ATLANTIS PRESS

Advances in Social Science, Education and Humanities Research, volume 348

3rd Asia-Pacific Research in Social Sciences and Humanities (APRiSH 2018)

Business Process Automation: Internal Audit Function Adaptation Lesson Learned from Indonesian Public Sector

Syanni Yustiani
Accounting Department, Faculty of Economics and Business
Universitas Indonesia
Indonesia
syanni.yustiani@gmail.com

Muhammad Ichsan
Accounting Department, Faculty of Economics and Business
Universitas Indonesia
Indonesia
muhammadichsan@yahoo.com

***Abstract*—The purpose of this study is to analyze the transformation of the Inspectorate General (ITJEN) at the Ministry of Finance as an impact of the Directorate General's (DGT) Taxation System Information (SIDJP) implementation. This study uses a case study and a qualitative approach with institutional theory to study the problem. Data collection is performed via documentation and interviews with key informants from the Institute of Internal Auditors (IIA), the DGT of Taxation, the Indonesian Supreme Audit Institution, the State Development Audit Agency, and the Auditor of Inspectorate General of Ministry of Finance. This study shows that the implementation of SIDJP engendered adaptation of ITJEN's scope and practice, structure, auditor skill requirements, audit tools, audit sizes, and relationship with information technology departments, whereas the audit source and its relationship with the external auditor remained the same.**

Keywords—Internal audit, system information, institutional theory, institutional logic, Business Process Automation, Indonesian Public Sector.

I. INTRODUCTION

Business process automation has been conducted for centuries, beginning long before the first industrial revolution with the invention of steam engines in 1775. Automation was performed by companies to improve performance, reduce errors, and improve the speed and quality of work through logistics, management, and business functions extant in companies [1].

Business reengineering and simplification resulting from automation threatens some occupations, especially those that do administrative work. Frey and Osborne studied work that was projected to be replaced by computers. From 702 types of jobs in the American labor market, they predicted that 47% would be replaced by computers and automation over two decades. Accountants and auditors were quite vulnerable, with 94% of tasks predicted to be replaced by computers [2].

The IIA in 2017 stated that business transformation caused by automation was a top-10 hot audit topic worldwide. The technological revolution improves businesses efficiency, but it also changes corporate risk. Such changes further require that the internal auditor make adaptations because of new business risks. Thus, the scope of auditing becomes wider, and the development of embedded technologies demand an internal audit with qualified technology [3].

The Inspectorate General (ITJEN) of the Ministry of Finance held an internal audit because of the same phenomenon. The Directorate General (DGT) of Taxes was an official auditee. The DGT Information System (SIDJP) was implemented in 2008 to perform most of the ITJEN of Taxes (DJP) core business administration activities. In 2017, the DGT of Taxation held its 2nd business transformation, implementing the CORETAX System, an upgrade to SIDJP, which will be used in all core business processes using a single database so that it will become more integrated and paperless.

The development of information systems at the DGT of Taxation is the main concern of the Ministry of Finance with the ITJEN as the internal auditor. DGT looks at high-risk institutions having responsibilities for management of government tax revenues of 1.618 trillion Rupiah, 73% of the total state budget in fiscal year 2018, accounting for most SIDJP information technology (IT) managers, compared to other echelons in the Ministry of Finance (~1,110 or 50% of the total 2,068 managers). Furthermore, to support the development of information systems in the DGT, the Ministry of Finance will allocate 49% of the ICT budget to the ministry level by 2018 [4]

Implementation of information systems within the organization will affect the organization and the existing professions within the organization. The organization for Economic Cooperation and Development (1988) said that information systems were highly pervasive, affecting all aspects of organizational performance, having the potential to influence the social and economic position of the entire nation and region [5]. Vowler [6] argued that the application of IT not only changes the business process of the organization, it also increases risks and the need to control and mitigate them. Vowler [6] increased risk because of the inability of the organization to engage the business when the system was not working properly, and he used technology to connect globally with external entities [7].

Research on internal audit functions that have changed because of the implementation of information systems was performed by Elbardan and Kholeif [9] on four types of companies in Egypt. The study resulted in the conclusion that enterprise resource planning resulted in adaptation through changes of structure and processes from the internal audit function to maintain legitimacy. Saharia, Koch and Tucker [10] examined the internal auditor's ability to identify and

manage risks associated with the application of information systems in the company. The study concluded that internal auditors faced higher technical risks, whereas financial and operational risks were reduced because of the application of information systems.

