-specific.

Table 2. 5: Janowski Digital Government Evolution Model (Janowski, 2015)

Stages	**Internal government transformation**	**Transformation affects external relationships**	**Transformation is sensitive to the context**
Digitization	no	no	no
Transformation	yes	no	no
Engagement	yes	yes	no
Contextualization	yes	yes	yes

Contextualization stage of the Digital Government evolution constitutes a significant step beyond other the first three initial stages functionalities - digitizing government, improving the internal operations of government and improving the relationships between government and constituencies - but it covers on improving the conditions for these constituencies to develop themselves by putting their outcomes at the service of public policy and development - specialization of Digital Government initiatives to local, sectorial and local-sectorial contexts (Janowski, 2015). According to Janowski (2015), the contextualization stage involves "the choice of locally-relevant and/or sector-specific goals, locally-acceptable and sectorally-feasible ways of pursuing such goals, and managing the impact on the local environment and sector involved".

Different researchers (Kalbaska, Estevez & Janowski, 2017; Janowski, 2015) indicates that the contextualization-stage of Digital Government has been applied to different sectorial contexts including Tourism – Destination resilience and smart tourism destinations (Gretzel & Scarpino-Johns, 2018); agriculture, e.g., the installation of appropriate and cost-effective mobile government services (Ntaliani, Costopoulou, & Karetsos, 2008), Androidbased online cattle card system for recording quality cattle in Semarang regency(Sugihartiet al., 2019), and Internet of Things for sophisticated e-governance in agriculture (Kumar, 2017); customs, e.g., the adoption of e-customs platforms (Urciuoli, Hintsa, & Ahokas, 2013); taxation, e.g., e-taxation system and its impact in Lagos state in Nigeria (Nchuchuwe & Oji, 2017); healthcare, e.g., evaluation of information technology in healthcare systems and patient monitoring through ICT (Krasniqi, Qehaja & Gabor, 2018) and A Smart Cross Border e-Gov Primary Health Care Medical Service (Sideridis, 2019); insurance, e.g., impact of the Florida Public Hurricane Loss Model (Chen et al., 2009); justice – adapting justice to technology and technology to justice worldwide experience (Ontanu, 2019); and water – Contribution of ICT monitoring system in agricultural water management and environmental conservation (Yoshida et al., 2017). This research focuses on the application of Digital Government on whistleblowing application sectors.

As a part of the Digital Government evolution model, the cause-effect framework will be used in this research to evaluate whether such a model can also be used in the whistleblowing domain. The framework discusses how organizations respond to such challenges by using accessible digital technologies at the time to improve and innovate their services, processes, structures, and policies and then over time these digital innovations are mainstreamed and institutionalized into government practice. To explore the relationship between whistleblower protection and Digital Government, the nature of whistleblowing and whistleblower protection concerning the four stages of Digital Government Evolution model (Janowski, 2015) can be analyzed.

In the Digitization stage, it concerned on practices focuses on technological development in a government without existing whistleblowing and whistleblower protection processes and work practice improvement. Whistleblower uses technologies like complain hotlines, new digital channels to report wrongdoing in an organization.

In the Transformation stage, government agencies transform internal information processes to support and protect whistleblowers internally. Government utilizes technology to improve organizational environment within government, on transforming the internal working of government through technology. Enabling better integration of technology and internal administration of institution to handle whistleblowers protection is crucial. Government could use middleware technologies for whistleblowers electronic records and digital signature to support burden of proof by transforming the internal working of government through technology and this could be institutionalize. All the institution information resources and services are well secured using appropriate controls and whistleblower information would not be available which could be used for reprisal.

In the Engagement stage of Digital Government Evolution model, the government whistleblowing portals accessible to all and engage citizens in government decision-making and the government data available online for all stakeholders including businesses and non-profits to build useful services for citizens. One of the example to engagement stage in Digital Government model is the launch of www.whistleblowing.gcg.gov.ph whistleblowing portal to curb corruption in government-owned and -controlled corporations (GOCCs) aimed at curbing corrupt practices in state-owned corporations in Philippines 2016 (ABSCBN, 2018). As per Janowski (2015) “Government is expected to create and maintain a platform for all relevant actors to create public value through collaboration and innovation and this role requires a range of legal, institutional, cultural and other transformations”. In addition, government agencies apply concrete whistleblower protection legislation on effective decision making process and whistleblowing on behalf of external organization outside government are protected by whistleblower protection mechanism including anonymity and confidentiality. Whistleblowers are unlikely to use Digital Government services without a guarantee of privacy and security. Governments also need to have a strong interest in maintaining whistleblowers trust - information provided will not be misused. Ensuring that Digital Government initiatives are in step with whistleblowers expectations in this area is a crucial means of building trust taking in to account the government need to adopt technological, organizational, social, legal values to protect whistleblowers.

Digital Government is not just digitize government information, utilizing technology to improve organizational environment within government and improving the relationships between government and its constituencies but also on “improving the conditions of these constituencies through better organization within government and improved relationships with government due to transformative use of technology” (Janowski, 2015). Janowski states that “Contextualization stage focus on a specific application environment”. Xnet (exEXGAE) - (whistleblowing platform against corruption for the City Council of Barcelona) is an example of how contextualization stage of Digital Government contribute in whistleblower protection. Xnet makes Barcelona City Hall the first municipal government to invite citizens to use tools which enable them to send information securely that guarantees privacy and gives citizens the option to be totally anonymous.

2.18. Digital Government in Ethiopia

As one of the fastest-growing economies in sub-Saharan African countries, Ethiopia has shown enormous economic success (more than 10 percent economic growth) with promising prospects for the future (MCIT, 2016). Implementation of effective, efficient and transparent governance is essential to ensuring dependable and responsible service delivery to citizens, and it remains one of the key drivers for sustainable economic development. These include the administration of e-services to replace manual operations at government institutions to ensure a faster disbursement of services, and Digital Government areas are a valuable tool to meet good governance goals. Researches indicates that e-Government is an effective way of improving public service delivery to citizens as well as substantially improving the ease of doing business for enterprises (Roy, 2017). In recognition of this, the government of Ethiopia considers e-governance as is a key enabler to ensure Streamlined, Meaningful, Adaptable, Relevant and Transparent business regulations in a country (MCIT, 2016). The government vigorously promoted an e-Government initiative since 2011 (MCIT, 2011). The first e-Government Strategy was between 2011 and 2015 (MCIT, 2015). The vision of the e-Government strategy has four key elements - Bring the Government closer to the people, Effective governance, improved service delivery, and Socio-Economic growth. These strategy envisages implementation of 219 e-services comprising informational and transactional services over a five year period. This strategy resulted in the implementation of 168 services on the national portal and the others still ongoing. The goals of this initiative include better internal efficiencies within the government organizations, better and more efficient delivery of government information and services for the general public, increased productivity among public servants, the encouragement of citizens' participation in government, and the empowerment of all Ethiopians in line with the development priorities outlined in Ethiopia's Vision.

Ethiopia’s Digital Government electronic enablement of services provides eServices around citizen needs both Informational Services (79 services) and Transactional Services (140 services), includes Online application of Registration as a Taxpayer, Online filling of Tax Return (Land tax, Rental Housing tax (paid by owner), Turnover tax, TV tax, VAT, and Excise tax) in Revenue and Customs Agency, and Web-based information publishing, Pension services (Pensioner registration, and pension payment) for Social Security Agency (MCIT, 2016). These online services benefit citizens and government, as well as increase government accountability, by making its operations more transparent and reducing opportunities for corruption (Walle, Janowski & Estevez, 2018). Digital services offer the opportunity for growth, such as livelihood, employment, and training in entrepreneurship (Jobe, 2009).

The Ethiopian’s e-Government strategy has been designed with a customer-centric focus so as to facilitate the delivery of services to customers (residents, businesses and visitors) and information through alternate channels in a manner that is convenient for the citizens and is in line with their expectations and aspirations (MCIT, 2016). Thus, Digital Government initiatives enable a paperless environment promote streamlined processes and make communication with government agencies more convenient for the public. This initiatives allows citizens to acquire and disseminate information, print forms, and submit complains, bids and proposals on the internet (Carter & Belanger, 2005). Additionally, the strategy was an electronic enablement of 219 services to be delivered through alternate channels such as the internet, mobile, call centre and the citizen facilitation centres (MCIT, 2016). The introduction of these alternate channels empowers the people with the choice of how, when and where they interact with the government to improve the customer satisfaction levels with the government services. According to Ethiopian Digital Government Strategic Implementation Plan 2020, 6 strategic plans, 39 nationwide programs, 40 ministry/agency level initiatives with 320 e-services are identified along the Enabling environment, e-Readiness Usage dimensions and operating models. Strategic Implementation Plan states that the vision of Digital Government strategy (MCIT, 2016) is

"To Realize the economic growth of Ethiopia and provide ***A****ffordable & quality services to all Stakeholders thereby* ***D****elivering effective, efficient and transparent governance, through* ***I****nnovation in everything we do, creating* ***c****ulture of entrepreneurship, Affecting the life of all Ethiopians and Leveraging SMART government initiatives".*

2.19. Digital Government whistleblowing initiatives in Ethiopia

As in many other parts of the world, there are signs that corruption and fraudulent activities taking roots and causing certain problems in Ethiopia as well (Rahman, 2018). Corruption remains a huge challenge in Ethiopia. Transparency International data shows that Ethiopia was ranked 96 out of 180 countries, with a score of 37 on the scale where 100 means very clean and 0 means highly corrupt on the 2019 Corruption Perception Index (TI, 2019). While the causes of corruption are varied, the research shows that the tools often suggested to combat corruption include expanded use of whistleblowing (Schultza & Harutyunyanb, 2015). Considering a key objective of e-governance in attaining transparency is in government procedures, Ethiopian government expands its whistleblowing service to its agencies as a part of its Digital Government strategy. Federal Anti-Corruption Commission (FACC) of Ethiopia expand its services to provide ethics and anticorruption training and information on online platforms to expand the reach of the same and increase awareness among the public (MCIT, 2016).

It also provide a service to register and track complaints online and to protect the identity of the informant/whistleblower - an eService for Complaint registry, Tracking and Witness Protection. The commission uses DARS which is a software for asset registration &

Case management system. The service provides a mechanism to receiving tips off and register; giving protection to witnesses and whistle blowers (if necessary).

Ethiopian Government Offices, ministries and agencies, provides its own corporate whistleblowing channels to fight fraudulent activities. A notable example is Ministry of Mines and Petroleum (MoMP) provides whistleblowing toll free call help lines or hot-lines free call center 6038 to combat fraudulent activities within mine sector including allegations of corruption/ issues involving the approval of mining, trades, reconnaissance, exploration and retention licenses (Mom, 2019). This free hotlines provides anonymous and confidential whistleblowing reporting service to all citizens of the country related with mining sector. Another notable example is Ethiopia Federal Police commission. The commission has eservice which provides both informational and transactional services. The service provides “Inform Us” platform to receive any complains at the federal government levels from all citizen across the country (FPC, 2019).

Another whistleblowing service is from Ethiopian food and drug authority (www.fmhaca.gov.et-service). This Electronic Regulatory Information System allows the citizen to report any drug-related problems, adverse drug reactions, product quality problems, and medical errors. Additionally, the authority provides free call center 8482 and pharmacovigilance@efda.gov.et reporting channels as an optional to report unlawful activities (Fmhaca, 2019).

In devolved countries such as the United States of America, United Kingdom, Canada and Germany, Digital Government whistleblowing services enabled citizens/employs to perform whistleblowing functions, such as reporting misconducts to ensure that serious crimes committed by a person in a senior position, to obtain up-to-date whistleblowing information’s and following the cases (Brevini, 2017; Thorsen, 2016). Compared to the western countries, an African countries of Ethiopia is experiencing substantial obstacles to establish and perfecting its corporate whistleblowing system. Thus, it is important to investigate factors that affect the citizens' acceptance of digitally enabled whistleblowing systems to help the Ethiopian government design and implement better whistleblowing systems.

2.20. Technology Acceptance Model (TAM)

Since its introduction, many researchers use TAM as a framework to explain a variety of human behaviors in the IT adoption context - how users adopt and use new technology (Davis, 1989; Petersen et, al, 2019) and to evaluate numerous different technologies, including email, voice mail, and areas beyond a single technology, such as e-schools, e-health diabetes self-management and mobile library application (Petersen et, al, 2019). TAM shows basic connections flowing in a series of beliefs, attitudes, intentions, and behaviors. When analyzing the actual use of an individual's system, most research concentrate on factors that affect the intention of the individual when adopting the system (Gefen, Karahanna & Elena, 2003; Petersen et, al, 2019).

A general model of TAM is depicted in Figure 2.5. TAM is based on the belief “that perceived ease of use and usefulness can predict attitudes toward technology” (Lederer et. al). Davis (1989) defined perceived usefulness as “the degree to which a person believes that using a particular system would enhance his or her job performance” and perceived ease of use as “the degree to which a person believes that using a particular system would be free of effort” (Torres, Pina & Acerete, 2005). Perceived usefulness of a technology and perceived ease of use of a technology combine to establish an attitude about the technology, affecting decisions as to whether the technology should be adopted. There has been a very few research on e-government services through TAM model in developing countries as shown in Table 2.6.

This study explores the relevance of TAM in the Digital Government enabled whistleblowing setting in Ethiopia and focuses on how Ethiopians behave differently, and exhibit different levels of acceptance, than other Digital Government users. Research’s (Evans, 2019) indicates that digital technologies are playing an increasingly vital role in the daily lives of people in Africa, revolutionizing work and leisure and changing the rules of doing business. They are providing unprecedented opportunities for governments, enabling them to radically transform their complex bureaucracies to become more agile, citizen centric and innovative (Accenture, 2015; Taylor & Todd, 1995). Ethiopia has displayed immense economic progress over the decade with bright prospects for the future. Efficient and effective governance is one of the key drivers for sustainable economic development and digital technologies are a valuable tool to meet the good governance goals (MCIT, 2016).

Lam & Harcourt (2019) suggested that Digital Government whistleblowing initiatives services includes information for whistleblowing activities, government whistleblowing reporting forms and services, whistleblowing policy information, whistleblowing reporting mechanisms, raising awareness of whistleblower protection, and submission of comments to government officials. The citizens find it difficult to organize themselves, coordinate their actions - whistleblowing, monitor public policies and influence public decisions in the absence of Digital Government strategy that encourages citizens' participation by being citizen oriented (Colvin, 2018). Those successful operation of Digital Government whistleblowing initiatives does not depend on the technology, but rather on the people (Brevini, 2017; Thorsen, 2016).

The e-participation portion of the whistleblowing initiatives of the Digital Government was designed to promote and reinforce the emerging TAM adoption model proposed by Davis in 1989. It was anticipated that there would be a sharing of information between the Ethiopian government and different stakeholders involved in the whistleblowing process of its Digital Government initiative. Thus, this study focuses on the influential factors of Digital Government whistleblowing success from the perspective of Ethiopian's citizens.

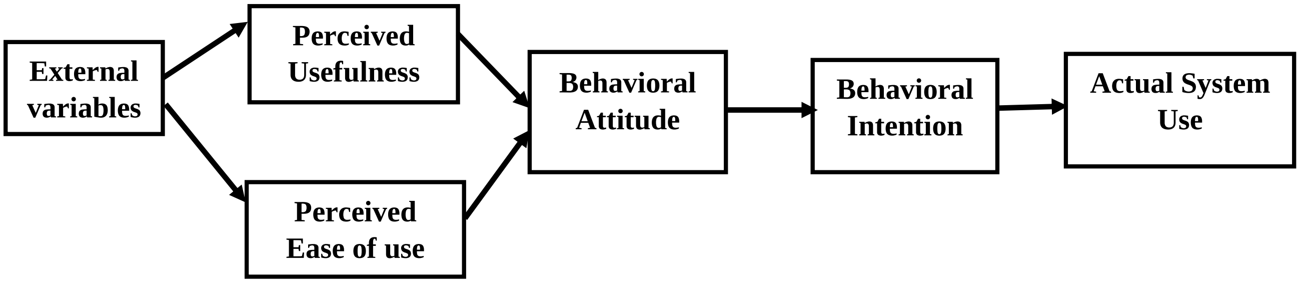


Figure 2. 5: The Technology Acceptance Model (TAM) (Adopted from (Davis, 1989))

Table 2. 6: Literature Review of e-government services evaluated through TAM model in developing countries

Studies	**Title**	**Research Purpose**	**Sample**	**Result**	**Sources**
Nandal & Singla (2019)	Investigating the impact of metaphors on citizens' adoption of e-governance in developing countries: An empirical study	The aim is to investigate the effect of metaphor "Digital India-Power to Empower" on citizens' intention to adopt the e-governance	Total of 224 respondents from India using a structural equation modeling technique	The result shows that the Metaphoric promotion of E-Governance leads to a higher intention to adopt E-Governance - Attitude leads to citizens' emotional attachment with E-Governance which in turn leads to citizens' positive behavioral intention to adopt E-Governance.	Transforming Government: People, Process and Policy
Srimuang et, al. (2017)	The study of public organization's intention to use an open government data assessment application: Testing with an applicable TAM	To test the acceptance of Thailand Open Government Data (OGD) application by using the Technology Acceptance Model (TAM)	The data were collected from 30 public organizations.	The result shows that most public organizations intend to use the application proposed model.	2017 12th International Conference for Internet Technology and Secured Transactions, ICITST 2017 pp. 231-236
Yarlikaş, Arpaci & Afacan (2012)	User acceptance of egovernment services: Analysis of users' satisfaction level based on	To identifies user satisfaction levels of e-School system eGovernment services in Turkey	The sample was taken from 30 teachers who are working in public and private schools in turkey through an Internet-based survey	The authors found that five main factors have a significant effect on the satisfaction of users related to the e-School system - Utilitarian ease of use, system	Innovation Policy, and Economic Growth through Technological Advancements

	technology acceptance model (Book Chapter)		questionnaire was applied.	usefulness, system content, system usability, and ease of use.	
Heierhoff & Hofmann (2012)	Adoption of municipal e-government services - a communication problem?(Conference Paper)	To investigate the role of communication in the acceptance of e-government in Germany	The data was collected from 103 citizens in a medium-sized municipality	Results reveal that both users and non-users of e-government services would like governments to provide more information especially on the existence of services.	18th Americas Conference on Information Systems 2012, AMCIS 2012
Alryalat (2017)	Measuring citizens' adoption of electronic complaint service (ECS) in Jordan: Validation of the extended technology acceptance model (TAM)(Article)	To empirically analyze the factors affecting the adoption of electronic government (e-government) systems by people.	A total of 250 usable responses were obtained from the respondents.	The results indicated that the perceived trust as the strongest whereas facilitating conditions as the weakest though significant predictor of behavioral intention.	International Journal of Electronic Government Research
Rabaa'i et, al. (2016)	Adoption of e-Government in Developing Countries: The Case of the State of Kuwait	To examined the factors that influence the adoption of e-government services Kuwait.	A survey collected data from 534 students at a private American University in relation to Kuwait's e-government services.	The results demonstrated that e-Government services adoption can be explained in terms of perceived usefulness, perceived ease of use, computer self-efficacy, subjective norm, perceived credibility, attitude and behavioural intension.	Journal of Emerging Trends in Computing and Information Sciences
Mensah & Min (2017)	Electronic government services adoption: The moderating impact of	To investigate the moderating impact of perceived service	520 completed instruments from public sector works,	The results have demonstrated that perceived service quality of e-government services does not	International Journal of Electronic

	perceived service quality(Article)	quality on the positive relationship between perceived usefulness of e-government services and intention to use e-government services.	Senior High School Teachers, and University Students in Accra were collected and used for the data analysis.	have any significant moderating effect on the positive relationship between perceived usefulness and intention to use e-government services.	Government Research
Petersen et, al	Challenges for the adoption of ICT for diabetes self-management in South Africa	To identify the challenges and barriers for the adoption of ICT tools for diabetes self-management in the Western Cape province of South Africa	Sample of 131 diabetic patients using semi structured interviews used.	Results indicate that all Four factors (educational, technological, economic, and sociocultural factors) form barriers to ICT adoption for diabetes self-management.	Electronic Journal of Information Systems in Developing Countries
Chemisto & Rivett (2018)	Examining the adoption and usage of an e-government system in rural South Africa: Examining e-government system adoption (Conference Paper)	To analysis for the adoption and usage of a software solution designed to manage water	qualitative interviews on CCMS useis conducted	External variables like design methods, system cost, novelty, technical costs, system availability and lower financial costs of the system had an impact on Perceived usefulness (PU) and Perceived ease of use (PEOU)	2018 Conference on Information Communications Technology and Society, ICTAS 2018 - Proceedings 29 May 2018, Pages 1-6

2.21. Summary

This chapter has presented a review of the literature in relation to Digital Government and whistleblowing thereby defining the scope of the research. Digital technologies is said to be an integral part of the fight against corruption development through the development of digital enabled whistleblowing initiatives. This chapter has also described the characteristics of Whistleblowers, and has discussed the risks of whistleblowers in exposing unlawful activities within an organization. This chapter also identified Digital Government evaluation models existed in the literature which confirms that Janowski Digital Government evolution model (contextualization stage) can used in sector specific domains. The identification of relevant literature on whistleblowing and Digital Government as well as factors that affect the adoption of Digital Government forms the basis of the research. The literature review shows that there exists a scarcity of literature that conceptualize the contribution of Digital Government in whistleblowing domain. In Addition, the review of the literature indicates that there is no study uses the TAM model to explain and predict user acceptance on whistleblowing systems in Sub-Saharan African Countries and concludes that Organizations in Ethiopia still lag behind in adoption and use of digital technologies in whistleblowing system, is necessary to develop and establish empirical support for the TAM in explaining citizens.

CHAPTER III

CONCEPTUAL FRAMEWORK AND RESEARCH HYPOTHESES

3.0. Introduction

In the literature review chapter, whistleblowing problems and the attributes of Digital Government were described. The use of Digital Government and their advantages must be placed in a framework of structured deployment in order to improve whistleblowing process. This chapter discusses the development of such a framework. This chapter starts by discussing the optimum use of Digital Government, then it presents the proposed model of using Digital Government in whistleblowing, with an overview of the use of Digital Government for effective whistleblowing program is presented. From there, an initial TAM model is proposed that captures the use of whistleblowing system quality and information quality as external variables for TAM, and explains the intention towards engagement and actual citizen participation and involvement in use of digitally enabled whistleblowing services in Ethiopia.

3.1. Digital Government for whistleblowing (DGOV4WB) Conceptual Framework

The conceptual framework of DGOV4WB is developed by explaining both Digital Government (DGOV) domain and whistleblowing (WB) domain independently based on their definition and comprising elements. The detail description of the parts for the development of conceptual framework is clearly stated in the literature review part (chapter two). Near & Miceli defines whistleblowing as “the disclosure by organization members (former or current) of illegal, immoral, or illegitimate practices under the control of their employers, to persons or organizations that may be able to effect action” (Near & Miceli, 1985). Whistleblowers enhance corporate and government accountability by being the first line of defense against wrongdoing, and it is recognized as one of the most effective and powerful tools for protecting the public interest (OECD, 2016c).

According to Transparency International (2013), whistleblowing Domain underpinned by three dimensions as described in the literature review section (section 2.4 to 2.6): 1) whistleblower protection, 2) whistleblowing procedure, and 3) whistleblowing organizational culture (TI, 2013). Following the above dimensions, the whistleblowing domain finds solutions to global problems including frauds, corruptions and any unlawful activities within the organizations. Whistleblowing Domain dimensions and its elements depicted as shown in Table 3.1.

Table 3. 1: Whistleblowing Domain dimensions and its elements (TI, 2013; Near, 1995)

Whistleblowing Dimensions		
Whistleblower Protection	**Whistleblowing Procedure**	**Whistleblowing Organizational Culture**
Anti-retaliation	Reporting mechanism	Communication
Anonymity and confidentiality	Response mechanism	Commitment from top managers
Burden of proof	Monitoring	
Criminal and Civil Liability		

There are numerous definitions of Digital Government provided by different organizations as stated in chapter one (OECD, 2016a; Accenture, 2015). For this study, the researcher adopted the definition of Digital Government from OECD (2016a) – "*Digital Government is digital technologies and user preference integrated in the design and receipt of services and broad public sector reform which is the integral part of government's modernization strategies to create public value*".

According to OECD (2019), DGOV is underpinned by six dimensions of DGOV: 1) User-driven (i.e. focus on user needs and citizens' expectations); 2) Government as a platform (i.e. Governments build supportive ecosystems - working together with the public to address common challenges); 3) Digital by design (i.e. rooting digital transformation within governments); 4) Data-driven (i.e. governments using data as a key strategic resources - uses data to predict needs, shape delivery, understand performance, and respond to change); 5) Pro-activeness (i.e. governments anticipating needs and delivery of services); and 6) Open by default (i.e. disclosing data in open formats - governments that are transparent and accountable). Following these dimensions cover the whole DGOV Solution space.

DGOV4WB --- the use of digital technology to foster governance of Whistleblowing Process and Whistleblowing Protection. It is a composited of (see Figure 1) three primary domains namely Public Governance (GOV), Digital Technology (DT) and Whistleblowing (WB); and three secondary domains: i) Digital Government (DGOV) – intersection between public governance and digital technology; ii) Digital Technology for Whistleblowing (DT4WB) – intersection between Digital Technology for Whistleblowing; and iii) Public Governance for Whistleblowing (GOV4WB) is the intersection of Governance and Whistleblowing. Figure 3.1 shows a mapping of three primary and three secondary domains contributing to DGOV4WB.

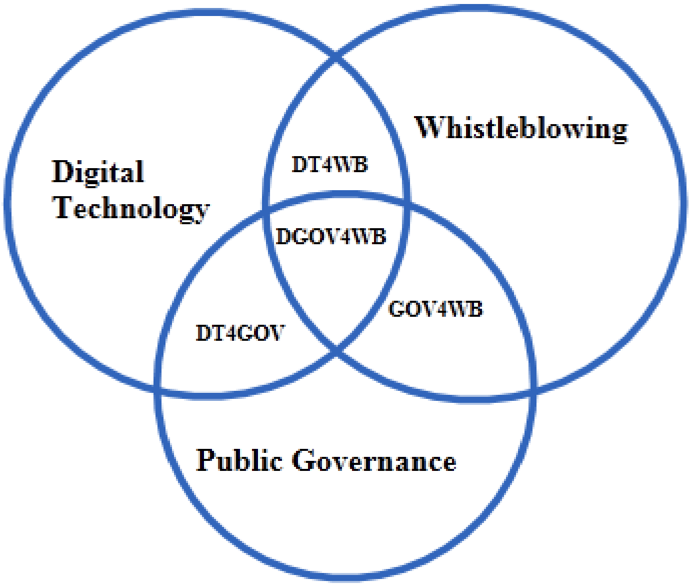


Figure 3. 1: DGOV4WB comprising domains and its relationships

The relationships between the domains are based on the concept of customer service domain relation. According to customer service domain relation, one domain helps the other domain to fulfil its goals. Considering the relationship between DT to WB and DT to GOV, Digital Technology is a service domain that helps to achieve the goal of Whistleblowing and Public Governance and they both are customer domain in this context. Whereas, Governance is service domain in relation to Whistleblowing. Based on the above definitions and list of dimensions the conceptual framework for DGOV4WB is shown in Figure 3.2.

The proposed approach aims to bridge the gap of the problem domain through the solution domains. The novelty of the framework emanates from the three characteristics – problem domain, solution domain and mapping of WB. It shows the contribution of Digital Government in solving the issues/problems of the whistleblowing domain as discussed in the literature review. The mapping is necessary in order to provide a quick and efficient means for understanding the relationships between Digital Government solutions and whistleblowing problem.

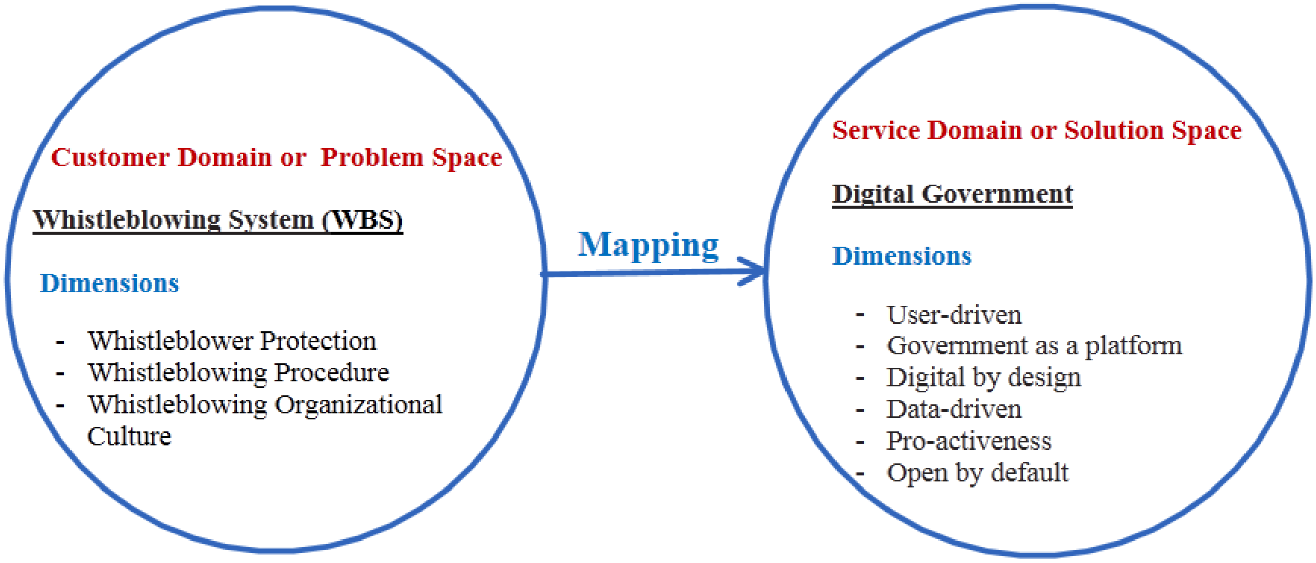

Customer Domain or Problem Space
Whistleblowing System (WBS)
Dimensions
- Whistleblower Protection
- Whistleblowing Procedure
- Whistleblowing Organizational Culture
Mapping
Service Domain or Solution Space
Digital Government
Dimensions
- User-driven
- Government as a platform
- Digital by design
- Data-driven
- Pro-activeness
- Open by default

Figure 3. 2: DGOV4WB Conceptual Framework

3.2. Research Hypotheses and TAM Model in Digital Government Whistleblowing Systems

TAM explains the motivation of users by three factors; perceived usefulness, perceived ease of use, and attitude toward the use of new technology. TAM asserts that intentions to perform behavior determine actual behavior (Davis, 1989). Intention itself represents an individual's attitude toward the behavior. Therefore, not only behavioral intention would be contained in TAM but also perceived usefulness and ease of use have considerable impact on attitude of the user, independent variables that can determine or influence potential user' attitudes toward behavioral intention, while the behavioral decisions ultimately dictate whether and how a technology is used (Davis, Bagozzi & Warshaw, 1989).

Davis (1989) indicates that perceived ease of use and perceived usefulness are shaped by external factors unique to the situation and called for further research to consider the role of additional external variables that influence perceived ease of use and perceived usefulness. Two important external variables – Whistleblowing systems quality and information quality – have been consistently found to be influential factors that affect the perceived usefulness and ease of use of IT. Whistleblowing systems quality, subjective norm, and information quality are the three critical external variables repeatedly found to be a significant factor affecting the perceived usefulness and ease of use of the whistleblowing system. Table 3.2 summarizes the preliminary study relevant to the variables used in the TAM empirical analysis mainly in developing countries (evaluation of e-government services through TAM model in developing countries).

Table 3. 2: Literature Review of evaluate e-government services through TAM model in developing countries

Studies	Title	Research Purpose	Sample	Result	Sources
Nandal & Singla (2019)	Investigating the impact of metaphors on citizens' adoption of e-governance in developing countries: An empirical study	The aim is to investigate the effect of metaphor "Digital India-Power to Empower" on citizens' intention to adopt the e-governance	Total of 224 respondents from India using a structural equation modeling technique	The result shows that the Metaphoric promotion of E-Governance leads to a higher intention to adopt E-Governance - Attitude leads to citizens' emotional attachment with E-Governance which in turn leads to citizens' positive behavioral intention to adopt E-Governance.	Transforming Government: People, Process and Policy
Srimuang et, al. (2017)	The study of public organization's intention to use an open government data assessment application: Testing with an applicable TAM	To test the acceptance of Thailand Open Government Data (OGD) application by using the Technology Acceptance Model (TAM)	The data were collected from 30 public organizations.	The result shows that most public organizations intend to use the application proposed model.	2017 12th International Conference for Internet Technology and Secured Transactions, ICITST 2017 pp. 231-236
Yarlikaş, Arpaci & Afacan (2012)	User acceptance of egovernment services: Analysis of users' satisfaction level based on technology acceptance model (Book Chapter)	To identifies user satisfaction levels of e-School system eGovernment services in Turkey	The sample was taken from 30 teachers who are working in public and private schools in turkey through an Internet-based survey questionnaire was	The authors found that five main factors have a significant effect on the satisfaction of users related to the e-School system - Utilitarian ease of use, system	Innovation Policy, and Economic Growth through Technological Advancements

			applied.	usefulness, system content, system usability, and ease of use.	
Heierhoff & Hofmann (2012)	Adoption of municipal e-government services - a communication problem?(Conference Paper)	To investigate the role of communication in the acceptance of e-government in Germany	The data was collected from 103 citizens in a medium-sized municipality	Results reveal that both users and non-users of e-government services would like governments to provide more information especially on the existence of services.	18th Americas Conference on Information Systems 2012, AMCIS 2012
Alryalat (2017)	Measuring citizens' adoption of electronic complaint service (ECS) in Jordan: Validation of the extended technology acceptance model (TAM)(Article)	To empirically analyze the factors affecting the adoption of electronic government (e-government) systems by people.	A total of 250 usable responses were obtained from the respondents.	The results indicated that the perceived trust as the strongest whereas facilitating conditions as the weakest though significant predictor of behavioral intention.	International Journal of Electronic Government Research
Rabaa'i et, al. (2016)	Adoption of e-Government in Developing Countries: The Case of the State of Kuwait	To examined the factors that influence the adoption of e-government services Kuwait.	A survey collected data from 534 students at a private American University in relation to Kuwait's e-government services.	The results demonstrated that e-Government services adoption can be explained in terms of perceived usefulness, perceived ease of use, computer self-efficacy, subjective norm, perceived credibility, attitude and behavioural intension.	Journal of Emerging Trends in Computing and Information Sciences
Mensah & Min (2017)	Electronic government services adoption: The moderating impact of	To investigate the moderating impact of perceived service quality on the positive	520 completed instruments from public sector works, Senior High School	The results have demonstrated that perceived service quality of e-government services does not have any significant moderating	International Journal of Electronic

	perceived service quality(Article)	relationship between perceived usefulness of e-government services and intention to use e-government services.	Teachers, and University Students in Accra were collected and used for the data analysis.	effect on the positive relationship between perceived usefulness and intention to use e-government services.	Government Research
Petersen et, al	Challenges for the adoption of ICT for diabetes self-management in South Africa	To identify the challenges and barriers for the adoption of ICT tools for diabetes self-management in the Western Cape province of South Africa	Sample of 131 diabetic patients using semi structured interviews used.	Results indicate that all Four factors (educational, technological, economic, and sociocultural factors) form barriers to ICT adoption for diabetes self-management.	Electronic Journal of Information Systems in Developing Countries
Chemisto & Rivett (2018)	Examining the adoption and usage of an e-government system in rural South Africa: Examining e-government system adoption (Conference Paper)	To analysis for the adoption and usage of a software solution designed to manage water	qualitative interviews on CCMS useis conducted	External variables like design methods, system cost, novelty, technical costs, system availability and lower financial costs of the system had an impact on Perceived usefulness (PU) and Perceived ease of use (PEOU)	2018 Conference on Information Communications Technology and Society, ICTAS 2018 - Proceedings 29 May 2018, Pages 1-6

A review of relevant literature on the Ethiopian Digital Government systems reveals wide range of digital technology implementations in most government departments and private sectors (EGES, 2019; MCIT, 2015, 2016). When citizens use Ethiopian Digital Government whistleblowing initiatives to look for information or to start a particular administrative whistleblowing procedure, they tend to expect more efficiency and effectiveness when compared to their expectations of the traditional whistleblowing service counter approach. Citizens will perceive the Ethiopian Digital Government whistleblowing initiatives to be a useful resource if it can help them collect information related to whistleblowing or complete administrative whistleblowing procedures quickly, easily and effectively, and furthermore report unlawful activities anonymously and confidentially (Brevini, 2017; Libit, Freier & Draney, 2014; Thorsen, 2016).

According to (Ajzen & Fishbein, 1972; Lin, Fofanah & Liang, 2011; Rabaa'I et. al., 2016), information quality, attitude and the subjective norms are important factors on the behavioral intention, a proposition that is supported by TAM. People with a more positive attitude towards IT will possibly be more pleased with the whistleblowing system and will find it more useful (Brevini, 2017; Libit, Freier & Draney, 2014). In addition, whistleblowers who consider whistleblowing systems are open to use and believe that the system does not have enough security for anonymous and confidential reporting will avoid using. Therefore, user attitude and whistleblowing system quality is hypothesized to positively affect perceived usefulness and behavioral intention.

