Research Journal of Economic and Management Studies (RJEMS)
Vol.1, No.2. (2021). ISSN: 2789-6803.

Adequacy of Information Security Programs in Small to Medium Enterprises in Zimbabwe

Gloria Evergrace Mawere[1], Kudakwashe Chindoza[2], Ivy Jean Marima[3], Lucia Winji[4] and Trust Mutero[5]

[1-5]*Department of Accounting and Information Systems, Great Zimbabwe University, Masvingo, Zimbabwe*

[1]*gmawere@gzu.ac.zw*, [2]*kchindoza@gzu.ac.zw*, [3]*imarima@gzu.ac.zw*, [4]*lwinji@gzu.ac.zw*, [5]*tmutero@gzu.ac.zw*

Abstract
Information technology plays a pivotal role in today's businesses and in as much as it brings about benefits to the business there are many risks associated with its use that also need to be addressed. In as much as we use information systems for our benefit, there are many risks associated with its use hence organisations no matter the size should have information security programs in waiting in case risks emanate from the use of technology. The aim of the study was to evaluate the adequacy of information security programs available in small to medium enterprises in Zimbabwe making use of key performance indicators for security governance as basis for measurement. A case study was done using a qualitative research approach. Non-random purposive convenient sampling technique was used to produce a sample of 5 small to medium enterprises in Gweru was used for data gathering. Interviews were done with 5 top management members and questionnaires were administered to 5 security administration/IT involved employees. Literature data was also used. The study found out that based on information security governance KPIs the security programs of the small to medium enterprises are inadequate and loaded with poor practices. Organisations are recommended to look at the constructs of the four generic KPIs strategy, risk, posture and compliance so as to come up with a sound security program for these strategic indicators are a prerequisite to presenting the state of and changes in the security program. Findings from this study contribute knowledge to the information security governance area of study by presenting simple and practical methods to evaluate information security programs allowing management to make plans and strides towards managing cyber risks in a world where information technology has become both a tool and a target. This research can also be used in coming up with an information security governance measurement framework that can be used by small and medium enterprises. This proposed framework will provide a roadmap for decision making and assist small and medium enterprises to give due attention to activities pertaining to security so that a secure computing environment can be attained.

Keywords: *Governance, Information Security, Information Security Programme, Key Performance Indicators, Small and Medium Enterprises.*

1. Introduction

The ongoing Covid19 pandemic has led to a rise in digital investment, dependence on automation systems, remote surveillance of infrastructure for continuing far reaching cost efficiency and near instantaneous decision making across the value chain which in consequence calls for sound information security programs in organisations. Sound information security program practices allow organisations to protect fundamental business processes, information technology resources, and worker information from potential associated risks. These programs also identify members or technological resources that may impact the security or confidentiality of those assets. Sound security programs security program help organisations ascertain that the three constructs of security of information, confidentiality, integrity and availability are guaranteed through effective security management practices and controls.

Due to the Covid19 pandemic most small to medium enterprises are the ones that have fallen into the category of non- essential enterprises hence they are the ones that have mostly adopted the working from home new norm else they collapse. Small to medium enterprises (SME's) can be defined as firms that maintain their incomes, assets or number of workers below a certain sill. United States and the European Union classify SMEs using the figures of staff members. (Hussey and Eagan, 2007). According to the European Union SMEs are defined by the cumulative statistics of staff members employed, yearlong productivity of the organisation, the valuation of the organisation's assets and enterprise ownership structure. The new amendments on the Zimbabwean SMEs Act Chapter 24:12 FOURTH SCHEDULE (Section2) states that small enterprises have a maximum number of 30 -40 fulltime paid employees depending on sector of economy and a maximum total annual turnover of $500 000, and on the other hand medium enterprises should have a maximum of 75 fulltime paid employees and a maximum annual turnover of $1 000 000. (Taylor and Murphy2004) and Martin and Matlay (2001) state that SMEs are enterprises that are owner managed which means that the owner to a greater extent manipulates and or incites enterprise arrangements, resolutions and ways.. The working definition for a small business for this study is a privately owned enterprise that employees not more than 100 workers and has an annual turnover of up to $1 000 000 and is highly creative, innovative and uses information technology.