The research related to this problem was mostly done in companies in developed countries with private companies. No research was done to investigate this phenomenon in public-sector ministries. Results were reinforced by the innovation report of a development of information and communication technology audit within the Ministry of Finance in 2017, which stated that there were various deviations between the actual conditions realized with ideal conditions planned. With the DGT performance report prepared by the Supreme Audit Board, which stated that the management and control of the tax information system was in compliance of monitoring taxpayers [11], the presentation of tax receipts and tax receivables [12] has not been effective. This supports the urgency to improve good governance and supervision of the DGT of Taxes conducted by ITJEN. These things push researchers to conduct research on business process automation and internal audit function adaptation lessons learned from the Indonesian public sector. We conduct this research by addressing two research questions. "What are the control assumptions of the DGT Information System that influence the adaptation of ITJEN as an internal auditor?" "How does ITJEN adapt after SIDJP is implemented in the DGT of Taxes?"

II. Research Methods

This research is structured with a qualitative approach, specifically descriptive research or content analysis. In this research, the phenomenon described is the impact of information-system implementation in the DGT (SIDJP) to the structure and business processes in ITJEN. This research uses several techniques and data collection tools as follows.

A. Library Studies

A literature review is performed by studying a number of reports, journals, books, articles, and other research results to obtain a theoretical framework to frame the foundation of this study. Additionally, the literature study is also conducted by studying the provisions and regulations of the current internal audit function of the Indonesian government.

B. Field Studies

Field studies are conducted via in-depth interviews with competent persons in internal audits and taxation. To obtain a comprehensive and objective overview of the phenomena, the authors conducted in-depth interviews with the Governor of the Public Relations Committee, the Governor of the Research Committee [13], the State Accountant Representative (BPKP) Computer Functional Staff at the DGT TIP Directorate, the Supreme Audit Board Auditors (BPK), the IT Audit Group Coordinator, the Young Auditor Inspectorate VII and Group Coordinator Inspectorate I. To gain more focus, this research faces some limitation as follows. This research only discusses the DGT of tax business process transformation under ITJEN, and this research only discusses the application of SIDJP in the DGT of taxes.

III. Literature Review and Theory

A. Development of the Internal Audit Function

Auditing is a social phenomenon judged by its practical utility. Its function has evolved in response to the needs of individuals and groups in communities seeking information, guaranteeing behavior or performance of entities that recognize and have legitimate interests [14]. Reeve expressed the collective effect of increasing complexity and transaction volume, the distance between the owner and manager (principal) of the source of the transaction and the potential bias of the reporting agent (agent), the need for technical expertise (accounting) to review and summarize the activities of business, the need for organizational status to ensure independence and objectivity, and the need for necessary procedures to become the eyes and ears of management. All of these things contributed to the creation of internal audit departments within organizations. Starting as an internal business function focused primarily on fraud protection in payroll systems, cash theft, and other assets, the scope of internal audits was rapidly expanded to verify almost all financial transactions, gradually shifting from audit for management to audit of management [15].

The internal auditor's role is divided into two activities: assurance and consultation. Assurance activities are defined as objective reviews of evidence to independently assess governance, risk management, and control systems within the organization, whereas consultancy activities are defined as those providing advice on client–service activities, where the type and scope of activities are based on agreement with clients. These activities aim to provide added value and improve governance, risk management, and control systems within the organization [16].

B. Three Lines of Defense Concepts

The 2013 IIA issued a position paper on the Three Lines of Defense in Effective Risk Management and Control. In the paper, IIA clearly divided roles and tasks related to the implementation of risk management and control in an organization. The concept used three defense lines in organizational governance as follows [16].

- The first line of defense comprises management-control systems.
- The second line of defense comprises various controls related to organizational risks and controls over compliance with oversight functions.
- The third defense line is supervised by an independent party.

C. Information System Implementation and Organizational Governance, Risk, and Control (GRC)

Governance and risk management are explicitly intertwined. McNamee and Selim (1998) said that corporate governance represented an organization's strategic response to risks faced. In the process, risk becomes a major component of corporate governance so that internal audit has changed from a control-based approach to a risk-based approach [7]. Vowler [6] suggested that key factors underpinning better governance requirements caused by the implementation of IT increased the dependence on technology in executing business processes and activities. Implementing IT not only changes the

organization's business processes, it also increases the risk and need to mitigate those risks. Vowler [6] discussed the increased risk of an organization's inability to resume business when the system is not working properly, using technology to connect globally with external entities [7].

The work of Felix, Gramling, and Maletta [8] stated that internal auditors could increase the benefits of IT by formulating and influencing the strategic direction of the organization's policies. The internal auditor can also coordinate with the external auditor in reviewing the application of IT to improve the scope of the audit. Board directors and senior management support this cooperation with the assumption that it will reduce overall audit costs [7] (Ramamoorti, 2004). The broader scope of the audit, followed by a reduction in total audit costs with improved audit effectiveness, will improve corporate governance by improving oversight, accountability, and accuracy of corporate transactions and financial statements.