The whistleblowing system is by measuring service quality. Pamungkas, Ghozali & Achmad (2017) defined whistleblowing system quality as the consistency shown in the overall performance of the system and evaluated by the perceptions of whistleblowers. It has a significant influence on the perceived usefulness of individual users. Since citizens are anonymous in the engagement of Digital Government, the whistleblowing system's quality becomes an “electronic storefront” where the first experience is made. If a citizen perceives a whistleblowing system to be of high quality, that citizen will be more likely to use whistleblowing systems to disclose information or access other whistleblowing services (Libit, Freier & Draney, 2014; Torres, Pina & Acerete, 2005; Shahid, 2017).

Subjective norm (or social influence) was hypothesised to have a direct effect on Perceived ease of use, perceived usefulness and behavioural intension (Brevini, 2017; Rabaa'I, 2016). Schepers & Wetzels (2007) indicate that subjective norm has a significant influence on perceived usefulness and behavioral intention to use. Venkatesh (2000) clarified why the subjective norm has a direct effect on intention. Citizens may choose to conduct a behavior even though they are not in favor of the behavior or its effects if they believe that one or more significant referents think they should, and are encouraged enough to comply with the referents. As measured by citizens, information quality (IQ) usually affects their satisfaction and perceived usefulness (Aggelidis & Chatzoglou, 2009). User perceptions of the importance of a whistleblowing system were used by Pamungkas, Ghozali and Achmad (2017) to determine the quality of whistleblowing.

The applications of Digital Government whistleblowing initiatives in Ethiopia promises to enhance whistleblowing services to citizens not only by improving the whistleblowing process and management of whistleblower cases, but also by redefining the traditional concept of a 'speak up' culture that values employees and citizens. With the emergence of whistleblowing system, the country of Ethiopia could combat fraud, unlawful activities and uncovering financial irregularities, Ethiopia could rise to higher levels of social, economic, and political development. This research introduces the following hypotheses based on the theory of TAM (Lederer et. al., 2000; Lin & Lu, 2000) and the research model with the hypothesis and their respective links are shown in Figure 3.3.

H1: Subjective norm has a significant effect on perceived ease of use.

H2: Subjective norm has a significant effect on perceived usefulness.

H3. The whistleblowing systems quality of Digital Government systems positively affects the perceived usefulness of using the digital technologies in reporting misconducts.

H4. The information quality of whistleblowing systems positively affects the perceived usefulness of using the Digital Government whistleblowing systems.

H5. The perceived ease of use of Digital Government whistleblowing systems positively affects the perceived usefulness of using the digital technologies to report misconducts.

H6. The perceived ease of use of Digital Government whistleblowing system has a positive effect on user attitudes toward the use of Digital Government whistleblowing system.

H7: Perceived usefulness use has a positive effect on users' attitude towards Digital Government whistleblowing system.

H8. User attitude on using the Digital Government whistleblowing system positively affects behavior intentions.

H9. The perceived usefulness of the Digital Government whistleblowing services has a positive effect on user behavior intentions.

H10: Subjective norm has a significant effect on behavioural intension.

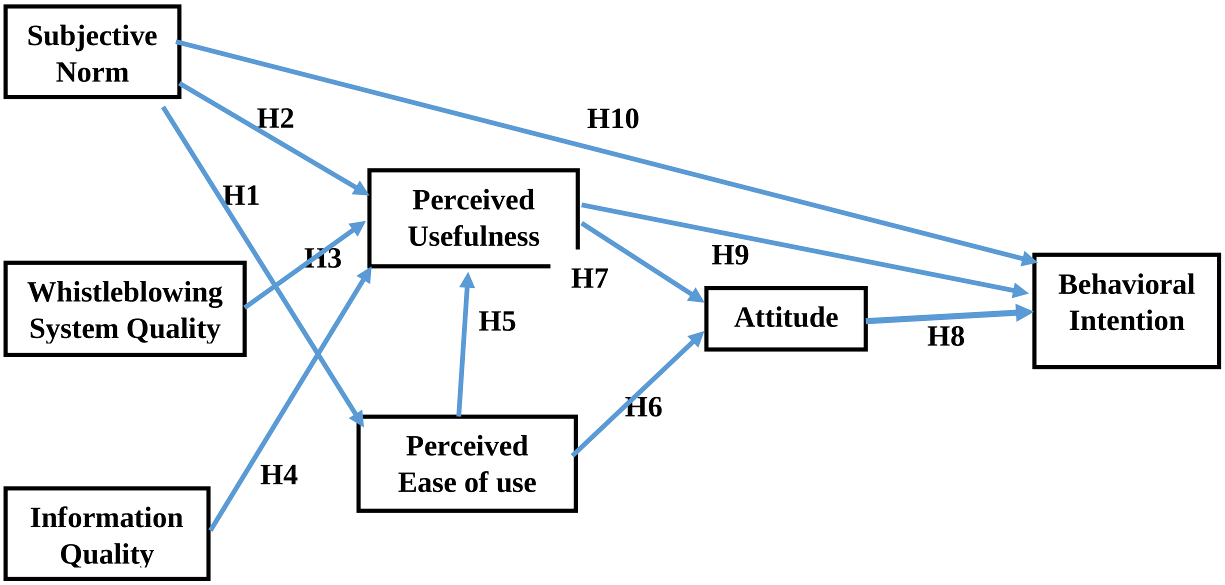


Figure 3. 3: TAM Model in Digital Government Whistleblowing Systems

3.3. Summary

This chapter has presented the conceptual framework for the research by explaining the two (Digital Government and whistleblowing) domains. This conceptual framework used to help to address whistleblowing problems through Digital Government (problem domain through the solution domains). The novelty of the framework emanates from the three characteristics – problem domain, solution domain and mapping of WB. The chapter also presents the TAM Model for Digital Government Whistleblowing Systems, particularly the Ethiopian context. The variables are defined and hypothesizes are stated to be proofed in the latter chapters.

CHAPTER IV

RESEARCH METHODOLOGY

4.0. Introduction

This chapter discusses the procedure by which the research was conducted with a justification for the chosen approach. It addresses the research methods adopted for capturing the data required and analyzed to achieve the research aim. Since this study comprises multiple stages, this chapter starts by describing the development of the research model used in the study. It presents justifications for the chosen research paradigm. Next, the research design that provides an explanation of the research process and methods of data collection and analysis applied in this research is presented, including a discussion of the development of the framework and validation process section. The qualitative research method was used in this study to identify strategies that would assist in increasing the adoption and effective utilization of Digital Government in the whistleblowing domain, in particular in Ethiopia. Furthermore, the first phase of the research is exploratory and descriptive and will assist in understanding emerging issues that are related to the subject.

4.1. Conducting Research in Digital Government

An on-going issue for debate in Digital Government research concerns the potential value of quantitative and qualitative approaches (Irani, et. al., 2012; Gil-Garcia, Dawes & Pardo, 2018; Hovy, 2008). A few researchers, according to Irani, et. al. (2012) have argued in the past that quantitative research based approach supported by statistical analysis was the most dominant approach applied by authors in the last decade. However, others have found that quantitative research based approach was not able to answer many of the human problems facing public governance and have turned to the body of qualitative-based approaches such as case studies and interviews for help with those problems (Irani, et. al., 2012). Then again, many researchers argue that both qualitative and quantitative approaches, with either deductive or inductive reasoning, are valid approaches for research in such information science and public governance contexts (Gil-Garcia & Pardo, 2016; Bolívar, Muñoz & Hernández, 2012; Irani, et. al., 2012).

Qualitative data is usually subjective (verbal) data and the two research methods used most often in qualitative research within the Digital Government are literature review and the case study approach (Irani, et. al., 2012) – with case studies, in particular, being used extensively in Digital Government research. Two types of case studies are used in the Digital Government sciences – the single case (embedded) - within a single case study, there are multiple units of analysis and multiple case (embedded) – Multiple case study (closely related cases) with multiple unit of analysis. It is also known that qualitative approach provides detail understanding of an issue, because it arises out of researching few individuals and exploring their views in great depth.

However, using a qualitative methodology alone would not free of problem (Creswell, 2017). There is also a concern of data generalization, since there is a limited number of people involved in interviews or focus group discussion or other qualitative methods. Furthermore, users such as policy makers, practitioners and others demand forms of what so called 'sophisticated' evidence, which are difficult to fulfil by those methods (Santos, et. Al., 2017; Creswell & Clark, 2017). On the one hand, a qualitative research approach is able to accept complexity and subjectivity and enables the researcher to use his/her experiences and perceptions observations of the phenomenon to gain insights and explore meaning about a specific experience, circumstance, cultural aspect or historical event (Bryman, 2016).

Quantitative research is focused on measuring and analyzing the causal relations among variables. Santos et. Al. (2017), among others, has discussed the distinction between quantitative and qualitative research by arguing that quantitative research refers to measureable and countable matters, while qualitative research refers to the meanings, concepts, definitions, characteristics, metaphors, symbols and descriptions of such matters. Bryman (2017) describes "*Quantitative research is especially efficient at getting to the* *'structural' features of social life, while qualitative studies are usually stronger in terms of 'processual' aspects* “.

On the other hand, Creswell (2017) states that the quantitative research mode is not ideal for exploring or describing such complexities, but is more suitable to validate what is already known about a phenomenon. Furthermore, quantitative research helps only the researcher to familiarize him / herself with the issue or concept to be examined and possibly generate hypotheses to be tested (Bryman, 2016).

Some might take the view that these respective approaches are entirely distinct, while others would be able to combine them by what is often referred to as 'mixed methods' for the unique and specific benefits they offer to understanding the topic under investigation. The objective of a mixed methods approach, then, is to extract benefits from both research approaches and address their weaknesses. This is commonly accepted that the use of interviews and observation is qualitative, whereas survey methods that extract measureable data from specifically constructed surveys of respondents or observed events are also accepted to reflect a quantitative approach.

4.2. Selecting the Research Design

A research design provides a framework for the collection and analysis of data (Bryman, 2016). Selection of a research design has been described as choosing “a procedural plan that is adopted by the researcher to answer questions validly, objectively, accurately and economically” (Kumar, 2019).

In general, as has already been noted, a choice must be made between approaches to qualitative, quantitative and mixed methods (Bryman, 2016; Hollstein, 2014; Creswell, 2017). The qualitative research approach typically includes asking questions, collecting replies, and performing inductive data analysis to create pictures of universal concepts and understandings from individual comments and responses, and through a method involving the researcher in interpreting the meanings (Holliday, 2007). In contrast, the process of quantitative research most often involves examining the relationships among measured variables using statistical procedures (Hollstein, 2014). Whereas, work on mixed methods includes the collection or analysis of both quantitative and qualitative data in a single study where the data are collected simultaneously or sequentially, are given a priority, and requires the integration of data at one or more stages in the process of research' (Bryman, 2016). Hollstein (2014) indicates that using mixed approaches, researchers can generalize from a sample to a population at the same time and obtain a deeper, contextual understanding of the phenomenon being investigated. Similarly, Bryman (2016) claims that mixed methods study is a rational process and pragmatic method, while stressing the value of using this process because the researcher is also conscious of possible drawbacks – one of which could be fairly costly as an approach.

A mixed method methodology was deemed most suitable for the present research study because this was felt to improve the validity of the results (Greene, 2007). The choice of a mixed mode of research for this research is consistent with the aim of the research to evaluate a complex phenomenon by taking into account the context of its settings. The history of mixed methods research actually started with researchers who believe that both quantitative and qualitative methods are useful as they address the research questions. Mixed methods researchers believe that combining both methods would compensate their weaknesses and would provide cohesive and comprehensive outcomes (Creswell, 2017). However, in the field of Digital Government in particular, mixed method is still under-utilized (Gil-Garcia & Pardo, 2016; Bolívar, Muñoz & Hernández, 2012). Thus, applying a mixed methods research would be a contribution for research in Digital Government.

The decision of the most appropriate design for this research was again based on the research questions and objectives. As stated earlier in chapter one (page 8) that this research is exploring the impacts of Digital Government on whistleblowing domain and to access the Citizen Adoption of Digital-Government whistleblowing system initiatives in Ethiopian. Based on the discussion on theoretical framework in chapter three, researcher proposed an initial research model (DGOV4WB conceptual framework) in Figure 3.2 and initial TAM model in Digital Government Whistleblowing Systems in Figure 3.3. In order to test the applicability of the initial TAM model, a qualitative approach based on field study of semi-structured interview was conducted. The field study was important to explore and refine the initial model, which then examined through quantitative approach based on survey (detail of research methods will be discussed in the next section). Based on the brief description of the methods and research objective, this research employed *exploratory sequential design* with the quantitative approach (*instrument-development variant*) as the major method.

4.3. Research Philosophical Paradigm

Saunders et al. (2003 & 2009) demonstrate that the philosophy of research is shaped by the way a researcher describes the acquisition and development of knowledge and can affect the way the researcher performs the study himself. Holden and Lynch (2004) states that ontology and epistemology are the two fundamental concepts of philosophy that have to be considered to match the research approach.

4.3.1. Epistemology

According to Grix (2002), Epistemology focuses on the knowledge-gathering process and is concerned with developing new models or theories that are better than competing models and theories. Epistemology is concerned with the theory of knowledge especially concerning its methods, validation and the possible ways of obtaining knowledge of social truth, or whatever it is understood to be (Grix, 2002). The epistemological assumption can be separated into either positivistic or interpretivist paradigms (Collis & Hussey, 2003). The rhetoric of positivism versus interpretivism has been widely studied by different researchers (Lin, 1998).

In this research a positivistic and interpretivism epistemology was experienced. Positivist and interpretivist modes of research can be addressed as supplementing each other. Where positivism can reveal causal interactions and relationships, causal processes and mechanism can be emphasized by interpretivism (Lin, 1998). In other words, positivism allows to discover causal ties between digital government and whistleblowing domain phenomenon, while interpretivism allow to profoundly examine the nature of these relationships and reveal their mode of action and their causal mechanisms. In this regard, in any research that aims for completeness, the two epistemological approaches should supplement each other. The previous researches suggest, digital government have been dominated by the positivist perspective, and thus, the application of interpretivist methods can greatly enhance research in these fields.

In addition, interpretivists typically perform a literature review to establish a detailed understanding of the subject under investigation, then create research questions on the basis of the literature review and prepare to conduct the analysis (Williamson et al., 2002). This research adopts literature review and case study as the main methods. The study considers the relationship between digital government and whistleblowing domain. While positivist approach has been used if it the research questions develops from the literature where variables and theories may exist that need to be tested and verified (Creswell, 2007). This where TAM model has been used to test the adoption of digitally enabled whistleblowing initiatives in case of Ethiopia.

4.4. Research Methods

The research methodology for this research comprises 9 main activities that are depicted in Figure 4.1 and described below. The first step in the methodology aims at identifying and documenting the most significant research literature in the Digital Government and whistleblowing domain. It involves data collection by selecting keywords to search for relevant publications on Scopus – the largest abstract and citation database of peer-reviewed literature, ACM Digital Library and Wiley InterScience. The outcome of this step is described in Section 4.4.1.

The second step in the methodology aims at identifying the source and documenting the policy literature including recommendations, initiatives, and experiences produced by research centers and major international organizations worldwide in the whistleblowing domain like the UN, EU, TI or OECD. The outcome is described in Section 4.4.2. The third step in the methodology aims at identifying the source and documenting the countries whistleblowing legislation in a country across the world. The outcome is described in Section 4.4.3.

The first three steps involves an extensive literature, policy and whistleblowing legislation review to identify the issues and gaps in the phenomenon of whistleblowing and Digital Government. Researcher identified potential key variables and developed an initial research model. The initial research model then was explored and enhanced using qualitative method. Qualitative method is suitable in exploring and capturing reality in detail, especially when the experiences of the actors are important (Chan & Ngai, 2007). The fourth step in the methodology aims in producing the whistleblowing performance measurement framework based on the inputs obtained from the research literature review, policy literature review and whistleblower legislation review. The fifth step involves developing a conceptual framework for DGOV4WB. The sixth step involves developing Digital Government Innovation cause-effect framework for whistleblowing and whistleblower protection based on janowski (2015) Digital Government evolution model. Through adopting DGOV4WB Assessment framework in seventh step, the eighth steps describes validating the impact of Digital Government on whistleblowing system through analyzing the case studies and indict where Digital Government can enhance the performance of whistleblowing initiatives. The final step, step nine, validating the impact of Digital Government for whistleblowing in Ethiopian context through Technology Acceptance Model (TAM). Based on the comprehensive research model, hypotheses were proposed to justify the relationships among constructs. Items for each construct were also identified and based on analysis of relevant literature and the feedback obtained from our interviews, the first version of a survey questionnaire was designed. Researcher performed pilot study to ensure the applicability and comprehensibility of the questionnaire. And eventually, there was a regional survey in Ethiopian involving 610 respondents- employees of public organizations - in Ethiopian. Survey data was analysed using SEM (Structural Equation Model) based on PLS (Partial Least Square). Therefore, this research basically employed two basic steps of data collection, which are pilot study and national survey. Description of each step are discussed in the sections below.

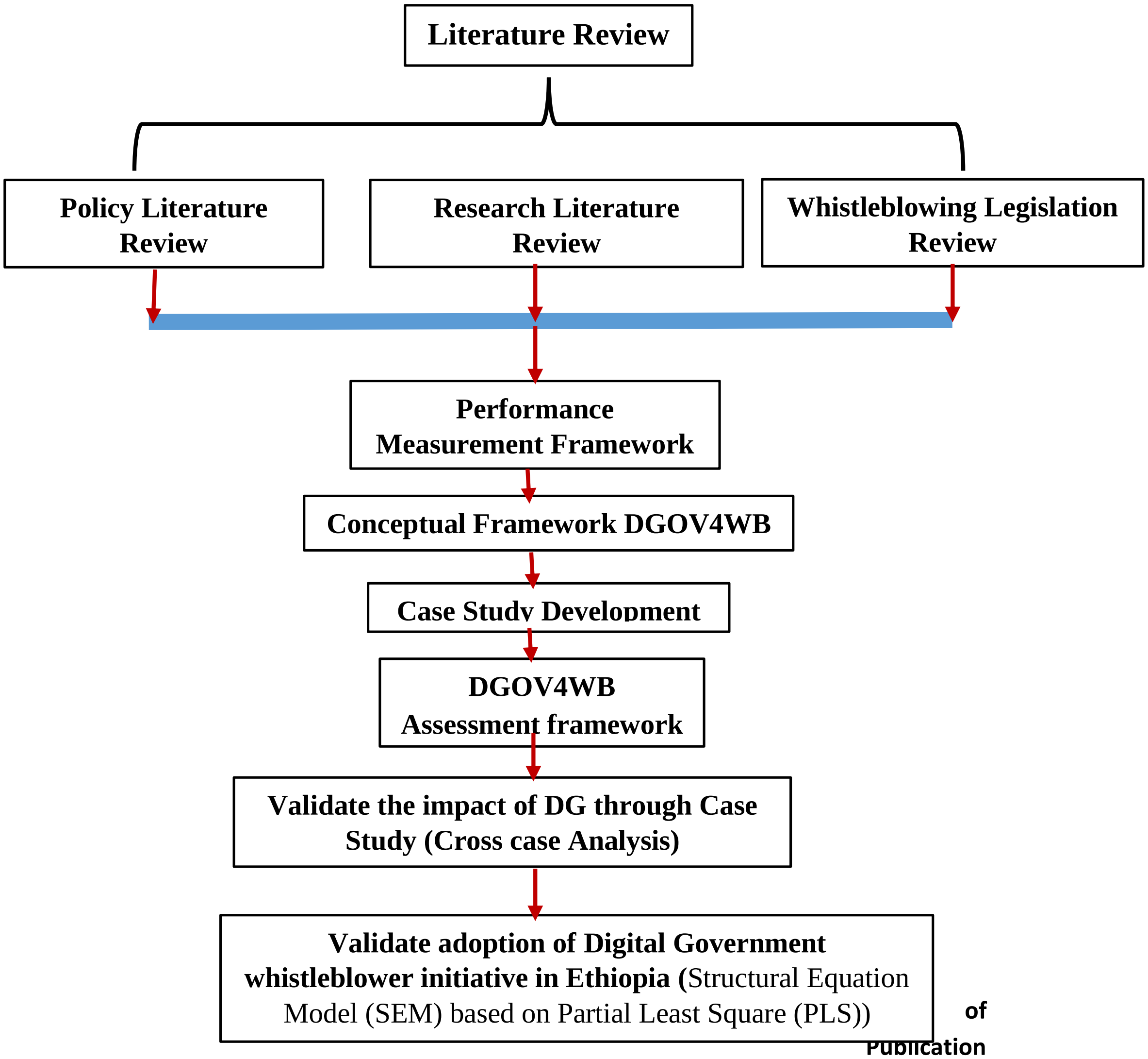

Literature Review
Policy Literature Review
Research Literature Review
Whistleblowing Legislation Review
Performance Measurement Framework
Conceptual Framework DGOV4WB
Case Study Development
DGOV4WB Assessment framework
Validate the impact of DG through Case Study (Cross case Analysis)
Validate adoption of Digital Government whistleblower initiative in Ethiopia (Structural Equation Model (SEM) based on Partial Least Square (PLS))

Figure 4.1: General Research Methodology

4.5. Qualitative Research Approach

4.5.1. Research Literature Review

Based on the research methodology, Step 1 involves a systematic search of the research literature. This literature review has been used for 3 major tasks including to identify the main stakeholder in the whistleblowing domain, to develop a systematic DGOV4WB research framework and to develop a performance measurement framework to measure the effectiveness of digital technologies enabled whistleblowing system. I.e. to measure the performance of whistleblowing system.

No	Criteria	No of Publication on Scopus
1	Journal Articles	80
	Book or Book Chapters	10
	Conference Papers	7
	Total Number of Publication	97

No	Criteria	No of Publication on Scopus
1	Journal Articles	211
	Book or Book Chapters	22
	Conference Papers	16
	Total Number of Publication	249

No	Criteria	No of Publication on Scopus
1	Journal Articles	211
	Book or Book Chapters	22
	Conference Papers	16
	Total Number of Publication	249

91

Book or Book Chapters
Conference Papers 7

4.5.1.1. Literature Review for whistleblowing performance measurement development (Scope of data collection , Collection and Documenting Articles)

The methodology applied to conduct research literature review for developing performance measurement framework for the whistleblowing included three tasks that are is shown in Figure 4.2 and described as follows: i) Data Collection to determine data sources, select keywords to search for relevant publications, and define criteria to identify publications to be analyzed; ii) Qualitative Analysis to document the main findings from the identified research literature, analyzed according to 3 whistleblowing dimensions identified by Transparency international (TI-NL, 2017): 1) Whistleblowing Procedure; 2) Organizational Culture; and 3)Whistleblower Protection, and iii) Summary of the findings from the qualitative analysis.

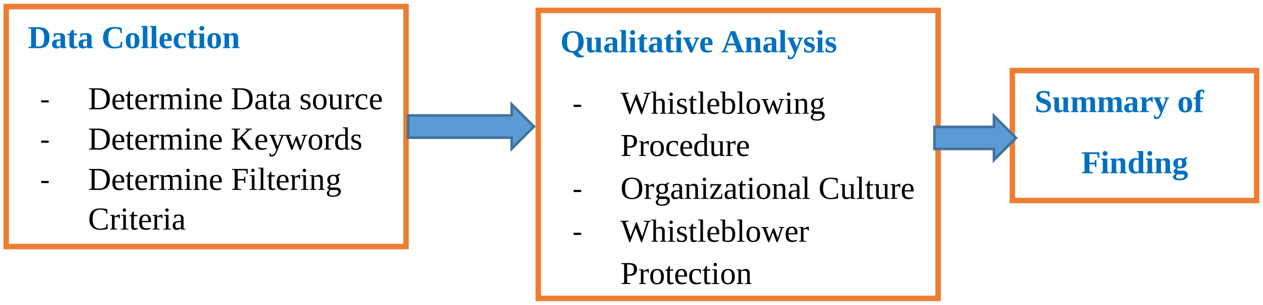


Figure 4. 2: Methodology for Research Literature Review to develop performance measurement framework

The data collection focused on the systematic search of the research literature in the Scopus database, ACM Digital Library and Wiley InterScience, The systematic search conducted using the keywords where they were mainly used to indicate the performance measurements in whistleblowing domain including “Whistleblowing”, “whistleblower”, “Impact”, “outcome”, “Measurement” and related terms in both singular and plural forms as the follows:

(Whistleblowing OR whistleblower OR whistleblowers) AND (performance OR outcome OR

outcomes OR impact OR impacts OR measure OR measures OR measuring OR mea surement)

The above expression was applied to search on Scopus Database, ACM Digital Library and Wiley InterScience on May 20, 2019 against article titles, abstracts, and keywords, and produced 249 publications in the rage of years from 1985 to 2019. To conduct a detailed data analysis of these papers, the researcher used the four-step filtering process to narrow down the number of articles. The first step includes i) identifying the most relevant publications – all journal articles, all book or book chapters, and all-conference papers. It has only 249 and 54 papers excluded.

The second step involves the exclusion of publications with no abstracts. From all 249 papers, the researcher found in step1, 12 Papers excluded - 11 journal articles and 1 conference papers - from the study with no abstract and it remains 237 Papers in total for analysis. Based on the second step in the process, the third step involved determining manually the relevance of each the 237 publications. The determination was done through the publications' titles and abstracts. Finally, the researcher found that only 97 papers were relevant and 140 papers were not non-relevant.

The Fourth step in our data collection process involves looking at the papers on the internet. However, out of 97 papers, 2 conferences and 4 books and 9 journal papers are not available. Finally, 84 publications were selected for detail analysis. The PRISMA flow diagram is depicted in Figure 4.3 and the result of each step of data collection is shown in Table 4.1.

The Qualitative Analysis conducted to document the main findings from the identified research literature, analyzed according to three whistleblowing dimensions identified by Transparency international (TI-NL, 2017): Whistleblowing Procedure, Organizational Culture, and Whistleblower Protection. 46 study papers or 55% of the study papers were cross-sectorial and 38 research papers 45 % were Sectoral with whistleblower protection papers takes the highest percentage by 27% from organizational culture 11% and whistleblowing procedure 7%.

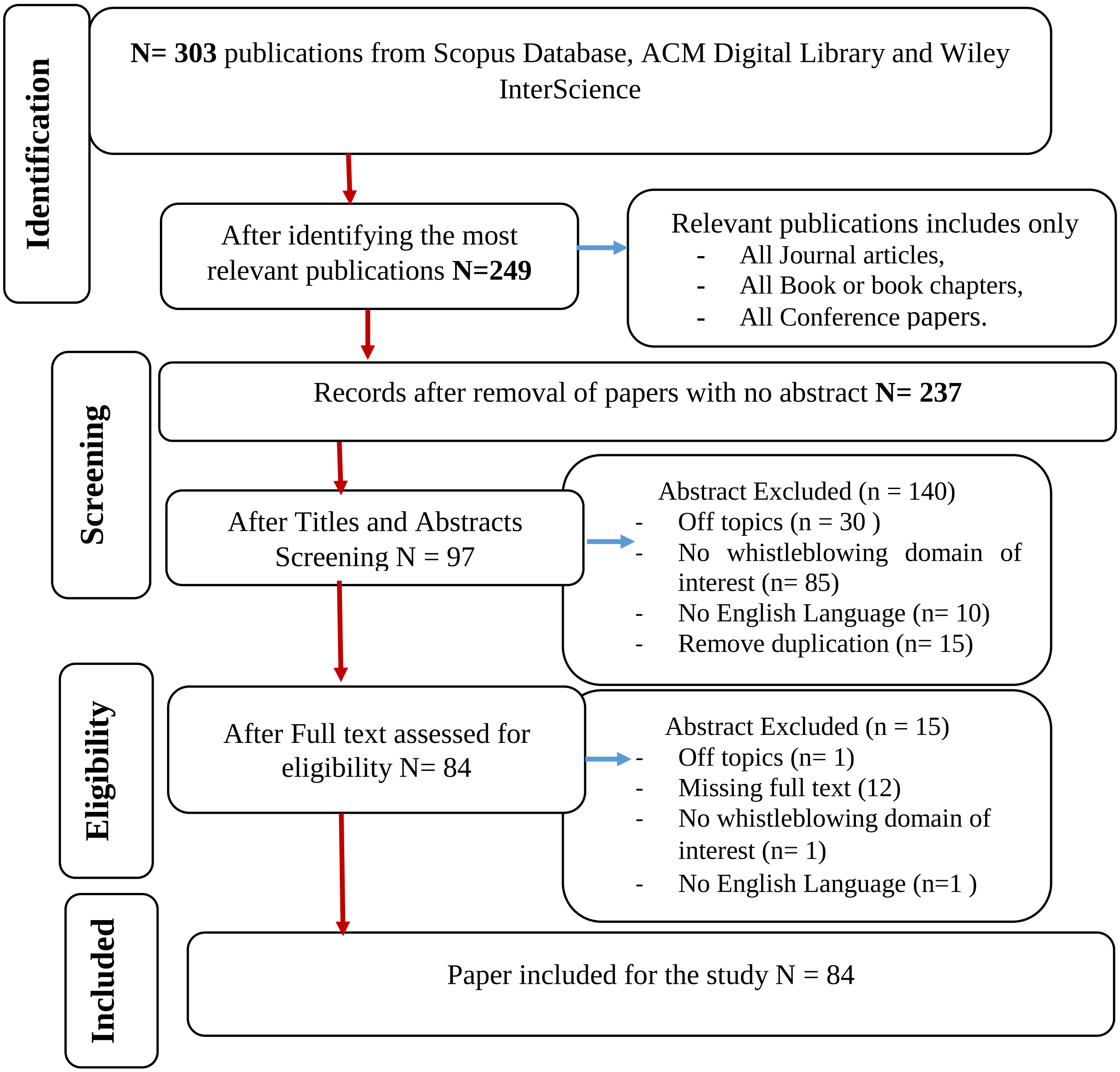

Identification
N= 303 publications from Scopus Database, ACM Digital Library and Wiley InterScience
After identifying the most relevant publications N=249
Relevant publications includes only
- All Journal articles,
- All Book or book chapters,
- All Conference papers.
Screening
Records after removal of papers with no abstract N= 237
After Titles and Abstracts Screening N = 97
Abstract Excluded (n = 140)
- Off topics (n = 30)
- No whistleblowing domain of interest (n= 85)
- No English Language (n= 10)
- Remove duplication (n= 15)
Eligibility
After Full text assessed for eligibility N= 84
Abstract Excluded (n = 15)
- Off topics (n= 1)
- Missing full text (12)
- No whistleblowing domain of interest (n= 1)
- No English Language (n=1)
Included
Paper included for the study N = 84

Figure 4. 3: Search results and publication selection process

Table 4. 1: Data Collection for Research Literature Review develop performance measurement framework – Step 1 to Step 4

No	**Criteria**	**No of Publication on Scopus**			
		Step 1	**Step 2**	**Step 3**	**Step 4**
1	Journal Articles	211	200	80	70
	Book or Book Chapters	22	22	10	8
	Conference Papers	16	1	16	6
	Total Number of Publication	249	237	97	84

4.5.1.2. Literature Review for stakeholder identification in the whistleblowing domain (Scope of data collection , collecting and documenting Articles)

The methodology applied to conduct a research literature review mainly used to identify the main stakeholder in the whistleblowing domain includes three tasks as shown in Figure 4.4 and described as follows: i) Data Collection to determine data sources, select keywords to search for relevant publications, and define criteria to identify publications to be analyzed; ii) Qualitative Analysis to identify the main stakeholders in whistleblowing domain from the identified research literature, analyzed based on USAID (2018) (and Four major attributes are important for Stakeholder Analysis by world bank (WB, 2020) : 1) end users and suppliers; 2) power to make to succeed/fail; 3) influence over other stakeholders, and 4) affected positively and negatively - the level of interest they have in the specific reform, and iii) Summary of the findings from the qualitative analysis.

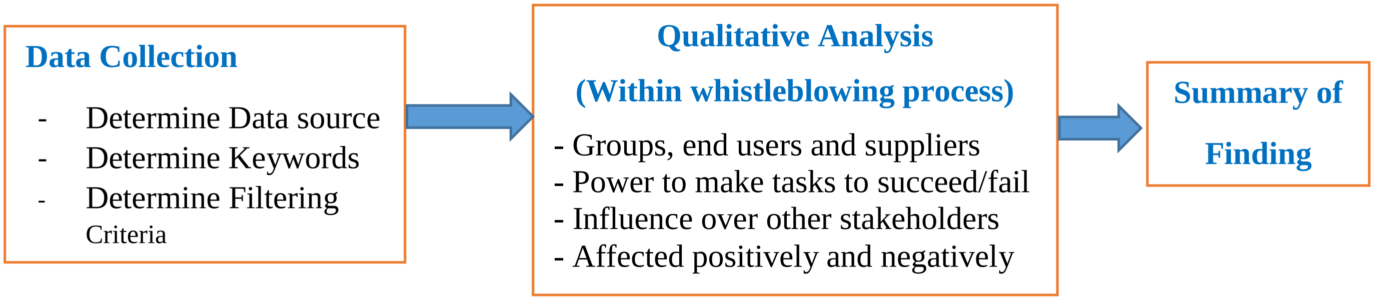

Data Collection
- Determine Data source
- Determine Keywords
- Determine Filtering Criteria
Qualitative Analysis
(Within whistleblowing process)
- Groups, end users and suppliers
- Power to make tasks to succeed/fail
- Influence over other stakeholders
- Affected positively and negatively
Summary of Finding

Figure 4. 4: Methodology for Research Literature Review to identify the whistleblowing stakeholders

As in the previous case, the data collection focused on the systematic search of the research literature in the Scopus database, ACM Digital Library and Wiley InterScience. The systematic search conducted using the keywords where they were mainly used to identify the main stakeholder in the whistleblowing domain including “Whistleblowing”, “Whistleblower” and “Stakeholder”. The search to identify the main stakeholder groups as relevant to the whistleblowing domain uses the following expression

(Whistleblowing OR Whistleblower) AND (Stakeholder OR Stakeholders)

The above expression was applied to search on Scopus Database, ACM digital library, and Wiley InterScience on December 25, 2019 against article titles, abstracts and keywords, and produced 43, 40 and 27 publications respectively. To conduct a detailed data analysis of these papers, a three-step filtering process is used to narrow down the number of articles. The first step involves identifying the most relevant publications – all journal articles, all book or book chapters, and all-conference papers. However, out of a total of 110 papers, 5 conferences, 6 books, and 12 journal papers were not available. In addition, 26 papers existed in either two of digital databases. It remains 61 Papers in total for analysis. The second step involves the exclusion of publications with no abstracts. From all 61 papers, the researcher found in step1, 6 Papers excluded - 5 journal articles and 1 conference papers - from the study with no abstract and it remains 55 Papers in total for analysis. Based on the second step in the process, the third step involved determining manually the relevance of each of the 55 publications. The determination was done through the publications’ titles and abstracts and full text review. Finally, the researcher found that only 35 papers were relevant and selected for detail analysis while 11 papers were not non-relevant. Search results and publication selection process to identify the whistleblowing stakeholders depicted in figure 4.5 and the result of each step of data collection is shown in Table 4.2.