Some SME's have gone completely virtual. The working from home scenario calls for much digital investment and cyber space presence therefore the adequacy of their information security programs need to be checked to avoid the consequences of having and inadequate program. According to Agwu and Murray (2015) information and communication technology (ICT) use places SMEs at the same competitive level with their fellow large enterprises in the universal market. Findings by Niebel (2018) show that there has been a significant rise in the adoption of ICT since 2005 by both large and small businesses in developed countries. According to Munyoro G. et.al (2019), in the study on "The contribution of ICT in the development of small business sector in Zimbabwe" the respondents confirmed to be using ICT in their businesses although it is being used at different levels and for various reasons. To confirm that ICT is being used

they found out that ICT's are of essence in the development of the small business sector as they contribute to various activities that lead to the betterment of the small business sector; ICT is an effective marketing tool for the small business sector as it allows firms to anticipate, identify and satisfy customer needs and ICTs ease the enterprise's daily operations and activities among other benefits. On this background of findings the researchers saw it fit to find out the adequacy of information security programs in SMEs in Zimbabwe since they use ICT's with information being the major resource.

At an enterprise level, working from home presents new and additional risk. Organizations will have to plan to identify, manage and mitigate the risk presented to them in this new normal. As long as teams were working from an access-controlled, audited, segregated and monitored environment, physical data protection risk areas were contained on the premises of the enterprise and more easily managed (Seshadri 2020). In the work-from-home scenario, the risk extends to the employee's home, which becomes another point that has to be secured. There will be need to improve information security capabilities such as improving the intrusion detection system and raising the level of awareness of risk among employees among others especially when working from home. Besides the working from home scenario that made them invest more in technology for business viability, there are no employees for specific tasks and or many levels of management in small to medium enterprises as what exists in large enterprises. According to Mahncke, McDermid and Williams (2009), extensive and complex information security management and governance processes can be executed in large enterprises with more employees to address information security practices as compared to small to medium enterprises yet these small enterprises are still susceptible to the same threats and vulnerabilities that larger enterprises face. With that in mind they are nevertheless required to meet the thresholds to safeguard their private information.Adding on to this, Mahncke, McDermid and Williams (2009) state that small to medium enterprises most of the times source their information security processes from third parties which amplifies concern in reverence to whether some governance actions and processes have been established so as to audit and control the wellness of the outsourced partner following the industry security best practices. This justifies the need to just use strategic security governance Key Performance Indicators (KPIs) as instruments to enable simple, straightforward and practical information security program evaluations.

De Haes and Van Grembergen (2015) state that prosperous enterprises exploit the potential of digital innovation and understand and manage the risk and limitations of technology. The study will use key performance indicators for security governance to assess the adequacy of the security program for security is seen as a means to achieve business objectives. According to Pironti (2007) using specific criteria such as KPIs is a satisfactory technique in justifying the effectiveness of security agendum enacted by enterprises. Key performance indicators to be used in this study are the ones highlighted by Volchkov (2020) which are strategy, risk, posture and compliance. Questions such as "Is our security adequate? To what extent does information security contribute to business objectives? And Can we

reduce IS spending?" are not just legitimate, they are essential (Volchkov, 2020). Assessing the effectiveness of security controls means being able to adjust programs and decide on investments (Slater, 2012). No initiative or investment can exist if it does not support strategy, risk mitigation, capacity improvement and reduction of compliance gaps hence these four strategic indicators are a prerequisite to presenting the state of and changes in the security program.

According to Volchkov (2020) good security governance relies on reports based on key indicators to evaluate the sufficiency of information security, security program quality, return on security investment (ROSI) and the strides towards achieving objectives. Oversight gives the regulatory organs all the applicable information required to evaluate the state of security at any given point in time and provide direction for decision making. To assess gaps in the governance process, standards can be used, such as International Organisation for Standardisation (ISO)/International Electrotechnical Commission (IEC) ISO/IEC 27014:2013 Information Technology-Security Techniques-Governance of Information Security, or some specific recommendations or code of good practices (Bakshi, 2016). For the population under study, thus small to medium enterprises, acquiring best practices or standards might be too expensive to them hence this assessment based on key performance indicators could thus be used to report on the adequacy of information security governance in their organizations. According to Bernik and Prislan (2016), some requirements and recommendations are far-fetched and complicated and taxing in terms of required expertise and financial capacity when looking at the capabilities of small to medium enterprises encountering unfavourable economic conditions. These recommendations fall short of transparency and are too scattered. The aim of the study is to present an instrument that enables elementary, straightforward and feasible information security evaluation that allows executives to spell out schedules for subsequent processes.

2. Literature review

Key performance indicators are to be used to present the state of information security from different perspectives hence a reflection on the adequacy of the information security programs available as well as information security governance maturity.