In clause 1,220 of the IPPF [3] it is said that the auditor should apply the principle of prudence thoroughly by applying professional due diligence and expertise. Clause 1,220.A2 stated that auditors should consider using audits with the help of technology or other analytical techniques. IIA [3] classified technologies supporting the performance of audit management system, data analytics, data mining, continuous auditing, and integrated technology solutions, where one application management service is combined with data analytics and data mining.

D. Theoretical Framework

Institutionalization according to Avgerou [5] is a process by which social patterns and rules can be accepted as social facts. Institutional theory describes and explains existence and strength as a result of interactions with the external environment influencing the formulation of rules, beliefs, values, and norms (Fogarty, 1996). There are two main principles of institutional theory.

1) *The institutional environment* is built on the social environment and affects individual behavior. Conversely, individual behavior affects the environment. Thus, it is humans who create institutional environments [17, 18].

2) *The organization* is seen as an open system, where the organizational structure and activities are shaped by the external environment and the actors of an organization. The ability to adapt environmental change is central to an organization's survival.

Friedland and Alford [20] developed the concept of institutional logic in the context of explaining the relationship between individuals, organizations, and society. They viewed organizations as patterns of activities based on material practices and systems in which individuals and organizations produce and reproduce their materials and make their experiences meaningful.

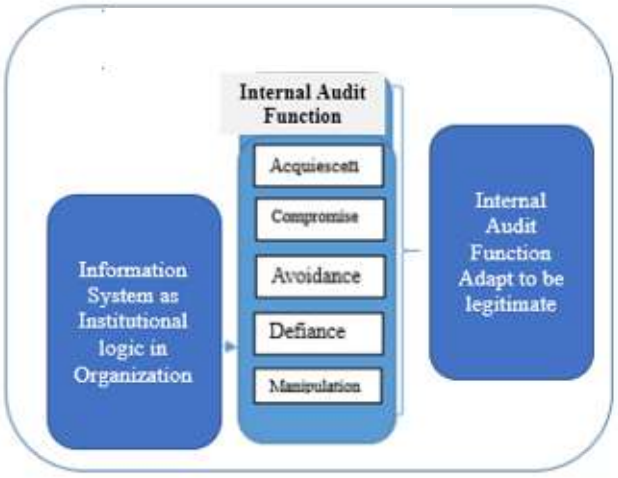
The information system is the subject of institutional pressure related to governance and control. Both serve as the foundation of institutional logic for information retention by maintaining rules of governance and control by limiting the activities of individuals within a particular model of interaction that may be unwanted by such individuals [9]. Studying the content of institutional logic contained in the information system will make it easier to understand and explain the nature and type of relationships between organizations and individuals [20]. Control is considered a principle commonly associated with logical rationalization and the focus of procedures in information systems that affect the internal audit function [21].

Oliver [19] developed institutional theory relate to resource dependence theory, which produced predictive organizational strategies in response to institutional processes. In the research, the resulting response comprises five types of responses.

- Acquiescence: organizations accept under institutional pressure.
- Compromise: the organization sees that the alignment of institutional pressure cannot be done completely, because there is a difference between institutional demand and organizational goals for efficiency and autonomy. Finally, the organization performs a compromise tactic with external parties.
- Avoid, organizations try to avoid the need for alignment. This strategy can occur in three forms (conceal, buffer and escape).
- Defiance: the organization actively rejects the institutional processes.
- Manipulate: the most active response, because the organization intends to actively change or exert its power for the purpose of the organization or, at its source, to strengthen the organization's position.

E. The Role of Basic Theory

This study uses institutional theory to explain the implementation of SIDJP as institutional logic, causing business processes to become unstable and require adaptation. ITJEN strategies were also discussed as an adaptation response based on the strategic criteria developed by Oliver [19].



Source: Elbardan And Kholeif

Fig.1. Research Framework

IV. Results and Discussion

A. Control of DGT Information Systems

Control is considered a principle commonly associated with logical rationale and the focus of procedures in information systems affecting internal audit functions [21]. The information system offers a better governance environment through various control assumptions [9]. Therefore, the authors analyze the assumptions of control principles in SIDJP, as follows.

1) Automation

SIDJP helps change business processes in the DGT to automatically reduce the human need to administer data. The SPT recording process is the example. Whereas the former tax information system (SIP) is implemented, it is still manually processed, so that it requires a large number of employees to accomplish the recording.

The automation process is accomplished via the introduction of a data-input application (e.g., e-SPT, e-filling, payment, MP3, and e-registration). Because of the implementation of SIDJP, the need for employees to operate this business process reduces, so that the idle human resources can be used in other business processes that provide added value. However, the application of SIDJP has not fully automated all business processes, because there are some functions that still must be manually performed, like case-management entry data.