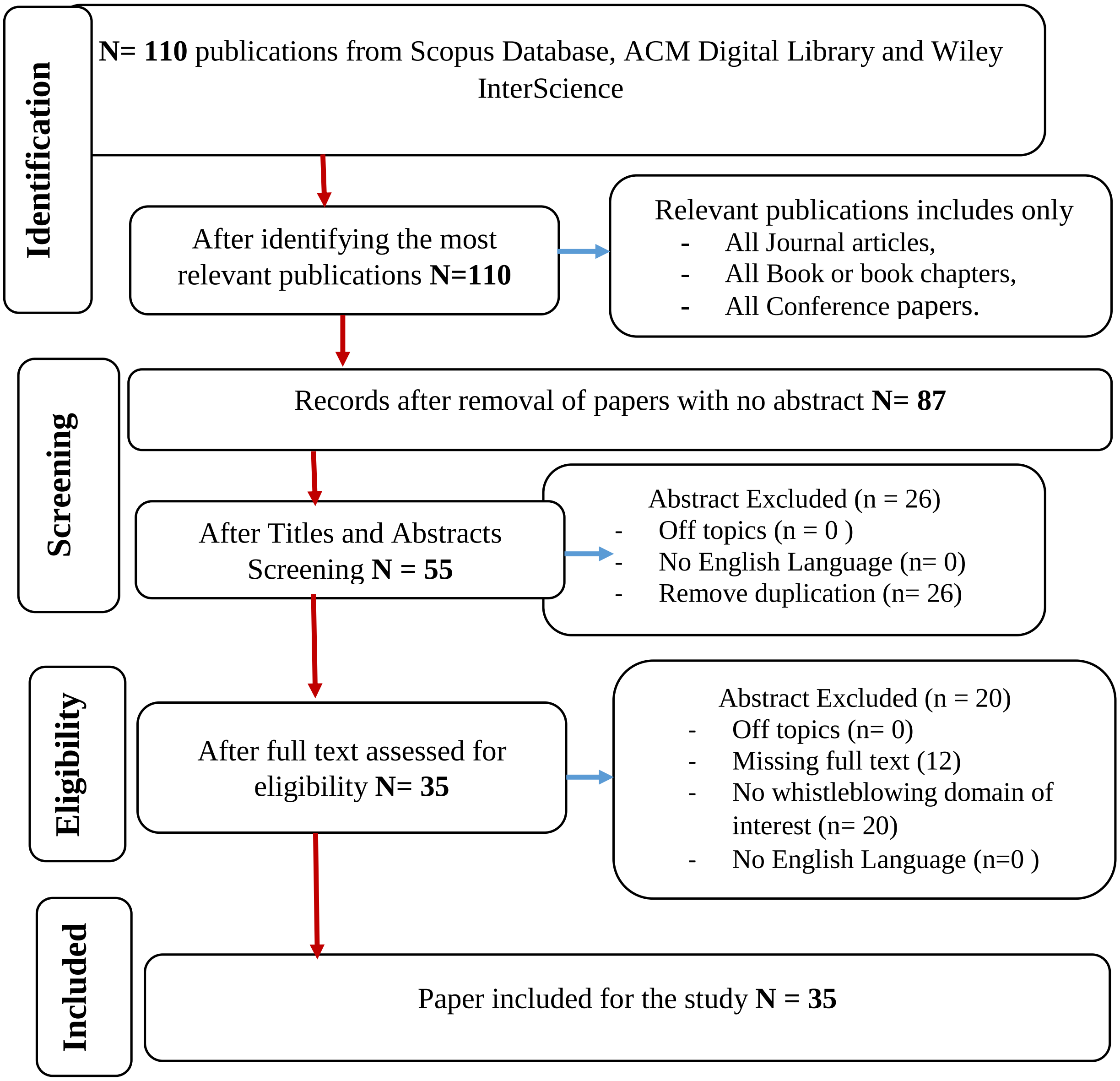

Identification
N= 110 publications from Scopus Database, ACM Digital Library and Wiley InterScience
After identifying the most relevant publications N=110
Relevant publications includes only
- All Journal articles,
- All Book or book chapters,
- All Conference papers.
Screening
Records after removal of papers with no abstract N= 87
After Titles and Abstracts Screening N = 55
Abstract Excluded (n = 26)
- Off topics (n = 0)
- No English Language (n= 0)
- Remove duplication (n= 26)
Eligibility
After full text assessed for eligibility N= 35
Abstract Excluded (n = 20)
- Off topics (n= 0)
- Missing full text (12)
- No whistleblowing domain of interest (n= 20)
- No English Language (n=0)
Included
Paper included for the study N = 35

Figure 4. 5: Search results and publication selection process to identify the whistleblowing stakeholders

Table 4. 2: Data Collection for Research Literature Review to identify the whistleblowing stakeholders – Step 1 to Step 3

No	**Criteria**	**No of Publication in all three Databases**		
		Step 1	**Step 2**	**Step 3**
1	Journal Articles	33	28	22
	Book or Book Chapters	12	12	5
	Conference Papers	16	1	8
	Total Number of Publication	61	55	35

4.5.1.3. Literature Review for related work in whistleblowing and Digital Government (Scope of data collection , collecting and documenting Articles)

The research methodology for analyzing the related work on the integration of the two domains - whistleblowing and Digital Government, involves three tasks that are shown in Figure 4.6 and described as follows: i) Data collection for determining data sources, selecting keywords to search for relevant publications, and defining criteria for identifying publications to be analyzed; ii) Qualitative Analysis to document the main findings from the identified research literature, analyzed according to Digital Government (DG) contribution in whistleblowing domain. Particularly in information security and surveillance, promoting whistleblowing services and Data Integration and iii) Summary of the findings from the qualitative analysis.

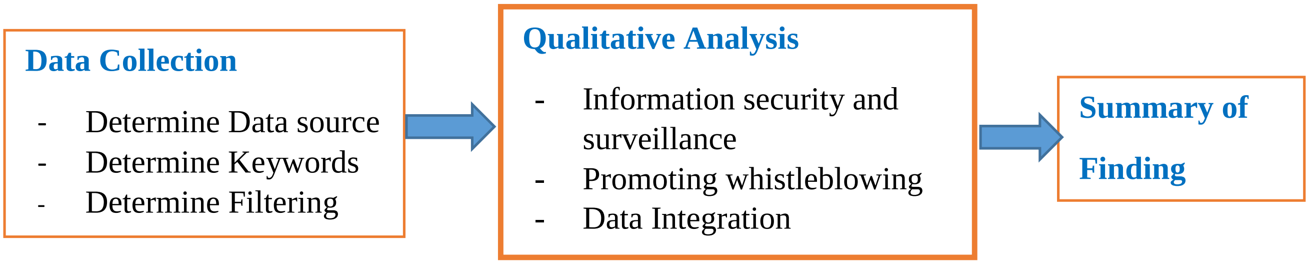


Figure 4. 6: Methodology for Research Literature Review to analyze the related works

On the other hand, the search used the following expression to identify related works that combine the whistleblowing domain and Digital Government domain. To this end, the researchers explored the content of the Scopus Database, ACM digital library and Wiley InterScience databases using the following keywords: *"Digital Government & Whistleblower", "Digital Government & Whistleblowing", "E-government & Whistleblowing", "E-government & Whistleblower", "Digital Technologies & Whistleblower", "Digital Technologies & Whistleblowing", "Technology & Whistleblowing", "Technology & Whistleblower", "ICT & whistleblower", "ICT & whistleblowing*".

The search result on the Scopus Database, ACM digital library and Wiley InterScience on December 25, 2019 against article titles, abstracts and keywords produced 52, 56 and 38 publications respectively. To conduct a detailed data analysis of these papers, the researcher used a three-step filtering process to narrow down the number of articles. The first step includes identifying the most relevant publications – all journal articles, all book or book chapters, and all-conference papers. As a result 4 papers are excluded. However, out of a total of 142 papers, 6 conferences and 3 books and 9 journal papers were not available. The second step involves the exclusion of duplications. Duplication exists either other searches using different keys or searches from other databases. As a result, 21 publications were excluded and 103 papers remain for further processing. The third step involved determining manually the relevance of each the 103 publications. The determination was done through the publications' titles and abstracts. 21 papers were excluded since they mentioned the whistleblowing area but did not show any separate contribution to it. Some other papers (15) were also excluded because of their lack of basic contribution compared to the other papers. Finally, 67 papers selected for detail analysis. The search results and publication selection process to analyze the related works is depicted in figure 4.7 and the result of each step of data collection is shown in Table 4.3.

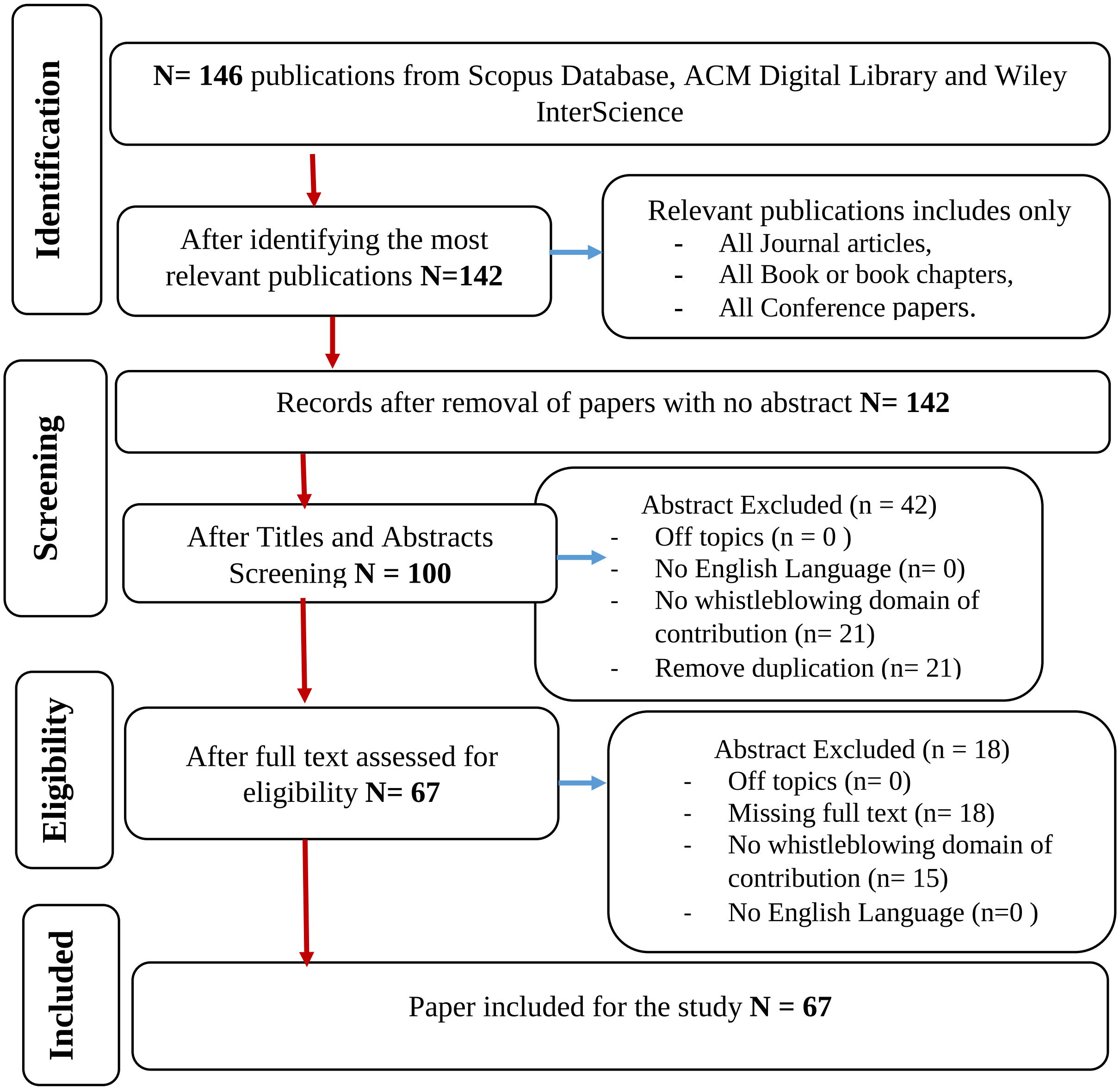

Identification
N= 146 publications from Scopus Database, ACM Digital Library and Wiley InterScience
After identifying the most relevant publications N=142
Relevant publications includes only
- All Journal articles,
- All Book or book chapters,
- All Conference papers.
Screening
Records after removal of papers with no abstract N= 142
After Titles and Abstracts Screening N = 100
Abstract Excluded (n = 42)
- Off topics (n = 0)
- No English Language (n= 0)
- No whistleblowing domain of contribution (n= 21)
- Remove duplication (n= 21)
Eligibility
After full text assessed for eligibility N= 67
Abstract Excluded (n = 18)
- Off topics (n= 0)
- Missing full text (n= 18)
- No whistleblowing domain of contribution (n= 15)
- No English Language (n=0)
Included
Paper included for the study N = 67

Figure 4. 7: Search results and publication selection process to analyze the related works

In general, only 67 papers were analyzed for the study and this papers are categorized into three basic problem areas – 1) Digital technologies promoting information security and surveillance – 29 publication; 2) Digital technology strategy for promoting whistleblowing – 22 publication and 3) Data Integration – 16 publication. The summary of the publication is shown in Table 4.3.

Table 4. 3: Data Collection for Research Literature Review to analyze the related works – Step 1 to Step 3

No	**Criteria**	**No of Publication in all three Databases**		
		Step 1	**Step 2**	**Step 3**
1	Journal Articles	73	65	42
	Book or Book Chapters	16	11	7
	Conference Papers	35	27	18
Total Number of Publication		124	103	67

Even though the existing research outlined in Table 4.4 presents few Digital Government applications in the whistleblowing domain, an all-rounded approach to the assessment of Digital Government initiatives in the area of whistleblowing domain is yet to emerge. This research paper tries to support research in this area by developing DGOV4WB coneptual framework and by conducting a Digital Government stakeholder analysis for whistleblowing. The finding will be interpreted through the Janowski (2015) Digital Government evolution model. The stakeholder analysis is outlined and the findings are discussed and interpreted later in this research.

Table 4. 4: Selected Papers for Research Literature Review - Digital Government applications in the whistleblowing domain

Authors	Title	Year	Source title	Category
Garrido M.V.	Contesting a biopolitics of information and communications: The importance of truth and sousveillance after snowden	2015	Surveillance and Society	Digital Technologies promoting information security and surveillance
Terzis G.	The end of hypocrisy: Online activism and ethno-political conflicts	2016	Pacific Journalism Review	
Busch A.	Privacy, technology, and regulation: Why one size is unlikely to fit all	2015	Social Dimensions of Privacy: Interdisciplinary Perspectives	
Jakubowicz K.	Early days: The UN, ICTs and freedom of expression	2015	The United Nations and Freedom of Expression and Information: Critical Perspectives	
Mansfield-Devine S.	Monitoring communications: The false positive problem	2013	Computer Fraud and Security	
Reich Z., Barnoy A.	The Anatomy of Leaking in the Age of Megaleaks: New triggers, old news practices	2016	Digital Journalism	
Waters S.	The Effects of Mass Surveillance on Journalists' Relations With Confidential Sources: A constant comparative study	2018	Digital Journalism	
Tryfonas T., Carter M., Crick T., Andriotis P.	Mass surveillance in cyberspace and the lost art of keeping a secret: Policy lessons for government after the snowden leaks	2016	Lecture Notes in Computer Science	
Balbir S. Barn, Ravinder Barn	Towards a unified conceptual model for surveillance theories: "we shall meet in the place where there is no darkness" - 1984, george orwell	2018	Proceedings of the 40th International Conference on Software Engineering: Software Engineering in SocietyMay	
Maheswaran, J., Jackowitz, D., Zhai, E., Wolinsky, D. I., & Ford, B.	Building Privacy-Preserving Cryptographic Credentials from Federated Online Identities	2016	Proceedings of the Sixth ACM Conference on Data and Application Security and Privacy	
Russell, A., Tang, Q., Yung, M., & Zhou, H.-S.	Generic Semantic Security against a Kleptographic Adversary.	2017	Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security	

Oliva, M. A., Palma, A. M. L., Murata, K., & Adams, A. A.	Information surveillance by governments: impacts of Snowden's revelations in Spain	2016	ACM SIGCAS Computers and Society,	
Kim, H., & Scott, C. R.	Going Anonymous. Proceedings of the 9th International Conference on Social Media and Society - SMSociety	2018	*Proceedings of the 9th International Conference on Social Media and Society*	
Das, S., Lo, J., Dabbish, L., & Hong, J. I.	Breaking! A Typology of Security and Privacy News and How It’s Shared.	2018	*Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems*	
Hohenberger S., Myers S., Pass R., Shelat A.	An overview of ANONIZE: A large-scale anonymous survey system	2015	IEEE Security and Privacy	
Bolsin S.N., Faunce T., Oakley J.	Practical virtue ethics: Healthcare whistleblowing and portable digital technology	2005	Journal of Medical Ethics	Digital technology strategy for promoting whistleblowing
Benchekroun T.H., Pierlot S.	Whistleblowers: An essential resource for the sustainable prevention of risks in sociotechnical systems	2012	Work	
Bernstein M., Jasper J.M.	Interests and credibility: Whistleblowers in technological conflicts	1996	Social Science Information	
Lee, J. S., Cuellar, M. J., Keil, M., & Johnson, R. D.	The role of a bad news reporter in information technology project escalation.	2014	ACM SIGMIS Database	
.Bodle, R.	The ethics of online anonymity or Zuckerberg vs. “Moot.”	2013	*ACM SIGCAS Computers and Society*	
Simon Rogerson	*Is professional practice at risk following the Volkswagen and Tesla revelations?: software engineering under scrutiny*	2017	*ACM SIGCAS Computers and Society*	
Bell G.B.	Digital whistleblowing in restricted environments	2011	Journal of Digital Information	
Mutungi, F., Baguma, R., Janowski, T.,	Towards Digital Anti-Corruption Typology for Public Service Delivery	2019	20th Annual International Conference on Digital Government Research	
Darusalam, Janssen, M., & Ubacht, J.	Towards generalized process patterns for detecting corruption within the government using open data.	2018	Proceedings of the 19th Annual International Conference on Digital Government Research Governance in the Data Age	
Heemsbergen L.	Whistleblowing and digital technologies: An interview with suelette dreyfus	2013	Platform	
Calvo P., Osal C.	Whistleblowing & big data: Monitoring and compliance of ethics and social responsibility	2018	Profesional de la Informacion	Data Integration

Tyagi, N., Gilad, Y., Leung, D., Zaharia, M., & Zeldovich, N.	*Stadium: A Distributed Metadata-Private Messaging System*	2017	*Proceedings of the 26th Symposium on Operating Systems Principles*	

4.5.2. Policy Literature Review

According to the research methodology described in the above Figure 4.1, the second process is policy literature review in the whistleblowing domain proposed by relevant research and international organizations. The methodology to conduct the policy literature review comprised three tasks that are shown in Figure 4.8 and described as follows: i) Data Collection to determine sources of policy literature including established research centers and international organizations that produce relevant research and policy recommendations, and identify policy documents; ii) Qualitative Analysis to analyze the policy documents based on whistleblowing dimensions identified by Transparency international (TI-NL, 2017) the same as for the research literature review: 1) Whistleblowing Procedure; 2) Organizational Culture; and 3)Whistleblower Protection, and iii) Summary of the findings from the qualitative analysis.

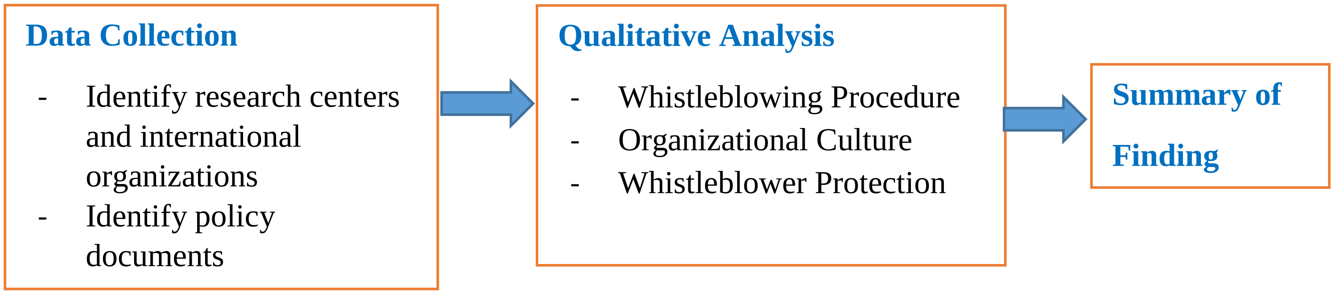

Data Collection
- Identify research centers and international organizations
- Identify policy documents
Qualitative Analysis
- Whistleblowing Procedure
- Organizational Culture
- Whistleblower Protection
Summary of Finding

Figure 4. 8: Methodology for Policy Literature Review

The data collection process has happened in two steps. First, identifying the most important sources of whistleblowing literature including research and international organizations. Second, identifying relevant policy literature produced by such organizations in the area of whistleblowing.

The first step involved conducting a Google search for the relevant organizations using a combination of "research center", "research unit", "whistleblower" and "whistleblowing" keywords. *("research center" OR "research unit") AND ("whistleblower" OR "whistleblowing").* A total of 34 organizations are identified as shown in Table 4.5. The second step involved exploring directly the websites of the organizations identified in the first step including the Organisation for Economic Co-operation and

Development (OECD), United Nation (UN), African Union (AU), Whistleblowing International Network (WIN), National Whistleblowers Center (NWC), Transparency International (TI), Government Accountability Project (GAP), Associated Whistleblowing Press (AWP), Inter-American Convention against Corruption (IACAC), European Commission (EC) and others to gather information about whistleblowing policies. After all these steps the researcher analyzed 14 documents.

Table 4. 5: List of identified websites working on whistleblowing domain

No	Name	Type	Websites
1	Transparency International (TI)	Non-Profit	https://www.transparency.org/
2	Organisation for Economic Co-operation and Development (OECD)	InterGov	https://www.oecd.org/
3	Public Concern at Work (PCAW)	Non-Profit	https://www.pcaw.org.uk/
4	Project on Government Oversight	Non-Profit	https://www.pogo.org/
5	The World Bank	InterGov	https:// www.worldbank.org
6	Centre for Free Expression Whistleblowing Initiative	Non-Profit	https://cfe.ryerson.ca/
7	National Whistleblower Center	Non-Profit	https://www.whistleblowers.org/
8	IRS Whistleblower Office	Government	
9	Whistleblower International Network (WIN)	Non-Profit	https://whistleblowingnetwork.org/
10	Government Accountability Project	Non-Profit	https://www.whistleblower.org/
11	Inter-American Convention against Corruption (IACAC)	InterGov	www.oas.org/en/
12	African Union	InterGov	https://au.int/
13	National Oversight and Whistleblowers (NOW)	Non-Profit	http://nowmalaysia.org/
14	Stefan Batory Foundation	Private	www.batory.org.pl/en

15	Public Employees for Environmental Responsibility	Non-Profit	https://www.peer.org/
16	Whistleblowing Research Unit	Academic	https://www.mdx.ac.uk/our-research/research-groups/whistleblowing-research-unit
17	Associated Whistleblowing Press	Non-Profit	https://awp.is/
18	WhistleblowersUK	Non-Profit	https://www.wbuk.org/
19	Society of Professional Journalist	Non-Profit	https://www.spj.org/whistleblower/whistleblowing-organizations.asp
20	Project On Government Oversight (POGO)	Non-Profit	*https://www.pogo.org*
21	Whistleblower Aid	Non-Profit	*https://www.whistlebloweraid.org*
22	Reporters Committee for Freedom of the Press	Non-Profit	*https://www.rcfp.org*
23	ExposeFacts	Non-Profit	*https://www.whisper.exposefacts.org*
24	United Nation	InterGov	https://www.un.org/en/
25	Freedom of the Press Foundation	Non-Profit	*https://www.freedom.press*
26	Whistleblowers of America	Non-Profit	*https://whistleblowersofamerica.org/*
27	Whistleblower Protection Program	Government	*https://www.whistleblowers.gov/*
28	Digital Whistleblowing Fund	Academic	*https://www.whistleblowingfund.org/*
29	Open Society Foundations	Private	https://www.opensocietyfoundations.org
30	Open Democracy Advice Centre	Non-Profit	*https://www.opendemocracy.org.za*
31	Open Government Partnership	InterGov	*https://www.opengovpartnership.org*
32	UNCAC Coalition	InterGov	*https://uncaccoalition.org*
33	International Whistlblower	Private	*https://www.internationalwhistleblower.com/*
34	Whistleblower Protection Blog	Government	https://www.whistleblowersblog.org/

As per the above Table (Table 4.5) among 34 organizations, 19 (56 %) are non-profit partisan organization, 7 (20 %) are Intergovernmental organizations, only 3 (9 %) are

Government organization, 3 (9 %) are Private Organizations and 2 (6 %) are Academic Institutions.

4.5.3. Whistleblowing Legislation Review

Considering the methodology section described in Figure 4.1, the third step in the methodology is whistleblowing legislative review in the whistleblowing domain proposed by countries around the world. The data collection process is executed by identifying the most important sources of whistleblowing legislation based on country level available on the internet and then analysis of policy and legislative documents concerning whistleblowing in the selected countries as shown in Table 4.6 and after all these steps the researcher analyzed 12 legislation documents.

Table 4. 6: Whistleblowing legislation act of countries

No	Whistleblowing Laws	Country	Legislation Dates
1	Public Interest Disclosure Act	United kingdom	1998
2	Sapin II Act	France	2017
3	Whistleblower Protection Act of 1989 and Sarbanes-Oxley Act of	USA	1989 and 2002
4	Protected Disclosures Act (no 26 of 2000)	South Africa	2000
5	Public Interest Disclosure Act 2013.	Australia	2013
6	Whistle Blowers Protection Act, 2011.	India	2011 & 14
7	Public Servants Disclosure Protection Act (The Act), PSIC	Canada	2007
8	Protected Disclosures Act (PDA) 2014	Ireland	2014
9	The whistleblowers protection act, 2010	Uganda	2010
10	Whistleblower Act (Act 720) 2006	Ghana	2006
11	(Disclosure of Offenses and Harm to Integrity or to Proper Administration) Law (Amendment No. 2), 5768-2008	Israel	2008
12	Whistleblower Protection Law (Law No. 122 of June 18, 2004).	Japan	2014

4.5.4. Case Study Development

In this research the case study qualitative methodological approach was designed to be a preliminary investigation into various aspects of Digital Government use in whistleblowing. The methodology to conduct case study development comprised four tasks that are shown in Figure 4.9 and described as follows: i) defining the assessment framework; ii) Data Collection to create a repository of digitally enabled whistleblowing initiatives, selecting the initiatives to be documented as case studies, and developing these case studies; iii) Qualitative Analysis to obtain in-depth understanding of various case studies including the types of initiatives, objectives/aims, and major achievements, and the features analyzed along 3 whistleblowing dimensions identified by Transparency international (TI-NL, 2017) the same as for the research and policy literature review: 1) Whistleblowing Procedure; 2) Organizational Culture; and 3)Whistleblower Protection, and iv) Summary of the findings from the qualitative analysis.

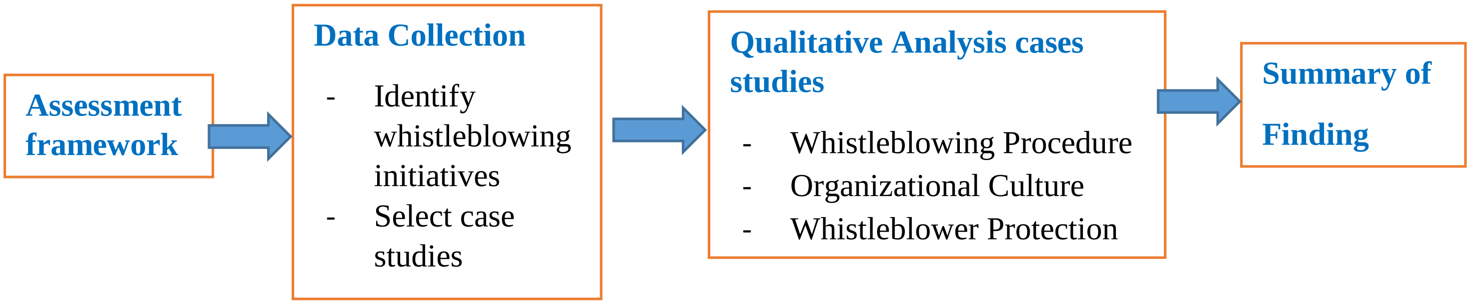

Assessment framework
Data Collection
- Identify whistleblowing initiatives
- Select case studies
Qualitative Analysis cases studies
- Whistleblowing Procedure
- Organizational Culture
- Whistleblower Protection
Summary of Finding

Figure 4. 9: Methodology for Case Study Development

4.5.5. Case Study Assessment framework

As the first phase of the research, exploratory or formative research using the technique of formal qualitative research through multiple case studies using secondary data – Digital Government initiatives on whistleblowing and whistleblower protections - is used. The researchers conducted exploratory case study research to understand how the Digital Government (solution domain) contributes to solving the issues/problem of whistleblowing and whistleblower protection (problem domain) based on DGOV4WB Conceptual Framework stated in Figure 3.2. The assessment framework of case studies provides a structured conceptual map of outcomes for each digitally enabled whistleblowing initiatives of study along with details of how achievement of the outcomes can be measured. The case study assessment framework used for this research is depicted in Figure 4.10.

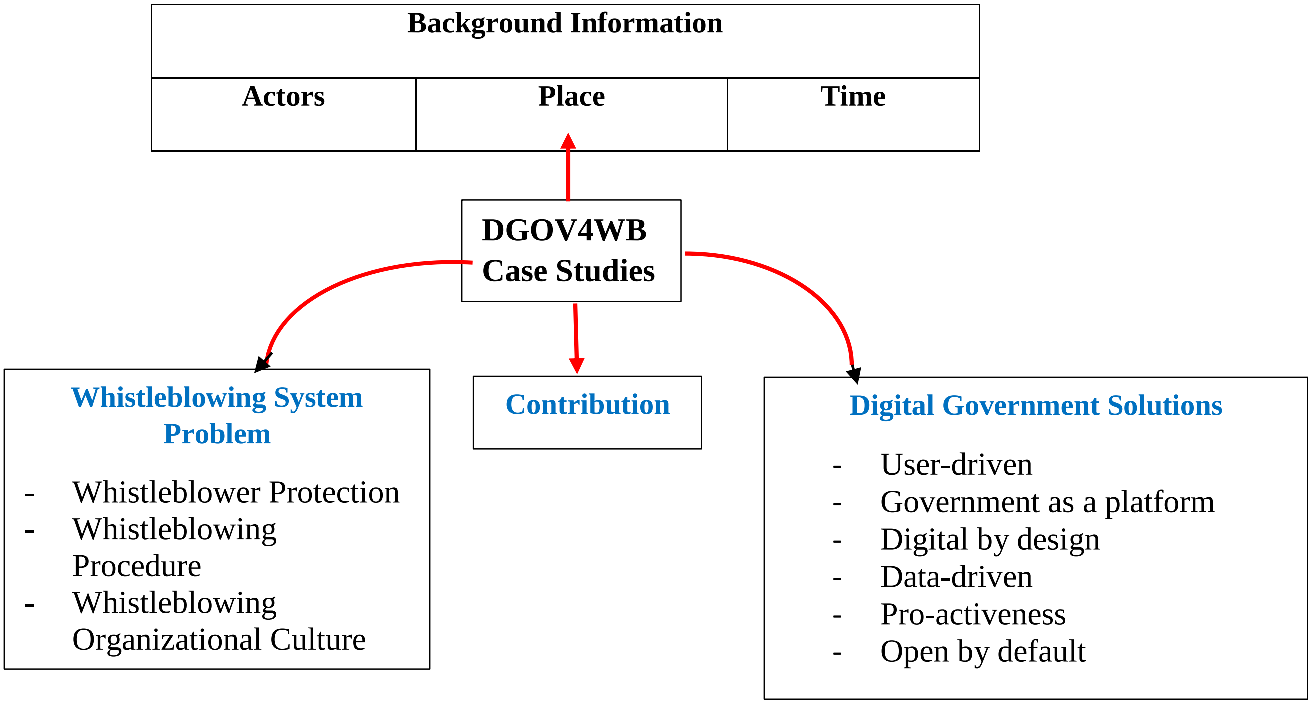

Background Information
Actors
Place
Time
DGOV4WB Case Studies
Whistleblowing System Problem
- Whistleblower Protection
- Whistleblowing Procedure
- Whistleblowing Organizational Culture
Contribution
Digital Government Solutions
- User-driven
- Government as a platform
- Digital by design
- Data-driven
- Pro-activeness
- Open by default

Figure 4. 10: DGOV4WB Assessment framework

The case study was designed to be a preliminary investigation into various aspects of Digital Government use in whistleblowing. The assessment framework applies for this research paper is adopted from (Estevez, Janowski & Dzhusupova, 2014). To characterize each of the case studies (DGOV4WB initiatives), the assessment framework comprises four constructs - Background, Problem/Objective, Solution and Contribution. Background is used to gather basic information about the initiative including the actors, launching place and time. Objective captures the ultimate goal of the initiative to address the problem of Whistleblowing. The third construct (solution) defines the Digital Government solution applied to solve whistleblowing problems, the outcome of the initiative such as policy, government tool, public service or capacity-building, and stages of Digital Government such as Digitization, Transformation, Engagement, and Contextualization (Janowski, 2015). The contribution construct defines how the DGOV solution addresses the WB problem.

The data collection was done through internet searches using search engines. As the concern was about Digital Government initiatives with the objective of whistleblowing and whistleblower protection, the researchers used the search keys such as 'whistleblower protection', 'governance', 'digital technology', 'Digital Government', 'whistleblowing' and 'e-government'. The case studies were selected based on the availability of enough resources on the web for the analysis, based on their region and their relevance to the paper.

4.6. Quantitative Data collection for the research

To conduct a survey for this research qualitative approaches has been used to develop a comprehensive questionnaires. considering one of the aim of this research - analyze the impact of Digital Government for whistleblowing initiatives in Ethiopian context through Technology Acceptance Model (TAM) and based on the above research framework (stated in section 3.2 and General Research Methodology in Figure 4.1), a series of personal interviews were carried with three Ethiopian Digital Government officials from the Ministry of Innovation and Technology, two anti-corruption officials from Federal Ethics and Anti-Corruption Commission of Ethiopia and one professor from University of Gondar to determine the validity of the proposed research TAM model.

Based on analysis of relevant literature and the feedback obtained from our interviews, the first version of a survey questionnaire were developed. Next, with comprehensive pretesting by ten scholars and government officials with considerable experience in operations of Digital Government whistleblowing programs, the researcher refined the questionnaire. Pre-test results indicate that the elements for the questionnaire were comprehensive. Table 4.7 shows the definitions of different variables as well as the questionnaire items used in the research model and their sources. A five point Likert scale with anchors of strongly disagree to strongly agree was used to measure each item of the other constructs in this study. The full list of questionnaire are stated in appendix II.

A. Sample Selection

For the survey, the unit analysis is individual. The samples are citizens who have experience in using Digital Government whistleblowing systems to report misconducts in their work place. Respondents were employed people in governmental organizations and institutions who, because of their career, were identified as having greater than average access to the internet or other digital technologies to access whistleblowing systems in Ethiopia. This ensures that the respondent sample represents the population of interest in Ethiopia's uses of Digital Government whistleblowing systems.

B. Data Collection

According to Creswell (2014) and Ivankova and Clark (2016), study samples should be sufficient and representative. The findings are more likely to be accurate both externally and internally, by using sufficient and representative samples. In quantitative analysis, the problem of external validity is not limited to population generalizability but also involves generalizability in circumstances (Creswell, 2014; Ivankova & Clark, 2016).

As described in the above (sample section bulletin), Data of users were collected from employees of government organizations and public academic institutions. Following formal request to Amhara National Regional State Ethics and Anti-Corruption Commission and Amhara National Regional State Police Commission whistleblowing officers, researcher could obtain whistleblowing data. Considering the number of population, hence researcher conducted personally administered survey in the data collection. In addition staffs of University of Gondar also included in the study. For those who were willing to participate in the survey, then research assistants brought the questionnaire to them and ask them to complete the questionnaire by themselves (face-to-face). As suggested by Ivankova and Clark (2016), this survey method offers a very high response rate compare to other methods. As a result, 800 copies of questionnaires were distributed, of which 610 were retrieved. A review then was undertaken to seek out errors in the form of invalid data and 56 were excluded due to being incomplete or being unreadable response. Finally 554 responses were usable in this research. Therefore the response rate is 76.25 % and the effective response rate in this study is 69.25%.

Table 4. 7: Definitions of the individual characteristics (constructs)

Construct	Definition
Attitude Toward Behavior (ATT)	Attitude is the user's willingness to use the system or to mediate an affective reaction between ease of use and usefulness and motive to use the target system (Karjaluoto, Mattila & Pento, 2002; Suki & Ramayah, 2010).
Perceived Usefulness (PU)	Perceived usefulness is the extent to which a person believes that using a particular application system can improve the quality of his or her job and enhance productivity within the scope of the organization (Davis, 1989).
Perceived Ease of Use (PEU)	Perceived Ease of Use is the extent to which a person believes that the use of a specific system would be effortless and could be done with a minimum of effort (Ajzen & Fishbein, 1972; Davis, 1989).
Whistleblowing System Quality (WSQ)	Whistleblowing System Quality is an individual's belief about the whistleblowing system quality when she/he wants to report misconduct and look for the update on whistleblowing information on the whistleblowing platform (Libit, Freier & Draney, 2014; Nieweler, 2014).
Information Quality (IQ)	The information quality of the whistleblowing systems will enable whistleblowers to study the information and look the news through online webpages, TV and radios (Shahid, 2017).
Subjective Norm (Sn)	Subjective norms refer to the idea that an influential person or group of people supports and encourages a particular behavior. Or it is "person's perception that most people who are important to him think he should or should not perform the behavior in question" (Venkatesh, 2000).
Behavioral Intention (BI)	Behavioral intention is a person's perceived likelihood or "subjective probability that he or she will engage in a given behavior" (Davis, 1989).

C. Data Analysis

Considering the one of the main aim of this research - investigate factors that affect the citizens' acceptance of digitally enabled whistleblowing systems in Ethiopian public organization and institutions - The analysis was conducted using the Partial Least Square – Structural Equation Modeling (PLS- SEM). A major point of contention has been the claim that PLS-PM can always be used with very small sample sizes (Kock & Hadaya, 2018; Hair et al. 2017). Additionally, Hair et al. (2017) indicates that Partial least squares structural equation modeling (PLS-SEM) has become a popular method for estimating (complex) path models with latent variables and their relationships (Hair et al. 2012). This is therefore, based on the consideration of small sample size in this research and the research design applied in this current study which is exploratory research, Partial Least Square is selected for the analysis.

4.7. Summary

The methodology and research design employed in this research are outlined in this chapter. The primary objective of this chapter was the development of a rigorous research methodology. The research used a mixed approach combining both quantitative and qualitative research methods. An in-depth description of the research method used for this research and a rationale for choosing the qualitative and quantitative mode of research was given. The chapter also described the different sources of data that have been used in the study. The choice of the research strategy was based on the nature of data. An extensive rigorous literature review was used in the first phase of the study while in the second phase, case study and survey used.

CHAPTER V

DATA ANALYSIS

5.0. Introduction

In this chapter, analysis of the data collected from 4 digitally whistleblowing initiatives (qualitatively) is undertaken to understand the impact of the Digital Government in whistleblowing domain. The Analysis was done through a case study assessment framework stated in section 4.4.5 and cross-case analysis is applied to the cases to Figure out the possible contribution of Digital Government on whistleblowing. Additionally, this chapter also analyzes data collected from 554 respondents (quantitatively) in order to test the reliability and validity of the TAM model stated in section 3.3 as well as the hypotheses. The analysis was conducted using the Partial Least Square (PLS) approach to Structural Equation Modelling (SEM).