2.1 Information security governance

The researchers will breakdown the term and start by defining information security, define governance in general then zero in to define information security governance. Whitman and Mattord (2008) defined Information Security as the safeguarding of processed data in its vital components as well as the programs and hardware that use, store and disseminate that information via the application of policy, education and awareness agendum. According to the ITGI publication, "Information Security Governance: Guidance for Boards of Directors and Executive Management," security relates to the protection of valuable assets against loss, misuse, disclosure or damage. In this regard, they classified valuable assets as the information recorded on, processed by, stored in, shared by,

transmitted or retrieved from an electronic medium. Information needs to be safeguarded against harm from threats leading to different types of vulnerabilities such as loss, inaccessibility, alteration or wrongful disclosure. Threats include errors and omissions, fraud, accidents and intentional damage. The publication highlighted that the goal of information security is to safeguard the concerns of individuals and organisations depending on information systems and communications from harm resulting from failures of the three constructs of information security that are availability, confidentiality and integrity. Availability is ensuring that information is always there when needed, confidentiality involves guaranteed accessibility of information to the permitted groups and integrity looks into its error free nature. According to the National Computing Centre Best Practice Series (2005) governance stipulates surveillance regulations, accountability and resolution rights. It is a collection of management, planning and performance review policies, practices and processes with associated decision rights, which establish controls and performance metrics over investments, plans, commitments and compliance with laws and organizational policies. Information security governance is therefore no much of a difference with general governance, it's just that its governance applied to information security. Information security governance regularise and clearly explains oversight, accountability and decision rights in security of information so as to ascertain availability, integrity and confidentiality of information.

2.2 Information security program

Whitman and Mattord (2008) defined Information Security Program as a program that describes the structure and organisation of the effort that strives to contain the risks to the information assets of the organisation. This program for information security is made up a set of initiatives, projects, and activities that support an enterprise's technology framework. The initiatives involved assist enterprises to achieve all associated business goals and meet corresponding baselines. According to Volchkov (2020) a security program is composed of a set of operational controls and an improvement plan with a road map of projects. The program is sometimes called a business plan or information security road map. Security programs mobilize resources, and their objectives must be justified (explained). The rationale of each project should be presented with origin, dependencies, duration and outcome. All organisations should make sure programs for information security are in place so as to be used to manage information technology induced risks.

According to the Ernst and Young (2014) publication on information security survey, data that is there concerning the present situation in the field of information security shows management of this particular area or field is in general not sufficient and prone to varying degrees of defective practices. This might be caused by the matter that majority of real information incidents is directly related to harsh economic conditions hence creating exceptional anomalous and complex circumstances. (Bernik and Prislan, 2016). These same aforementioned authors also state that enterprises working on establishing their systems for security of information face varying intertwined impediments that

include limited financial capacity, knowledge and competencies which presently illustrates the major concern. The security of less developed small to medium enterprises is mostly characterised by the belief that security of information is the exclusive obligation of IT office while the obligation of technology, security and privacy are oftentimes accredited to just a single individual.. The skillset and expertise of the encumbered individual determines the performance and behaviour of the entire security system. (Nguyen, Newby and Macaulay, 2015). According to Chang and Ho (2006) this is not a healthy situation considering that organisations are immensely self- assured and immensely optimistic in evaluating their own susceptibility and capability to maintain aforementioned circumstances and situations.

2.3 Key performance indicators (KPIs)

Strategic Indicators of a security program are high-level operational metrics that are employed to present the state of information security from various perspectives. Volchkov (2020) state the key performance indicators as Strategy, Risk, Posture and Compliance as shown in Figure 1 below.

