Audit Process Automation and Redesign:
A Case Study

Kristyn Calabrese, Andrea Rozario, Chanta Thomas, and Abigail (Chanyuan) Zhang

1. Background

- A medium-sized CPA firm in the United States approached the authors looking for guidance to automate and redesign the audit planning processes of its Single Audit services to improve their efficiency and effectiveness. This CPA firm was at the time one of the leading providers of Single Audits in the United States.

- Single Audits are organization-wide audits of non-federal entities (e.g., states, local governments, universities, and not-for-profit entities) that expend $750,000 or more of Federal funds in one year.

- Single Audits are performed annually to assure the US federal government that the Federal funds are managed and used properly. The amount of time this firm spends on conducting Single Audits varies and depends on the magnitude and complexity of the programs being tested.

2. The Need For Process Automation and Redesign

1) Manual

Even though the audit working papers are digitized using CaseWare and Excel, manual procedure is still prevalent.

2) Time-consuming

Since the planning process involves a large amount of manual procedures, it is very time-consuming.

3) Error-prone

Current planning procedure is prone to errors that are caused by the manual execution of data referencing, calculation, and classification.

4) Non-standardized

Different auditors tend to annotate working papers in diverse ways, adding complexities in the audit reviewing procedure.

3. The Audit Planning Process Before Automation and Redesign
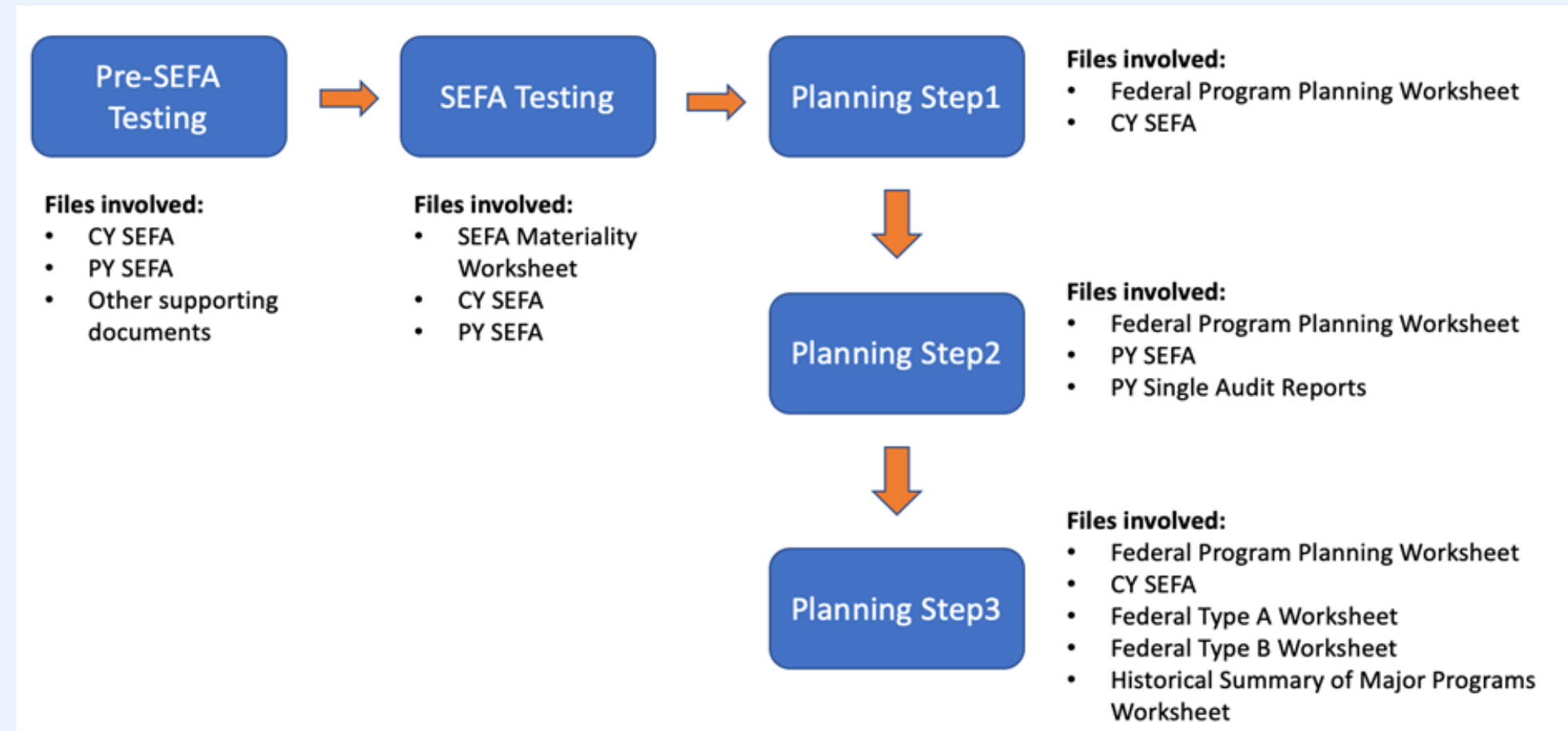
Pre-SEFA Testing

Before the audit of the Current Year (CY) Schedule of Expenditures of Federal Awards (SEFA), auditors first need to ensure the integrity of the data provided by the clients.

SEFA Testing

In SEFA Testing, the auditors use the SEFA Materiality Worksheet to decide the SEFA-wide materiality.

Planning Step1/2/3

From this step, the auditor needs to use the Federal Program Planning Worksheet (FPPW) to perform other planning procedures with extra documents, such as the Federal Type A Worksheet.

Before redesign, auditors generally spend about 3 hours completing the rule-based and repetitive tasks in the audit planning.
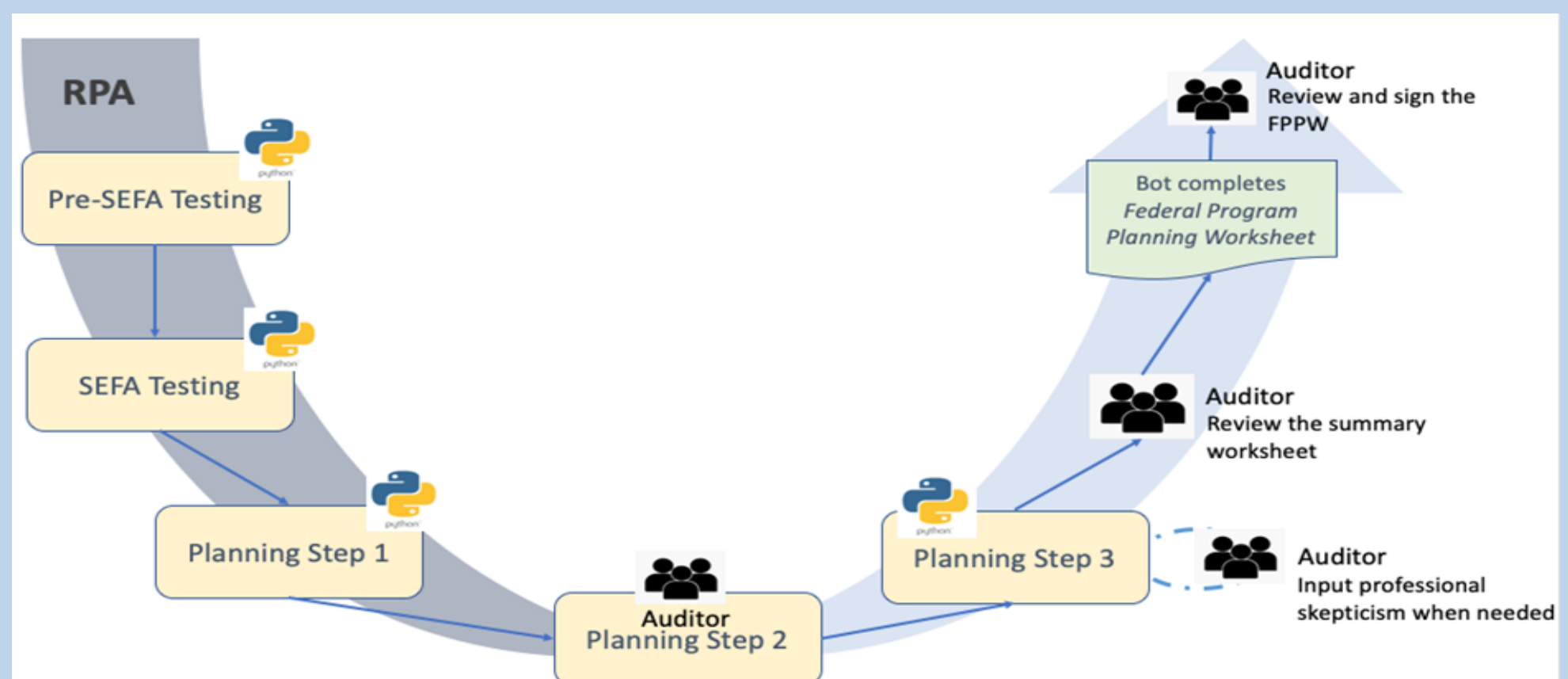
4. The Audit Planning Process After Automation and Redesign

We first identified the rule-based, repetitive, and standardized tasks in the audit planning procedure.

Then we developed Python codes to read information from the spreadsheets and perform corresponding rule-based analytics to generate results.

Next, we configured Robotic Process Automation (RPA) software 1) to execute different Python codes; 2)to interact with auditors when their professional judgements are needed, and 3)to open the planning worksheet and fill it out with the information in the Summary Worksheet.

The automation prototype can finish the rule-based and repetitive tasks in the audit planning in about 3 minutes .

5. The Impacts of Automation and Redesign on Audit Quality

The automated and redesigned planning procedure in Single Audits can bring the following benefits to audit quality: 1)time spent on mundane tasks is largely reduced. Therefore, auditors can focus on the tasks that require professional judgements; 2)the audit procedures assisted by automation are more coherent and organized than those executed manually; 3)the audit working papers are further standardized and are both machine-readable and human-readable, making audit review easier and faster.

However, some unintended consequences may hamper audit quality: 1)errors intentionally or unintentionally embedded in the automation tools can cause mistakes in the audit procedure; 2)poor management of the automation tools may lead to malicious manipulation of the audit evidence; 3)configuration errors can slow down or even break down the automated audit procedures, decreasing the efficiency.

6. Conclusions

This research explored the need and the methods for the audit process to be automated and redesigned. Future study can look at the quantitative impacts of audit automation on audit quality.

RUTGERS
Rutgers Business School
Newark and New Brunswick

Continuous Auditing using Government Blockchain Applications

Eid Alotaibi, Mauricio Codesso, and Hussein Issa

Blockchain & Smart-Contracts as Continuous Auditing

- There has been a recent interest in a specific emerging technology, namely blockchain, due to the myriad of potential applications in the business world, such as blockchain- enabled smart contracts.

- Smart contracts are automated contracts and self-executing with specific instructions written on its code which get executed when certain conditions are made. This process can enable real-time monitoring on particular audit testing, such as confirmations and authorizations.

- Smart-contract software is a technological improvement that are generated to monitor particular settings and perform based on pre-set rules and different procedures that respond to the input rules (Christidis & Devetsikiotis, 2016).

- Blockchain with its smart-contracts is a technology that permits the decentralized and anonymous recording of disaggregate data to a public ledger in real-time database access.

- The motivation of this paper dawns from the point that the proposed framework has the potential to improve transparency and audit by providing a public Blockchain with its smart-contracts system.

What

- Using Smart-contracts in blockchain as an automatic method used to perform auditing activities, such as control and risk assessments, on a more frequent basis.

Why

- Automating error checking and data verification in real time

- Monitoring control automatically on a more frequent basis

- Enabling auditors to extract audit evidences from one source

How

- Describe the core concepts and features of blockchain and smart-contracts

- Proposed a blockchain with smart-contracts based framework to store and publish government open checkbook data

- Continuous auditing method used to perform auditing activities

Our Conceptual Model

Our framework is the consistency of three routes the process purchases of goods or services, process payment, and process blockchain:

- The first component of the methodology is to process procurement conditions and prices to smart contracts in the blockchain because smart contracts can enforce certain rules and conditions, which are very important in government contracts. This step automatically applies the actual process flows from procurement from activity logs to the baseline model established in the first step in the framework to create the smart contract.

- The second component of the methodology is to basically ensures that regular payments comply with prescribed process flows.

The third component, process data, automatically apply the actual process flows from procurement from activity logs to the baseline model established in the first step in the framework to create the smart contract. After the state or agency complete the invoice process, the blockchain verifies with the smart **4.The Audit Planning Process After Automation and Redesign**

GovBlockchain Conceptual Model

Simplified Model

RUTGERS
Rutgers Business School
Newark and New Brunswick
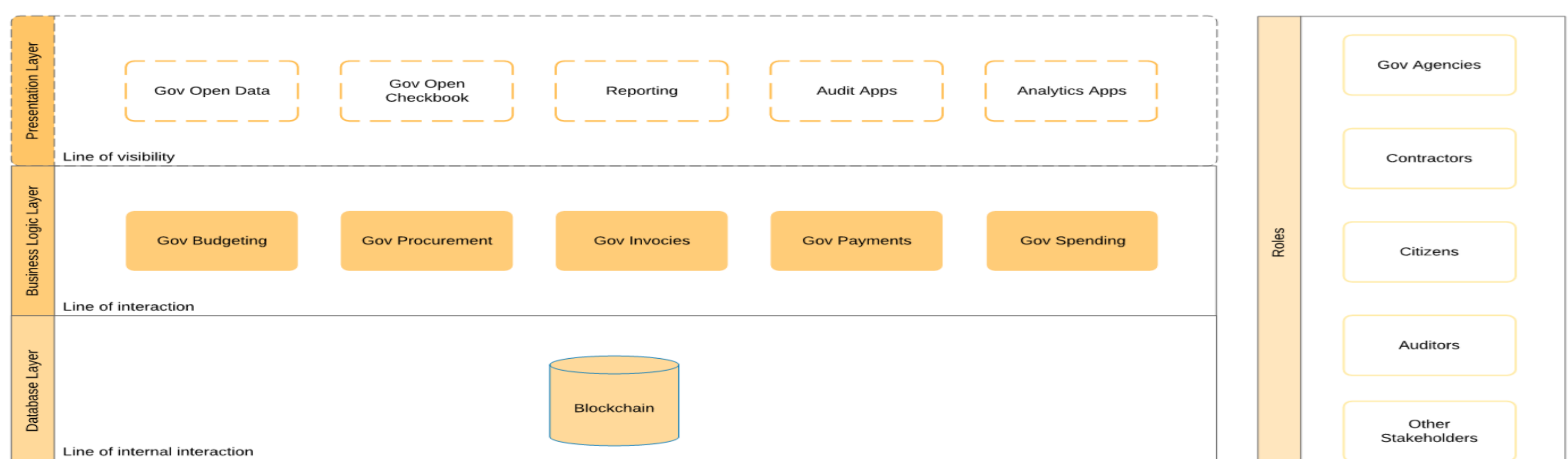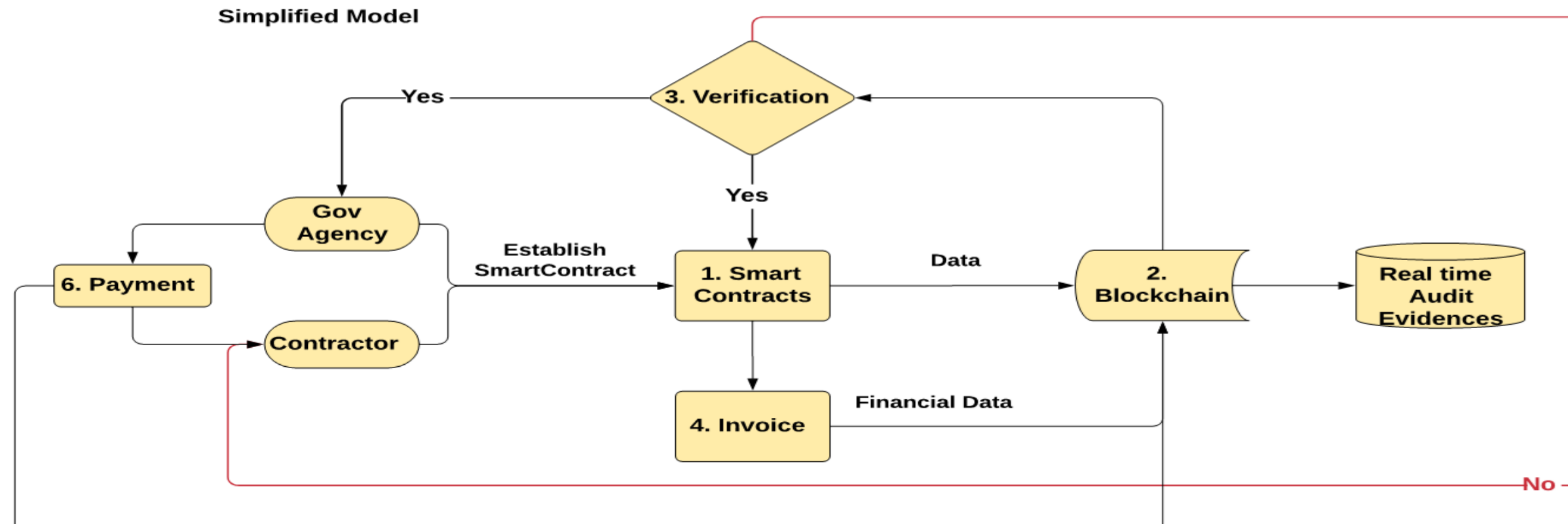
Cryptocurrency Pricing for Tax and Financial Reporting

Eyal Beigman, Gerard Brennan, Sheng-Feng Hsieh, and Alexander J. Sannella

Research Objective

- To develop and theoretically justify a fair value (FV) methodology for proper measurement, classification, and disclosure of investments in cryptocurrencies.

- To review the relevant literature on cryptocurrencies and FV accounting and examine the current guidance available from public accounting firms and standard setters.

- To advocate the use of FV accounting with all unrealized gains and losses recognized in earnings, grounded in the *Conceptual Framework* and precedent accounting guidance.

- To present and exemplify our proposed methodology to **dynamically** determine a principal market and to measure the spot FV for cryptocurrencies.

Current Accounting Guidance for Cryptocurrency Investments

- The Conceptual Frameworks of both the FASB and IASB clearly support the notion that a cryptocurrency is an asset (FASB 2010; IASB 2010). However, transparent financial reporting requires that the economic substance of this resource be properly measured and disclosed.

- Under both U.S. GAAP and IFRS, cryptocurrencies do not meet the definition of cash, cash equivalents, property, or investments in financial assets.

- Current practice indicates that cryptocurrencies are generally considered inventory or a commodity for a broker-dealer and an indefinite-lived intangible asset for an entity investing in cryptocurrencies on its own behalf (CPA Canada 2018; Deloitte 2015; EY 2018a, 2018b; Grant Thornton 2018; KPMG 2018; PwC 2018).

Conceptual Framework

- The objective of financial reporting and the qualitative characteristics of useful accounting information are articulated in the FASB's Concepts Statement No. 8, Conceptual Framework for Financial Reporting (FASB 2010). Under the Conceptual Framework, the fundamental qualitative characteristics that make accounting information useful are **relevance** and **faithful representation**.

- In most cases, there is agreement that the use of FVs in the financial statements better reflects the economic value of an entity's resources and obligations. The use of FV measurement better enables financial statement users to predict future earnings and cash flows and also enhances the confirmatory value of the previously reported information (Barth 2007).

- We argue that cryptocurrencies held by firms on their own behalf and related transactions involving cryptocurrencies should be accounted for under a FV model with all unrealized gains and losses recognized in earnings and classified into "**intangible investment**" asset category from an economic perspective.

