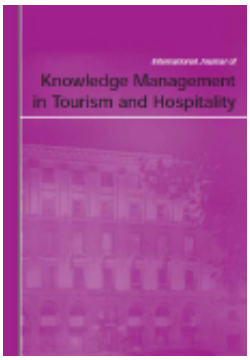

International Journal of Knowledge Management in Tourism and Hospitality

ISSN online: 1756-0330 - ISSN print: 1756-0322
https://www.inderscience.com/ijkmth

Control self-assessment on information technology business processes as COBIT 2019-based pre-audit activities

Lukman Abdurrahman

DOI: 10.1504/IJKMTH.2023.10057578

Article History:

Received:	19 May 2023
Last revised:	21 May 2023
Accepted:	29 May 2023
Published online:	30 January 2024

Control self-assessment on information technology business processes as COBIT 2019-based pre-audit activities

Lukman Abdurrahman

Information Systems Study Program,
School of Industrial and Systems Engineering,
Telkom University,
Bandung, Indonesia
Email: abdural@telkomuniversity.ac.id

Abstract: Control self-assessment (CSA) is a management tool to help management identify some shortcomings within the business processes. The CSA resembles the auditing process, viz. the CSA benefited business process owners by helping them evaluate their businesses, while the auditing process was conducted by internal or external auditors. This study aims to examine the management of risks and their controls to assess their effectiveness in mitigating the risks within business processes. To apply the CSA, Directorate of Centre of Information Technology (DCIT) of Telkom University Bandung will be a venue to do so. There are 29 risks with medium- or high-risk level. To examine the control effectiveness, the CSA has performed the control designs and their operation. The results show that four controls are ineffective, while the others are effective. In other words, the CSA resulted in 13.79% of controls being ineffective, while 86.21% were effective. This circumstance indicates that the DCIT's controls are mostly effective.

Keywords: control self-assessment; CSA; auditing; business process; internal control; risk.

Reference to this paper should be made as follows: Abdurrahman, L. (2024) 'Control self-assessment on information technology business processes as COBIT 2019-based pre-audit activities', *Int. J. Knowledge Management in Tourism and Hospitality*, Vol. 3, No. 3, pp.185–200.

Biographical notes: Lukman Abdurrahman is a Lecturer at the Information Systems Study Program, School of Industrial and Systems Engineering, Telkom University, Bandung, Indonesia. He obtained his Bachelor of Engineering in Physics from Bandung Institute of Technology in 1988, Master of Information Systems from Claremont Graduate University, Claremont, California, USA in 1999 and Doctor of Philosophy in Electrical Engineering and Informatics from Bandung Institute of Technology in 2017. Also, he had worked for PT. Telekomunikasi Indonesia, Tbk. (Telkom) for more than 28 years. His research interests are IT value engineering, IT governance, IT risk assessment and management, IT audit, and IT general control.

1 Introduction

Control self-assessment (CSA) has been management tools to control some business processes that have become their responsibility in daily operations. Usually, the CSA manifested to become a measurer of risk management to mitigate its magnitude of destructive power under the control that it has managed. It means that the risk management mitigation is the goal of the CSA so that the business process operates to achieve its objectives, while in its operation will result in risks that forbid its achievement. For that reason, it should be controls to mitigate the risks so that the business process operates smoothly toward its goals. As a result, the CSA's functions are to give awareness to business process's owners in controlling the risks (Huang, 2021).

Meanwhile, Abbot et al. (2019) mentioned that CSA is applicable to monitor effectivity of control procedure and to raise change communication in operations of the control procedure and design. Furthermore, Endrianto (2016) said that CSA could reduce fraud action within the firm, while CSA resembles auditing practices that its activity emphasises preventive actions rather than detective ones. Likewise, Jacobus (2015) stated that CSA consisting of method and process that could analyse and mitigate some risks as registered on enterprise risk management. Additionally, du Plessis and Grobler (1999) wrote that CSA was one of methods that is useful to evaluate risks with creating, estimating, fixing, and observing regulators to report risks. Moreover, Melville and Hafen (2000) researched the consciousness to measure the relations among implementation effectiveness of CSA and the application of control reproductions and to classify definite zones of finest exercise for the usage of control reproductions.