Each process in SIDJP is automatically recorded in a log book that can be accessed by the DGT IT manager and auditor to see if there are any anomalous activities that can be followed up with supervision. SIDJP has also changed the basis of previous documentation transferred into data streams via user activity. SIDJP will automatically update data stored in a database and taxpayer profile. In the past, before SIDJP implementation, all work was accomplished using the local Kantor Pelayanan Pajak (KPP) database. Then, synchronized data with central database that is updated manually.

2) Consistency of data through centralization.

The application of SIDJP alters the data storage process that is originally spread over the local database, comprised of 331 primary tax offices throughout Indonesia into a centralized database at DGT headquarters. The current Minister of Finance provides clear direction for data centralization, aiming to improve the quality of data related to data consistency issues and transparency. Despite centralized database policies, local databases linked to the current central database are retained. The information in the local database is not as complete as the central database and is used for local specifics (e.g., local tax returns). Data centralization also makes it easier for the auditor to request data to be used in the auditee oversight process, both at the KPP and at the DGT headquarters.

3) Standardization

SIDJP has implemented standardized formats in business processes that run from the required documents. The processes flow through to the format of the final report and outcome of the activities performed. Prior to application of SIDJP, the legal product formats created differ according to the preferences of each person, meaning that there are differences in fonts and paper sizes. However, by using the SIDJP, especially in the case management (CM) section, all legal products have the same form according to the format provided and the same workflow of a legal product. In CM, all jobs have their own workflow so that they cannot be mixed with other types of workflows. This creates standardized business processes. SIDJP restricted users to customize the data formats and procedures developed by implementing controls. This makes it easy for internal auditors to detect anomalous activity.

4) Transparency

The digitalization of processes and activities through SIDJP has improved their transparency. It is also reinforced by the interdependence of data because of the use of a single database. Thus, each section involved in the process at SIDJP will observe indirectly the work of other sections. The digitalization process also provides additional monitoring tools for management and internal audit logs for CM.

5) Data security

When maintaining data security in SIDJP, the DGT's IT managers apply controls to provide assurance for the integrity and security of data owned, as follows.

- Authentication: the user must enter a username and password to be able to access SIDJP.
- Authorization: user authority is adjusted to the duties and functions related to the positions assigned.
- Every activity in SIDJP is recorded in the log book so that it will be possible to monitor suspicious transactions.
- Centralized databases and applications make it easier to implement consistent and more reliable controls via single application control strategies prior to the non-uniform implementation of SIDJP, individually conducted by each KPP.

Data security should be the main focus of the internal auditor, because, when data security is not guaranteed, the integrity of data owned will be uncertain. When the internal auditor uses the data without integrity as its input in the process of supervision, it will produce bad output.

6) Ongoing monitoring

The CM module in SIDJP allows the control of user-initiated processes. In addition to providing tools for monitoring the progress of work performed, the CM module also provides an alarm for unfinished work. SIDJP also allows data processing and implementation of controls in real-time. This provides an adequate infrastructure for continuous auditing. Nevertheless,

some respondents from the ITJEN, IIA, and BPKP stated that the installation of continuous audit tools directly in the auditee's proprietary information system was inhibited in terms of regulations that authorize internal audits and slightly violated the concept of three lines of defense because of the responsibility to follow anomalies recognized by direct-attached surveillance tools in management information systems are the responsibility of management as the first line of defense. The internal auditor is the third line of defense but must test based on management assertion. Thus, the most appropriate function is the internal audit, which should provide supervision based on management assertions with the help of IT used by both auditee and auditor to facilitate the preparation of management reports to support the function ITJEN as ex-ante auditor.

B. Adaptation of Internal Audit Function

1) Scope of services and practices

Implementation of SIDJP through control as institutional logic has driven governance changes in the DGT and the changes require the ITJEN to adapt to these changes to maintain its legitimacy as an internal audit function. The governance change from a traditional environment to an IT-based environment will encourage the auditor to have a different control focus.

In the governance of IT organizations, the responsibility of internal auditors increases with the emerging obligation to supervise the governance of IT, (e.g., SIDJP). Thus, the reliability of the information system becomes key to the relevancy of outputs produced by SIDJP as the sources for monitoring. In IT business processes, supervision at DGT is performed differently than traditional audits, which use application processing data from the auditee. The results of data processing from the IT audit unit presents an anomaly that will be confirmed by the internal auditor.

All interview respondents of this study agreed that the application of the information system provided the infrastructure and generated demands for continuous monitoring, The inspectorate with its IT audit unit also initiated continuous audits of the DGT business process. However, at this time, the ITJEN has not been given the authority to provide continuous updating of data from the auditee. Thus, updated data in the new ITJEN data portal will be given after showing the assignment letter to the DGT.