Proposed Methodology for Cryptocurrency FV Measurement

Step 1: Assign each exchange for each pair of cryptocurrency a **Base Exchange Score (BES).**

BES is determined by computing a weighted average of the values assigned to four different exchange characteristics

- Exchange oversight
- Microstructure efficiency of exchange
- Data transparency
- Data integrity

$$s_{ex_i}^{BES} = \omega_{ov} \cdot s_{ex_i}^{ov} + \omega_{eff} \cdot s_{ex_i}^{eff} + \omega_{tran} \cdot s_{ex_i}^{tran} + \omega_{int} \cdot s_{ex_i}^{int}$$

$$s_{ex_i}^{ov}, s_{ex_i}^{eff}, s_{ex_i}^{tran}, s_{ex_i}^{int}$$

$\omega_{ov}, \omega_{eff}, \omega_{tran}, \omega_{int}$ – corresponding weights

Step 2: Adjust the BES based on the relative monthly volume each exchange. This new score is the **Volume Adjusted Score (VAS).**

$$s_{ex_i}^{VAS} = \frac{vol_{ex_i}}{\sum_j vol_{ex_j}} \cdot s_{ex_i}^{BES}$$

Step 3: Decay the adjusted score based on the time passed since last trade on exchange. Here, we are assessing the level of activity in the market by considering the frequency of trades. The decay factor reflects the time since the last trade on the exchange. This is the final **Decayed Volume Adjusted Score (DVAS).**

$$s_{T,ex_j}^{DVAS} = e^{-\kappa \cdot |T - \bar{t}_{ex}|} \cdot s_{ex_i}^{VAS}$$

$|T - \bar{t}_{ex}|$ – Time since last transaction on exchange ex_i

$t_{ex_i} = \max\{0 < t < T : \{p_\tau^{ex_i} : t < \tau < T\} \neq \emptyset\}$

κ – decay coefficient

Step 4: Rank the exchanges by the DVAS score and designate the highest-ranking exchange as the **Principal Market** for that time point.

$$ex^{principal} = argmax\{s_{T,ex_j}^{DVAS} : ex_1, \ldots, ex_n\}$$

Step 5: Designate **the price of the last transaction** on the principal market as the **spot FV** at that point of time.

$$p_T = p_{t_{ex^{principal}}}^{ex^{principal}}$$

$ex^{principal}$ – principal exchange

$t_{ex^{principal}}$ – time of last trade on principal exchange

RUTGERS

Rutgers Business School
Newark and New Brunswick

Design of an Evidence Chain to Implement SOX 404

A Prototype for a University's Purchase-to-Payment Process

Jiahua (Edward) Zhou, Alexander Kogan, Michael Alles

- This study developed a modular-based data-driving schema (See Figure 1-1) to assess the quality of internal controls. The design applies the evaluation by investigating error risks (PCAOB, 2004) and discovering the inherent risks of the internal control system. This schema is named evidence chain because of the chain-based evidence accumulation. The schema applies subsequent investigation with the digitized transaction details to look into the effectiveness and efficiency of the operation and controls, instead of testing the configuration of the information systems.

- A potential issue to digitize the whole internal control system is that the space of the database should be big enough to cover all of the activities in reality. This paper tests two actions to ensure the completeness of the digitization. The first is to apply the CobiT 5 as a framework of the transformation. Also, we developed a semantic data model to capture the three essential elements of decision-making in internal controls, including objective, user, and control actions (See Figure 1-2). Control rules provide a platform to improve communication between the managers and auditors. It is approachable to combine two or three operation attributes to compose control rules by using the business rule approach.

- The schema uses benchmarking practice (PCAOB, 2004) to accumulate evidence and discovers inherent risks within the internal control system. The benchmark is the test result of the internal control statement from the management. We apply a rule-based scoring system to have an exhaustive investigation of how the company complies with the control rules from the management statement. A potential issue is that the management's report may have inherent risks if the administration does not employ controls. We applied the multiple correspondence analysis (MCA) to explore potential risk areas of the system. The study validates the design by applying these analytics with a purchase-to-payment process in a state university. The result of the MCA in the case study (See Figure 1-3) shows that there are four risky attributes, including conflict of interests, invoice source, segregation of duties, and payment being later than invoice date. Then, the study confirms these risky attributes by a Welch t-test (See Table 1). This study contributes to the literature and professionals by developing a data-driven solution to provide quantifiable audit evidence for the assessment of internal controls.
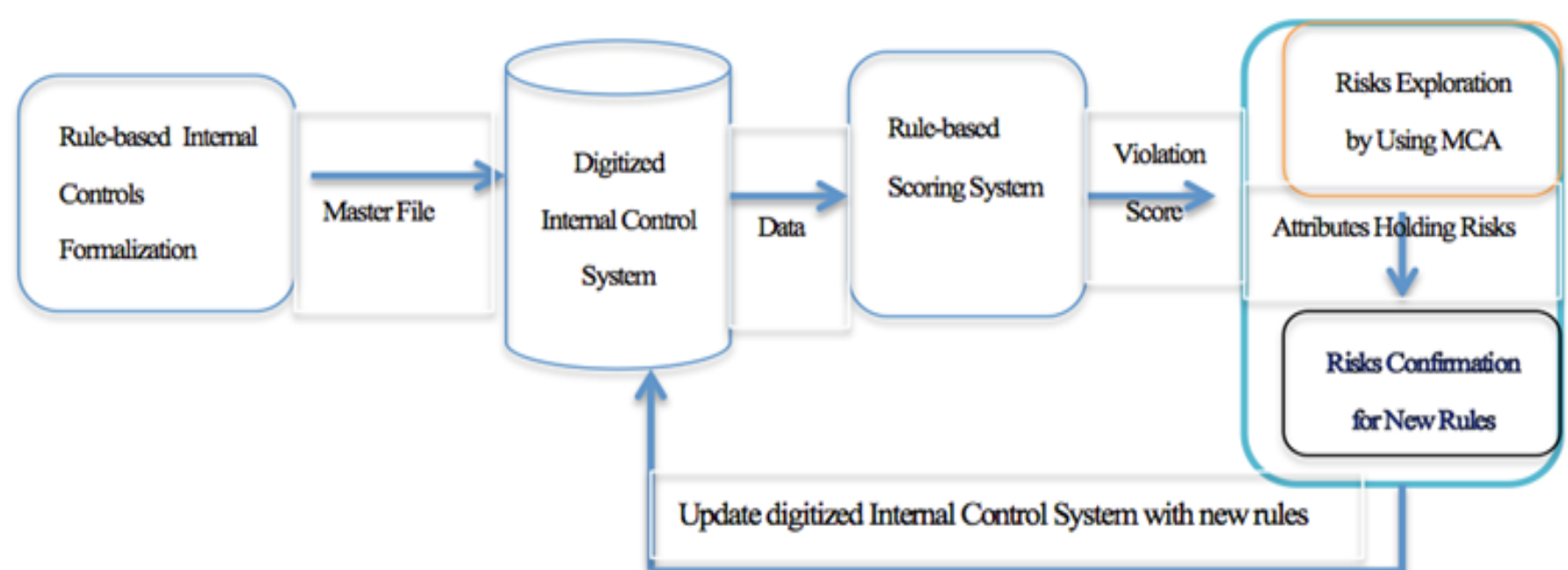

Figure 1-1: The Four Modules of the Evidence Chain

Figure 1-2: The Description of The Master Data of the OUA Model
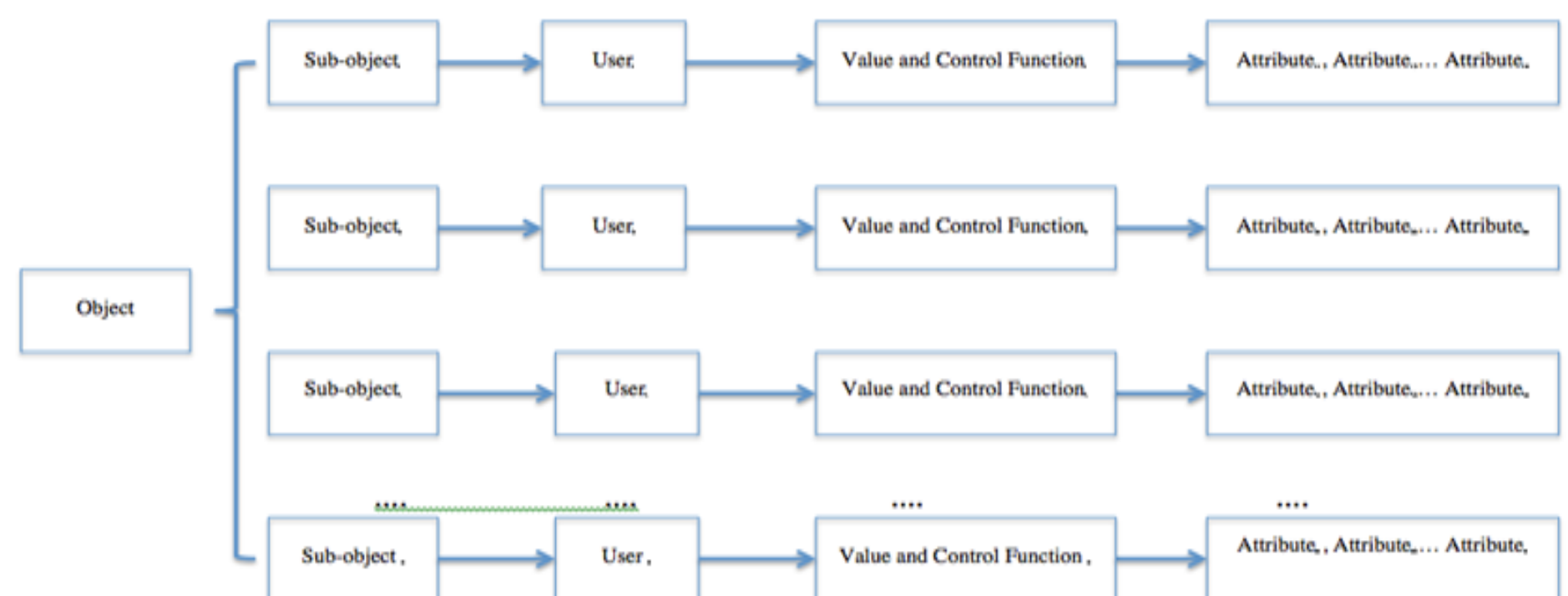
Figure 1-3: The Burt plot of the two dimensions of the MCA
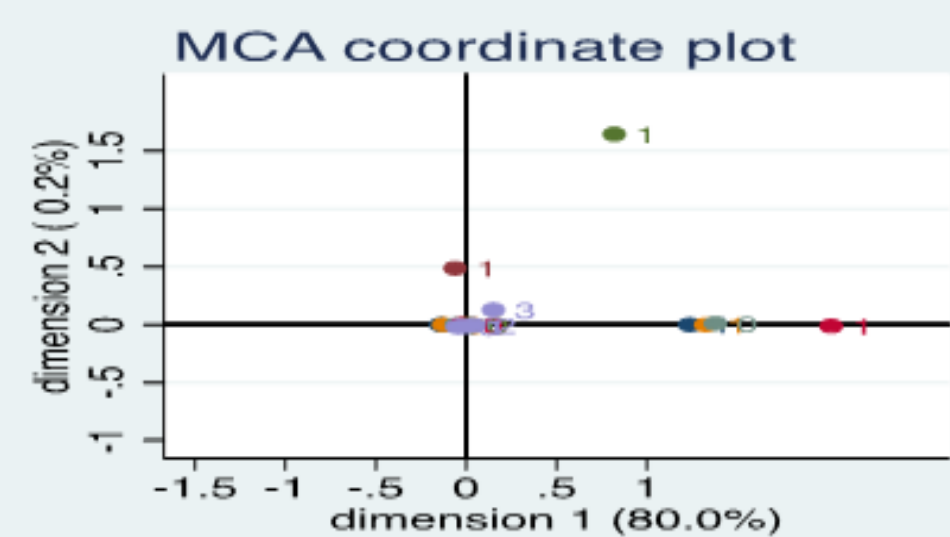
Table 1: Results of the Welch t-test between the Control Groups and the Tested Groups

Potential rules	Violation Score		Transaction Amount	Risk Index
	Z-score	t-statistics	Score	
Rule$_1$: Requestor cannot be the same person as the approver.	-0.5155	-47.24***	1.9724	1.4569 (accepted)
Rule$_2$: The companies owned by active students (casual employees, or part-time employees) have a conflict of interest as an active vendor.	6.48	18.39***	0 (the mean, $1679, is less than the threshold)	2.24 (accepted)
Rule$_3$: If the vendor the invoice is manual type, approvers have to be separated from requestors.	0	-0.97 (The difference is not significant.	2.53	Rejected (The rule-related group cannot meet the first condition.)
Rule$_4$: If the approver has 70% or above transaction with the same vendor, the invoice cannot be manual type.	-0.329	8.25***	2.47	2.041 (accepted)
Rule$_5$: If an approver has 70% or above transaction with the same vendor, the requestor must be different from the approver.	-1.03	9.25***	1.15	0.02 (Rejected)

RUTGERS

Rutgers Business School
Newark and New Brunswick

Examining the Usability of the Comprehensive Annual Financial Report's MD&A using Textual Analytics

Xinxin Wang, Mauricio Codesso and Hussein Issa

Introduction

Comprehensive Annual Financial Report, known as CAFR, is a set of U.S. government financial information including the financial report of a governmental entity that complies with the accounting requirements (GASB statements) by the Governmental Accounting Standards Board (GASB). "Comprehensive" suggesting that CAFRs are comprehensive report to look at the government's financial performance. CAFR more likely is really a snapshot of a government's finances at a given point in time (Walters, 2012). GASB statement No.34 and its amendment Statement No.37 - Basic Financial Statements—and Management's Discussion and Analysis—for State and Local Governments, actually required local governments to include much useful information in their MD&A section. The GASB Chairman characterized the statement as "the most significant change to occur in the history of government financial reporting."

The city of Dixon, Illinois announced the city will receive a $40 million settlement from CliftonLarsonAllen (CLA), Fifth Third Bank, and Janis Card and Associates for the fraud Rita Crundwell committed in twenty years and was not detected by the CPA firms or the bank (Hancox, 2013). Governments faced more criticism from the public because everyone is the stakeholder instead of a small number of shareholders that the corporations have. Everyone wants to know how to measure the usefulness of CAFR to the information users. The usability of information released from CAFRs are not matching with the increasing needs for government accountability and transparency from the public.

The purpose of this study is to measure the usability of the MD&A section in Municipality CAFR to the public. **There are three dimensions of usability include the timeliness, readability, and usefulness.**

Literature Review

GASB No.34 and No.37 Disclosure Requirements

The accessibility of the MD&A section in the financial report includes three dimensions: size, readability, and timeliness (Yusuf & Jordan, 2017). Statement No.34 clearly stated that financial management team are the preparer for the MD&A section of CAFR and financial managers will be asked to share their insights in MD&A by giving readers an objective and easily readable analysis of the government's financial performance (GASB, Governmental Accounting Standards Series Statement No.34, 1999).

Users and usability of the Comprehensive Annual Financial Report (CAFR)

GASB Statement No.1 identified three groups as the primary users of external financial reports: the citizenry, legislative and oversight bodies, and investors and creditors (GASB, 1987).

According to Quesenbery, there are five characteristics of usability – effective, efficient, engaging, error-tolerant, easy to learn – helps guide the user-centered design tasks to the goal of usable products (Quesenbery, 2001).

Textual analysis on MD&A

. Bloch (2016) focused on the information needs of municipal bond analysts as users of the MD&A, while Guo et al. (2009) identified a broader audience of Municipality MD&A readers. Other studies have examined the readability of local government MD&As ((Marsh, Montondon, & Kemp, 2005) (Shannon Lutz. Treba L. Marsh, 2003). Some study examined the timeliness of report issuance or the size of MD&A documents (Yusuf & Jordan, 2017). None of the studies have examined the usability of the MD&A section of CAFR issued by municipality governments in the United States.

## Research Design

Sample Selection and Data Sources

We collected the fiscal year 2014 to 2016 CAFRs for all municipality participants and selected those from New York State. We found 20 municipalities in New York State for Fiscal Year 2015 and 2016.

Methodology

Reporting Leg is the difference between the independent auditor's report issue date and the date of the end of Fiscal Year. This study manually extract the MD&A section of the CAFRs in .txt files and we used both Fog-Index and Flesch–Kincaid to test the readability. This research created a new dictionary based on Loughran and McDonald (Loughran & Mcdonald, 2011) dictionary to classify the positive and negative words because even the Loughran and McDonald dictionary is widely used in textual analysis field, but the content of MD&A section of CAFRs are different from corporate 10K files. Imported the new dictionary into the Linguistic Inquiry Word Count (LIWC) software to calculate the "tone" of MD&A.

Results

Report Leg
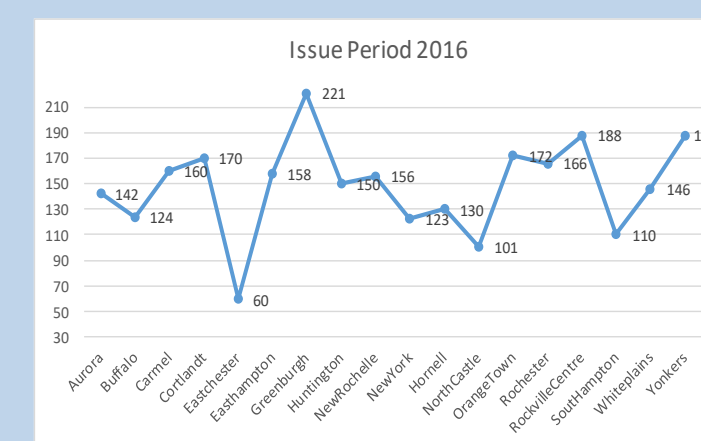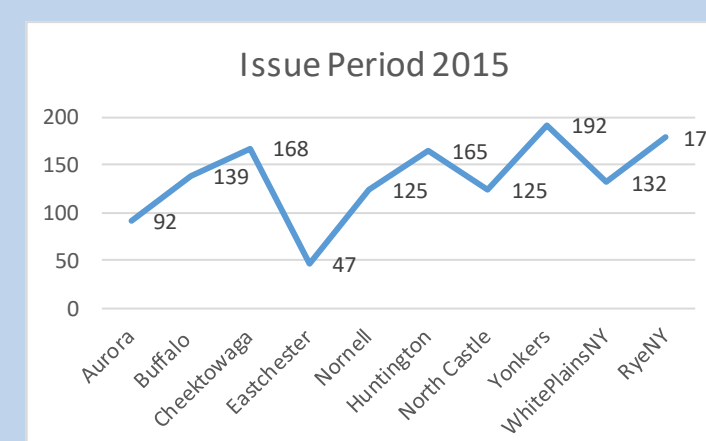
Readability

According to the result, we found that in the fiscal year 2015, the hardest to understand MD&A section among all the municipalities was the city of Yonkers and in the year of 2016, the New York City's MD&A appears to be the one that most hard to understand.

Similarity

The average similarity score is 98.16% (without the Nornell), the outlier of the data. The municipalities using the same templet to prepare their MD&A with changes of numbers every year. In conclusion, the usability of the MD&A of New York State Municipalities in this study is fairly low.

Discussion and Recommendation

- The results of this study show that the poor usability of MD&A of different municipalities in the New York States. MD&A section doesn't help the primary users to understand what is the main content of the MD&A section.

- Our research shows that the same municipality issues the high similarity MD&A in different fiscal years, which indicated the little adjustment made over the years will provide less usefulness to the financial information users.

- A potential recommendation would be require local government to prepare CAFR in XBRL format. In the future, with the help of XBRL, we might be able to analyze the usability of footnotes in CAFRs using the methods that this paper proposed.

RUTGERS

Rutgers Business School
Newark and New Brunswick

Enhancing Audit Team Brainstorming Quality Utilizing Design Thinking

Sheneya Wilson

Fraud Brainstorming

- SAS 99 requires an exchange of ideas or "brainstorming" among the audit team members, about how and where they believe the entity's financial statements might be susceptible to material misstatement due to fraud, how management could perpetrate and conceal fraudulent financial reporting, and how assets of the entity could be misappropriated.

- However, PCAOB inspectors have:

(1) Identified audits in which the audit team was unable to demonstrate that brainstorming sessions were held

(2) Identified audits in which the audit teams' brainstorming sessions occurred after planning and after substantive fieldwork had begun

(3) Identified audits in which key members of the audit team did not attend the brainstorming sessions

(PCAOB 2007)

Literature Review

- Hoffman & Zimbelman (2009) found that modifying auditor work environments by actively encouraging brainstorming (strategic reasoning) was positively associated with the number and quality of audit plan modifications in relation to known fraud risk

Issue With Current Fraud Brainstorming Practices:

- Open discussions are organized and held at the discretion of the audit team leaders allowing for extreme variation

- Checklists have been proven to impair an auditor's ability to assess fraud risk (e.g., Pincus 1989; Hackenbrack 1992; Asare and Wright 2004; Hammersley 2011; Wood 2012)

Design Thinking

- Design Thinking can be defined as a method of problem solving that is used to achieve strategic innovation

- Unlike analytical thinking, which is associated with the "breaking down" of ideas, design thinking is a creative process based on the "building up" of ideas.