In this research, the CSA applicable method is to notify some documents and to observe them with their operations in the field (Serra et al., 2022). As for the field is Directorate of Centre of Information Technology (DCIT) of Telkom University Bandung, that is a place to implement information technology governance and management based on COBIT 2019. Likewise, to implement the method has been based on enterprise risk management (Huang, 2021). It means that current CSA has conducted on the DCIT's risk map, which is every management practice has high risk to evaluate its control whether its mitigation to the risk effective or not. In other words, the researchers have used risk-based audit methodology (Sastra et al., 2018) for the CSA. For the ineffective control, it suggests repairing the control, however, for effective ones, it continues to evaluate effectiveness of the control operation. Thus, the control operation proofs should be ready to evaluate if the control operation had fulfilled control designs before. In turn, the control operation results will be two results, i.e., effective operational controls and ineffective ones.

From the CSA's field, the results stated that the DCIT have 29 controls with their risks medium or high risks within three units of the DCIT, which four controls are ineffective, and the others are effective. In other words, the DCIT appears in good circumstance because its internal controls equal to 13.79% ineffective. It means that the others internal controls are 86.21% effective.

Furthermore, the paper provides discussion as follows: Section 1 discusses introduction to recognise the aim of the paper. Furthermore, Section 2 presents theory about control self-assessment that resulted from the previous ones and COBIT 2019. Section 3 provides methodology that is used in the research as above-mentioned shortly. In addition, Sections 4 and 5 are CSA results and discussion so that we can get

description about DCIT's performance in the CSA's viewpoint. Eventually, Section 6 is the conclusion about the CSA and this research.

2 Literature review

2.1 Control self-assessment

In essence, control self-assessment (CSA) is part of auditing involving business process owners to assess risk levels to mitigate with a level control. In other words, CSA can create effectiveness and efficiency in operating business processes because the impact of risks immediately acknowledged as soon as possible due to CSA by business process owners (Spiering, 2022). Accordingly, before internal or external auditors investigate the shortcoming of internal controls due to risks, the business process owners find them before. Therefore, earlier business process owners could fix the internal control deficiencies. In other worlds, some ineffective activities should be well when the internal or external auditors evaluate them (Abbot et al., 2019; Endrianto, 2016). Hence, the business processes have operated for fewer risks, although the risks will appear in every activity, however they are controlled well.

Essentially, the CSA is intertwined with the Committee of the Sponsoring Organisations of the Tradeway Commission (COSO), which it started to create innovative outline of risk management in 2001. Nowadays, the outline is named as the enterprise risk management-integrated framework (COSO 2004), which has been utilised by many firms in the world (Damayanti, 2017). In other words, to manage the risks over business processes within the firms, COSO provided an outline of risks with to be controlled. Therefore, after risk registers exist, the firm should prepare some controls to mitigate the risks. The control also should be effective to mitigate the risks. Hence, to do so, business process owners should involve evaluating the controls periodically, accordingly this activity is mentioned as control self-assessment. In addition, the importance of CSA is on the conclusion creation performed by the business process owners consisting of management and employees of the unit (Jacobus, 2015; Endrianto, 2016; Melville and Hafen, 2000).

Furthermore, the CSA contains good relationship among management, employees, and auditors because their understanding of risk management will increase by themselves. This is because CSA necessitates communication among them to register the risks, to mitigate using control, and compensate an ineffective control. So do auditors, they should communicate with employees, who are responsible with the business processes. In other words, the auditors should read and communicate the CSA's results before downing to the field of audit. Of course, the auditors must need to audit business processes after the owner's assessment to risk and control (Jacobus, 2015). Accordingly, the CSA can improve effectiveness and efficiency of business processes and possession at all levels of employees.

Currently, US Securities and Exchanges Commission (US SEC) suggests that CSA should contain inspector neutrality (Huang, 2021). In other words, CSA might give dismissal of regulation supervising and assessment because external auditors must assess the effectivity of a firm's internal controls to reduce a view on internal control over financial reporting (ICoFR) for every Section 404 of Sarbanes-Oxley Act. Accordingly,

external auditor will diminish CSA supervision attempts to utilise larger audit attempt in examining regulations to confirm regulation agreement (Abbot et al., 2019).

Furthermore, according to the Institute of Internal Auditors, CSA consists of three words, namely control, self, and assessment. Therefore, control means the outline of cohesive extensive reflect all inside aspects mainly moving the accomplishment of executive aims. And self means different from audit processes, viz. it has widespread opportunity of control that needs different people to do this, namely business process's owners. Moreover, assessment requires valuation of control in diminishing risks due to business processes (Yin et al., 2021). In order to reinforce the freedom, fairness, and superiority in the method, in addition to authentic authority, it is assumed that the internal auditor should be included in the exposure procedure the consequences autonomously to primary supervision and boarding commissions (Endrianto, 2016).