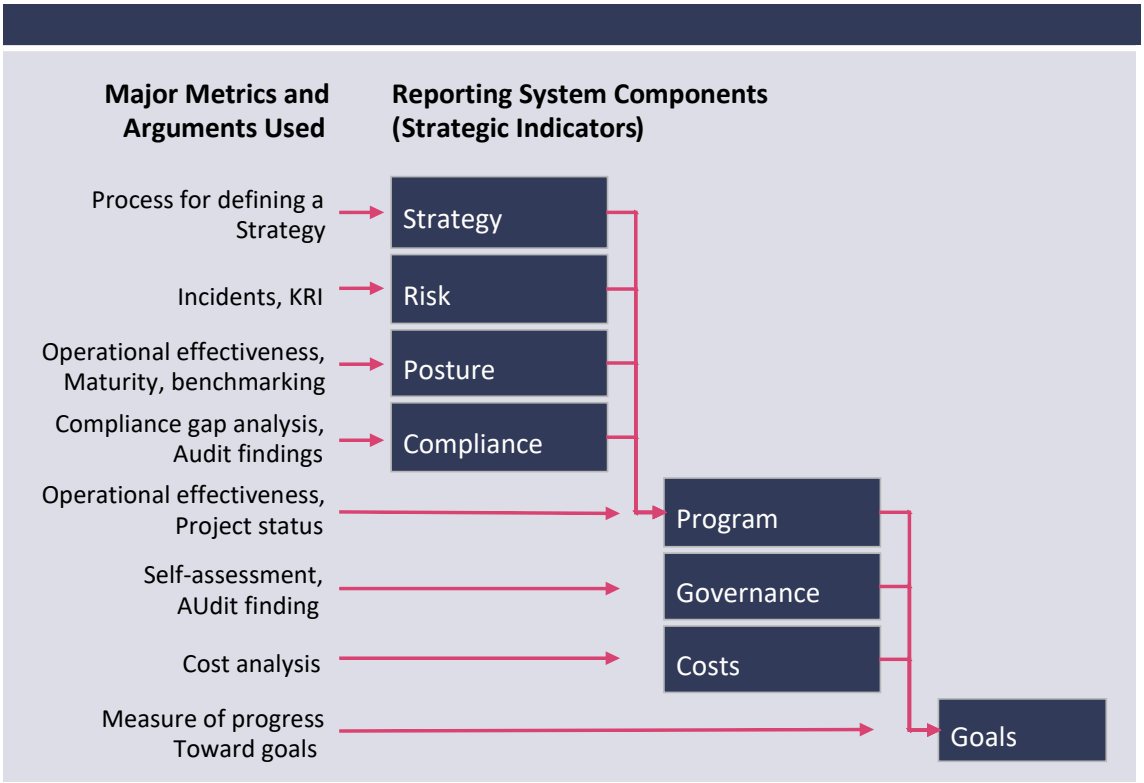

Figure 1. Strategic KPIs
(Source: ISACA Journal 2020 Vol 6.)

Strategy: This is about strategic initiatives as defined in the information security strategy.
It looks at how information security contribute to achieving the enterprise's strategy and identifies information security strategic initiatives. Information security strategy should include the vision (security strategic objectives) and major

initiatives that support either the security strategic objectives, business strategic objectives or compliance objectives.

Risk: Mitigating security risk as defined in the action plan. Indicator answers questions on the enterprise's main security risk areas the organisation's action plan to mitigate the security risk.
Posture/Maturity: Improving the level of maturity. The indicator looks at the enterprise's information security maturity level and the processes/controls that need to be improved and why. Governance requires simple, standardized ways to visualize the current and desired state of information security. A maturity assessment process should be established and accepted. It can be conducted using maturity modelling tools, through a benchmarking study, by mandating an external consultancy or by completing an audit. Many examples of value scales exist, such as ISO/International Electrotechnical Commission (IEC) ISO/IEC 15504 *Information Technology- Process Assessment* in Figure 2 below:

Figure 2. Process Maturity Scale
(Source: ISACA Journal 2020 Vol 6.)

The process maturity scale can be used to assess maturity in an organisation showing the current state versus the desired state. Level 0 shows very low maturity and the highest attainable level is level 5 which will be showing optimised security activities. According to Shinn (n.d), Security Posture is an enterprise's comprehensive security agendum which protects it from both inside and outside threats. Technical and non-technical policies, procedures and controls make up the security plan.

Compliance/Regulatory gap: Closing the gaps. The indicator answers questions on the enterprise's major information security compliance and audit gaps as well as the status of fixing the compliance and audit gaps. Compliance gap analyses and audit findings have established priorities among information security initiatives and projects.

The security program will not propose initiatives apart from those coming from one of these sources/indicators. In other words, if a security project is not triggered by strategic alignment, the need to mitigate a risk, the need to fill a regulatory gap

or the need to improve capacities to protect company assets, then there is no reason for senior executives to approve it (Volchkov, 2020).

3. Methodology

Case study was used as the research design in this study. It permits the researchers to gain an insight about the holistic and meaningful characteristics of real life events such as individual life cycles, organisational and managerial processes, neighbourhood change, international relations and the maturation of industries (Yin, 2002). Logic of design, methods of data collection and specific techniques for analysing the data are covered under this design. Using this approach enables data collected from multiple techniques that is questionnaires and literature review for this study to be presented so as to provide a holistic story. A qualitative research approach was used in the study. Qualitative research allows freedom to seek answers to queries and also getting conclusions based on delineated set of procedures. This technique is more focused on comprehending individuals' perceptions of the world. According to Qureshi (2011) it looks for acuity rather than the numerical attitudes and perceptions of the world This enabled the researchers to find out more on whether the constructs of the key performance indicators were incorporated in the security program for a sound and adequate security program. It would had been ideal to assess the adequacy of the information security programs by implementing a mixture of qualitative and quantitative methods so as to attain the most reliable results but Bojanc and Jerman (2008) as cited by Bernik and Prislan (2016), assert that mixed approaches and quantitative analyses are fundamentally endorsed for bigger organisations with intricate systems and greater quantities of resources whilst small to medium enterprises are greatly urged and advised to mostly implement qualitative system process analyses since they are easier to use and promote accelerated results generation.