- According to Baeck & Gremett (2011), analytical approaches focus on narrowing the design choices, while Design Thinking focuses on going broad.
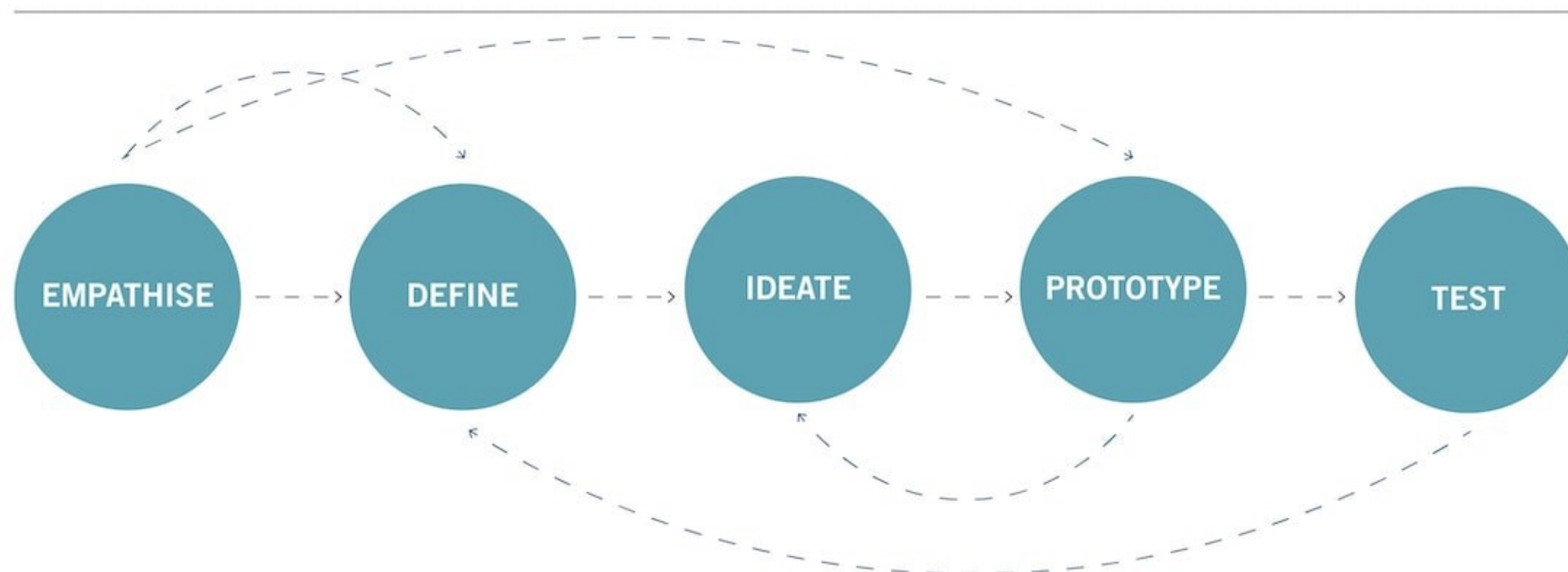
Hypotheses

Hypothesis 1:

Design Thinking auditors will identify more hypothesis about fraud than using open discussion and checklist

Hypothesis 2:

Design Thinking will lead to more conservative fraud risk assessments than using brainstorming or open discussion

5 PHASES OF THE DESIGN THINKING PROCESS

EMPATHISE — DEFINE — IDEATE — PROTOTYPE — TEST

Internal Controls Monitoring and Data Sharing Using Blockchain and Smart Contracts

Jamie Freiman

Internal Controls Monitoring

- An internal control is a process designed to provide assurance as to the reliability of financial information. This information is digested by potential investors, current shareholders, business partner, and other interested stake holders.

- The Sarbanes –Oxley act requires auditors to provide assurance as to the material effectiveness of such internal controls.

- As a result there is a need to effectively and efficiently lock and share internal controls related information amongst many interested parties in a secure environment.

Blockchain and Smart Contracts

- Blockchain is a secure distributed ledger technology. It was developed to share cyber currencies but has been proposed for a variety of business use cases. (Dai & Vasarhelyi 2017,   Kokina et al. 2017)

- Smart contracts are self executing programs designed to operate in a business environment. They are designed to automate monotonous laborious human tasks. When utilized with a blockchain environment these become secure. Adapted from these original uses there are proposals to use smart contracts as monitoring systems. (Maasoumy et al 2015, Watanabe et al. 2015)

Integrated Controls Monitoring

- Blockchain technology can be leveraged to provide a secure, distributable record of internal control related data.

- Smart contracts can be integrated to operate as control checks.

- This system is designed so that smart contracts on the blockchain query databases as well as the blockchain for relevant information. Once they locate the pertinent data they follow a logic path to make a decision on the appropriateness of a transaction. If a transaction is accepted it may be loaded onto the blockchain. If a transaction fails a control check it will not get accepted onto the ledger and related parties will be notified.

- Blockchains can be expensive to run and difficult to query. As a result this methodology limits the usage of the blockchain to only essential functions.

- Utilizing the system can provide time logs of events that can subsequently be used in process mining.

- This framework facilitates the usage of existing controls in an automated and secure data environment.

- Additional controls may be implemented utilizing the features of this framework such as automatically issued authorizations from external businesses when extending additional credit in a B2B environment.

- The diagram to the right illustrates how this may be implemented in the purchase request process for a business. As each stage of the process progresses different external databases are queried to retrieve relevant information. At key checkpoints information is logged in the blockchain which can be located to validate later controls or shared with interested parties.

Process Map for Purchase Request and Authorization
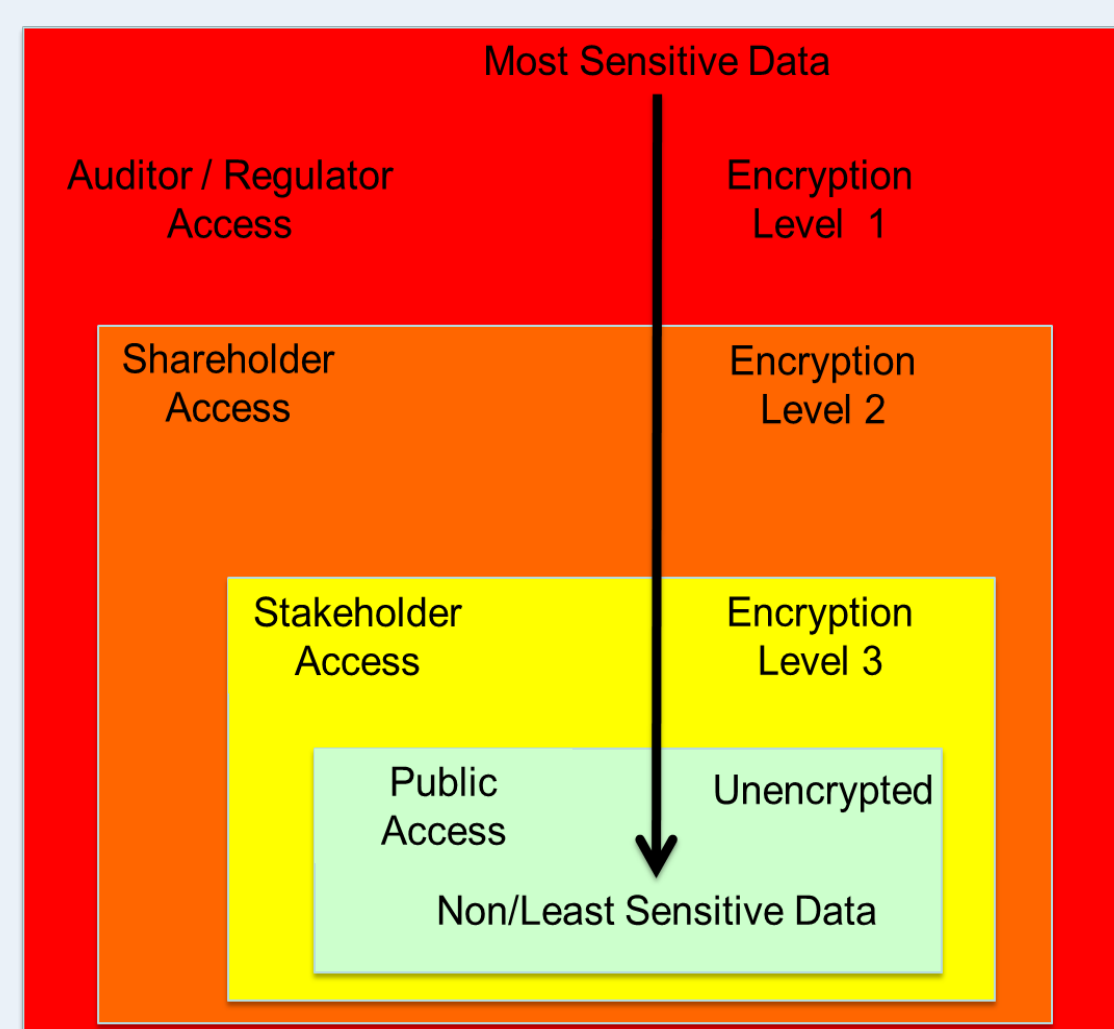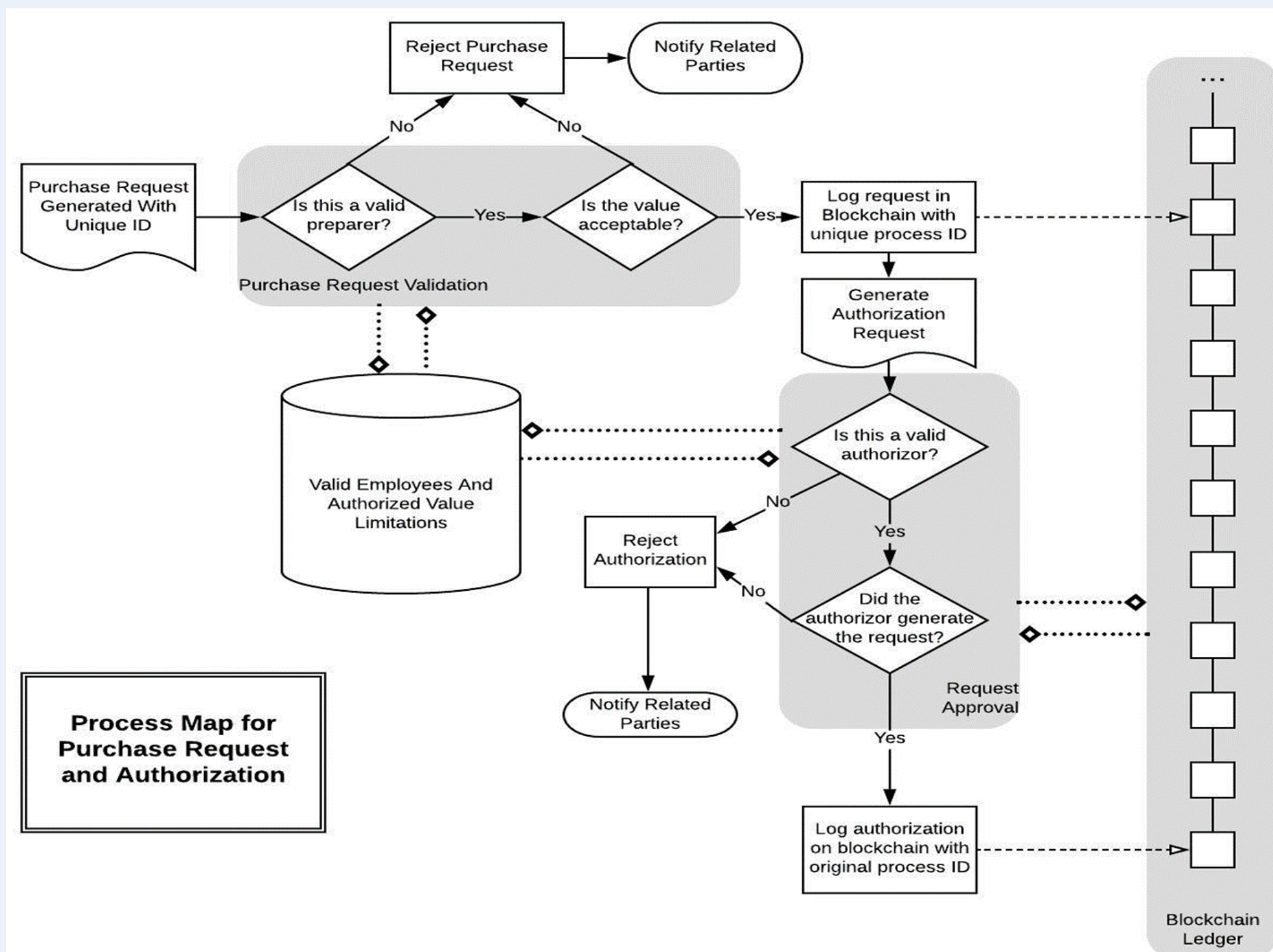
Data Sharing Environment

- In order to facilitate the communication of relevant control data with interested parties there is a proposal for an encrypted data framework.

- While this ledger may be "public" to many parties the company in question may not wish to share data with all individuals.

- To avoid this issue data can be encrypted on different levels. Keys can then be provided to different parties to grant different levels of access.

- Auditors may have all the keys as they are permitted to read all the data. Interested stakeholders such as a bank providing a loan may only be granted access to certain keys.

Limitations and Concerns

- Not all controls are suitable for this type of system. Some controls are impossible to monitor with such a system. For example this cannot be used to monitor independence between a CEO and the board of directors.

- Additionally, controls that are flexible and require frequent management override are not recommended for such a system.

RUTGERS

Rutgers Business School
Newark and New Brunswick

Visual Audit Exploratory Data Analysis: Framework and Demonstration

Lu Zhang, Qi Liu and Heejae Lee

Introduction

- Using interactive visualizations in accounting information systems can assist users understand very large sets of financial information.

- Continuous monitoring and continuous auditing increases the value of interactive visualization in an accounting information system context.

- However, there are only few studies that examine how interactive visualization should be applied in accounting, especially in auditing.

The aim of the study is to:

- Examine how interactive visualization can be used in auditing and suggest a novel framework for visual audit.

- Demonstrate six visual audits using a hospital database with over six million transaction records, namely: (i) visual audit for business understanding; (ii) visual audit for revenue analysis; (iii) visual audit for transaction analysis: (iv) visual audit for receivable analysis; (v) visual audit for internal control tests; (vi) visual audit for audit analytical procedures.

Apply Visual Audit using Exploratory Data Analysis Framework

Upper level: Zoom in approach giving main directions for Visual Audit EDA.
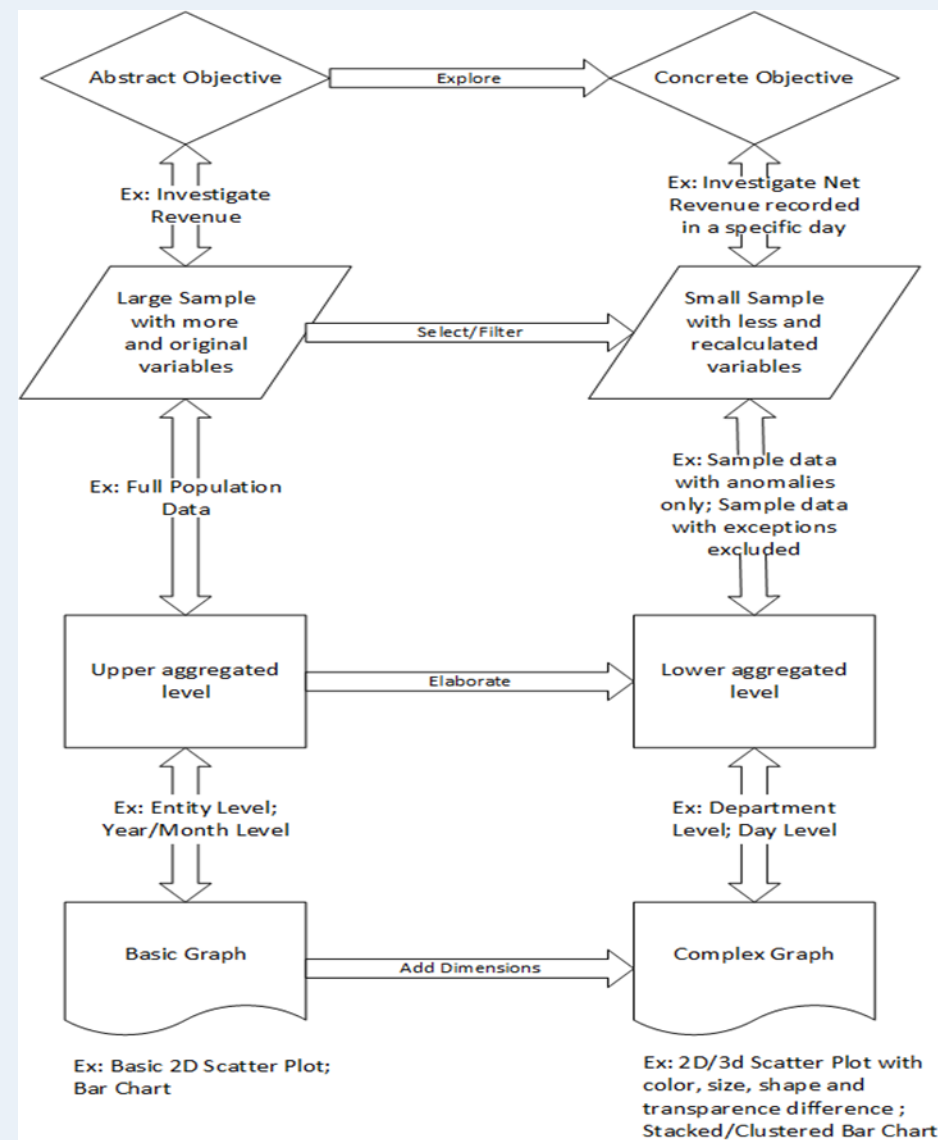
Apply Visual Audit using Exploratory Data Analysis Framework