Therefore, the procedure of CSA is the involvement and collaboration amongst supervision and personnel as business process owners in CSA consultations. In here, there are identification, analysis, and risks qualification in a joint problematic answering to assist analysis of hazards and regulators throughout the organisation. Accordingly, it is begun with recognising the unit business goal and its main presentation pointer as hazard is expressed as the consequence of ambiguity. Moreover, the contributor meeting should talk about the risks evaluation to identify, analyse, assess, and formulate the treatment of risks (Yin et al., 2021). Accordingly, the CSA contributors should consist of supervision and personnel of unit in authority of the procedure of which subjects are to be conferred in the consultation. In addition, the quantity of them is supposed to be odd and assisted by two workers from risk management/internal audit units, of which one of them would be responsible of helping the argument process and the other would be responsible of minutes of meeting (Jacobus, 2015).

2.2 COBIT 2019

COBIT 2019 introduces enterprise governance information and technology (EGIT), which is an important measure of commercial authority. It could be implemented by the boarding that administers the description and application of procedures, constructions, and interactive devices in the corporation. Thus, that allows together commercial and IT society to perform their charges in backing of commercial or IT configuration and the conception of commercial worth from information and technology-permitted commercial financings (De Haes et al., 2018a). Additionally, the terms governance or enterprise governance and EGIT could be distinctive connotations relating to a managerial situation such as age, business, supervisory condition, and idiosyncratic background among additional issues. Accordingly, it is well if we can build on and improve present methods to contain Information and Technology rather than create a novel method for Information and Technology (De Haes et al., 2018d).

In essence, EGIT is not an inaccessible regulation, but an important portion of enterprise governance. For transparency and effective management of enterprise risk, the governance of an enterprise level is important to provide stakeholder value as well. Accordingly, EGIT can take full advantage of Information and Technology, developing advantages, exploiting prospects, and increasing economic improvement (De Haes et al., 2018d; Damayanti, 2017).

From an audit or CSA point of view, COBIT has created a further and supplementary inclusive information and technology authority and corporation outline and remains to

determine itself as a commonly recognised outline for I&T authority (De Haes et al., 2018b). Accordingly, COBIT agrees on the function and reportage preparations for audit or CSA involvement through the period of the package (De Haes et al., 2018d).

In the meantime, COBIT'S outline distinguishes between governance and management as follows (De Haes et al., 2018b):

- Governance relates to stakeholders for circumstances and possibilities in determining composed and agreed-on firm objects. Besides, the target is put across prioritising and judgement composing. Also, presentation and obedience are supervised against agreed-on ways and goals. In practice, governance is the board of directors' responsibility supervised by the chairperson. Although, unusual governance responsibilities may be delegated to unusual administrative configurations at an applicable stage, especially in greater organisations.
- Management relates to planning, building, running and monitoring activities relevant to the guidance put by the governance organisation to reach corporate goals. This management is under the responsibility of the executive management or the chief executive officer (CEO).

Furthermore, the governance and management objectives of COBIT have five domains as follows (De Haes et al., 2018b):

- Governance objectives contain the evaluate, direct and monitor (EDM) domain. This is a strategic domain dealing with strategic responsibilities.
- Management objectives have four domains:
  a Align, plan and organise (APO) relates to a general corporation, scheme, and supportive actions for information and technology.
  b Build, acquire and implement (BAI) that defines how to create, attain, and realise information and technology resolutions and their incorporation into business processes.
  c Deliver, service and support (DSS) talks about the working distribution and backing of Information and Technology assistance, comprising protection.
  d Monitor, evaluate and assess (MEA) talks about presentation supervising and conformance of information and technology with inside presentation intention, internal control purposes and outside supplies.

Therefore, to contribute to enterprise goals for information and technology, some governance and management objectives should be accomplished. Elementary ideas connecting to governance and management objectives are:

- A governance or management objective permanently reports to one procedure and a series of connected constituents of additional categories to assist to realise the objective.
- A governance objective tells a governance procedure, whereas a management objective tells a management procedure.

Boarding and exclusive administration are classically responsible for governance procedures, whereas administration procedures are the area of leading and mid-administration (De Haes et al., 2018c; Damayanti, 2017).

3 Research methodology

CSA research methodology consists of methods as follows:

1 Learning CSA and COBIT 2019 concept, especially relating to several medium and high risks that should be controlled to mitigate the risks.

2 Comprehending the business processes and risks map running in the object, viz. Directorate of Centre of Information Technology (DCIT), Telkom University, Bandung, Indonesia.

