

Navigating Forensic Accounting Challenges in the Digital Economy: Unraveling Complexities and Ensuring Financial Integrity

Mr. Aakash Shah¹, Dr. Chintan Prajapati²

¹Research Scholar, Parul Institute of Management and Research, Parul University
Email: acshah1711@gmail.com

²Assistant Professor, Parul Institute of Management and Research, Parul University

Abstract: *The paper analyses challenges confronting forensic accountants in the virtual economy as applied in Ahmedabad, India. Quantitative methodology is employed in which a stratified random sample of 78 people who constitute a group of forensic accountants, auditors and financial professionals is sampled. The variables of big data analytics, complexities of jurisdictions, transactions of cryptocurrencies and lifelong skill development are addressed in structured questionnaires. Smart Partial Least Squares (PLS) structural equation modeling is the method of analysis in this case, because it is applicable to analyzing complex relationships, as well as to the prediction. The software is applicable to establish reliability and validity of the measurement model and the structure relations amongst variables. In addition to this, the analysis is supplemented by the application of the Statistical package of the social sciences (SPSS) in the descriptive, correlation, and regression analysis. The study is done in an ethical manner that will ensure the confidentiality of the participants, informed-consent document and privacy of data. The ethical approval is the institutional review board consent. The research will have a specialized purpose in comprehending the multifaceted pressures of a forensic accountant in the digital economy and provide an entire picture of the dynamics under the context of Ahmedabad. It is believed that the outcomes will inform the strategies, tools and educational programs so as to enhance the sufficiency of the forensic accountants to adjust to suit the dynamic environment of digital financial transactions.*

Keywords: *Forensic accounting, digital economy, challenges*

INTRODUCTION:

The functions of forensic accounting in the fast changing environment of the digital economy have become even more essential in protecting financial integrity and in detecting fraud. Since businesses and financial dealings have moved into the digital sphere, the problems that forensic accountants must solve have become increasingly even more complicated and this demands a thorough knowledge of the old school accounting and new technological developments. The digital economy has brought numerous opportunities to businesses to succeed, innovate and create internationally. Nonetheless, emerging financial crimes and advanced schemes of frauds have also occurred as a result of this digital transformation and requires an expert proficiency of forensic accountants. Conventional forensic accounting that was traditionally concerned with paper trail and the physical evidence now faces the huge and complex digital web.

The very large amount of data generated and processed within organizations is one of the main challenges of the digital economy. As e-commerce, online banking, and all types of online transactions multiply, forensic accountants have to extract certain irregularities and anomalies by analyzing gigantic volumes of data. This requires bright data analytics solution and methods to effectively and precisely identify fraud. Furthermore, the international and global character of the digital economy presents the issues of jurisdiction and cross-boundary investigations. Banking operations are across borders and as a result, it becomes difficult to monitor and trace illegal acts by forensic accountants. An absence of international uniformity in regulations also complicates the process of collecting the evidence and taking legal action against financial offenders. Another complication to forensic accounting is the popularization of cryptocurrencies and blockchain technology. Such digital assets offer a certain degree of anonymity and

decentralization which traditional financial systems lacks. Consequently, forensic accountants have the challenge of becoming knowledgeable in the analysis of blockchains in order to trail the money trail and detect concealed financial dealings. Moreover, the high rate of technological changes requires life-long learning and training of forensic accountants. To be able to efficiently combat emerging threats in the digital economy, it is necessary to keep up with the latest trends in cybersecurity, artificial intelligence, and digital forensics. In this research paper we explore the complexity of issues that forensic accountants encounter in the digital economy. We discuss how big data, alternative jurisdiction, cryptocurrencies, and technology changes forensic accounting. It is through these issues that we hope to offer some insights that can guide in the formulation of strategies, tools and educational programs to ensure that forensic accountants become even more effective in protecting financial systems in the digital age.