Lower level: Visual audit loop offering guidance for work sheets generation and dashboards preparation
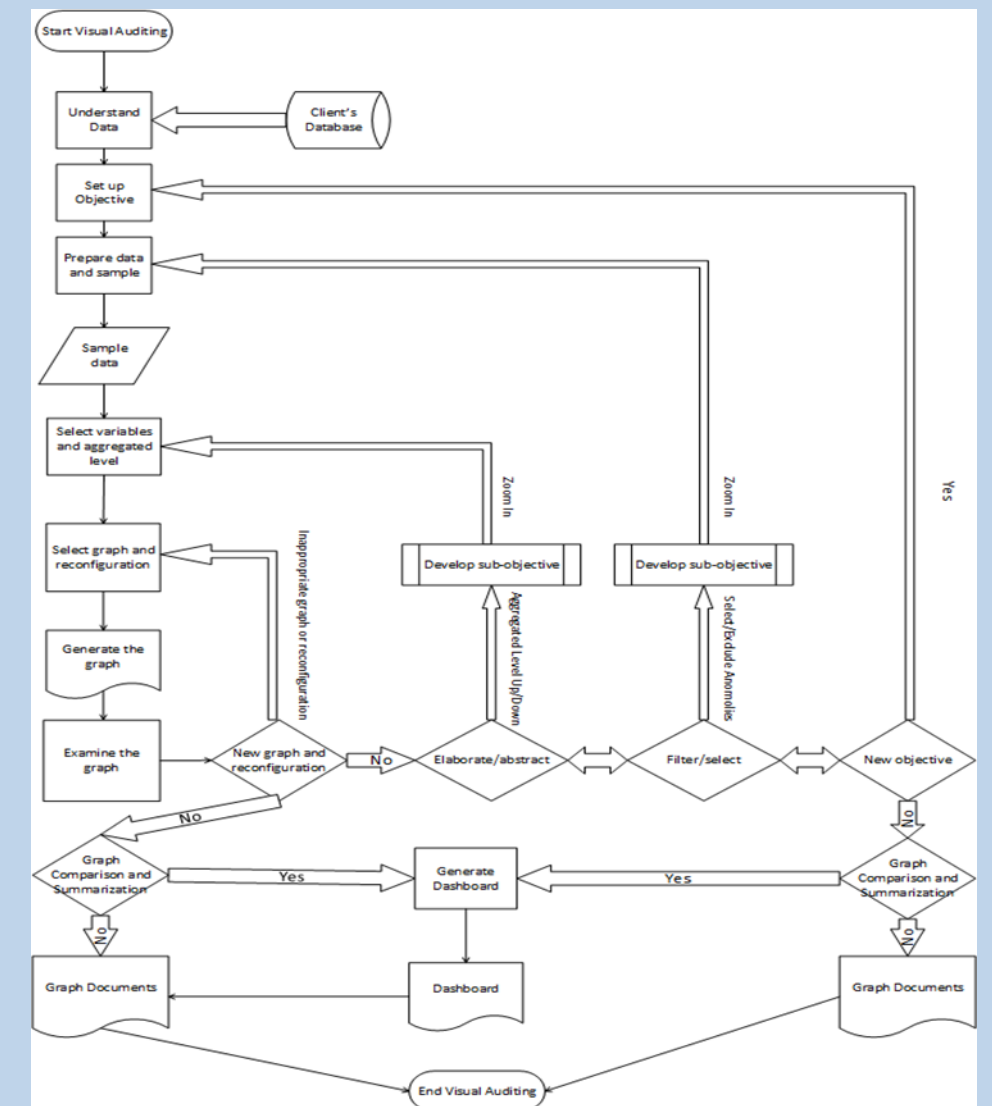
Visual Audit 1: Business Understanding
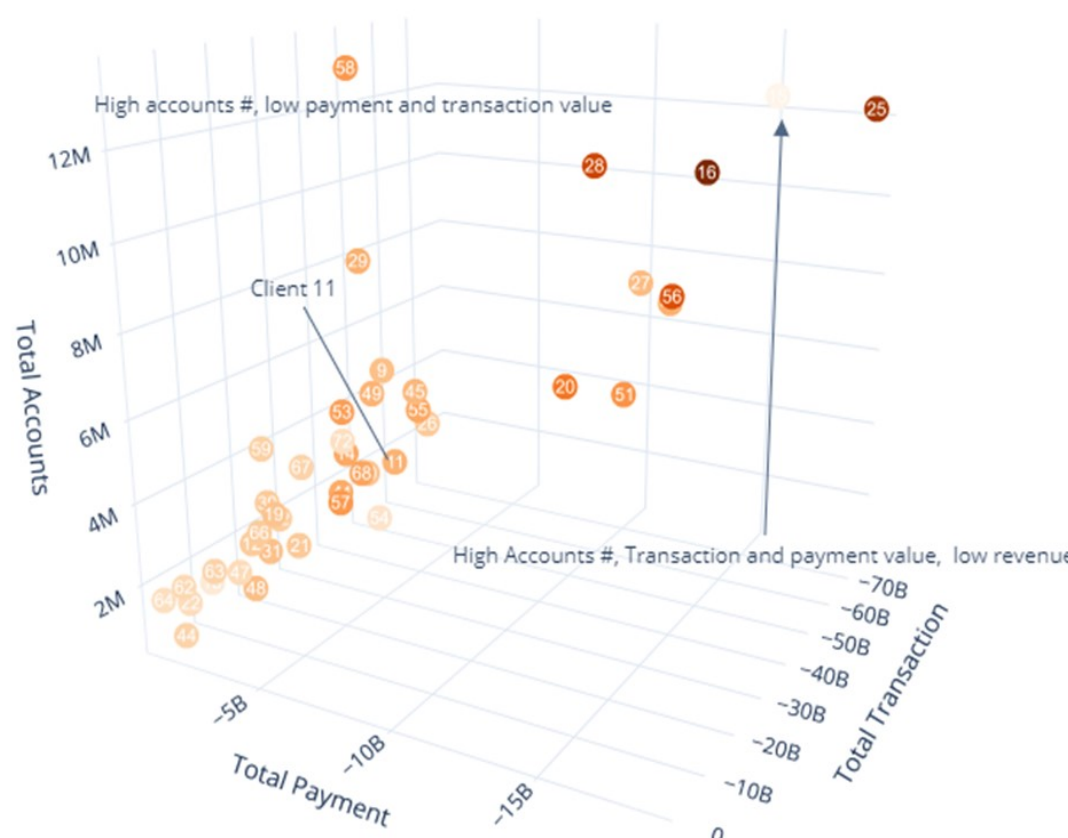
Visual Audit 2: Revenue Analysis
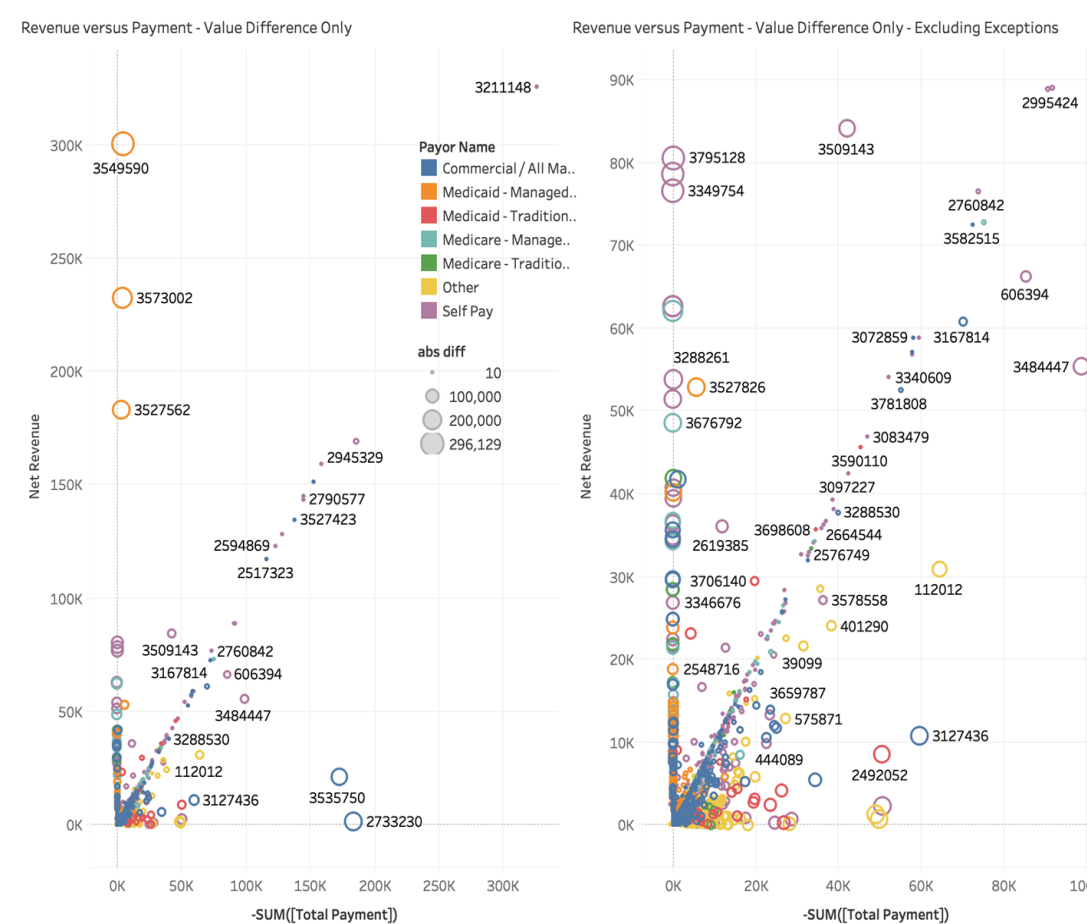
Visual Audit 3: Transaction Analysis
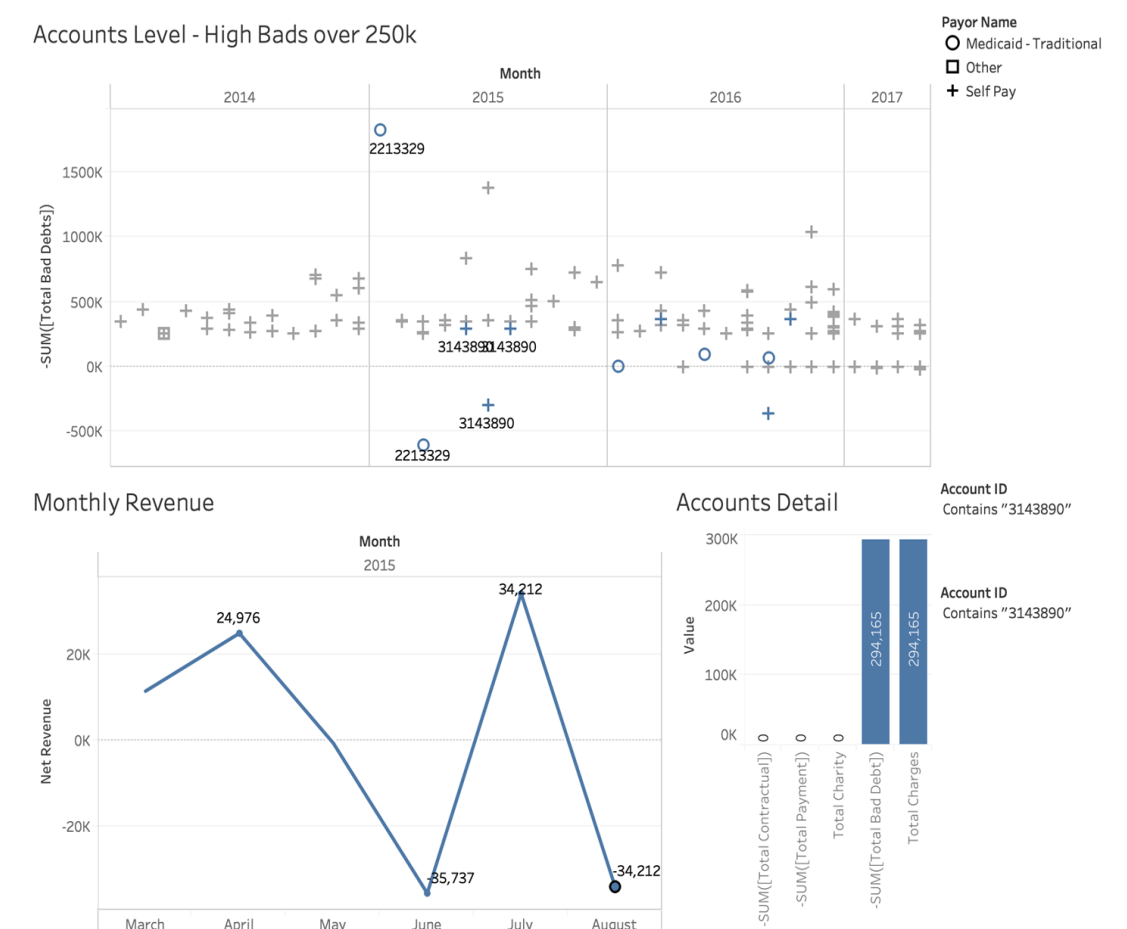
Visual Audit 4: Receivable Analysis
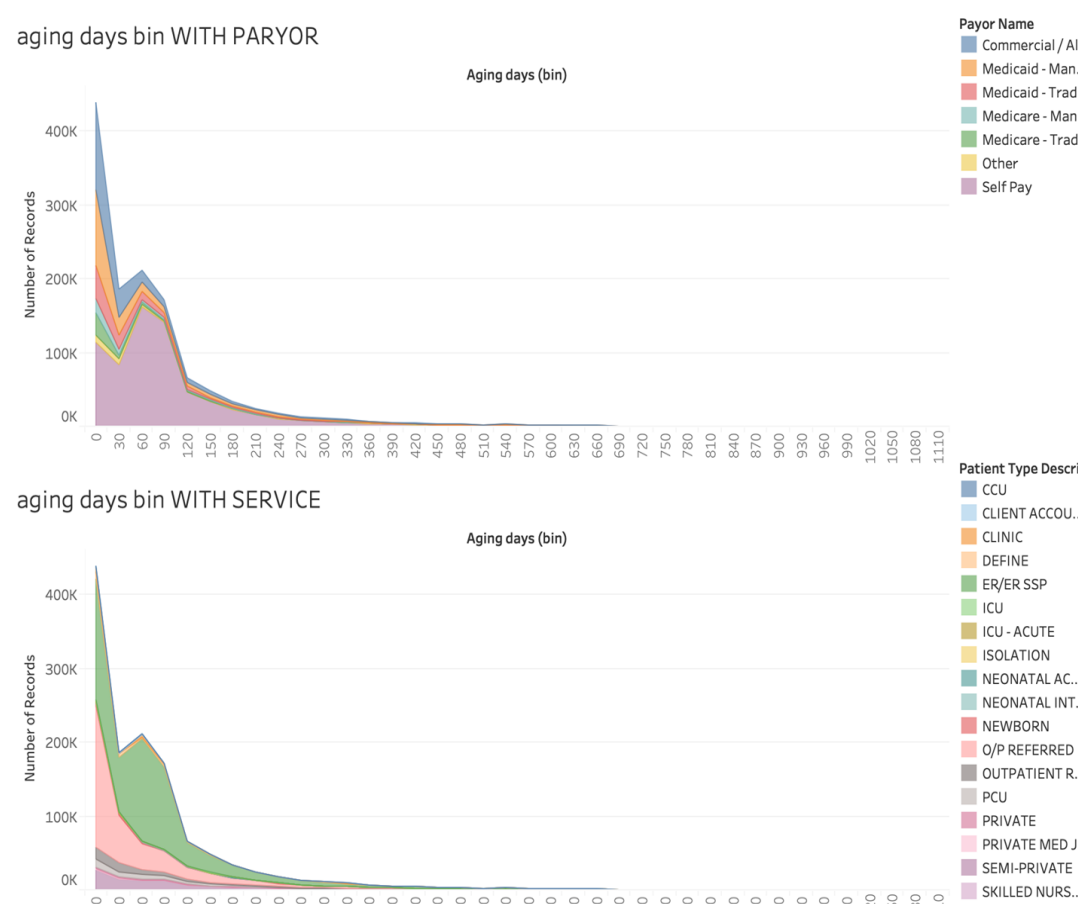
Visual Audit 5: Internal Control Tests
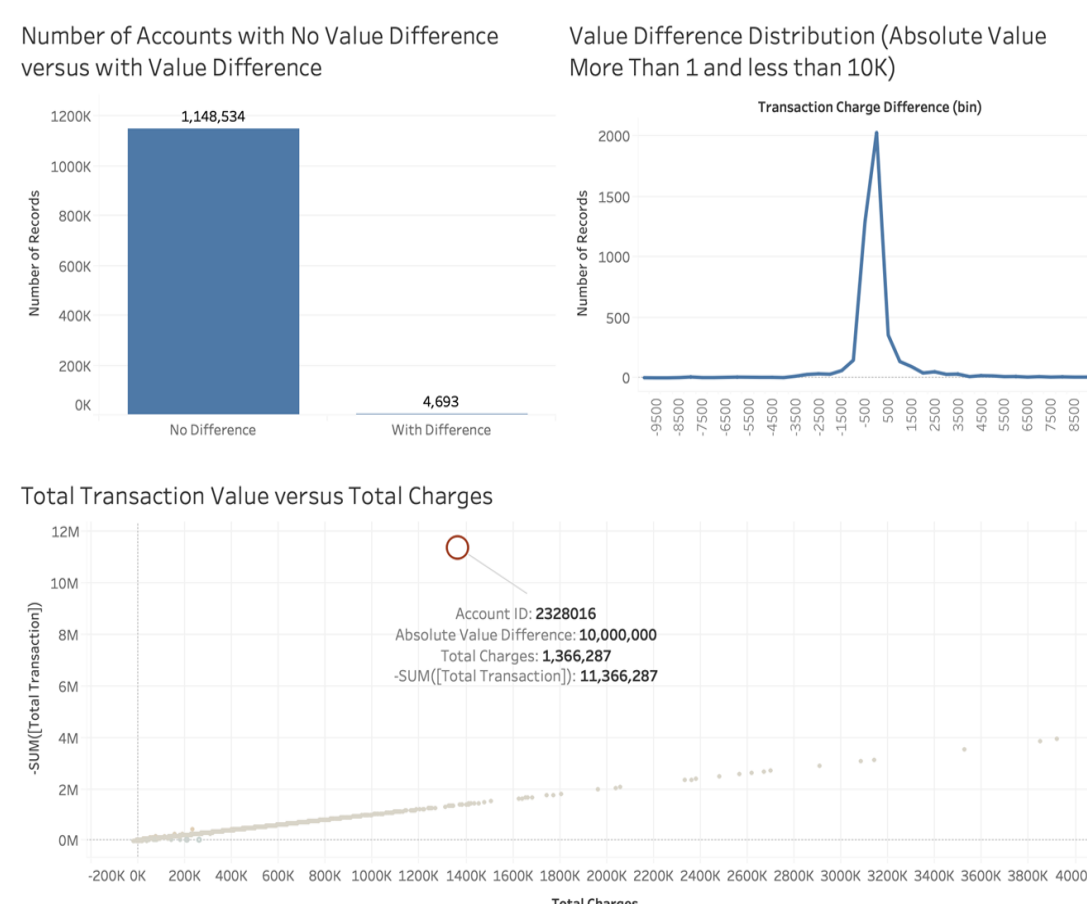
Visual Audit 6: Analytical Procedure
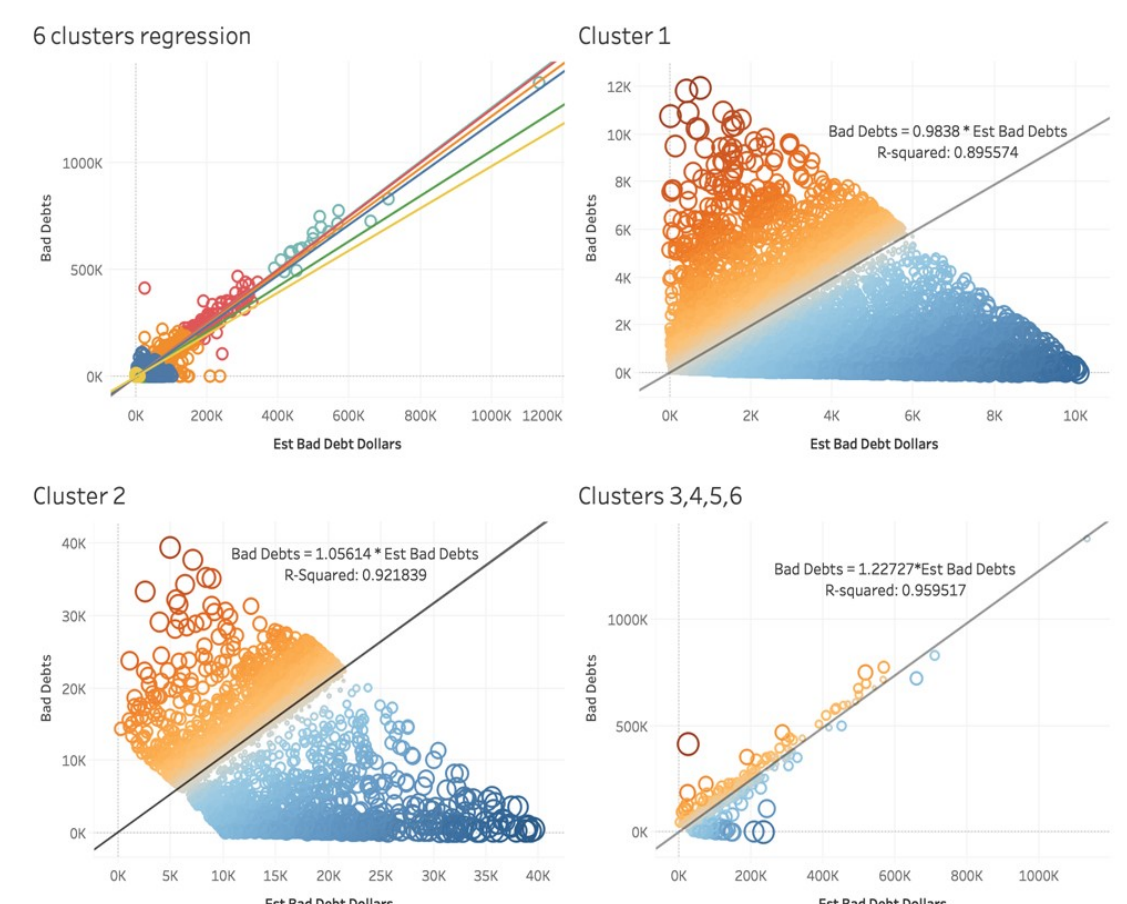
RUTGERS

Rutgers Business School
Newark and New Brunswick

The Ethical Implications of using Artificial Intelligence in Auditing

Ivy Munoko, Helen Brown-Liburd and Miklos A. Vasarhelyi

Technology Analysis

The overall objective of this conceptual analysis is to identify the potential ethical issues that the audit profession should consider as they adopt Artificial Intelligence (AI).

First, at the technology level, this paper considers the features of AI of ethical concern, independent of its current or potential use. At this level, the inherent and consequential ethical risks of the technology are identified.

Key features of ethical concern discussed include: *AI's Intelligence, Computational complexity, Data use* and *Retrieval capabilities*.

Artifact Analysis

Secondly, at the artifact level, this paper considers the "physical configuration that, when operated in the proper manner and the proper environment, produces the desired result" (Brey 2012).

At this level, the paper focuses on the AI artifacts (Assisted AI, Augmented AI and Autonomous AI) independent of their actual applications, and identifies the risks associated with the intended use of these artifacts.

Ethical issues identified at the AI artifact level include: *User autonomy, Accountability, Value-sensitive design, Non-isolation* and *Beneficence.*

Application Analysis

Third, at the application level, the actual use of AI in the audit practice is considered and the possible unintended consequences for the users and other stakeholders.

At this level, the paper focuses on the impact of AI on *audit quality across the practice, auditor skepticism, competence* and *due care.*

Forth, this paper provides: *an evaluation of the potential importance of the issues identified, responsibility assignment, governance assessment* and *policy recommendations.*

Method of analysis

Two technology ethics frameworks are used to perform this assessment: ETICA (Stahl et al. 2010) and ATE (Brey 2012). These frameworks advocate for the use of a bibliometric analysis and ethical checklists to evaluate the ethical implications of the use of emerging technology, given its inherent features, nature, and intended functions.

