International Journal of Innovation Scientific Research and Review
Vol. 05, Issue, 03, pp.4202-4207, March 2023
Available online at http://www.journalijisr.com
SJIF Impact Factor 2023: 6.599

Research Article

ISSN: 2582-6131

THE IMPACTS OF CONTROL ENVIRONMENT, RISK ASSESSMENT, CONTROL ACTIVITY, INFORMATION AND COMMUNICATION TECHNOLOGY AND MONITORING ON ORGANIZATIONAL INTERNAL CONTROL: THE CASE OF MONGOLIA

*** RENTSENBYAMBA Damdinsuren**

Ph.D student at University of Internal Affairs, Mongolia.

Received 21th January 2023; Accepted 22th February 2023; Published online 30th March 2023

ABSTRACT

The aim of this study is to analyze the requirements for the impacts control environment, risk assessment, control activity, information and communication technology and monitoring on organizational internal control. There are many scholars studied the relationship factors organizational internal control in the world, but there are lack of study our topic in Mongolian public sector. Thus, we interested this topic in here. Current public and social trends have made it imperative for almost all large organizations to maintain an internal control system. The result of data determined through online in first quarter 2022 and estimated by SMART PLS 3.0 software and Cronbach's alpha index have been used for data analysis and reliability analysis of the questionnaire, respectively in our study. Our study from many others is we analyzed 5 hypotheses, one of them had a positive relationship with considered impacts. On the other hand, four hypotheses could not have positive relationship on considered impacts. Research has established the significant impact such as experience on organizational internal control in this study.

Keywords: control environment, risk assessment, control activity, information and communication technology and monitoring on organizational internal control.

INTRODUCTION

Globalization and the advancement in technology has become the hallmark for employers today and the public sector is no exception. Public organizations have been expanding their operations and activities beyond the domestic borders because of globalization and improved technology. The expansion of public sector, globalization and the advanced technology also exposes business to increased risk, fraud, altercations, and other irregularities. This has made internal controls an imperative system to maintain by every business and for that matter the banking sector. Globalization of businesses, technological advancements, increasing risk of social failures, the fraud and altercations that emerged in the public sector call for the proper maintenance of an effective internal control systems.

THEORETICAL FRAMEWORK

Internal controls are intended to prevent errors and irregularities, identify problems and ensure that corrective action is taken. In many cases, process owners within your department perform controls and interact with the control structure daily, sometimes without even realizing it because controls are built into operations.

Every organization needs strong internal controls to ensure the integrity of financial statements, promote ethical values, and drive transparency across the enterprise. Internal controls are the mechanism to do those things; controls help identify risks and reduce them to an acceptable level. Vital processes supported by robust internal control systems allow an organization to comply consistently with all applicable laws and regulations and to earn confidence, trust, and loyalty among its stakeholders. Internal controls also play an essential role in preventing employees and others from committing fraud.

***Corresponding Author: RENTSENBYAMBA Damdinsuren,**
Ph.D student at University of Internal Affairs, Mongolia.

Conversely, a lack of internal controls can weaken the integrity of accounting and financial reporting. Costs can rise because of reduced operational efficiency and increased potential for fraud and other kinds of crime. Ultimately, these issues affect the company's reputation and financial standing in the market.

Internal control is a process, effected by an entity's board of directors, management and other personnel, designed to provide reasonable assurance:

- That information is reliable, accurate and timely.
- Of compliance with applicable laws, regulations, contracts, policies and procedures
- Of the reliability of financial reporting

The internal control structure is derived from the way management runs an operation or function and is integrated with the management process. Although the components apply to the entire University, small and mid-size departments may implement them differently than large ones do. Together, they are designed to provide reasonable assurance that overall established objectives and goals are met. The internal control structure consists of five inter-related components:

Control environment and internal control

The control environment is the comprehensive set of actions taken by management that set the tone for how employees engage in their day-to-day activities. The control environment is comprised of all policies and procedures, the actions taken by management to deal with issues, and the values they espouse. Taken as a whole, the control environment shows the level of support that management has for the system of internal controls. A strong control environment is needed to reduce the number and severity of control failures within an organization. The control environment sets the tone of an organization, influencing the control consciousness of its people. Control environment factors include (1) the integrity, ethical values,

and competence of the entity's people; (2) management's philosophy and operating style; (3) the way management assigns authority and responsibility and organizes and develops its people; and (4) the attention and direction provided by the University. Additional examples are:

- Tone from the top
- University policies
- Organizational authority

A control environment, also called "Internal control environment", is a term of financial audit, internal audit and Enterprise Risk Management. It means the overall attitude, awareness and actions of directors and management (i.e. "those charged with governance") regarding the internal control system and its importance to the entity. They express it in management style, corporate culture, values, philosophy and operating style, the organisational structure, and human resources policies and procedures.According to the literature review, we were hypothesized as below:

Hyphothesis 1. Control environment have an influence on organizational internal control .