The study population was SMEs in Zimbabwe and the study sample was 5 organisations in Gweru CBD selected using non- random purposive convenience sampling for the researchers wanted to make sure they get data from organisations that have cyber presence. Questionnaires and interviews were used to collect data from primary sources and literature study was used for secondary data. Much attention was placed in guarding against ambiguity in questions so as to ensure that the respondents would understand what is being asked. The process encompassed firstly the taking of feedback on questions from information security practitioners, effect modifications, then lastly administering the questionnaire to the set respondents. The questions were crafted basing on basic objectives of the research. Questions were crafted from the constructs of the key performance indicators so as to make sure we got answers on whether the security program is adequate or not. The questionnaires were administered through email and whatsapp platform for convenience purposes due to the lockdown restrictions. For the interviews interviewees were booked in advance and they were done over the phone.

Data analysis is a vital component of any research. Sue (2008) states that data obtained from qualitative methodology enables the researcher to carry out perception studies and explore what is going on at the work place according to the employees. Data from interviews was thoroughly analysed and discussed. Graphs showing percentages of the various responses were used to present and explain data from the questionnaires. Thorough discussion of questionnaires was done.

4. Findings and discussion

Results from the questionnaires and interviews will be presented, analysed and discussed as per the generic KPIs

Strategy

For KPIs based on strategy interviews were carried out. Top management was asked if it defined its security objectives with respect to business objectives and to what extent is information security team involved in modifying and developing the policies that can achieve these objectives. Most of them responded that the IT people just come up with the security programs as per general information security requirements not considering business objectives hence no strategic alignment. On being asked if the business objectives were communicated to security personnel they said no hence emphasising the absence of formalisation of information security policies based on business objectives in the organisations. These findings don't satisfy Volchkov (2020)'s assertions that information security strategy should include the vision (security strategic objectives) and major initiatives that support either the security strategic objectives, business strategic objectives or compliance objectives.

Risk

Questions on risk KPI constructs were asked in questionnaires to ensure that the security program has measures embedded in it to mitigate the security risks.

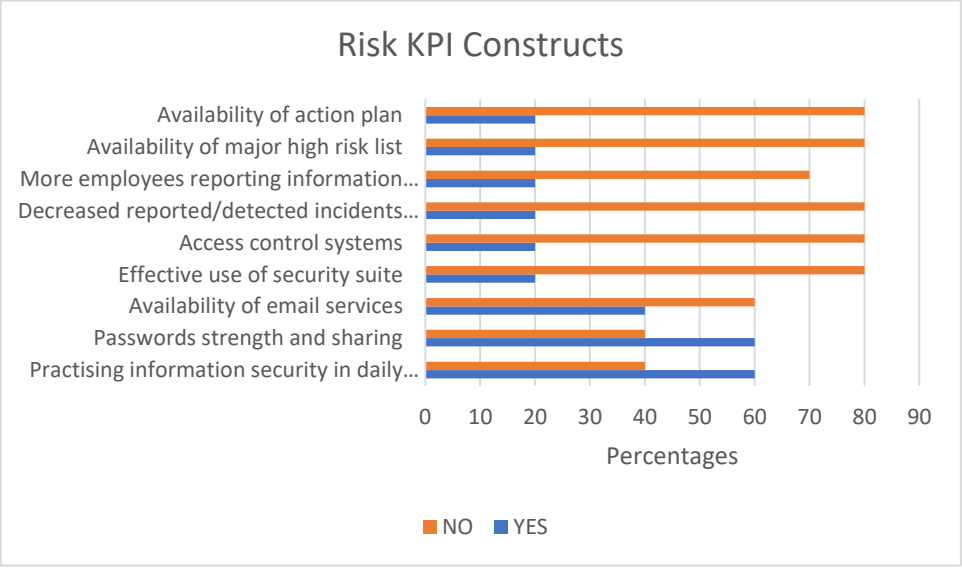

Figure 3. Analysis of Risk KPIs

The responses showed that 80% of the organisations do not have an action plan available in the event that disaster strikes, there are no access control systems in place like biometrics and face recognition to enhance security and there is no effective use of security suites. 80% of the respondents showed that there is also no increased reported/detected incidents due to internal users and less employees are reporting information security incidents. Most of the respondents also showed the absence of major high risk list and organisation email services highlighting that people mostly use the public email services like goggle and yahoo. 60% of the respondents showed that they are aware of the need to use strong passwords and practise information security in daily routine like backup data, setting file permissions and logging out when leaving their workstations. The risk KPI's responses show that there are poor risk mitigating controls in security programs of most of the organisations. Absence of monitoring of authorised access of resources and optimal recommended use of resources coupled with use of public email services is a disaster especially when people are working from home there is more tendency of abusing resources for personal use hence compromising organisation security. Knowing they are not being monitored, workers are inclined to swap and trade attachments like recorded and taped videos and photos which might inseminate pernicious and malevolent software into the enterprise's systems.