Procedures followed in this paper

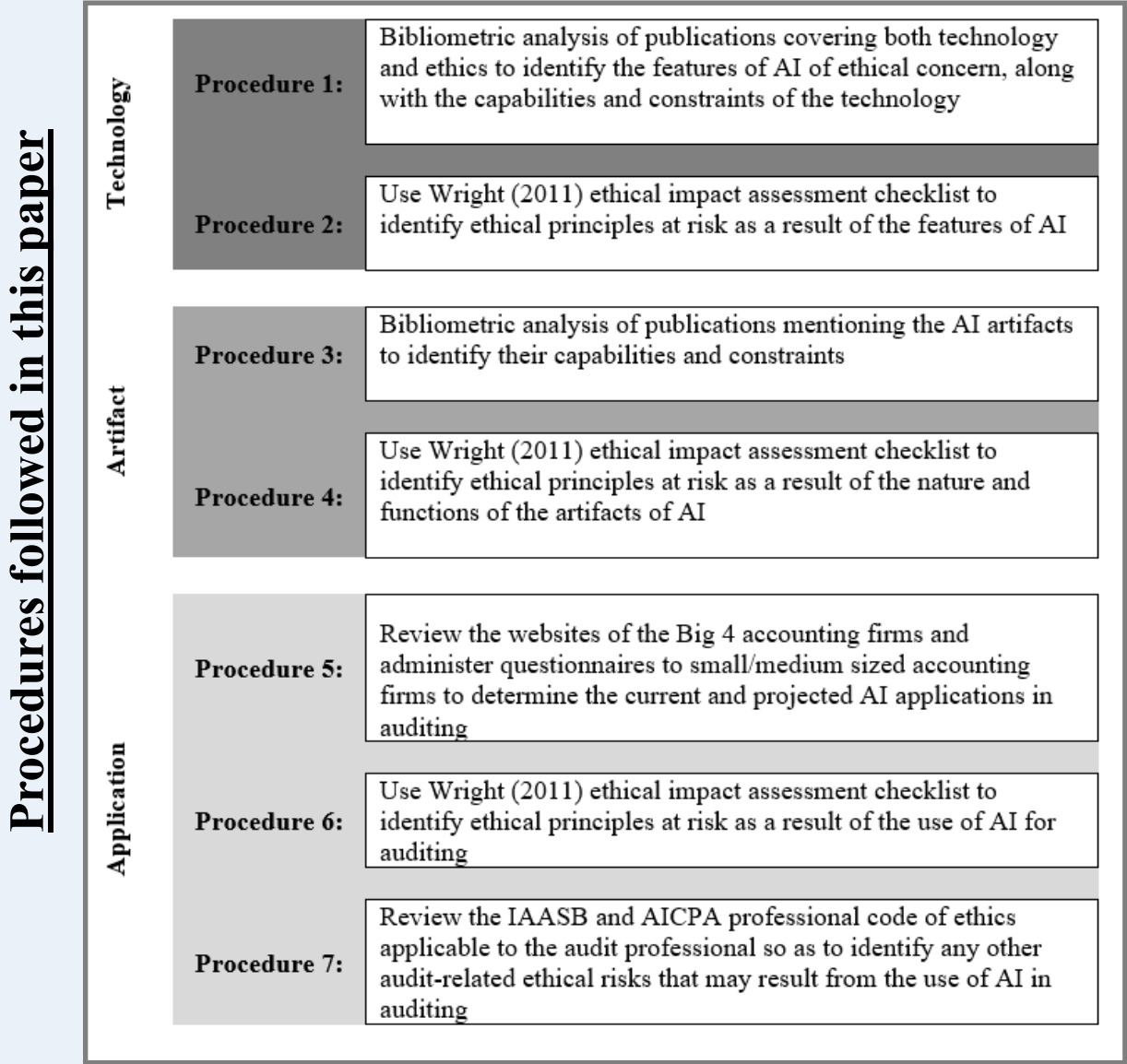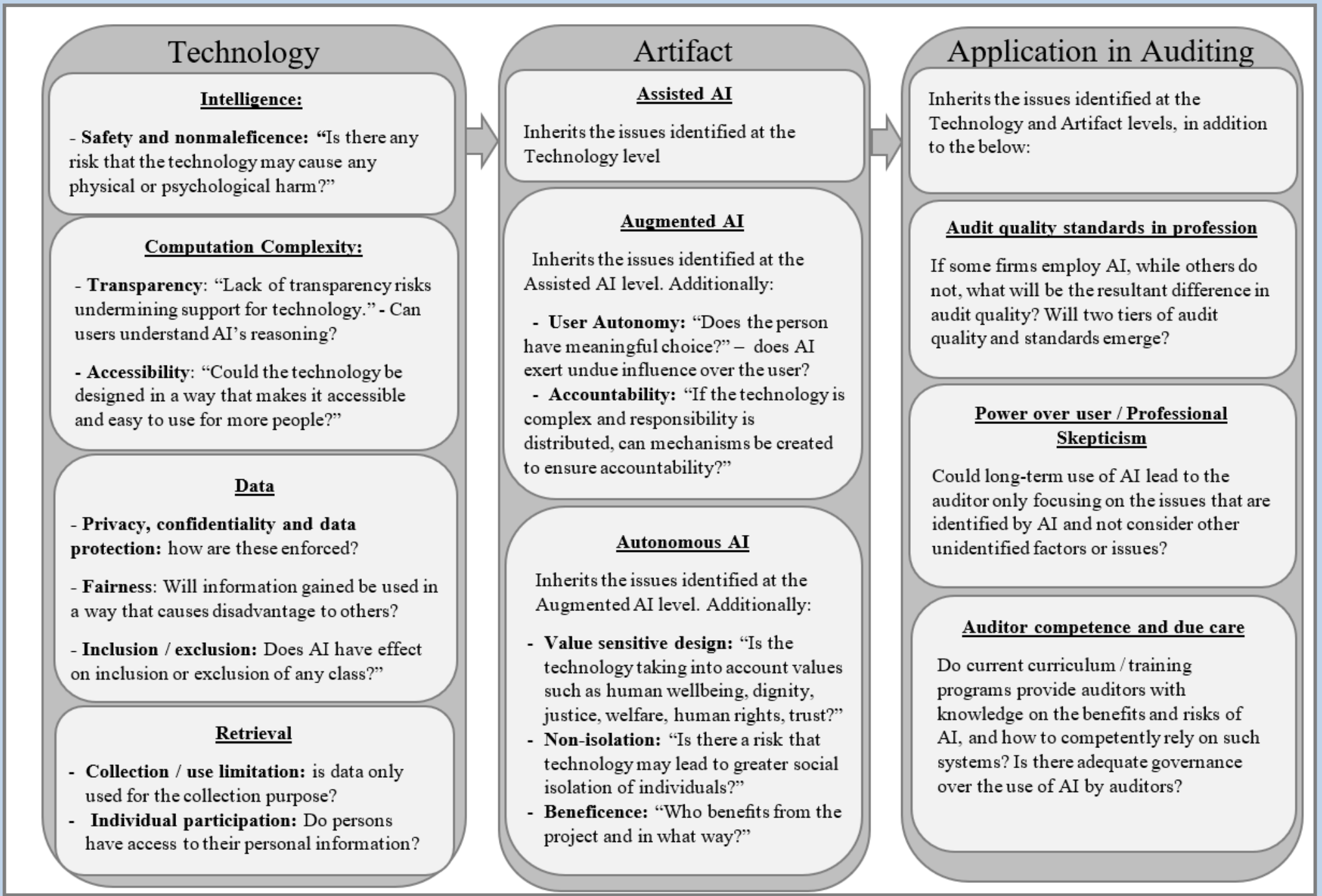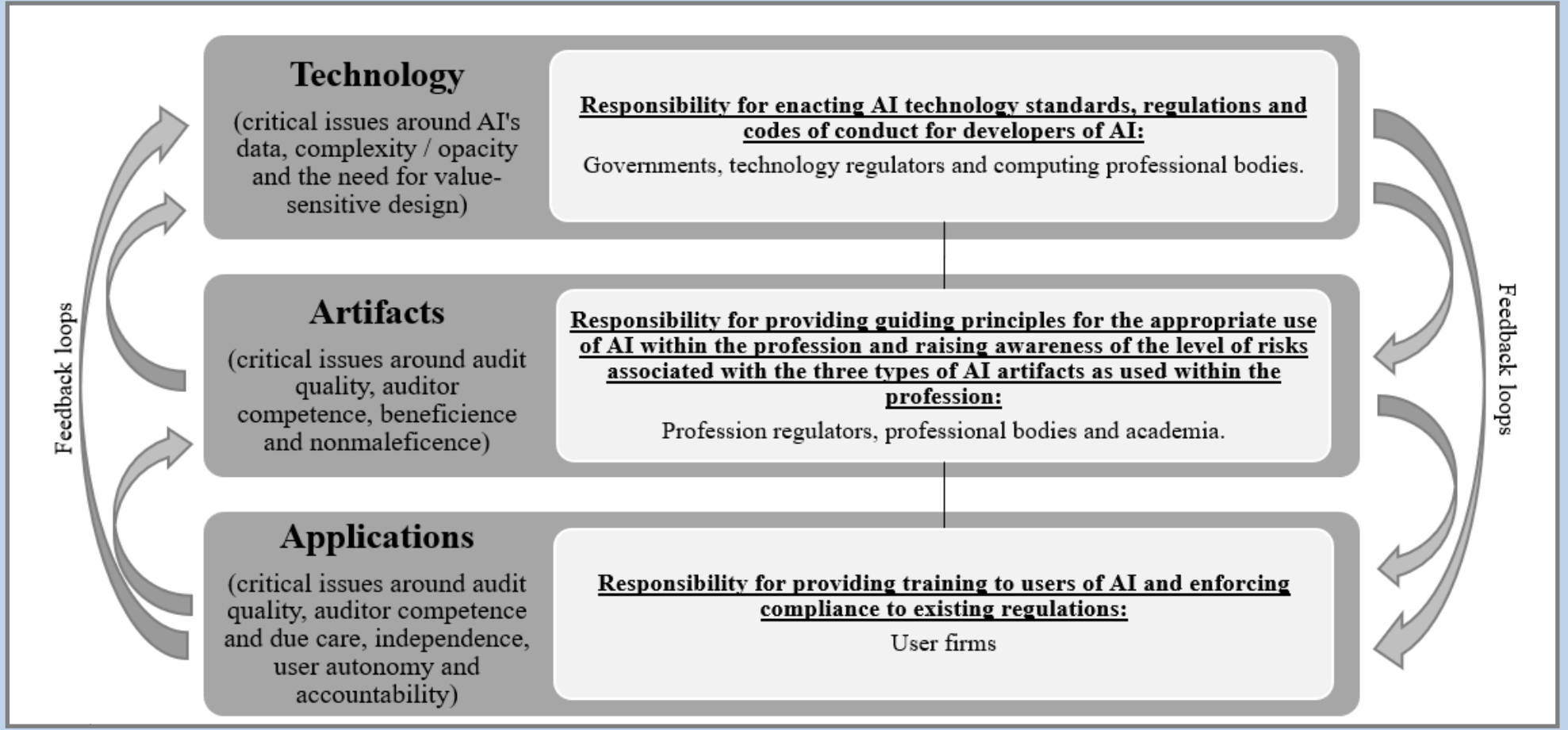|		
Technology	Procedure 1:	Bibliometric analysis of publications covering both technology and ethics to identify the features of AI of ethical concern, along with the capabilities and constraints of the technology
	Procedure 2:	Use Wright (2011) ethical impact assessment checklist to identify ethical principles at risk as a result of the features of AI
Artifact	Procedure 3:	Bibliometric analysis of publications mentioning the AI artifacts to identify their capabilities and constraints
	Procedure 4:	Use Wright (2011) ethical impact assessment checklist to identify ethical principles at risk as a result of the nature and functions of the artifacts of AI
Application	Procedure 5:	Review the websites of the Big 4 accounting firms and administer questionnaires to small/medium sized accounting firms to determine the current and projected AI applications in auditing
	Procedure 6:	Use Wright (2011) ethical impact assessment checklist to identify ethical principles at risk as a result of the use of AI for auditing
	Procedure 7:	Review the IAASB and AICPA professional code of ethics applicable to the audit professional so as to identify any other audit-related ethical risks that may result from the use of AI in auditing

Ethical principles at risk with the use of AI within the Audit Practice

Ethical issues were identified through the bibliometric analysis, the use of the technology checklist by Wright (2011) and the code of ethics for the auditing profession

Technology

Intelligence:

- **Safety and nonmaleficence:** "Is there any risk that the technology may cause any physical or psychological harm?"

Computation Complexity:

- **Transparency:** "Lack of transparency risks undermining support for technology." - Can users understand AI's reasoning?

- **Accessibility:** "Could the technology be designed in a way that makes it accessible and easy to use for more people?"

Data

- **Privacy, confidentiality and data protection:** how are these enforced?

- **Fairness**: Will information gained be used in a way that causes disadvantage to others?

- **Inclusion / exclusion:** Does AI have effect on inclusion or exclusion of any class?"

Retrieval

- **Collection / use limitation:** is data only used for the collection purpose?
- **Individual participation:** Do persons have access to their personal information?

Artifact

Assisted AI

Inherits the issues identified at the Technology level

Augmented AI

Inherits the issues identified at the Assisted AI level. Additionally:

- **User Autonomy:** "Does the person have meaningful choice?" – does AI exert undue influence over the user?
- **Accountability:** "If the technology is complex and responsibility is distributed, can mechanisms be created to ensure accountability?"

Autonomous AI

Inherits the issues identified at the Augmented AI level. Additionally:

- **Value sensitive design:** "Is the technology taking into account values such as human wellbeing, dignity, justice, welfare, human rights, trust?"
- **Non-isolation:** "Is there a risk that technology may lead to greater social isolation of individuals?"
- **Beneficence:** "Who benefits from the project and in what way?"

Application in Auditing

Inherits the issues identified at the Technology and Artifact levels, in addition to the below:

Audit quality standards in profession

If some firms employ AI, while others do not, what will be the resultant difference in audit quality? Will two tiers of audit quality and standards emerge?

Power over user / Professional Skepticism

Could long-term use of AI lead to the auditor only focusing on the issues that are identified by AI and not consider other unidentified factors or issues?

Auditor competence and due care

Do current curriculum / training programs provide auditors with knowledge on the benefits and risks of AI, and how to competently rely on such systems? Is there adequate governance over the use of AI by auditors?

Proposed responsibility mapping for AI use within the Audit Practice

Feedback loops

Technology
(critical issues around AI's data, complexity / opacity and the need for value-sensitive design)

Responsibility for enacting AI technology standards, regulations and codes of conduct for developers of AI:
Governments, technology regulators and computing professional bodies.

Artifacts
(critical issues around audit quality, auditor competence, beneficence and nonmaleficence)

Responsibility for providing guiding principles for the appropriate use of AI within the profession and raising awareness of the level of risks associated with the three types of AI artifacts as used within the profession:
Profession regulators, professional bodies and academia.

Applications
(critical issues around audit quality, auditor competence and due care, independence, user autonomy and accountability)

Responsibility for providing training to users of AI and enforcing compliance to existing regulations:
User firms

Feedback loops

Some Applications of AI in Auditing identified through the survey of CPA firms (ongoing study)

Current Applications

- Risk assessments
- Testing transactions
- Analytics
- Preparing audit workpapers

Anticipated Applications (next 2 years)

- Monitoring and Evaluating internal controls
- Going concern evaluations
- Substituting auditor judgement

RUTGERS
Rutgers Business School
Newark and New Brunswick

Distance Based Suspicion Score
for Audit Data Selection

Nuriddin Tojiboyev, Alexander Kogan

LITERATURE REVIEW

- Kogan et. al. (2014) proposes Transaction Verification as a part of Continuous Audit Framework

- Issa (2013) introduces methodology for outlier prioritization and ranking

- No et. el. (2019) proposes and Multidimensional Audit Data Selection Framework (MADS)

- Most approaches take weights and number of filters into account for prioritization
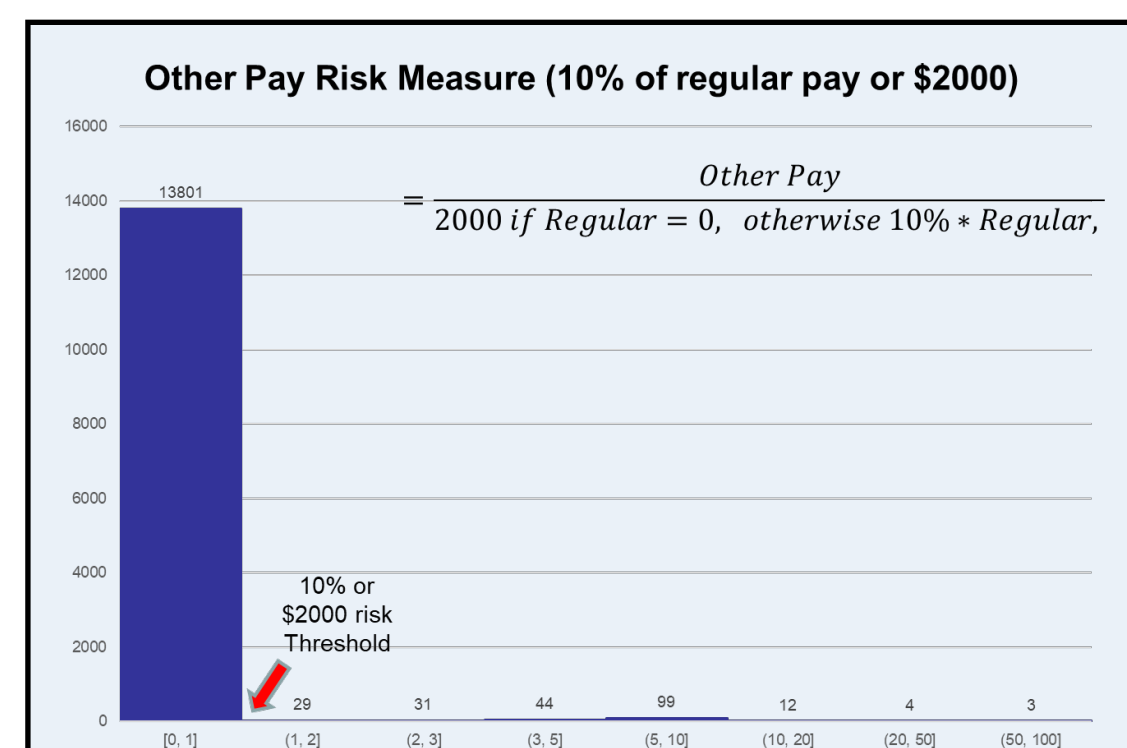
FEATURE

5/29/2019 10:45

Posted Time
HH:MM

Weekday
M, T, W, Th, F, Sa, Su

End of Period
(Yes/No)
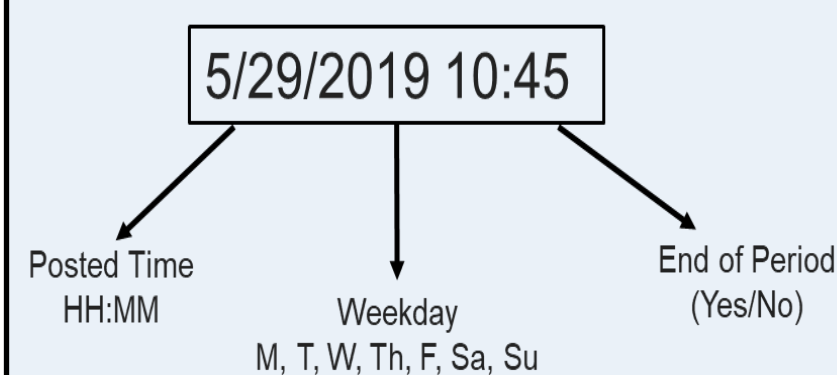
New Approach to Measure Risk

- Under MADS, each assertion is tested through filter(s)

- Under this approach, these filters are engineered into risk features (measures)

