Jurnal Computech & Bisnis, Vol. 17, No. 2, December 2023, 104-124
ISSN (print): 1978-9629, ISSN (online): 2442-4943

I-Pos Information System Security Audit Using Framework Control Objectives for Information and Related Technologies 2019 And Information Technology Infrastructure Library 4

Titan Parama Yoga[1], Chairul Habibi[2] , Nizar Hizbi Abdul Aziz[3]
Universitas Informatika dan Bisnis Indonesia[1,2,3]
titanparama@unibi.ac.id[1], chairulhabibi@unibi.ac.id[2], nizar@gmail.com[3]

Abstract

Information system security is used to protect against cyber attack crimes. Generally, cyber attacks occur because someone wants to intervene in a system to find out the confidentiality and availability of information. PT. Pos Indonesia is a company under the auspices of SOEs engaged in distributing letters and packages. Both domestic package distribution and overseas package distribution. To facilitate the delivery of packages, PT Pos Indonesia developed an information system called I-POS. Based on the results of the researchers' analysis, the I-POS information system is an information system that aims at mail and package delivery transactions, so using the I-POS information system can facilitate the process of delivery transactions, as well as provide accurate, timely, and relevant information. The purpose of this study is to determine the level of maturity of information system security in the field of I-POS information systems at PT. Pos Indonesia, Analyzing the findings and gaps of the level of maturity of the information system security. Based on the results of research that has been conducted through questionnaires using the COBIT 2019 framework with APO13 and DSS05 domains, it was found that the Existing Capability obtained was at level 2 while the expected Capability Level was at level 5 so the Capability Gap produced in these conditions was 3 levels

Keywords : *Information System Security Audit, COBIT 2019, APO13, DSS05, ITIL 4, I-POS*

INTRODUCTION

Information security is utilized to safeguard against cyber-attacks and criminal activities. Cyberattacks commonly transpire when individuals purposefully interact in a system to obtain unauthorized access to personal information and disrupt its availability (Ramdhan, 2019). In the contemporary era of digital advancements, the prevailing objective is to evaluate the robustness of a system's security measures. Nevertheless, upon successfully infiltrating a system, they use this advantageous situation to acquire illicit financial gains. These cybercriminals exhibit a lack of ethical consideration as they strategically focus on targeting a wide range of companies and government entities to obtain advantageous outcomes. Cyber attackers leverage weaknesses in information security protocols, enabling them to penetrate a system and disrupt its operations, impeding authorized users from accessing their systems.

PT. Pos Indonesia, a government-owned enterprise specializing in the transportation of mail, has diversified its business activities over several years to encompass the delivery of parcels, both within the country and across international borders.

In order to enhance the efficiency of package delivery services, PT Pos Indonesia has developed a proprietary information system known as I-POS. According to the analysis conducted by the researcher, the primary objective of the I-POS information system is to enhance the efficiency of mail and package delivery transactions by offering precise, prompt, and pertinent information.

Recently, the I-POS information system has seen disruptions, resulting in system problems that impede the timely delivery of mail and packages. The disruptions were a result of effective cyber-attacks that successfully breached the system.

In order to safeguard the integrity and confidentiality of the I-POS information system from potential virus threats and illegal access, as well as to optimize customer service, it is imperative to establish robust security measures. If not adequately attended to, there is a possibility of disruptions in the distribution process of mail and shipments, which can lead to inconvenience and a decrease in trust towards PT Pos Indonesia. Hence, it is imperative to conduct a security audit to comprehensively understand the security measures used inside the I-POS information system.

The researcher conducted the audit using the COBIT 2019 and ITIL 4 frameworks. The COBIT 2019 framework serves as a valuable tool for effectively managing information technology, including comprehensive rules that promote the establishment of robust information system security measures. The COBIT 2019 framework emphasizes four primary domains: planning and strategy, implementation and operation, monitoring and assessment, and maintenance and improvement. Organizations benefit from utilizing information system security measures to effectively mitigate risks and safeguard valuable information assets against cyber threats.

ITIL 4 is a framework designed to facilitate the effective and efficient management of IT services within enterprises. The ITIL 4 framework emphasizes five key domains: guiding principles, governance, service value chain, practices, and ongoing improvement. This process aids companies in identifying the information technology service requirements necessary for the organization while ensuring that these services have sufficient security measures.

METHOD

The researcher utilized a qualitative descriptive approach as the chosen methodology for this investigation. The researchers employed a qualitative descriptive technique in order to obtain a comprehensive comprehension of the conditions of information system security, as outlined by COBIT 2019 and ITIL 4. The data-collecting process in this study encompassed the acquisition of information derived from questionnaire responses and observations about the security capabilities of the I-POS information system at PT. Pos Indonesia. This study, which employed a qualitative descriptive approach, assessed information about the continuous performance of the security measures implemented in the I-POS system. Following this, a connection was established between the ideas above and the frameworks of COBIT 2019 and ITIL 4. The many stages of this research endeavor can be discerned using the subsequent research framework:

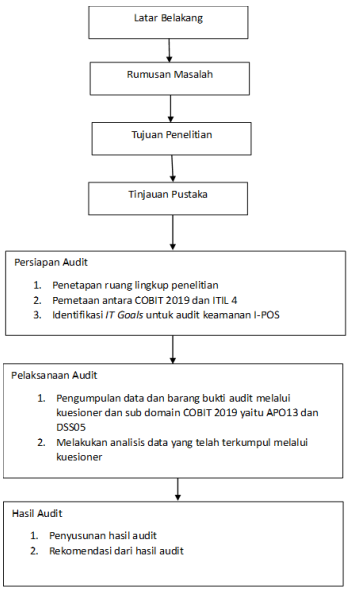

Figure 1 . Research Flow

RESULTS AND DISCUSSION

Audit Preparation

Audit preparation is a crucial stage in ensuring the smoothness and success of the audit process. During this stage, researchers need to conduct thorough preparation to identify audit objectives, determine the scope, and identify IT processes and IT goals.

Determination of Audit Scope

Establishing the audit scope under the COBIT 2019 framework entails a methodical and organized approach to achieve efficient auditing outcomes. The COBIT 2019 framework has been specifically developed to govern, regulate, and assess information systems effectively. Within the framework of COBIT 2019, establishing the audit scope encompasses the systematic procedure of discerning audit entities, electing audit domains, and outlining suitable constraints on the scope. Researchers can utilize COBIT 2019 as a reference to incorporate defined control objectives and the existing framework, ensuring comprehensive consideration of all pertinent issues within the audit scope.

The primary purpose of COBIT 2019 is to offer guidance on mapping and selecting domains and processes to ensure that assessments comply with research requirements. This pertains to the strategic objectives of the research subject, namely the enhancement of the I-POS information system at PT. Pos Indonesia.

Identify IT Processes and IT Goals

At this stage, researchers identify IT Processes, IT Goals and SWOT analysis which are described below:

Identify IT Processes

The IT process identification stage is a process of mapping IT goals that have been obtained previously with the IT process in COBIT 2019. The purpose of the IT process identification stage is to find out what processes exist or are being implemented within the organization. The results of mapping IT goals and IT processes can be seen in table 4.1 below. in the research contained in table 1, namely:

Table 1. IT Mapping and Process

Tujuan IT	Proses IT	
	DSS	APO
1. Mendefinisi, mengoperasikan dan mengawasi sistem untuk manajemen keamanan informasi yang dipakai dilembaga instansi menjaga agar dampakdan kejadian dari insiden keamanan informasi terkendali	05	
2. Melindungi sistem informasi I-POS untuk mempertahankan tingkatan dari keamanan informasi menetapkan, mengelola hak akses user dan melakukan pengawasan keamanan dengan tujuan meminimalisasikan dari kerentanan dan insiden dari keamanan informasi operasional		13

The table above is the result of mapping between IT processes and IT goals which obtains

2 IT processes. The mapping results listed in the table above are then combined with the supporting processes contained in the COBIT 2019 framework. The mapping table above is also used as a basis for preparing the questionnaire. The function of the questionnaire is to determine the importance of each IT process in the 2019 COBIT Framework.

Identify IT Goals

The identification of IT goals is an essential component in the management and auditing of information systems. IT goals refer to a business's specific objectives by utilizing and executing information technology. The initial stage in creating IT goals entails comprehending the business requirements and plans of the organization. Auditors or IT teams can discern pertinent IT objectives when examining many dimensions of information technology, such as security, availability, operational efficiency, and innovation.

Establishing IT objectives for the I-POS information system relies on data gathered from interviews or surveys conducted with high-level respondents. This method aims to understand the vision, mission comprehensively, and SWOT analysis (Strengths, Weaknesses, Opportunities, and Threats) encountered by PT. Pos Indonesia.

SWOT analysis

At this juncture, the researcher proceeds to give the SWOT analysis of the I-POS information system, drawing upon interviews conducted with the head of the security section at PT. Pos Indonesia.

One area of focus that demonstrates notable proficiency or advantage. Enhances the efficiency of the audit trail tracking procedure. The system exhibits a centralized integration, facilitating convenient control over its operations. One area of concern or limitation that can be identified is the presence of weaknesses. The complexity of conducting audits in the event of security problems is still evident in the system.

The complete delivery of activity logs to the Security Information and Event Management (SIEM) system needs to be observed. The topic of opportunities is a subject of interest and importance. The tracking of user activity and access is implemented. The vulnerability assessment exam was passed successfully.

The persistence of access rights misuse about system utilization remains a concern.

Audit Implementation

The execution of the audit is a pivotal phase conducted to assess and appraise the facets under scrutiny. During this phase, the researcher will stick to the specified methodology and refer to the COBIT 2019 framework. The researcher will execute predetermined duties, including gathering data, identifying IT processes and goals, and evaluating control efficacy. The outcomes of this audit implementation will be utilized to assemble an audit report that includes findings, recommendations for improvement, and an evaluation of the system or process's adherence to relevant standards.