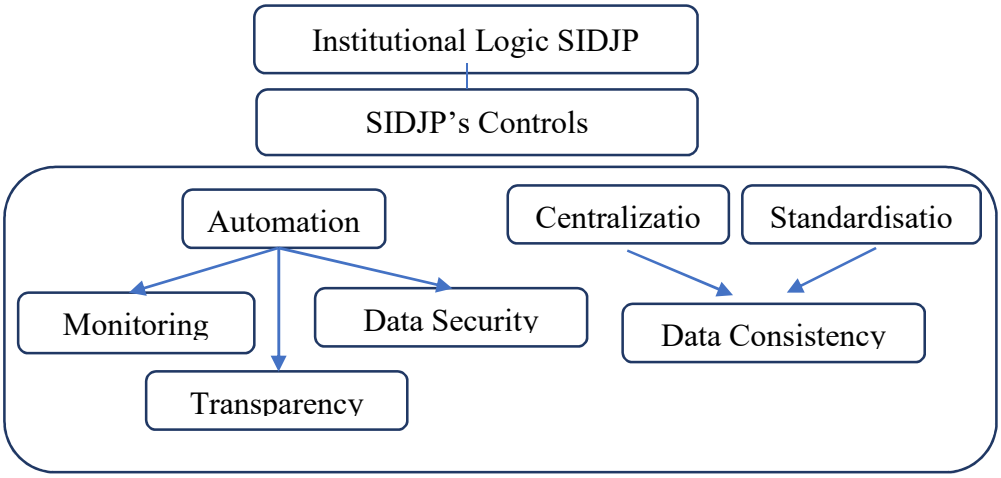


Fig.2. Controls Embedded in SIDJP

The integration of data in one database at the Ministry of Finance is designed to meet the requirement of the Minister of Finance to have consistency of data. However, the regulation for implementation has not been written. Implementation of the concept of Continuous Audit actually get support from our responden, IT managers in DJP, because it is considered will simplify the provision of data for auditors.

a) Structure of the internal audit function.

The change in governance of an IT-based auditee has led to a change in the structure of the ITJEN with the addition of an IT audit unit responsible for overseeing the reliability of information systems applied to auditee management. Changes also occur in the composition of the audit team, where an integrated audit concept is introduced, and oversight in governance based on IT has supported the need for an IT specialist on the operational audit team. It seems that the implementation in ITJEN is not yet complete. The portion of the integration audit is still small because there are a different priorities between the operational auditor and the IT audit unit.

b) Establishment of IT Audit Unit

The ITJEN performs its functions as an internal audit unit with comprehensive supervision not only business processes but also an auditee organization. With the changes in business processes and auditee organizations mostly based on IT, the ITJEN supervises the management of IT. In this regard, ITJEN,

in 2014, established an IT audit unit with the function of overseeing IT management.

The IT audit strategy document discussed the implementation of ITJEN IT audits using two general strategies.

1) Integrated IT Auditing: the assignment of an IT audit to support the implementation of operational audits (auditee business processes) conducted by request of other inspectorates. The audits cover the entire business cycle end-to-end. Integrated IT audit objects include general control and IT application control.

2) IT Thematic Audit: a type of IT audit assignment carried out on specific IT teams for an IT risk profile, leader direction, current issue, or liability to specific regulations or policies on the utilization of information technologies that may not be directly related to the audit conducted by another inspectorate. This includes specific IT coverages with more detailed depth levels. Objects of the audit include IT governance audits, project management audits, SI development cycle audits, security audits, and IT operations and business continuity plans.

c) Skills possessed by internal auditors

It is ITJEN's policy to separate the IT audit function with the operational audit function. The policy raises the different skills requirements required by auditors to have an inspectorate as an operational audience of the DGT with the IT audit unit as the DGT IT auditor. The separation is considered the best because of the following reasons.

1) The Auditor of Inspectorate I is deemed incapable of being required to study both fields simultaneously because of the rapid development of technology.

2) There is unequal ability of auditors in the ITJEN where there is a gap between the older and the younger generation in auditors in terms of technology literacy.

In the IT audit unit of the ITJEN, there are auditors at the technical and management levels. Both must play a balanced role. There are three kinds of competencies that auditors must have on the IT unit, including audit skills ranging from planning to compilation of supervisory reports, knowledge of IT governance, and operations, such as governance and managerial IT, IT operations, IT project management, IT security, and knowledge of every echelon-1 business process in the finance ministry as an object of inspection. The auditee sees that the ITJEN's internal auditors have a good understanding of SIDJP.