- Each transaction in an account or a table is measures with risk features

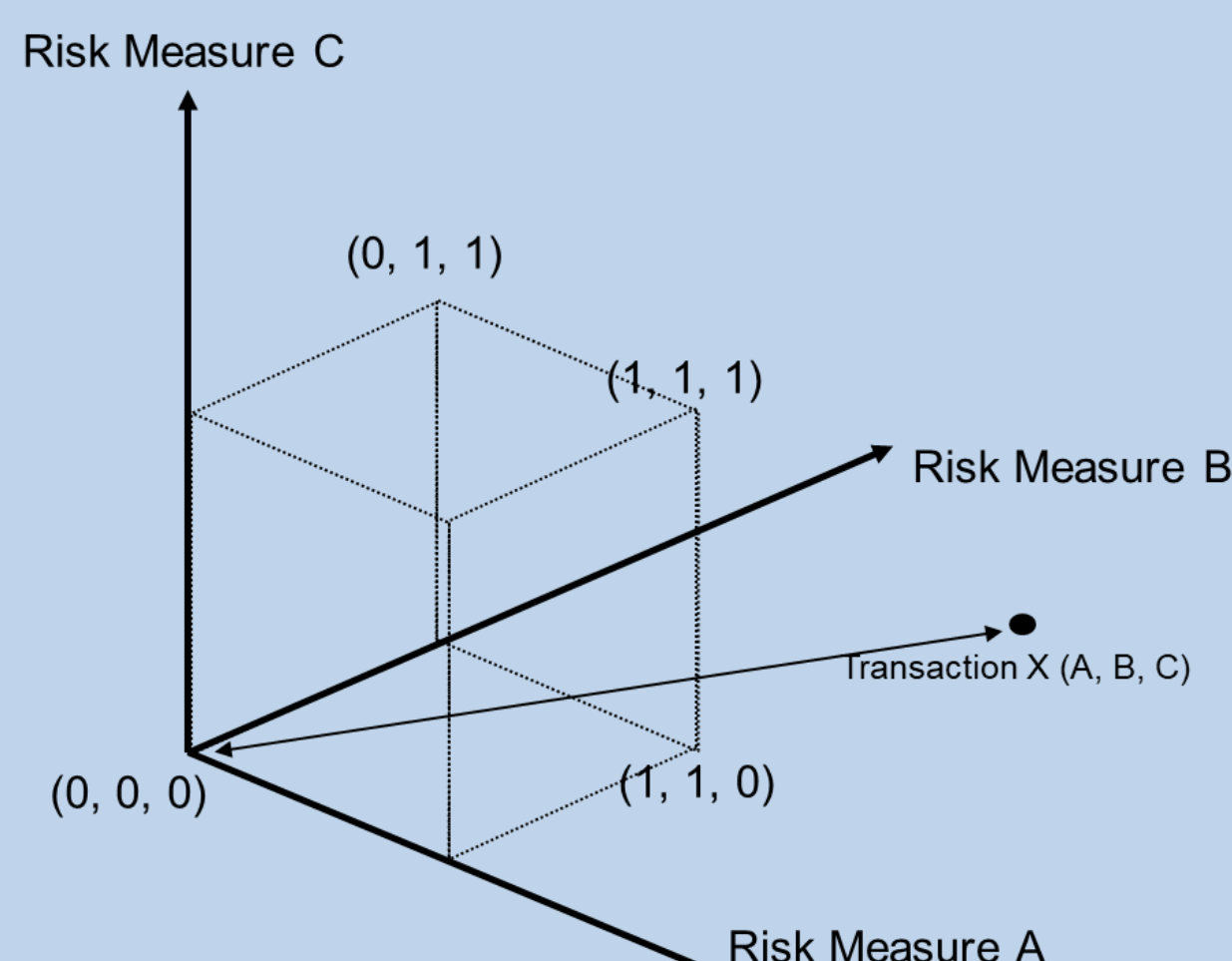- All transactions with their risk measure values are plotted into risk "space"

Filters	Feature
Other Pay > 10%*Regular pay	$= \dfrac{Other\ Pay}{2000\ if\ Regular = 0,\ otherwise\ 10\% * Regular,}$
Overtime > 25%*Regular Pay	$= \dfrac{Overtime}{25\% * Regular}$
Regular > 110%*Salary	$= \dfrac{Regular - Salary}{10\% * Salary}\ if\ Regular > Salary,\ otherwise\ 0$
Regular > 110*Mode(Regular)	$= \dfrac{Regular - Mode(Emp.Reg.)}{20\% * Mode(Emp.Reg.)}\ if\ Regular > Mode(Emp.Reg.),\ otherwise\ 0$
Check Date > Termination Date + 15	$= \dfrac{Check\ Amount}{1000}\ if\ Check > Termination + 15,\ otherwise\ 0$
Count(Check by period) > 1	$= COUNT(By\ Period, By\ Employee) - 1$
If |Hire Date-Check Date|<15: Regular Pay ≥ Salary	$= \dfrac{Regular}{Salary/15} - (Check - Hire)\ if\ 0 < Check - Hire < 13, otherwise\ 0$

Other Pay Risk Measure (10% of regular pay or $2000)

$= \dfrac{Other\ Pay}{2000\ if\ Regular = 0,\ otherwise\ 10\% * Regular,}$

10% or $2000 risk Threshold

Bins	Filter 1	Filter 2	Filter 3	Filter 4	Filter 5	Filter 6	Filter 7
from 0 to 0.5	13785	13794	13990	13497	13925	12977	14002
from 0.5 to 1	16	135	6	248	15	976	0
from 1 to 2	29	67	20	103	13	66	1
from 2 to 5	75	21	7	153	26	4	20
from 5 to 10	99	3	0	21	29	0	0
from 10 to 50	16	3	0	1	12	0	0
from 50 to 100	3	0	0	0	2	0	0
from 100 to 1000	0	0	0	0	1	0	0
	14023	14023	14023	14023	14023	14023	14023

Risk	MIN	MAX	MEAN	MEDIAN	SD	Exceptions (≥1)
Unauthorized Other Pay	0.00	87.69	0.11	0.00	1.41	222
Unauthorized Overtime Pay	0.00	36.26	0.03	0.00	0.39	94
Unauthorized Regular Pay	0.00	3.56	0.00	0.00	0.09	27
Unauthorized Regular Pay Increase	0.00	12.77	0.09	0.00	0.54	278
Check Issue after Termination	0.00	174.38	0.06	0.00	1.82	83
Duplicate Payments	0.00	3.00	0.08	0.00	0.29	1046
Missing Adjustment for First Period of New Employee	0.00	4.00	0.01	0.00	0.14	21

Risk "Space"

Risk Measure C

(0, 1, 1)

(1, 1, 1)

Risk Measure B

Transaction X (A, B, C)

(0, 0, 0)

(1, 1, 0)

Risk Measure A

TranID	Filter 1	Filter 2	Filter 3	Filter 4	Filter 5	Filter 6	Filter 7	Euclidean distance	Manhattan Distance
15	27.69	0.00	0.00	0.00	174.38	0.00	0.00	176.56	202.06
11662	87.69	0.00	0.00	0.00	53.97	1.00	0.00	102.98	142.67
6627	60.00	0.00	0.00	0.00	40.48	1.00	0.00	72.39	101.48
10967	60.00	0.00	0.00	0.00	39.00	1.00	0.00	71.57	100.00
68	9.71	0.00	0.00	0.00	58.58	0.00	0.00	59.38	68.29
4754	36.92	0.00	0.00	0.00	24.87	0.00	0.00	44.52	61.79
3900	36.92	0.00	0.00	0.00	23.73	2.00	0.00	43.94	62.66
449	0.00	36.26	0.00	0.00	0.00	1.00	0.00	36.27	37.26
3901	0.00	0.00	0.00	0.00	34.81	2.00	0.00	34.87	36.81
4942	0.00	0.00	0.00	0.00	29.55	0.00	0.00	29.55	29.55
11193	27.69	0.00	0.00	0.00	0.00	1.00	0.00	27.71	28.69
7843	0.00	0.00	0.00	0.00	27.31	0.00	0.00	27.31	27.31
10468	16.46	0.00	0.00	0.00	0.00	0.00	0.00	16.46	16.46
5400	14.92	0.00	0.00	0.00	0.00	0.00	0.00	14.92	14.92
6271	13.55	0.00	0.00	0.00	0.00	0.00	0.00	13.55	13.55
589	13.44	0.00	0.00	0.00	0.00	0.00	0.00	13.44	13.44

The Informativeness of Cybersecurity Risk Disclosure

Arion Cheong, Soohyun Cho, Won Gyun No, Miklos A. Vasarhelyi

Research Questions:

R1a: Risk topics in firms' cybersecurity risk disclosures are different before and after firms experienced a cybersecurity breach.

R1b: Risk topics in firms' cybersecurity risk disclosure are different before and after firms received an adverse SOX 404 opinion.

R2a: Firms will emphasize vulnerability than control after experiencing a cybersecurity breach.

R2b: Firms will emphasize control than vulnerability after receiving an adverse SOX 404 opinion.

1. Textual Factor Analysis on Cybersecurity Risk Disclosure

We analyze firms' disclosures of cybersecurity risks in the risk factor section (i.e., Item 1A) of 10-K filings (henceforth cybersecurity risk disclosures) and assess the informativeness of the disclosures under two circumstances: after firms experienced a cybersecurity breach and after firms received an adverse SOX 404 opinion. That is, we examine whether firms provide more informative cybersecurity risk disclosures after they experienced a cybersecurity breach and received an adverse SOX 404 opinion. To that end, we first collect 25,344 cybersecurity risk disclosures of 4,952 companies for the period between 2012 and 2017. Next, we identify risk topics in the cybersecurity risk disclosures by applying text analytics. We then group the risk topics by performing an Exploratory Factor Analysis (EFA) to uncover the underlying structure of them. That is, we classify each risk topic into a factor. This results in six factors: business continuation, data regulation, data security, third-party security, network security, and electronic commerce security. Finally, we classify the six factors into two groups: internality and externality. The internality group represents risks coming from a firm's internal system or its business operation. We group business continuation, data regulation, and data security where risks and controls are mostly related to internal factors (e.g., data loss and authentication). On the other hand, the externality group includes third party security, network security, and electronic commerce platform where risks and controls are related to external factors (e.g., third-party software and cloud services).

Factor	Risk Topic	Component	Label	Most Relevant Keywords
Business Continuation	T16	Vulnerability	System Interruption	System, Security, Interruption
	T24	Vulnerability	Service Discontinued	System, Disruption, Customer
	T17	Control	Data Back-up	Repatriation, Duplication, Informatics
	T21	Vulnerability	System Intrusion	Breach, Attack, TPSPS
	T01	Control	Breach Reporting (Whistleblower)	Qui, Tam, Whistleblower
	T03	Vulnerability	System Breach	System, Breach, Technology
	T05	Control	Identification/Detection Model	ROM, DSH, CLO
	T25	Control	Remedial Action	Remediate, Imperfection, Azusa
Data Regulation	T06	Vulnerability	Violation of Data Regulation	Information, Security, Regulation
	T27	Vulnerability	Privacy Law	Privacy, Law, Regulation
	T30	Vulnerability	Violation of HIPAA	Privacy, Health, Breach
	T02	Control	Regulation Compliance	Regulation, Compliance, Guidance
Data Security	T07	Vulnerability	Litigation Cost (Data Breach)	Litigation, Cost, Loss
	T08	Vulnerability	Data Loss	Data, Information, Loss
	T23	Control	Access Control	Onesign, Authentication, Control
	T29	Vulnerability	Data Breach	Information, breach, security, loss
	T04	Control	Intrusion Prevention	NGIPS, SM, Fingerprint
	T15	Vulnerability	Reputation Loss	Reputation, Loss, Customer
Third-Party Security	T13	Vulnerability	SCM Data Leak	Data, Breach, TPSPS
	T10	Control	Supply Chain Security	CRD, RSD, ELA
	T14	Control	SCM Risk Mitigation	Fluctuation, Remediate, PGE
Network Security	T18	Vulnerability	Network Breach	Security, Breach, Network
	T22	Control	Network Security	IoT, Internet, IPSec
	T19	Control	Countermeasures for Network Security	Instrument, logon, hacktivists
Electronic Commerce	T20	Control	e-commerce Assurance	Websense, Auditing, CLO
	T28	Control	Transaction Platform Security	RSD, CRD, Tract

2. Contextual Changes of Cybersecurity Risk Disclosure

Among 30 topics, the confirmatory factor analysis results shows that only 16 topics displayed below loaded significantly to the high-order construct (i.e. *Breach*, and *ICW*). Further, followed by regression analysis with fixed effects, only Regulation Compliance (Topic 2), Data Loss (Topic 8), and Transaction Platform Security (Topic 28) had significant correlation to the high-order construct. The result has shown breached firms disclose about their cybersecurity incident (Topic 8) due to the required regulations. Notably, they have significantly reduced their disclosure on control (Topic 2) while disclosing more toward their vulnerability related to the data loss incident (Topic 8). However, ICW reported firms (adverse SOX 404 opinion related to cybersecurity) have disclosed less about their internal regulation compliance (Topic 2) while more about the security control which is regulated by external third-parties (Topic 28).

Dependent Variables			Label	Breach		ICW	
Factor	Risk Topic	Component		Estimates	t-statics	Estimates	t-statics
Business Continuation	Topic 16	Vulnerability	System Interruption	-.004	-.97	.005	1.43
	Topic 24	Vulnerability	Service Discontinued	-.000	-.12	.002	.79
	Topic 21	Vulnerability	System Intrusion	-.000	-.10	.002	.93
	Topic 03	Vulnerability	System Breach	-.002	-.47	-.001	-.55
	Topic 05	Control	Identification/Detection Model	.000	.05	-.005	-1.64
	Topic 25	Control	Remedial Action	.003	1.05	.003	1.20
Data Regulation	Topic 30	Vulnerability	Violation of HIPAA	.005	1.53	.000	.31
	Topic 02	Control	Regulation Compliance	-.007	-1.75*	-.007	-2.32**
Data Security	Topic 08	Vulnerability	Data Loss	.007	1.78*	-.000	-.12
	Topic 29	Vulnerability	Data Breach	.001	.36	-.000	.01
	Topic 15	Vulnerability	Reputation Loss	.000	.23	-.002	-1.24
Third-Party Security	Topic 14	Control	SCM Risk Mitigation	.000	.01	.002	.74
Network Security	Topic 18	Vulnerability	Network Breach	-.000	-.13	-.003	-1.25
	Topic 22	Control	Network Security	-.007	-1.57	.005	1.31
	Topic 19	Control	Countermeasures for Network Security	.001	.27	-.003	-1.12
Electronic Commerce	Topic 28	Control	Transaction Platform Security	-.005	-1.22	.009	2.52**
Firm and Year Fixed Effects			Included				
# of Observations			8,181				

3. Negative Effect of Disclosing Cybersecurity Incident

We further investigate two risk topics (i.e., Topic 2 and T) by comparing the potential negative effect resulting from disclosing each topic. The negative effect is proxied by the recipient of ICW opinion which is an effective and observable negative signal imposed to the firm. In particular, we perform a 2-Stage Least Square (2SLS) regression analysis to compare the negative effect of two risk topics. The test is intended to examine further whether breached firms disclosed more about their data breach incidents than their control toward regulation compliance even it is likely to impose more negative effect. The results show that firms with higher disclosures on Data Loss (Topic 8) and Data Regulation (Topic 2) have a higher possibility to receive an ICW opinion. This suggests that even though firms have a higher probability of receiving future ICW opinion, they tend to report more data loss incidents and regulation compliance issues in their disclosures, suggesting that the SEC guidelines affect firms' cybersecurity risk disclosures.

Dependent Variable (ICW)	Estimates	z-statistics	P>|z|
Data Loss (Topic 8)	2.988	2.08	0.037
Data Regulation (Topic 2)	.792	1.88	0.060
Constant	-1.909	-2.03	0.044
Firm Fixed Effects	Included		
Year Effects	Included		
# of Observations	8,181		

Conclusion

Examining the informativeness of firms' cybersecurity risk disclosures is crucial since the disclosures are the primary source where stakeholders rely on and gauge the cybersecurity risks of the firms. Our results show that firms' cybersecurity risk disclosures differ after they experienced a cybersecurity breach and after they received an adverse SOX 404 opinion. Furthermore, we find that firms disclose limited but relevant contents related to their cybersecurity breaches to inform their stakeholders. Our study contributes to the existing literature by providing a methodology to identify risk topics in the cybersecurity risk disclosures while grouping the topics into six major factors. The decoding process is critical since assessing firms' cybersecurity risks should start with identifying their vulnerability (i.e., risks) and evaluating the effectiveness of cybersecurity risk countermeasures and controls for each factor that we have identified. We argue that the segmentation is more intuitive to practitioners to understand the nature of cybersecurity risk disclosures. Future studies may benefit by analyzing the mitigation effect of disclosed controls on different types of cybersecurity breaches.

Contact Information:
Arion Cheong
e-mail: arion.cheong@rutgers.edu

RUTGERS
Rutgers Business School
Newark and New Brunswick

Designing a Classifying System for Non-profit Organization with Textual Contents in The Mission Statement

Heejae Lee, Xinxin Wang, and Richard Dull

Abstract

Classifying Non-profit Organizations (NPOs) helps all stakeholders (including donors, management, researchers, policy-makers and other interested parties) understand the characteristics of NPOs. Since the National Center for Charitable Statistics (NCSS) developed the National Taxonomy of Exempt Entities (NTEE) code, NPO stakeholders generally rely on the NTEE classification to categorize nonprofit entities. However, many researchers argue that the NTEE codes do not fully represent the mission and activities of NPOs, resulting in the NTEE system's inadequate identification of NPOs pursuing similar objectives. The mission statement of NPOs has the potential to improve the classification system since it disseminates the purpose of the NPO, both internally and externally.

The purpose of the current study is to design a new classification method to categorize NPOs using the textual content of their mission statement. The result show that Xgboost classifier and Multinomial Naïve Bayesian classifier have lower false negative rates than NTEE. Also, Xgboost classifier has a lower error rate than Multinomial Naïve Bayesian classifier and NTEE. A new classification algorithm using NPOs' mission statements allows us to draw a larger sample of "Housing & Shelter" organizations compared to the NTEE code. In conclusion, the mission statement has the potential to improve the traditional classification system of NPOs.

Introduction

What is the problem?

The NTEE code has been widely used to categorize NPOs for decades (Fyall, Moore, & Gugerty, 2018). However, empirical evidence shows that NTEE codes do not always represent an organization's mission and activities (Fyall et al., 2018; Turner, Nygren, & Bowen, 1993).

Why this research is important?

Identifying peer groups and comparing peers can enable the evaluation of financial performance of NPOs, and detect (and predict) abnormal financial events.

Research Question

Can a new classification system using the textual content in the mission statement of NPOs work better than the current NTEE classification?

Table 1 Data Preparation

	Numbers
Whole Population from Form 990 database	80,631
Not available in Current Master NTEE Lookup file	4,847
Duplicate EIN code	239
'see schedule' in the mission statement	866
'see part iii' in the mission statement	220
'attachment' in the mission statement	46
'501' in the mission statement	1,028
Mission Statement is Missing	2
Final Sample Size	73,385

Methodology

Data Collection

We linked Form 990 database and "Current Master NTEE Lookup file" from NCCS Data Archives using Employer Identification Number (EIN).
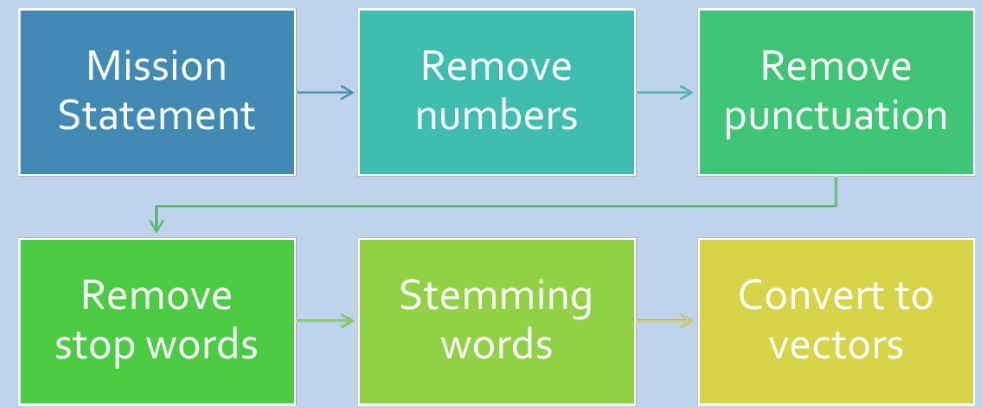
We labeled those organizations which have either keywords related to 'Housing & Shelter' in their mission statement or classified as 'L' in NTEE system.

Keywords Lists
affordable hous, emergency shelter, group home, homeless, homeowner, low income homeown, low house, rental house, home ownership, affordable home, apartment, low income home, home owner, rental, residential, build home, living facility, low income house, senior house, housing, homelessness(exclude if the mission have 'animals', 'pets', or 'dogs' in their mission)

We randomly split the data into training (80%) and testing data (20%).