3 Studying relationship, the business processes to COBIT 2019, in which COBIT 2019 should be a standard for the DCIT's business processes. In here, the business processes should relate to governance/management objectives of COBIT 2019, whereas each governance/management objective has primary enterprise and alignment goals with each metric to measure its achievement. Furthermore, using seven components, consisting of process; organisational structures; information flows and items; people, skills and competencies; policies and procedures; culture, ethics and behaviour; and services, infrastructure and applications, each governance/management objective is measured to comply with the standard (De Haes et al., 2018b). From this method, we can comprehend a description about the relationship between the DCIT's business processes and the governance/management objectives of COBIT 2019. In other words, the linking of the DCIT's business processes and COBIT 2019 might occurred. Accordingly, we can evaluate the control that mitigates the risks by COBIT 2019 criteria through the CSA approach.

4 Comprehending the risks causing the business processes did not achieve the target. The risks chosen are those have medium or high risks based on the risk map, which has two parameters of risk, viz. the likelihood and the severity (Maman et al., 2022, Damayanti, 2017).

5 Moreover, studying the control to mitigate the medium or high risks. To evaluate the control, we assess from two type of evaluations, i.e., from the design control and the operation of control. If the control does not mitigate the risk from the design of control point of view, we stop the evaluation and suggest the business process owners to redesign the control and make other compensation controls to fix the existing one as COBIT 2019 recommends as well. Furthermore, if the control design is effective, we continue to evaluate the operation of control, viz. we ask for the proof of the control operation. If on the proof of the control operation contains manager or supervisor approval and has some required evidence, we evaluate that the control was effective. If vice versa, the control was deficient in the operation (Maman et al., 2022).

6 Discussing the results of assessment with the business process owners surround ineffectiveness of the evaluated controls. If the controls are deficient in the design, we suggest redesigning to fulfil the control design to fit in mitigating the risks. Otherwise, we recommend obeying the control design in the operation to mitigate the risks (Hauck et al., 2021).

7 All notes relating the CSA are written as CSA documents, which are to communicate the business process owners with their users to repair the control and mitigate the risks to minimise the risks and enlarge the business process achievement.

8 Besides that, the note is also used to create the CSA reporting for management.

4 Results

The directorate of the Centre of Information Technology (DCIT) of Telkom University became a venue to research business processes, and their controls should be evaluated in the CSA context. The researched business processes are those that have risks medium and high, meanwhile, the low risks are ignorable. Accordingly, the following are units within the DCIT that have been experienced during the CSA: information technology development unit, information technology infrastructure unit, and information technology research and services unit. The followings are tables resulting in the CSA effort:

Table 1 Risk ID in information technology development unit

Risk ID	*Risk description*	*Risk value*	*Business process*	*COBIT 2019 GMO*
DevTI-1	Slow resources	High	Developing software applications	BAI02, APO08
DevTI-2	More prioritised applications	Medium	Planning the existing resources and project	EDM04, APO07
DevTI-3	The number of available resources is not sufficient	Medium	Reducing the number of resources to suffice the number of projects and ticketing in the information technology development unit.	APO03, BAI11
DevTI-4	The timeline for project work is delayed	Medium	Developing software applications	BAI07, DSS02

Table 1 depicts that the information technology development unit has four risks valuing medium and high, meanwhile, the other risks have been low. Each risk relates to the business process of the information technology development unit possess, in turn, if we link to the governance and management objective of the COBIT 2019, we can obtain its relevance, see Table 1. Accordingly, the business process has been defined in the COBIT 2019, which we can refer to repair some shortcomings if needed. In addition, the information technology development unit also had controls to mitigate the risks, see Table 2. Those controls have been assessed by the CSA approach to testing its design and its operation to assess its effectiveness to overcome the risks. The control design test comprises the segregation of duty, owning the essential power and capability to achieve the control effectively, fulfilling the company's control objectives and can effectively avoid or sense error or deceit that could cause substantial misstatements in the financial reports (Auditing Standard No. 13, 2016). The control operation is to test its implementation in daily operation with cooperation between staff and his/her manager to sign the proof of control operation or a control designated for examining through fixing

whether the control is functioning as planned and whether the human presenting the control owns the essential power and capability to achieve the control effectively (Auditing Standard No. 13, 2016). If all exist, the controls are effective, if there is no control design, the control operation also does not exist, and the control is ineffective, see Table 2.

Table 2 CSA in information technology development unit

Risk ID	*Control*	*Control self-assessment*		*CSA result*
		Control design	*Control operation*	
DevTI-1	Delay the development of new applications and adjust the new timeline agreement with the user by explaining the constraints. For resources that are about to go out, they need to be informed 1 month in advance and speed up incoming resources.	OK	OK	Effective
DevTI-2	Coordinate with related units to request direction from the leadership regarding the priority of application development outside the strategic plan, especially related to the application contained in the roadmap that must be shifted from existing human resources, as well as added value for business activities.	OK	OK	Effective
DevTI-3	Adding resources, delaying the development of applications with lower urgency, and increasing working hours	OK	OK	Effective
DevTI-4	Delayed application development, recruitment of new resources, and evaluation of available resources	OK	OK	Effective

Likewise, Tables 3 and 4 demonstrate that the information technology infrastructure unit has six risks with medium and high risks. Risk number 3 or Risk ID IsTI-3 is ineffective because its design does not exist as well. Accordingly, its operation does not work; therefore, its value is ineffective.