Risk assessment

A risk assessment is a process to identify potential hazards and analyze what could happen if a hazard occurs. Risk assessment determines possible mishaps, their likelihood and consequences, and the tolerances for such events. The results of this process may be expressed in a quantitative or qualitative fashion. Risk assessment is an inherent part of a broader risk management strategy to help reduce any potential risk-related consequences. More precisely, risk assessment identifies and analyses potential (future) events that may negatively impact individuals, assets, and/or the environment. It also makes judgments "on the tolerability of the risk on the basis of a risk analysis" while considering influencing factors. Risk assessment is the identification and analysis of relevant risks to achievement of the objectives, forming a basis for determining how the risks should be managed. Examples include:

- Monthly meetings to discuss risk issues.
- Internal audit risk assessment
- Formal internal departmental risk assessment

Risk assessments can be done in individual cases, including in patient and physician interactions. In the narrow sense chemical risk assessment is the assessment of a health risk in response to environmental exposures. The ways statistics are expressed and communicated to an individual, both through words and numbers impact his or her interpretation of benefit and harm. An individual´s own risk perception may be affected by psychological, ideological, religious or otherwise subjective factors, which impact rationality of the process. Individuals tend to be less rational when risks and exposures concern themselves as opposed to others.There is also a tendency to underestimate risks that are voluntary or where the individual sees themselves as being in control, such as smoking. Risk assessment can also be made on a much larger systems theory scale, for example assessing the risks of an ecosystem or an interactively complex mechanical, electronic, nuclear, and biological system or a hurricane (a complex meteorological and geographical system). Systems may be defined as linear and nonlinear (or complex), where linear systems are predictable and relatively easy to understand given a change in input, and non-linear systems unpredictable when inputs are changed.As such, risk assessments of non-linear/complex systems tend to be more challenging. In the engineering of complex systems, sophisticated risk assessments are often made within safety engineering and reliability engineering when it concerns threats to life, natural environment, or machine functioning. The agriculture, nuclear, aerospace, oil, railroad, and military industries have a long history of dealing with risk assessment. Also, medical, hospital, social service, and food industries control risks and perform risk assessments on a continual basis. Methods for assessment of risk may differ between industries and whether it pertains to general financial decisions or environmental, ecological, or public health risk assessment.According to the literature review, we were hypothesized as below:

Hyphothesis 2. *Control environment have an influence on organizational internal control*

.

Control activities – Control activities are the policies and procedures that help ensure management directives are carried out. They include a range of activities as diverse as approvals, authorizations, verifications, reconciliations, reviews of operating performance, security of assets and segregation of duties. Additional examples are:

- Purchasing limits
- Approvals
- Security
- Specific policies

The security is another preventive control activity. It's critical to limit physical access and implement internal controls for cash, equipment, inventory, checks, and all other assets considered business-critical for the organization. In addition to physical control, financial assets should be counted and compared with amounts shown on control records and documents. Internal Control Activities, unlike preventive control activities, detective controls aim to find errors and problems (and their root causes) after the mistakes have already occurred. Although these controls don't prevent problems from occurring, detective controls are essential because they provide an after-the-fact opportunity to identify, understand, and correct irregularities. Detective controls are implemented to support organizational objectives such as fraud prevention, legal and regulatory compliance, and quality control. These controls also confirm that the organization's preventive controls are operating as intended.According to the literature review, we were hypothesized as below:

Hyphothesis 3. *Control environment have an influence on organizational internal control .*