5.1. Qualitative Data Analysis

5.1.1. Cases Studies

This section will cite a real-world scenario, Digital Government whistleblowing initiatives, to give a case study of our approach. The data collection was done through internet searches using search engines. Since the research were concerned Digital Government initiatives with the objective of whistleblowing and whistleblower protection, the study used the search keys such as ‘whistleblower protection’, ‘governance’, ‘Digital Technology’, ‘Digital Government’, ‘whistleblowing’ and ‘e-government’. The case studies were selected based on the availability of enough resources on the web for the analysis, based on their region and their relevance to the paper.

As described in the previous chapter (chapter 4), the case study is designed to be a preliminary investigation into various aspects of Digital Government use in whistleblowing. To characterize each of the case studies (DGOV4WB initiatives), the assessment framework comprises four constructs - Background, Problem/Objective, Solution and Contribution. In addition, the study analyzed all-Digital Government whistleblowing initiatives - digitally-enabled whistleblowing program - based on the three whistleblowing dimensions. This analysis helps to identify which indicator within the performance measurement framework stated in the above section (section 6.4) is affected by digitalization or not. The full analysis of the case studies is described in a simplified Table below (Table 5.1). The Table describes the relationship between the cases and the three whistleblowing dimensions. All the four case studies of DGOV4WB initiatives and their evaluation based on the conceptual framework defined in section 3.1 is discussed below.

Case 1 - Platform to Protect Whistleblowers in Africa (PPLAAF) – Senegal

Background: -

PPLAAF initiative is a Senegalese NGO launched in Dakar 2017 by lawyers, anti-corruption activists and investigative journalists with the mission to help whistleblowers and leaks through legal strategy, financing, research, legislation, and technology (PPLAAF, 2019; Safdar, 2017; OpenDemocracy, 2017)).

Problem / Objective: -

The initiative aims to reduce whistleblowing risks and costs to the point that they are insignificant – primarily for the teacher, the accountant, the soldier, the attorney on the African continent where their disclosures speak to African citizens ' public interest (Dalby, 2020; Safdar, 2017; OpenDemocracy, 2017). The founder of the initiative, William Bourdon, states, "We have decided to protect whistleblowers here in Africa, the continent where they take the greatest of risks and are the least protected" (PPLAAF, 2019). The initiative seeks to protect whistleblowers, and to strategically litigate and advocate on their behalf where their disclosures speak to the public interest of African citizens. Generally speaking, PPLAAF was established to assist whistleblowers whose revelations are related to Africa (OpenDemocracy, 2017).

Solution: -

The initiative PPLAAF plays the intermediary role by providing a community of in-house and external experts to ensure the process of 'blowing the whistle' is removed from the immediate danger and threats. PPLAAF provides the all the necessary services for whistleblowers, NGOs, media and governments (Dalby, 2020; Safdar, 2017; OpenDemocracy, 2017). Among other things, PPLAAF provides Secure Communication, Legal assistance, Media assistant - Connection to credible investigative partners, and Advocacy and research (PPLAAF, 2019). Secure Communication includes: i) Telephonic support (Hotline) 24x7 service which offers the opportunity to an individual to open a dialog by contacting PPLAAF team either English or French language; ii) A secure GlobaLeaks platform – It provides Technological platform which guarantees confidentiality and anonymity all along the communication process through Tor Technology where connection goes through a number of encrypted channels which makes it difficult to trace the source of the information and the identification of the person is more protected. The Legal assistant offers Pro bono legal advice and/or defense. The platform provides guidance on how to approach journalists and which ones to contact for whistleblowing and it will look forward for any assistance.; 3) Media assistant - Connection to credible investigative partners; and 4) Advocacy and research (Dalby, 2020; Safdar, 2017; OpenDemocracy, 2017; PPLAAF, 2019).

The Initiative provides whistleblowing information through its website and based on the needs of the whistleblower, it provides a way of reporting wrongdoings through a secure website, encrypted messaging service, and hotlines. PPLAAF provides a secure web portal for sending information and documents, as well as secure hotlines at the disposal of whistleblowers in both French and English. PPLAAF’s website operates through the GlobaLeaks platform. It can be accessed through the TOR browser separating PPLAAF’s website and the GlobaLeaks platform. The initiative provides two types of technological elements to disclose sensitive information submitted through communication channels (Dalby, 2020; Safdar, 2017; OpenDemocracy, 2017) . These are: 1) PPLAAF’s hotline and 2) GlobaLeaks (submission of a report/ TIP through a webform) as well as the website. No sensitive information should be shared through the hotline (Voice) and web channels while Deep-web GlobaLeaks platform used only for sensitive information which is available through the TOR network allowing for individuals to safely connect and share any sensitive content. Case Management Tool is used to securely centralize, document and manage all cases. Since July 2017, PPLAAF delivered training on security and communication for more than one hundred stakeholders including activists, journalists, and bloggers with a West African network called Africtivistes to avoiding surveillance (Dalby, 2020; Safdar, 2017; PPLAAF, 2019).

Problem / Objective Analysis

The whistleblowing dimensions problem addressed includes Whistleblowing Procedure and Whistleblowing Protection. The whistleblowing procedure is a reporting channel which can be easily accessed at any time. The whistleblowing protection, on the other hand, provides secured reporting channel that makes anonymity and confidentiality.

Solution Analysis

The solution is related to Local and Regional Governance and Stakeholder participation. The Digital Government evolution model is engagement. The following Digital Government elements were applied: 1) Digital by design – Publishing information on the portal, providing secured communication using digital tools GlobaLeak and tor technology, and use of Case Management Tool; Providing interface through website channel and telephonic support (Hotline) accessible 24 hours a week and it provides different platforms accessible through different channels; 2) Data-Driven – provide training for 100 stakeholders and it uses data as a key strategic asset; 3) User-Driven - addresses citizen demand on who wants reporting wrongdoing and providing enhanced service; 4) Government – providing legal and media assistant to whistleblowers.

Case 2 - XNET (Xnet – Internet Freedoms) Barcelona, Spain

Background: -

Xnet, an activist project which has been working on and for networked democracy and digital rights since 2008, launches in the Barcelona City Hall. It is considered as the first public Anti-Corruption Complaint Box using anonymity protection technology like TOR and GlobaLeaks (P2P, 2017; Sainz, 2014; Xnet, 2019).

Problem /Objective: -

The ultimate goal is to create access to the citizens of the Barcelona city to send information safely, confidentially and anonymous, and to enable civil societies to be an active participant in fighting against corruption in supporting freedom of expression (Xnet, 2019).

Solution: -

Xnet is a non-profit activist platform operates in various fields related to digital rights, networked democracy and freedom of expression (P2P, 2017; Sainz, 2014; Xnet, 2019). Xnet provides a Whistleblowing Platform against corruption for the City Hall of Barcelona – powered by GlobaLeaks and TOR friendly. Xnext launches this Anti-Corruption Complaint Box (XnetLeaks mailbox). The Box uses GlobaLeaks platform and the reporter can access through the Tor network which enables people to maintain anonymization of communications (Xnet, 2019). There is no possibility to learn the identity of the person sending information even the City Hall itself (P2P, 2017). The Anti-Corruption Complaint Box is a means of which citizens can fight corruption and other practices that are damaging for good governance in the city of Barcelona. Utilizing the Box, citizens can send their complaints, suspicions, and evidence of cases that they believe the City Hall should investigate in a way that secures and permits total anonymity. The City Hall responds to every single compline and inquiries into those that are deemed plausible, or send them on to the appropriate institution. The initiative has a capability for the whistleblower reserves the right whether or not to reveal his or her identity. Besides, the reporter can check the status and process of his complain (P2P, 2017). Xnet provides for journalists and citizens a FAQ service regarding the Box. One notable example is *the Blesa emails* (whistleblowing channel) which reveal Spain's biggest ever leak on banking corruption in 2012 (Sainz, 2014). It exposes thousands of corporate emails related to cases of corruption from the former president of Caja Madrid. It now considered one of the best whistleblowing systems in a fight against corruption that provides a safe and secure anonymous mailbox in addition to protecting whistleblowers from reprisals (P2P, 2017; Sainz, 2014; Xnet, 2019).

Problem / Objective Analysis

The whistleblowing System dimensions problem addressed includes Whistleblowing Procedure and Whistleblowing Protection. Whistleblowing Procedure is clear and understandable procedures to report wrongdoings and to communicate in response, and channels available for reporting the wrongdoing. The Whistleblowing Protection, on the other hand, provides anonymous and confidential communicating digital tool, Protection of whistleblower identity at all stages of the investigation process.

Solution Analysis

The solution is related to Local and Regional Governance and Stakeholder participation. The output is public service. The Digital Government evolution model is Contextualization. The following Digital Government elements were applied: 1) Digital by design – Publishing information on the portal, Anti-Corruption Complaint Box powered by GlobaLeak and tor technology; providing interface through website channel accessible 24 hours a week and *the Blesa emails*, and 2) User-Driven – provides active participation through civil society in combating corruption. 3) |Government – providing a platform for reporting suspicious corruption activities for the citizens.

Case 3 - Vale Whistleblowing Channel (VWC), Indonesia

Background: - Vale Whistleblower Channel (VWC) was launched on January 1, 2016, by PT Vale Indonesia Tbk Company. It is a whistleblowing service that is managed independently and professionally by a violation reporting service provider in Indonesia - PT Deloitte Konsultan Indonesia. The VWC is directly linked to the Vale S.A Code of Ethics and Conduct (vale, 2018; VWC, 2019).

Problem/ Objective: -

The mission of PT Vale Indonesia Tbk ("PT Vale") is to transform natural resources into prosperity and to commit to sustainable development (Vale, 2018). To be increasingly competitive in the business environment, Val implements good corporate governance ("GCG") by continuously improving its performance, transparency, accountability, and responsibility in the eyes of its stakeholders. VWC aims to provide reporting mechanisms for the customers and employees to any illegal activities in a company with at most secured systems and to train all employees on its whistleblowing system (VWC, 2019; MarketScreener, 2017).

Solution: - In achieving the Mission and the Vision, PT Vale conducts its operational activities, guided by a set of values that reflects high ethical and moral standards. This leads to raising credibility, and maintaining the positive image of the Company in markets, both in the short and long term. The company introduces a violation reporting mechanism, called Vale Whistleblower Channel (VWC), which is managed independently by third parties where its existence thinks the violations can be prevented or detected earlier (vale, 2018).

The VWC mechanism contains a reporting system that includes various types of violation, including Fraud, Corruption, Theft, Breach of policy, Conflict of interest, Financial Statement Fraud, Bribery and other types of Harassment, Discrimination, Environment, Health and safety in PT Vale included in the scope. Violation reports may be submitted in Bahasa Indonesia or English, through the channels provided. VWC is equipped with stringent follow-up procedures, therefore PT Vale expects that prospective offenders are reluctant to conduct fraud (Vale, 2018; VWC, 2019).

Vale Whistleblower Channel includes: 1) 24 hour a week accessible Toll free number, SMS, fax, website, email, and PO Box provided for whistleblower to report suspected incidents of misconduct; 2) Employee education and training on policies and procedures to prevent misconduct; 3) Comprehensive awareness-raising of PT Vale employees of the Whistleblower system; 4) Specialist call center operators with knowledge of PT Vale; 4) Expert forensic investigators to analyze reports 5) Timely reporting of incidences to PT Vale WB team. 6) Recommendations on corrective action (Vale, 2018; VWC, 2019).

Problem / Objective Analysis

The whistleblowing System dimensions problem addressed includes Whistleblowing Procedure, Whistleblowing organizational culture and Whistleblowing Protection. Whistleblowing Procedure is free channels reporting wrongdoing accessible 24x7. Whistleblowing organizational culture is regular training for employees responsible for receiving and investigating reports – Whistleblowing System Team and Regular training for employees on whistleblowing frameworks. Whistleblowing Protection, on the other hand, provides secured reporting channel.

Solution Analysis

The solution is related to Local and Regional Governance and Stakeholder participation. The output is public service and capacity building. The Digital Government evolution model is Engagement. The following Digital Government elements were applied: 1) Government - Providing services to enhance public services and providing informational services; 2) Digital by design – promoting digital technologies to support service delivery and providing digital tools to report wrongdoings; forensic investigators to analyze reports; Providing interface through website channel and email application to its customers and employees. 3) User-Driven – capacity building through training based on the need of the society.

Case 4 – WildLeaks, First Wildlife Crime Whistleblowing initiative, USA

Background: - WildLeaks is a nonprofit collaborative project created, funded and managed by the Elephant Action League (EAL) based in the United State of America. WildLeaks launched on February 7th, 2014 and it is considered as the first whistleblower initiative dedicated to Wildlife and Forest Crime in the world (WildLeaks, 2019; ELI, 2020; WB, 2018; DW, 2014).

Problem / Objective:-

According to the founder of the project "The mission of the project is to receive and evaluate anonymous information and tips regarding wildlife crime, including corruption, and to transform them into concrete actions" (WildLeaks, 2019). This includes "preventing wildlife crimes through by facilitate the identification, arrest, and prosecution of criminals, traffickers, businessmen, and corrupt governmental officials behind the poaching of endangered species and the trafficking of wildlife and forest products, including ivory, rhino horn, big cats, apes, pangolins, birds, illegal fishing and illegal timber all over the world". The initiative was developed to expose the key players in the international crime networks, not the low-level operatives on the ground around the world (WildLeaks, 2019; ELI, 2020; WB, 2018; DW, 2014).

Solution: - The initiative starts with a target group of any person in the world who witnessed any wildlife crimes. The project consists of the WildLeaks website which has 16 different language versions and smartphone applications. WildLeaks has implemented a very secure online platform built on the Tor technology in order to allow the sources to stay anonymous and to submit ‘sensitive’ information in the most secure way possible, always encrypted, with respect to data transmission and management (WB, 2018; DW, 2014). All leaked information through WildLeaks is reviewed, evaluated, and filtered before releasing any of the data to outside parties. It is an extremely very pro-active initiative with a solid investigative component and a diverse of intelligence gathering assets in target countries (WildLeaks, 2019). The online portal allows the whistleblower unique receipt number to connect once again in a secure and anonymous way which enables them to add more information about your original submission, to send us a message, and to interact in an anonymous way.

The initiative protects whistleblowers by providing both on a state-of-the-art secure anonymous system and by managing and using the information professionally. WildLeaks does NOT dump unfiltered data and information onto the web and does NOT pander for media headlines (WB, 2018; DW, 2014).

For any whistleblowers WildLeaks provides two possible options to send information and files in a very secure platform (WildLeaks, 2019; ELI, 2020; WB, 2018; DW, 2014): 1) Confidential – without the use of Tor Browser, it uses the usual web browsers (Firefox, explorer and google chrome) and the connection to WildLeaks will be automatically completed via HTTPS, which encrypts and secures data as it travels between whistleblower and secure servers where the transmission of the information is secured and encrypted but entities like employers or governmental agencies, may still be able to understand where you are and to see that you are uploading documents. or 2) Anonymous - If whistleblowers want total anonymity, Using Tor Browser submit information to WidlLeaks where the connection is not only secure but also anonymous, leaving no traces behind. Tor technology is considered the best technology for digital anonymity available to Internet users and academics. Tor guarantees that no personal traces remain in WildLeaks systems (WB, 2018; DW, 2014). To assess the information and decide what to do, WildLeaks uses intelligence methodologies, a vast network of contacts and the latest technologies (WildLeaks, 2019).

Problem / Objective Analysis

The whistleblowing System dimensions problem addressed includes Whistleblowing Procedure and Whistleblowing Protection. Whistleblowing Procedure is receive and evaluate anonymous information, reporting channel for whistleblowers. Whistleblowing Protection, on the other hand, provides secured communication channel with total anonymity and confidentiality.

Solution Analysis

The solution is related to Local and Regional Governance and Stakeholder participation. The output is public service. The Digital Government evolution model is contextualization. The following Digital Government elements were applied: 1) Digital by design – online portal to report wrongdoings. Allows the whistleblower unique receipt number, providing secured communication using digital tools WildLeaks website and Tor technology; Providing interface through website channel and mobile application and it provides service through 16 different language versions and smartphone applications; 2) User-Driven – gaining the accessibility of the public service. 3) Government - providing informational services.

Table 5. 1: Digital enabled whistleblowing initiatives case study analysis

Dimension	**Case 1 - PPLAAF**	**Case 2 - XNET**	**Case 3 - VWC**	**Case 4 - WildLeaks**
Whistleblowing Procedures	- Website channel, PPLAAF’s hotline and GlobaLeaks platform - Provide Reporting Mechanism either English or French language - Allows to accept both voice (hotline) and written (platform) discloser - Uses of Case Management Tool to manage all the cases - Secure website, encrypted messaging service, and hotlines.	- Provides GlobaLeaks platform and *the Blesa emails as* whistleblowing channel - Provides English and Spanish, Catalan Language	- 24 hour a week accessible Toll free number, SMS, fax, website, email, and PO Box provided for whistleblower to report suspected incidents of misconduct; - Reporting either in Indonesia or English language - Expert forensic investigators to analyze reports	- Provides WildLeaks online platform to send sensitive information. - Reporters can report in either of 16 languages on the web.
Organizational Structure	- Legal assistant - Pro bono legal advice and/or defense. - Provides guidance on how to approach journalists - Provides how to get Media assistant - Connection to credible investigative partners. - Provides training on security and	- Provides for journalists and citizens a FAQ service regarding the whistleblowing channel	- Employee education and training on policies and procedures to prevent misconduct; - awareness raising of PT Vale employees of the Whistleblower system; - Specialist call centre operators with knowledge of PT Vale;	- It Provides information in16 different language versions and smartphone applications - It allows the whistleblower to add more information about your original submission, Send us a message and Interact

	communication to staffs and activists - Notification message on new arrival report		- Timely reporting of incidences to PT Vale WBS team. - Recommendations on corrective action.	with the system in an anonymous way.
Whistleblower protection	- Provides secure website, encrypted messaging service, and hotlines through TOR network allowing for individuals to safely connect - Provides a digital record for both oral and written disclosure	- It uses Tor network and GlobaLeaks which enables Secure anonymizes communications (Secure anonymous mailbox) and - Xnetleaks mailbox - Provides a digital record for blesa email	- Encrypt the message to manage anonymity and confidentiality - Provides a digital record for protected disclosure	- Provides both confidential and anonymous disclosure - It provides very secure online platform built on the Tor technology - Always encrypted in respect to data transmission and management. - Provides a digital record for both oral and written disclosure

5.1.2. Cross Case Analysis

The cross-case analysis is a method that involves the in-depth exploration of similarities and differences across cases. This section presents the finding of the analysis of the case studies (Digital Government for whistleblowing initiatives) based on the conceptual framework of DGOV4WB described in section Four.

In whistleblowing analysis, the researcher managed to identify a total of 8, 4 and 2 problems/issues for whistleblowing procedure, whistleblower protection and whistleblowing organizational culture respectively as shown in Table 5.2, 5.3 and 5.4. The solution analysis of the case studies identifies 10, 6 and 10 types of solutions related to government as a platform, Digital by design and user-driven respectively. The DGOV solutions are listed in Tables 5.5, 5.6 and 5.7 respectively as government as a platform, user-driven and digital by design.

Table 5. 2: Whistleblowing Dimensions - Whistleblowing Procedure

S.No	Whistleblowing Procedure related problems / objectives	Case No
1	Providing easily accessible reporting channel	1,4
2	Providing reporting channels available at all-time 24x7	1,2,3,4
3	Providing secured channel to communicate in response – to receive feedback	2
4	Providing clear and understandable procedures for internal reporting.	1,2,4
5	Providing digital tool (Case Management System) for recording, investigating and monitoring reports.	2
6	Receive and evaluate anonymous information	1
7	Providing FAQ for the society	2
8	Providing access for status and process of the complain	2

Table 5. 3: Whistleblowing Dimensions - Whistleblowing Protection

S.No	Whistleblowing Protection related problems/objectives	Case No
1	Providing secured reporting channel (secured communication)	1,2,3,4
2	Providing anonyms connection	1,2,4
3	Providing confidential connection	1,2,4
4	Providing Protection of whistleblower identity ensured throughout all stages of the investigation process	2, 4

Table 5. 4: Whistleblowing Dimensions - Whistleblowing Organizational Culture

S.No	Whistleblowing Organizational Culture related problems/objectives	Case No
1	Providing regular trainings for WB team	2
2	Providing regular trainings for employees on whistleblowing frameworks	2

Table 5. 5: Digital Government Dimensions – Government as a platform

S.No	Digital Government Dimensions – Government as a platform	Case No
1	Providing service through different language versions	4
2	Providing user friendly interfaces website channel	2,4
3	Providing user friendly mobile application.	4
4	Providing simple interfaces	1
5	Providing unified identity for each complain	2
6	Providing telephonic support (Hotline)	1
7	Providing interaction through email	3
8	Providing service through smartphone applications	4
9	Providing different platforms accessible through different forms of channels	1
10	Promoting digital technologies to support service delivery	3

Table 5. 6: Digital Government Dimensions - User-Driven (societal)

S.No	**Digital Government Dimensions – User Driven related solutions**	**Case No**
1	Developing human capacity through training	2
2	Delivering enhanced public service	4
3	Empowering citizens	1
4	Empowering citizens through civil society	2
5	Enhancing citizen participation	2
6	Addresses citizen demand on who wants reporting wrongdoing and providing enhanced service.	2

Table 5. 7: Digital Government Dimensions – Digital by Design

S.No	**- Digital Government Dimensions – Digital by Design related solutions**	**Case No**
1	Providing online portal to report wrongdoings	1,2,4
2	Providing digital tools to report wrong doings	3
3	Providing mobile based platform for service delivery	2,3
4	Providing secured communication using digital tools WildLeaks website and Tor technology	1,4
5	Provide digital tools to analyze reports	2
6	Publishing information on the portal	1,2
7	Providing Case Management Tool	1
8	Promoting Anti-Corruption Complaint Box powered by GlobaLeak and Tor technology	2
9	Applying secured technologies	1,2,4
10	Providing digital forensic investigators service to analyze reports	3

5.1.3. Whistleblowing and Whistleblower Protection Stakeholders Identification

Freeman (1984) defines a stakeholder as "any group or individual that affects or is affected by firm behavior or organizational objectives" (Freeman, 1984). This includes entities or individuals that can reasonably be expected to be significantly affected by the organization's activities, products and/ or services; and whose actions can reasonably be expected to affect the ability of the organization to successfully implement its strategies and achieve its objectives (Amadi, Carrillo & Tuuli, 2014). On its stakeholder analysis, World Bank (WB, 2020) states that stakeholders fall into one or more of the following categories: "international actors (e.g. donors), national or political actors (e.g. legislators, governors), public sector agencies (e.g. MDAs), interest groups (e.g. unions, medical associations), commercial/private for-profit, nonprofit organizations (NGOs, foundations), civil society members, and users/consumers". Based on the above definitions, whistleblowing stakeholder represents all parties, including public, private and voluntary sectors with interest and concern in whistleblowing and whistleblower protection and their progress and outcomes within the organizational ability.

In our database searches as stated in section three, 35 research papers (publications) further elaborated and provides concrete values to identifying the possible stakeholders in whistleblowing domain. Based on the analysis, they were fairly evenly distributed along the 11 types of stakeholder's of whistleblowing domain: media outlets and journalist (29%), ombudsman (25%), courts (15%), whistleblower (90%), judiciaries/lawyers (55%), NGO (65%), government (80%), civil society organizations (35%), Board Members (68%), Business Association and Public Associations (45%). The qualitative analysis on the state of the research on whistleblower and whistleblower protection is described below and summarized in Figure 5.1.

The analysis result shows that whistleblowing within an organization is developed on the basic maturity level of ten main stakeholders. Whistleblowers - comprise different people including current employees and consultants as the key whistleblowers within an organization; and former employees and consultants, citizens and customers as rising stakeholders to speak up wrongdoing activities. The current employees are typical beneficiaries. Therefore, eligible parties should also encompass former employees, current and former consultants, contractors, suppliers and clients.

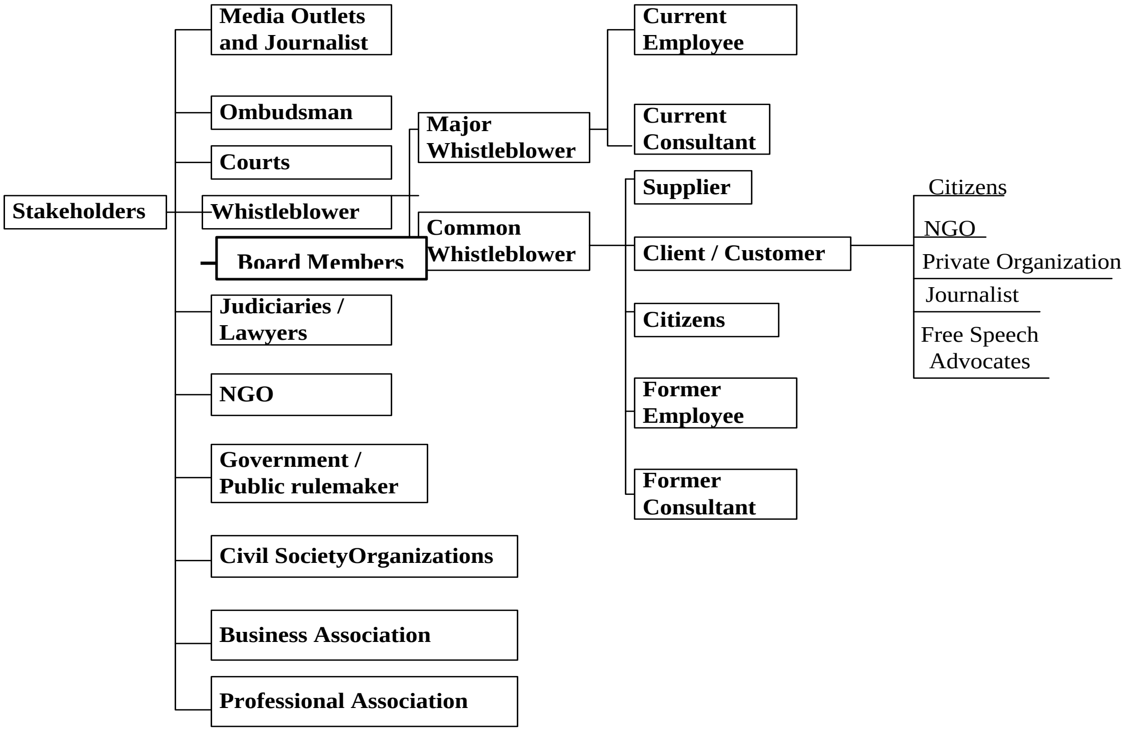


Figure 5. 1: Stakeholder Analysis Model for whistleblowing and whistleblower protection

Depending on the organization, even members of the public or NGOs may hold valuable information about ethical lapses or legal breaches. Whistleblowing and whistleblower protection should involve government, organizational board members, whistleblowing ombudsman and judiciaries / lawyers, courts as the main stakeholders, engaging them in the design of policy, investigation of wrongdoing complaints and prosecutions is one of the pillars which enforcement action relies upon. This concept also introduce non-governmental organization (NGO), business association, professional association and civil societies as a stakeholders. In order to provide the best whistleblowing services to whistleblower, their different contribution should be taken into account in planning and design of whistleblowing program.

Whistleblowers could be inside the organization (internal) - employee of the organization or a related entity or outsiders (external) (Near & Miceli, 1995). However, many organizations have internal whistleblowing processes / platform for managing complaints (Benchekroun & Pierlot, 2012). Considering the types of whistleblowing - internal and external, the organizational whistleblowing including the stakeholder's linkages is shown in Figure 5.2. The legend with its description (Table 5.8) helps to understand detail functionality of each stakeholders.

Considering the target organization, there are the various stakeholders that could interact in the whistleblowing process. Civil society, professional association and business associations may promote or oppose whistleblowing. They could also plays crucial role in protection the whistleblower against retaliation. Media outlets and journalists could play their role in publicize the disclosed information by the whistleblower and this could put pressure on the target organization. Public rule-makers (government) could create rules to protect the whistleblowers from any means of unlawful penalty due to whistleblowing including retaliation. Courts, organizational ombudsman and judiciaries may act on violations of the law based on the disclosed information by the whistleblower.

The target organization could use the digital technologies tools thinking on the different advantages on protecting the whistleblowers and help disseminate the disclosed information such as WikiLeaks or the International Consortium of Investigative Journalists, and encouraging the potential whistleblowers through providing better support for whistleblowing likes of the Government Accountability Project (Tom & Shelley, 2013).

Table 5. 8: Legend description

Legend	**Description**
⇢	This legend defines the flow of information's from whistleblowers
➔	Advocacy or protection of whistleblowers
→	Legal contact, or rejection of the whistleblowing
➝	Indicates boundary of target organization / institution

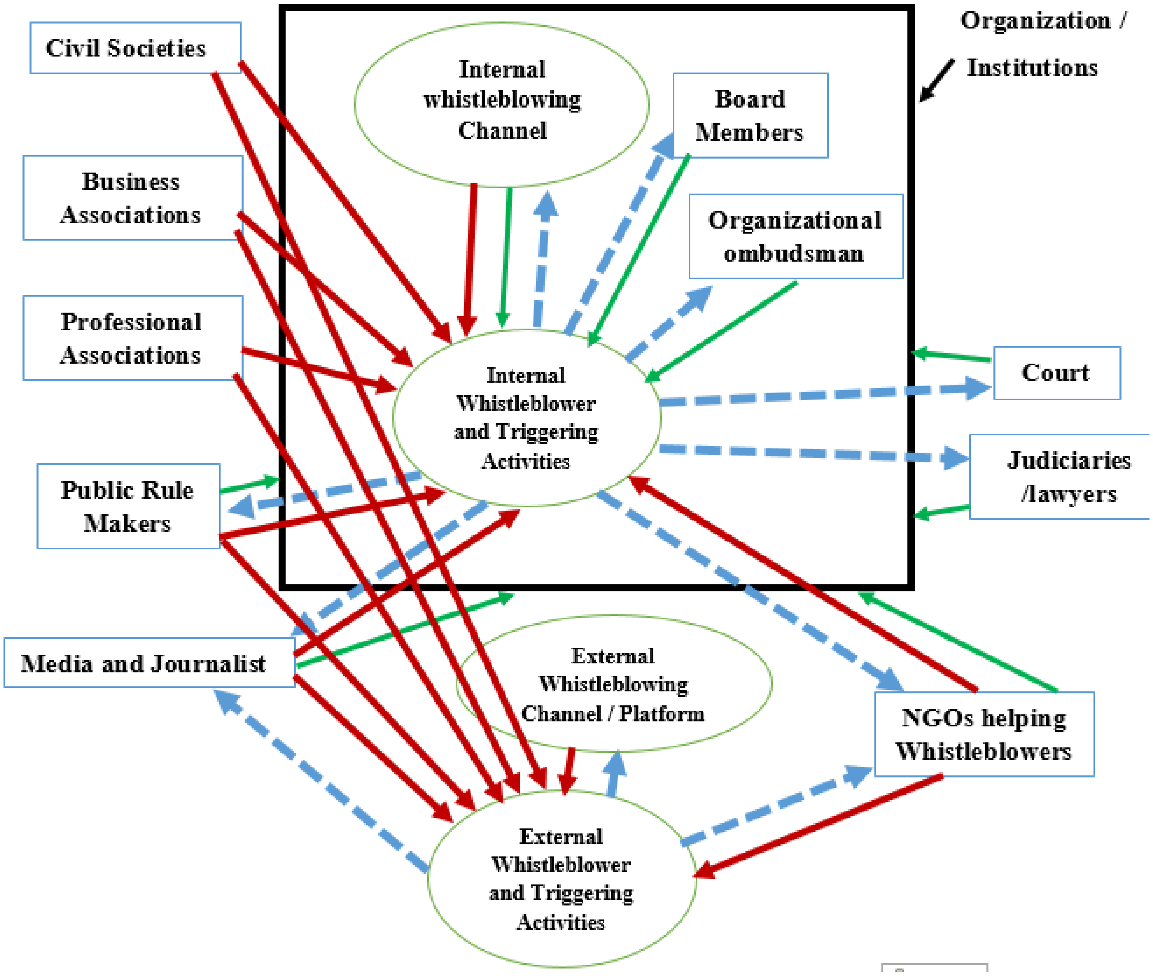

Civil Societies
Business Associations
Professional Associations
Public Rule Makers
Media and Journalist
Internal whistleblowing Channel
Board Members
Organizational ombudsman
Organization / Institutions
Internal Whistleblower and Triggering Activities
Court
Judiciaries /lawyers
External Whistleblowing Channel / Platform
NGOs helping Whistleblowers
External Whistleblower and Triggering Activities

Figure 5. 2: Relation of Stakeholders with respect to the whistleblower

5.1.4. Digital Government Stakeholder Analysis in Whistleblowing and Whistleblower protection

As clearly described in the above sections, whistleblowing and whistleblower protection is essential to encourage the reporting of misconduct, fraud and corruption. The Stakeholders represent all parties, including public, private and voluntary sectors with interest (Amadi, Carrillo & Tuuli, 2014) and concern in whistleblowing and whistleblower protection progress and outcomes. As a general classification, there are six main stakeholders identified that can have an impact on both whistleblowing and whistleblower protection. This includes government, employees, customers/ citizens, whistleblowers, non-governmental organizations (NGOs) (including civil societies, professional associations, and business associations), and media outlets. The multi-stakeholder analysis includes six types of interaction between stakeholders which is created from government - public authority- to other 5 stakeholders and government itself. It includes government-to-government (G2G), government-to-employee (G2E), government-to-citizen/customer (G2C), Government-to-NGO (G2N), government-to-whistleblower (G2W) and government-to-media outlets (G2MO). The description of each interaction is stated in Table 2.3 and a detail explanation of the impact of Digital Government strategies in each interaction for whistleblowing and whistleblower protection described later on the paper.

The six types of Digital Government interaction discussed in this paper include the illustration of Digital Government approaches and applications that provide target stakeholder groups with information and services related to the whistleblowing domain. The purpose was to construct the cause-effect framework based on Janowski (2015). All the cases and applications used to demonstrate the interaction were found from September to December 2019 by visiting whistleblowing websites.

5.1.5. Government-to-Government (G2G) Relationship

Government to Government (G2G) interaction is a collaboration of two or more governments or governmental agencies, departments or organizations sharing information, and cooperation. This involves both intra-agency and inter-agency exchanges at the national level, as well as exchanges between the national, provincial, and local levels (Hiller & Belanger, 2001). It can lead to effective service and the realization of the monitoring goals (Fan, Zhang & Yen, 2014). The interactions that include communication and collaboration between government and other public entities have also increased substantially due to a need to monitor and react to illegal activities. G2G has a more domain-specific and inter-organizational orientation and this can benefit from digital technological advancement that improves communication, data access and data sharing or better service delivery through the Digital interaction between a government and governments /agencies (De Vries, 2007).

In whistleblowing domain, A well-known illustrations in the use of digital technologies to G2G relation are the sharing of open whistleblowing data collected by local governments with other local governments and national agencies to enhance policymaking, the sharing of whistleblowing data between countries to learn the extent and types of unlawful activities, or the sharing of whistleblowers protection policies to improve the safety of the whistleblowers globally. This interactions and collaboration can benefit from the technological advancement. Notable example in technology enabled G2G interaction is statistical dashboard provided by Organisation for Economic Co-operation and Development (OECD) which has 36 member countries (OECD, 2014). Available at http://www.oecd.org/corruption/ethics/whistleblower-protection.htm - OECD is a leader in intergovernmental whistleblower protection instruments. It released a recommendation on improving ethical conduct in the Public Service. It provides a guide where areas for reform and proposes next steps to strengthen effective and comprehensive whistleblower protection laws in both the public and private sectors. OECD provides a platform for sharing of best practices and policy recommendations to enact an effective whistleblower protection laws at national and European levels.

Another notable example for G2G interaction is Occupational Safety and Health Administration (OSHA) Whistleblower Protection Programs under United States Department of Labor which provides a comprehensive statistics - Whistleblower Investigation Data - across the country for more than twenty whistleblower statutes protecting employees who report violations of various workplace safety and health, airline, commercial motor carrier, consumer product, environmental, financial reform, food safety, health insurance reform, motor vehicle safety, nuclear, pipeline, public transportation agency, railroad, maritime, and securities laws which is available on https://www.whistleblowers.gov/factsheets_page/statistics.

Another notable example is The European Corruption Observatory available on http://transparency.eu/project/european-corruption-observatory/ an online database of media articles about cases of corruption in the European Union. This online tool fosters awareness around trans-boundary corruption trends and main whistleblowing cases and allows citizens, journalists, and civil society to search for and access articles about corruption cases published by different media sources.

5.1.6. Government-to-Employee (G2E) Relationship

The goal of Government-to-Employee (G2E) is the interactions between public authorities and their employees to coordinate internal operations and improve the internal efficiency through sharing and accessing of information such as policies, training (Tang et al., 2011; Rao, 2017) and exchange of information regarding works and performance, personnel policy, data, and notice for career management and development of government employees, etc. Different research outcomes shows that the G2E interaction services not only boost internal communications management, automation, procurement, recruitment, etc. **(**Ho K., Yu C. & Lai M., 2005) but also improve efficiency, transparency, reliability, accountability, and quality of services (OECD & ITU, 2012; Golubeva & Merkuryeva, 2006).

Digital technologies offers a range of tools, documents and data that help employees maintain communication and coordinate work with their offices (katsois, 2015). This includes initiatives that will facilitate the management of the civil service and internal communication with governmental employees. Public administrations can maintain online records of personal information of their employees or create shared platforms for internal documentation to promote paperless interactions. They can also create an online platform to receive any wrongdoing activities across the organization so as to improve the efficiency and competitiveness of the organization.