Data Collection and Audit Evidence Using COBIT 2019. Examining data and audit findings using the COBIt 2019 framework starts by examining the results of creating questionnaires

related to information system security represented by the APO13 and DSS05 domains. After the findings are collected, validation must be done to determine whether the answers to the questionnaire distributed are correct. Valid. Each question will be categorized in detail according to each question domain, as follows:

Table 2. Data collection categories for each domain

Domain / Proses Number : APO13		
Data Collection	**Description**	**Metode Pengumpulan Data**
PA 1.1 – Process Performance	1. Pembangunan dan pemeliharaan sistem manajemen keamanan informasi (SMKI) 2. Pemantauan dan Peninjauan SMKI 3. Pendefinisian dan pengelolaan rencana perlakuan resiko keamanan informasi	Kuesioner
Domain / Proses Number : DSS05		
Data Collection	**Description**	**Metode Pengumpulan Data**
PA 1.1 – Process Performance	1. Perlindungan terhadap malware 2. Pengelolaan keamanan jaringan dan konektifitas 3. Memonitor infrastuktur untuk kegiatan yang berhubungan dengan keamanan 4. Mengelola keamanan *endpoint* 5. Mengelola identitas pengguna dan akses yang logis	Kuesioner

Domain / Proses Number : APO13		
Achievement	**Description**	**Metode Pengumpulan Data**
PA 2.1 – Performance Management	1. Pendefinisian tujuanuntuk kinerja proses 2. Pemantauan dan perencanaan kinerja proses 3. Penyesuaian kinerja proses untuk memenuhi rencana 4. Pendefinisian, penugasan dan pengkomunikasikan tanggung jawab dan wewenang untuk melakukan proses. 5. Pendefinisian, pengalokasikan dan penggunaan sumber daya dan informasi yang diperlukan untuk melakukan proses 6. Komunikasi antara pihak-pihak yang terlibat dikelola untuk memastikan komunikasi yang efektif dan kejelasan penugasan tanggung jawab	Kuesioner
PA 2.2 – Work Product Management	1. Pendefinisan persyaratan untuk produk kerja dari proses 2. Pendefinisian persyaratan untukdokumentasi dan kontrol dari produk kerja 3. Pengidentifikasikan, pendokumentasikan dan pengendalian produk kerja secara tepat	Kuesioner

Domain / Proses Number : APO13		
Achievement	**Description**	**Metode Pengumpulan Data**
	4. Peninjauan produk kerja apakah sudah sesuai dengan pengaturan yang direncanakan dan disesuaikan seperlunya untuk memenuhi persyaratan	
PA 3.1 – Process Definition	1. Pendefinisian proses standar yang menggambarkan unsur-unsur mendasar yang harus dimasukkan kedalam sebuah proses tersebut. 2. Penentuan urutan dan interaksi dari proses standar dengan proses lainnya 3. Pendefinisian kompetensi yang dibutuhkan dan peran untuk melakukan proses sebagai bagian dari proses standar 4. Pengidentifikasian infrastruktur yang diperlukan dan lingkungan kerja untuk melakukan proses sebagai bagian dari proses standar 5. Penetapan metode yang cocok untuk memantau efektifitas dan kesesuaian proses tersebut	Kuesioner

Domain / Proses Number : APO13		
Achievement	**Description**	**Metode Pengumpulan Data**
PA 3.2 – Process Deployment	1. Pemilihan atau penyesuaian proses yang didefinisikan ditempatkan didasarkan pada standar proses yang tepat 2. Pendefinisian, penugasan dan pengkomunikasian peran, tanggung jawab dan kewenangan yang diperlukan untuk melakukan proses 3. Pendefinisian kompetensi personil yang melaksanakan proses atas dasar pendidikan, pelatihan dan pengalaman. 4. Pendefinisian, pengalokasian dan penggunaan sumber daya yang diperlukan dan informasi yang diperlukan untuk melakukan suatu proses 5. Pendefinisian, pengelolaan dan pemeliharaan infrastruktur yang diperlukan dan lingkungan kerja untuk melakukan proses 6. Data yang sesuai dikumpulkan dan dianalisis sebagai dasar untuk memahami perilaku dari proses untuk menunjukan kesesuaian dan efektifitas, serta mengevaluasi perbaikan berkelanjutan dari proses yang dapat dibuat	Kuesioner

Domain / Proses Number : APO13		
Achievement	**Description**	**Metode Pengumpulan Data**
PA 4.1 – Process Measurement	1. Informasi proses yang dibutuhkan mendukung tujuan bisnis relavan 2. Tujuan pengukuran proses yang berasal dari kebutuhan informasi proses 3. Tujuan kuantitatif untuk kinerja proses dalam mendukung tujuan bisnis yang relavan ditetapkan 4. Tindakan dan frekuensi pengukuran diidentifikasi dan didefinisikan sejalan dengan tujuan pengukuran proses dan tujuan kuantitatif untuk kinerja proses 5. Pengumpulan, penganalisaan dan pelaporan hasil pengukuran untuk memantau sejauh mana tujuan kuantitatif untuk kinerja proses terpenuhi 6. Hasil pengukuran yang digunakan menggambarkan kinerja proses	Kuesioner
PA 4.2 – Process Measurement	1. Penentuan dan penerapan analisis dan kontrol teknik yang berlaku 2. Penetapan batas kontrol variasi untuk kinerja proses normal	Kuesioner

Domain / Proses Number : APO13		
Achievement	**Description**	**Metode Pengumpulan Data**
	3. Penganalisaan data pengukuran untuk penyebab khusus variasi 4. Pengambilan tindakan korektif untuk mengatasi penyebab khusus variasi 5. Pendirian kembali (jika diperlukan) batas kontrol berikut tindakan korektif	Kuesioner
PA 5.1 – Process Innovation	1. Dampak dari semua perubahan yang diusulkan dinilai terhadap tujuan dari proses yang didefinisikan dan proses standar 2. Pengelolaan persetujuan pelaksanaan semua perubahan untuk memastikan bahwa setiap gangguan terhadap kinerja proses dipahami dan diberi tindakan 3. Berdasarkan kinerja aktual, efektivitas proses perubahaan dievaluasi terhadap persyaratan produk dan tujuan proses yang ditetapkan untuk penentuan hasil apakah dikarenakan sebab umum atau khusus	Kuesioner

Domain / Proses Number : APO13		
Achievement	**Description**	**Metode Pengumpulan Data**
	3. Berdasarkan kinerja aktual, efektivitas proses perubahaan dievaluasi terhadap persyaratan produk dan tujuan proses yang ditetapkan untuk penentuan hasil apakah dikarenakan sebab umum atau khusus	
PA 5.2 – Process Optimisation	1. Dampak dari semua perubahan yang diusulkan dinilai terhadap tujuan dari proses yang didefinisikan dan proses standar 2. Pengelolaan persetujuan pelaksanaan semua perubahan untuk memastikan bahwa setiap gangguan terhadap kinerja proses dipahami dan diberi tindakan 3. Berdasarkan kinerja aktual, efektivitas proses perubahaan dievaluasi terhadap persyaratan produk dan tujuan proses yang ditetapkan untuk penentuan hasil apakah dikarenakan sebab umum atau khusus	Kuesioner

Domain / Proses Number : DSS05		
Achievement	**Description**	**Metode Pengumpulan Data**
PA 2.1 – Performance Management	1. Pendefinisian tujuanuntuk kinerja proses 2. Pemantauan dan perencanaan kinerja proses 3. Penyesuaian kinerja proses untuk memenuhi rencana 4. Pendefinisian, penugasan dan pengkomunikasikan tanggung jawab dan wewenang untuk melakukan proses. 5. Pendefinisian, pengalokasikan dan penggunaan sumber daya dan informasi yang diperlukan untuk melakukan proses	Kuesioner

Domain / Proses Number : DSS05		
Achievement	**Description**	**Metode Pengumpulan Data**
	6. Komunikasi antara pihak-pihak yang terlibat dikelola untuk memastikan komunikasi yang efektif dan kejelasan penugasan tanggung jawab	
PA 2.2 – Work Product Management	1. Pendefinisan persyaratan untuk produk kerja dari proses 2. Pendefinisian persyaratan untukdokumentasi dan kontrol dari produk kerja 3. Pengidentifikasikan, pendokumentasikan dan pengendalian produk kerja secara tepat 4. Peninjauan produk kerja apakah sudah sesuai dengan pengaturan yang direncanakan dan disesuaikan seperlunya untuk memenuhi persyaratan	Kuesioner
PA 3.1 – Process Definition	1. Pendefinisian proses standar yang menggambarkan unsur-unsur mendasar yang harus dimasukkan kedalam sebuah proses tersebut. 2. Penentuan urutan dan interaksi dari proses standar dengan proses lainnya	Kuesioner

Domain / Proses Number : DSS05		
Achievement	**Description**	**Metode Pengumpulan Data**
	3. Pendefinisian kompetensi yang dibutuhkan dan peran untuk melakukan proses sebagai bagian dari proses standar 4. Pengidentifikasian infrastruktur yang diperlukan dan lingkungan kerja untuk melakukan proses sebagai bagian dari proses standar 5. Penetapan metode yang cocok untuk memantau efektifitas dan kesesuaian proses tersebut	
PA 3.2 – Process Deployment	1. Pemilihan atau penyesuaian proses yang didefinisikan ditempatkan didasarkan pada standar proses yang tepat 2. Pendefinisian, penugasan dan pengkomunikasian peran, tanggung jawab dan kewenangan yang diperlukan untuk melakukan proses 3. Pendefinisian kompetensi personil yang melaksanakan proses atas dasar pendidikan, pelatihan dan pengalaman 4. Pendefinisian, pengalokasian dan penggunaan sumber daya yang diperlukan dan informasi yang diperlukan untuk melakukan suatu proses	Kuesioner

Domain / Proses Number : DSS05		
Achievement	**Description**	**Metode Pengumpulan Data**
	5. Pendefinisian, pengelolaan dan pemeliharaan infrastruktur yang diperlukan dan lingkungan kerja untuk melakukan proses 6. Data yang sesuai dikumpulkan dan dianalisis sebagai dasar untuk memahami perilaku dari proses untuk menunjukan kesesuaian dan efektifitas, serta mengevaluasi perbaikan berkelanjutan dari proses yang dapat dibuat	
PA 4.1 – Process Measurement	1. Informasi proses yang dibutuhkan mendukung tujuan bisnis relavan 2. Tujuan pengukuran proses yang berasal dari kebutuhan informasi proses 3. Tujuan kuantitatif untuk kinerja proses dalam mendukung tujuan bisnis yang relavan ditetapkan 4. Tindakan dan frekuensi pengukuran diidentifikasi dan didefinisikan sejalan dengan tujuan pengukuran proses dan tujuan kuantitatif untuk kinerja proses	Kuesioner

