organisational information
Source: Research data (2019)

The study tested the fitness of the model at 5% level of significance to find that the probability value (p-value) was 0.000 which was less than 0.05. This implies that at α=0.05, there exists enough evidence to conclude that at least one of the IVs; identifying critical organisational information, identifying threats to information systems critical assets, analysing infrastructure vulnerabilities, and protection security strategy and mitigation plan wasuseful in estimating the mobile banking Security Framework for commercial banks in DRC and hence the model is relatively suitable in explaining the variance of levels of security framework for commercial banks in DRC as explained by the variance in these factors.

The regression results to estimate the study model are shown in Table 10.

Table 9: Regression Results of Dependent Variable against Predictor Variables

Coefficients[a]

	Unstandardized Coefficients		Standardized Coefficients	t	Sig.
	B	Std. Error	Beta		
(Constant)	0.592	0.336		1.763	0.080
Identifying critical organisational information	0.151	0.062	0.163	2.428	0.016
Identifying threats to information systems critical assets	0.149	0.048	0.195	3.087	0.002
Analysing infrastructure vulnerabilities	0.152	0.074	0.137	2.047	0.042
Protection security strategy and mitigation plan	0.304	0.051	0.381	5.936	0.000

a. Dependent Variable: Mobile banking security framework among commercial banks in Democratic of Congo
Source: Research data (2019)

These results show that each explanatory variables;Identifying critical organisational information (p-value = 0.016), identifying threats to information systems critical assets (p-value = 0.002), analysing infrastructure vulnerabilities (p-value = 0.042), and protection security strategy and mitigation plan (p-value = 0.000), had p-values of less than the 0.05. So,they were goodestimators of security framework for commercial banks in DRC. The coefficient for identifying critical organisational information (β_1= 0.151), identifying threats to information systems critical assets (β_2= 0.149), analysing infrastructure vulnerabilities (β_3= 0.152), and protection security strategy and mitigation plan (β_4=-0.304) were used to estimated model fitted as;

$Y = 0.592 + 0.151X_1 + 0.149X_2 + 0.152X_3 + 0.304X_4$……. (i)

The fitted regression equation is in the form of Security Framework for commercial banks in DRC = 0.592 + 0.151 (identifying critical organisational information) + 0.149 (identifying threats to information systems critical assets) + 0.152 (analysing infrastructure vulnerabilities) + 0.304(protection security strategy and mitigation plan).

Table 10: Model Summary for Security Framework for commercial banks in DRCs

Model Summary

R	R Square	Adjusted R Square	Std. Error of the Estimate
.529[a]	0.2795	0.2637	.65719

a. Predictors: (Constant), protection security strategy and mitigation plan, identifying threats to information systems critical assets, analysing infrastructure vulnerabilities, identifying critical organisational information

Source: Research data (2019)

Table 20 shows the coefficient of determination was .2795, an indication that 27.95% of variation in Security Framework for commercial banks in DRCs is explained by change in; identifying critical organisational information, identifying threats to information systems critical assets, analysing infrastructure vulnerabilities, and protection security strategy and mitigation plan. Therefore, all the variable; identifying critical organisational information, identifying threats to information systems critical assets, analysing infrastructure vulnerabilities, and protection security strategy and mitigation plan are strong determinants of Security Framework for commercial banks in DRC**.**

Conclusions

The study concludes that identifyingcritical organisational information has a statistically significant and positiveinfluence on the development of mobile banking security framework among commercial banks in DRC. The core consideration in developing the framework are; properly addressing information technology systems, addressing attacks on banks critical assets, ensuring properly following security requirements for critical assets, and mitigating threats to security practices

The study concludes that the identification of threats to critical M-banking assets has statistically significant and positively influences design of mobile banking security framework for commercial banks in DRC. This is characterized by restrictions of IT specialists access on the system with data transfer between the banks, strength of encryption used, level of operating patches, used and active administrative accounts in MS Active Directory; security storage of confidential information; presence of appropriate disaster recovery and business continuity documentation; configuration of firewall; staff awareness of IS threats and secure storage of information.

The study concludes that there is statistically significant and positiveinfluence of analysing infrastructure vulnerabilities moderately on the design of the mobile banking security framework. The key components for consideration are for protection against these vulnerabilities, addressing technical vulnerabilities, mitigating current technologies, protecting against vulnerabilities on key customer mobile data components, and providing high level of deterrence on customer mobile data.

The study concludes that risk mitigations (protection security strategy and mitigation plan)has a statistically significant and positive influence in the design of mobile banking security framework. The core consideration in risk mitigation are; detecting risk occurrence on customer mobile banking, mitigation of risks to organizational customer mobile banking information, customer accounts, records program, customer reports, protection of computers especially those used for online banking, back-up disks stored the strong room and company records. There is an important need to protect router and the network equipment and company information.