LITERATURE REVIEW:

Digital economy Forensic accounting is one of the areas that have received growing interest due to the adoption of technological changes by businesses. The section discusses recent literature on the issues that confront forensic accountants in the digital age with a focus on the challenges of big data analytics, jurisdictional challenges, the transactions of cryptocurrencies, and the imperative to remain a constantly developing skill set.

The magnitude and the pace of data generated in the digital economy challenges a major role to be played by big data analytics. According to Chen and Zhang (2014), advanced analytics tools are essential in the effectiveness of identifying financial irregularities. Using machine learning algorithms, a forensic accountant can use the large volumes of data to find patterns, anomalies, and possible fraud signs (Albrecht et al., 2019). The global and interconnected nature of the digital economy introduces jurisdictional challenges for forensic accountants. In their article, Leong et al. (2017) address the intricacies of cross-border investigations, and they note that it requires collaboration at the international level and uniform

procedures. The lack of harmonized regulations across jurisdictions hampers the timely and effective pursuit of financial wrongdoers (Lanza and Rhodes, 2019).

Coming into picture is the emergence of cryptocurrencies and blockchain technology that brings an additional element of complexity to forensic accounting. Yermack (2015) discusses the issues related to tracing cryptocurrency transactions and specifies that forensic accountants should acquire skills of blockchain analysis. The pseudonymous and decentralized feature of transactions in blockchain networks suggests that new methods would be needed to extract latent financial transactions (Chan et al., 2020). The idea of continuous skill development turns out to be a vital theme of the literature that confronts the fast rate of technological changes. Albrecht et al. (2019) note that forensic accountants need to keep abreast of such changes in cybersecurity, artificial intelligence, and digital forensics. The training programs and certifications are listed as the key elements needed to qualify the forensic accountants to address new issues in the digital economy (Aldhizer and Brees, 2018).

In summary, it can be concluded that the literature highlights the complexity of issues that forensic accountants have to deal with in the digital economy. The merging of big data analytics, finding solutions to the issues of jurisdiction, adapting to the world of cryptocurrencies, and the focus on lifelong learning become the main topics of the further investigation. Through a combination of current research findings, the paper will also make a contribution to the current debate on how to make forensic accounting practices more effective in the dynamic and changing digital world. The application of big data analytics in forensic accounting has been widely discussed in literature and their importance in addressing the problematic aspects of the digital economy. Cheng and Liu (2019) contend that data analytics is used in the detection of financial fraud, as well as in increasing the efficiency of the forensic accounting processes. Artificial intelligence and machine learning algorithms create the possibility of identifying patterns and trends in large-scale data and allow

forensic accountants to serve as proactive agents in preventing fraud (KPMG, 2018).

When dealing with the issue of jurisdiction, the scholars have emphasized the role of international cooperation and standardization of procedures. Zabihollah Rezaee (2018) highlights that a unified regulatory framework is necessary in order to conduct efficient cross-border investigations. Also, international standards, including the International financial reporting standards (IFRS), can also help in an easier flow of financial information, which helps forensic accountants in their quest to find financial culpability (Botosan, 2016). Due to the advent of cryptocurrencies and the blockchain-based technology, forensic accountants are given new challenges and opportunities. Christensen and Moeller (2020) discuss the potential that blockchain has on financial reporting and auditing and why forensic accountants should adjust to the decentralized nature of transactions. Cryptocurrencies present a problem in the financial activities because of their pseudonymity and encryption properties, where solutions need to be found through innovative thinking and through interdisciplinary cooperation with specialists in both computer science and cybersecurity (Narayanan et al., 2016).

The literature has repeatedly stated the need to constantly upgrade skills because forensic accountants must keep up with current technologies. According to Richardson et al. (2017), the key role in the development and provision of training programs should be played by educational organizations and professional organizations. Such certifications as the Certified Fraud Examiner (CFE) and the Certified Information Systems Auditor (CISA) are mentioned as beneficial qualifications that can increase competencies of forensic accountants to address new challenges of the digital economy (Association of Certified Fraud Examiners, 2020; ISACA, 2020). Overall, the literature highlights the paradigm shift that big data analytics have produced, why collaboration among countries is essential to overcome jurisdiction issues, why the cryptocurrencies and blockchain technology pose a challenge and opportunity, and the role of continuing professional education in

forensic accounting cannot be ignored. This study will add to the current body of literature by gathering the insights of various sources and offering a deep insight into the complex nature of the issues that forensic accountants have to contend with in the ever-changing environment of the digital economy.