Posture

The indicator looks at the enterprise's information security maturity level and the processes/controls that need to be improved and why. Respondents were asked questions to enable assessment of the adequacy of the security program in terms of maturity capacity.

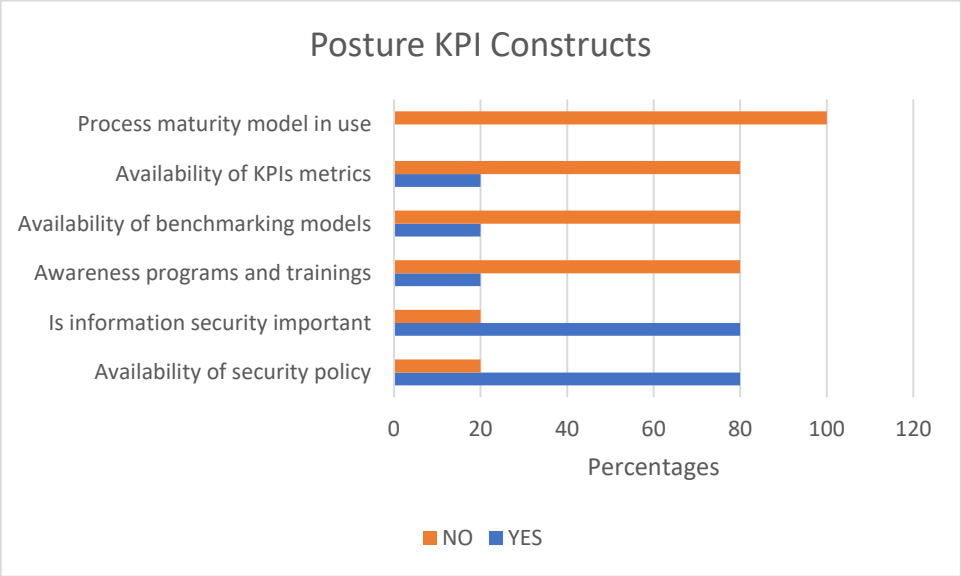

Figure 4. Analysis of Posture KPIs

80% of the organisations showed that they are aware that information security is important and they have a security policy in place. 80% of respondents showed that they are not aware of KPIs used by the organisation and there are no security awareness programs and trainings available. When employees become more conscious and aware of security issues it to a greater extent assists in the comprehensive safeguarding of the organisation's security. According to 80% of the respondents, there are also no benchmarking models available in the organisation meaning based on the ISO/International Electrotecnical Commission (IEC) ISO/IEC 15504 Information technology – Process assessment scale, maturity is ranked at low, which is a reflection on the inadequacy of the security program. 100% of the respondents said there is no process maturity model in place to use for maturity assessments that shows the security program is lacking in terms of maturity KPIs metrics. The current indicators of maturity are falling short of the desired indicators hence pointing to not sound security programs in the organisations.

Compliance

Questions were asked on the enterprise's major information security compliance and audit gaps indicators and the respondents' responses were noted. The process of compliance gap analysis must be established and well understood by senior management. The aim here is to point out the problems and solutions that may lead to better management of these activities.