Recommendations

Proposed Framework

The study proposes for a proportionate regulatory framework which ensures that commercial banks in Democratic Republic of Congo maintains active risk management in its mobile banking. Thus, the study recommends for development of a comprehensive risk framework for banks offering M-Banking services. It also recommends for mFSPs to create a flexible, proportionate framework within which an on-going, active supervision of mFSPswould take place. This would ensure adequate attention in identifying, monitoring and controlling the mobile channel risks while providing adequate room for risk appropriate innovations that might be excluded if entrenched, inflexible technology standards exist.

OCTAVE-Sshould be used during the mapping of data resources with the help of information producers and users of M-banking. organizations are engaged in a public dialog to explore genres in which data is transmitted through supporting resources. In addition, the identified information assets for further risk assessment are incorporated into OCTAVE-S. Accordingly, the suggestsimplementation of anoctave-s based framework with five processes, where;

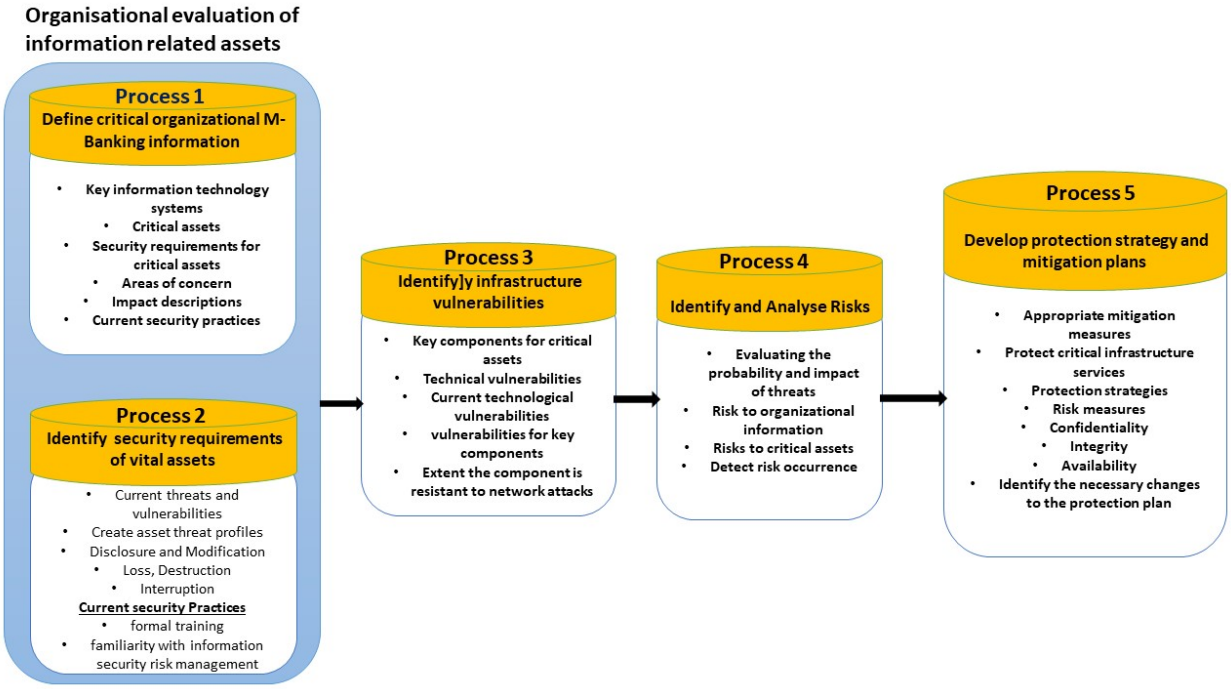
Processone will include defining sensitive organizational information in order to set up a special group for M-Banking offering banks to recognize essential M-Banking information resources and to develop a collection of impact requirements and current security practices for banks. The information obtained is significant for the creation of resource-based risk profiles.

Process two is to recognize the risks to vital information system resources by assessing the facets of the bank in which users of the data system contribute their views on what is relevant and what is being done to protect those assets by the bank. The project team would then identify the security requirements of the vital asset and then create a risk profile for each asset. The risk profile should be established; the information previously obtained from the various users of critical information assets should be grouped; the critical assets identified and the threat profile established for each critical asset. The group should also assess whether the consequences of the identified threats lead to; disclosure or representation of sensitive information; alteration of valuable or sensitive data; destruction or degradation of important information; interruption of access to significant information, technology, applications or services.

Process three involves finding vulnerabilities in infrastructure Key components of vulnerabilities are being checked (technological vulnerabilities) that could contribute to unauthorized action on sensitive property. This is a high-level survey to refine the threat profiles of infrastructure and technology practices. Physical reviews of computer hardware and components would be conducted to identify vulnerabilities that could be abused by threats.

Process four and five includes a risk analysis and implementation of security management measures and mitigation plans. The group must define, assess and then take decisions on all risks to the core resources of the company. The group should now develop a corporate security policy and mitigation strategy to address the threat to critical resources based on information collected from research. The impact and probability of all identified risks will be qualitatively assessed in the risk analysis.