Domain / Proses Number : DSS05		
Achievement	**Description**	**Metode Pengumpulan Data**
	5. Pengumpulan, penganalisaan dan pelaporan hasil pengukuran untuk memantau sejauh mana tujuan kuantitatif untuk kinerja proses terpenuhi 6. Hasil pengukuran yang digunakan menggambarkan kinerja proses	
PA 4.2 – Process Measurement	1. Penentuan dan penerapan analisis dan kontrol teknik yang berlaku 2. Penetapan batas kontrol variasi untuk kinerja proses normal 3. Penganalisaan data pengukuran untuk penyebab khusus variasi 4. Pengambilan tindakan korektif untuk mengatasi penyebab khusus variasi 5. Pendirian kembali (jika diperlukan) batas kontrol berikut tindakan korektif	Kuesioner
PA 5.1 – Process Innovation	1. Dampak dari semua perubahan yang diusulkan dinilai terhadap tujuan dari proses yang didefinisikan dan proses standar	Kuesioner

Domain / Proses Number : DSS05		
Achievement	**Description**	**Metode Pengumpulan Data**
	2. Pengelolaan persetujuan pelaksanaan semua perubahan untuk memastikan bahwa setiap gangguan terhadap kinerja proses dipahami dan diberi tindakan 3. Berdasarkan kinerja aktual, efektivitas proses perubahan dievaluasi terhadap persyaratan produk dan tujuan proses yang ditetapkan untuk penentuan hasil apakah dikarenakan sebab umum atau khusus	
PA 5.2 – Process Optimisation	1. Dampak dari semua perubahan yang diusulkan dinilai terhadap tujuan dari proses yang didefinisikan dan proses standar 2. Pengelolaan persetujuan pelaksanaan semua perubahan untuk memastikan bahwa setiap gangguan terhadap kinerja proses dipahami dan diberi tindakan 3. Berdasarkan kinerja aktual, efektivitas proses perubahan dievaluasi terhadap persyaratan produk dan tujuan proses yang ditetapkan untuk penentuan hasil apakah dikarenakan sebab umum atau khusus	Kuesioner

Questionnaire Respondents

The questionnaire respondents were selected based on this study's specific requirements, encompassing managers, division heads, security system workers, and users actively engaged with the I-POS information system at PT. Pos Indonesia. During this phase, the researcher will stick to the specified methodology and refer to the COBIT 2019 framework. The researcher will execute predetermined duties, including the gathering of data, identification of IT processes and IT goals, and evaluation of the effectiveness of controls. The outcomes of this audit implementation will be employed to assemble an audit report comprising discoveries, suggestions for improvement, and an evaluation of the system or process's adherence to relevant standards.

Examination of Audit Findings Data for Process Number APO13

The APO13 number process has a derivative for determining the results as follows:

Tabel 3. Outcome dari Proses APO13

Outcome	Deskripsi
APO13.01	Sebuah sistem ditempatkan pada tempat yang dianggap efektif untuk menangani persyaratan keamanan informasi perusahaan
APO13.02	Sebuah rencana keamanan telah dibentuk, diterima dan dikomunikasikan di seluruh perusahaan
APO13.03	Solusi keamanan informasi di implementasikan dan dioperasikan secara konsisten di seluruh perusahaan

The total percentage of achievement/outcome determines the value of Total achievement PA 1.1 and Rating by Criteria for APO13. However, the percentage of achievement/outcome for each outcome is determined based on the percentage of achievement/component. The components of each outcome are as follows.

Table 4. Components of each outcome in the APO13 process

Outcome	*Component*	*Number*	*Description*
APO13.01	*Work Product Output*	APO13-WP1	Kebijakan SMKI
		APO13-WP2	Pernyataan lingkup SMKI
		APO13-WP5	Laporan audit SMKI
		APO13-WP6	Rekomendasi untuk menigkatkan SMKI
	Base Practice + Work Product Input	APO13-BP1	Membangun dan memeliharan SMKI
		APO13-BP3	Memantau dan meninjau SMKI
APO13.02	*Work Product Output*	APO13-WP3	Rencanan perlakuan resiko keamanan informasi
		APO13-WP4	Kasus bisnis keamanan informasi
	Base Practice + Work Product Input	APO13-BP2	Mendefinisikan dan menegelola rencana perilaku kontrol
APO13.03	*Work Product Output*	APO13-WP5	Laporan audit SMKI
		APO13-WP6	Rekomendasi untuk meningkatkan SMKI
	Base Practice + Work Product Input	APO13-BP13	Memantau dan meninjau SMKI

The component process is obtained from the total of all "Y" answers divided by the total number of questions from each component, as in the following table.

Table 5. Tabulation of audit assessment of process number APO13

Number	*Description*	*Achievement/ component*	*Achievement/ Outcome*	*Outcome*	*Total Achievement PA 1.1 (APO13)*
APO13-WP1	Kebijakan SMKI	100%	100% (100%+100%)/2	APO13.01	86% (100%+93%+65%)/3
APO13-WP2	Pernyataan lingkup SMKI				
APO13-WP5	Laporan audit SMKI				
APO13-WP6	Rekomendasi untuk menigkatkan SMKI				
APO13-BP1	Membangun dan memeliharan SMKI	100%			
APO13-BP3	Memantau dan meninjau SMKI				
APO13-WP3	Rencanan perlakuan resiko keamanan informasi	100%	93% (100%+86%)/2	APO13.02	
APO13-WP4	Kasus bisnis keamanan informasi				

Number	*Description*	*Achievement/ component*	*Achievement/ Outcome*	*Outcome*	*Total Achievement PA 1.1 (APO13)*
APO13-BP2	Mendefinisikan dan menegelola rencana perilaku kontrol	86%			
APO13-WP5	Laporan audit SMKI	50%	65% (50%+80%)/2	APO13.03	
APO13-WP6	Rekomendasi untuk meningkatkan SMKI				
APO13-BP13	Memantau dan meninjau SMKI	80%			

The provided table depicts the audit assessment tabulation for the APO13 process. The initial achievement/component outcomes are derived from the summation calculation of the mean scores obtained from the participants who have been computed.

The cumulative percentage of respondent results for APO13-WP1, APO13-WP2, APO13-WP4, and APO13-WP5 amounts to 100% in APO13. Subsequently, the computation of APO13-BP1 and APO13-BP5 yields a 100% outcome. Following this, the combined values of APO13-WP1, APO13-WP2, APO13-WP5, APO13-WP5, APO13-BP1, and APO13-BP5 are divided by two, yielding the ultimate score of APO13.01 as 100%.

The computation of the subsequent components, namely APO13-WP3 and APO13-WP4, produces a perfect score of 100%, while APO13-BP2 elicits a respondent answer rate of 86%. Subsequently, the summation of APO13-WP3, APO13-WP4, and APO13-BP2 is divided by two, yielding the ultimate score of APO13.02 as 93%.

The final computation encompasses APO13-WP5 and APO13-WP6, wherein the respondents collectively provide a response rate of 50% out of 5 respondents. Conversely, APO13-BP3 elicits a response rate of 80% from the respondents. Following this, the combined values of APO13-WP5, APO13-WP6, and APO13-BP3 are divided by two, yielding the ultimate score of APO13.03 as 65%.

The cumulative score for Performance Area 1.1 (P.A 1.1) of APO13 is determined by adding the individual scores of 100%, 93%, and 65% and dividing the sum by 3. This calculation yields a final result of 86% for APO13 P.A 1.1.

Examination of Audit Findings Data for Process Numbered DSS05

The numbered DSS05 process has derivatives for determining results as follows:

Table 6. Outcomes from process number DSS05

Outcome	*Description*
DSS05.01	Jaringan dan keamanan komunikasi memenuhi kebutuhan bisnis
DSS05.02	Informasi di proses, disimpan, dan dikirimkan oleh perangkat *endpoint* yang dilindungi
DSS05.03	Semua pengguna unik diidentifikasi dan memiliki hak akses sesuai dengan peran bisnis perusahaaan

The total achievement/outcome presentation determines the value of Total achievement P. A 1.1 and Rating by Criteria for DSS05; however, each outcome's achievement/outcome presentation is determined based on the achievement/outcome presentation. The components of each outcome are as follows.

Table 7. Components of each outcome in Process Number DSS05

Outcome	*Component*	*Number*	*Description*
DSS05.01	*Work Product Output*	DSS05-WP1	Kebijakan pencegahan perangkat lunak berbahaya
		DSS05-WP2	Evaluasi potensi ancaman
		DSS05-WP10	Karakteristik insiden keamanan
		DSS05-WP11	Log peristiwa keamanan
		DSS05-WP12	Tiket insiden keamanan
		DSS05-WP13	Inventarisasi dokumen sensitif dan perangkat
		DSS05-WP14	Hak akses
	Base Practice + Work Product Input	DSS05-BP1	Melindungi malware
		DSS05-BP2	Mengelola keamanan jaringan dan konektivitas
		DSS05-BP7	Memonitor infrastruktur untuk acara yang berhubungan dengan keamanan
DSS05.02	*Work Product Output*	DSS05-WP3	Kebijakan keamanan konektivitas
		DSS05-WP4	Hasil tes penetrasi
		DSS05-WP5	Kebijakan keamanan untuk perangkat endpoint
	Base Practice + Work Product Input	DSS05-BP1	Melindungi terhadap malware
		DSS05-BP3	Mengelola keamanan endpoint
DSS05.03	*Work Product Output*	DSS05-WP6	Hak akses disetujui
		DSS05-WP7	Hasil tinjauan dari akun pengguna dan hak istimewa
	Base Practice + Work Product Input	DSS05-BP4	Mengelola identitas pengguna dan akses logis

The Component process is obtained from the total of all "Y" answers divided by the total number of questions from each Component, as in the following table:

Table 8. tabulation of audit assessment of process number DSS05

Number	*Description*	*Achievement/ component*	*Achievement/ Outcome*	*Outcome*	*Total Achievement PA 1.1 (DSS05)*
DSS05-WP1	Kebijakan pencegahan perangkat lunak berbahaya	100%	85% (100% + 70%)/2	DSS05.01	85% (85% + 77% + 94%)/3
DSS05-WP2	Evaluasi potensi ancaman				
DSS05-WP10	Karakteristik insiden keamanan				
DSS05-WP11	Log peristiwa keamanan				
DSS05-WP12	Tiket insiden keamanan				
DSS05-WP13	Inventarisasi dokumen sensitif dan perangkat				
DSS05-WP14	Hak akses				
DSS05-BP1	Melindungi malware	70%			
DSS05-BP2	Mengelola keamanan jaringan dan konektivitas				
DSS05-BP7	Memonitor infrastruktur untuk acara yang berhubungan dengan keamanan				
DSS05-WP3	Kebijakan keamanan konektivitas	67%	77% (67% + 87%)/2	DSS05.02	
DSS05-WP4	Hasil tes penetrasi				
DSS05-WP5	Kebijakan keamanan untuk perangkat endpoint				
DSS05-BP1	Melindungi terhadap malware	87%			
DSS05-BP3	Mengelola keamanan endpoint				
DSS05-WP6	Hak akses disetujui	100%	94% (100% + 88%)/2	DSS05.03	
DSS05-WP7	Hasil tinjauan dari akun pengguna dan hak istimewa				
DSS05-BP4	Mengelola identitas pengguna dan akses logis	88%			

The table presents the audit assessment tabulation for process number DSS05, specifically for the first Achievement/Component. This tabulation is derived from the recapitulation computation of

the average scores acquired from the respondents. The cumulative percentage of responder results for DSS05-WP1, DSS05-WP2, DSS05-WP10, DSS05-WP11, DSS05-WP12, DSS05-WP13, and DSS05-WP14 amounts to 100%. Subsequently, the computation of DSS05-BP1, DSS05-BP2, and DSS05-BP7 yields a cumulative score of 70%, averaged by dividing it by 2, resulting in the ultimate score of DSS05.01 85%.

The computation of DSS05-WP6 and DSS05-WP7 yields a responder % response rate of 67% based on a sample size of 5 respondents. In the context of the calculations conducted for DSS05-BP1 and DSS05-BP3, the result indicates that 87% of the total respondents, which amounts to 5 individuals, provided the same response. The summation of these two computations is divided by two, yielding the ultimate score of DSS05.02 as 77%.

The computation of DSS05-WP3, DSS05-WP4, and DSS05-WP5 yields a responder response rate of 100% from a sample size of 5 respondents. In the context of the DSS05-BP4 calculation, it is seen that the outcome yielded an 88% response rate based on the feedback received from a sample size of 5 individuals. The summation of these two computations is divided by two, yielding the ultimate score of DSS05.03 as 94%.

The cumulative Achievement P. A 1.1 for DSS05 is determined by aggregating the individual scores of 85%, 77%, and 94% and dividing the sum by 3. This computation yields the conclusive outcome for DSS05 P.A 1.1 as 85%.

The Achievement P. A 1.1 score from each domain is collected and entered into the adjusted format. The ratings for each level and each domain are acquired in the following manner.

Table 9. Ratings for APO13 Domains

Process Name	Level 1	Level 2		Level 3		Level 4		Level 5	
APO13	PA 1.1	PA 2.1	PA 2.2	PA 3.1	PA 3.2	PA 4.1	PA 4.2	PA 5.1	PA5.2
Rating by Criteria	86%	88%	81%	70%	58%	63%	70%	60%	83%
Rating	F	F	L	L	L	L	L	L	L
Capability Level Achieved	1	1	2	Stop!	Stop!	Stop!	Stop!	Stop!	Stop!

The table presented above displays the ratings about the APO13 domain. The process is denoted as Level 1 in P. A 1.1 generates a Rating by Criteria of 86%. This rating falls within category F, and the Achievement capability level is classified as level 1.

Subsequently, the Level 2 process designation inside P. A 2.1 produces a Rating by Criteria of 88%, accompanied by a rating in category F, while the Achievement capacity level remains at level 1. Following this, the Level 2 process designation in P. A 2.2 produces a Rating by Criteria of 81%, categorized as F, while the Achievement capability level remains at level 2.

In the context of P. A 3.1, the Level 3 process is denoted by a Rating by Criteria of 70%. This rating falls inside category L, and the Achievement capability level is indicated as STOP! Due to its value being below 85% in P.A 3.1. Moreover, the process is denoted as Level 3 in P. A 3.2 yields a Rating by Criteria of 58%, categorized as L. Notably, the Achievement capability level is marked as STOP! Due to the cessation of the preceding process in P.A 3.2, thereby resulting in the discontinuation of the Level 3 process in P.A 4.2.

Furthermore, the Level 4 process name in P. A 4.1 yields a Rating by Criteria of 63%,

accompanied by a rating in category L. Notably, the Achievement capability level is denoted as STOP! Due to the cessation of the preceding process, resulting in the discontinuation of the Level 4 process name in P.A 4.1. Moreover, the Level 4 process designation in P.A 4.2 yields a Rating by Criteria of 70%, accompanied by a rating in category L. Additionally, the Achievement capability level is denoted as STOP! Due to the cessation of the preceding process, resulting in the discontinuation of the Level 4 process designation in P.A 4.2.

In the context of P. A 5.1, it is observed that the degree 5 process name yields a Rating by Criteria of 60%. This rating is categorized as L, indicating a specific degree of achievement. Notably, the Achievement capability level is marked with the notation STOP! Due to the cessation of the preceding process, P.A 4.2. Consequently, the Level 5 process name in P. A 5.1 is terminated. Following this, the process is denoted as Level 5 in P. A 5.2 demonstrates a Rating by Criteria of 83%, with a rating assigned to category L. Additionally, the Achievement capability level is marked as STOP! Due to the cessation of the preceding process, resulting in the discontinuation of the Level 5 process in P.A 5.2.

Tabel 10. Rating untuk Domain DSS05

Process Name	Level 1	Level 2		Level 3		Level 4		Level 5	
DSS05	PA 1.1	PA 2.1	PA 2.2	PA 3.1	PA 3.2	PA 4.1	PA 4.2	PA 5.1	PA5.2
Rating by Criteria	85%	88%	69%	75%	67%	83%	90%	80%	67%
Rating	F	F	L	L	L	L	F	L	L
Capability Level Achieved	1	1	2	Stop!	Stop!	Stop!	Stop!	Stop!	Stop!

The table presented above depicts the ratings assigned to the DSS05 domain. The process is denoted as Level 1 in P.A 1.1 yields a Rating by Criteria of 85%. This rating corresponds to category F, and the process demonstrates an Achievement capacity level of 1.

Subsequently, the Level 2 process designation inside P. A 2.1 results in a Rating by Criteria of 88%, accompanied by a rating of category F, while the Achievement capacity level remains at level 1. Following this, the Level 2 process designation in P. A 2.2 produces a Rating by Criteria of 69%, accompanied by a rating in category F, but the Achievement capacity level remains at level 2.

In the context of P. A 3.1, the degree 3 process is denoted by a Rating by Criteria of 75%. This rating falls inside category L, indicating a specific degree of performance. Notably, the Achievement capability level is marked with a notation STOP! Due to its value being below the threshold of 85% in P.A 3.1. Moreover, the Level 3 process designation in P.A 3.2 yields a Rating by Criteria of 67%, accompanied by a rating in category L. Additionally, the Achievement capability level is marked with the notation STOP! Due to the cessation of the preceding process in P. A 3.2, thus, resulted in discontinuing the Level 3 process designation in P—a 4.2.

Furthermore, the Level 4 process name in P. A 4.1 yields a Rating by Criteria of 83%, accompanied by a rating in category L. Notably, the Achievement capability level is denoted as STOP! Due to the cessation of the preceding process, which therefore results in the discontinuation of the Level 4 process name in P.A 4.1. Moreover, the Level 4 process designation in P. A 4.2 produces a Rating by

Criteria of 90%, accompanied by a rating in category F. Additionally, the Achievement capability level is denoted as STOP! Due to the cessation of the preceding process, resulting in the discontinuation of the Level 4 process designation in P.A 4.2.

In the context of P. A 5.1, it is observed that the degree 5 process name yields a Rating by Criteria of 60%. This rating is categorized as L, indicating a specific degree of achievement. Notably, the Achievement capability level is marked with the notation STOP! This signifies that the process preceding P. A 4.2 has ceased, thereby resulting in the discontinuation of the Level 5 process name in P.A 5.1. Following this, the process is denoted as Level 5 in P. A 5.2 demonstrates a Rating by Criteria of 83%, with a rating assigned to category L. Additionally, the Achievement capability level is marked as STOP! Due to the cessation of the preceding process, resulting in the discontinuation of the Level 5 process in P.A 5.2.

Obtaining a rating by criteria is the basis for determining the rating obtained from

a. N (Not Achieved / Not Achieved)
   This category occurs if the range obtained from the rating by criteria is between 0-15%
b. P (Partially Achieved)
   This category occurs if the range obtained from the rating by criteria is between 15-50%
c. L (Large Achieved / Mostly Achieved)
   This category occurs if the range obtained from the rating by criteria is between 50-85%
d. F (Fully Achieved)
   This category occurs if the range obtained from the rating by criteria is between 85-10%

Assessment of Existing Results

The process of obtaining ratings for each domain has been completed, and the subsequent phase involves evaluating the current outcomes, which encompass:

The current state of APO13.

The outcomes derived from the current state encompass the following: There needs to be more documentation of procedural steps outlining the controls (in the form of a control matrix) associated with establishing, implementing, and overseeing information security management systems.

The lack of a comprehensive quality plan that outlines the necessary work products, quality criteria, documentation requirements, and change control procedures about the establishment, operation, and monitoring of information security management systems.

The absence of rules and standards that establish organizational goals for processes, minimum performance criteria, standardized procedures, and reporting and monitoring obligations about the definition, operation, and monitoring of information security management systems.

The need to identify essential infrastructure and working conditions required for executing standard processes for defining, operating, and monitoring information security management systems.