Information and communication technology and internal control

Information and communications technology is an extensional term for information technology that stresses the role of unified communications and the integration of telecommunications (telephone lines and wireless signals) and computers, as well as necessary enterprise software, middleware, storage and audiovisual, that enable users to access, store, transmit, understand and manipulate information. Information and communications technology is also used to refer to the convergence of audiovisuals and telephone networks with computer networks through a single cabling or link system. There are large economic incentives to merge the telephone networks with the computer network system using a single unified system of cabling, signal distribution, and management. Information and communications technology is an umbrella term that includes any communication device, encompassing radio, television, cell phones, computer and network hardware, satellite systems and so on, as well as the various services and appliances with them such as video conferencing and distance learning. Information and communications technology also includes analog technology, such as

paper communication, and any mode that transmits communication. Information and communications technology is a broad subject, and the concepts are evolving. It covers any product that will store, retrieve, manipulate, transmit, or receive information electronically in a digital form (e.g., personal computers including smartphones, digital television, email, or robots). Skills Framework for the Information Age is one of many models for describing and managing competencies for information and communications technology professionals for the 21st century. Information and communication technologies is defined as a diverse set of technological tools and resources used to transmit, store, create, share, or exchange information. These technological tools and resources include computers, the Internet (websites, blogs and emails), live broadcasting technologies (radio, television and webcasting), recorded broadcasting technologies (podcasting, audio and video players, and storage devices) and telephony. According to the literature review, we were hypothesized as below:

Hyphothesis 4. *Information and communication technology have an influence on organizational internal control*

.

Monitoring

Monitoring involves paying close attention. It's a type of systematic observation.Monitoring of a program or intervention involves the collection of routine data that measures progress toward achieving program objectives. It is used to track changes in program outputs and performance over time. Monitoring provides regular feedback and early indications of progress (or lack of progress). Its purpose is to permit the management and stakeholders to make informed decisions regarding the effectiveness of programs and the efficient use of resources.

Internal control systems need to be monitored, a process that assesses the quality of the system's performance over time. This is accomplished through ongoing monitoring activities, separate evaluations, or a combination of the two. Ongoing monitoring occurs during operations. Internal control deficiencies should be reported upstream, with serious matters reported to top management and the Regents. The benefits of monitoring are:

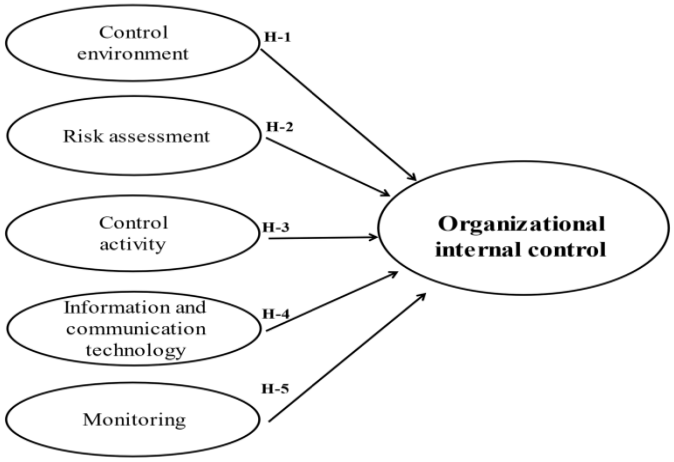
- Ensure that the allotted budget is spent correctly and can be altered if needed.
- To make sure that the selected task and deadlines are met.
- To encourage accountability regarding the task assigned by the members of the team.
- To shift the workforce to a particular task if it requires so.
- To boost communication between the team members to increase quality and reduce time.

The monitoring happens after the plan is implemented. You need to take a few steps to track the project. First, you need to share the workload according to the capacity of your teammates. You need to figure out the issue you may encounter related to budget and time. Third, you need to share the workload according to the capacity of your teammates. Monitoring is a key component of any system. Process monitoring informs management and a donor about the actual implementation of project activities in the field.

At the same time process monitoring let the project staff on ground know how well they implements the project and what improvement they can bring to the work they are doing in field.Process monitoring is conducted using checklists and guidelines. Those checklists are developed jointly with project staff. The same checklists and guidelines are used by field staff while implementing project activities. Participants were shared a sample of monitoring guidelines. To undertake process monitoring, a monitoring tool is required that capture the following information. According to the literature review, we were hypothesized as below:

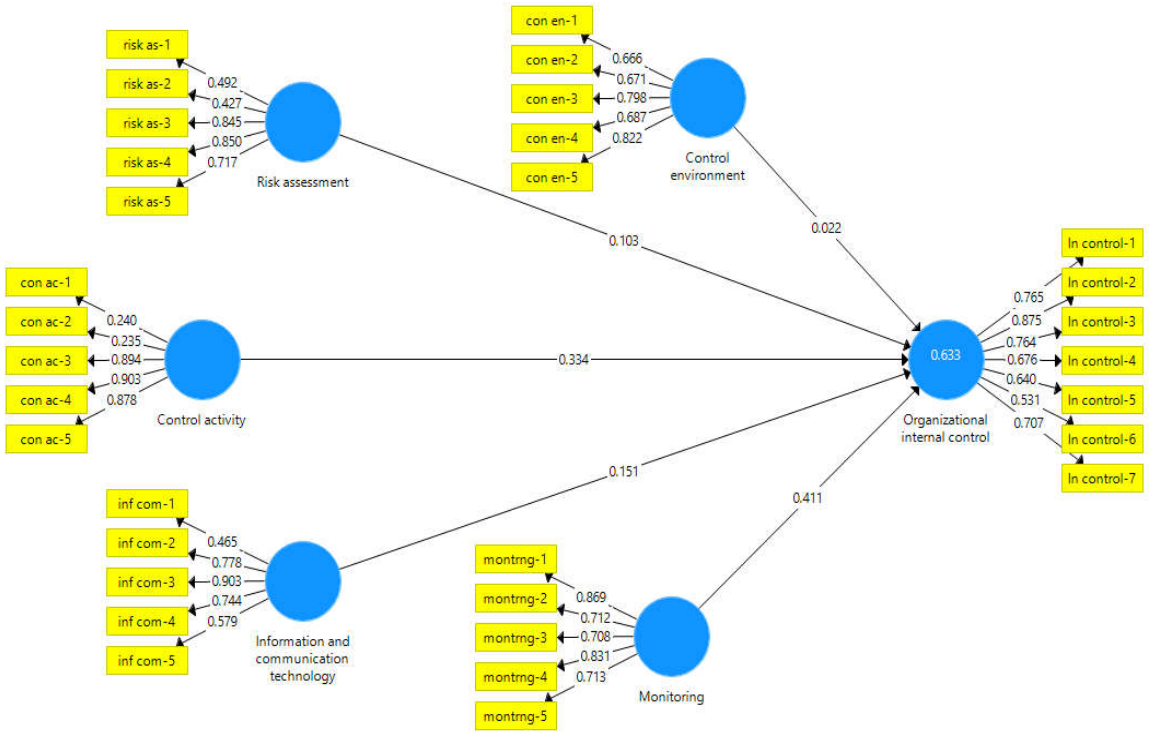
Hyphothesis 5. *Information and communication technology have an influence on organizational internal control .*

Figure 2.1. Conceptual models of factors on organizational internal control



RESULT OF STUDY

We studied to includetwo kinds of problems in terms of theoretical and practical frameworks. The first, in theoretical frameworks, previous researchers dem attention on performance management in many public organizations. Second, from the practical frameworks deemed attention in a fiscal year in 2022.



***Noted*:** con en- control environment, risk as- risk assessment, con ac- control activity, inf com- information and communication technology, montrng- monitoring, In control- Organizational internal control

Table 1. List of items of control environment for each Construct of respondents

Factor	item	Results of item	Cronbach's alpha	CR	AVE
Control environment	con en-1	0.666	0.784	0.851	0.536
	con en-2	0.671			
	con en-3	0.798			
	con en-4	0.687			
	con en-5	0.822			

Notes: con en- control environment

In table 1, control environment of 5 items measuring ranged from **0.666**-**0.822**, Cronbach's Alpha of **0.784,** Composite Reliability (CR) of **0.851,**Average Variance Extracted (AVE) was **0.536.**

Table 2. List of items of risk assessment for each Construct of respondents

Factor	item	Results of item	Cronbach's alpha	CR	AVE
Risk assessment	risk as-1	0.492	0.709	0.809	0.475
	risk as-2	0.427			
	risk as-3	0.845			
	risk as-4	0.850			
	risk as-5	0.717			

Notes: risk as- risk assessment

In table 2, risk assessment of 5 items measuring ranged from **0.427**-**0.850**, Cronbach's Alpha of **0.709,** Composite Reliability (CR) of **0.809,** Average Variance Extracted (AVE) was **0.475.**

Table 3. List of items of control activity for each Construct of respondents

Factor	item	Results of item	Cronbach's alpha	CR	AVE
Control activity	co ac-1	0.240	0.713	0.799	0.500
	co ac-2	0235			
	co ac-3	0.894			
	co ac-4	0.903			
	co ac-5	0.878			

Notes: con ac- control activity

In table 3, control activity of 5 items measuring ranged from **0.235**-**0.903**, Cronbach's Alpha of **0.713,** Composite Reliability (CR) of **0.799,** Average Variance Extracted (AVE) was **0.500.**