In relation to whistleblowing and whistleblower protection domain, government and organizational authorities are working on the delivery of information about the organization law and practice of whistleblowing across the organization and establishing safe channels for reporting within an organization through an internal digital platform. It also includes digital tools used by government authorities to provide online training and education on cases of whistleblowing and whistleblower protection to their employees.

The most notable example in G2E whistleblowing interaction is OSHA. In US federal Employees have a right to file a safety and health complaint or a whistleblower complaint with OSHA (under US department of labor) if employees believe that their employer retaliated against them for exercising their rights as an employee under the whistleblower protection laws enforced by OSHA. In states with OSHA-approved State Plans, employees may file complaints with Federal OSHA and with the State Plan. OSHA also accepts whistleblower complaints made orally (telephone or walk-in at any OSHA office) or in writing, and in any language. https://www.osha.gov/whistleblower/WBComplaint.html https://www.whistleblowers.gov/

Germany's banking supervisor introduced Germany's Federal Financial Supervisory Authority (BaFin) https://www.bafin.de/EN/Homepage/homepage_node.html which has created an anonymous online portal for bank workers who want to report money-laundering and corruption. French electric utility company, Électricité de France S.A. (EDF; Electricity of France) https://www.edf.fr/en/the-edf-group/our-commitments/ethics-compliance/whistleblowing-system provides an ethics and compliance whistleblowing system designed to receive, record and process on a secure platform, in complete confidentiality for its employees and occasional employees and its third parties.

5.1.7. Government-to-Customer / Citizen (G2C) Relationship

Government-to-Customer / Citizen (G2C) interaction involves initiatives designed to facilitate people's interaction with the government as consumers of public services and as citizens (Hiller & Belanger 2001). This includes interactions related to the delivery of public services as well as participation in the consultation and decision-making process, exchange of instant messages directly with public administrators, electronic voting, and declaration of taxes online, agency hotlines or call centers, etc. The main goal of the G2C interaction is to enhance the relationships through digital technology – technology-mediated or technology-enhanced- between public authorities and citizens/customers under the jurisdiction of the authority. There are digital tools that can create a better communication link between a public authority and citizens/customers.

In the case of whistleblowing and whistleblower protection domain, government and organizational authorities are working on the provision of information about the organization law and practice of whistleblowing and whistleblower protection and provision of establishing safe channels for reporting allegations of serious wrongdoing or gross mismanagement both within an organization and to public authorities. It provides information -informs citizens - on how and when to protect whistleblowers against dismissal, demotion and other forms of retaliation.

A notable example of the G2C relationship is Indian government digital whistleblowing channel Central Vigilance Commission (CVC). It is working on awareness creation about corruption in India to its citizens. To encourage the fight against corruption, CVC has provided on their website, a "Lodge Complaints Online" portal available at http://portal.cvc.gov.in/cvproject/.

Another notable example is South Korea anti-corruption & civil rights commission (ACRC) which provides online whistleblowing platform for any person to report an act of corruption to the ACRC through digital whistleblowing channels available at https://www.clean.go.kr/index.do. This allows citizens to report if anyone discovers that a violation occurred or occurring that may violate or has violated public interest.

5.1.8. Government-to-NGO (G2N) Relationship

G2N is the interactions between public authorities in one side and non-governmental organizations on the other side to jointly address social, economic and political problems related to the impact of whistleblowing and whistleblower protection improvement on countries and communities. While it is the responsibility of the governments to facilitate safe and effective channels for whistleblowing and to protect public interest whistleblowers, non-governmental organizations play an effective role on providing as much of their long expertise defending whistleblowers through the courts and in the public arena as it could and provision of information delivery, regulations, and financial support to the organizations. Digital technologies play a crucial role in creating links between governments and NGOs to achieve their common targets – encouraging whistleblowers to report any wrongdoing activities and providing legal support for whistleblowers such as protection against any reprisals and to advocate for stronger and more comprehensive legal rights and protections for whistleblowers.

One of the examples in G2N is the Digital Whistleblowing Fund available in https://www.whistleblowingfund.org - a small-grant project by the Hermes Center for Transparency and Digital Rights and Renewable Freedom Foundation that will provide fund for digital whistleblowing projects in the areas of “Anti-corruption Activism” or “Environmental Digital Whistleblowing Activism” or “Human Rights Digital Whistleblowing Activism”.

Another notable example is Whistleblowing International Network (WIN) - the international network of whistleblowing NGOs – is available on https://whistleblowingnetwork.org/ which connects and strengthens civil society organizations that defend and support whistleblowers. WIN provides “counsel, tools, and expertise needed by those working in their countries to address corruption, waste, fraud, abuse, illegality, and threats to the public interest”.

The Centre for Free Expression (CFE) Whistleblowing Initiative - https://cfe.ryerson.ca/key-resources/initiatives/cfe-whistleblowing-initiative - is another NGO project of the Centre for Free Expression at Ryerson University with the aims of protecting Canadian society by making responsible whistleblowing possible through effective protection for Canadian whistleblowers. Its work is undertaken in collaboration with academic and community-based organizations across Canada and internationally. This helps Canadians to live and work with integrity and to combat misconduct that may threaten the well-being of communities and their democracy.

Transparency International Ireland http://transparency.ie/ is an independent of government, politically non-partisan, and not profit-making Irish chapter of the worldwide movement against corruption to empower people with the support they need to promote integrity and stop corruption in all its forms.

The National Whistleblower Center (NWC) https://www.whistleblowers.org/, a non-profit, tax-exempt, non-partisan organization, is the leading whistleblower legal advocacy organization with an almost 30-year history of protecting the right of individuals to report wrongdoing without fear of retaliation. The National Whistleblower Legal Defense and Education Fund (NWLDEF) is a non-profit law firm that provides services to the NWC and whistleblowers from around the world.

5.1.9. Government-to-Whistleblower (G2W) Relationship

G2W interactions catch relationships between public authorities and whistleblowers or non-residents to the nation or domain beneath its jurisdiction; such whistleblowers might, for instance, be national or international whistleblowers. G2W services include information services that explain to whistleblowers how to blow the whistle - actual procedures for making a disclosure whenever they witness illegal activities and provide detail information on protection mechanisms, and other topics.

Technological innovations have been used extensively in this domain, especially through the provision of online information and digital whistleblowing to prospective authorities or the public. Different national, regional and local whistleblowing or complaint portals are used, along with mobile apps. Example of an online report platform is corruption watch in South Africa in fighting corruption https://www.corruptionwatch.org.za/ and Uganda anti-corruption unit https://reportcorruption.go.ug/ .

In addition, public authorities use digital technology to enhance the experience of whistleblower through the provision of whistleblowing information and mobile app programs, e.g., in Indonesia (https://www.sprm.gov.my/en/enforcement/maccmobile-application) MACCMobile public to disseminate corruption information to the Malaysian Anti-Corruption Commission (MACC). In the latter case, the interface is provided in 23 languages; this service could not be easily offered at a physical border.

5.1.10. Government-to-Media (G2M) Relationship

G2M involves the interaction between public authority and Media outlets. It emphasizing an important role of mass media as a bridge in public relations between government and citizen, NGO, whistleblowers, and others. Media outlets include newspapers, magazines, radio, television, and the internet that provides whistleblowing news and feature stories to the public through various distribution channels. The notable example of G2M interaction is broadcasting the latest whistleblowing news through broadcast media such as CNN on 737 max jets after a fatal crash of Ethiopian Airlines and Lion airlines https://edition.cnn.com/2019/04/26/politics/faa-hotline reports/index.html and BBC on (787 Dreamliner oxygen system) https://www.bbc.com/news/business-50293927. Another example is in the United Kingdom https://www.whistleblower.co.uk/ the digital platform allows people to have the option of confidentially selling stories to the press while retaining their anonymity. Whistleblowing requires the participation of the whistleblower and a publication platform: generally a role performed by the media. Bradley Manning turned to WikiLeaks only after he was rejected by a number of other publications, but WikiLeaks also offered anonymity.

5.2. Quantitative Data Analysis

5.2.1. Study Sample and Descriptive Analysis

One of the main focuses of this research is on people who use Digital Government whistleblowing systems to report misconducts in their work place. Respondents were employed people in governmental organizations and institutions who, because of their career, were identified as having greater than average access to the internet or other digital technologies to access whistleblowing systems. This ensures that the respondent sample represents the population of interest in Ethiopia's uses of Digital Government whistleblowing systems.

5.2.2. Overview of the Survey

5.2.2.1. Response Rate

According to Allen (2017), Low response rate has been recognized as one of the main problems in research surveys. This low response rate can give rise to sampling bias if the nonresponse is unequal among the participants regarding the outcome. There are lots of strategies recommend to increase the response rate; however, a combination of common strategies incorporated in the design, development, and administration of surveys has proven to be effective in maximizing response rate. Some of the common strategies includes making survey user-friendly --- survey is simple and easy to complete --, Appearance matters --- Make sure the questionnaire is “user-friendly” and of reasonable length, and Focus on essential questions ---, and Ensure confidentiality -- Provide assurance that respondents’ information will be kept confidential. Let respondents know who will be viewing the survey results and how the information will be used. Having this in mind, the existing questionnaire was reviewed to ensure the questionnaire was understood via the pilot test not only by other participants but also by potential respondents. Personally administered survey used in this study since it can provide high response rate, enables quick data collection and allows the respondents the opportunity to ask direct questions about the research and questionnaire. To maintain the independency and secrecy, the questionnaire was completed by the respondent. Some individuals (with proper background) has been participated in collecting the survey.

As presented in Table 5.9, the total questionnaires distributed to respondents was 800. The survey received 610 total responses. A review was then undertaken to seek out errors in the form of invalid data, including missing values or incomplete responses. This step was conducted to produce clean data for research analysis. As a result, 56 questionnaires were found to be incomplete.

Table 5. 9: Survey result of response rate review

Response Number	
Total Questionaries’ distributed	800
Total responses	610
Incomplete responses	56
Effective usable responses	554

Therefore, those incomplete questionnaires were excluded to avoid fallacious results. Finally, 554 responses were found to be useable in this research, indicating the response rate is 76.25 % and the effective response rate in this study is 69.25%.

5.2.2.1. Descriptive Analysis of the Sample

Considering the final data of the survey, a descriptive analysis using PLS was undertaken to understand the respondents' demographic characteristics in this research. Table 5.10 presents the detailed demographic data of the respondents.

Table 5. 10: Demographic data of the respondents

Data	Items	Frequency	Percentage
Gender	Male	376	67.87
	Female	178	32.13
Age	22 – 30	332	59.92
	31 – 40	171	30.86
	>40	51	9.22
Occupation	Government organization	170	30.68
	Government Institutions	384	69.32
Whistleblowing System usage per a week	< 1 time	55	9.93
	1 – 5 times	265	47.83
	5 – 10 times	151	27.26
	> 10 times	83	14.98

As presented in Table 6.11 above, only 32.13 percent of respondents are females while majority of 67.87 percent are males. Most of the respondents (or about 59.92 % of the respondents) were from 22 to 30 years old; 30.86 % were age between 31 - 40 years; only 9.22 % were above 40 years of age. The respondents were engaged in various governmental occupations: 30.68% of them were employed by the government organizations and 69.32 % of them were from public institutions. However, the result shows that the highest no of interaction (engagement) of the respondents with digitally enabled whistleblowing system usage per a week is 1 to 5 times (47 %) and 5 to 10 times a week interaction counts 151 respondents (27%); only 83 respondents 14.98 % were interact the system greater than 10 times whereas 55 respondents (9.93) may not be contacted the digitally enabled whistleblowing system at all in a week.

5.3. Summary

The qualitative and quantitative data analysis for this research is outlined in this chapter. The qualitative data analysis was used mainly to understand the impact of Digital Government in whistleblowing and whistleblower protection while quantitative data analysis is done to investigate factors that affect the citizens' acceptance of digitally enabled whistleblowing systems to help the Ethiopian government design and implement better whistleblowing systems. This chapter also describes the Digital Government Stakeholder Analysis in Whistleblowing and Whistleblower protection through real-life concrete examples.

CHAPTER VI

RESULTS AND DISCUSSION

6.0. Introduction

This chapter aims to discuss and interpret the findings by using the results of this study. This chapter will make use of descriptive outcomes in order to provide additional explanations and clarity to the findings discussed. Mainly, cases-study results will be discussed in descriptive way. This chapter also introduces the performance measurement framework for whistleblowing and discusses the impact of Digital Government on such a framework. Based on Janwoski (2015) Digital Government evolution model, this chapter introduces Digital Government Cause-Effect framework for whistleblowing domain. The last but not least, this chapter discuss the evaluation of the TAM Model in the context of Digital Government whistleblowing system implementation in Ethiopia.

6.1. Case Study Results

Considering the DGOV4WB conceptual and assessment frameworks described in chapter 3 and chapter 4 respectively, the researcher started to analyze all the case studies. In our analysis, the themes are identified through the iterative process of identifying WB problems and DGOV solutions based on case studies.

Our case study analysis showed that DGOV4WB initiatives/projects positively contributed to solving a variety of whistleblowing (WB) issues/problems. Specifically, WB problems addressed by the WB dimensions includes whistleblowing procedure, whistleblowing organizational structure, and whistleblower protection. Whistleblowing Procedure is concerned with whistleblowing reporting mechanism and monitoring the process; Whistleblowing Organizational culture is about communication (training all involved stakeholders); Whistleblower Protection aims at anonymity and confidentiality of communication.

The analysis also showed that DGOV4WB initiatives applied to a variety of DGOV solutions in different DGOV dimensions: supportive ecosystems which are an easy and interactive interface of communicating channels to report the wrongdoing activities (government), ICT-enabled services and government ICT infrastructure based on user preference, and enabling the citizens/customers or any stakeholders to involve in the process through different languages and platforms and active citizen participation and civil societies contribution (User-driven), Digital transformation within the government and secured communication channel and Case Management Tools for recording and managing the complaints (Digital by design). The correlation between the dimensions of WB problems and the dimensions of DGOV solutions, problem to solution relation, as they occur within the case studies are presented in Table 6.1 based on the WB problems and DGOV solutions code mapping as depicted in Figure 6.1.

.

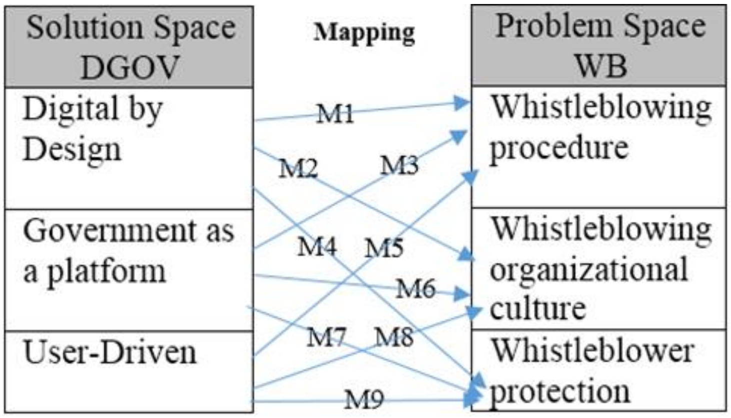


Figure 6. 1: WB problems and DGOV solutions code mapping

For each problem-solution pair, the Table lists all case studies that apply the solution to address the problem. Figures 6.2 and 6.3 depicts the distribution of the problems and solution across the WB and DGOV dimensions respectively.

As indicated in Figure 6.3, whistleblowing procedure is the highest-ranked categories of whistleblowing dimensions in problem description while according to Figure 6.2 the highest-ranked categories of DGOV solutions belong to digital by design and Government as a platform. While DGOV4WB solutions may be expected to holistically address all whistleblowing dimensions, this expectation is also the main challenge facing such initiatives.

Table 6. 1: Correlation between DGOV solutions to WB Problems through code words

Code Word	Case Numbers	Code Word	Case Numbers
M1	All cases	M7	1
M2	All cases	M8	3,4
M3	1,4	M9	1,3,4
M4	All cases		
M5	2,3		
M6	4		

The case study evidence indicates that digitally-enabled whistleblowing reporting channels, both electronic platforms and hotlines, used to facilitate individual disclosures. It eases the disclosure of organizational wrongdoing for protection against fraud and any wrongdoing activities. All the four cases provide a dedicated channel to whistle-blowing. An electronic platform whistleblowing channel exists in all of the case studies and except Xnet the other three whistleblowing initiatives provide dedicated hotlines. These reporting channels are open to receive reports for 24 hours of a day for all 365 days of the year. Both whistleblowing electronic platforms and whistleblowing hotlines enable the individuals to report unlawful activities through different language in either of whistleblowing disclosure methods --- oral or written. The finding identified Tor technologies have been used to provide whistleblower protection – anonymity and confidentiality. Our finding also shows that Case Management Tool has been used in two of our cases to manage the reported cases for recording, investigating, and monitoring reports. This case management tool provides a mechanism for notifications, analysis, and reporting management for each reported case. This enables the whistleblowers to track their whistleblowing reports at every stage of the whistleblowing process. This enables the whistleblowers to track their whistleblowing reports at every stage of the whistleblowing process and to communicate with the government/organization officials for further information. This capability of the whistleblowing system enables the active participation of employees in the whistleblowing process.

From the case studies, all the initiatives were classified either engagement (Electronic Governance) or contextualization (Policy-Driven Electronic Governance) stage of the Digital Government evolution model. Engagement stage enables engaging citizens and other nonstate actors in government decision making and trust building. It aims to transform relationships between government and citizens through the use of digital channels to build trust (Janowski, 2015). This digitally whistleblowing systems smooths the relationship between the government and its citizens in combating misconduct and frauds in an organization. According to Janowski (2015) Contextualization stage involves “the choice of locally-relevant and/or sector-specific goals, locally-acceptable and sectorally-feasible ways of pursuing such goals, and managing the impact on the local environment and sector involved”. It enables sectors, territories, communities, citizens, etc. to pursue development action by themselves. It aims to create better conditions through digital technology to pursue public policy and development goals. Whistleblowing systems allow the citizen to participate in tackling corrupt, unlawful activities within the organization.

The three case studies/initiatives: Xnet, Wildleaks, and PPLAAF are all developed by non-governmental organizations or individuals who are an active activist and lowers. VWC is a VAL company whistleblowing channel to support its good corporate governance (GCO) principles that could help to achieve accountability and transparency in the VAL Company. Interestingly, the result of the study indicates whistleblowing systems developed by non-governmental organizations are more user-driven (language and whistleblowing methods varieties) compared to governmental whistleblowing.

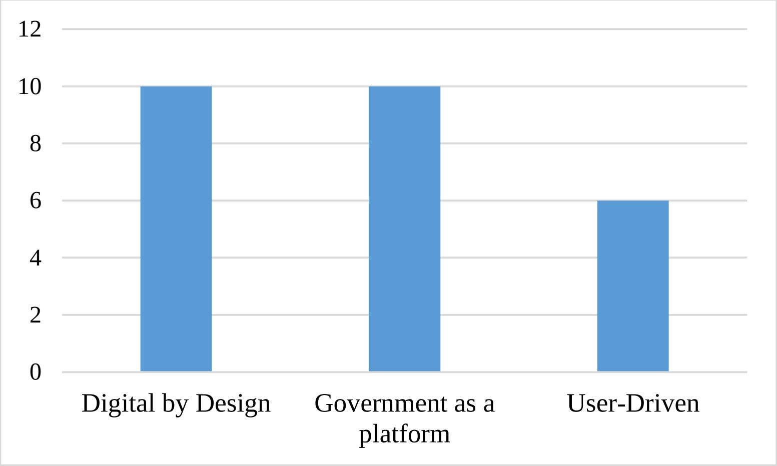


Figure 6. 2: Distribution of DGOV Solution

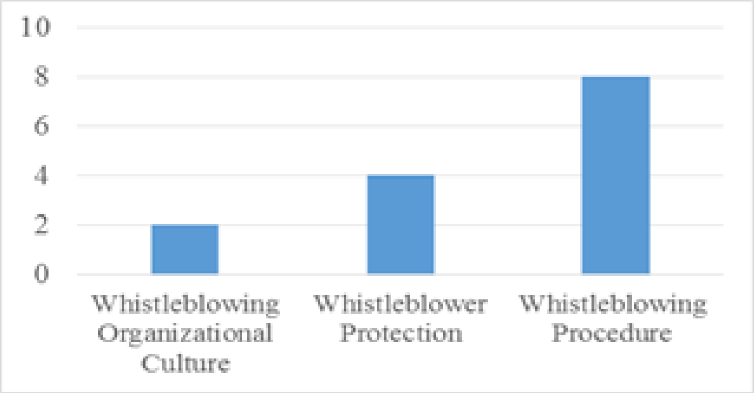


Figure 6. 3: Distribution of WB Problems

6.2. Whistleblowing Program Performance

This section aims to contribute to the study of whistleblowing performance by providing a conceptualization of performance that emphasizes on whistleblowing and whistleblower protection outputs. There has been lots of definition of performance in the literature. Jeffrey S. Kane (1996) defines “Performance is the record of outcomes achieved in carrying out a specified job aspect during a specified period.” Kane definition implies that i) performance occurs in reference to some particular aspect of a job, such as a job function; ii) record implies the discernibility of outcomes of different desirability levels and their differential occurrence rates; and iii) Performance is a record of outcomes compiled during some finite period of time (Kane, 1996). In this research, the performance of the whistleblowing program refers to an organization's overall whistleblowing activities or completion of a whistleblowing task. This involves problem-solving, and whether the program of rules successfully contribute to the desired problem-solving and looks to whether and to what extent a particular whistleblowing goal is achieved, considering of the actors that shape that achievement. It also conceptually bound to assessing organizational accomplishments in relation to the fraud and illegal activities detection goals of an organization.

Research indicates that the better a company is at collecting and responding to information brought forward by employees, the better they will be at detecting and limiting losses (Cordis, 2017). Most of the whistleblowing studies focus on scoring the availability, protection, and variety of whistleblowing channels and services, and strengthening whistleblowing system (i.e. Greenberg & Andy 2016; Maheran Zakaria, 2015; Nurhidayat & Kusumasari, 2016), but there is a lack of evaluation on the effectiveness and efficiency of whistleblowing services, which are core values of public administration as applicable to whistleblowing program successes. Overall, there is a deficiency in the rigorous development of multiple performance indicators and user-level empirical investigation of the determinants of the multiple aspects of performance. The following section [section 6.3] will develop a whistleblowing performance measurement framework.

6.3. Whistleblowing System Performance Measurement Framework

Based on the research literature review (Section 4.4.1), policy literature review (Section 4.4.2) and Whistleblowing legislation review (Section 4.4.3), this section presents the performance measurement framework for whistleblowing and whistleblower protection. This whistleblowing process performance measurement Framework will help to i) Evaluate the impact of technology-enabled whistleblowing process comparing before and after situations or comparing expected impact with a reference situation; ii) Monitor the progress of an organization as a whole towards its goals. The indicators/dimensions may be used to show to what extent the overall policy goals of the organization have been reached, or are within reach. In addition, whistleblowing process indicators may be used to compare organizations with each other by considering different factors. iii) Assess how the whistleblowing process has contributed to the objectives at the organizational level.

The following Table [Table 6.2] - shows whistleblowing program performance measurement frameworks based on the three whistleblowing dimensions identified by transparency international (TI-NL, 2017). The Table indicates that the whistleblowing dimension includes i) Whistleblowing Procedure; ii) Whistleblowing Organizational Culture and iii) Whistleblowing Protection. Variables in the Tables represent the main contributing components of each dimension. Whistleblowing Procedure dimensions expressed in reporting and response mechanism and monitoring the whistleblowing activities; Whistleblowing Organizational Culture includes communication between all member of staffs, commitment of higher officials of the organization and employee or citizen participation in whistleblowing; and whistleblower protection is explained through anti-retaliation mechanism, anonymous and confidential communication, Burdon of proof and civil and criminal liability. Each variable is described below.

Reporting Mechanism – is used to define the accessibility of different whistleblowing reporting channels for reporting of wrongdoings (TI, 2016; OECD, 2016c). These could be internal disclosures to a designated body and external disclosures to the public. This variable could measure through different indicators including variety of reliable reporting channels to report misconduct, guaranteeing confidentiality or anonymity preferably accessible 24 hours a day and 365 days a year either orally or written and., the ease of use of whistleblowing channel and availability of clear steps for the reporting channels, and the variety of language in which the reporting channels support to disclose unlawful activity.

Response (Responding) Mechanism – this variable defines the process of investigation of alleged wrongdoings to ensure thorough, timely and independent investigations of reports of misconduct. Research shows that once the report is made the investigation it should be clear and informed to all employees and response has to be provided to the whistleblower (TI, 2016; OECD, 2016c). This variable can be measured through indicators that include types and ways of communication with the reporters - feedback to reporters throughout all stages of the investigation process.

Monitoring – These variables define following valid whistleblower disclosures. This indicates that it shall be referred to the appropriate regulatory agencies for follow-up, corrective actions and/or policy reforms In fact, any whistleblowing program requires monitoring (TI, 2016; OECD, 2012, 2016).. The key statistics on whistleblowing cases collected and reviewed on a regular basis. This includes the number of whistleblowing reports or disclosure and its type (internal and external). It can also be measured through unlawful or fraudulent activities that have already occurred, to occur and still occurring, and it can also be dealt retaliation reports.

Commitment of Top Management (higher officials) this variable defines the direct involvement of top officials of organizations and their strong engagement in the whistleblowing program. It determines to what extent potential whistleblowers feel safe and comfortable to report wrongdoing internally (Maheran, 2015). The variable will be measured through the rate of organization/government information is published and the statistics on whistleblowing cases monitored and discussed regularly by the top management follow with regular advice and support for employees about whistleblowing (TI, 2016; OECD, 2012, 2016). In addition, top management has to confirm the whistleblower disclosures shall be referred to the appropriate regulatory agencies for follow-up. It also includes gathering information on the issues raised through whistleblowing program/frameworks and allows organizations to detect patterns and make improvements to their policies and procedures.

Communications – defines clear support of organizational higher officials for its employees and customers. This support will be measured through regular training for employees on whistleblowing frameworks which will include lessons from former whistleblowing cases (Maheran, 2015; TI, 2016; OECD, 2016c). In addition, the communication will also be measured by being transparent on the whistleblowing reports which can be published internal or externally on a monthly or annual base.

Employee or Citizen Participation – it defines employee or citizen engagement in the whistleblowing program. This includes key statistics on the number of complaints per individual employee in a given time frame (Maheran, 2015). *Anti-Retaliation (Anti –*

Victimization) - This variable defines the state of the retaliation of an employee within the organization due to the disclosure of unlawful activities (Dixon, 2017; Maheran, 2015; TI, 2016; OECD, 2016c & 2014). These variables could be indicated by discrimination or intimidation at the workplace due to whistleblowing and denied work necessary for promotion or demotion because the whistleblower has made a protected disclosure.

Anonymity and Confidentiality – it defines protection of whistleblower identity throughout the whistleblowing process If employees who raise concerns internally feel protected, the likelihood they will report their concerns internally and not externally, increases. This level of protection can be measured by looking at the possibility of raising a concern confidentially or anonymously (Dixon, 2017; TI, 2016; OECD, 2016c). These variables can be measured through the protection of whistleblower identity ensured throughout all stages of the investigation process and the number of third parties who might access this data without whistleblowers individual's explicit consent.

Burdon of Proof – this variable defines the protection of whistleblowers against any measures taken to whistleblowers were in no sense connected with or motivated by, a whistleblower's disclosure (Dixon, 2017; TI, 2016; OECD, 2016c). This variable will be measured by studying the number of cases of whistleblowers' harassment or any measure due to a whistleblower's disclosure. *Criminal and civil liability (Personal Protection):* it defines the protection of whistleblowers and his family by-laws from disciplinary laws - Protection against court action (Dixon, 2017; TI, 2016; OECD, 2016c). It could be measured through the reports from the whistleblowers and their families whose lives or safety is in jeopardy even though disclosure is made within the scope of whistleblower legislation.

On the framework Table (Table 6.2), the variable title is phrased as evaluating a static situation. A static indicator, assessing the situation at a certain recurrence in time, will allow monitoring over various periods. The framework also includes whether the indicator is affected by digitalization or not. The detailed description of the framework is explained in Table 6.3.

Table 6. 2: Whistleblowing Performance Measurement Framework

Whistleblowing Dimensions	**Variable**	**Variable Titles**	**Variable Identification**	**Definition**	**Reference**	**Digitization**
Whistleblowing Procedure	Report mechanism	Accessibility of Whistleblowing Reporting Channels /communication channel/	Numerical identification of the specific indicator	Detailed Definitions of specific indicator	Sources for the specific indicator	Whether the indicator is affected by digitalization or not.
	Response mechanism	Clear Procedures to ensure thorough, timely and independent investigations of reports of misconduct	”	”	”	”
	Monitoring	The key statistics on whistleblowing cases collected and reviewed on a regular basis.	”	”	”	”
Whistleblowing Organizational Culture	Communication	Clear support of organizational higher officials for its employees and customers	”	”	”	”
	Commitment of higher officials	Direct Involvement of Top officials and their strong engagement in the whistleblowing process	”	”	”	”

	Employee or Citizen Participation	Employee engagement in whistleblowing process	”	”	”	”
Whistleblower protection	Anti-retaliation	The state of the retaliation of an employee within the organization	”	”	”	”
	Anonymous and confidential	Protection of Whistleblowing Identity	”	”	”	”
	Burdon of proof	Protection against any measures taken to whistleblowers were in no sense connected with, or motivated by, a whistleblower’s disclosure.	”	”	”	”
	Civil and Criminal Liability	Protection of whistleblowers and his family by laws from disciplinary laws - Protection against court action	”	”	”	”

Table 6. 3: Detailed Whistleblowing Performance Measurement Framework

Whistleblowing Dimension	**Variable**	**Variable Title**	**Indicator ID**	**Indicator**	**Reference (Source)**	**Digitization**
Whistleblowing Procedure	**Report Mechanism**	Accessibility of Whistleblowing Reporting Channels /communication channel/	1.1	Extent in which types of channels that are available for reporting wrongdoing.	OECD, 2013; Bourne et al., 2015	Yes
			1.2	Number of channels by which protected disclosures can be made.	Bourne et al., 2015; Kaplan et al 2012	yes
			1.3	Extent to which whistleblowing reporting channels are available 24 hours a day, 7 days a week throughout the year.	Kaplan et al 2012; Ghana, 2016	yes
			1.4	The number of channel available for oral disclosure		yes
			1.5	The number of channel available for written disclosure.	Park H. & Lewis D., 2018; Ghana, 2016	yes
			1.6	Extent to which the availability of clear steps for the existing reporting channels		yes
			1.7	Extent to which the ease of use of whistleblowing channel	TI, 2013; Bourne et al., 2015	yes
			1.8	The number of language in which the reporting channels support to disclose unlawful activity.		yes
	Response Mechanism	Clear Procedures to ensure thorough, timely and independent investigations of reports of misconduct	2.1	The extent to which clear and understandable procedures for internal reporting including whistleblower regulations and procedures are highly visible and understandable.	Crook D,2000; OECD 2014	yes
			2.2	The extent to which feedback provided to whistleblowers throughout all stages of the investigation process is conducted.	Vandekerckhove W. & Lewis D., 2012; De Maria, 2008	yes
			2.3	The extent to which whistleblower are participated in providing input to subsequent investigations or inquiries.	TI, 2013; Crook D,2000	
			2.4	The extent to which whistleblower allowed to be informed of the outcome of any investigation or finding, and they are allowed to review and comment on any results.	De Maria, 2008; Crook D,2000	yes
			2.5	The extent to which the use of Case Management System for recording, investigating and monitoring reports.		yes

			2.6	The extent to which the assignment of clear accountability for all stages in the process.	Wei L. & Hsu C, 2014; Vandekerckhove W. & Lewis D., 2012	yes
			2.7	The extent in which reports are screened independently to assess the relevance and type of wrongdoing.		
			2.8	The extent to which the existence of transparent, enforceable and timely mechanisms to follow up on whistleblowers' retaliation complaints.	OECD, 2013	yes
	Monitoring	The key statistics on whistleblowing cases collected and reviewed on a regular basis. (Valid whistleblower disclosures shall be referred to the appropriate regulatory agencies for follow-up, corrective actions and/or policy reforms).	3.1	The number of whistleblowing reports or disclosure per reporting channel		yes
			3.2	The total number of disclosure by the whistleblower where conduct about which they are making the disclosure is unlawful, illegal or corrupt.	Ghana, 2016; TI, 2013; Vandekerckhove W. & Lewis D., 2012	yes
			3.3	The number of reports or protected disclosure made by written.	Ghana, 2016; TI, 2013, Lewis D., 2012	yes
			3.4	The number of reports or protected disclosure made by Verbal.	Ghana, 2016; TI, 2013	yes
			3.5	The number of oral disclosure within a given period of time.	Ghana, 2016; TI, 2013	yes
			3.6	The number of written disclosure within a given period of time.	Ghana, 2016; TI, 2013, Lewis D., 2012	yes
			3.7	The number of disclosure about unlawful or fraudulent activities that has already occurred	Ghana, 2016; TI, 2013	yes
			3.8	The number of disclosure about unlawful or fraudulent activities that is still occurring.	Ghana, 2016; TI, 2013	yes
			3.9	The number of disclosure about unlawful or fraudulent activities that is about to occur.		yes
			3.10	The number of reports per employee		yes
			3.11	The number of reports per department	Vandekerckhove W., Lewis D., 2012	yes
			3.12	The number of reports per issue type (internal)	Vandekerckhove W., Lewis D., 2012; Culiberg B.& Mihelič K.K., 2017	yes
			3.13	The number of reports from outsiders (outsiders)		yes

			3.14	The number of reports per issue type from outsiders (External)	Vandekerckhove W., Lewis D., 2012; Culiberg B.& Mihelič K.K., 2017	yes
			3.15	The number of retaliation reports	McIntosh T.,2019; OECD, 2013	yes
			3.16	The percentage of retaliation reports investigated in a time frame		yes
			3.17	The percentage of reports investigated in a time frame		yes
			3.18	The percentage of reports reported anonymously in a time frame	Ghana, 2016	yes
			3.19	The outcomes of cases / reports (i.e. dismissed, accepted, investigated, validated)	Canada, 2007; McIntosh T.,2019	yes
			3.20	The average time that takes to notify the complainer about the case (acceptance or Rejected)	McIntosh T.,2019;TI, 2013	yes
			3.21	The average number of days that cases / reports are awaiting		yes
			3.22	The Percentage of complaints substantiated	TI, 2013	yes
			3.23	The Length of time to investigate and close reports		yes
			3.24	The number of reports to external parties	TI, 2013; Culiberg B.& Mihelič K.K., 2017	yes
			3.25	The ratio of Repeat versus first-time reporters		yes
			3.26	The average number of disclosures received and complaints made in relation to reprisals are acted that were acted on and those that were not acted on.	TI, 2013	yes
	Commitment of Top Management (higher officials) - Whistleblowing	Direct Involvement of Top officials and their strong engagement in the whistleblowing process	4.1	To what extent potential whistleblowers feel safe and comfortable to report wrongdoing internally - the organisation's corporate culture comfortable.	(Wang et al., 2017; Stevens S.C.& Norris K., 2009; TI, 2016)	yes
			4.2	The extent to which organizational / government information is published - Whistleblower laws and procedures posted clearly in public to inform employees of their rights in connection with protected disclosures.	(Wang et al., 2017; Apaza C.R.& Chang Y., 2011)	yes
			4.3	The extent to which organizational / government published the functioning of whistleblower frameworks	(Stevens S.C.& Norris K., 2009; TI, 2016)	

Whistleblowing Organizational Culture				(in compliance with relevant privacy and data protection laws) annually.		
			4.4	The extent into which the establishment of the procedures to ensure the confidentiality of information collected in relation to disclosures of wrongdoings.	(Kaptein, 2011; Stevens S.C.& Norris K., 2009)	yes
			4.5	The extent to which the progress towards a whistleblowing and compliance with requirements is being monitored and reported		
			4.6	The extent to which senior executives accountable for the whistleblowing frameworks.	(Behrens A., 2015)	
			4.7	The extent to which the statistics on whistleblowing cases monitored and discussed regularly by the top management.	Kaptein, 2011	
			4.8	The extent to which the whistleblowing frameworks reviewed on a regular basis - effectiveness of the whistleblowing framework reviewed periodically.	Behrens A., 2015	
			4.9	The extent to which regular employee surveys to measure the awareness of whistleblowing frameworks.	Crook D.,2000; OECD, 2013	yes
			4.10	The extent to which regular trainings for employees responsible for receiving and investigating reports.		yes
			4.11	The extent to which regular comprehensive trainings for management and staff on Whistleblower laws and procedures.	Behrens A., 2015	yes
			4.12	The extent to which training to organization managers to recognise and prevent occurrences of discriminatory and disciplinary action taken against whistleblowers	Smith R., 2010	
			4.13	The extent to which regular advice and support for employees about whistleblowing.	Behrens A., 2015; TI, 2018	
			4.14	The extent to which the management works raise public awareness to encourage the use of whistleblower provisions, and enhance cultural acceptance of whistleblowing. (To changing cultural perceptions and public attitude towards whistleblowing, to be considered an act of loyalty to the organisation)	TI, 2013	yes
			4.15	The extent to which valid whistleblower disclosures shall be referred to the appropriate regulatory agencies for follow-up.		