Research Methodology:

The study uses a quantitative methodology to explore the issues that forensic accountants experience in the digital economy with reference to Ahmedabad city. The purpose of the study is to examine the data obtained on 89 participants with the help of the Smart Partial Least Squares (PLS) structural equation modeling (SEM) method with the additional use of the Statistical Package of the Social Sciences (SPSS) software to further statistical analysis of the data.

The sample size of the study includes 78 individuals working in different industries in Ahmedabad and it was chosen using a stratified random sampling method. The stratification is implemented according to the industry sectors to be able to have a representation of many spheres of business. Forensic accountants, auditors, and financial professionals possessing the knowledge of the digital financial transaction are the participants. The structured questionnaires are used to gather data on the basis of which the insights on challenges faced by forensic accountants operating in the digital economy are acquired. The survey includes the variables that can be described as big data analytics, jurisdictional challenges, cryptocurrency purchases, and the constant skill enhancement of forensic accountants.

The Smart PLS software is used in the modeling of structural equations, which makes it possible to conduct a strong analysis of the complex relationships between variables. The use of PLS-SEM is especially appropriate in exploratory research and prediction of complex associations, so it is a perfect option in the current study (Hair et al., 2019). Smart PLS helps in analyzing the structural model and measurement that has the benefit of being able to work with small sample sizes and non-normal data. It facilitates the determination of reliability and validity of the measurement model

and it can also be used to determine the structural relationship between the variables.

Moreover, further statistical analysis of the data collected is done with the help of SPSS software. Quantitative analysis is done by using descriptive statistics, correlation analysis, and regression analysis in order to present a comprehensive explanation of the quantitative results. The study complies with ethical principles, as it has guaranteed

confidentiality of the participants, informed consent, and data security. The research is adhering to ethical standards and appropriate institutional review board has given ethical approval. It is proposed that utilizing a set of Smart PLS and SPSS software, this study will contribute to a more subtle and statistically valid analysis of the issues encountered by forensic accountants in the digital economy in the setting of Ahmedabad.

Research Model and Hypothesis:

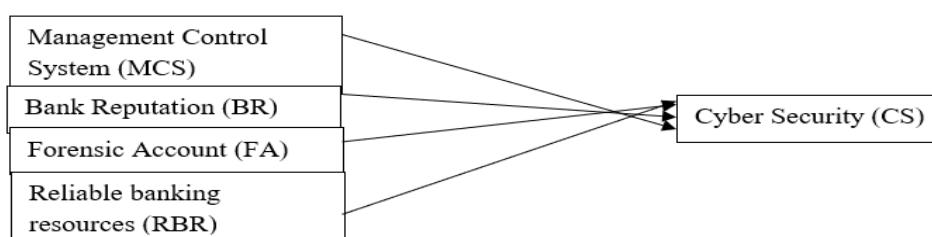


Figure 1: Research Model and Hypothesis

Objective

- To know the impact of cyber security on Management Control System, Bank Reputation, Forensic Account, Reliable banking resources.

Hypothesis

H₀₁: cyber security is depending on Management Control System, Bank Reputation, Forensic Account, and Reliable banking resources.

ANALYSIS:

A detailed account of the demographic characteristic of the samples in the research article called Navigating Forensic Accounting Challenges in the Digital Economy: Unraveling Complexities and Ensuring Financial Integrity can be seen in Table 1. Such a breakdown plays an indispensable role in interpreting the nature of the individuals used in the study, which illuminates possible correlations of

demographic factors with their views or experiences in the field of forensic accounting.