The proposed framework model captured hereunder should lead to the development of an organizational security policy and risk mitigation plan based on findings from process one to five



Octave-s based Proposed framework model

Recommendations on Research Findings

The study made recommendations based on study findings as well as for future research, which are contained in this section. The study found that 27.95% of change in Mobile banking security framework among commercial banksin DRC is explained by; identifying critical organisational information has positive significant, identifying threats to information systems critical, analysing infrastructure vulnerabilities, and protection security strategy and mitigation. This means there are other factors accounting for the remaining 71.05%. The study therefore, recommends that other studies should be conducted to establish what contributes to the 71.05% variation in Mobile banking security framework among commercial banks in DRC.

Further studies should be done to assess the viability of the framework in other banking industry.

References

Alberts, C. J. &Dorofee, A. (2002). *Managing information security risks: The OCTAVE SM approach.* Boston: Addison-Wesley Anderson

Alberts, C. J. &Dorofee, A. (2003). *Managing information security risks: the OCTAVE approach*, Pearson Education, Inc. Boston

Alberts, C., Dorofee, A., Stevens, J. & Woody, C. (2003*). Introduction to the OCTAVE® Approach.* Pittsburgh, PA: Carnegie Mellon University

Ashraf, I. (2012), *Mobile Banking Security. A security model* (Doctoral Thesis, Vrije Universiteit, Amsterdam, The Hague, The Netherlands).

Audu, J. (2018). *Technology adoption in Democratic Republic of Congo (DRC): An Empirical study investigating factors that influence online shopping adoption* (Master's Thesis, University of Ottawa, Ottawa, Ontario, Canada)

Bankable Frontier Associates. (2008). *Managing the risk of mobile banking technologies*.Bankable Frontier Associates LLC.Retrieved fromwww.bankablefrontier.com.

Betelhem B. G-H. (2017). *Conceptual security framework for mobile banking key authentication and message exchange protocols: Case of Ethiopian Banks* (Master Thesis, St. Mary's University, Addis Ababa, Ethiopia).

BSI (2005) *ISO/IEC 27001:2005 Information technology – security techniques –information security management systems – requirements.* British Standard Institute.

BSI (2008) *ISO/EIC 27005:2008 Information technology — Security techniques — Information security risk management*. British Standard Institute.

Campbell, P, L. & Stamp, J. E. (2004). *A Classification Scheme for Risk Assessment Methods?*, Sandia National Laboratories.Retrievedfrom http://energy.sandia.gov/wp/wp-content/gallery/uploads/sand_2004_4233.pdf.

Douramanis, M. (2014). *Risk assessment for the cyber threats to networked critical infrastructure* (Master's Thesis, Leiden University, Leiden, The Netherlands).

ITGI (2007) *COBIT 4.1*. Rolling Meadows, IL: IT Governance Institute.

GSMA Intelligence. (2016). *The Mobile Economy Africa*. *GSM Association*. Retrieved from www.gsmaintelligence.com

Janulevicius, J. (2016). *Method of information security risk analysis for virtualized systems* (Doctoral dissertation, Vilnius Gediminas Technical University)

Kaur, R. (2014). Control Issues and Mobile Devices.

Keung, Y. A. U. H. (2014).Basic principle of information security.*Advances in Robotics & Automation*, *3*(2), 9695. Retrieved from http://doi.org/10.4172/2168-9695.1000e118.

Kothari, C. R. (2012). *Research methodology: methods and techniques.* New Delhi: New Age International.

Moyo, M. (2014). *Information security risk management in small-scale organisations: A case study of secondary schools? computerised information systems* (Master dissertation, University of South Africa, cape Town, Republic of South Africa).

Ochuko, R. E. (2012). *E-banking operational risk assessment A Soft Computing Approach in the Context of the Nigerian Banking Industry* (Doctoral Thesis, University of Bradford)

Padyab, A. M. (2014), *Towards more structured information asset identification approach for risk assessment methods using genre based Method* (Master's Thesis, Luleå University of Technology).

Rovito, S. M. (2016). *An Integrated Framework for the Vulnerability Assessment of Complex Supply Chain Systems* (Master's Thesis, Massachusetts institute of technology)

Shaaban, H. K. (2014). *Enhancing the governance of information security in developing countries: The case of Zanzibar* (Doctoral Thesis, University of Bedfordshire).

Sosonkin, M. (2005). *OCTAVE: Operationally Critical Threat, Asset and Vulnerability Evaluation*.Retrieved from http://isis.poly.edu/courses/cs996-management-s2005/Lectures/octave.pdf.

Storms, A. (2003). *Using vulnerability assessment tools to develop an OCTAVE risk profile*. Retrieved from http://www.sans.org/reading_room.

Taubenberger, S. (2014). *Vulnerability Identification Errors in Security Risk Assessments* (Doctoral thesis, The Open University).

Woody, C., Coleman, J., Fancher, M., Myers, C. & Young, L. (2006). *Applying OCTAVE: Practitioners Report*. Retrievedfrom http://www.sei.cmu.edu/publications/pubweb.html/06tn010.pdf.