			4.16	The extent to which based on the valid whistleblower disclosures corrective actions and/or policy reforms performed.	Culiberg B. & Mihelič K.K., 2017; Canada, 2007	
			4.17	The extent to which the confidential advisor appointed for advising employees about the reporting of wrongdoing	Culiberg B. & Mihelič K.K., 2017	
			4.18	The extent into which Investigations into complaints are to be conducted as informally and expeditiously as possible	Canada,2007	
			4.19	The number of recommendations that has been made in relation to complaints made in relation to reprisals.	Canada,2007; Culiberg & Mihelič, 2017	
			4.20	The number of recommendations that has been made in relation to the number of settlements of issues.	Canada,2007	
			4.21	The extent to which ensuring effective implementation of currently existing internal and external reporting mechanisms;	Culiberg & Mihelič, 2017	
			4.22	The extent to which promoting greater public understanding of reporting practices and available channels.	Crook D.,2000	yes
			4.23	The extent to which whistleblower disclosures shall be referred to the appropriate regulatory agencies for follow-up, corrective actions and/or policy reforms.	Crook D.,2000; OECD, 2014	
			4.24	The extent to which an independent review mechanism is provided to have a check on authority and helps to balance powers within an organisation.		
	Communications	Clear support of organizational higher officials for its employees and customers	5.1	Number of publishing lessons learned from whistleblowing cases	D'Cruz P. & Bjørkelo B. 2016; TI, 2013	yes
			5.2	The extent to which regular trainings for employees on whistleblowing frameworks.	Chordiya R. et al.,2019; D'Cruz P. & Bjørkelo B. 2016	yes
			5.3	The extent to which regular communication to employees about whistleblowing frameworks	Apaza C.R.& Chang Y., 2011; TI, 2013	yes
			5.4	The extent to which lessons learned from whistleblowing cases spread internally among employees	Apaza C.R. & Chang Y., 2011; Chordiya R. et al.,2019	yes
			5.5	The extent to which whistleblowing reports published externally (for example, in an annual report, website)		yes

	Employee or Citizen Participation	Employee engagement in whistleblowing process	6.1	The number of individuals actively participated in reporting as a percentage of the total employees of the organization.	Young R.F., 2017; Chokprajakchat S., 2017	
			6.2	Average number of complaints per employee in a given time frame.	Chokprajakchat S., 2017	yes
			6.3	The extent into which a single case is reported repeatedly by different employees.	TI, 2016	
			6.4	The extent into which whistleblower participation in court proceedings	Latimer et al, 2000; OECD, 2014	
			6.5	The extent into which the right of appeal for any whistleblower who believes he or she has suffered retaliation.		
Whistleblowing Protection						
	Anti-Retaliation (Anti – Victimization)	The state of the retaliation of an employee within the organization	7.1	The number of reporting retaliation related to the termination of employment of the whistleblower due to the case of related to whistleblowing.	Pacella J.M., 2015; Uys & Smit., 2016	
			7.2	The number of reporting retaliation related to the Suspension from job of the whistleblower due to the case of related to whistleblowing.	Uys & Smit, 2016; Australia, 2013	
			7.3	The number of disclosures received and complaints made in relation to reprisals.	De Maria W.,2006; Hassink et al.,2007;OECD,2017	
			7.4	The extent to which separate anti-retaliation policy that prohibits any form of retaliation against a whistleblowers who, in good faith, makes a complaint or raises a concern exists	Culiberg B.& Mihelič K.K., 2017	
			7.5	The extent to which the report of discrimination or intimidation at the workplace due to whistleblowing.	Canada, 2007; Keenan & McLain,1992	
			7.6	The extent in which whistleblowers physically isolated and given very little work to do or over-worked.	Uganda,2010;TI,2013	
			7.7	The extents in which the number of whistleblowers abused by work colleagues due to whistleblowing.	OECD, 2017	
			7.8	The average number of complaints received by whistleblowers on denied work necessary for promotion or demotion because the whistleblower has made a protected disclosure.	Volosova N.Y. & Zhurkina O.V. 2018; PCaW, 2015	

			7.9	The extent in which the average number complaints received on the attack or threat on personally (imprisonment and personal safety) of whistleblowers per period.	PCaW, 2015; GAP,2015	
			7.10	The average number of complaints received due to any measure taken to whistleblower that adversely affects the employment or working conditions whistleblower;	Canada 2007, Siallagan H. et al.,2017	yes
			7.11	The average number of complaints received due to disciplinary measure taken to whistleblower because of the whistleblower has made a protected disclosure;	Canada 2007, Siallagan H. et al.,2017	
			7.12	The average time takes to report against their reprisal by whistleblowers.	Canada 2007, Siallagan H. et al.,2017	yes
			7.13	The average amount of days where whistleblower reports against their reprisal from the day of reprisal by employer – the time for making complaint of against Reprisal		
			7.14	The average time necessary to take to notify the complainer about the reported retaliatory case.	Siallagan H. et al.,2017	
	Anonymity and Confidentiality	Protection of Whistleblowing Identity	8.1	The extent in which the possibility of reporting wrongdoing on an anonymous basis given to whistleblowers.	Volosova N.Y. & Zhurkina O.V. 2018; Hassink H, 2007	yes
			8.2	The extent in which the protection of whistleblower identity ensured throughout all stages of the investigation process.		yes
			8.3	The extent in which the availability of policy that gives full protection whistleblowers who have disclosed information anonymously and who subsequently have been identified without their explicit consent.	Hassink et al., 2007; Kaplan et al, 2012	
			8.3	The extent in which full protection shall be granted to whistleblowers who have disclosed information anonymously and who subsequently have been identified without their explicit consent.	Kaplan et al, 2012; OECD, 2014	
			8.4	The extent in which whistleblower identity is identified without their explicit consent.	TI, 2018	
			8.5	The extent to which identity of the whistleblower is disclosed without the individual's explicit consent.	Al-Haidar, 2017; Hassink H, 2007	
			8.6	The extent in which the number of illegal harassment happened to whistleblowers per period.	OECD,2017;TI,2013	

			8.7	The extent in which the amount of personal data stored and the number of third parties who might access this data without whistleblower consent.		yes
			8.8	The extents in which the availability of an anonymous channels which allows protection of free speech.	Lewis D., 2003	yes
			8.9	The extent in which the number against illegal harassment due to whistleblowing is decreased.		
	Burdon of Proof	Protection against any measures taken to whistleblowers were in no sense connected with, or motivated by, a whistleblower’s disclosure.	9.1	The extent in which the number of cases of whistleblowers harassment or any measure due to a whistleblower’s disclosure.	Uganda, 2010; Al-Haidar, 2017	yes
			9.2	The number of cases reported any measures taken to the detriment of the whistleblower were motivated by latter’s disclosure other than the reasons.	Al-Haidar, 2017; OECD, 2014; Chordiya R. et al.,2019	yes
			9.3	The extent to which the number of cases of whistleblowers harassment or any measure due to a whistleblower’s disclosure were returned.)	Chordiya R. et al.,2019; TI, 2016;OECD,2017	
	Criminal and Civil liability (Personal Protection)	Protection of whistleblowers and his family by laws from disciplinary laws - Protection against court action	10.1	The number of whistleblowers charged by criminal, civil and administrative laws even though their disclosure was made within the scope of whistleblower legislation.	De Maria 2008; Chordiya R. et al.,2019;OECD 2014	
			10.2	The number of cases (reports) where whistleblowers whose lives or safety is in jeopardy even though disclosure is made within the scope of whistleblower legislation.	De Maria 2008;TI,2016	
			10.3	The extent to which the number of cases (reports) where whistleblowers family members lives or safety is in jeopardy.		
			10.4	The number of whistleblowers charged by criminal, civil and administrative laws due to reports by whistleblowers where they knew that the information contained in the disclosures is false and the disclosure was made with malicious intent.	Lewis D., 2003, Canada, 2007	

6.4. Digital Government Contribution on Performance of whistleblowing

The whistleblowing system is now considered ass main key element of sound corporate governance (Libit, Freier & Draney, 2014; Brevini, 2017). This needs a fair and transparent process to enable the whistleblowing system to protect organization or business, the whistleblower and any the actors affected. However, Whistleblowing channel works effectively when all employees can use it without fear of retaliation or persecution for blowing the whistle on wrongdoing. Digital Government playing a key role in enhancing whistleblowers' information dissemination mechanisms, protecting reporting channels, anonymous technology and the burden of proof through digital records. This is Digital Government applications result from contextual, institutional, and organizational characteristics from each locality (Hoetker, 2002; Gil-Garcia, 2012; Luna-Reyes et al., 2014).

Based on our case study analysis digitally-enabled whistleblowing initiatives provides better capability to protected whistleblowers through anonyms and confidential secured communication through advanced digital technologies and easily accessible reporting channels 24x7 a week which makes the service delivery to automate and increased public participation in whistleblowing process, and government/organization electronic whistleblowing portals can be used to publish basic information, and this systems can be used to create and follow-up on specific requests. The opening of government data encourages information sharing between the staff of the organization thus enabling the re-use and exploitation of data to create public value (Kalampokis, Tambouris, & Tarabanis, 2011). This helps to build confidence in public institutions through effective procedures for the disclosure of wrongdoings and for protecting public servants who disclose wrongdoings. Above all, Digital Government whistleblowing initiatives created a space for interaction between the user (employees, citizens, businesses, etc.) and the government /organizations. Generally, Digital Government technology has the ability to increase efficiencies and reduce cost in government operations and improve transparency and accountability of the public sector (Gil-Garcia & Helbig, 2007).

The general Digital Government impact model in the whistleblowing process is depicted in Figure 6.4. However, digital-enabled whistleblowing channels – electronic platforms, emails, and hotlines – alone cannot change the employee's initiation/motivation to blow the whistle whenever they see irregular activities. Lack of trust in the ability or willingness of the relevant body to investigate the case and to hold the responsible person to account is one of the key factors in deterring potential whistleblowers from disclosing information. Efficient reporting channels should be backed by follow-up mechanisms. Whistleblowing authority or employer leadership is required to establish such mechanisms in all sized organizations ranging from public bodies to companies and non-profit organizations. It is very important for an organization to have a standard legal recourse or equal application of procedures once information is received. Our case study finding shows that electronic platforms help to achieve follow-up whistleblowing activities through notification message to whistleblowing authorities when there is a new arrival whistleblowing report. In a general description, the analysis shows that the impact of Digital Government on the whistleblowing domain includes more effective information dissemination and exchange, better and more efficient service delivery, and increased public participation in public decision making.

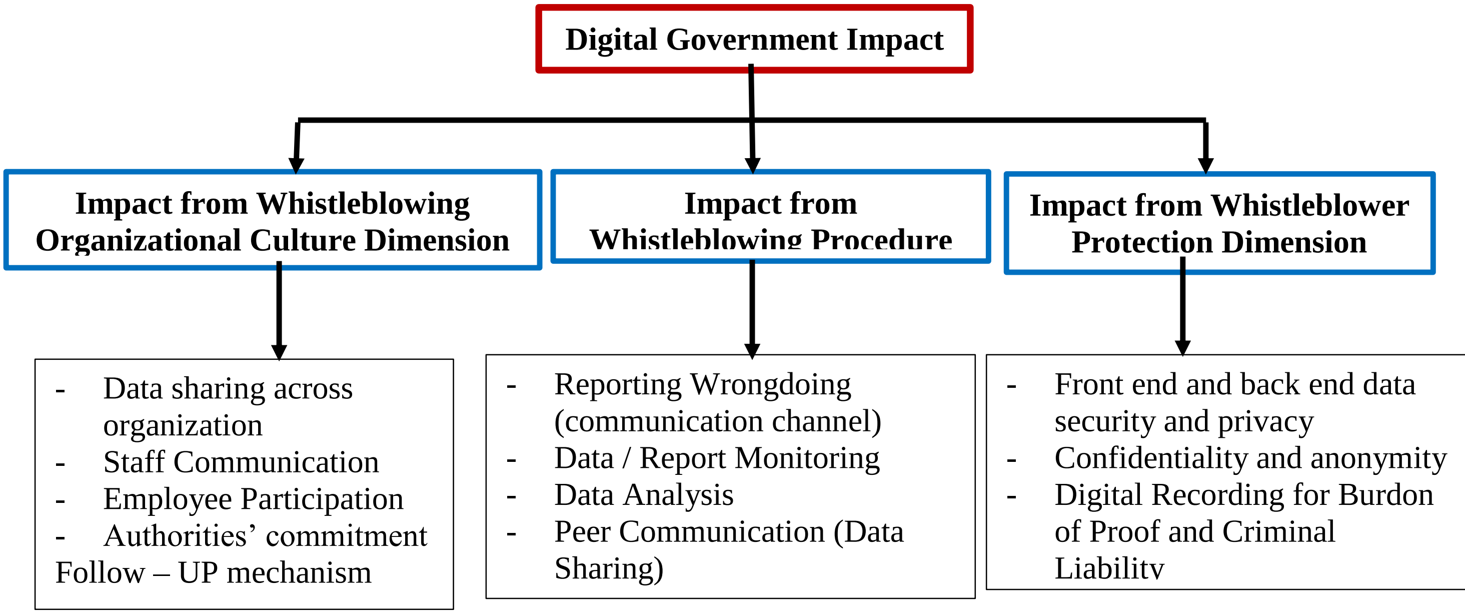

Digital Government Impact
Impact from Whistleblowing Organizational Culture Dimension
Impact from Whistleblowing Procedure
Impact from Whistleblower Protection Dimension
- Data sharing across organization
- Staff Communication
- Employee Participation
- Authorities' commitment Follow – UP mechanism
- Reporting Wrongdoing (communication channel)
- Data / Report Monitoring
- Data Analysis
- Peer Communication (Data Sharing)
- Front end and back end data security and privacy
- Confidentiality and anonymity
- Digital Recording for Burdon of Proof and Criminal Liability

Figure 6. 4: Digital Government Impact whistleblowing Measurement Model

Digitizing a government needs to have attention to two major considerations in the whistleblowing domain. I) digitization efforts including the methods and tools they use to provide whistleblowing services, the whistleblowing processes they implement (Digitizing processes), their approach to making decisions –through advanced analytics systems, and their sharing and publishing of useful data using digital tools. II) Accelerators of digital whistleblowing digital initiatives in government including organizational whistleblowing strategy; governance system; organizational leadership and culture. For example, Leadership commitment is the key in the whistleblowing process which involves engaging in the planning and implementation of digital initiatives by taking charge of decisions, reinforcing framework and the process through frequent communications, and closely monitoring the progress of whistleblowing digital initiatives toward established goals.

The result of the case study analysis shows that Digital Government can contribute to all the three dimensions of the whistleblowing process. Table 6.4 presents the correlation of case studies with the indicators for each variable from the performance measurement framework.

Table 6. 4: Correlation of case studies with the indicators for each variable

Case Number	Variable Number	Indicator No	Variable Number	Indicator No
1	1	1.1, 1.2, 1.3, 1.4, 1.5, 1.6, 1.7, 18	6	6.1, 6.2, 6.3
	2	2.1, 2.2, 2.4, 2.5, 2.6, 2.8	7	NA
	3	All from 3.1 - 3.26	8	8.1, 8.2, 8.7, 8.8
	4	4.1, 4.2, 4.4, 4.9, 4.10, 4.11, 4.14, 4.22	9	9.1, 9.2
	5	5.2, 5.3, 5.4	10	NA
2	1	1.1, 1.2, 1.3, 1.5, 1.6, 1.7, 18	6	NA
	2	2.1, 2.2, 2.4, 2.6, 2.8	7	NA
	3	NA	8	8.1, 8.2, 8.7, 8.8
	4	4.1, 4.2, 4.4, 4.9, 4.10, 4.11, 4.14, 4.22	9	9.1, 9.2
	5	5.2, 5.3, 5.4	10	NA
3	1	1.1, 1.2, 1.3, 1.4, 1.5, 1.6, 1.7, 18	6	NA
	2	2.1, 2.2, 2.4, 2.6, 2.7, 2.8	7	NA
	3	NA	8	8.1, 8.2, 8.7, 8.8

	4	4.1, 4.2, 4.4, 4.9, 4.10, 4.11, 4.14, 4.22	9	9.1, 9.2
	5	5.2, 5.3, 5.4	10	NA
4	1	1.1, 1.2, 1.3, 1.5, 1.6, 1.7, 18	6	NA
	2	2.1, 2.2, 2.4, 2.6, 2.8	7	NA
	3	NA	8	8.1, 8.2, 8.7, 8.8
	4	4.1, 4.2, 4.4, 4.9, 4.10, 4.11, 4.14, 4.22	9	9.1, 9.2
	5	5.2, 5.3, 5.4	10	NA

The Digital Government impacts areas in the whistleblowing domain and their relationships are shown in the simplified model below (Figure 6.5).

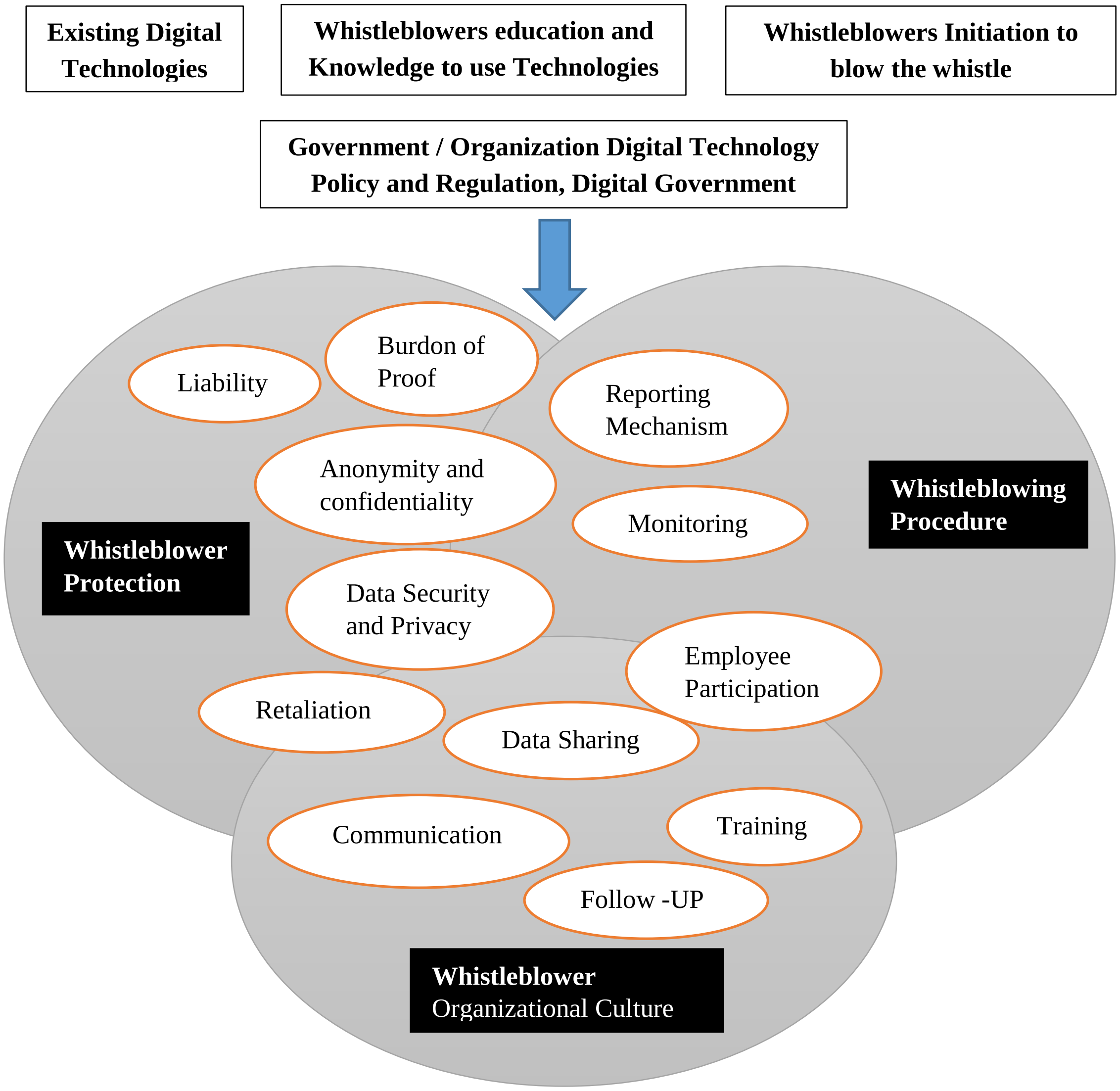

Existing Digital Technologies
Whistleblowers education and Knowledge to use Technologies
Whistleblowers Initiation to blow the whistle
Government / Organization Digital Technology Policy and Regulation, Digital Government
Liability
Burdon of Proof
Reporting Mechanism
Anonymity and confidentiality
Monitoring
Whistleblowing Procedure
Whistleblower Protection
Data Security and Privacy
Employee Participation
Retaliation
Data Sharing
Communication
Training
Follow -UP
Whistleblower Organizational Culture

Figure 6. 5: Digital Government impact relationship on whistleblowing (Positive and Negative)

The model indicates the web of relationships between impact areas and with the broader whistleblower procedure, whistleblower protection, and organizational culture. Impacts of Digital Government on whistleblowing and whistleblower protection arise through Digital Technologies supply and Digital Technologies demand is likely to be influenced by the following factors: i) Existing digital technologies infrastructure, which enables digital technologies critical mass that can amplify impacts; ii) whistleblowers level of education and knowledge; iii) Whistleblowers Initiation to blow the whistle; and iv) Government digital technology policy and regulation.

6.4.1. Impact of Digital Government on Whistleblowing Procedure Performance

Study indicates that organizations need to provide an opportunity for the whistleblowers to choose between different reporting channels – including independent external options. The availability of multiple channels enables employees to select the person with whom they are most comfortable sharing sensitive information, and the channel they find easiest to use.

The nature of whistle-blowing has become transformed by technological advances in the online environment through the use of digital technology which enables to create a new platform that instantaneously transmitting information across the globe (Brown et al., 2014). It was common to report any whistle-blowing occurred internally via channels within the organization or externally via the news media or government agencies officially dedicated to whistle-blowing. However, with the surge of technology whistleblowing via social media or online sources has become increasingly common given the associated benefits of speed, anonymity and/or impact.

Our finding shows that Case Management Tool has been used to manage the reported cases including recording, investigating and monitoring reports. In addition, it also provides notifications, analysis and reporting management for each reported cases and whistleblowers can track their reports and tasks. 2/4 of the case studies used Case Management Tool and it enables to communicate whistleblowers at every stage of the whistleblowing process. This capability enables the active participation of employees in the whistleblowing process.

However, with the large quantity of information received by electronic whistleblowing platforms and hotlines create needs to have a sophisticated system for the vetting process. For example in the literature by OECD, In Hungary, a special witness hotline receives 10,000 calls in 2008 alone and Latvia’s State Labour Inspectorate hotline receives 200 anonymous voice messages in two years - 2007 and 2008. It was identified that the biggest challenge in hotline is difficulties to get additional data for further processing in some cases when it required.

6.4.2. Impact of Digital Government on Whistleblower Protection Performance

6.4.2.1. Anonymous and Confidential Reporting

On the traditional whistleblowing procedure, providing the right degree of confidentiality or even anonymity to the whistleblower considered to be the major challenge for reporting channels to work efficiently. Our case studies – PPLAAF, XNET, and WildLeaks uses TOR technologies (tor browser) for their electronic platform to provide anonymous communication which provides a file of information sent without a return address and Tor guaranteeing anonymity and preventing back contacts. Anonymous hotlines also provide an untraceable telephone call to a hotline. Our case studies VAL provides confidential communication through Encrypt the message where employee /whistleblower is known only by the recipient of the disclosure – organizational ombudsman - who has an obligation to keep the name secret, both towards members of the concerned organization and to the wider public. Our finding shows that each whistleblowing electronic platforms not only provide secured discourse but also data security through encryption mechanism. Data security is another very important issue to achieve confidentiality. All case studies indicate that only an authorized person can enter into the system and see the reports. Encryption technique is applied to the data at the back end - when they store in the system.

6.4.2.2. Retaliation and Burdon of proof

Retaliation is a critical concern in the whistleblowing process. It can hinder whistleblowers to make disclosure due to fear of retaliation. Organizations /Governments need to establish safeguards against workplace reprisals which are easy for the whistleblower to access. There must be a way to encourage the conveying of the message while protecting the messenger 41 and to guarantee that the individual (and his or her family) will be protected from retribution. Without protection, the cost of reporting may be too high for individuals to come forward. Electronic platforms provide an easy way of reporting mechanisms for any form of retaliation against whistleblowers.

In our case studies - all electronic whistleblowing platforms provide digital records - including the time and place where the disclosure is made - in both written and oral disclosure which helps as the burden of proof. In some cases where retaliation against whistleblowers, the burden of proof should be reversed. It should be proven by the accused that any measures taken to the detriment of the whistleblower were motivated by reasons other than the latter's disclosure.

6.4.3. Impact of Digital Government on Whistleblowing Organizational Culture Performance

Semsudin and Ujkanovic (2011) state that information organization enables to remove of unnecessary levels of coordination within an organization which leads to a considerable increase in effectiveness. Digital technologies play a vital role in transforming organizational culture from the organizing and dissemination of digital information. They stated that the consequences of digital technologies on the organization culture include Transactions, Geographic, Automation, Analytics, Information Decimation, Knowledge and Management, Monitoring tasks and Exchange.

Our finding based on our case studies shows that digitally-enabled whistleblowing electronic platforms help to create an open organizational culture where employees are not only aware of how to report but also have confidence in the reporting procedures. It increases the participation of employees and citizens in the whistleblowing process. Such impacts may occur as a result of greater communication and information dissemination offered by digital technologies, through the use of electronic whistleblowing platforms. Whist blowers /employees are frequently enabled by electronic information and services offered by government and organization (digital-government), usually via the electronic platforms.

This leads employees in an organization to greater engagement in whistleblowing processes through digital platforms. It enables internal and external whistleblowers to interact with regulatory bodies or media through online tools, participate in online whistleblowing campaigns, express themselves online confidentially, and share information and culture anonymously. All our cases indicate that whistleblowers can effectively deliver information on how to get Media and legal assistant; how to connect to credible investigative partners and how to approach journalists. One of our case studies - Wildleak – provides whistleblowing information's through 16 different languages which help to get a report in a wider-angle.

Technological determinism in an organization considers technology as a powerful tool that can transform social structures (Hoetker, 2002; Leavitt & Whisler, 1958; Orlikowski, 1992; Smith & Marx, 1994) and technology is the main actor in the transformation process. Our case study finding shows that Digital Government implies that digital technology applications, such as government/ organizational whistleblowing electronic portals, have an effect on creating new forms of interaction between citizens and government or changing work practices or organizational structures in fighting against wrongdoing activities within an organization. This electronic portal helps to provide awareness-raising, strengthening communication and training. It enhancing whistleblowers' information dissemination mechanisms and ease the communication between the partners /colleagues before and after whistleblowing; between whistleblowing authority and whistleblower. In addition, all four case studies studied in this research provides online training on how to use the whistleblowing channel to all interested whistleblowers.

However, digital-enabled whistleblowing channels – electronic platforms, emails, and hotlines – alone cannot change the employee's initiation/motivation to blow the whistle whenever they see irregular activities. Lack of trust in the ability or willingness of the relevant body to investigate the case and to hold the responsible to account is one of the key factors in deterring potential whistleblowers from disclosing information. Efficient reporting channels should be backed by follow-up mechanisms. Whistleblowing authority or employer leadership is required to establish such mechanisms in all sized organizations ranging from public bodies to companies and non-profit organizations. It is very important for an organization to have a standard legal recourse or equal application of procedures once information is received. Our case study finding shows that electronic platforms help to achieve follow-up whistleblowing activities through notification message to whistleblowing authorities when there is a new arrival whistleblowing report.

6.5. Digital Government Cause-Effect framework for whistleblowing

All stakeholders in whistleblowing and whistleblower protection – Public authorities in an organization; non-governmental organizations acting on to defend whistleblowers through the courts and in the public arena as it could, and providing funds for different projects and researches in the area of whistleblowing; whistleblowers; organizational employees and citizens; and media – plays a crucial role in the domain of whistleblowing. Considering the importance of whistleblowing in detecting fraudulent activities within an organization, it is required to have coordination and collaborations among all stakeholders (Amadi, Carrillo & Tuuli, 2014). Sometimes the interactions between stakeholders often pose conflicts of interest or need to be strictly regulated in order to ensure fair play and protection of rights and responsibilities between entities. Managing the impact of whistleblowing program on the organizations requires policy-level decisions and coordination and collaboration among stakeholders. These decisions involve typical tasks for sector-specific public governance. Nevertheless, due to the widespread adoption of digital technologies, these interactions and generally the performance of public governance in the whistleblowing domain have changed considerably in recent years. As a result, Digital Government has become an important tool in the governance of the whistleblowing domain.

As presented in the earlier sections, Digital Government multi-stakeholder analysis for the whistleblowing domain may help to address the challenges described in the introduction. This includes the new business model and legal framework created by the implementation of digital technologies in the whistleblowing domain that must be regulated while the development of such regulations requires the clear identification of various stakeholders and analysis of their interactions. Whistleblowing services in the digital world requires that whistleblowing service providers must confirm transparency and accountability in their operations to enable public authorities and whistleblowers to exercise their role and responsibility. In addition, legal regulation and transparency are required to ensure whistleblowers and public authorities to exercise prepare care with respect to the use private data's, while the regulatory authorities act on information they receive and protect those who provide it, and that wider disclosures, to the media for example, are protected when necessary. Besides, through clear governance principles, stakeholder participation and transparency, the entire whistleblowing program and its participants must ensure that whistleblowers data and privacy are protected. As the opportunities for public disclosures, particularly to the media and public interest groups, are increasing with new technology, all stakeholders need to work to protecting whistleblowing in the public interest.

Due to the substantial improvements of digital technologies and their widespread adoption cross different organizations, the overall public governance structure in whistleblowing and whistleblower protection is fundamentally changed including accessibility of reporting channels for 7/24/365 and privacy protections. This shows that Digital Government is important tool in the governance and plays its crucial role in the whistleblowing and whistleblower protection.

As stated previously, research in the area includes technology-driven innovations in service delivery, such as the use of Data Compression, Cloud Computing, Big Data and Network Monitoring to improve the quality of public service provision (Yang et. al., 2017). Due to the adoption of this technologies, whistleblowing and whistleblower protection is leading in the innovation of electronic public service delivery. However, assurance of data integration and interoperability to deliver complex whistleblowing services should get a research considerations in the future. This types of problems can be enclosed within the contextualization stage of the Digital Government evolution (Janowski, 2015).

Considering Janowski (2015), the Digital Government analysis cause-effect framework for whistleblowing and whistleblower protection is depicted in Figure 6.6. Elements of the framework are obtained from the related work on Digital Government and whistleblowing and whistleblower protection in chapter 4 (Table 4.4) and from the Digital Government stakeholder analysis for whistleblowing and whistleblower protection on chapter 5 section 5.1.4. This cause-effect analysis framework is populated with public authorities within the governments organizations are under pressure on managing whistleblowing and whistleblower protection including creating free reporting channels protected where disclosures can be made and accessible for 7/24/365; Description of Digital Technologies available at the time in order to respond to such pressures; how the public authorities respond to such pressures in using available digital technologies and then the ways that these technological innovations are institutionalized in the organization.

DIGITAL TECHNOLOGIES	
Internet	Portable computing devices
Intranet	**Recommender systems**
Hotlines	Data-sharing
Web Pages (online plat forms)	Social networks / social media
SMS	Websites
Email	Information exchange
Mobile Platform	Surveillance systems
Network monitoring	Data compression
Data process	Big-data
Mobile phone	Data center
Data encryption	Case management System
Digital fingerprinting	Survey System
Data Surveillance	Intrusion Detection System IDS
Digital fingerprinting	Telephone
Cloud Computing	Mobile Apps

PRESSURE ON PUBLIC AUTHORITIES IN WHISTLEBLOWING AND WHISTLEBLOWER PROTECTION
Free Reporting channels accessible for 7/24/365
Free reporting channels protected where disclosures can be made
Privacy protection of whistleblowers personal information
Protect whistleblowers from retaliation
Promoting whistleblowing on wrongdoing activities
Providing a secure access for recording, investigating and monitoring whistleblowing reports
Providing equity in all whistleblowing stakeholders
Accommodate clear accountability for all stages in the whistleblowing process

DIGITAL GOVERNMENT INNOVATIONS	
Public Internet for whistleblowers	Email based whistleblowing service
International, National, local and organizational whistleblowing portals	Hotlines/telephone based whistleblowing service
Case management System for whistleblowing service	Online whistleblower feedback
BaFin website as platform	Anonymous online portal
Whistleblowing statistics dashboard	Secure platform BKMS System
Online training for whistleblowing Service	Confidential encryption and data retention
SMS based whistleblowing service	EDF's information systems
Data exchanges and sharing of information related to whistleblowing reports	Tor anonymity and privacy Technology
Digital whistleblowing service	e- confidential advice service
Chase Information Technology Services (Chase ITS system)	Programmed portable digital technology / personal digital assistant (PDA) system
Online whistleblower protection campaign	Online whistleblowing campaign
Anonymous Survey System	ZIP compression Technique
Social Media platforms for mass dissemination of information	Online publishing technology
Mass eavesdropping technologies	Security and privacy technologies
Using open source software	Strong cryptography - encryption and security technologies

DIGITAL GOVERNMENT INSTITUTIONALIZATION
Smart whistleblowing System
Accessible and accountable whistleblowing system
Anonymous and confidential whistleblowing Service
Sustainable whistleblowing and whistleblowing system
Smart Civil society organizations to defend whistleblowers

Figure 6. 6: Digital Government Innovation Cause-Effect Framework adopted for Whistleblowing Domain (Adopted from Janowski 2015)

6.6. Validation of the Measurement Scales for TAM Model

In order to validate our measurement model, the researcher have undertaken content validity assessments, internal consistency, items' loadings, discriminate, and convergent validity. The content of this survey was based on existing literature and our measurements were built by the adoption of constructs validated by other researchers. Pre-tests were carried out with professionals in the field of Digital Government whistleblowing system in Ethiopia. The final set of 30 items of the questionnaire was selected. Cronbach's Alpha (Cronbach, 1951), Composite Reliability and item loadings and Average Extracted Variances (AVE) (Fornell & Larcker, 1981) were used to measure internal consistency reliability and reliability of indicators, all exceeding the required reliability and uni-dimensionality criteria.

$$\alpha = \frac{N \cdot \bar{c}}{\bar{v} + (N-1) \cdot \bar{c}} \qquad (1)$$

Where: N = the number of items, c̄ = average covariance between item-pairs, and v̄ = average variance.

$$\frac{\left(\sum_{i=1}^{p} \lambda_i\right)^2}{\left(\sum_{i=1}^{p} \lambda_i\right)^2 + \sum_{i}^{p} \mathrm{V}(\delta)} \qquad (2)$$

Where: λi = completely standardized loading for the ith indicator, V(δi) = variance of the error term for the ith indicator, and p = number of indicators.

$$\mathrm{AVE} = \frac{\sum_{i=1}^{k} \lambda_i^2}{\sum_{i=1}^{k} \lambda_i^2 + \sum_{i=1}^{k} \mathrm{Var}(e_i)} \qquad (3)$$

Here, k is the number of items, λi the factor loading of item i and Var(ei)the variance of the error of item i.

The computed values (equation (1, 2, and 3)) through SPSS are shown in Table 6.5. Table 6.6 provides evidence of the discriminant validity of the item scales used in this study. In all cases, the bolded items in the matrix diagonals, representing the square roots of the AVEs, are larger than the off-diagonal elements in their corresponding row and column, which support the discriminant validity of the item scales.

When AVE is greater than 0.5 of the total variances, convergent validity is defined, according to (Fornell & Larcker, 1981), and the convergent validity of all six Digital

Government whistleblowing factors that the researcher used is verified. Our AVE values ranged from 0.664 to 0.874, over the required threshold, as shown in Table 6.5. Additionally, a common rule of thumb to indicate convergent validity is that all items should load greater than 0.7 on their own construct, and should load more highly on their respective construct than on the other constructs.

Table 6. 5: Discriminant Validity (Inter-Correlations) of the Item Scales

	SN	WSQ	IQ	PU	PEU	ATT	BI
SN	**0.881**						
WSQ	0.518	**0.934**					
IQ	0.660	0.691	**0.933**				
PU	0.434	0.752	0.616	**0.814**			
PEU	0.705	0.652	0.910	0.595	**0.926**		
ATT	0.690	0.822	0.915	0.620	0.812	**0.919**	
BI	0.721	0.830	0.866	0.631	0.868	0.904	**0.925**

Table 6. 6: Descriptive Statistics of the Constructs.

Measurement	Items	Loading	Mean	Std. Deviation	Cronbach's Alpha	Composite Reliability	AVE
ATT	ATT1	.914	3.106	1.298	0.983	0.942	0.846
	ATT2	.920					
	ATT3	.925					
PU	PU1	.817	3.41	1.446	0.893	0.854	0.664
	PU2	.711					
	PU3	.906					
PEU	PEU1	.945	2.981	1.213	0.987	0.947	0.858
	PEU2	.945					
	PEU3	.889					
WSQ	WSQ1	.943	3.436	1.449	0.852	0.984	0.874
	WSQ2	.942					
	WSQ3	.955					
	WSQ4	.949					
	WSQ5	.952					
	WSQ6	.851					
	WSQ7	.959					
	WSQ8	.943					

	WSQ9	.914					
IQ	IQ1	.952	2.899	1.19293	0.985	0.971	0.871
	IQ2	.881					
	IQ3	.936					
	IQ4	.942					
	IQ5	.955					
SN	SN1	.889	3.259	1.476	0.833	0.912	0.777
	SN2	.862					
	SN3	.895					
BI	BI1	.924	3.366	1.369	0.973	0.959	0.856
	BI2	.938					
	BI3	.916					
	BI4	.923					

6.7. The Structure Model

The structural model mainly involves Estimates for path coefficients (β), Determination of coefficient (R2), and Estimates for total effects (Chin, 1998). The assessment of the structural model was done using linear regression and individual path coefficients (β) of the structural model interpreted as standardized beta coefficients. According to Urbach and Ahlemann (2010), Path coefficients should exceed .100 to account for a certain impact within the structural model. Furthermore, path coefficients should be significant at least at the .050 level (Henseler, Ringle & Sinkovics, 2009; Urbach & Ahlemann, 2010). Figure 6.7 shows the structural model results through SPSS. All beta path coefficients (β) are positive (i.e. in the expected direction) and statistically significant (at $p < 0.05$).