Data Preprocessing

Mission Statement → Remove numbers → Remove punctuation → Remove stop words → Stemming words → Convert to vectors

Result

We compared Xgboost, and Multinomial Naïve Bayesian classifier to NTEE classification. Xgboost classifier and Multinomial Naïve Bayesian classifier showed lower false negative rate (15%) than NTEE (40%). Also, Xgboost classifier showed lower error rate (higher accuracy rate) (2.5%) than Multinomial Naïve Bayesian classifier (6.5%) and NTEE (4.9%)

Table 2 Descriptive Statistics of Testing and Training Sample

	Training	Testing
Total	58,706	14,677
Housing & Shelter	7,293	1,629
'L' organizations	4,364	1,098
% Housing & Shelter	12.4%	11.0%
% 'L' organizations	7.4%	7.5%

Table 3 Classification Report

	Precision	Recall	F1-Score
Multinomial Naïve Bayesian			
No	**0.98**	0.95	0.96
Yes	0.70	0.85	0.76
XGboost			
No	**0.98**	0.99	0.99
Yes	0.95	0.85	0.90
NTEE code			
No	**0.95**	1.00	0.97
Yes	1.00	0.60	0.75

Table 4 Confusion Matrix of Multinomial Naïve Bayesian, XGboost, and NTEE

Label \ Predict	Multinomial Naïve Bayesian			XGboost			NTEE code		
	No	Yes	Error	No	Yes	Error	No	Yes	Error
No	12193	668	5%	12772	89	0.6%	12861	0	0%
Yes	280	1536	**15%**	272	1544	**15%**	718	1098	**40%**

Conclusion

Comparing financial statements among entities can provide new information when evaluating the financial performance of an entity. Especially, for NPOs, the nature of the financial statement can differ based on the mission or if the organization provides multiple activities.

A new classification algorithm using NPOs' mission statements allow us to draw larger sample of "Housing & Shelter" organizations compare to NTEE code. The mission statement have potential to improve traditional classification system of NPO. The new classification algorithm can improve the usefulness of NPOs' financial statements by providing a better benchmark to the information users.

Limitation

First, the new classification method mainly relies on keywords to label the organizations. Some NPOs might be mislabeled as "non-Housing" while they are providing "Housing & Shelter" services.

Second, the model only included the classification of "Housing & Shelter" organizations. The algorithm might not be generalizable to other types of NPOs.

RUTGERS
Rutgers Business School
Newark and New Brunswick

Are Stable Coins Better Coins：

A Literature Review of Cryptocurrency

Ruanjia (Katerina) Liu

What is Bitcoin

Bitcoin is a "peer-to-peer electronic cash system" which makes digital transactions possible without a trusted intermediary. However, Bitcoin price fluctuates on a daily basis. It is much more volatile than national currency and physical commodities such as gold. The main purpose of Bitcoin is to facilitate speculation rather than to boost an alternative form of payment.
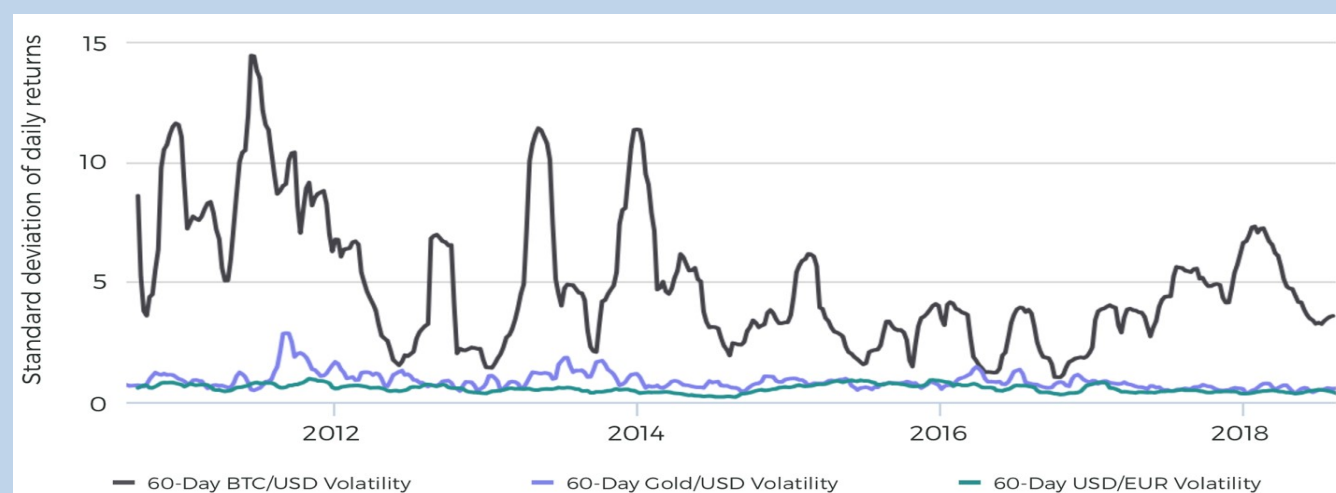
Bitcoin-enabling technologies: two cryptography technologies

1) Public-private key cryptography to store and spend money

Standard public-private key cryptography enables anyone to remain anonymous by using a public key and an associated private key (Diffie and Hellman 1976). Someone with the private key can decode a message scrambled with a public key. Likewise, a specified sender can encode messages with a private key and the encrypted messages can be descrambled with the corresponding public key.

2) *Cryptographic validation of transactions*

Thus, only the specified recipient can read the encrypted message and confirm that the message is coming from the sender.

The bitcoin-transactions in blockchain:

1) Payers initiate a bitcoin payment which results in pending transactions that are broadcast on the global bitcoin network

2) Bitcoin system issues a challenge string with only one response solution

3) Once every ten minutes or so, miners compete to solve a difficult mathematical equation (a "hash function"), and broadcasts this "proof-of-work" which is designed to be a security measure against alterations

4) The other miners check the proof-of-work and the validity of the transactions. If they approve, the winning miner gets a reward of 25 newly minted bitcoin

5) This chain of blocks is backed up and stored on the computer memory of each user

6) The payee can use his wallet software to see whether the bitcoin has arrived

The bitcoin network structure:

A decentralized operation system, e.g., Peer-to-Peer network, is utilized.

Swan and Melanie (2015) find that every entity within the network closely monitors transaction activities and keeps track of the whole history of all transactions and account balances. Only miners can confirm transactions, ensuring Bitcoin's safety. The possibility of tampering with transaction records is minimal because of economical unfeasibility. The following diagram demonstrates decentralized network (Chiu and Koeppl 2017).
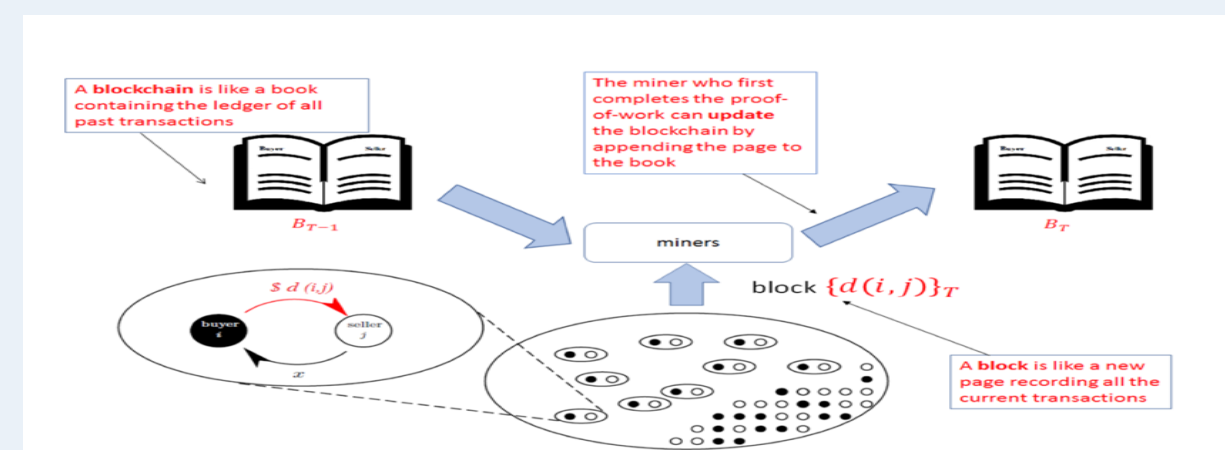
- Cryptocurrency exchange-controversy

Money laundering is the particular criminal act that benefits from a decentralized ledger.

- Cryptocurrency exchange-legitimacy

Some sovereigns ban or shut down the Bitcoin exchanges while others recognize its legitimacy.

What is Stable Coin

Cryptocurrency prices are subject to large price swings, resulting in the business world being reluctant to accept cryptocurrency as a payment option. Stable coins offer solutions which minimize price volatility and secure transactions. There are four types of stable coins:

1) *fiat collateralized:* rely on fiat currencies such as the U.S. dollar to maintain their value

2) *commodity-collateralized stable coins*: are backed by interchangeable assets, such as metals and oil

3) *crypto collateralized:* are backed by other cryptocurrencies such as Ether (ETH)

4) *non-collateralized stable coins:* use an algorithmically governed approach to control the coin supply and demand

Criticism of Tether:

1) fails to provide sufficient evidence of adequate fiat reserves

2) shares the same chief executive officer with the Bitfinex exchange (a sister company)

3) lacks long-term banking relationships

4) recent scandal: The New York Attorney General sued Bitfinex for fraud in April 2019. Crypto Capital, the intermediary for Bitfinex exchange, reported that $850 million in customer funds could not be returned

# Identifying Audit Processes for Automation Using Robotic Process Automation

Hongmin W. Du, Soo Hyun Cho

Robotic Process Automation in Auditing

- Robotic Process Automation (RPA) is the automation of certain repetitive tasks that may be deemed to be tedious or time-consuming, in an attempt to save human resources and time on these activities.

- RPA has been researched frequently in many fields such as engineering and in computer science, but is considered an emerging technology in the Auditing field.

- RPA has the potential to aid auditors in various parts in the audit process which includes account reconciliations, substantive testing, assessment of internal controls, risk assessment, and other activities during an audit engagement. So the question we want to address is which audit processes are suitable for automation? Or how do we determine whether an audit process is suitable for automation?

- To begin, we want to first understand more about different types of automation.

- Devanney et al (2016) presents three different type of categories of software robots seen in Table 5. Robot activities are classified as either Task bot, Meta bot or IQ bot. The function of Task bot matches exactly with the idea of RPA in that it is the automation of repetitive tasks. When we look at Meta bots which perform more complex processes, it would need to be considered whether RPA can be classified as a Meta bot. RPA can perform certain Meta bot activities, which will be a more complex form of simply repeating repetitive tasks. Looking at the last category of software robots, the function of IQ bots are more along the lines of Artificial Intelligence because the processes require learning through repetitive experience. Under IQ bot, RPA would definitely not be classified under this category.

Table 5: Categories of software robots, as defined by Devanney et al. (2016).

| Name	Function
Task bot	Repetitive tasks in multiple different processes.
Meta bot	Complex processes requiring multiple skills.
IQ bot	Processes involving unstructured data that requires learning via experience.
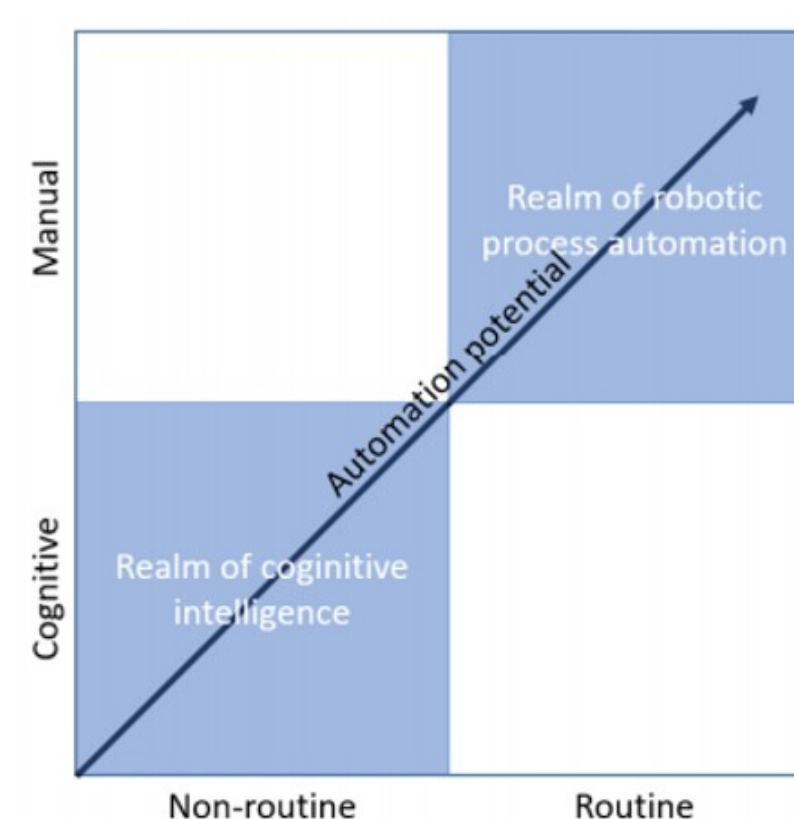
Figure 5: Realms of cognitive intelligence and RPA (Asatiani & Penttinen, 2016).

RPA vs Artificial Intelligence

- RPA is different from Artificial Intelligence, because it lacks the learning aspect that Artificial Intelligence provides.

- Asatiani and Penttinen (2016) presents another model depicting the differences between intelligence learning and RPA. Processes that are non-routine and require more cognitive learning will more likely fall under Artificial Intelligence. As processes become more routine and become more manual, the potential for automation increases, which is where RPA is classified.

Characteristics of RPA

- RPA are more suitable for processes with certain characteristics. These characteristics include processes that are high in volume, highly repetitive, time consuming and prone to error.

- RPA can save auditor's time in tasks that are highly repetitive and high in volume.

- Tasks that are highly prone to error can be performed more efficiently if delegated to a programmed software using RPA.

- Since RPA can only perform basic robotic functions, it is also more suitable in a stable environment such as documents being processed in a single format instead of having multiple different formats.
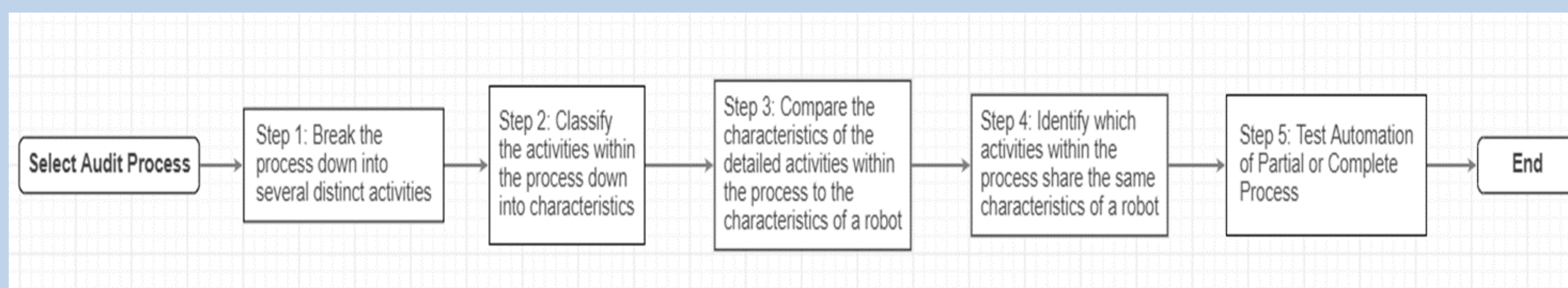
Identifying which processes in Audit are suitable for RPA

- After understanding the characteristics of RPA, a framework was formulated to model how to test for processes that have the potential for automation using RPA.

- In the framework, we would first select an Audit Process that we want to examine, and break down the process into several distinct activities. Then we would classify the broken down activities with certain predefined characteristics. Some of these characteristics may be appropriate for RPA and some may not. We then want to compare the classified characteristics to the characteristics of a robot and identify which ones share similar characteristics. Some activities may not be broken down into fully automatable activities the first time, so they may need to be reclassified again in step 1 to readjust activities. Once we determine which activities share robotic characteristics, we can then proceed to test automation by creating a test model to see if the audit process or parts of it can be automated using RPA.

RUTGERS

Rutgers Business School
Newark and New Brunswick

Management Self-Efficacy and Future Firm Performance

Ben Yoon and Kevin C. Moffitt

Research Background

- Self-efficacy is a person's belief about its own ability to achieve a goal. Bandura (1986) defines the perceived self-efficacy as "people's judgments of their capabilities to organize and execute courses of action required to attain designated types of performances."

- Prior literature finds that the higher self-efficacy has a positive association with the actual performance at the personal level and the group level.

- However, most of the prior research relies on the survey methodology for measuring the level of self-efficacy. Due to the limitation of the survey methodology, the number of sample size is limited, or the subjects of the research have been restricted (Forbes 2005; Gong et al. 2009; Hill et al. 1987; Hmieleski and Corbett 2008).

- In this research, we deploy the textual analysis methods for measuring the self-efficacy. More specifically, we focus on the self-efficacy at the company level; we name it as the management self-efficacy, management confidence level about its ability.

- We analyze the managements' comments during the earnings conference call transcripts in order to calibrate the level of management self-efficacy. And we investigate the relationship between the management self-efficacy and the company's future performance.

Research Hypothesis

- Self-efficacy works as a strong motivational and cognitive factor for achieving goals because the belief about itself makes him/her endure the unfavorable situation and pursuit its goals. And we assume that this self-efficacy level is expressed by the managements official comments during the conference call.

- Earnings conference calls have two distinct sessions. The first presentation session is usually prepared in advance and the management explains its results of the operation during the fiscal year. Whereas, the second question-and-answer session is conducted instantly between the management and the analysts (call participants). We assume that if we measure the difference between the presentation session and the Q&A session, it will reveal the true self-efficacy level of the specific company.

- If the management expresses a higher management self-efficacy during the conference call, the company may realize the improved results in the future, compared to other companies with lower self-efficacy. In other words, we test the mechanism of self-efficacy at the company level in this study.

H: The company with higher management self-efficacy during the conference call will have better financial performance in the future.

Constructing Self-efficacy Measurement with Textual analysis

- We utilize the textual analysis methodology for measuring the level of management self-efficacy. We use multiple methods from the simple bag-of-words approach to the application of the sentence structure or tense of verbs.

- Finding specific words, also known as bag-of-words approach, has been a widely used textual analysis method. We also define 28 words list. If a sentence contains one of these words, we classified it as the self-efficacy sentence.

- We use the sentence structures for identifying the self-efficacy sentences. If the sentence 1) has a certain verb phrases (i.e., can, is able to, will, have been, etc.) and 2) has any of pre-defined words (341 words) which are related to the self-efficacy, and 3) has first-person pronoun in its subject phrase, then, we classify this sentence as the management self-efficacy sentence.

- We use the tense of the verbs. We assume that self-efficacy is more related to the actions in the future. Thus, if a sentence does not have any of the past tense verbs, and has any of pre-defined words (341 words), we classify the sentence as the management self-efficacy sentence.

- By combining the above-mentioned rules, we identify the management self-efficacy sentences from the earnings conference calls.

Results

- We revise our initial rules for identifying the management self-efficacy sentence. With three times iterations of the rule revisions, the accuracy ratio is enhanced from 74.0% to 76.5%.

- **Future financial performance (next year's ROA [return on assets])**

$$\text{ROA}_{it+1} - \text{ROA}_{it} = \beta_0 + \beta_1 \text{ Self\_efficacy}_{it} + \beta_2 \text{ ROA}_{it} + \beta_3 \text{ ROA}_{it}$$

$$+ \text{ other control variables}_{it} + \text{fixed\_effect (year and industry)} + \varepsilon$$

COEFFICIENT	ΔROA_{it+1}		
SELF_EFFICACY	**0.0513**	(2.778)	**
ROA	-0.4260	(-35.337)	***
ΔROA_t	0.0040	(1.708)	.
Controls and fixed effects			
Observations	13,659		
R2	0.1754		

t-value reported in the parenthesis,. p< 0.10, * p<0.05, ** p<0.01, *** p<0.001

- **Future financial performance (year after the next)**

ROA improvement trend (Dummy variable)

$$= \beta_0 + \beta_1 \text{ Self\_efficacy}_{it} + \beta_2 \text{ ROA}_{it} + + \beta_3 \text{ ROA}_{it}$$

$$+ \text{ other control variables}_{it} + \text{fixed\_effect (year and industry)} + \varepsilon$$

COEFFICIENT	ROA_IMPROVED_TREND$_{t+2}$		
SELF_EFFICACY	**0.0868**	(2.469)	*
ROA	-0.4658	(-20.312)	***
ΔROA_t	0.0049	(1.093)	.
Other 8 controls			
Observations	13,658		
R2	0.0677		

t-value reported in the parenthesis,. p< 0.10, * p<0.05, ** p<0.01, *** p<0.001

Contributions

- To our best knowledge, this is the first trial to measure the self-efficacy by using textual analysis, instead of questionnaire survey methodology.

- By overcoming the limitations of survey methodology, we can incorporate the large samples in this research. And by doing this, we show the empirical evidence of self-efficacy in broader and more generalizable context.

- We propose a new measurement named as the management self-efficacy in the business context. And this study shows that the management self-efficacy has a prediction power over the firm's future financial performance.

- We deploy the new textual attributes for developing the management self-efficacy measurement. Based on the bag-of-words approach, we introduce the usage of sentence structures which are relatively complex, tense of the verb, and part-of-speech of each word. These traits help us to capture more accurate meanings of the sentences.