Table 3 Risk ID in information technology infrastructure unit

Risk ID	*Risk description*	*Risk value*	*Business process*	*COBIT 2019 GMO*
IsTI-1	Threats to information security because data security holes were detected on academic and non-academic database devices	Medium	Data centre service request	DSS01, DSS03
IsTI-2	Influence on network, electricity, air conditioning, access control, and fire, due to submissions outside the IsTI standard	Medium	Data centre service request	DSS01, DSS03
IsTI-3	Unable to access internet service	Medium	Data centre service request	DSS01, DSS03

Table 3 Risk ID in information technology infrastructure unit (continued)

Risk ID	*Risk description*	*Risk value*	*Business process*	*COBIT 2019 GMO*
IsTI-4	Internet and Intranet access is down because the optical fibre is broken	Medium	Information technology service functionality	APO01, APO09, BAI06
IsTI-5	Internet and intranet access is dead because it cannot log in (tune)	Medium	Information technology service functionality	APO01, APO09, BAI06
IsTI-6	Internet access and data centre area intranet not working (dead)	Medium	Information technology service functionality	APO01, APO09, BAI06

Table 4 CSA in information technology infrastructure unit

Risk ID	*Control*	*Control self-assessment*		*CSA result*
		Control design	*Control operation*	
IsTI-1	Perform image backups	OK	OK	Effective
IsTI-2	Confirm according to information technology infrastructure unit standards	OK	OK	Effective
IsTI-3	Confirm according to information technology infrastructure unit standards	NOT OK	NOT OK	Ineffective
IsTI-4	• Close doors or rack openings to prevent mice from getting in • Increase the prudence of every engineer on duty • Prepare a backup of the number of fibre optic cores in each building	OK	OK	Effective
IsTI-5	Monitoring the health system regularly	OK	OK	Effective
IsTI-6	Monitoring the health system regularly	OK	OK	Effective

Similarly, Tables 5 and 6 exhibit the CSA in information technology research and services unit, which has 19 risks with medium and high risks.

Table 5 Risk ID in information technology research and services unit

Risk ID	*Risk description*	*Risk value*	*Business process*	*COBIT 2019 GMO*
RiyanTI-1	Error entering domain name to destination IP address in DNS	Medium	Website making	EDM05, BAI04, DSS03
RiyanTI-2	Ticket details are rarely seen	Medium	Reporting and repairing complaint service functionality via the ticketing helpdesk application	APO09, DSS02

Table 5 Risk ID in information technology research and services unit (continued)

Risk ID	*Risk description*	*Risk value*	*Business process*	*COBIT 2019 GMO*
RiyanTI-3	Security vulnerabilities in plugins that damage websites	Medium	Monitoring the functionality of information technology services (website)	APO01, APO13
RiyanTI-4	Security vulnerabilities in the theme that broke the website	Medium	Monitoring the functionality of information technology services (website)	APO01, APO13
RiyanTI-5	Misuse of user accounts that threaten security	Medium	Monitoring the functionality of information technology services (website)	APO01, APO13
RiyanTI-6	Security vulnerabilities in plugins that damage websites	Medium	Monitoring the functionality of information technology services (website)	APO01, APO13
RiyanTI-7	Server configuration problem	Medium	Website making	EDM05, BAI04, DSS03
RiyanTI-8	Configuration error on SSL	Medium	Website making	EDM05, BAI04, DSS03
RiyanTI-9	Incompatibility of PHP settings on WordPress needs	Medium	Website making	EDM05, BAI04, DSS03
RiyanTI-10	Cannot access the domain or website in a row for one week	Medium	Webometric ranking	EDM01, EDM05, MEA02
RiyanTI-11	The existence of a non-personal non-scholar Google profile account (journal or unit account)	High	Webometric ranking	EDM01, EDM05, MEA02
RiyanTI-12	The existence of an account profile: more than one Google scholar for the same person and content that does not contain the name of the account owner and content with special signs (* and .)	High	Webometric ranking	EDM01, EDM05, MEA02
RiyanTI-13	No subnet backlink growth	High	Webometric ranking	EDM01, EDM05, MEA02
RiyanTI-14	The user does not understand the service material delivered	Medium	User education service	DSS01, DSS06