Considering purpose of structural model's is to test the relationships between hypothetical constructs, coefficient of determination (R2) of each construct plays the major role. Researches (Chin, 1998; Urbach & Ahlemann, 2010) indicates that R2 values should be high enough to provide the model with a minimum level of explanatory power.

Chin in 1998 finds R2 values of around 0.67, 0.33, and 0.19 respectively to be substantial, moderate and weak. Figure 3 displays the R2 values of this analysis. Perceived usefulness scores value of R2= 0.586, Perceived ease of use scores value of R2= 0.501, Attitude scores value of R2= 0.841 and behavioural intention scores value of R2= 0.904.

Table 6.7 displays the total effects on the four predicted constructs based on their Estimates for path coefficients (β).

Table 6. 7: Structural Model Effects of the Four Constructs

	PU	PEU	ATT	BI
SN	-0.050	0.111	0.045	0.13
WSQ	0.644	-0.075	0.485	0.259
IQ	-0.057	0.946	0.070	-0.168
PU		0.007	-0.158	-0.032
PEU	0.251		0.589	0.239
ATT				0.552

As shown in the above Table (Table 6.7), ATT (0.552) is the greatest effect on the intention to use Digital Government whistleblowing system. The highest ATT effect is PEU (0.589) followed by WSQ (0.485). Besides, WSQ also has a strong effect on both PU and BI (0.644 and 0.259) respectively, and IQ provides the strong effect on PEU with value of 0.946.

6.8. Hypothesis Testing

This study is primarily aimed at evaluating the TAM Model in the context of Digital Government whistleblowing system implementation in Ethiopia. The extended TAM model's empirical evaluations were able to pinpoint constructs that would determine the intention to adopt Digital Government whistleblowing system. In predicting the intention of citizens to use Digital Government whistleblowing system, many adoption factors, such as attitudes towards using Digital Government whistleblowing system, are important. Figure 6.7 depicts the adoption factors for using Digital Government whistleblowing system. All the hypotheses of the analysis have been identified and verified with the findings. The hypotheses and findings are listed in Table 6.8.

Hypotheses 1 examines the relation between “Subjective Norm” to “Perceived Ease of Use“. Subjective Norm is strongly related to Perceived Ease of Use of citizen's in using Digital Government whistleblowing systems (β=0.104; Pb=0.000). Therefore, hypotheses 1 are supported.

Hypotheses 2, 3, 4 and 5 explores the impact of “Subjective Norm”, “whistleblowing system quality”, “Information Quality” and “Perceived Ease of Use” on “Perceived usefulness” to use the Digital Government whistleblowing systems. It is observed that Subjective Norm, Information Quality and Perceived Ease of Use had no significant impact on Perceived usefulness toward using e-Government at the 0.217, 0.710 and 0.141 significance levels, respectively.

However, “whistleblowing system quality” has a significant impact on Perceived usefulness (β=0.366; Pb=0.000). The greater the Ethiopian government willingness to emphasize on “whistleblowing system quality” the greater will be influenced citizen's perceived usefulness on Digital Government whistleblowing systems. As a result, Hypotheses 2, 4 and 5 are not supported, while Hypotheses 3 is supported.

Hypotheses 6 and 7 examined the impact of “perceived ease of use” and “perceived usefulness” on “attitude” to use digital enabled whistleblowing system. The study shows both Perceived usefulness perceived ease of use has a strong impact on attitude at 0.00 significant level. The positive effects of both PEU and PU on the attitude towards using the Digital Government enabled whistleblowing system was verified, as indicated by the original TAM. Hypotheses 6 are supported.

Hypothesis 8 and 10 explores the relation between "attitudes" and “Subjective Norm” to "behavioral intention" use of digitally enabled whistleblowing systems. Both attitude and Subjective norm are closely related to the behavioral intention of people to use digitally enabled whistleblowing systems at (β=0.808; Pb=0.000) and (β=0.133; Pb=0.000) respectively. This finding confirms TAM's argument. Nevertheless, there is no significant effect of "perceived usefulness” on "behavioral intention" (β=0.133; Pb=1.28). Hypothesis 9 is therefore not supported.

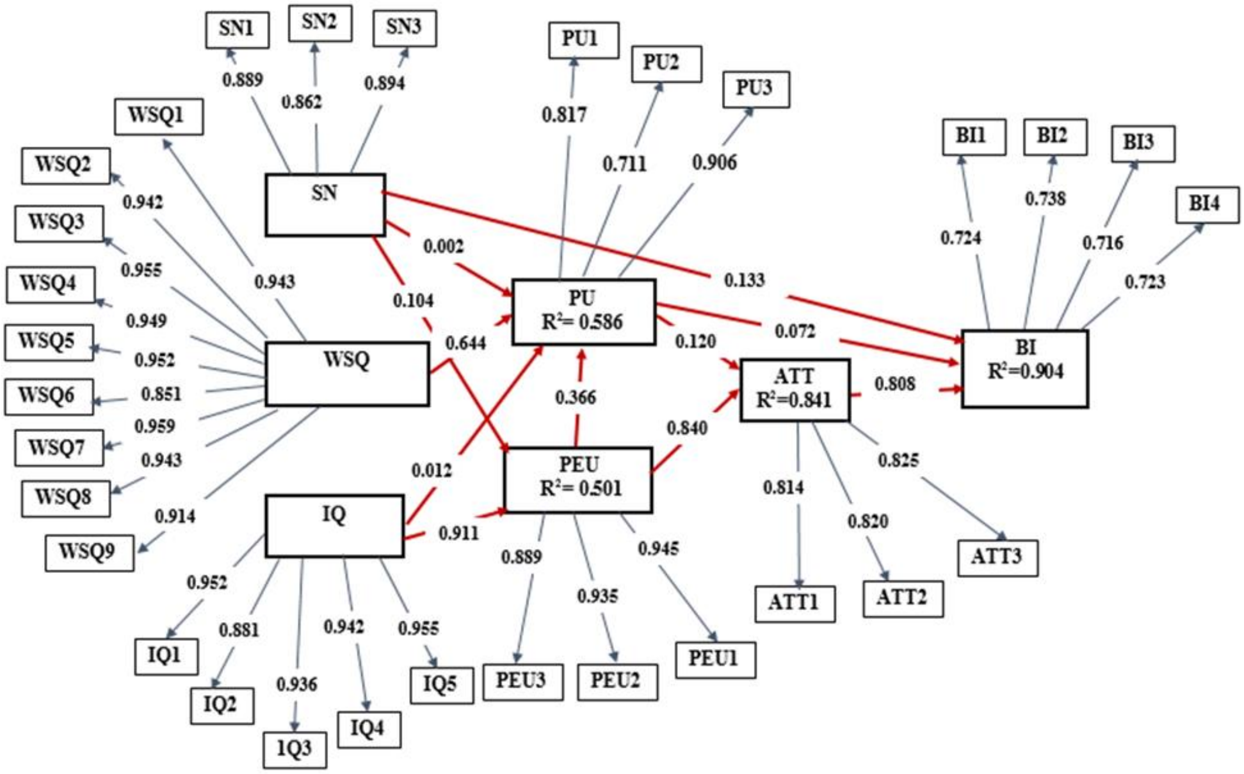


Figure 6. 7: Research Model - Model of TAM in Digital Government whistleblowing system adoption

Table 6. 8: Summary of Hypotheses Testing

Hypothesis	Relationship	T- Value	P-Value	Results
H1	SN ➞ PEU	10.866	0.000	Supported
H2	SN ➞ PU	-1.237	0.217	Not Supported
H3	WSQ ➞ PU	16.337	0.000	Supported
H4	IQ ➞ PU	-0.372	0.710	Not Supported
H5	PEU ➞ PU	1.731	0.141	Not Supported
H6	PEU ➞ ATT	9.505	0.000	Supported
H7	PU ➞ ATT	-9.163	0.000	Not Supported
H8	ATT ➞ BI	11.417	0.000	Supported
H9	PU ➞ BI	-1.526	0.128	Not Supported
H10	SN ➞ BI	6.978	0.000	Supported

With countries in the world deploying different types of Digital Government whistleblowing system initiatives with the hope to achieve an advanced level of digitally enabled whistleblowing services and enhance the good governance by combating fraudulent activities within the organization and increasing citizen participation in unveiling misconducts and accessibility of whistleblowing services to citizens/employees. According to [31], the effectiveness of Digital Government initiatives success of Digital Government initiatives depends not only on the support of the government but also on the ability of people to embrace and implement whistleblowing services.

The results of this study show that TAM's key concepts have a significant influence on citizen intentions to use Digital Government whistleblowing systems. Our empirical results indicate that in the Ethiopian Digital Government whistleblowing systems, WSQ has a positive influence on the PU. Additionally, PEU has a significant impact on the citizen's attitudes to use Digital Government whistleblowing systems. While, attitudes towards the use of Digital Government whistleblowing systems have a major impact on the behavioral intentions of Ethiopian people. In line with previous TAM studies, the key TAM constructs including perceived usefulness, perceived ease of use, attitude towards using, and behavioral intention have a major and influential impact on Ethiopian intention to use Digital Government whistleblowing systems.

The findings, however, do not support the H2, H4, H5, H7 and H9 hypotheses. The perceived usefulness of Ethiopia has a poor relationship with Attitudes and Behavior Intentions. This might be attributed to the incoherent and unreliable nature of electricity and the internet in Ethiopia compared to the Developed world. A factor in failed Digital Government whistleblowing initiatives is Ethiopia's poor government infrastructure including electricity and ICT. Ethiopians find it difficult to access government whistleblowing information’s through Digital Government whistleblowing system resources. In certain situations, due to slow internet service, Ethiopians have to wait hours for browsers to connect to a particular website.

Because of problems with internet connections, many Ethiopians tend to use conventional methods to process whistleblowing activities rather than Digital Government whistleblowing systems. Perceived usefulness in developing countries with inconvenient IT infrastructure has no big impact on behavioral intentions and attitudes. The Ethiopian government should implement management systems and web portals on their sites to enhance the perception of Ethiopia's Digital Government whistleblowing systems. Accessibility to information is difficult and users often feel obliged to access Digital Government whistleblowing systems online.

Additionally, Subjective Norm, Information Quality and Perceived Ease of Use have week linkage with perceived usefulness H2, H4, H5. This is because the citizens in Ethiopia is much relying on the security of the whistleblowing system. Mostly the citizens prefer not to "speak up" the unlawful misconducts due to unreliability of the systems and lack of trust from the government whether the whistled information will be used for further investigation by the government. This study reveals that the government of Ethiopia should work to the transparency and accountability on the investigation of whistled information to build the trust of its citizens. Additionally, this study shows that Ethiopian Digital Government whistleblowing system available online does not provide the information required by Ethiopians and some government web portals are not in place properly. Access to information is difficult, and people are reluctant to use Digital Government whistleblowing system.

6.9. Summary

Performance measurement framework for whistleblowing and Digital Government Cause-Effect framework for whistleblowing domain has been developed in this chapter. The impact of Digital Government on whistleblowing performance has been evaluated through the case studies developed in chapter 5. Additionally, the Digital Government analysis cause-effect framework for whistleblowing and whistleblower protection. Elements of the framework are obtained from the related work on Digital Government and whistleblowing and whistleblower protection in section 4.1 and from the Digital Government stakeholder analysis for whistleblowing and whistleblower protection in section 5.1.4.

CHAPTER VII

CONCLUSIONS AND RECOMMENDATIONS

7.0. Introduction

This chapter is aimed at concluding the current research. A summary of the research is given in the next section and provides an extensive explanation of the entire research of the aim of the methodology, analyses, results and interpretation of the findings. This chapter is dived in to six sections. The first section provides an overview of the research. Discussions based on the accomplishment of the research aim and research questions are in the second and third section respectively. The fourth section provides the key contributions of this research towards the advancement of relevant theories and practices, mainly to knowledge, method and practice. Furthermore, the implications of the findings on the development of Digital Government whistleblowing initiatives in Ethiopia are also presented. The sixth section provides some of the research limitations of the study and suggestions for further research are presented in order to identify potential areas that could be valuable in the seventh section. Finally, a summary which concludes the chapter is presented in the eighth section.

7.1. An Overview of the Research

In today's digital world, The advent of digital technologies from cloud computing to mobile to analytics, is fundamentally transforming both public and private sector organizations operates (Deloitte, 2015) and it has been an important enabling tool for reform (Katsonis, 2015). Researchers explore that Digital Technologies have the potential to significantly transform how governments perform their functions and relate to citizens, businesses, and other governments (Hoetker, 2002, 2004; Jaeger & Bertot, 2010; Kraemer & King, 2006; Luna-Reyes & Gil-Garcia, 2011). It has been used to alleviate some of the challenges of whistleblowing and government/organizations around the world started to use different digitally-enabled whistleblowing initiatives. There is a very few research on the possible contribution of technologies in whistleblowing and its side effect but the interaction of the Digital Government and whistleblowing domain is yet to emerge. In addition, there are few researches on digital enabled whistleblowing initiatives adoption but all are focused on developed countries with none of them in developing countries especially in Sub-Saharan African (SSA) countries.

In Ethiopia, there is no any attempt to capture precisely the actual situation of Digital Government adoption/utilization in organizations whistleblowing process based on empirical studies that can provide a good explanation of the existing situation. However, the result of this research provides the comprehensive report on the case of Ethiopia with specifically on health and mining industries. The overall aim of this research has been to investigate the possible contribution of Digital Government in whistleblowing domain and to ascertain factors affecting the adoption and effective utilisation of Digital Government in Ethiopian governmental organizations whistleblowing process.

In this study, key motivators for governmental organizations decisions to adopt Digital Government in their whistleblowing program have been identified. It is intended that the recommendations put forward, based on empirical findings in this research, would help to provide a guide for Ethiopian government organizations to increase their take-up of digitally enabled whistleblowing initiatives. The following section provides an overview of the research findings and outcomes.

7.2. Overview of the Research Findings and Research outcomes

This research plays a key role in investigating the contribution of Digital Government for whistleblowing domain, developing whistleblowing performance measurement framework and analyzing the contributing of Digital Government and ascertain factors affecting the adoption of digitally enabled whistleblowing initiatives among some of government organizations in Ethiopia.

The key objectives of the research was to identify influence of Digital Government on whistleblowing and whistleblower protection and to identify strategies that could assist in resolving the challenges faced by Ethiopian organizations with respect to digital enabled whistleblowing initiatives adoption and utilization.

Reviewing literature in the area Digital Government revealed the lack of strategy that could help in use of Digital Government in whistleblowing process and literatures also lacks a success strategy that could serve as a guide in promoting the adoption and effective utilization of digitally enabled whistleblowing initiatives in developing countries particularly in Ethiopia. The subsequent sections briefly present and discuss the significant findings of each phase of the research, then examine whether the research aim was achieved. The study's academic contribution and implications for practice are also discussed. The last section addresses the limitations of the study and some possible future research directions.

7.3. Contributions of the Research

The contribution of this research is classified in to General Body of Knowledge (Theoretical Contributions), Practical Contributions and Methodological Contributions. Each contribution discussed below.

7.3.1. Theoretical contribution – Contribution to the General Body of Knowledge

This research pioneers an advance in the theoretical account of the Digital Government. It has contributed to the existing body of literature and the field of Digital Government and whistleblowing by identifying the inadequacies of previous studies regarding Digital Government utilization in organizational whistleblowing process in developing countries, with particular emphasis on Ethiopia.

As mentioned before, the previous studies on Digital Government focused on its contribution in the other domain areas in public services including truism, tax and justices. The study goes beyond previous research by extending the application area in the whistleblowing domain. This finding contributes to the more advanced explanations of the Digital Government whistleblowing initiatives as a socio-economic phenomenon. Overall, this research makes four contributions to theory.

Firstly, this research made an important contribution in identifying the potential issues in whistleblowing domain and explores how Digital Government has been used to address these issues. There was no previous study in the literature for the use of Digital Government in whistleblowing domain. This study develops a conceptual framework, exhibiting how DGOV solutions are contributing to WB problems, to show the importance of digitally enabled whistleblowing initiatives. In addition, this research establishes a foundation for further DGOV4WB research.

Secondly, this study also made another contributions in developing Digital Government innovation cause-effect framework for whistleblowing domain. This framework used to populate a Digital Government cause-effect framework that identified pressures on organizational authorities on whistleblowing domain and determined how the public authorities respond to such pressures by innovation in their policies, processes, services and structures using existing digital technologies; and explored how such digital innovations are institutionalized over time. The cause-effect framework enables organizations to raise awareness and educate about the development and use of digital technologies to perform governance functions in the whistleblowing domain. The framework could also help to predict how the whistleblowing governance function is transformed in the process.

Third, this research has also made a novel contribution to the area of Digital Government and whistleblowing as it has identified the main stakeholder stakeholders responsible for whistleblowing process and examines the usage of digital technology by public authorities and other stakeholders as part of governance processes within the whistleblowing domain, which has not been identified in previous researches.

Fourth, this study develops digitally enabled whistleblowing program performance measurement frameworks. Despite the surge in online whistleblowing systems implementations across the world, however, there is no previous research on performance measurement framework to measure the effectiveness of digital technologies enabled whistleblowing system. This is therefore, this research contribute to the study of whistleblowing performance by providing a conceptualization of performance that emphasizes on whistleblowing and whistleblower protection outputs.

Fifth, No previous study had empirically considered how Ethiopian government public organizations utilise digitally enabled whistleblowing systems. There is lack of scholarly articles on the level of utilisation of digitally enabled whistleblowing systems amongst Ethiopian government public organizations. Therefore, this study adds to the existing body of literature and makes specific contributions to the field of application of Digital Government in public services by providing insights on the level of digitally enabled whistleblowing systems utilization amongst Ethiopian government public organizations. It was observed that no previous research had put forward the possible use of Digital Government on whistleblowing process. Hence, this research is considered as one of the pioneer studies in the area, as the study develops a conceptual framework that can assist the use of Digital Government, in whistleblowing domain.

7.3.2. Methodological Contribution

This research again makes a substantial contribution from the research methodology, having established and validated measures relating to the different constructs of the research, including those in the framework. This research is the pioneer in integrating whistleblowing domain (as problem domain) and Digital Government (as solution domain).

The study makes a methodological contribution by using mixed approach to increase the validly of the research findings. The research employed both qualitative and quantitative approaches in order to provide indepth information about the subject. The analysis of data collected involving content and thematic analysis was further used to develop a framework. Many of the previous researcher in Digital Government studying its application were mainly in qualitative research methodology. However, this research used mixed approach to investigate the possible contribution of Digital Government in the whistleblowing domain and to assess the utilization of Digital Government in Ethiopian public organizations through empirical investigation. In other word, this research employs content and thematic analysis for analysing empirical data.

7.3.3. Practical Contribution

The result of this research have important practical implications, particularly in relation to improving digitally enabled whistleblowing initiatives in Ethiopian public organizations. It offered suggestions on how the Ethiopian public organizations use digitally enabled whistleblowing initiatives, which can help to fight unlawful activities and fight against corruption with organizations and expand the country's economy. This research provides a more comprehensive understanding of the issue of the digitally enabled whistleblowing initiatives, as the basis for a new integrative policy for the Ethiopian government to close the gap in a fight against corruption through an integrated whistleblowing initiatives.

7.4. Limitations of the Research

This research has its own limitations as of any other researches. This limitations are discussed below. The first limitation of this research is the fact that the study was limited to few governmental organizations but the researchers believes that although the research was limited to few governmental organizations, nevertheless, some of the research findings are likely to be similar to those in other governmental organization of Ethiopia. However, the research result could be different if collection of empirical data was includes non-governmental organizations in Ethiopia (but it is hard to get access to the researcher).

The second limitation of this research is in focus on the economic, social, and cultural environment that is distinctive and unique to Ethiopia. This may restrict the generalisation of the results to other cultures. Even inside Ethiopia – a country of more than 80 ethnic groups with diversified beliefs and culture living together – there are huge cultural difference across each regions and sub-regions and ethnic groups. However, In terms of socioeconomic environment, other developing countries especially Sub-Saharan African countries may also have a similar environment to that of Ethiopia. Notwithstanding possible cultural limitations, this research makes an overall contribution to Digital Government research by validating and assessing the applicability of the research in the context of developing countries in Ethiopia.

The third limitation of this research is concerned with the use of the multiple case study approach to investigate the contribution of Digital Government in whistleblowing. Although this research made use of multiple case studies which assisted in providing broad and unique insights on Digital Government adoption in whistleblowing process, nonetheless the data obtained from this individual companies whistleblowing initiatives cannot be generalised. In addition, this research is limited in analyzing at what stage of Digital Government is required for each whistleblowing dimensions based on Janowski (2015) – digitization, transformation, engagement and contextualization.

7.5. Recommendations for Further Research

The finding and the abovementioned limitations of this research have resulted in the identification of potential future research directions for investigation. The recommendations for further research are indicated below.

The lack of ability to generalize on the impact of Digital Government on whistleblowing, due to the socio-economic and cultural environment in the world, points to the need for cross-country and cross continental case studies. Cross continental and cross country case study research could widen the applicability of the conceptual model when used under different circumstances.

Additional research is needed to further validate the findings, in order to increase the generalisation of the findings in different organization (both private and public) within Ethiopia. Re-testing the research results and the recommendations in in different public and private organization within Ethiopia especially, will help to determine whether the findings have the same impact or are less significant in other organizations inside Ethiopia.

As a researcher, we pointed out three recommendations to the Ethiopian government. First, enhance the ICT infrastructure. Second, provide continuous training to employees to increase the level of education and knowledge of whistleblowing. Third, introduce new whistleblowing policies and legislations. Besides, the government/organizations need to adopt and exercise a more open organizational culture.

The performance measurement framework should be validated in different context with multiple case studies to extend the generalisability and contribution of the framework. Also, there could be further investigations that can extend the framework as new measurement matrix could emerge after some time. Although much research has been conducted in the area of Digital Government utilization in different sectors of public services, the area related to Digital Government utilization in organizations whistleblowing program is still relatively new. This indicates that more research still needs to be conducted other developing countries especially in Sub-Saharan African countries.

Finally, from the review of the literature, it appears that no existing research had examined the level of Digital Government stages required for each whistleblowing dimensions – whistleblowing procedure, whistleblowing organizational structure and whistleblowing protection. It will be useful to conduct further research in this area.

7.6. Summary

Digital Government has been acknowledged to be an essential system for delivering government services nowadays. It has been used for different domain areas. Whistleblowing is considered as a front runner mechanism in a fight against fraudulent activities. However, there was no previous study that investigate the possible contribution of Digital Government for whistleblowing domain. In addition, digital enabled whistleblowing initiative in Ethiopian public organization are not effective due to different challenges, as empirical evidence is still lacking. Moreover, the understanding of the issue of Digital Government on whistleblowing requires further work. This study aims to fill the research gap.

It is expected that the findings obtained in this study would be beneficial in providing some necessary guidance for organization wishing to adopt and effectively use Digital Government in other developing countries. This research has fulfilled its goals and expectations and has answered all research questions set out at the beginning of the study. The research has provided significant contributions towards explaining the contribution of Digital Government in whistleblowing domain and the factors influencing/affecting the adoption and effective utilisation of digitally enabled whistleblowing initiatives in Ethiopian public organizations. Although many researchers have tried to investigate the application of Digital Government in different domain areas, no approach had yet been put forward which could serve as a guide in resolving the problems facing Ethiopian whistleblowing programs through Digital Government. Based on the result, this research contributes significantly to theoretical developments in the literature on the Digital Government and whistleblowing.

This chapter has presented the contributions of this research to the body of knowledge which include the developed framework, the research methods adopted for the study and how they were applied, key limitations of the present research as well as recommendations for future research. The research also adds to the body of knowledge by empirically providing evidence that can increase the knowledge of Digital Government adoption and usage in Ethiopian public organizations thereby expanding the research area, in the field of Digital Government. The research findings are beneficial to academics, practitioners, and policy makers.

REFERENCE

ACFE. (2016). *Report to the Nations on Occupational Fraud and Abuse*: 2016 Global Fraud Study. Association of Certified Fraud Examiner (ACEF) publishing. https://www.acfe.com/rttn2016/docs/2016-report-to-the-nations.pdf

ABSCBN. (2018). "Whistleblowing portal launched to curb corruption in GOCCs" http://news.abs-cbn.com/nation/05/02/16/whistleblowing-portal-launched-to-curb-corruption-in-goccs. ABSCBN News. Accessed on July 2018.

Accenture. (2015). *Digital Government Pathways to Delivering Public Services for the Future: A comparative study of Digital Government Performance across 10 countries.* 2015 Accenture Report, Accenture publishing. https://www.accenture.com

ACUPCC. (2003). *African Union Convention on Preventing and Combating Corruption*, Preamble, Adoption July 01- 2003.

Afrileaks. (2019). Securely share information with Africa's finest journalists. https://www.afrileaks.org/. Accessed on June 25, 2019

Aggelidis, V. P., & Chatzoglou, P. D. (2009). Using a modified technology acceptance model in hospitals. *International journal of medical informatics*, *78*(2), 115-126.

Aiello, J. R. (1993). Computer-Based Work Monitoring: Electronic Surveillance and Its Effects. *Journal of Applied Social Psychology*, 23: 499–507

Allen, M. (2017). The sage encyclopedia of communication research methods (Vols. 1-4). Thousand Oaks, CA: SAGE Publications, Inc doi: 10.4135/9781483381411

Alleyne, P., & Watkins, A. (2017). Whistleblowing as a corporate governance mechanism in the Caribbean. In Snapshots in Governance: *The Caribbean Experience* (2nd ed., pp. 176–198). University of the West Indies.

Ajzen, I., & Fishbein, M. (1972). Attitudes and normative beliefs as factors influencing behavioral intentions. *Journal of personality and social psychology*, *21*(1), 1.

Apaza, C. R., & Chang, Y. (2011). What makes whistleblowing effective: Whistleblowing in Peru and South Korea. *Public Integrity*, 13(2), 113-130.

APC. (2015). *The protection of sources and whistleblowers*. Association for Progressive Communications (APC) 29th June 2015

Bartels, D.M., Bauman, C.W., Cushamn, F.A., Pizarro, D. & McGraw, A.P. (2014). Blackwell reader of judgment and decision making, *Blackwell, Malden*, MA (2014).

Banisar, D. (2011). Whistleblowing: International standards and developments. *Corruption and transparency: Debating the frontiers between state, market and society, I. Sandoval, ed., World Bank-Institute for Social Research, UNAM, Washington, DC*.

Barkemeyer, R., Preuss, L., & Lee, L. (2015). Corporate reporting on corruption: An international comparison. *Accounting Forum*, 39(4), 349–365. doi: 10.1016/j.accfor.2015.10.001

Benchekroun, T. H., & Pierlot, S. (2012). Whistleblowers: an essential resource for the sustainable prevention of risks in sociotechnical systems. *Work, 41*(Supplement 1), 3051-3061.

Berry, B. (2004). Organizational Culture: A Framework and Strategies for Facilitating Employee Whistleblowing. *Employee Responsibilities and Rights Journal*, 16(1), 1–11. doi: 10.1023/b:errj.0000017516.40437.b1

Bertot, J. C., Jaeger, P. T., & Grimes, J. M. (2010). Using ICTs to create a culture of transparency: E-government and social media as openness and anti-corruption tools for societies. *Government Information Quarterly*, 27(3), 264–271. doi: 10.1016/j.giq.2010.03.001

Bolívar, M. P. R., Muñoz, L. A., & Hernández, A. M. L. (2012). Studying e-government: Research methodologies, data compilation techniques and future outlook. *Academia. Revista Latinoamericana de Administración*, (51), 79-95.

Bowden, P. (2006). A comparative analysis of whistleblower protections. *Australian Journal of Professional and Applied Ethics, 8*(2).

Brevini, B. (2017). WikiLeaks: Between disclosure and whistle-blowing in digital times. *Sociology Compass*, 11(3). doi: 10.1111/soc4.12457

Bryman, A. (2016). Social Research Methods (5th ed.). London: Oxford University Press.

Bryman, A. (2017). Quantitative and qualitative research: further reflections on their integration. In *Mixing methods: Qualitative and quantitative research* (pp. 57-78). Routledge.

Bwalya, K. J. (2009). Factors affecting adoption of e-Government in Zambia. *Electronic Journal of Information Systems in Developing Countries*, 38(4), 1−13.

Carter, L., & Belanger, F. (2005). The utilization of e-government services: Citizen trust, innovation and acceptance factors. *Information Systems Journal*, 15, pp. 5-25. http://dx.doi.org/10.1111/j.1365-2575.2005.00183.x

Casal, J. C. & Zalkind, S. (1995). Consequences of Whistle-Blowing: A Study of the Experiences of Management Accountants. *Psychological Reports* 77, 795–802.

CETS174. (1999). *Council of Europe Civil Law Convention on Corruption*. Civil Low Convention on Corruption. CETS Publishing.

Chan, S. C., & Ngai, E. W. (2007). A qualitative study of information technology adoption: how ten organizations adopted Web-based training. *Information Systems Journal*, 17(3), 289-315.

Chemisto, M., & Rivett, U. (2018, March). Examining the adoption and usage of an e-government system in rural South Africa: Examining e-government system adoption. In *2018 Conference on Information Communications Technology and Society (ICTAS)* (pp. 1-6). IEEE. 10.1109/ICTAS.2018.8368752.

Chen, S. C., Chen, M., Zhao, N., Hamid, S., Chatterjee, K., & Armella, M. (2009). Florida public hurricane loss model: Research in multi-disciplinary system integration assisting government policy making. *Government Information Quarterly*, *26*(2), 285-294.

Chêne. (2009). *Good Practice in Whistleblowing Protection Legislation (WPL)*, U4 Helpdesk, Transparency International 2009.

Chin, W. (1998). The partial least squares approach to structural equation modeling. In G. A. Marcoulides (Ed.), *Modern Methods for Business Research*, *295*(2), (295-358).

CM. (2014). PROTECTION OF WHISTLEBLOWERS, Recommendation CM/ Rec (2014)7 adopted by the Committee of Ministers of the Council of Europe on 30 April 2014 and explanatory memorandum.

Cohen. (2017). Whistleblower laws in the financial markets: lessons for emerging markets, christian chamorro-courtland. *Arizona Journal of International and Comparative Law*, Spring 2017.

Collis, J. and Hussey, R. (2003). Business Research: A Practical Guide for Undergraduate and Postgraduate Students, Palgrave Macmillan, Houndmills, Basingstoke, Hampshire.

Colvin, N. (2018). Whistle-blowing as a Form of Digital Resistance: State Crimes and Crimes Against the State. *State Crime Journal*, *7*(1), 24-45.

Corydon, B., Ganesan, V., & Lundqvist, M. (2016). Transforming government through digitization. *Public Sector*. McKinsey & Company publishing. https://www.mckinsey.com/~/media/McKinsey/Industries/Public Sector/Our Insights/Transforming government through digitization/Transforming-government-through-digitization.ashx

Creswell, J. W., & Clark, V. L. P. (2017). *Designing and conducting mixed methods research*. Sage publications.

Creswell, J.W. (2007). Research Design: Choosing among five approaches. Thousand Oaks, CA: Sage.

Creswell, J. W., & Creswell, J. D. (2017). *Research design: Qualitative, quantitative, and mixed methods approaches*. Sage publications.

Cronbach, L. J. (1951). Coefficient alpha and the internal structure of tests. *Psychometrika*, 16(3), 297-334.

Dalby, D. (2020). What is the Platform to Protect Whistleblowers in Africa? Retrieved January, 2020, from https://www.icij.org/investigations/luanda-leaks/what-is-pplaaf/

Davis, F. D. (1989). Perceived usefulness, perceived ease of use and user acceptance of information technology. *MIS Quarterly*, 13(3), 319−339.

Davis, F. D., Bagozzi, R. P., & Warshaw, P. R. (1989). User acceptance of computer technology: a comparison of two theoretical models. *Management science, 35*(8), 982-1003.

DBIS. (2015). Whistleblowing: Guidance for Employers and Code of Practice. United Kingdom Department for Business, Innovation and Skills www.gov.uk/bis

Dehn, G. & Calland, R. (2004). Whistleblowing - The state of the art. The role of the individual, organisations, the state, the media, the law and civil society. London: Public Concern at Work, 2004, p. 12.

Deloitte. (2015). *How are digital trends reshaping government financial organizations? Findings from Deloitte NASACT 2015 Digital Government Transformation Survey*. Deloitte Development LLC Publishing, https://www2.deloitte.com/content/dam/Deloitte/us/Documents/public-sector/us-state-nasact-survey.pdf

Denzin, N. K., & Lincoln, Y. S. (Eds.). (2011). *The Sage handbook of qualitative research*. sage.

Devine, T., & Maassarani, T. F. (2011). *The corporate whistleblower's survival guide: A handbook for committing the truth*. Berrett-Koehler Publishers.

Devine, T., & Walden, S. (2013). International best practices for whistleblower policies. *Government Accountability Project.*

Diaz, C. (2005). *Anonymity and privacy in electronic services*, Technical Report, Leuven, Belgium, December 2005.

DW. (2014). DW Made for Minds. WildLeaks: a whistlebower platform for poaching and wildlife crimes. Retrieved January, 2020, from https://www.dw.com/en/wildleaks-a-whistlebower-platform-for-poaching-and-wildlife-crimes/a-17881961

EGES. (2019). Ethiopian Government Electronic Services | eService. Retrieved December 7, 2019.

ELI. (2020). Earth League International (ELI). THE WORLD’S FIRST WHISTLEBLOWER INITIATIVE DEDICATED TO WILDLIFE CRIME. WildLeaks Reporting. https://wildleaks.org/wp-content/uploads/2020/09/WildLeaks-Report-Sept2020.pdf

Emura, K., Kanaoka, A., Ohta, S., & Takahashi, T. (2017). Establishing secure and anonymous communication channel: KEM/DEM-based construction and its implementation. *Journal of Information Security and Applications*, 34, 84–91. doi: 10.1016/j.jisa.2016.12.001

ERC. (2012). Ethics Resource Center, National Business Ethics Survey 2011 - Workplace Ethics in Transition. Retrieved from https://community.corporatecompliance.org/HigherLogic/System/DownloadDocumentFile.ashx?DocumentFileKey=c2a5b260-d132-49f0-baff-b145a2b1cf7d

Estevez, E., Janowski, T., & Dzhusupova, Z. (2014). Electronic governance for sustainable development: how EGOV solutions contribute to SD goals?. In *Proceedings of the 14th Annual International Conference on Digital Government Research* (pp. 92-101).

Evans, O. (2019). Digital Government: ICT and public sector management in Africa. New Trends in Management: Regional and Cross-border Perspectives, Publisher: London Scientific, pp.269-286

EY. (2016). *Whistle-blowing: - The pillar of sound corporate governance, Building Better Government.* Ernst & Young LLP. Publishing, India. www.ey.com/in

Fang, Z. (2002). E-Government in Digital Era: Concept, Practice, and Development. *International Journal of The Computer, The Internet and Management*, *10*(2), 1–22.

Fedorowicz, J., & Dias, M. A. (2010). A decade of design in Digital Government research. *Government Information Quarterly, 27*(1), 1-8.

Figg, J. (2000). Whistleblowing. *Internal Auditor*, 30–37.

Fornell, C., & Larcker, D. F. (1981). Evaluating structural equation models with unobservable variables and measurement error. *Journal of marketing research*, *18*(1), 39-50.

FPC. (2019). Ethiopian Federal Police Commission Retrieved December 7, 2019.

Fmhaca. (2019). Ethiopian food and drug authority Retrieved December 7, 2019.

French, J. R., & Raven, B. (2004). The bases of social power. *Studies in social power*, 1959-150.

Gefen, D., Karahanna, E., & Straub, D. W. (2003). Trust and TAM in online shopping: An integrated model. *MIS quarterly*, *27*(1), 51-90.

GFIR. (2018). *Exploring the links between customer recognition, convenience, trust and fraud risk.* The 2018 Global Fraud and Identity Report. Experian Information Solutions Publishing. https://www.experian.com/assets/decision-analytics/reports/global-fraud-report-2018.pdf

GFR. (2015). *Vulnerabilities on the Rise annual edition:* 2015/2016 Global Fraud Report, Kroll and the Economist Intelligence Unit Ltd Publishing. http://anticorruzione.eu/wp-content/uploads/2015/09/Kroll_Global_Fraud_Report_2015low-copia.pdf

Gil-Garcia, J. R., & Pardo, T. A. (2006). Multi-method approaches to Digital Government research: Value lessons and implementation challenges. In *Proceedings of the 39th*

Annual Hawaii International Conference on System Sciences (HICSS'06) (Vol. 4, pp. 67a-67a). IEEE.