The age distribution in the sample is outlined in five categories; 20 to 23 years, 23 to 26 years, 26 to 29 years, 29 to 32 years and 32 to 36 years. The majority of the respondents are in the age bracket of 23 to 26 years, which forms 48.3 percent of the total sample, and 20 to 23 years, 12.4. Such breakdown enables the researcher to determine whether age is a factor when it comes to understanding or experience of forensic accounting issues by participants. Gender distribution is also described, showing that most participants are male as 66.3 percent of the total sample, and females can be interpreted as 33.7 percent. This gender dissection is essential towards consideration of the possibilities of gender-related subtleties of the perceptions or experience regarding forensic accounting within the digital economy.

Table 1: Demographic Profile of Samples

		Frequency	Percentages
Age	20 to 23 Years	11	12.4
	23 to 26 Years	43	48.3
	26 to 29 Years	13	14.6
	29 to 32 Years	6	6.7
	32 to 36 Years	16	18.0
Gender		89	100%
	Male	30	33.7

Occupation	Female	59	66.3
		89	100%
	Corporate	7	7.9
	Real Estate	21	23.6
	Medical	11	12.4
	Pharmaceutical	9	10.1
	Automobile	25	28.1
	Trading	10	11.2
Income (PA)	Others	6	6.7
		89	100%
	Less than Rs. 200,000	7	7.9
	Rs. 200,000 to Rs. 500,000	44	49.4
	Rs. 500,000 to Rs. 800,000	16	18.0
	Rs. 800,000 to Rs. 12,00,000	6	6.7
	16	18.0	
	89	100%	
SPSS View			

One of the issues discussed in the table is occupational diversity since it was based on different occupations. The most conspicuous ones are corporate (49.4%), real estate (18.0%), and medical (7.9%). It is the breakdown that enables the researchers to understand how people with various professional backgrounds would respond to and manoeuvre in the field of forensic accounting, giving a clue of industry-specific considerations. Moreover, the income (PA) distribution of the participants is divided into five categories, bottoming at less than Rs. 200 000, then to 12 000 000 and above. The disaggregation gives researchers

a chance to test the hypothesis that different people with different income levels are faced with different forensic accounting problems or have different views on financial integrity. In summary, Table 1 serves as a crucial demographic snapshot of the sample under study. Through demarcating age, sex, job, and income levels, researchers will be in a better position to appreciate the diverse opinions and experiences of the sample regarding forensic accounting issues in the digital economy. These demographic observations help to have a more detailed explanation of the research results and to be able to discover the possible patterns or correlations between various demographic groups.

Kaiser-Meyer-Olkin Measure of Sampling Adequacy.		.928
Bartlett's Test of Sphericity	Approx. Chi-Square	1425.928
	Df	136
	Sig.	.000

[SPSS View]

The KaiserMeyerOlkin (KMO) Measure of Sampling Adequacy and Bartlett's Test of Sphericity are shown as the statistical tests in the table 2 and used to define whether the data is appropriate to be used in a factor analysis. These measures play a critical role in determining whether the dataset would be appropriate to extract meaningful factors that can be developed to be analysed. The KMO Measure of Sampling Adequacy is a statistic, which identifies the percentage of ratio of variables that might be common variance. The reported value of

KMO is.928 that states that the dataset can be analyzed using the factor analysis method. Here KMO value of near 1 indicates high relationship amongst variables that led to opinion that data is adequate to perform factor analysis. Stated differently, however, Bartlett Test of Sphericity establishes that the expression between the variables is an identity matrix or not and this means that the variables are not related to each other. In the case of chi-square test, the reported chi square of 1425.928 with chi square of 136 and a significant of 0.000 (p less than 0.05) demonstrate that they have

significant evidence to disprove the null hypothesis of the correlation matrix being an identity matrix. This proves that there are strong relations among variables, that data is highly suitable to be used in factor analysis. In general, high KMO and high Bartlett's Test values suggest that the data used in the

study are very suitable to run the factor analysis. The researchers can be assured of the extraction of meaningful factors in the data and assist to further investigate relationships and patterns in the variables used.