Table 5 Risk ID in information technology research and services unit (continued)

Risk ID	*Risk description*	*Risk value*	*Business process*	*COBIT 2019 GMO*
RiyanTI-15	The slow speed of response time to complaints	Medium	User education service	DSS01, DSS06
RiyanTI-16	Did not submit a licensed budget in the previous year	Medium	License application	APO02, APO10
RiyanTI-17	Security vulnerabilities in plugins that damage websites	Medium	Monitoring the functionality of information technology services (blog)	APO01, AP011, APO13
RiyanTI-18	Misuse of user accounts that threaten security	Medium	Monitoring the functionality of information technology services (blog)	APO01, AP011, APO13
RiyanTI-19	Attachment not filled	Medium	Reporting and repairing complaint service functionality via the ticketing helpdesk application	APO09, DSS02

Moreover, Table 6 shows that three controls that mitigate the risks are ineffective because their control design does not exist, therefore the control does not operate, and the internal controls are ineffective as well.

Table 6 CSA in information technology research and services unit

Risk ID	*Control*	*Control self-assessment*		*CSA result*
		Control design	*Control operation*	
RiyanTI-1	Repair of domain name data and domain IP address directions	OK	OK	Effective
RiyanTI-2	Socialising the helpdesk application in more detail and adding an explanation of 'ticket details' in the ticket input flow at the beginning	OK	OK	Effective
RiyanTI-3	Restore backup	OK	OK	Effective
RiyanTI-4	Restore backup	OK	OK	Effective
RiyanTI-5	Restore backup	OK	OK	Effective
RiyanTI-6	Restore backup	NOT OK	NOT OK	Ineffective
RiyanTI-7	Adjusting the web server configuration to the needs of the application	OK	OK	Effective
RiyanTI-8	Update SSL according to the latest license	OK	OK	Effective
RiyanTI-9	Update according to PHP with the application used	OK	OK	Effective

Table 6 CSA in information technology research and services unit (continued)

Risk ID	*Control*	*Control self-assessment*		*CSA Result*
		Control design	*Control operation*	
RiyanTI-10	Inform the information technology infrastructure unit to monitor (events)	NOT OK	NOT OK	Ineffective
RiyanTI-11	Informing the directorate of research and community services to deactivate the journal account during the Webometric assessment period (June–July)	OK	OK	Effective
RiyanTI-12	Inform the directorate of student affairs, faculties, and direct account owners	OK	OK	Effective
RiyanTI-13	Socialising website owners to take care of SEO; updating content, updating plugins, themes, and WordPress regularly; meeting the content standard rules.	OK	OK	Effective
	For the DCIT part: ensure no malware spreads; follow up on reports from other apps like Google search console and email notifications from security plugins; do a blog walk; research the development of web applications that can help improve the content			
RiyanTI-14	Making service usage information in the form of videos, documents, and websites	OK	OK	Effective
RiyanTI-15	Conduct awareness related to complaints handling responses to the service desk	OK	OK	Effective
RiyanTI-16	Using other budget posts	OK	OK	Effective
RiyanTI-17	Restore backup	OK	OK	Effective
RiyanTI-18	Restore backup (every three months)	OK	OK	Effective
RiyanTI-19	Socialising the helpdesk application in more detail	NOT OK	NOT OK	Ineffective

5 Discussion

Based on the abovementioned results, several things can be discussed as follows: CSA should be begun by enterprise risk management (ERM), which means that the control or internal control is existing because some risks emerge within the business process (Maman et al., 2022; Damayanti, 2020, 2017). The risks should be identified and registered in an ERM. Regularly, the ERM is mapped in a risk map, which shows risk values measured on the frequency and their severity from the risk map (Farar, 2016). Therefore, the risks have high, medium, and low values, in which we can recognise the risk scale, in turn, we must mitigate the risks to minimise their uncertainty to the business

processes. The mitigation manifests in control to anticipate their uncertainty. In other words, the business process owners should comprehend the mechanism to evaluate the effectiveness and deficiency of the controls they have (Jacobus, 2015).

Likewise, this mechanism focuses on risk-based CSA as well as risk-based audits (Sastra et al., 2018). Moreover, CSA also relates to Sections 302 and 404 of the Sarbanes-Oxley Act (SOX 2002) in internal control and internal control over financial reporting, especially for firms listed on the US SEC. In other words, internal control over financial reporting must obtain escort in day-to-day operations, so the business process owners should implement built-in control instead of built-on control. In addition, the internal control should regularly attain assessment using the CSA before auditing by external auditors (Damayanti, 2020; Abbot et al., 2019).