- We utilize the unique setting of the earnings conference call transcripts. We focus on the difference between the two sessions within each conference call. And we show the different characteristics between the first presentation session and the second question-and-answer session. Furthermore, we utilize this characteristic for measuring true management self-efficacy.

- By deploying our findings, the market participants can enhance their decision making with respect to the firm's future performance. The external auditors and regulators can make more accurate assessments about the risk of the companies.

RUTGERS

Rutgers Business School
Newark and New Brunswick

The Effect of Nonprofit Governance on Asset Diversion

Chengzhang Wu and Richard B. Dull

Introduction

- Fraud can be devastating to nonprofit organizations. According to the recent Association of Certified Fraud Examiners Report to the Nations, nonprofit organizations that experienced fraud had a median loss of USD 75,000, an amount that may severely reduce the effectiveness for entities whose financial resources are extremely limited.

- In 2008, the IRS revised Form 990 to require all tax-exempt public charities to disclose any significant diversion of the organization's assets during the year. A diversion of assets is unauthorized significant conversion or use of the organization's assets, including but not limited to embezzlement and theft.

- Prior research (Harris, 2015) finds that stronger governance in an organization reduces the likelihood of asset diversions.

Hypothesis Development

- Prior research (Harris, 2015) finds consistent evidence that good governance in non-profit organizations is negatively associated with the probability of an asset diversion

H1: The amount of assets diversion is negatively associated with governance level

- A recent research (Timofeyev, 2016) finds that the duration of asset misappropriation depends on certain anti-fraud control mechanism.

H2: The duration of assets diversion level is negatively associated with governance level

- Marciukaityte et al. (2006) finds that, in for-profit setting, companies increased the proportion on the monitoring committees of the boards after accusations of corporate fraud.

H3: The governance level increases in the tax year after asset diversion year

Research Design

- This research adopts Weighted Governance Index, which is depicted in Boland (2018), to measure the governance level in a nonprofit organization. This is an index that sums up 16 governance indicators, which are disclosed in IRS Form 990, but weight each by its standard deviation.

- In order to test the effects of nonprofits' governance on the amount of assets diversion, the flowing regression model is proposed.

- Logit regression and T-test are used to test the hypotheses proposed in this research.

- In the robustness test, another index is used to measure governance level in nonprofits.

Conclusion

- The disclosed dollar amount of asset diversion event is negatively associated with the governance level of non-profit organizations.

- The duration of asset diversion event is not significantly associated with the governance level of non-profit organizations.

- The governance level in the following year becomes significantly higher than that in the year when asset diversion event is discovered.

- The results of robustness test conform to those in the primary test.

RUTGERS
Rutgers Business School
Newark and New Brunswick

New York City Street Cleanliness:
Apply Text Mining Techniques to Social Media Information

Huijue Kelly Duan, Miklos A. Vasarhelyi
Mauricio Codesso, Zamil S. Alzamil, Deniz Appelbaum

Objective

- Examine social media information to identify temporal trends and patterns of street cleanliness
- Analyze if crowdsourcing information shows trends and patterns that are consistent with NYC cleanliness ratings
- Assess the performance of municipal services via sentiment analysis

Motivation

- NYC government performs a cleanliness inspection every year by relying on inspectors' subjective judgment during visual inspection. This method has not changed for nearly fifty years

- The inspection is based on the ratings that are provided by inspectors, and the ratings are adjusted for street miles but not for population, housing density, or the nature of activity in the inspected area, such as residential, commercial, or parks and recreation

- Based on current rating system, NYC government rates the majority of its streets as acceptably clean

- However, NYC residents increasingly contact Department of Sanitation via 311 about missing trash pickups, overflowing litter baskets, and dirty conditions
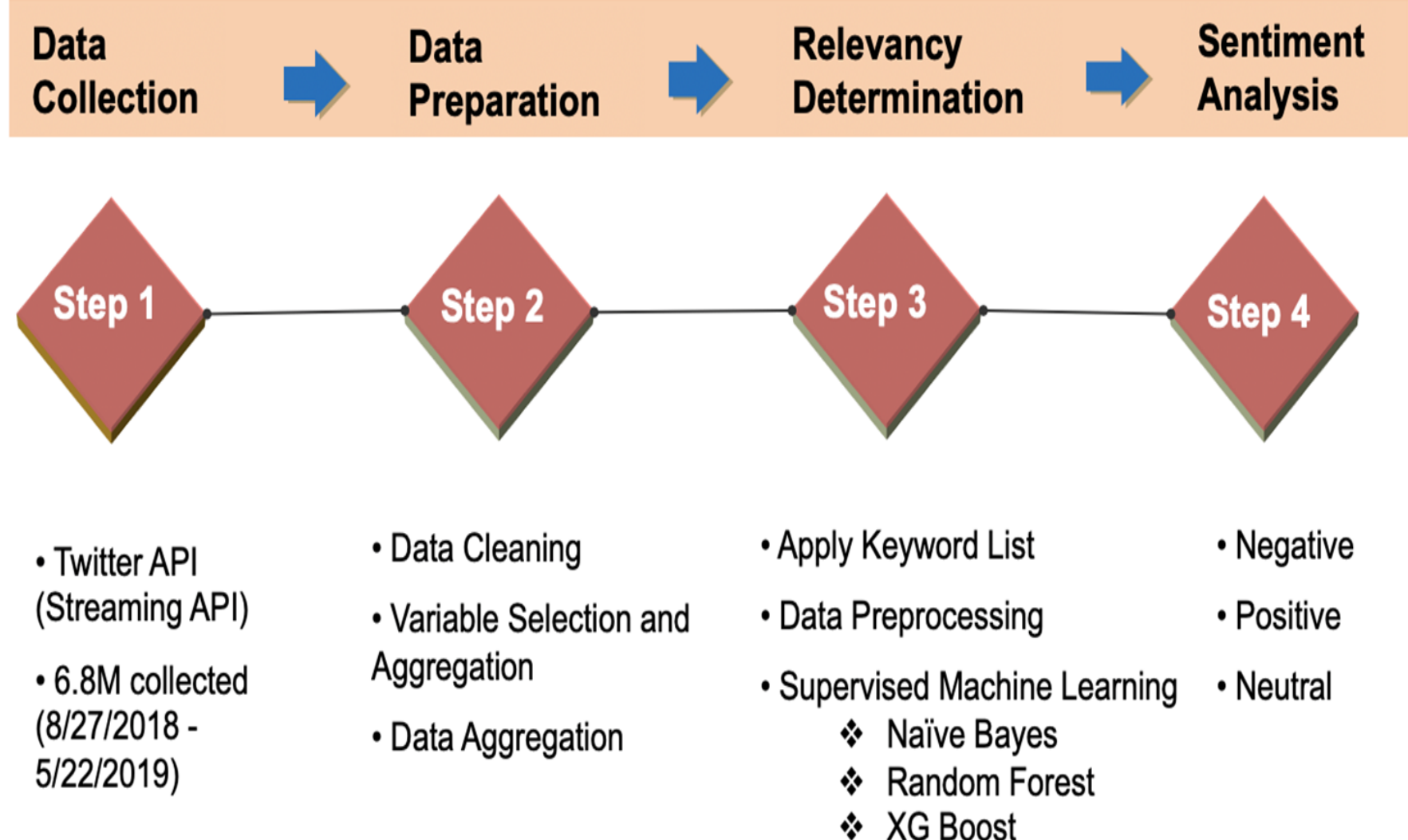
Relevancy Determination

- Supervised machine learning algorithms are used (Naïve Bayes, Random Forest, XGBoost)

- The performance of all three classifier models is excellent based on accuracy score; however, the dataset is facing an imbalanced class issue

- Two sampling methods are used to solve the imbalanced dataset issue
  - Random under-sampling
  - Random over-sampling

- 10-fold cross-validation is performed on all models based on precision, recall, F-1 score, the result indicates that Random Forest over-sampling performs better
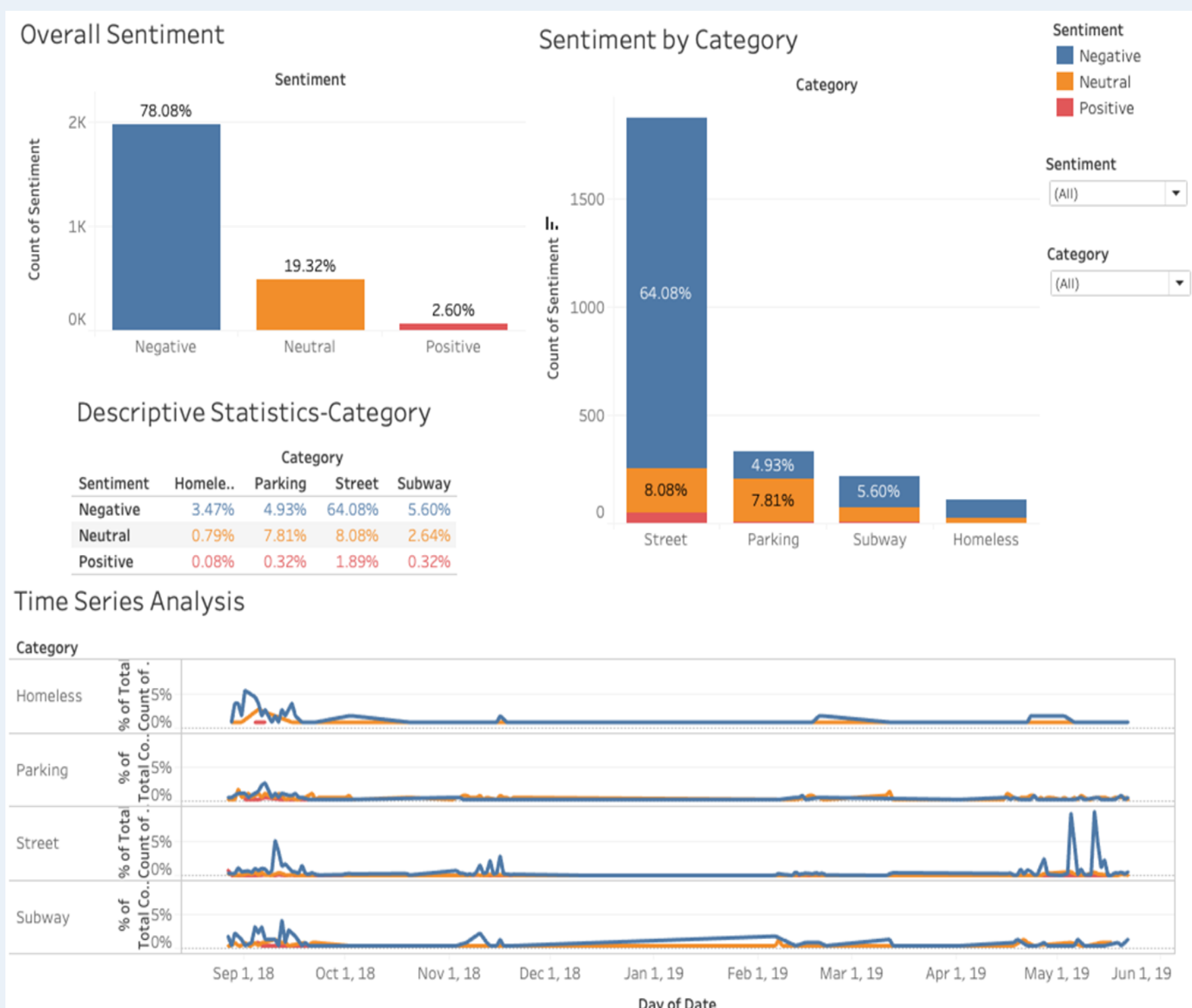
Conclusions

- The overall sentiment of the Twitter dataset is negative

- Majority of the negative tweets is related to street condition

- The sentiment results could be impacted by specific events, as the time series analysis shows that people tweet more on certain days

- Considering the location limitation of the Twitter dataset, the framework is extended to another social media platform, Facebook. A sample of NYC community pages is selected. The sentiment is assessed based on location and category

Workflow

Data Collection	Data Preparation	Relevancy Determination	Sentiment Analysis
Step 1	Step 2	Step 3	Step 4
• Twitter API (Streaming API) • 6.8M collected (8/27/2018 - 5/22/2019)	• Data Cleaning • Variable Selection and Aggregation • Data Aggregation	• Apply Keyword List • Data Preprocessing • Supervised Machine Learning ❖ Naïve Bayes ❖ Random Forest ❖ XG Boost	• Negative • Positive • Neutral

Dashboard

Overall Sentiment — Sentiment: Negative 78.08%, Neutral 19.32%, Positive 2.60%

Sentiment by Category — Street 64.08%, 8.08%; Parking 4.93%, 7.81%; Subway 5.60%; Homeless

Descriptive Statistics-Category

Sentiment	Homele..	Parking	Street	Subway
Negative	3.47%	4.93%	64.08%	5.60%
Neutral	0.79%	7.81%	8.08%	2.64%
Positive	0.08%	0.32%	1.89%	0.32%

Time Series Analysis — Category: Homeless, Parking, Street, Subway (Sep 1, 18 – Jun 1, 19)

Sentiment: Negative, Neutral, Positive

# Continuous Monitoring and Audit Methodology for Medication Procurement

Wenru Wang, Mauricio Codesso, Miklos A. Vasarhelyi

Project Overview

Continuous audit has been widely adopted by public and private firms, despite at different adoption levels (PwC, 2006; Vasarhelyi, et al., 2012). However, implementations of continuous monitoring and audit on government procurement analysis are rare, while government procurement easily generates wastes and abuses during the process. By identifying and analyzing the anomalous patterns of medication acquisition value through text mining techniques, this project uses data from a Brazil city and establishes a continuous monitoring and audit dashboard to achieve timely and less costly management in procurement procedures. The methodology created in this project will not only shed light on government procurement analysis, but also give insights to armchair auditors to investigate government open data from different perspectives.

Research Design

This study is a joint project with the mayor's office of Rio de Janeiro, Brazil and focuses on the medication procurement analysis. The mayor's office (PRJ) oversees procurement of a wide range of hospitals, schools, and other entities in a city of 7.5 million inhabitants where a large set of services are provided by the government. The focus of the joint project is to rank the top purchased medications and find possible procurement waste or abuse under this concentration. PRJ also provides with Lista Declassificação De Material (Material Classification List) to use as data dictionary for data extraction. The sample period used in this study covers 2 years from 2017-2018, considering audit timeliness.
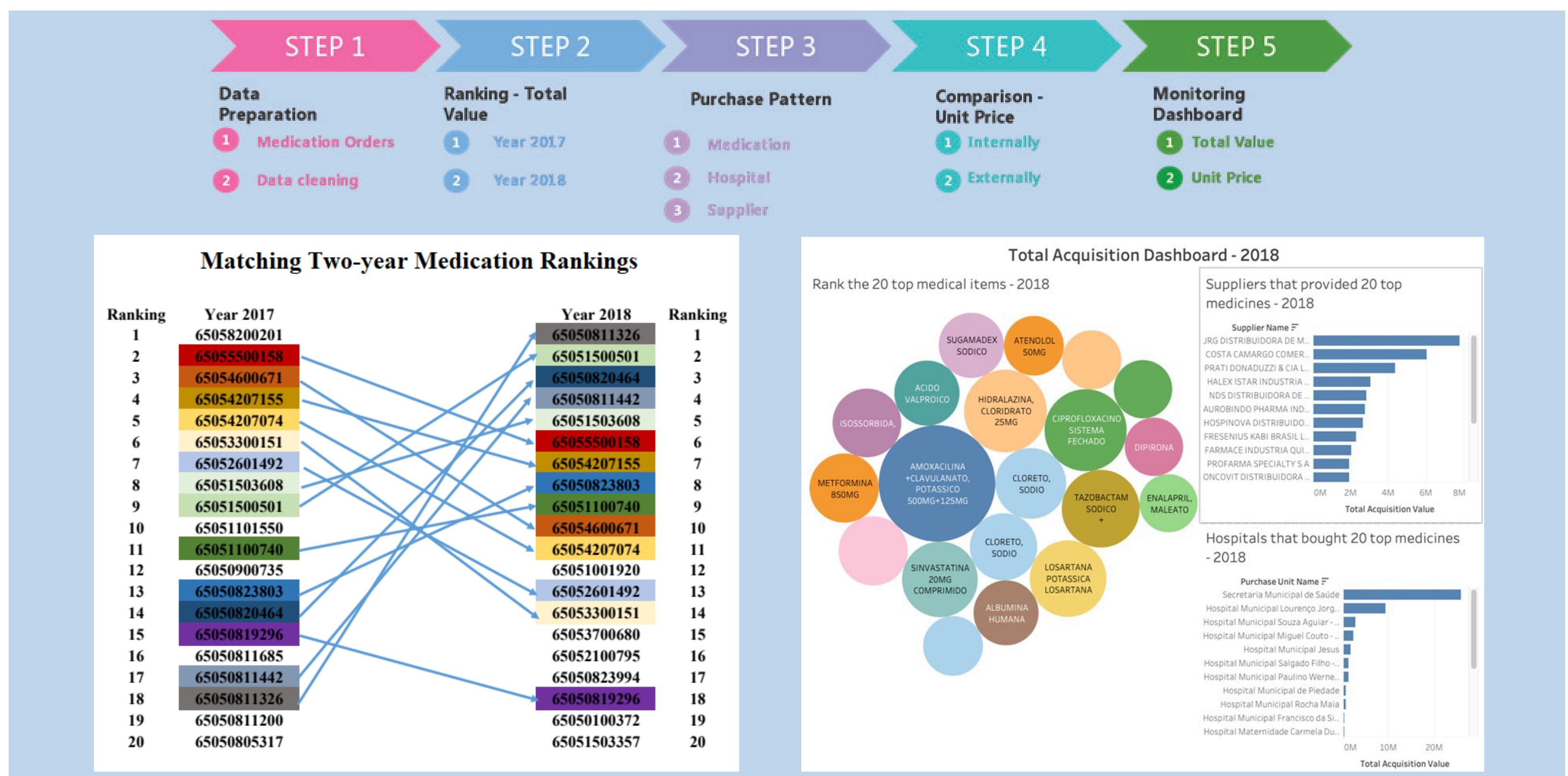
Government Procurement Audit

- Government has started to adopt electronic procurement system since a long time ago. Many researchers provided evidence that electronic procurement facilitates a flexible, open and efficient way of doing business easily and rationally with a large pool of suppliers and conducting all the subsequent transactions electronically (Coulthard and Castleman, 2001).

- However, electronic procurement system may not reach its perceived efficiency due to the complexity of government organizations and hierarchy. When an electronic procurement system is implemented, it is possible that not all nodes of the process follow the rules set by the system.

- Although audit is usually required for nearly all government activities, it is unreasonable to require either internal or external auditors to detect all errors.

Open Government Data and Armchair Audit

- Research interests on government procurement audit are extensive, especially when more governments start to provide open database for public use.

- There are some issues that auditors encounter while dealing with open database of government. Data quality is not always good enough for audits. Not all of the records in the database is related to an audit topic, and not all required information is contained in the open database.

- Performing audit sometimes requires cross comparison between different databases, which will easily create barriers to compare because no clear connections exist between the two databases.

- Open database may not provide sufficient information, and yet the most valuable information is hidden due to intentional disguised by corruption.

Continuous Monitoring and Audit

- The concept of continuous auditing emerged in the late 1980s and early 1990s (Groomer and Murthy, 2018; Vasarhelyi and Halper, 1991), when data processing technologies such as electronic data interchange and database system advanced.

- While continuous audit becomes a wide-open research area in recent years, continuous monitoring helps management in assessing the effectiveness of internal controls by ensuring the business is operating effectively under policies and procedures (De Aquino, Da Silva, & Vasarhelyi, 2008).

- Text mining, also known as text data mining, is viewed as an extension of data mining or knowledge discovery from databases. Researchers have proposed several audit apps for government procurement audit. The implementation of continuous audit and monitoring methodology or text mining analysis in government analysis is rare.

RUTGERS

Rutgers Business School
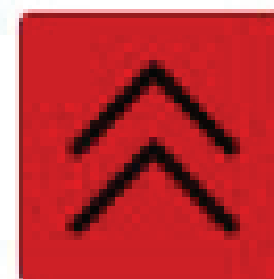Newark and New Brunswick

FREE ACCOUNTING EDUCATION!!!

RUTGERS ACCOUNTING DIGITAL LIBRARY

Providing over 500 online classes & counting to students, faculty, and the public!

Undergraduate Level

- Introduction to Financial Accounting
- Introduction to Managerial Accounting
- Auditing Principles
- Business Law & More!

Graduate Level

- Accounting Principles and Practices
- Income Taxation
- Information Technology & More!

Ph.D. Level & More

- Machine Learning
- Special Topics in Audit Analytics
- Survey of Accounting Information Systems & More!

Come check us out! No strings attached!

Rutgers Accounting Web

Rutgers Accounting Web