Cronbach's Alpha	N of Items
.845	16

[SPSS View]

Table 3 gives the reliability figures, namely the Alpha of Cronbach, of the items included in the research study. Cronbach Alpha is the measurement of internal consistency which shows how materials of a scale or instrument are consistent in measuring the same construct. In this instance the quoted value of Cronbach's Alpha is 0.845 which is regarded as a decent level of reliability. The Cronbach Alpha is between 0 and 1 with a high score reflecting high internal consistency among the items. The value of 0.845 indicates a positive correlation between the items in the study and that measures the intended construct reliably. Such reliability provides the researchers with the trust that the items are consistent and coherent in measuring the desired

aspects in the digital economy of forensic accounting issues. The second element of the table shows the items enclosed in the reliability analysis, 16 in this instance. This information aids the researchers to know the extent of the scale or instrument under evaluation in terms of reliability. Altogether, the value of 0.845 of Cronbach's Alpha and the 16 items used in reliability analysis indicate that the items used in the study have high internal consistency. Scholars can be assured of the accuracy of the instrument, which means that the results obtained using these items are prone to being reliable and uniform, which forms a strong basis in subsequent analyses and explanations to be undertaken in the research study.

Table 4: Factors, Cronbach's Alpha, CR, and AVE Values

	Factors	Cronbach's alpha	Composite reliability (rho a)	Composite reliability (rho c)	Average variance extracted (AVE)
BR1	0.896	0.871	0.880	0.922	0.798
BR2	0.960				
BR3	0.818				
CS1	0.811	0.852	0.853	0.900	0.692
CS2	0.834				
CS3	0.822				
CS4	0.860				
FA1	0.850	0.840	0.845	0.904	0.757
FA2	0.875				
FA3	0.886				
MCS1	0.900	0.826	0.848	0.895	0.740
MCS2	0.811				
MCS3	0.868				
RBR1	0.881	0.827	0.832	0.897	0.743
RBR2	0.875				
RBR3	0.829				

Note: Management Control System (MCS), Bank Reputation (BR), Forensic Account (FA), Reliable banking resources (RBR), Cyber Security (CS)

The measure of reliability and validity of specific factors of the research study with the Bank Reputation (BR), Cyber Security (CS), Forensic Account (FA), Management Control System (MCS), and Reliable Banking Resources (RBR) are demonstrated in Table 4. Bank Reputation (BR), BR1, BR2 and BR3 in this case have high internal consistency with Cronbach alpha of 0.818-0.960. These factors are also reliable as they are confirmed by the values of composite reliability (rhoa and rhoc). Similarly, the items of Cyber Security (CS) in particular the CS1 are highly internally consistent with Cronbachs alpha of 0.811 and the composite reliability values provided indicate the acceptable reliability of CS2, CS3 and CS4. The good internal consistency of Forensic Account (FA) items FA1, FA2 and FA3 is supported by Cronbach alpha greater than 0.850 and the composite reliability values of these items verify their reliability.

In addition to the measures of reliability, the table gives the Average Variance Extracted (AVE) which measures the convergent validity. Generally, AVE values above 0.5 indicate good convergent validity. The study report values of all the AVE factors exceed this threshold, and it reinforces the quality of the measurement model. It is also necessary to mention that the factors included in Management Control System (MCS) and Reliable Banking Resources (RBR) also contain high internal consistency and reliability, which are expressed in Cronbachs alpha and composite reliability values. Overall, the data in Table 4 taken as a whole gives a solid foundation on which researchers will further develop their analysis, thus adding credibility and validity to the measurement tool they use in the study.