The competencies developed in Inspectorate I are nearly the same as the IT auditor's skills, but the priority differs. The auditor in Inspectorate I is required to understand the business processes of DJP and then to have computer-assisted auditing techniques (TABK) as new requirements arising with IT-based auditees. Operational auditors should enrich themselves beyond studying TABK to acquire knowledge about IT by following training. Currently the capabilities of the auditor in Inspectorate I and the IT audit unit require improvement, because they are not yet in ideal condition. However, the leader (technical controller) believes that the human resources they have are ready and able to pursue changes.

d) Supervision tools

To support a changing control environment after the implementation of information systems in most auditee business processes has encouraged the ITJEN to use technology in overseeing its audiences, the application of the technology used includes:

- Audit Management System by using Teammate.
- Computer-Based Audit Techniques using Excel, ACL, and AXSCORE.
- The usage of TABK in the internal audit process by the inspectorate as an operational auditor is monitored directly by the IT audit unit. It is something positive that directly encourage the Inspectorate to apply the tools.
- Continuous Audit.

The ITJEN requests all echelons of the Ministry of Finance to transmit examination request data through the data exchange portal. At that time, IR VII with Inspectorate I and SIP explain the concept of audit changes in the future by using continuous audit. ITJEN is expected to have the authority to force the other echelon I to update the data in the portal automatically without having to go through data requests through assignment. The one responsible for monitoring an anomaly resulting from CA is the IT audit unit.

e) Internal audit resources

At the Inspectorate I and the IT audit unit, most auditors are from a controls background (accounting science) who studied IT (e.g., IT unit auditors, BPK auditors, Research Governor IIA). This kind of auditor usually has a better sense of audit than auditors with only IT backgrounds, because their focus is different. An auditor will focus on controlling the application system, whereas the IT person will focus on building a functioning and usable system.

In private-sector practice, when organizations do not have the function of internal auditors, they often outsource the functions to public accounting firms or consultant offices. In the public sector, many still believe that outsourcing of problems, such as complex implementation, is necessary, because they have to go through procurement and the issue of confidentiality of government data. All the auditor's needs are met by ITJEN internal resources.

According to the public governor of IIA Indonesia (2018), audits are accepted if a public-sector company using a third party in performing the internal audit function as long as they are competent and comply with the standards and code of ethics so that there will be no problem with confidentiality. Nevertheless, the main reason for only fulfilling the internal auditors' needs internally is the belief that their human resources are good and adaptive, quick to follow the changing environment.

f) Size of the internal auditor unit

After the introduction of the information system at the Ministry of Finance, the number of auditors of the ITJEN increased with the new function of the IT audit unit as part of Inspectorate VII. With the addition of a new unit, there was a

change in the number of audit teams overseeing the DGT, because the audit is an integration unit in collaboration with the IT audit unit. Thus, this audit team is one that understands IT, finance, law, etc., as a team. Thus, it is considered competent.

g) Relationship of Inspectorate I and IT audit unit with SIP

When carrying out supervision at the DGT, the inspectorate depends on the SIP division to obtain examination data from the DGT. An echelon-2 at the Ministry of Finance, the Center for Information Systems and Financial Technology (PUSINTEK), became the data custodian at the central level. Owing to the difficulty of coordination, they created a mechanism of data exchange through a portal created by PUSINTEK with the flow of data requesters to apply for any data needed. By looking at the less mature ITJEN auditor in understanding the IT field, it was decided to provide admin positions in the ITJEN at the SIP (ITJEN IT Division). However, this condition could be improved with the increasing ability of auditors in IT. Nevertheless, this current condition is favorable for operational auditors, because they do not need to think about technical matters related to data retrieval. Thus, they can focus on the audit itself.

In the early days of its establishment in 2014, the IT audit unit relied heavily on SIP, because only a few came from an IT background. Thus, when they were in charge, they used SIP officers to assist with IT audits. Then, the auditors in the IT audit unit were pushed to understand IT technical information by taking various IT-related audit certifications. As more IT auditors have a technical IT-related understanding and a mutation of SIP employees to the IT audit unit, the unit is now self-supporting in carrying out IT supervision at the Ministry of Finance.

h) Relationship of Inspectorate I (internal auditor) with Supreme Audit Board (external auditor of DGT)

The control environment at the ITJEN Ministry of Finance is the most advanced control environment at the Government Internal Supervisory Apparatus in Indonesia. However, it is not necessarily related to the increased use of ITJEN's work by external auditors. External Auditors agree that the implementation of business process automation, based on theory, will reduce detection risk when they perform supervision. Yet, they point out that the risk of detection does not shrink and tends to increase when the information system applied is not yet mature and reliable.

The automation process has encouraged the BPK to adapt by changing its audit practices by developing the concept of e-audits in 2011. Basically e-audit is a system integrator that connects the BPK information system to the entity's information system using IT as the basis for compiling data and information in the Center for Management Data and Responsibility for the State Finance module in the BPK information system. This was built to ease data exchange between the BPK and entities examined, including the Ministry of Finance. With the collection of information from various audit entities in data centers, it would be easier for BPK to carry out data analysis, especially when identifying patterns of data linkages among audit entities.