One of the challenges identified is the need for high-quality records and performance records. The Process GWP 9.0 is required to

present substantiating proof of the reviews that have been completed about the establishment, implementation, and oversight of information security management systems.

The failure to implement designated procedures aligned with the relevant context about establishing, functioning, and overseeing information security management systems.

One of the critical challenges identified in this study is the need for more apparent establishment and effective communication of roles, duties, and powers regarding the execution of defined processes associated with managing information security systems.

The primary concern is sufficient confidence in one's ability to effectively execute the required procedures to define, operate, and monitor information security management systems.

The need for adequate resources and information to facilitate the execution of designated procedures for establishing, implementing, and supervising information security management systems.

The lack of process plans that encompass comprehensive process architecture and working environment for each process instance about the Defining, running, and monitoring of systems for information security management.

The absence of process improvement plans that encompass process improvement objectives and proposed improvement activities about the definition, operation, and monitoring of information security management systems.

One of the key issues identified is the need for clearly defined quantitative objectives for process performance, specifically about aligning processes with business objectives about establishing, operating, and monitoring information security management systems.

There is a need for process measurement plans that outline comprehensive analytical techniques about the definition, operation, and monitoring of information security management systems.

The absence of gathering measurement outcomes about the performance of designated processes associated with the definition, operation, and monitoring of information security management systems.

The present study highlights the issue of insufficient identification and selection of suitable analytical and control methodologies for effectively managing process performance in the context of defining, running, and monitoring information security management systems.

Established process control plans are needed to ascertain the standard performance for Defining, running, and monitoring systems for information security management.

A comprehensive framework for identifying, implementing, and overseeing appropriate parameters to regulate the performance of processes about the definition, operation, and monitoring of information security management systems is needed.

The absence of process improvement plans that outline specific objectives and planned activities for enhancing the Defining, operating, and monitoring systems for information security management.

There is a need for clearly defined process improvement targets for the processes supporting pertinent business objectives about establishing,

operating, and supervising information security management systems.

More process improvement plans are needed to offer a comprehensive analysis of optimal practices about the definition, operation, and monitoring of information security management systems.

The absence of a precise determination regarding the implementation strategies that align with the long-term vision and objectives of the definition, operation, and monitoring of information security management systems.

The effectiveness of process improvements on process performance, capability goals, and business objectives can be evaluated based on actual performance. The absence of a systematic approach to measuring, evaluating, and reporting the efficacy of post-implementation process modifications in establishing, operating, and overseeing information security management systems is evident.

The current state of DSS05.

The findings derived from the current state encompass the absence of comprehensive process documentation that outlines the controls (control matrix) about the protection of company information, which is necessary to uphold an acceptable level of information security risk by the firm's security policy.

A comprehensive quality plan needs to outline the necessary work products, quality criteria, documentation requirements, and change control procedures for protecting firm information to uphold an acceptable level of information security risk, as mandated by the organization's security policy.

The deficiency lies in the failure to thoroughly evaluate and modify work products to adhere to defined standards about the protection of company information and to maintain an acceptable level of risk associated with information security, as outlined in the organization's security policy.

The lack of rules and standards that outline a process map containing specific specifics regarding standard procedures and the anticipated sequence and interaction about the protection of firm information to uphold an acceptable level of information security risk by the company's security policy.

The absence of identification regarding the essential infrastructure and working environment required for executing standard operations is associated with safeguarding firm information to uphold an acceptable degree of information security risk per the organization's security policy.

There is a need for comprehensive and reliable documentation about quality and performance records. Process GWP 9.0 is required to furnish substantiation of conducted reviews about safeguarding company information in order to uphold an acceptable threshold of information security risk by the firm's security policy.

The absence of comprehensive process plans, which should have specific resource plans for each process instance about protecting firm information, helps maintain an acceptable level of information security risk by the organization's security policy.

The absence of comprehensive process plans encompassing specific process infrastructure and

working environment for each process instance about protecting firm information poses challenges in maintaining an acceptable level of information security risk by the organization's security policy.

The insufficiency in providing appropriate process infrastructure to facilitate the execution of designated processes about safeguarding firm information in order to uphold an acceptable level of information security risk by the organization's security policy.

The absence of data collection and analysis about process performance hinders the ability to showcase compliance and efficacy in safeguarding firm information, hence maintaining an acceptable level of information security risk by the organization's security policy.

The lack of process measurement plans that outline specific recommended actions, indicators, data-gathering techniques, and procedures connected to safeguarding firm information is a challenge in maintaining an acceptable level of information security risk, as mandated by the organization's security policy.

The absence of identification of

Using product and process measures is crucial in facilitating the attainment of quantitative objectives pertaining to process performance, specifically in safeguarding firm information to uphold an acceptable threshold of information security risk, as outlined in the organization's security policy.

There needs to be more process control plans to establish control limits for regular performance regarding safeguarding company information to uphold an acceptable level of information security risk by the organization's security policy.

The absence of data measurement analysts hinders the ability to detect actual and possible deviations in process performance concerning safeguarding company information, hence maintaining an acceptable level of information security risk by the firm's security policy.

The lack of process improvement plans that offer comprehensive implementation strategies for enhancing processes connected to safeguarding firm information in order to uphold an acceptable level of information security risk by the organization's security policy.

The absence of effective management of agreed-upon changes to designated areas of specified processes and standards by the implementation strategy about protecting company information is a concern for maintaining an acceptable level of information security risk as outlined in the firm's security policy.

Gap

The gap is the difference between the target level to be achieved and the capability level achieved. From the existing results for the two domains above, a gap graph can be obtained, as shown in the image below:

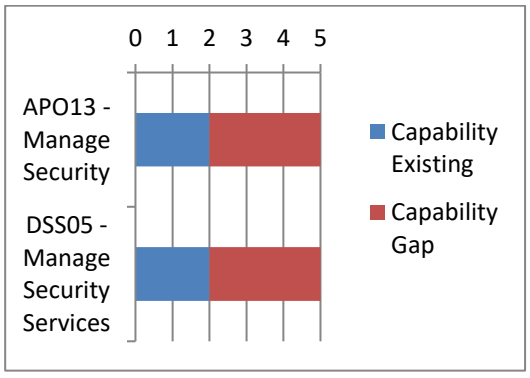

Figure 2. Graph of existing Capability and Capability gap

The graph illustrates that the company's desired level is 5; however, the I-POS capability level is at PT. Pos Indonesia, as indicated by the results and audit data, is now at level 2. According to the available information, PT. Pos Indonesia is now positioned at level 3. In order to attain the required level set by PT. Pos Indonesia, the organization must rectify its deficiencies and strive towards meeting the specified objectives.

I-POS Information System Security Audit Results Report

The audit outcomes on the information system security will encompass identified findings and corresponding recommendations to enhance the current security measures of the I-POS information system. The report's structure may differ among organizations due to the absence of a universally regulated format for its compilation. The forthcoming audit report will provide a comprehensive assessment of PT's existing information system security status. Pos Indonesia, enabling the organization to undertake appropriate measures.

Based on the assessment results from the I-POS security audit at PT. Pos Indonesia, security capability level can be seen from the table below

Table 11. Final report of I-POS information system security audit

Domain	*Capability Target*	Capability Existing	*Gap*	Kondisi *Existing*	Rekomendasi
APO13	5	2	3	a. Belum adanya dokumentasi proses yang memberikan rincian kontrol (matriks kontrol) terkait Mendefinisikan, mengoperasikan dan memantau sistem untuk manajemen keamanan informasi. b. Belum adanya rencana kualitas yang memberikan rincian produk kerja, kriteria kualitas, persyaratan dokumentasi dan kontrol perubahan terkait Mendefinisikan, mengoperasikan dan memantau sistem untuk manajemen keamanan informasi.	a. Perlu dibuatkannya dokumentasi proses yang memberikan rincian kontrol (matriks kontrol) terkait Mendefinisikan, mengoperasikan dan memantau sistem untuk manajemen keamanan informasi. b. Perlu dibuatkannya rencana kualitas yang memberikan rincian produk kerja, kriteria kualitas, persyaratan dokumentasi dan kontrol perubahan terkait Mendefinisikan, mengoperasikan dan memantau sistem untuk manajemen keamanan informasi.

Domain	*Capability Target*	Capability Existing	*Gap*	Kondisi *Existing*	Rekomendasi
				c. Belum adanya kebijakan dan standar harus memberikan rincian tujuan organisasi untuk proses, standar minimum kinerja, prosedur standar, dan persyaratan pelaporan dan pemantauan terkait Mendefinisikan, mengoperasikan dan memantau sistem untuk manajemen keamanan informasi. d. Belum adanya identifikasi infrastruktur dan lingkungan kerja yang diperlukan untuk melakukan proses standar terkait Mendefinisikan, mengoperasikan dan memantau sistem untuk manajemen keamanan informasi.	c. Perlu dibuatkannya kebijakan dan standar harus memberikan rincian tujuan organisasi untuk proses, standar minimum kinerja, prosedur standar, dan persyaratan pelaporan dan pemantauan terkait Mendefinisikan, mengoperasikan dan memantau sistem untuk manajemen keamanan informasi. d. Perlu dibuatkannya identifikasi infrastruktur dan lingkungan kerja yang diperlukan untuk melakukan proses standar terkait Mendefinisikan, mengoperasikan dan memantau sistem untuk manajemen keamanan informasi.