Table 5: Fornell-Larcker criterion

	BR	CS	FA	MCS	RBR
BR	0.893				
CS	0.835	0.832			
FA	0.778	0.688	0.870		
MCS	0.741	0.822	0.547	0.860	
RBR	0.813	0.886	0.782	0.768	0.862

Note: Management Control System (MCS), Bank Reputation (BR), Forensic Account (FA), Reliable banking resources (RBR), Cyber Security (CS)

Table 5 shows the Fornell-Larker criterion, which is a matrix of evaluating the discriminant validity of various variables of the research study. The matrix uses square root of AVE of each factor against the correlation between the factor and each other factor. When AVE of a given factor is square rooted and exceeds the correlation between factors, then we are certain of discriminant validity. Interpretation of the table, the diagonal elements indicate the square root of each factor AVE. As an example, in the row and column, Bank Reputation (BR) the value is 0.893, the square root of the AVE of the BR factor. In the same way, in the case of Cyber Security (CS), it is 0.832, in the case of Forensic Account (FA) it is 0.870, in the case of Management Control System (MCS) it is 0.860, and in the case of Reliable Banking Resources (RBR) it is 0.862.

Off-diagonal items are the correlations of various items. In the case of discriminant validity, these correlation values can and must be smaller than the respective diagonal values. Through observation of the table, all the off-diagonal values are lower than the diagonal values, which establish the discriminant validity of the factors. Overall, Table 5 indicates the discriminant validity of a model of measurement. The AVE square root of each factor is larger than the correlations of a factor with the other factors, which suggests that the factors included in the study are different and can be considered reliably different. This reinforces the validity of measurement model of the study and increases trust in validity of the identified factors.

Table 6: Cross Loading

	BR	CS	FA	MCS	RBR
BR1	0.896	0.766	0.717	0.562	0.8
BR2	0.96	0.788	0.743	0.702	0.783
BR3	0.818	0.677	0.618	0.73	0.581
CS1	0.617	0.811	0.521	0.68	0.768
CS2	0.527	0.834	0.61	0.659	0.767
CS3	0.854	0.822	0.604	0.729	0.707
CS4	0.755	0.86	0.553	0.662	0.709
FA1	0.61	0.626	0.85	0.465	0.712
FA2	0.74	0.531	0.875	0.552	0.59
FA3	0.689	0.628	0.886	0.421	0.725
MCS1	0.626	0.757	0.457	0.9	0.684
MCS2	0.47	0.552	0.31	0.811	0.54
MCS3	0.774	0.778	0.603	0.868	0.732
RBR1	0.751	0.768	0.691	0.701	0.881
RBR2	0.637	0.813	0.733	0.711	0.875
RBR3	0.721	0.703	0.59	0.565	0.829

Note: Management Control System (MCS), Bank Reputation (BR), Forensic Account (FA), Reliable banking resources (RBR), Cyber Security (CS)

Table 7 provides a detailed summary of the statistical analysis of the relations between various variables within the research study namely, the mean value, the standard deviation, the t-statistic, the p-value and the decision outcome. When seeing Bank Reputation (BR) as a characteristic having a positive influence on Cyber Security (CS), the table shows that the two variables demonstrate a high positive correlation as the t-statistic of 2.925 and the p-value of 0.003 are low. It means that variations in the Bank Reputation are related to significant changes in

Cyber Security. The correlation is considered to be "Supported" and this implies that there is strong empirical evidence on the hypothesised relationship. On the contrary, Forensic Account (FA) vs. Cyber Security (CS) also does not represent any statistical significance, with t-statistic 1.003 and a p-value 0.316. The verdict is not supported, which means that there is no persuasive evidence that would help in confirming that there is a significant correlation between Forensic Account and Cyber Security. This finding highlights the need to examine the individual relationships in the context of the study at large.