In practice, CSA commonly precedes auditing whether by internal or external auditors so that the CSA can repair some shortcomings in the internal controls. Thus, the auditor will audit more smoothly than if the CSA has not been carried out (Endrianto, 2016). Consequently, the business processes always run on the right track if the CSA is regularly performed as well because the risks will be regularly mitigated by the business process owners.

From COBIT'S 2019 point of view, the CSA is assessing the application business processes, especially related to risk management and its controls. At DCIT, not all government and management objectives (GMOs) of COBIT 2019 have been implemented, see Tables 1, 3 and 5, merely a few GMOs of COBIT 2019 have been implemented, especially those related to medium or high risk. However, the use of COBIT 2019 at DCIT is the forerunner that DCIT in the future will become a large organisation that must fully implement the COBIT standard. Likewise, the use of COBIT must always be accompanied by the implementation of the CSA so that its implementation will be following the purpose of COBIT'S existence as a framework for managing systems and information technology. This good habit is not only an internal improvement of the organisation, but also part of the improvement when it will be audited by both internal and external audits, to produce the best always (Chung and Hsiao, 2020; De Haes et al., 2018a; Schorning, 2015).

As for CSA in DCIT's Telkom University, we can see that the results stated that the DCIT have 29 controls, in which their risks are medium or high in three units of the DCIT. Of the controls, four controls are ineffective, and the others are effective. Consequently, the DCIT appears in a safe situation because its internal controls (Damayanti, 2020) are equal to 13.79% ineffective. It means that the other internal controls or 86.21% are effective.

In the information technology development unit, there are four controls with one control being in high-risk value, and three controls being medium ones. The CSA results exhibit that all controls are effective, therefore information technology development unit gets away in CSA as a pre-audit, see Table 2. As for the information technology infrastructure unit, one control is ineffective because the control design did not effective as well, so the control operation did not run well, and the control is ineffective. However, the other controls are effective, meaning that the controls in the unit run to mitigate the risks, see Table 4.

In the meantime, the information technology research and services unit have 19 controls with medium or high-risk values, however, three controls are ineffective due to corruption in control design. Accordingly, the control operation did not run as well, see Table 6.

In this study, we have evaluated that the effective controls in DCIT are 86.21% if referred to Farar (2016), that the controls are equal to 80–99% effective, therefore the control performance is most effective. It means that the DCIT can face the auditing process easier because merely 13.79% of controls should be repaired to be effective. Hence, the DCIT should design the controls to mitigate the risks, in turn, it should operate to run the control operation as well.

The CSA gives benefits to knowing a risk-control map within business processes so that we can anticipate mitigating the risks to minimise their uncertainty to the goals of business processes. Therefore, the business owners can fix the inadequacies in their business processes to avoid disturbances, and they will be more ready to face audit processing whenever the auditor will evaluate them. In other words, the CSA always anticipate the interest of both business owners and stakeholders (Sastra et al., 2018).

6 Conclusions

Here are the conclusions regarding the research on CSA:

- CSA delivers an outline for assisting firms to govern their risks to realise their business objectives. In easy expressions, CSA comprises an organised method to verify business objectives, risks and controls and consuming working organisation and team to evaluate the acceptability of controls.
- CSA relates to the business owners and the other stakeholders to operate the business processes in healthy and good governance. Meanwhile, the COBIT 2019 is a framework to manage a system and technology of information, to escort the implementation of the framework, CSA can smoothen the current or future implementation of this framework.
- CSA in the DCIT exhibit that the venue is most effective because 86.21% of controls are effective. The CSA was conducted by valuing controls to mitigate the risks of both design and control operation so that the business processes operate without disturbances.

Acknowledgements

I would like to thank the Directorate of Research and Community Service at Telkom University, Bandung, Indonesia, for funding this research so that the results can be published in this journal.

References

Abbot, L.J., Parker, S., Peters, G.F. and Presley, T. (2019) 'The effect of control self-assessment on certain costs of compliance with Sarbanes-Oxley Section 404', *Journal of Management Accounting Research*, Vol. 31, No. 3, pp.1–49.

Auditing Standard No. 13 (2016) *The Auditor's Responses to the Risks of Material Misstatement* [online] https://pcaobus.org/oversight/standards/archived-standards/pre-reorganized-auditing-standards-interpretations/details/Auditing_Standard_13 (accessed 3 September 2022).

Chung, C.Y. and Hsiao, I.H. (2020) 'Investigating patterns of study persistence on self-assessment platform of programming problem-solving', *SIGCSE '20*, 11–14 March, Portland, OR, USA.