Domain	*Capability Target*	Capability Existing	*Gap*	Kondisi *Existing*	Rekomendasi
				e. Belum adanya catatan kualitas dan catatan kinerja Proses GWP 9.0 harus memberikan bukti tinjauan yang dilakukan terkait Mendefinisikan, mengoperasikan dan memantau sistem untuk manajemen keamanan informasi. f. Belum adanya penerapan proses yang ditentukan yang memenuhi konteks terkait Mendefinisikan, mengoperasikan dan memantau sistem untuk manajemen keamanan informasi. g. Belum adanya penetapan dan mengkomunikasikan peran, tanggung jawab dan wewenang	e. Perlu dibuatkannya catatan kualitas dan catatan kinerja Proses GWP 9.0 harus memberikan bukti tinjauan yang dilakukan terkait Mendefinisikan, mengoperasikan dan memantau sistem untuk manajemen keamanan informasi. f. Perlu dibuatkannya penerapan proses yang ditentukan yang memenuhi konteks terkait Mendefinisikan, mengoperasikan dan memantau sistem untuk manajemen keamanan informasi. g. Perlu dibuatkannya penetapan dan mengkomunikasikan peran, tanggung jawab dan wewenang

Domain	*Capability Target*	Capability Existing	*Gap*	Kondisi *Existing*	Rekomendasi
				untuk melakukan proses yang ditentukan terkait Mendefinisikan, mengoperasikan dan memantau sistem untuk manajemen keamanan informasi. h. Belum adanya pemastian kompetensi yang diperlukan untuk melakukan proses yang ditentukan terkait Mendefinisikan, mengoperasikan dan memantau sistem untuk manajemen keamanan informasi. i. Belum adanya penyediaan sumber daya dan informasi untuk mendukung kinerja proses yang ditentukan terkait Mendefinisikan,	untuk melakukan proses yang ditentukan terkait Mendefinisikan, mengoperasikan dan memantau sistem untuk manajemen keamanan informasi. h. Perlu dibuatkannya pemastian kompetensi yang diperlukan untuk melakukan proses yang ditentukan terkait Mendefinisikan, mengoperasikan dan memantau sistem untuk manajemen keamanan informasi. i. Perlu dibuatkannya penyediaan sumber daya dan informasi untuk mendukung kinerja proses yang ditentukan terkait Mendefinisikan,

Domain	*Capability Target*	Capability Existing	*Gap*	Kondisi *Existing*	Rekomendasi
				mengoperasikan dan memantau sistem untuk manajemen keamanan informasi. j. Belum adanya rencana proses yang mencakup rincian infrastruktur proses dan lingkungan kerja untuk setiap contoh proses terkait Mendefinisikan, mengoperasikan dan memantau sistem untuk manajemen keamanan informasi. k. Belum adanya rencana perbaikan proses yang memberikan tujuan perbaikan proses dan tindakan Peningkatan yang diusulkan terkait Mendefinisikan,	mengoperasikan dan memantau sistem untuk manajemen keamanan informasi. j. Perlu dibuatkannya rencana proses yang mencakup rincian infrastruktur proses dan lingkungan kerja untuk setiap contoh proses terkait Mendefinisikan, mengoperasikan dan memantau sistem untuk manajemen keamanan informasi. k. Perlu dibuatkannya rencana perbaikan proses yang memberikan tujuan perbaikan proses dan tindakan Peningkatan yang diusulkan terkait Mendefinisikan,

Domain	*Capability Target*	Capability Existing	*Gap*	Kondisi *Existing*	Rekomendasi
				mengoperasikan dan memantau sistem untuk manajemen keamanan informasi. l. Belum adanya penetapan tujuan kuantitatif untuk kinerja proses yang ditetapkan, sesuai dengan keselarasan proses dengan tujuan bisnis terkait Mendefinisikan, mengoperasikan dan memantau sistem untuk manajemen keamanan informasi. m. Belum adanya rencana pengukuran proses yang memberikan rincian prosedur analitis yang diusulkan terkait Mendefinisikan, mengoperasikan	mengoperasikan dan memantau sistem untuk manajemen keamanan informasi. l. Perlu dibuatkannya penetapan tujuan kuantitatif untuk kinerja proses yang ditetapkan, sesuai dengan keselarasan proses dengan tujuan bisnis terkait Mendefinisikan, mengoperasikan dan memantau sistem untuk manajemen keamanan informasi. m. Perlu dibuatkannya rencana pengukuran proses yang memberikan rincian prosedur analitis yang diusulkan terkait Mendefinisikan, mengoperasikan

Domain	*Capability Target*	Capability Existing	*Gap*	Kondisi *Existing*	Rekomendasi
				dan memantau sistem untuk manajemen keamanan informasi. n. Belum adanya pengumpulan hasil pengukuran produk dan proses melalui melakukan proses yang ditentukan terkait Mendefinisikan, mengoperasikan dan memantau sistem untuk manajemen keamanan informasi. o. Belum adanya penentuan teknik analisis dan kontrol yang tepat untuk mengontrol kinerja proses terkait Mendefinisikan, mengoperasikan dan memantau sistem untuk manajemen keamanan informasi.	dan memantau sistem untuk manajemen keamanan informasi. n. Perlu dibuatkannya pengumpulan hasil pengukuran produk dan proses melalui melakukan proses yang ditentukan terkait Mendefinisikan, mengoperasikan dan memantau sistem untuk manajemen keamanan informasi. o. Perlu dibuatkannya penentuan teknik analisis dan kontrol yang tepat untuk mengontrol kinerja proses terkait Mendefinisikan, mengoperasikan dan memantau sistem untuk manajemen keamanan informasi.

Domain	*Capability Target*	Capability Existing	*Gap*	Kondisi *Existing*	Rekomendasi
				p. Belum adanya rencana kontrol proses yang ada untuk menentukan untuk setiap batas kontrol untuk kinerja normal terkait Mendefinisikan, mengoperasikan dan memantau sistem untuk manajemen keamanan informasi. q. Belum ada penentuan parameter yang cocok untuk mengontrol kinerja proses terkait Mendefinisikan, mengoperasikan dan memantau sistem untuk manajemen keamanan informasi. r. Belum adanya rencana perbaikan proses yang memberikan tujuan perbaikan proses dan	p. Perlu dibuatkannya rencana kontrol proses yang ada untuk menentukan untuk setiap batas kontrol untuk kinerja normal terkait Mendefinisikan, mengoperasikan dan memantau sistem untuk manajemen keamanan informasi. q. Perlu dibuatkannya penentuan parameter yang cocok untuk mengontrol kinerja proses terkait Mendefinisikan, mengoperasikan dan memantau sistem untuk manajemen keamanan informasi. r. Perlu dibuatkannya rencana perbaikan proses yang memberikan tujuan perbaikan proses dan

Domain	*Capability Target*	Capability Existing	*Gap*	Kondisi *Existing*	Rekomendasi
				perbaikan proses dan tindakan perbaikan yang diusulkan terkait Mendefinisikan, mengoperasikan dan memantau sistem untuk manajemen keamanan informasi. s. Belum adanya penentuan tujuan peningkatan proses untuk proses yang mendukung tujuan bisnis yang relevan terkait Mendefinisikan, mengoperasikan dan memantau sistem untuk manajemen keamanan informasi. t. Belum adanya rencana perbaikan proses yang memberikan rincian analisis terhadap praktik terbaik terkait Mendefinisikan,	tindakan perbaikan yang diusulkan terkait Mendefinisikan, mengoperasikan dan memantau sistem untuk manajemen keamanan informasi. s. Perlu dibuatkannya penentuan tujuan peningkatan proses untuk proses yang mendukung tujuan bisnis yang relevan terkait Mendefinisikan, mengoperasikan dan memantau sistem untuk manajemen keamanan informasi. t. Perlu dibuatkannya rencana perbaikan proses yang memberikan rincian analisis terhadap praktik terbaik terkait Mendefinisikan,

Domain	*Capability Target*	Capability Existing	*Gap*	Kondisi *Existing*	Rekomendasi
				mengoperasikan dan memantau sistem untuk manajemen keamanan informasi. u. Belum adanya penentuan strategi implementasi berdasarkan visi dan tujuan perbaikan jangka panjang terkait Mendefinisikan, mengoperasikan dan memantau sistem untuk manajemen keamanan informasi. v. Berdasarkan kinerja aktual, mengevaluasi efektivitas perubahan proses terhadap kinerja proses, tujuan kemampuan dan tujuan bisnis. Belum adanya efektivitas perubahan yang dilakukan pada proses diukur,	mengoperasikan dan memantau sistem untuk manajemen keamanan informasi. u. Perlu dibuatkannya penentuan strategi implementasi berdasarkan visi dan tujuan perbaikan jangka panjang terkait Mendefinisikan, mengoperasikan dan memantau sistem untuk manajemen keamanan informasi. v. Berdasarkan kinerja aktual, mengevaluasi efektivitas perubahan proses terhadap kinerja proses, tujuan kemampuan dan tujuan bisnis. Perlu dibuatkannya efektivitas perubahan yang

Domain	*Capability Target*	Capability Existing	*Gap*	Kondisi *Existing*	Rekomendasi
				dievaluasi dan dilaporkan setelah implementasi terkait Mendefinisikan, mengoperasikan dan memantau sistem untuk manajemen keamanan informasi.	dilakukan pada proses diukur, dievaluasi dan dilaporkan setelah implementasi terkait Mendefinisikan, mengoperasikan dan memantau sistem untuk manajemen keamanan informasi.

Domain	*Capability Target*	Capability Existing	*Gap*	Kondisi *Existing*	Rekomendasi
DSS05	5	2	3	a. Belum adanya dokumentasi proses yang memberikan rincian kontrol (matriks kontrol) terkait Melindungi informasi perusahaan untuk menjaga tingkat risiko keamanan informasi yang dapat diterima oleh perusahaan sesuai dengan kebijakan keamanan. b. Belum adanya rencana kualitas yang memberikan rincian produk kerja, kriteria kualitas, persyaratan dokumentasi dan kontrol perubahan terkait Melindungi informasi perusahaan untuk menjaga tingkat risiko keamanan informasi yang dapat diterima oleh perusahaan sesuai dengan kebijakan keamanan.	a. Perlu dibuatkannya dokumentasi proses yang memberikan rincian kontrol (matriks kontrol) terkait Melindungi informasi perusahaan untuk menjaga tingkat risiko keamanan informasi yang dapat diterima oleh perusahaan sesuai dengan kebijakan keamanan. b. Perlu dibuatkannya rencana kualitas yang memberikan rincian produk kerja, kriteria kualitas, persyaratan dokumentasi dan kontrol perubahan terkait Melindungi informasi perusahaan untuk menjaga tingkat risiko keamanan informasi yang dapat diterima oleh perusahaan sesuai dengan kebijakan keamanan.