Table 4. List of items of information and communication technology for each Construct of respondents

Factor	item	Results of item	Cronbach's alpha	CR	AVE
Technical equipment	Tech-1	0.465	0.832	0.829	0.505
	Tech -2	0.778			
	Tech -3	0.903			
	Tech -4	0.744			
	Tech -5	0.579			

Notes: *tech-technical equipment*

In table 4, information and communication technology of 5 items measuring ranged from **0.465**-**0.903**, Cronbach's Alpha of **0.832,** Composite Reliability (CR) of **0.829,** Average Variance Extracted (AVE) was **0.505.**

Table 5. List of items of monitoring for each Construct of respondents

Factor	item	Results of item	Cronbach's alpha	CR	AVE
Monitoring	montrng-1	0.869	0.825	0.878	0.592
	montrng-2	0.712			
	montrng-3	0.708			
	montrng-4	0.831			
	montrng-5	0.713			

Notes: montrng- monitoring

In table 5, monitoring of 5 items measuring ranged from **0.708-0.869**, Cronbach's Alpha of **0.825,** Composite Reliability (CR) of **0.878,**Average Variance Extracted (AVE) was **0.592.**

Table 6. List of items of internal control for each Construct of respondents

Factor	item	Results of item	Cronbach's alpha	CR	AVE
Organizational internal control	IN CONTROL-1	0.765	0.837	0.878	0.512
	IN CONTROL-2	0.875			
	IN CONTROL-3	0.764			
	IN CONTROL-4	0.676			
	IN CONTROL-5	0.640			
	IN CONTROL-6	0.531			
	IN CONTROL-7	0.707			

Notes: In control- Organizational internal control

In table 6, organizationalinternal control of 7 items measuring ranged from **0.531**-**0.875**, Cronbach's Alpha of **0.837,** Composite Reliability (CR) of **0.878,**Average Variance Extracted (AVE) was **0.512.**

Table 7. Estimated Path Coefficients of respondents on organizational internal control.

Hypothesis	Standard deviation	T Statistic	P value	Remarks
H1. Control environment positive related on organizational internal control.	0.138	0.159	0.874	No supported
H2. Risk assessment positive related on organizational internal control.	0.151	0.682	0.496	No supported
H3. Control activity positive related on organizational internal control.	0.181	1.843	0.077	No supported
H4. Information and communication technology positive related on organizational internal control.	0.178	0.846	0.398	No supported
H5. Monitoring positive related on organizational internal control.	0.134	3.073	0.002	Supported

Notes: *The result of study*

In table 7, Hypothesis 1 such as control environment have not related on organizational internal control (Standard deviation 0.138), (T statistic 0.159) and (P value 0.874). Hypothesis 2 such as risk assessment has not related-on organizational internal control (Standard deviation 0.151), (T statistic 0.682) and (P value 0.496). Hypothesis 3 such as control activity has not related-on organizational internal control(Standard deviation 0.181), (T statistic 1.843) and (P value 0.077). Hypothesis 4 such as information and communication technology have no related-on organizational internal control (Standard deviation 0.178), (T statistic 0.843) and (P value 0.398). Hypothesis 5 such as monitoring has related on organizational internal control(Standard deviation 0.134), (T statistic 3.073) and (P value 0.002).

CONCLUSION

We studied in the fiscal year of 2022 our paper collected and delivered an online-form- questionnaire with an official inquiry that requested quantitative and qualitative surveys in our study. There are participated 185 public servants who work education, health and special service sector. One of them is supported and four of them is not supported in path analysis. We are recommending our study as bellow:

a. To study more hypotheses, result in the future.
b. To study and compare factors on organizational internal control with another special agency.
c. To study and compare the factors with foreign scholars' study in the future.

Finally, we will study our next research paper, need to correlation skills, leadership, job satisfaction, engagement, behavior with organizational internal control etc.

REFERENCES

Ashima Aggarwal, G. T. (2017). Techniques of Performance Appraisal. Semantic Scholar, 254-268.

Cooper, H. (1998). Synthesizing research: A guide for literature 3rd ed. Oaks: CA: Sage Publications, Thousand.

Cross Ogohi Daniel, S. J. (2020). Effective time management on employee performance. International journal of research science & management, 72-84.

Imran Khan, H. D. (2014). Impact of Attitude on Employees Performance: A Study of Textile Industry in Punjab, Pakistan. World Applied Sciences Journal, 191-199.