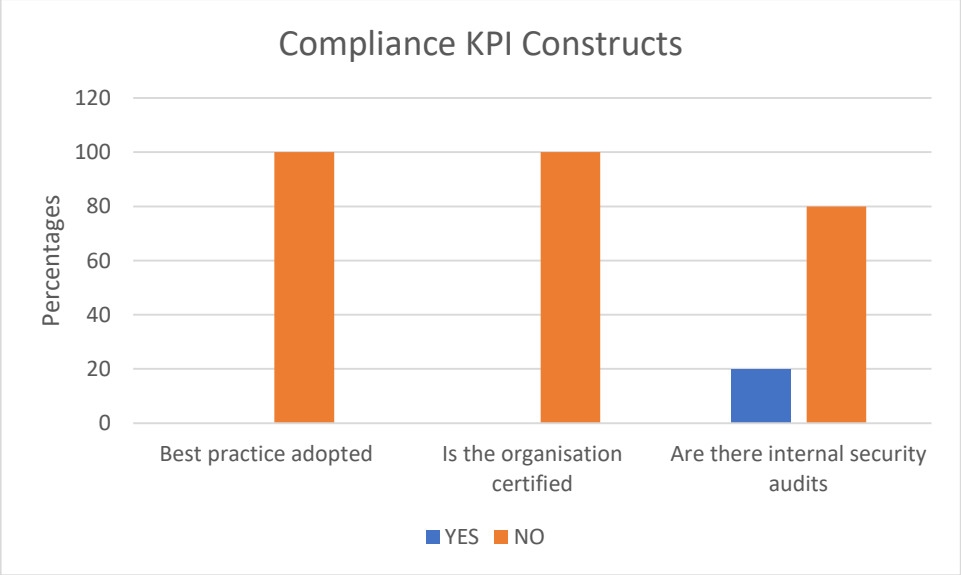

Figure 5. Analysis of Compliance KPIs

The responses showed that there are no Best Practices like COBIT, COSO and IS27005 to mention but a few adopted by the organisations. From the responses no organisation is certified or registered with security industry regulators and most (80%) of the organisations don't do internal security audits. The results show high compliance gaps hence reflecting on inadequacy of the security program. The findings tally with Wolcott Group (2008) study on assessment of information security governance benchmarks based on the ISO27001/27002 guidelines. The

study gave comprehensive findings on the lack an industry best practice based approach by enterprises when implementing security management. Their recommendation was that enterprises should adopt the ISO27001/27002 best practice at a strategic level to enhance security, save resources and to contribute to the success of the organisation. Nonetheless utilising ISO 27001/27002 best practices as they are may not be realistic and practical within general practises of small to medium enterprises as the codes of practice and recommendations are compound and intricate. This confirms Bernik and Prislan (2016)'s assertion that when taking note of the potential and competence of an ordinary enterprise suffering unfavourable economic conditions, specific codes of practice can be too intricate and challenging when it comes to mandatory skills and fiscal means. Considering small to medium enterprises in Zimbabwe are facing unfavourable economic conditions and disruptions caused by the prevailing Covid19 pandemic this is true.

5. Conclusion, limitations and recommendations

5.1 Conclusion

The research sought to evaluate the adequacy of information security programs available in small to medium enterprises in Zimbabwe making use of key performance indicators for security governance as a basis for measurement. Using the four generic KPI's strategy, risk, posture and compliance the research found out that most of the constructs of these KPI's are not being addressed thereby not providing sound security programs. For strategy KPIs there is no aligning of security objectives and business objectives and the objectives are not communicated to members so this contributes to inadequacy of security programs because Brotby (2009) states that it is difficult to come up with useful metrics when you do not have defined objectives for an information security program. Risk KPIs show lack of mechanisms to mitigate risks, Posture of the security program is ranked low as evidenced by the absence of maturity models and less security awareness programs, benchmarking models and known KPIs metrics. Compliance KPIs also show that security program is inadequate as showed by the absence of Best practices and internal security audits. This confirms Ernest and Young (2014) that says data concerning the present situation in the field of information security show that the management of this field is generally not sufficient and has a lot of poor practices All this show that the constructs of information security availability, confidentiality and integrity are not ascertained by the security programs available hence their inadequacy. Like Volchkov (2020) said, the security program will not propose initiatives apart from those coming from one of these sources/indicators therefore they need to realign them to the four strategic KPIs for them to be sound and address associated risks and liabilities. In other words, if a security project is not triggered by strategic alignment, the need to mitigate a risk, the need to fill a regulatory gap or the need to improve capacities to protect company assets, then there is no reason for senior executives to approve it. The available security programs for the organisations under study are not adequate according to the findings.

5.2 Limitations

The limitations to the study are that the study sample is not large enough to represent all the small to medium enterprises but this was because of Covid19 restrictions that could not allow the researcher to use a larger sample. The study was done using only qualitative methods since it was targeting small enterprises and aiming to present an instrument to enable a straightforward and practical evaluation of information security that will permit management to make future plans. This is therefore a limitation as well for the study can also be done applying a mixed approach which consequently can attain the most reliable results.

5.3 Recommendations

In light of the study carried out, the above presented discussion and the broad conclusions given, the following recommendations are given:

- Organisations should look at the constructs of the four generic KPIs strategy, risk, posture and compliance so as to come up with a sound security program.
- Organisations should conduct security awareness and training programs and workshops so that employees will be able to identify and verify suspicious content even when it is received from known sources and practise information security in daily routines.
- Organisations should create stronger access controls systems and use risk sensing solutions.

6. Further study

The study can be carried out further by looking at large enterprises for they are the ones with structured security departments security programs built upon best practices. The assessment will go a great way in assisting the organisations especially considering that almost half of their staff is working from home, and as long teams used to working from an access-controlled, audited, segregated and monitored environment where physical data protection risk areas were contained on the premises of the enterprise and more easily managed they really need to assess the adequacy of their security programs.