Domain	*Capability Target*	Capability Existing	*Gap*	Kondisi *Existing*	Rekomendasi
				c. Belum adanya peninjauan dan menyesuaikan produk kerja untuk memenuhi persyaratan yang ditentukan terkait Melindungi informasi perusahaan untuk menjaga tingkat risiko keamanan informasi yang dapat diterima oleh perusahaan sesuai dengan kebijakan keamanan. d. Belum adanya kebijakan dan standar yang menyediakan pemetaan proses dengan rincian proses standar dan urutan dan interaksi yang diharapkan terkait melindungi informasi perusahaan untuk menjaga tingkat risiko keamanan informasi yang dapat diterima oleh perusahaan sesuai dengan kebijakan keamanan.	c. Perlu dibuatkannya peninjauan dan menyesuaikan produk kerja untuk memenuhi persyaratan yang ditentukan terkait Melindungi informasi perusahaan untuk menjaga tingkat risiko keamanan informasi yang dapat diterima oleh perusahaan sesuai dengan kebijakan keamanan. d. Perlu dibuatkannya kebijakan dan standar yang menyediakan pemetaan proses dengan rincian proses standar dan urutan dan interaksi yang diharapkan terkait melindungi informasi perusahaan untuk menjaga tingkat risiko keamanan informasi yang dapat diterima oleh perusahaan sesuai dengan kebijakan keamanan.

Domain	*Capability Target*	Capability Existing	*Gap*	Kondisi *Existing*	Rekomendasi
				e. Belum adanya identifikasi infrastruktur dan lingkungan kerja yang diperlukan untuk melakukan proses standar terkait Melindungi informasi perusahaan untuk menjaga tingkat risiko keamanan informasi yang dapat diterima oleh perusahaan sesuai dengan kebijakan keamanan. f. Belum adanya catatan kualitas dan catatan kinerja Proses GWP 9.0 yang memberikan bukti tinjauan yang dilakukan terkait Melindungi informasi perusahaan untuk menjaga tingkat risiko keamanan informasi yang dapat diterima oleh perusahaan sesuai dengan kebijakan keamanan.	e. Perlu dibuatkannya identifikasi infrastruktur dan lingkungan kerja yang diperlukan untuk melakukan proses standar terkait Melindungi informasi perusahaan untuk menjaga tingkat risiko keamanan informasi yang dapat diterima oleh perusahaan sesuai dengan kebijakan keamanan. f. Perlu dibuatkannya catatan kualitas dan catatan kinerja Proses GWP 9.0 yang memberikan bukti tinjauan yang dilakukan terkait Melindungi informasi perusahaan untuk menjaga tingkat risiko keamanan informasi yang dapat diterima oleh perusahaan sesuai dengan kebijakan keamanan.

Domain	*Capability Target*	Capability Existing	*Gap*	Kondisi *Existing*	Rekomendasi
				g. Belum adanya rencana proses harus mencakup rincian rencana sumber daya untuk setiap contoh proses terkait Melindungi informasi perusahaan untuk menjaga tingkat risiko keamanan informasi yang dapat diterima oleh perusahaan sesuai dengan kebijakan keamanan. h. Belum adanya rencana proses yang mencakup rincian infrastruktur proses dan lingkungan kerja untuk setiap contoh proses terkait Melindungi informasi perusahaan untuk menjaga tingkat risiko keamanan informasi yang dapat diterima oleh perusahaan sesuai dengan kebijakan keamanan.	g. Perlu dibuatkannya rencana proses harus mencakup rincian rencana sumber daya untuk setiap contoh proses terkait Melindungi informasi perusahaan untuk menjaga tingkat risiko keamanan informasi yang dapat diterima oleh perusahaan sesuai dengan kebijakan keamanan. h. Perlu dibuatkannya rencana proses yang mencakup rincian infrastruktur proses dan lingkungan kerja untuk setiap contoh proses terkait Melindungi informasi perusahaan untuk menjaga tingkat risiko keamanan informasi yang dapat diterima oleh perusahaan sesuai dengan kebijakan keamanan.

Domain	*Capability Target*	Capability Existing	*Gap*	Kondisi *Existing*	Rekomendasi
				i. Belum adanya penvediaan infrastruktur proses yang memadai untuk mendukung kinerja proses yang ditentukan terkait Melindungi informasi perusahaan untuk menjaga tingkat risiko keamanan informasi yang dapat diterima oleh perusahaan sesuai dengan kebijakan keamanan. j. Belum adanya pengumpulan dan menganalisis data tentang kinerja proses untuk menunjukkan kesesuaian dan efektivitasnya terkait Melindungi informasi perusahaan untuk menjaga tingkat risiko keamanan informasi yang dapat diterima oleh perusahaan sesuai dengan kebijakan keamanan.	i. Perlu dibuatkannya penvediaan infrastruktur proses yang memadai untuk mendukung kinerja proses yang ditentukan terkait Melindungi informasi perusahaan untuk menjaga tingkat risiko keamanan informasi yang dapat diterima oleh perusahaan sesuai dengan kebijakan keamanan. j. Perlu dibuatkannya pengumpulan dan menganalisis data tentang kinerja proses untuk menunjukkan kesesuaian dan efektivitasnya terkait Melindungi informasi perusahaan untuk menjaga tingkat risiko keamanan informasi yang dapat diterima oleh perusahaan sesuai dengan kebijakan keamanan.

Domain	*Capability Target*	Capability Existing	*Gap*	Kondisi *Existing*	Rekomendasi
				k. Belum adanya rencana pengukuran proses yang memberikan rincian tindakan dan indikator yang diusulkan bersama dengan prosedur pengumpulan data dan prosedur terkait Melindungi informasi perusahaan untuk menjaga tingkat risiko keamanan informasi yang dapat diterima oleh perusahaan sesuai dengan kebijakan keamanan. l. Belum adanya pengidentifikasian ukuran produk dan proses yang mendukung pencapaian tujuan kuantitatif untuk kinerja proses terkait Melindungi informasi perusahaan untuk menjaga tingkat risiko keamanan informasi yang	k. Perlu dibuatkannya rencana pengukuran proses yang memberikan rincian tindakan dan indikator yang diusulkan bersama dengan prosedur pengumpulan data dan prosedur terkait Melindungi informasi perusahaan untuk menjaga tingkat risiko keamanan informasi yang dapat diterima oleh perusahaan sesuai dengan kebijakan keamanan. l. Perlu dibuatkannya pengidentifikasian ukuran produk dan proses yang mendukung pencapaian tujuan kuantitatif untuk kinerja proses terkait Melindungi informasi perusahaan untuk menjaga tingkat risiko keamanan informasi

Domain	*Capability Target*	Capability Existing	*Gap*	Kondisi *Existing*	Rekomendasi
				dapat diterima oleh perusahaan sesuai dengan kebijakan keamanan. m. Belum ada rencana kontrol proses yang ada untuk menentukan batas kontrol untuk kinerja normal terkait Melindungi informasi perusahaan untuk menjaga tingkat risiko keamanan informasi yang dapat diterima oleh perusahaan sesuai dengan kebijakan keamanan. n. Belum ada penganalisis data pengukuran proses untuk mengidentifikasi variasi nyata dan potensial dalam kinerja proses terkait Melindungi informasi perusahaan untuk menjaga tingkat risiko keamanan informasi yang dapat	yang dapat diterima oleh perusahaan sesuai dengan kebijakan keamanan. m. Perlu dibuatkannya rencana kontrol proses yang ada untuk menentukan batas kontrol untuk kinerja normal terkait Melindungi informasi perusahaan untuk menjaga tingkat risiko keamanan informasi yang dapat diterima oleh perusahaan sesuai dengan kebijakan keamanan. n. Perlu dibuatkannya penganalisis data pengukuran proses untuk mengidentifikasi variasi nyata dan potensial dalam kinerja proses terkait Melindungi informasi perusahaan untuk menjaga tingkat risiko keamanan informasi yang dapat

Domain	*Capability Target*	Capability Existing	*Gap*	Kondisi *Existing*	Rekomendasi
				diterima oleh perusahaan sesuai dengan kebijakan keamanan. o. Belum ada rencana perbaikan proses yang memberikan rincian strategi implementasi untuk perbaikan proses terkait Melindungi informasi perusahaan untuk menjaga tingkat risiko keamanan informasi yang dapat diterima oleh perusahaan sesuai dengan kebijakan keamanan. p. Belum ada pengelolaan implementasi perubahan yang disepakati ke area yang dipilih dari proses yang ditentukan dan standar sesuai dengan strategi implementasi terkait Melindungi informasi perusahaan untuk menjaga tingkat risiko	diterima oleh perusahaan sesuai dengan kebijakan keamanan. o. Perlu dibuatkannya rencana perbaikan proses yang memberikan rincian strategi implementasi untuk perbaikan proses terkait Melindungi informasi perusahaan untuk menjaga tingkat risiko keamanan informasi yang dapat diterima oleh perusahaan sesuai dengan kebijakan keamanan. p. Perlu dibuatkannya pengelolaan implementasi perubahan yang disepakati ke area yang dipilih dari proses yang ditentukan dan standar sesuai dengan strategi implementasi terkait Melindungi informasi perusahaan untuk menjaga tingkat

Domain	*Capability Target*	Capability Existing	*Gap*	Kondisi *Existing*	Rekomendasi
				keamanan informasi yang dapat diterima oleh perusahaan sesuai dengan kebijakan keamanan.	risiko keamanan informasi yang dapat diterima oleh perusahaan sesuai dengan kebijakan keamanan.

CONCLUSION

The conclusions were drawn from the I-POS security system audit conducted at PT. Pos Indonesia is as follows:

The audit process in this study encompasses multiple stages, which include providing the background information, formulating the problem, establishing research objectives, conducting a literature review, preparing for the audit, implementing the audit, and preparing the audit results.

The audit and evaluation of the I-POS information security system at PT. Pos Indonesia has determined that the capacity level, assessed based on the existing conditions of domains APO13 and DSS05, is now at level 2. However, the targeted capability level for the organization is level 5. Hence, the capability discrepancy observed under these circumstances amounts to three levels. In order to get the desired degree of capacity, the researcher offers several recommendations that PT. Pos Indonesia may take this into account. These recommendations encompass:

It is imperative to develop comprehensive process documentation that outlines the controls (in the form of control matrices) associated with the activities of Defining, Operating, and Monitoring information security management systems.

The necessity arises to develop a comprehensive quality plan that encompasses specific information on work products, quality criteria, documentation prerequisites, and change control procedures about the Defining,

Operating, and Monitoring systems for information security management.

