Jurnal Teknologi Sistem Informasi dan Aplikasi **ISSN: 2654-3788**
Penerbit: Program Studi Teknik Informatika Universitas Pamulang **e-ISSN: 2654-4229**
Vol. 7, No. 3, Juli 2024 (903-911) **DOI: 10.32493/jtsi.v7i3.39650**

Analisis Keamanan Sistem Informasi Menggunakan Cobit 2019 pada Sistem Sawit Rakyat Online (SRO) Studi Kasus PTPN V

Hanifan Arifin[1], Angraini[2], Tengku Khairil Ahsyar[3], Syaifullah[4]

Department of Information System, Fakultas Sains dan Teknologi, Universitas Islam Negeri Sultan Syarif Kasim Riau, Pekanbaru, Riau, Indonesia
e-mail: [1]11950311556@students.uin-suska.ac.id, [2]angraini@uin-suska.ac.id, [3]tengkukhairil@uin-suska.ac.id, [4]syaifullah@uin-suska.ac.id

Submitted Date: May 23rd, 2024 Reviewed Date: June 14th, 2024
Revised Date: June 18th, 2024 Accepted Date: June 20th, 2024

Abstract

One of the businesses that utilise information technology (IT), especially at PTPN V, is using the Sawit Rakyat Online (SRO) system, which is used to buy and sell oil palm seeds online. The SRO system has previously been attacked by malware. And there is also no related security for users and the system. Thus the need for Information System Security Analysis Using Cobit 2019 on the SRO System. 2019 COBIT framework is one of the frameworks used to analyse information system security in an organisation. Data collection through interviews and questionnaires with stakeholders, as well as data evaluation using the 2019 COBIT Framework used in this study, especially the DSS (Deliver, Service, and Support) area, with a focus on subdomain DSS05 (manage security services). The goal is to find out how secure the actual handling of the SRO information system at PTPN V is. This research looks at how secure the Sawit Rakyat Online (SRO) information system is at PT Perkebunan Nusantara V (PTPN V). This shows that DSS05.01 and DSS05.02 are at level 5, namely "Optimizing" On the other hand, DSS05.03, DSS05.04, DSS05.06, and DSS05.07 are at level 4 "Quantitative", and DSS05.05 is at the "Optimizing" level. And for the security level, it is at level 4 "Quantitative" because the total rating is 4.33. Although the SRO system meets the requirements of COBIT 2019, new ideas are still needed to deal with security risks.

Keywords: Cobit 2019; *Maturity level; Security level*; PTPN V

Abstrak

Salah satu usaha yang memanfaatkan teknologi informasi (TI) khususnya di PTPN V yaitu menggunakan sistem Sawit Rakyat Online (SRO) yang mana sistem ini digunakan untuk jual beli bibit kelapa sawit secara online. Sistem SRO sebelumnya pernah diserang oleh *malware*. Dan juga belum adanya keamananan terkait bagi pengguna dan sistem tersebut. Demikian diperlukannya Analisisi Keamanan Sistem Informasi Menggunakan Cobit 2019 Pada Sistem SRO. kerangka kerja COBIT 2019 merupakan salah satu *framework* yang digunakan untuk menganalisis keamanan sistem informasi pada sebuah organisasi. Pengumpulan data melalui wawancara dan kuisioner dengan pemangku kepentingan, serta evaluasi data menggunakan Kerangka kerja COBIT 2019 yang digunakan dalam penelitian ini, terutama area DSS (*Deliver, Service, and Support*), dengan fokus pada subdomain DSS05 (*manage security services*). Tujuannya untuk mengetahui seberapa aman sebenarnya penanganan sistem informasi SRO di PTPN V. Penelitian ini melihat seberapa aman sistem informasi Sawit Rakyat Online (SRO) di PT Perkebunan Nusantara V (PTPN V). Hal ini menunjukkan bahwa DSS05.01 dan DSS05.02 berada pada level 5 yaitu "*Optimizing*" Di sisi lain, DSS05.03, DSS05.04, DSS05.06, dan DSS05.07 berada pada level 4 "*Quantitative*", dan DSS05.05 berada pada level "*Optimizing*". Dan untuk tingkat keamanan nya berada pada level 4 "*Quantitative*"karena total ratingnya adalah 4,33. Meskipun sistem SRO memenuhi persyaratan COBIT 2019, namun tetap diperlukan ide-ide baru untuk menghadapi risiko keamanan.