Nishant Uppal, N. V. (2014). Prior Related Work Experience and Job Performance: Role of personality. International Journal of Selection and Assessment, 39-44.

Stoyanova, I. G. (2011). Skill and Performancebjir_779 515..536. British Journal of Industrial Relations, doi: 10.1111/j.1467-8543.2010.00779. 2011 0007–1080 pp. 515–536.

Imran, A. (2019). Personality traits, individual innovativeness and satisfaction with life. Journal of Innovation and Knowledge, 38-46.

Janie, B. B. (2006). Ethics in Organizations and Leadership. Jones and Bartlett .

Klingborg, D. J. (2014). What Is Leadership? Leadership and Professional Development, 280-285.

Mihelič, K. K. (2010). Ethical leadership. International Journal of Management and Information Systems, 31-44.

Sharma, R. T. (n.d.). Managerial Skills for Managers in the 21st Century.

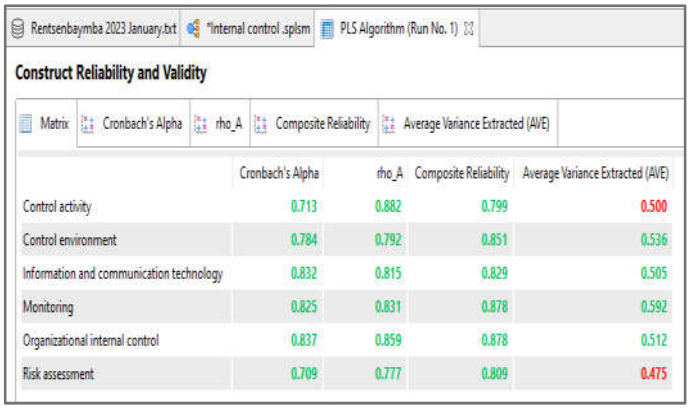
Singh, S. K. (2008). Role of leadership in knowledge management: A study . Journal of Knowledge management , 3-15.

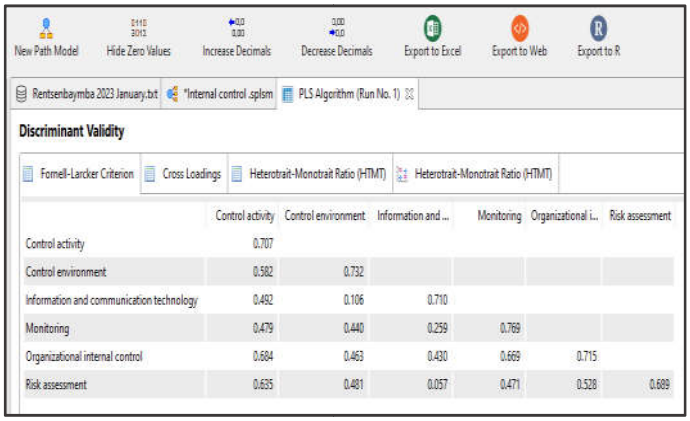
Smuthy, P. (2012). The Relationship between Managerial Skills and Managerial Effectiveness in a Managerial Simulation Game . Etrategia Organizaion Czech Science Foundation, 11-21.

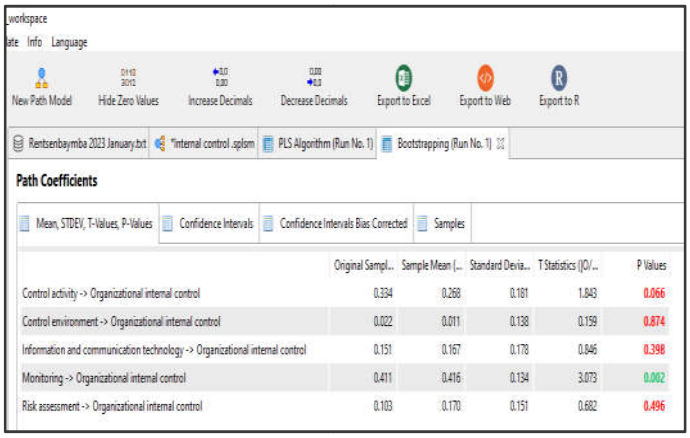
Stogdill, R. (1948). Personal factors associated with leadership: A survey of the literature. Psychol, 64.

WK Hoy, C. M. (1987). Educational Administration: Theory, Research, and Practice 3rd ed. New York: Random House .

EVIDIENCE OF STUDY







****