The necessity to generate comprehensive process documentation that outlines control matrices about safeguarding organizational information.

REFERENCES

Agustin, H. (2018). Sistem Informasi Manajemen Menurut Prespektif Islam. Jurnal Tabarru': Islamic Banking and Finance, 1(1). https://doi.org/10.25299/jtb.2018.vol1(1).2045

Algiffary, A., M. Izman Herdiansyah, & Yesi Novaria Kunang. (2023). Audit Keamanan Sistem Informasi Manajemen Rumah Sakit Dengan Framework COBIT 2019 Pada RSUD Palembang BARI. Journal of Applied Computer Science and Technology, 4(1). https://doi.org/10.52158/jacost.v4i1.505

Amalia, M. N., Akbar, F., Risdiani, I., Islaha, A., & Srilena, N. (2020). Audit Sistem Informasi pada Perpustakaan ARS University Menggunakan Framework COBIT 5. Jurnal Sains Dan Informatika, 6(2). https://doi.org/10.34128/jsi.v6i2.226

Aritonang, I. J., Udayanti, E. D., & Iksan, N. (2018). Audit Keamanan Sistem Informasi Menggunakan Framework Cobit 5 (APO13). ITEJ (Information Technology Engineering Journals), 3(2). https://doi.org/10.24235/itej.v3i2.27

AXELOS. (2019). ITIL Foundation ITIL 4 Edition , Norwich UK, TSO (The Stationery Office)

David Purba, A., Adi Purnawan, I. K., & Agus Eka Pratama, I. P. (2018). Audit Keamanan TI Menggunakan Standar ISO/IEC 27002 dengan COBIT 5. Jurnal Ilmiah Merpati (Menara Penelitian Akademika Teknologi Informasi). https://doi.org/10.24843/jim.2018.v06.i03.p01

Driya, P. D., Putra, I. G. L. A. R., & Pradyana, I. M. A. (2022). Teknik Pengumpulan Data Pada Audit Sistem Informasi Dengan Framework COBIT. INSERT : Information System and Emerging Technology Journal, 2(2). https://doi.org/10.23887/insert.v2i2.40235

Gede Endra Bratha, W. (2022). Literature Review Komponen Sistem Informasi Manajemen: Software, Database Dan Brainware. Jurnal Ekonomi Manajemen Sistem Informasi, 3(3). https://doi.org/10.31933/jemsi.v3i3.824

Gusman, D. V., Prasetyo, F. H., & Adi, K. (2021). Audit Sistem Keamanan TI Menggunakan Domain DSS05 Pada Framework COBIT 5 (Studi Kasus: Diskominfo Kabupaten Karawang). Jurnal Informatika Upgris, 7(1). https://doi.org/10.26877/jiu.v7i1.8607

Habiba, A. (2021). Evaluasi Tata Kelola Keamanan Sistem Informasi

Menggunakan Framework COBIT 5 Pada PT. Tsabita Cake. JATISI (Jurnal Teknik Informatika Dan Sistem Informasi), 8(2). https://doi.org/10.35957/jatisi.v8i2.838

ISACA. (2018). COBIT 2019 FRAMEWORK Introduction and Methodology, Schaumburg, IL 60173, USA.

Jauhari, I. (2021). Sistem Informasi Manajemen Pendidikan Islam. Tarbawi Ngabar: Jurnal of Education, 2(2). https://doi.org/10.55380/tarbawi.v2i2.130

Kusuma, R. P. (2020). Audit Teknologi Informasi Menggunakan Framework COBIT 5 Pada Domain DSS (Deliver,Service, And Support) (Studi Kasus : Konsultan Manajemen Pusat). Jurnal Digit, 9(1). https://doi.org/10.51920/jd.v9i1.137

Loisa, J., Hosea, H., Claudio, A. C., Alvin, A., Anthonio, A., & Andry, J. F. (2018). Audit Sistem Keamanan Teknologi Informasi di PT. MNC Sekuritas Menggunakan COBIT 4.1 Domain DS5. JBASE - Journal of Business and Audit Information Systems, 1(2). https://doi.org/10.30813/.v1i2.1257

Matin, I. M. M., Arini, A., & Wardhani, L. K. (2018). Analisis Keamanan Informasi Data Center Menggunakan COBIT 5. Jurnal Teknik Informatika, 10(2). https://doi.org/10.15408/jti.v10i2.7026

Meyliana, A., Tristiyanto, T., & Prabowo, R. (2020). Audit Keamanan Sistem Informasi Di Dinas XYZ Provinsi Lampung Menggunakan Standar ISO/IEC 27001:2013. Jurnal Pepadun, 1(1). https://doi.org/10.23960/pepadun.v1i1.16

Miftahurrizqi, M., Windiarti, I. S., & Prabowo, A. (2021). Analisis Keamanan Sistem Pada Sistem Informasi Akademik Menggunakan Cobit 5 Framework Pada Sub Domain Dss05. Jurnal Sains Komputer Dan Teknologi Informasi, 3(2). https://doi.org/10.33084/jsakti.v3i2.2293

MIRA, T., Sediyono, E., & Iriani, A. (2021). Audit Pemanfaatan Sistem Informasi Akademik Di Universitas Kristen Wira Wacana Sumba Menggunakan Framework Cobit 5. Jointer - Journal of Informatics Engineering, 2(02). https://doi.org/10.53682/jointer.v2i02.39

Nurkholis, O., Fitroh, F. F., & Rustamaji, E. (2021). Usulan Keamanan Sistem Informasi pada Penyelenggara Financial Technology (Fintech) Menggunakan Cobit 5 (Studi Kasus: Gandengtangan.org). Applied Information System and Management (AISM), 2(2). https://doi.org/10.15408/aism.v2i2.20162

Parama Yoga, T., Alamsyah, R.. & Adwa, S. S. (2023). Audit Keamanan Sistem Informasi Menggunakan Cobit 5 di PT. Paramita Surya Makmur Plastika. Jurnal Accounting Information System

(AIMS, 6(1), 75–88. https://doi.org/10.32627

Parinsi, M. T., Mewengkang, A., & Rantung, T. (2021). Perancangan Sistem Informasi Sekolah Di Sekolah Menengah Kejuruan. Edutik : Jurnal Pendidikan Teknologi Informasi Dan Komunikasi, 1(3). https://doi.org/10.53682/edutik.v1i3.1340

Pradipta, Y. C., Rahardja, Y., & Sitokdana, M. N. N. (2019). Audit Sistem Manajemen Keamanan Informasi Pusat Teknologi Informasi Dan Komunikasi Penerbangan Dan Antariksa (PUSTIKPAN) Menggunakan SNI ISO/IEC 27001:2013. Sebatik, 23(2). https://doi.org/10.46984/sebatik.v23i2.782

Putri, H., Rini, F., & Pratama, A. (2022). Sistem Informasi Perpustakaan Berbasis Web. Jurnal Pustaka Data (Pusat Akses Kajian Database, Analisa Teknologi, Dan Arsitektur Komputer), 2(1). https://doi.org/10.55382/jurnalpustakadata.v2i1.138

Putu, P., Putra Pertama, G., & Ardiyasa, W. (2019). Audit Keamanan Sistem Informasi Perpustakaan STMIK STIKOM Bali Menggunakan Kerangka Kerja COBIT. Jurnal Sistem Dan Informatika (JSI), Vol 13, No. 2.

Ramadhan, I. (2020). Strategi Keamanan Cyber Security Di Kawasan Asia Tenggara. Jurnal Asia Pacific Studies, 3(2), 181–192. https://doi.org/10.33541/japs.v3i1.1081

Rochmadi, T., & Ike Yunia Pasa. (2021). Pengukuran Risiko Dan Evaluasi Keamanan Informasi Menggunakan Indeks Keamanan Informasi Di BKD XYZ Berdasarkan ISO 27001 / SNI. Cyber Security Dan Forensik Digital, 4(1). https://doi.org/10.14421/csecurity.2021.4.1.2439

Sepis, Y. T. (2022). Analisa Keamanan Sistem Informasi Menggunakan Framework COBIT 5 Dengan Domain DSS05 Dan APO13 DI PT XYZ. TeIKa, 12(01). https://doi.org/10.36342/teika.v12i01.2821

Setiawan, Suci Fitriani, Parama Yoga, Titan, Budiman Budiman. (2023). Information System Security Audit SIMKA(Sistem Informasi Kearsipan) at Badan Pendapatan Daerah Jawa Barat Kota Bandung III Using COBIT 5 Framework and Standard IS0/IEC 27002. International Journal of Quantitative Research and Moadeling (IJQRM), Vol 4, No 3 (2023). Copyright (c) 2023 International Journal of Quantitative Research and Modeling. http://journal.rescollacomm.com/index.php/ijqrm/article/view/499

Sukmana, Putra Pamungkas, Parama Yoga, Titan, Habibi, Chairul. (2023). Audit Manajemen Risiko Sistem Informasi pada Website Digo.id dengan Framework COBIT 5 dan ISO 31000. Jurnal Accounting Information System (AIMS). Vol. 6 No. 2 (2023).

Accounting Information Systems Study Program, Ma'soem University, Bandung. https://jurnal.masoemuniversity.ac.id/index.php/aims/article/view/816

Wijatmoko, T. E. (2020). Evaluasi Keamanan Informasi Menggunakan Indeks Keamanan Informasi (KAMI) Pada Kantor Wilayah Kementerian Hukum Dan HAM DIY. Cyber Security Dan Forensik Digital, 3(1). https://doi.org/10.14421/csecurity.2020.3.1.1951

Yuliani, S., Ramadhini, N. T., Gustisyaf, A. I., & Wahyudin, A. (2020). Asesmen Keamanan Informasi Menggunakan Indeks KAMI. Naratif : Jurnal Nasional Riset, Aplikasi Dan Teknik Informatika, 2(1). https://doi.org/10.53580/naratif.v2i1.76

Yusnanto, T., Mustofa, K., Machmudi, M. A., & Wahyudiono, S. (2021). Tantangan Fenomena Keamanan Informasi Pasca Era Revolusi Industri 5.0. TRANSFORMASI, 17(2). https://doi.org/10.56357/jt.v17i2.271