References

1. Agwu, E.M., and Murray, P.J. (2015). Empirical study of barriers to electronic commerce uptake by SMEs in developing economies, International Journal of Innovation in the Digital Economy, Vol. 6 No. 2.
2. Bakshi, S. (2016). Performance Measurement Metrics for IT Governance, ISACA Journal Vol. 6, www.isaca.org/archives.
3. Bernik, I., and Prislan, K. (2016). Measuring Information Security Performance with 10 by 10 Model for Holistic State Evaluation, PLOS ONE DOI:10.1371/journal.pone.0163050.
4. Bojanc, R., and Jerman Blazlic, B. (2008). An Economic Modelling Approach to Information Security Risk Management, International Journal of Management.

5. Chang, S.E., and Ho, C.B. (2006). Organisational factors to the effectiveness of implementing information security management. Industrial Management and Data Systems.
6. De Haes, S., and Van Grembergen, W. (2004). IT Governance and its Mechanisms; Information Systems Control Journal 1, Retrieved January 05 2021, from http://www.isaca.org.
7. Ernst and Young. (2014). Get ahead of Cybercrime. Insight on Governance, risk and Compliance, Global Information Security Survey. Available:http://www.ey.com/Publication/vwLUAssets/EY-globalinformation-security-survey-2014/$FILE/EY-global-information-security-survey-2014.pdf.
8. Hussey, D.M., and Eagan, P.D. (2007). Using Structural Equation Modelling to Test Environmental Performance in Small and Medium- Sized Manufacturers: SEM, Journal of Cleaner Production, Vol. 15.
9. Mahncke, R.J., McDermid, D.C., and Williams, P.A. (2009). Measuring Information Security Governance within General Medical Practice; School of Computer and Security Science, Edith Cowan University, Australian Information Security Management Conference.
10. Martin, L.M., and Matlay, H. (2001). Blanket Approaches to Promoting ICT in Small Firms: Some Lessons from the DTI Ladder Adoption Model in the UK, Internet Research, Electronic Networking Application and Policy, 11(5)
11. Munyoro, G., Mungana, S.L., Muchaendepi, P.D., and Nhevere, W. (2019). The Contribution of ICT in the Development of Small Business Sector in Zimbabwe: A Case Study of Harare Metropolitan; International Journal of Research in Business Management (IMPACT: IJRBM) ISSN (P): 2347-4572; ISSN (E): 2321-886X Vol. 7, Issue 4 April 2019.
12. National Computing Centre. (2005). IT Governance: Developing a Successful Governance Strategy: A Best Practice Guide for Decision Makers in IT, Go ISBN: 0-85012-877-8 v.
13. Niebel, T. (2018). ICT and Economic Growth – Comparing Developing, Emerging and Developed Countries, World Development Vol. 104 No. C.
14. Nguyen, T.H., Newby, M., and Macaulay, M.J. (2015). Information Technology Adoption in Small Business: Confirmation of a Proposed Framework, Journal of Small Business Management; 53(1):207±227. doi: 10. 1111/jsbm.12058
15. Pironti, J.P. (2007). Developing Metrics for Effective Information Security Governance, Information Systems Control Journal, 2 1-5. Retrieved January 02, 2021.
16. Qureshi,.M.S. (2011). Measuring Efficacy of Information Security Policies: A Case Study of UAE Based Company
17. Seshadri, D. (2020). Security and Privacy in the New Normal; ISACA Journal Vol6 2020 Issues.
18. Shinn, L. (2009). Slouching? Measure your Security Posture. Retrieved January 05, 2021 from Inc.TechnologyWebsite:http://technology.icn.com/security/articles/200805/posture.html
19. Sue, G. (2008). Business Research Methods. Ventus Publishing Aps.
20. Taylor, M., and Murphy, A. (2004). SMEs and E-Business, Journal of Small Business and Enterprise Development, 11 (3), 280-289.

21. Volchkov, A. (2020). Key Performance Indicators for Security Governance, Part 2 Security Reporting for Senior Management; ISACA Journal Vol6 2020 Issues.
22. Volchkov, A. (2020). Key Performance Indicators for Security Governance, Part 1, ISACA Journal Vol6 2020 Issues.
23. Whitman, M.E., and Mattord, H.J. (2004). Management of Information Security, Boston: Course Technology.
24. Wolcott Group. (2008). The 2007 ISO 27001 Benchmark study on Information Security Governance. A Benchmark Study Measuring the Effectiveness of organisations to Govern Information Security. Retrieved January 12, 2021 from http://benchmark. Wolcottgroup.com
25. Yin, R.K. (2002). Case study research: design and methods, Sage Publications