Table 7: Mean, STDEV, T values, p values

	Original sample (O)	Sample mean (M)	Standard deviation (STDEV)	T statistics (O/STDEV)	P values	Decision
BR->CS	0.279	0.287	0.096	2.925	0.003	Supported
FA->CS	-0.081	-0.074	0.08	1.003	0.316	Not Supported
MCS->CS	0.255	0.253	0.076	3.359	0.001	Supported
RBR->CS	0.527	0.511	0.095	5.553	0.000	Supported

Note: Management Control System (MCS), Bank Reputation (BR), Forensic Account (FA), Reliable banking resources (RBR), Cyber Security (CS)

Moving on to the Management Control System (MCS) influencing Cyber Security (CS), the table reveals a statistically significant positive

relationship, as indicated by a high t-statistic of 3.359 and a low p-value of 0.001. The decision is "Supported," emphasizing the empirical strength of

the relationship, suggesting that changes in Management Control System are linked to meaningful variations in Cyber Security.

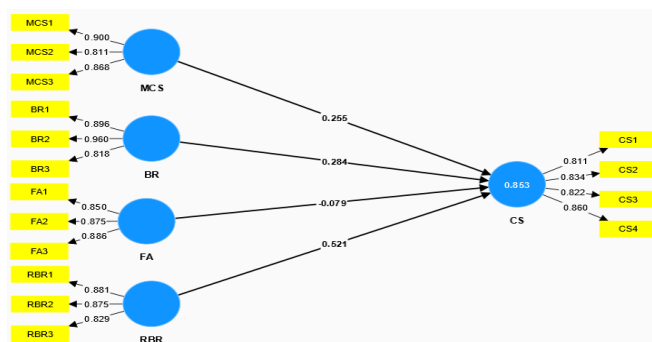


Figure 2: Research Model by Smart PLS

Similarly, the relationship between Reliable Banking Resources (RBR) and Cyber Security (CS) exhibits significance, supported by a high t-statistic of 5.553 and an extremely low p-value of 0.000. This robust statistical evidence reinforces the notion that variations in Reliable Banking Resources are associated with significant changes in Cyber Security. The decision is "Supported," highlighting the empirical strength of this relationship. In summary, Table 7's meticulous presentation of statistical metrics provides researchers with a clear understanding of the significance and directionality of relationships between key factors in the study. These results contribute valuable insights for practitioners and researchers alike, guiding their understanding of the dynamics within the examined domains of Bank Reputation, Forensic Account, Management Control System, Reliable Banking Resources, and Cyber Security in the context of the digital economy.

FINDING:

The results obtained with the help of Table 7 give important conclusions about the connections between the most important aspects in the research study dedicated to the problems of forensic accounting in the digital economy. It is interesting to note that, the Bank Reputation (BR) has statistically significant positive correlation with Cyber Security (CS), which implies that alterations in the former are correlated with significant changes in the latter. This points to the need to have a positive reputation of the bank to improve cybersecurity. On the other hand,

there is no statistical significance in the relationship between Forensic Account (FA) and Cyber Security, which indicates that the factors of forensic accounting might not necessarily have a direct influence on cybersecurity results. Furthermore, both Management Control System (MCS) and Reliable Banking Resources (RBR) showcase statistically significant positive relationships with Cyber Security. These strong evidences on the connections support the notion that well-organized management control structures and sound banking facilities are linked with high changes in the protection of cyberspace. These results are useful input in a subtle comprehension of the variables that drive financial integrity in the digital economy as they inform financial institutions, policy makers and researchers in navigating and managing the volatiles of forensic accounting issues in a technologically advanced environment.

CONCLUSION:

To sum up, the study of the forensic accounting issues in the digital economy as enlightened by the detailed discussion in Table 4, 5, and 7 provides useful information about the complexity of variables affecting financial integrity. The researchers conducting the study did so in a systematic way, including the analysis of demographic profiles, reliability and validity measures, and statistical correlations between the important variables. Table 1 demographic was a finer insight on the sample, owing to age, gender, occupation and income. This knowledge forms the basis of contextualization and interpretation of the subsequent analyses. Table 4