The use of e-audits will change the pattern of communication between the Ministry of Finance and the BPK, where the process of data collection and data analysis in conducting audits is done electronically. It is expected that the scope of the BPK examination will be broader when not using sampling methods but instead are based on population. The audit process is also expected to be shorter without sacrificing accuracy of the analysis. Finally, all improvements are expected to improve the use of audit resources (e.g., auditors, time, and costs) to be more efficient.

i) Strategic response conducted by ITJEN

Implementation of IT-based governance raises awareness of ITJEN for adapting to changes. However, transformation requires time, causing variations in strategies used by the ITJEN in response to changes. At the first introduction of SIDJP, the strategic response is defiance with dismissal tactics with which the organization ignores the values and rules. The strategy typically applies to organizations when external parties have weak coercive powers or when the objectives of the organization are too far with the values and requirements. This was taken because, at the time, ITJEN did not have the ability to conduct IT audits. Thus, they kept auditing using the traditional/manual methods (working around computers) regardless of the different control needs resulting from SIDJP implementation.

In 2014, with the establishment of an IT audit unit, the strategic response used by ITJEN compromises the balancing tactics of the organization's efforts to balance the interests of stakeholders with the internal interests of the organization, bargaining where the organization actively requests concessions from external parties with expectations or organizational desires. The strategy was chosen considering that ITJEN's human resources cannot meet the new requirement by fully. Thus, the demands of IT technical understanding are assigned to some auditors in the IT audit unit.

After the human-resources capabilities of ITJEN improved through formal education, training, and certification, the ITJEN compromised and continued to make changes to adapt to the changed governance by increasing the auditing tools from TABK. The strategy is based on a desire to apply better professional and international practices to maintain the legitimacy of ITJEN as an internal auditor.

V. CONCLUSION

SIDJP controls, as institutional logic of changes of function of internal auditors, comprise automation, centralization, standardization, transparency, authentication, authorization, and continuous monitoring. Control within the SIDJP provides pressure to the internal auditor to adapt to internal audit structures and processes. After implementing IT, the responsibility of the internal auditor increases with the emerging obligation to supervise IT governance: in this case, SIDJP. In business processes based on IT, supervision of DGT is done differently than traditional audits, which processes data from the auditee. The results of data processing from the IT audit unit raises an anomaly that is soon confirmed by the operational auditor in ITJEN. The change in auditee management, based on IT, is driven by a change in the structure of the ITJEN with the

addition of an IT audit unit responsible for overseeing the reliability of the applied information system on the auditee. Changes also occur in the composition of the audit team, where an integrated audit concept is introduced and governance-based IT oversight creates the need for an IT specialist on the operational audit team.

At the first introduction of SIDJP, the strategic response used by ITJEN as defiance with dismissal tactics, in which the organization ignored values and rules. This was accepted, because, at that time, ITJEN did not have the ability to conduct IT audits. Thus, they audited using the traditional manual method, regardless of the different control needs resulting from SIDJP implementation. Then, in 2014, with the establishment of an IT audit unit, the strategic response used by ITJEN included compromising with balancing tactics of organizational efforts to balance the interests of stakeholders with the internal interests of the organization, bargaining where the organization actively requests concessions from external parties accordingly with expectations or organizational desires. The strategy was chosen with consideration that ITJEN's human resources could not meet the new requirement. Thus, the demands of IT technical understanding were given to some auditors in the IT audit unit. After the capability of human resources of ITJEN improved via formal education, training, and certification, the ITJEN used compromise consciously applied by the ITJEN, so that they actively continued to make changes to adapt to changing governance by increasing the auditing tools from TABK to review ongoing audits. The strategy is based on a desire to apply better professional and international practices to maintain legitimacy of ITJEN as an internal auditor.

REFERENCES

[1] McKinsey Global Institute. (2017). A Future That Works: Automation, Employment, And Productivity.McKinsey & Company. January, 2017.

[2] Frey, C. B., & Osborne. M. A. (2013). The future of employment: How susceptible are jobs to computerisation?. UK: Oxford University Engineering Sciences Department.

[3] IIA. (2017).10 Hot Topics for the 2017 Internal Audit Plan. IIA:USA

[4] Pusintek. (2018). Ministry of finance report on ICT management in 2017. Jakarta: Kementerian Keuangan

[5] Avgerou, C. (2000). IT and organizational change: An institutionalist perspective. *Information Technology & People, 13,* 234-262

[6] Vowler, J. (2003). Make Sure IT's Risk Factor is Built into Governance, Computer Weekly, February 13, 2003, 28.