Gil-Garcia, J. R., Dawes, S. S., & Pardo, T. A. (2018). Digital Government and public management research: finding the crossroads. *Public Management Review*, 20:5, 633-646, DOI: 10.1080/14719037.2017.1327181

GlobaLeaks. (2018). GlobaLeaks implementation. https://en.wikipedia.org/wiki/GlobaLeaks#Implementations Accessed on June 25, 2018

Gold, D. L. (2012). Introduction: Speaking Up for Justice, Suffering Injustice: Whistleblower Protection and the Need for Reform. *Seattle J. Soc. Just.*, *11*, 555.

Grace, D., & Cohen, S. (1998). *Business ethics: Australian problems and cases* (pp. 35-36). Melbourne: Oxford University Press.

Greene, J. C. (2007). *Mixed methods in social inquiry* (Vol. 9). John Wiley & Sons.

Gretzel, U., & Scarpino-Johns, M. (2018). Destination resilience and smart tourism destinations. *Tourism Review International*, 22(3-4), 263-276.

Grix, J. (2001) Introducing students to the generic terminology of social research. Politics, 22(3), pp. 175-186.

Grönlund, Å., & Horan, T. A. (2005). Introducing e-gov: history, definitions, and issues. *Communications of the association for information systems*, *15*(1), 39.

Guardians. (2013). Edward Snowden and the NSA files – timeline. https://www.theguardian.com/world/2013/jun/23/edward-snowden-nsa-files-timeline Accessed on June 26, 2017

Hair, J.F.; Hult, G.T.M.; Ringle, C.M.; Sarstedt, M. (2017). A Primer on Partial Least Squares Structural Equation Modeling (PLS-SEM) (2 ed.). Thousand Oaks, CA: Sage. ISBN 9781483377445.

Hedin, U. C., & Månsson, S. A. (2012). Whistleblowing processes in Swedish public organisations—complaints and consequences. *European Journal of Social Work*, 15(2), 151-167.

Heemsbergen, L. (2013). Whistleblowing and digital technologies: an interview with Suelette Dreyfus. *Platform: journal of media and communication*, *5*, 67-71.

Hoetker, G. (2002). Building the Virtual State: Information Technology and Institutional Change Building the Virtual State: Information Technology and Institutional Change, by Fountain Jane E.. Washington, DC: Brookings Institution Press, 2001. Academy of Management Review, 27(4), 619–622. doi: 10.5465/amr.2002.7566114

Holliday, A. (2007). *Doing and Writing Qualitative Research. London:* Sage Publications Ltd. http://dx.doi.org/10.4135/9781446287958

Hollstein, B. (2014). Mixed methods social networks research: An introduction. *Mixed methods social networks research: Design and applications*, 3-34.

Hovy, E. (2008). An outline for the foundations of Digital Government research. In *Digital Government* (pp. 43-59). Springer, Boston, MA.

Huawei. (2019). Digital Government, Intelligent Government 2019. Huawei Technologies Co., Ltd.

IACAC. (1996). Inter-American Convention against Corruption, Article III (8).

ILO. (2015). International Labour Organization Thesaurus. ILO Thesaurus 2005. Retrieved from http://www.ilo.org/public/libdoc/ILO-Thesaurus/english/index.htm

IPB. (2010). The public interest disclosure and protection to Persons making the disclosures bill. India PID Bill. Bill No. 97 of 2010

Intuit. (2017). *The Path to Digital Governance: An Agenda for Public Service Innovation and Excellence*. Intuit Publishing, Canada. https://iog.ca/docs/The-Path-to-Digital-Governance.pdf

Irani, Z., Weerakkody, V., Kamal, M., Hindi, N. M., Osman, I. H., Anouze, A. L., ... & Al-Ayoubi, B. (2012). An analysis of methodologies utilised in e-government research. *Journal of Enterprise Information Management*, Vol. 25 No. 3, pp. 298-313. https://doi.org/10.1108/17410391211224417

IRISH. (2014). Shatter apologises to whistleblowers and defends handling of taping controversy. IRISH Times https://www.irishtimes.com/news/politics/shatter-apologises-to-whistleblowers-and-defends-handling-of-taping-controversy-1.1738693 accessed on June, 2017

Isensee, C., Teuteberg, F. &Griese, K. (2020). The relationship between organizational culture, sustainability, and digitalization in SMEs: A systematic review. *Journal of Cleaner Production* 275 (2020) 122944

Ivankova, N. V., & Clark, V. L. P. (2016). Mixed methods research: a guide to the field.

Jaeger, P. T. (2003). The endless wire: E-Government as global phenomenon. *Government Information Quarterly*, 20(4), 323−331.

Janowski, T. (2015). Digital Government evolution: From transformation to contextualization. *Government Information Quarterly*, 32(3), 221–236. doi: 10.1016/j.giq.2015.07.001

Jobe, E. D. (2009). Electronic/mobile government in Africa: Progress made and challenges ahead. Retrieved April 20, 2010 from. http://unpan1.un.org/intradoc/groups/public/documents/un/unpan033668.pdf.

Jos, P. H. (1991). The nature and limits of the whistleblower's contribution to administrative responsibility. *The American Review of Public Administration*, 21(2), 105-118.

Kalbaska, N., Janowski, T., Estevez, E., & Cantoni, L. (2017). When Digital Government matters for tourism: a stakeholder analysis. *Information Technology & Tourism*, *17*(3), 315-333.

Katsonis, M., & Botros, A. (2015). Digital Government: A Primer and Professional Perspectives. *Australian Journal of Public Administration*, *74*(1), 42–52. doi: 10.1111/1467-8500.12144

Kaye, D. (2017). Challenges to Freedom of Information in the Digital Age. *Journal of international media & entertainment law*, vol. 7, no. 2

Kelly, D. (2009). A taxonomy for and analysis of anonymous communications networks. Technical Report, Air Force Institute of Technology, March 2009.

King III, G. (1997). The effects of interpersonal closeness and issue seriousness on blowing the whistle. *The Journal of Business Communication* (1973), 34(4), 419-436.

Kock, N., & Hadaya, P. (2018). Minimum sample size estimation in PLS-SEM: The inverse square root and gamma-exponential methods. Information Systems Journal, 28(1), 227–261.

Korkea-Aho, M. (1999). Anonymity and privacy in the electronic world. In *Seminar on Network Security, Helsinki University of Technology*.

Kraemer, K., & King, J. L. (2006). Information Technology and Administrative Reform. *International Journal of Electronic Government Research*, *2*(1), 1–20. doi: 10.4018/jegr.2006010101

Krasniqi, G., Qehaja, B., & Gabor, A. (2018). Evaluation of information technology in healthcare systems and patient monitoring through ICT. *In Conference Book of Proceedings* (p. 25).

Kumar, S. P. (2017). Internet of Things for sophisticated e-governance: A special focus on agricultural sector. *International Journal of Trend in Research and Development*.

Kumar, R. (2019). *Research methodology: A step-by-step guide for beginners*. Sage Publications Limited.

Lachman, V. D. (2008). Whistleblowing: role of organizational culture in prevention and management. *Dermatology Nursing / Dermatology Nurses' Association (Dermatol Nurs), 20*(5), 394–396.

Lam, H., & Harcourt, M. (2019). Whistle-blowing in the digital era: motives, issues and recommendations. *New Technology, Work and Employment*. doi: 10.1111/ntwe.12139

Lederer, A., Maupin, D. J., Sena, M. P. & Zhuang, Y. (2000). The technology acceptance model and the World Wide Web. *Decision Support Systems*, 29(3), 269−282.

Li, J., Zhu, L., & Gummerum, M. (2014). The relationship between moral judgment and cooperation in children with high-functioning autism. *Scientific Reports*, 4, 4314.

Liaba, B. & Erdin, E. (2013). An overview of anonymity technology usage. *Computer Communications*, 36 (2013) 1269–1283

Libit, B., Freier, T., & Draney, W. (2014). Elements of an effective whistleblower hotline. In *Harvard Law School Forum on Corporate Governance and Financial Regulation*.

Limaj, E., & Bernroider, E. W. N. (2019). The roles of absorptive capacity and cultural balance for exploratory and exploitative innovation in SMEs. *Journal of Business Research*, 94(September), 137-153. https://doi.org/10.1016/j.jbusres.2017.10.052

Lin, A.C. (1998). Bridging Positivist and Interpretivist Approaches to Qualitative Methods. Policy Studies Journal 26(1), 162–180 (1998)

Lin, J. C. C., & Lu, H. (2000). Towards an understanding of the behavioural intention to use a web site. *International journal of information management, 20*(3), 197-208.

Lin, F., Fofanah, S. S., & Liang, D. (2011). Assessing citizen adoption of e-Government initiatives in Gambia: A validation of the technology acceptance model in information systems success. *Government Information Quarterly*, *28*(2), 271-279.

Loyens, K., & Vandekerckhove, W. (2018). Whistleblowing from an international perspective: A comparative analysis of institutional arrangements. *Administrative Sciences*, *8*(3), 30.

MarketScreener. (2017). Vale Indonesia Tbk PT: PT Vale won the 2017 SBA Award. Retrieved January, 2020, from https://www.marketscreener.com/quote/stock/PT-VALE-INDONESIA-TBK-6493452/news/Vale-Indonesia-Tbk-PT-PT-Vale-won-the-2017-SBA-Award-25616764/ Marx, G. (2004). Internet anonymity as a reflection of broader issues involving technology and society. *Asia-Pacific Review*, 11(1), 142-166.

MCIT. (2011). e-Government Strategy and Implementation Plan - Ministry of Communication and Information Technology (MCIT) Ethiopia publishing.

MCIT. (2015). Assessment of Ministries, Ministry of Communication and Information Technology (MCIT) Ethiopia. KPMG Publishing.

MCIT. (2016). Ethiopian eGovernment Implementation Strategic Plan 2020 of the Ministry of Communication and Information Technology (MCIT) Ethiopia. © 2016 KPMG Publishing.

Mendel, T., Puddephatt, A., Wagner, B., Hawtin, D., & Torres, N. (2012). *Global survey on Internet privacy and freedom of expression*. UNESCO.

Mensah, I. K., & Mi, J. (2017). Electronic Government Services Adoption: The Moderating Impact of Perceived Service Quality. *International Journal of Electronic Government Research* (IJEGR), 13(3), 38-54.

Mehrotra, S., Mishra, R. K., Srikanth, V., Tiwari, G. P., & Kumar, E. V. M. (2019). State of Whistleblowing Research: A Thematic Analysis. FIIB Business Review, 231971451988831. doi:10.1177/2319714519888314

Mesmer-Magnus, J. R., & Viswesvaran, C. (2005). Whistleblowing in organizations: An examination of correlates of whistleblowing intentions, actions, and retaliation. *Journal of business ethics*, 62(3), 277-297.

Miceli, M. P., Near, J. P., & Dworkin, T. M. (2008). Whistle-blowing in organizations. Psychology Press.

Miceli, M. P., Dozier, J. B., & Near, J. P. (1987). Personal and situational determinants of whistle-blowing. *In Meeting of the Academy of Management*. New Orleans, LA

Miceli, M. P., & Near, J. P. (2002). What makes whistle-blowers effective? Three field studies. *Human Relations*, 55(4), 455-479.

Miceli, M. P., & Near, J. P. (1994). Relationships among value congruence, perceived victimization, and retaliation against whistle-blowers. *Journal of Management*, 20(4), 773-794.

Miceli, M. P., Dozier, J. B., & Near, J. P. (1991a). Blowing the whistle on data fudging: A controlled field experiment 1. *Journal of Applied Social Psychology*, 21(4), 271-295.

Miceli, M. P., Near, J. P., & Schwenk, C. R. (1991b). Who blows the whistle and why?. *Industrial and Labor Relations Review*, 45(1), 113-130.

MoMP. (2019). Ministry of Mines and Petroleum. Retrieved December 7, 2019, from

NAO. (2014). Government whistleblowing policies, Design and Production by NAO Communications DP Ref: 10332-001 | © National Audit Office 2014, UK.

Nchuchuwe, F. F., & Ojo, D. A. (2017). E-governance, revenue generation and public service delivery in Nigeria: An overview of the e-taxation system in Lagos state.

Near, J. P., & Miceli, M. P. (1995). Effective-Whistle Blowing. *Academy of Management Review*, *20*(3), 679–708. doi: 10.5465/amr.1995.9508080334

Near, J. P., & Miceli, M. P. (1985). Organizational dissidence: The case of whistle-blowing. *Journal of Business Ethics*, *4*(1), 1–16. doi: 10.1007/bf00382668

Neuendorf, K. A. (2019). Content analysis and thematic analysis. *Advanced Research Methods for Applied Psychology*, 211.

Nissenbaum, H. (1998). Toward an Approach to Privacy in Public: The Challenges of Information Technology, 7 ETHICS BEHAV. 207 (1997), and Helen Nissenbaum, Protecting Privacy in an Information Age: The Problem of Privacy in Public. *LAW PHILOS.*, 17, 559-596.

Nissenbaum, H. (1999). The meaning of anonymity in an information age. *The Information Society*, 15(2), 141-144.

Ntaliani, M., Costopoulou, C., & Karetsos, S. (2008). Mobile government: A challenge for agriculture. *Government Information Quarterly*, *25*(4), 699-716.

OECD. (2003). *The e-Government Imperative*. OECD Publishing, Paris. https://doi.org/10.1787/9789264101197-en

OECD. (2012). *Whistleblower protection: encouraging reporting. CleanGovBiz Integraty Practice*. OECD Publishing, Paris.

OECD. (2014a). *whistleblower protection frameworks, compendium of best practices and guiding principles for legislation*. G20 Anti-Corruption Action plan Protection of Whistleblowers. OECD Publishing.

OECD. (2014b). *Recommendation of the Council on Digital Government Strategies*. Public governance and Territorial Development Directorate, July 2014. OECD Publishing.

OECD. (2015). *G20/OECD Principles of Corporate Governance*. OECD Publishing, Paris. http://dx.doi.org/10.1787/9789264236882-en

OECD. (2016a). *Digital Government Strategies for Transforming Public Services in the Welfare Areas: OECD COMPARATIVE STUDY*. OECD Publishing, Paris. http://www.oecd.org/gov/digital-government/Digital-Government-Strategies-Welfare-Service.pdf

OECD. (2016b). *Broadband Policies for Latin America and the Caribbean*: A Digital Economy Toolkit © OECD, IDB 2016

OECD. (2016c). *Committing to Effective Whistleblower Protection*. OECD Publishing, Paris.

OECD. (2019). *Strengthening Digital Government*. OECD Going Digital Policy Note, OECD Publishing, Paris. www.oecd.org/goingdigital/strengthening-digital-government.pdf.

Ontanu, E. (2019). Adapting Justice to Technology and Technology to Justice. A Coevolution Process to e-Justice in Cross-border Litigation. *East European Quarterly*, *8*(2), 54-74.

OpenDemocracy. (2017). Open Democracy free thinking the world. A whistleblowing platform against corruption for the City Council of Barcelona. Retrieved January, 2020, from https://www.opendemocracy.net/en/digitaliberties/whistleblowing-platform-against-corruption-for-city-council-of-barcelona/

P2P. (2017). P2P FUNDATION. Xnet installs a Whistleblowing Platform against corruption for the City Hall of Barcelona – powered by GlobaLeaks and TOR friendly. Retrieved January, 2020, from https://blog.p2pfoundation.net/xnet-installs-whistleblowing-platform-corruption-city-hall-barcelona-powered-globaleaks-tor-friendly/2017/01/19

PAAIS, M. &, PATTIRUHU, J. (2020) Effect of Motivation, Leadership, and Organizational Culture on Satisfaction and Employee Performance. *Journal of Asian Finance, Economics and Business* Vol 7 No 8 (2020) 577–588

Pamungkas, I., Ghozali, I. & Achmad, T. (2017). The Effects of The Whistleblowing System on Financial Statements Fraud: Ethical Behavior As The Mediators. *International Journal of Civil Engineering and Technology*. 8. 1592-1598.

Parmerlee, M. A., Near, J. P., & Jensen, T. C. (1982). Correlates of whistle-blowers' perceptions of organizational retaliation. *Administrative Science Quarterly*, 17-34.

Pathak, R. D., Naz, R., Rahman, M. H., Smith, R. F. I., & Nayan Agarwal, K. (2009). E-governance to cut corruption in public service delivery: A case study of Fiji. *Intl Journal of Public Administration*, 32(5), 415-437.

Petersen, F., Brown, A., Pather, S., & Tucker, W. D. (2019). Challenges for the adoption of ICT for diabetes self-management in South Africa. *The Electronic Journal of Information Systems in Developing Countries*, e12113.

PPLAAF. (2017). *Platform to Protect Whistleblowers in Africa*, Firs year Activity Report. PPLAAF Publishing. https://pplaaf.org/downloads/annual_report.pdf

Qusqas, F., & Kleiner, B. H. (2001). The difficulties of whistleblowers finding employment. *Management Research News*, *24*(3/4), 97–100. doi: 10.1108/01409170110782702

Rabaa'i, A.A., Zogheib, B., AlShatti, A. & AlJamal, E. (2016). Adoption of e-Government in Developing Countries: The Case of the State of Kuwait 1. *Journal of Emerging Trends in Computing and Information Sciences.* Vol. 7, No. 2.

Rahman, K. (2018). Overview of corruption and anti-corruption in Ethiopia, *U4 Anti-Corruption Helpdesk A free service for staff from U4 partner agencies*

REHG, M. T., MICELI, M. P., NEAR, J. P., & VAN SCOTTER, J. R. (2004). PREDICTING RETALIATION AGAINST WHISTLE-BLOWERS: OUTCOMES OF POWER RELATIONSHIPS WITHIN ORGANIZATIONS. *In Academy of Management Proceedings* (Vol. 2004, No. 1, pp. E1-E6). Briarcliff Manor, NY 10510: Academy of Management.

Reiter, M. K., & Rubin, A. D. (1998). Crowds: Anonymity for web transactions. *ACM transactions on information and system security (TISSEC)*, 1(1), 66-92.

Richard, H. & Savita, B. (2007). Analyzing E-Government Research: Perspectives, Philosophies, Theories, Methods, and Practice. *Government Information Quarterly - GOVT INFORM QUART*. 24. 243-265. 10.1016/j.giq.2006.06.005.

Richardson, B. K., & Garner, J. (2019). Stakeholders' Attributions of Whistleblowers: The Effects of Complicity and Motives on Perceptions of Likeability, Credibility, and Legitimacy. *International Journal of Business Communication*, 232948841986309. doi:10.1177/2329488419863096

Rosen, B. (1998). *Holding government bureaucracies accountable*. Greenwood Publishing Group.

Rosenbloom, T. (2003). Risk Evaluation and Risky Behavior of High and Low Sensation Seekers. *Social Behavior and Personality: an International Journal, 31*(4), 375–386. doi: 10.2224/sbp.2003.31.4.375

Rothschild, J., & Miethe, T. D. (1999). Whistle-blower disclosures and management retaliation: The battle to control information about organization corruption. *Work and occupations,* 26(1), 107-128. doi: 10.1177/0730888499026001006

Roy, J. (2017). Digital Government and service delivery: An examination of performance and prospects. *Canadian public administration*, *60*(4), 538-561.

Santos, J. D., Erdmann, A. L., Meirelles, B. H. S., Lanzoni, G. D. M., Cunha, V. D., & Ross, R. (2017). Integrating quantitative and qualitative data in mixed methods research. *Texto Contexto Enferm*, *6*(2), e1590016.

Safdar, A. (2017). William Bourdon: PLAAF aims to support whistle-blowers. Retrieved January, 2020, from https://www.aljazeera.com/features/2017/4/6/william-bourdon-plaaf-aims-to-support-whistle-blowers

Sainz. J. (2014). Spain's WikiLeaks-inspired Xnet peaceful guerrilla movement fights graft using technology, courts. Retrieved January, 2020, from https://www.smh.com.au/world/spains-wikileaksinspired-xnet-peaceful-guerrilla-movement-fights-graft-using-technology-courts-20141213-126e1d.html.

SAPDA. (2000). Republic of South Africa Protected Disclosure Act of 26 of 2000.

Sapin. (2016). French Anti-Corruption Legal Framework. Sapin II Law. TRANSPARENCY, ANTI-CORRUPTION AND ECONOMIC MODERNISATION BILL. French Official Journal on December 10, 2016

SCB. (2005). Supreme Court of Brazil, Inquiry No. 1.957, en banc, 11 May 2005

Schepers, J. & Wetzels, M. (2007). A meta-analysis of the technology acceptance model: Investigating subjective norm and moderation effects. *Information & Management*. 44. 90-103. 10.1016/j.im.2006.10.007.

Schultza, D., & Harutyunyanb, k. (2015). Combating corruption: The development of whistleblowing laws in the United States, Europe, and Armenia. *International Comparative Jurisprudence* Volume 1, Issue 2, December 2015, Pages 87-97

Schwartz, H. S. (2018). Organization in the age of hysteria. In: Society against Itself (pp. 163-189). London, UK: Routledge.

Schwartz, M., 2013. Developing and sustaining an ethical corporate culture: The core elements. Bus. Horiz. 56, 39–50.

Seifert, J. W., & Chung, J. (2008). Using E-Government to Reinforce Government—Citizen Relationships. *Social Science Computer Review*, *27*(1), 3–23. doi: 10.1177/0894439308316404

Shahid, R. (2017). Essential Elements of an Effective Whistleblower Hotline and Reporting Program.

Siau, K., & Long, Y. (2005). Synthesizing e-government stage models – a meta-synthesis based on meta-ethnography approach. *Industrial Management & Data Systems*, 105(4), 443–458. doi:10.1108/02635570510592352

Sideridis, A. B. (2019). A Smart Cross Border e-Gov Primary Health Care Medical Service. In *International Conference on e-Democracy* (pp. 67-78). Springer, Cham.

SKA. (2008). South Korea’s Act on Anti-Corruption 2008 and the Establishment and Operation of the Anti-Corruption and Civil Rights Commission (2008) Article 64.

SNDGG. (2018). Digital Government Blueprint (Summary), A SINGAPORE GOVERNMENT THAT IS DIGITAL TO THE CORE, AND SERVES WITH HEART. Smart Nation Digital Government Group Publishing.

St-Martin, F. (2014). Measuring the Effectiveness of Canadian Whistleblowing Law. *Iaca - international anti-corruption academy*, 2014

Suh, B.J & Shim, H.S (2020)The effect of ethical corporate culture on anti-fraud strategies in South Korean financial companies: Mediation of whistleblowing and a sectoral comparison approach in depository institutions. *International Journal of Law, Crime and Justice*. https://doi.org/10.1016/j.ijlcj.2019.100361

Suh, J., Shim, H., Button, M., 2018. Exploring the impact of organizational investment on occupational fraud: mediating effects of ethical culture and monitoring control. *Int. J. Law, Crime Justice 53* (June), 46–55.

Suki, N. M., & Ramayah, T. (2010). User acceptance of the e-government services in Malaysia: structural equation modelling approach. *Interdisciplinary Journal of Information, Knowledge, and Management*, 5(1), 395-413.

Sulistyowati. 2007. Pengaruh Kepuasan Gaji Dan Struktur Organisasi Terhadap Persepsi Aparatur Pemerintah Daerah Tentang Tindak Korupsi. JAAI Vol.11 No.1, Universitas Sanata Darma

Taylor, S., & Todd, P. (1995). Assessing IT usage: The role of prior experience. *MIS quarterly*, 561-570.

TheGlobalFund. (2019). The Global Fund office of the inspector general. Whistle-blowing Policy and Procedures for the Global Fund to Fight AIDS, Tuberculosis and Malaria. Retrieved from https://www.theglobalfund.org/media/2942/core_whistleblowing_policy_en.pdf

Thorsen, E. (2016). Whistleblowing in a digital age: Journalism after Manning and Snowden. In *The Routledge companion to digital journalism studies* (pp. 568-578). Routledge.

TI. (2013). *Whistleblower protection and the UN convention against corruption*. Transparency International Publishing. http://www.europarl.europa.eu/meetdocs/2009_2014/documents/libe/dv/ti_report_/ti_report_en.pdf

TI. (2019). *Transparency International: Corruption Perceptions Index 2019*. Published by Transparency International, Germany.

TI-NL. (2017). *Whistleblowing Frameworks. Assessing Dutch Publicly Listed Companies.* Transparency International Nederland Publication. https://www.transparency.nl/wp-content/uploads/2017/12/Whistleblowing-Frameworks-TI-NL-final-report-13-12-2017.pdf

Torres, L., Pina, V. & Acerete, B. (2005). E-Government developments on delivering public services among EU cities. *Government Information Quarterly*, 22(2), 217−238.

UNCAC. (2005). *United Nations Convention Against Corruption*, United Nations Office on Drugs and Crime.

UNDESA. (2019). *DIGITAL GOVERNMENT*. Department of Economic and Social Affairs Public Institutions. UN publishing.

UNEGOV. (2018). *United Nations E-government Survey 2018*, gearing e-government to support transformation towards sustainable and resilient societies. UN publishing.

UNESCO. (2015). *Access to information and knowledge, Freedom of Expression, Privacy, and Ethics on a Global Internet.* United Nations Educational, Scientific and Cultural Organization. Keystones to foster inclusive Knowledge Societies, 3-4 MARCH, 2015

UNESCO. (2018). *The UN Educational, Scientific and Cultural Organization, FACT SHEET SUB-SAHARAN AFRICA, Education for all global monitoring report.* UNESCO publishing.

UNHRC. (2014). *The right to privacy in the digital age: Report of the Office of the United Nations High Commissioner for Human Rights.* United Nations' Human Rights Council. Office of the High Commissioner for Human Rights. Accessed 22nd June 2015.

UNODC. (2004). UN Anti-Corruption Toolkit, 3rd Edition, Vienna, 2004, p. 67. United Nations Office on Drugs and Crime. UN publishing.

Urbach, N. & Ahlemann, F. (2010). Structural Equation Modeling in Information Systems Research Using Partial Least Squares. *Journal of Information Technology Theory and Application*, 11(2), pp. 5-40.

Urciuoli, L., Hintsa, J., & Ahokas, J. (2013). Drivers and barriers affecting usage of e-Customs—A global survey with customs administrations using multivariate analysis techniques. *Government Information Quarterly, 30*(4), 473-485.

USWPC. (1989). *United State Whistleblower Protection Act of 1989*. Public law 101-2-April 10 1989.US government publishing office.

Vale. (2018). Code of ethics and conduct. Retrieved January, 2020, from http://www.vale.com/EN/aboutvale/ethics-and-conduct-office/code-of-ethics/Documents/codigo-conduta-etica/code-of-ethics_conduct_vale.pdf

Venkatesh, V. (2000). Determinant of perceived ease of use: Integrating control, intrinsic motivation, and emotion into technology acceptance model. *Information Systems Research*, 11(4), 342−365.

VWC. (2019). Whistleblowing system. Retrieved November 27, 2019, from http://www.vale.com/indonesia/EN/investors/corporate-governance_id/whistleblower-system/Pages/default.aspx.

Walle, Y.M., Janowski, T. & Estevez, E. (2018). Fighting administrative corruption with Digital Government in sub-saharan Africa. *18th European Conference on Digital Government, ECDG 2018*; Santiago de Compostela; Spain; 25 October 2018 through 26 October 2018; Code 142843

WB. (2018). The World Bank group. Environmental and natural resource for global practice. Tools and resources to combat illegal wildlife crime. The World Bank publishing. http://pubdocs.worldbank.org/en/389851519769693304/24691-Wildlife-Law-Enforcement-002.pdf

WildLeaks. (2019). Retrieved November 27, 2019, from https://wildleaks.org/.

Williamson, K., Burstein, F. and McKemmish, S. (2002). The two major traditions of research. In: Williamson, K., Research methods for students and professionals: Information management and systems (2nd ed.) Wagga Wagga, Australia: Centre for Information Studies, Charles Sturt University.

Wisnewski, J. (2016). WikiLeaks and whistleblowing: privacy and consent in an age of digital surveillance. In *Ethics and the Future of Spying* (pp. 221-232). Routledge.

Xnet. (2019). Internet freedoms & digital rights. Retrieved November 27, 2019, from https://xnet-x.net/en/.

Yang, K., & Rho, S. Y. (2007). E-government for better performance: Promises, realities, and challenges. *International Journal of Public Administration*, 30(11), 1197-1217.

Yoshida, K., Tanaka, K., Hariya, R., Azechi, I., Iida, T., Maeda, S., & Kuroda, H. (2016). Contribution of ict monitoring system in agricultural water management and environmental conservation. In *Serviceology for Designing the Future* (pp. 359-369). Springer, Tokyo.

APPENDIXES A: QUESTIONNAIRE SURVEY

Department of Computer Science
College of Graduate Studies
Sudan University of Science and Technology
Dear Sir/Madam,

I am a PhD student in Computer Science at the Sudan University Science and Technology, Sudan. I am currently conducting research on Digital Government and Whistleblowing and whistleblower Protection.

I would like to invite you to be a part of a research study. The purpose of the research is to explore factors affecting the user acceptance of Digital Government whistleblowing initiatives in Ethiopian public organizations. Understanding the acceptance of employees in Ethiopian public organization for Digital Government whistleblowing initiatives will make a new contribution to the knowledge.

The questionnaire consists of three parts:

Part A: Demographic Information.

Part B: Background of Your Whistleblowing System Usage

Part C: Attitudes and Motivations,

Any information you provide will be kept strictly confidential and will not be attributed to the individual or organization. All responses will be stored in a secure environment. The results of this research would be used for academic purposes only. Your help would be greatly appreciated, thank you very much for your time and cooperation. I would be very grateful if you could participate in a questioner regarding this research.

Thank you for your time and cooperation.

SECTION A: DEMOGRAPHIC INFORMATION

(Please check (√) only one answer)

A1. Age

1	22 – 30	**2**	31 - 40	**3**	>40

A2. Gender

1	Male	**2**	Female

A3. Where do you employed?

1	Government organization	**2**	Government Academic Institutions

SECTION B: BACKGROUND OF YOUR WHISTLEBLOWING SYSTEM USAGE

Please answer [√] only one answer for the following questions.

B1. **How long have you been using the digitally enabled whistleblowing systems**?

1	Less than 1 year	**2**	1-5 years	**3**	6-10 years	**4**	More than 10 years

B2. **How often do you use the digitally enabled whistleblowing systems per a week**?

1	< 1 Time	**2**	1 – 5 Times	**3**	5 – 10 Times	**4**	> 10 Times

B3. What is your self-assessment about using digitally enabled whistleblowing systems?

1	Low experience	**2**	Moderate experience	**3**	High experience

B4. Currently, do you think that you use the digitally enabled whistleblowing systems enough or not enough or too much?

1	Not enough	**2**	Enough	**3**	Too much

SECTION C: ATTITUDES AND MOTIVATIONS

Please circle the appropriate number to indicate the level of your agreement or disagreement with the following statements on a scale of 1 to 5, where: 1= Strongly Disagree 2= Disagree 3= Neutral 4= Agree 5= Strongly Agree.

ITEMS	Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree
Behavioural Intention to Use whistleblowing services					
A. I would use Digital Government whistleblowing services to tackle misconducts in an organization	1	2	3	4	5
B. I would see myself using Digital Government whistleblowing services for reporting unlawful activities.	1	2	3	4	5
C. I intend to use Digital Government whistleblowing system on a regular basis in the future.	1	2	3	4	5
D. I will strongly recommend others to use Digital Government whistleblowing system.	1	2	3	4	5
Attitude toward Using whistleblowing services					
A. Using Digital Government whistleblowing services is a good idea.	1	2	3	4	5
B. Using Digital Government whistleblowing services in the Ethiopia is a pleasant idea.	1	2	3	4	5
C. In my opinion, it would be desirable to use Digital Government whistleblowing services	1	2	3	4	5
Perceived Usefulness					
A. Using Digital Government whistleblowing services would enable me to blow the whistle more quickly	1	2	3	4	5
B. Using Digital Government whistleblowing system would improve the performance the organization workplace.	1	2	3	4	5

C. I would find Digital Government whistleblowing services useful and advantageous	1	2	3	4	5
Perceived ease of use					
A. Learning to operate the Digital Government whistleblowing system would be easy for me.	1	2	3	4	5
B. I would find it easy to get the Digital Government whistleblowing system to report wrongdoings.	1	2	3	4	5
C. It would be easy for me to become skillful at using the Digital Government whistleblowing service on the internet and other digital technologies.	1	2	3	4	5
Whistleblowing System Quality					
A. Using Digital Government whistleblowing services would not divulge my privacy/identity throughout all stages of the investigation.	1	2	3	4	5
B. I would find Digital Government whistleblowing service reliable in conducting my whistleblowing activities.	1	2	3	4	5
C. I would find Digital Government whistleblowing service kept my information confidential.	1	2	3	4	5
D. The Digital Government whistleblowing system provides convenient access.	1	2	3	4	5
E. The Digital Government whistleblowing services are easy to use.	1	2	3	4	5
F. I could use Digital Government whistleblowing services at anytime, anywhere I want.	1	2	3	4	5
G. I could use Digital Government whistleblowing services for oral disclosure or written disclosure to report unlawful activities.	1	2	3	4	5
H. I could use Digital Government whistleblowing services to report misconducts in my own language.	1	2	3	4	5

I. I would find Digital Government whistleblowing services very transparent, enforceable and timely to follow up on whistleblowing.	1	2	3	4	5
Subjective Norm					
A. What Digital Government whistleblowing system stands for is important for me as a citizen in this country.	1	2	3	4	5
B. I like using Digital Government whistleblowing services on the similarity of my values and society values underlying its use.	1	2	3	4	5
C. People who are important to me believe that I should be using Digital Government whistleblowing services.	1	2	3	4	5
Information Quality					
A. The Digital Government whistleblowing service will provide accurate whistleblowing information when I prepare to use it.	1	2	3	4	5
B. The Digital Government whistleblowing service will provide complete information.	1	2	3	4	5
C. The Digital Government whistleblowing service will provide reliable information.	1	2	3	4	5
D. The Digital Government whistleblowing service will provide the timely information about the whistleblowing.	1	2	3	4	5
E. The Digital Government whistleblowing service will provide relevant whistleblowing information I need.	1	2	3	4	5

APPENDIXES BI: THE ITEMS THAT MEASURE THE RESEARCH MODEL CONSTRUCTS

BI - BEHAVIOURAL INTENTION

BI1. I would use Digital Government whistleblowing services to tackle misconducts in an organization

BI2. I would see myself using Digital Government whistleblowing services for reporting unlawful activities.

BI3. I intend to use Digital Government whistleblowing system on a regular basis in the future.

BI4. I will strongly recommend others to use Digital Government whistleblowing system.

ATT - ATTITUDE

ATT1. Using Digital Government whistleblowing services is a good idea.

ATT2. Using Digital Government whistleblowing services in the Ethiopia is a pleasant idea.

ATT3. In my opinion, it would be desirable to use Digital Government whistleblowing services.

PU - PERCEIVED USEFULNESS

PU1. Using Digital Government whistleblowing services would enable me to blow the whistle more quickly

PU2. Using Digital Government whistleblowing system would improve the performance the organization workplace.

PU3. I would find Digital Government whistleblowing services useful and advantageous.

PEU - PERCEIVED EASE OF USE

PEU1. Learning to operate the Digital Government whistleblowing system would be easy for me.

PEU2. I would find it easy to get the Digital Government whistleblowing system to report wrongdoings.

PEU3. It would be easy for me to become skillful at using the Digital Government whistleblowing service on the internet and other digital technologies.

WSQ - WHISTLEBLOWING SYSTEM QUALITY

WSQ1. Using Digital Government whistleblowing services would not divulge my privacy/identity throughout all stages of the investigation.

WSQ2. I would find Digital Government whistleblowing service reliable in conducting my whistleblowing activities.

WSQ3. I would find Digital Government whistleblowing service kept my information confidential.

WSQ4. The Digital Government whistleblowing system provides convenient access.

WSQ5. The Digital Government whistleblowing services are easy to use.

WSQ6. I could use Digital Government whistleblowing services at anytime, anywhere I want.

WSQ7. I could use Digital Government whistleblowing services for oral disclosure or written disclosure to report unlawful activities.

WSQ8. I could use Digital Government whistleblowing services to report misconducts in my own language.

WSQ9. I would find Digital Government whistleblowing services very transparent, enforceable and timely to follow up on whistleblowing

SN - SUBJECTIVE NORM

SN1. What Digital Government whistleblowing system stands for is important for me as a citizen in this country

SN2. I like using Digital Government whistleblowing services on the similarity of my values and society values underlying its use

SN3. People who are important to me believe that I should be using Digital Government whistleblowing services.

IQ - INFORMATION QUALITY

IQ1. The Digital Government whistleblowing service will provide accurate whistleblowing information when I prepare to use it.

IQ2. The Digital Government whistleblowing service will provide complete information.

IQ3. The Digital Government whistleblowing service will provide reliable information.

LIST OF PUBLICATIONS

Walle, Y.M., Janowski, T. & Estevez, E. (2018). Fighting administrative corruption with Digital Government in sub-Saharan Africa 18th European Conference on Digital Government, ECDG 2018; Santiago de Compostela; Spain; 25 October 2018 through 26 October 2018; Code 142843

Walle, Y. M. (2020). The Impact of Digital Government on Whistleblowing and Whistle-blower Protection: Explanatory Study. Journal of Information Technology Management, 12(1), 1-26. doi: 10.22059/jitm.2019.291003.2409

Walle, Y.M. (2020). Citizen Adoption of Digital-Government whistleblowing system initiatives in Ethiopian: A validation of the Technology Acceptance Model (TAM) in whistleblowing systems success. *SUST Journal of Engineering and Computer Sciences (JECS), Vol. 21, No. 1, 2020*