Damayanti, K. (2017) *Control Objective for Information and related Technology (COBIT) & COSO Enterprise Risk Management (COSO ERM)* [online] https://medium.com/@khristdamay/control-objective-for-information-and-related-technology-cobit-742e51efbade. (accessed 8 September 2022).

Damayanti, K. (2020) *The Effect of Information Technology Utilization, Management Support, Internal Control, and User Competence on Accounting Information System Quality (Study on Finance Company in Jakarta)* [online] https://medium.com/@khristdamay/the-effect-of-information-technology-utilization-management-support-internal-control-and-user-d6723cf20909 (accessed 8 September 2022).

De Haes, S., Goorden, M., Grijp, S., Peeters, B., Poels, G. and Steuperaert, D. (2018a) *COBIT 2019 Framework: Introduction and Methodology*, ISACA, Schaumburg, IL 60173, USA.

De Haes, S., Goorden, M., Grijp, S., Peeters, B., Poels, G. and Steuperaert, D. (2018b) *COBIT 2019 Framework: Governance and Management Objectives*, ISACA, Schaumburg, IL 60173, USA.

De Haes, S., Goorden, M., Grijp, S., Peeters, B., Poels, G. and Steuperaert, D. (2018c) *COBIT 2019 Framework: Designing an Information and Technology Governance Solution*, ISACA, Schaumburg, IL 60173, USA.

De Haes, S., Goorden, M., Grijp, S., Peeters, B., Poels, G. and Steuperaert, D. (2018d) *COBIT 2019 Framework: Implementing and Optimizing an Information and Technology Governance Solution*, ISACA, Schaumburg, IL 60173, USA.

du Plessis, L. and Grobler, G.P. (1999) 'The process of control self-assessment and its use in risk management', *Meditari Accountancy Research*, Vol. 7, pp.49–73.

Endrianto, W. (2016) 'Optimization of control self assessment application to minimize fraud', *Binus Business Review*, Vol. 7, No. 1, pp.59–64.

Farar, R. (2016) *Risk Tip #2 – How Do We Measure Control Effectiveness?* [online] https://paladinrisk.com.au/risk-tip-2-measure-control-effectiveness/ (accessed 31 August 2022).

Hauck, J.C.R., Zwirtes, A.G.L., Galimberti, M.F. and Bosse, J. (2021) 'How has process assessment been automated by organizations? A systematic literature mapping', *SBSI 2021*, 07–10 June, Uberlândia, Brazil.

Huang, Y. (2021) 'Work motivation and operational risk assessment: a new direction for organisational behaviour studies', *Int. J. Risk Assessment and Management*, Vol. 24, No. 1, pp.54–72.

Jacobus, D. (2015) 'New paradigm of managing risks: risk and control self-assessment', *Agriculture and Agricultural Science Procedia*, Vol. 3, pp.32–34.

Maman, L., Volpe, G. and Varni, G. (2022) 'Training computational models of group processes without groundtruth: the self- vs external assessment's dilemma', *International Conference on Multimodal Interaction (ICMI '22 Companion)*, 7–11 November, Bengaluru, India, ACM, New York, NY, USA.

Melville, R. and Hafen, M. (2000) 'Control models and control self-assessment: results of a survey of the IIA CSA Centre', *Integrity and Internal Control in Information Systems*, Springer Science+Business Media, New York.

Sastra, C.D., Yuhertiana, I. and Budiwitjaksono, G.S. (2018) 'The use of risk based audit techniques in government entities: Indonesia case', *Account and Financial Management Journal*, Vol. 3, No. 6, pp.1581–1586.

Schorning, J. (2015) *Does a COBIT 5 Self-assessment Help the Business to Get Control of a Shared Service Center?* [online] https://www.isaca.org/resources/news-and-trends/industry-news/2015/does-a-cobit-5-self-assessment-help-the-business-to-get-control-of-a-shared-service-center (accessed 8 September 2022).

Serra, G., De Falco, F., Maggi, P. and De Piano, R. (2022) 'Website complexity and usability: is there a role for mental workload?', *Int. J. Human Factors and Ergonomics*, Vol. 9, No. 2, pp.182–199.

Spiering, S. (2022) 'Self-reflexive practice through the human scale development approach – competencies needed for transformative science research', *Int. J. Sustainable Development*, Vol. 25, No. 1, pp.132–159.

Yin, K., Zou, H., Chen, J, and Zhao, C. (2021) 'An approach to the application of the Dempster-Shafer theory in the megacity community security risk assessment', *Int. J. Reliability and Safety*, Vol. 15, Nos. 1–2, pp.37–50.