[7] Ramamoorti, S., & Weidenmier, M. L. (2004). The pervasive impact of information technology on internal auditing. Florida: IIARF.

[8] Felix, W. L., Gramling, A. A. & Maletta, M. J. (1998). Coordinating total audit coverage: The relationship between internal and external auditors. Altamonte Springs, FL: The Institute of Internal Auditors Research Foundation

[9] Elbardan, Kholeif. (2017). Enterprises resource planning, corporate governance and internal auditing: An institutional Perspective. Switzerland: Springer Nature.

[10] Saharia, A., Koch, B., & Tucker, R . (2008). ERP systems and internal audit. Issues in Information Systems, IX.

[11] BPK-RI. (2012). Audit report of management of tax information system management and control in taxpayer compliance supervision. Jakarta: BPK

[12] BPK-RI. (2015). Audit report of management supervision and control of tax information systems in the presentation of accounts of tax receipts and tax receivables. Jakarta: BPKIIA Indonesia. (2017). Lanskap Praktik Audit Internal Di Indonesia. Indonesia: The IIA Indonesia

[13] Flint, D. (1988). Philosophy and principles of auditing: An introduction. London: Macmillan Education.

[14] Ramamoorti, S. (2003). Internal auditing: History, evolution, and prospects. Florida: The IIA.

[15] IIA, (2013). International Professional Practices Framework .IPPF., The Institute of Internal Auditors (IIA),:USA.

[16] DiMaggio, P. J., & Powell, W. W. (1991). The iron cage revisited: Institutional isomorphism and collective rationality. In W. W. Powell & P. J. DiMaggio (Eds.), *The new institutionalism in organizational analysis, Chicago: University of Chicago Press Originally published.* 1983., American Sociological Review, 38, 147-160.

[17] Meyer, J. W., & Rowan, B. (1977). Institutionalised organisations: Formal structure as myth and ceremony. *American Journal of Sociology, 83,* 340-363.

[18] Oliver, C., (1991). Strategic responses to institutional processes. *Academy of Management Review, 16,* 145-179.

[19] Friedland, R., & Alford, R. (1991). Bringing society back. In W. W. Powell & P. J. DiMaggio (Eds.), *Symbols, practices, and institutional contradictions', in The New Institutionalism in Organizational Analysis* (pp. 232-263). Chicago: University of Chicago Press.

[20] Yoo, Y., Lyytinen, K., & Berente, N. (2007). An Institutional Analysis of Pluralistic Responses to Enterprise System Implementations, International Conference on Information Systems, 1-19.

Regulations:

Circular letter of Director General of Taxes No. SE-136/PJ/2010 on the User Account / Password Usage, Security Log-on to Information Technology Facilities, Use of E-Mail Facilities, and internet and intranet access Guidelines. (2011).

Circular letter of Director General of Taxes No. SE-15/PJ/2011 on the Malicious Software (Malware) Prevention Guidelines. (2011).

Circular letter of Director General of Taxes No. SE-16/PJ/2011 on the Security and Data and Information Processing Tools. (2011).

Law No. 15 on the Auditing over the Financial Management of the Government Institutions. (2004)

Presidential Decree No 29 on Government Agency Performance Accountability System (2014)

Presidential Instruction No 9 on Quality Improvement of the Internal Control System and Reliability of the Implementation of Internal Oversight Function towards People's Welfare realization. (2014)

Regulation No. 60 on Internal Control System. (2008)

Regulation of Director General of Taxes No. Per-41/PJ/2010 on the control over system software.(2010).

Regulation of Minister of Finance No. 129/KMK.01/2012 on the Integration of Information and Communication Technology Devices within the Ministry of Finance (2012).

Regulation of Minister of Finance No. 237/PMK.09/2016 on the Governance of Internal Oversight within the Ministry of Finance. (2016).

Regulation of Minister of Finance No. 260/KMK.01/2009 on the Information and Communication Technology Management Policy in the Ministry of Finance. (2009).

Regulation of Minister of Finance No. 275/KMK.01/2010 on the Electronic Data Exchange Policies and Standards. (2010).

Regulation of Minister of Finance No. 330/KMK.01/2011 on the Management Policies and Standards for Information and Communication Technology Projects within the Ministry of Finance.(2011).

Regulation of Minister of Finance No. 338/KMK.01/2012 on the direction of Development of Information and Communication Technology within the Ministry of Finance.(2012).

Regulation of Minister of Finance No. 350/KMK.01/2010 on the Policies and Standards for Electronic Data Management in the Ministry of Finance. (2010).

Regulation of Minister of Finance No. 479/KMK.01/2010 on the Information Security Management System Policies and Standards in the Ministry of Finance. (2010)