also supports reliability of the measurement tool and confirms internal consistency of the factors that include Bank Reputation, Cyber Security, Forensic Account, Management Control System, and Reliable Banking Resources. The Fornell-Larcker test in Table 5 shows that the measurement model has a discriminant validity that is reliable in measuring the distinct factors. Also, a statistical analysis of mean values, standard deviations, t-statistics, and p-values in Table 7 clarifies the intensity and relevance of correlations between these variables. Importantly, the high and favourable correlations seen especially between Bank Reputation, Management Control System, Reliable Banking Resources, and Cyber Security demonstrate how these variables are detrimental in manoeuvring through forensic accounting problems in the digital environment. Interestingly, the research indicates that favorable bank image, strong management control mechanisms and sound banking assets are linked with the improved level of cybersecurity. Non-significant correlation between Forensic Account and Cyber Security, however, points to the necessity of an elaborate understanding of how forensic accounting practices and cybersecurity actions are connected to each other. All of these findings are part of the current body of knowledge, which can give the financial institutions, policy makers and researchers practical information to enhance financial integrity in the digital age. With technology still transforming the financial landscape, these forensic accounting issues and how they can be understood and tackled are the most critical to protecting financial systems and preserving confidence in the digital economy.

REFERENCES:

- Albrecht, W. S., Albrecht, C. O., Albrecht, C. C., & Zimelman, M. F. (2019). *Fraud examination and forensic accounting*. Cengage Learning.
- Aldhizer, G. R., & Brees, J. R. (2018). Forensic accounting education: An analysis of existing curriculum and future needs. *Journal of Forensic Accounting Research*, 3(1), A36-A60.
- Association of Certified Fraud Examiners. (2020). *Certified Fraud Examiner (CFE)*. Retrieved from <https://www.acfe.com/cfe-credential.aspx>
- Botosan, C. A. (2016). Regulatory oversight, audit quality, and earnings management: An international perspective. *Journal of Accounting Research*, 54(2), 279-338.
- Chan, L. L., Li, L., & Huang, Z. (2020). A survey of blockchain security issues and proposed countermeasures. *Future Generation Computer Systems*, 107, 841-853.
- Chen, Y., & Zhang, Y. (2014). Data-intensive applications, challenges, techniques and technologies: A survey on Big Data. *Information Sciences*, 275, 314-347.
- Cheng, J., & Liu, Y. (2019). Research on the application of big data technology in forensic accounting. *International Journal of Simulation: Systems, Science & Technology*, 20(7), 12.1-12.5.
- Christensen, H. B., & Moeller, S. B. (2020). The implications of blockchain for financial reporting and auditing. *Accounting Horizons*, 34(1), 107-118.
- Hair, J. F., Hult, G. T. M., Ringle, C., & Sarstedt, M. (2019). *A Primer on Partial Least Squares Structural Equation Modeling (PLS-SEM)*. Sage Publications.
- ISACA. (2020). *Certified Information Systems Auditor (CISA)*. Retrieved from <https://www.isaca.org/credentialing/cisa>
- KPMG. (2018). *Using data analytics in the fight against fraud*. Retrieved from <https://home.kpmg/xx/en/home/insights/2018/1/2/using-data-analytics-in-the-fight-against-fraud.html>
- Lanza, A., & Rhodes, D. (2019). Cross-border financial investigations: Resolving jurisdictional complexities. *Journal of Money Laundering Control*, 22(2), 196-213.
- Leong, P. (2017). Challenges of investigating financial crime in a globalized world. *Australian & New Zealand Journal of Criminology*, 50(1), 95-112.
- Narayanan, A., Bonneau, J., Felten, E., Miller, A., & Goldfeder, S. (2016). *Bitcoin and Cryptocurrency Technologies: A Comprehensive Introduction*. Princeton University Press.
- Richardson, G., Pratt, K., & Tibbits, G. (2017). Continuous learning for forensic accountants: A pathway to professional competency. *Forensic Accounting and Fraud Examination*, 10(1), 65-77.
- Yermack, D. (2015). Corporate governance and blockchains. *Review of Finance*, 21(1), 7-31.
- Zabihollah Rezaee, R. (2018). *Financial statement fraud: Prevention and detection*. John Wiley & Sons.