Kata kunci: Cobit 2019; *Maturity level*; Tingkat keamanan; PTPN V

1. Pendahuluan

Keamanan informasi adalah perlindungan informasi dan sistem informasi dari akses, pengguna, manipulasi, memodifikasi, dan penghancuran oleh pengguna yang tidak memiliki kewenangan (Nurul et al., 2022). Keamanan informasi yang kuat akan membantu melindungi reputasi perusahaan. Hilangnya data pelanggan atau serangan dunia maya dapat merusak citra dan kepercayaan pelanggan. Keamanan informasi ini ditujukan untuk melindungi data dan informasi bisnis.

Perusahaan dan organisasi harus memperhatikan keberadaan Teknologi Informasi (TI) dan memanfaatkannya. Oleh karena itu, di perlukan pengelolaan TI yang efesien dan tepat untuk penggunaan Teknologi Informasi (TI) sebagai pendukung, bisa mengalami peningkatan evektifitas sumber daya dan efesiensi prosedur kerja (Setiawan & Wasilah, 2022)

Teknologi informasi yang digunakan harus dikelola dengan baik agar konsisten dengan realisasi strategi bisnis. Untuk mengatur penerapan teknologi informasi, telah dikembangkan metode pengelolaan teknologi informasi atau tata kelola TI (Ria & Budiman, 2021).

Salah satu perusahaan yang memanfaatkan TI adalah PT Perkebunan Nusantara V (PTPN V) beralamatkan di Jl. Rambutan No. 43, Sidomulyo Timur, Marpoyan Damai, Kota Pekanbaru, Riau 28294. PTPN V bergerak di sektor perkebunan kelapa sawit dan karet dalam pengelolaannya.

Sistem informasi yang digunakan perusahaan untuk proses bisnis ini disebut dengan sistem Sawit Rakyat Online (SRO). Sistem ini digunakan untuk transaksi jual beli bibit sawit secara online, selain menjual bibit sawit, sistem ini juga ada fitur lain nya seperti berbagi informasi/berita tentang seputar sawit/bibit sawit. Sistem ini dibuat sederhana dengan tujuan untuk memudahkan para pengguna (*user*) untuk mengakses dan menggunakan sistem tersebut.

Berdasarkan wawancara dengan Bapak M. Reiza Novianda S.T (Bidang TI) Pernah terjadi penyerangan *malware* pada sistem Sawit Rakyat Online (SRO) sehingga membuat pengguna tidak bisa membuka dan mengakses sistem Sawit Rakyat Online (SRO) tersebut. Dari penyerangan *malware* tersebut mengakibatkan sistem SRO mengalami *server down*, hal ini berpengaruh terhadap pembaharuan data yang tersedia tidak sesuai dengan realita di lapangan. Selain itu, belum ada keamanan sistem informasi yang mencakup perlindungan terhadap user dan sistem itu sendiri. Insiden tersebut menyebabkan gangguan serius terhadap operasional perusahaan, mengancam kerahasiaan data, integritas sistem, dan ketersediaan layanan. Dalam konteks ini, penelitian ini tidak hanya bertujuan untuk mengevaluasi kepatuhan sistem terhadap standar COBIT 2019, tetapi juga untuk memberikan wawasan yang mendalam tentang kelemahan yang ada dalam infrastruktur TI perusahaan, serta rekomendasi perbaikan yang spesifik untuk menghadapi ancaman keamanan yang semakin baik.

Penelitian ini menggunakan rangkaian kerja COBIT 2019 (*Control Objectives for Information and Related Technology)* yang dikembangkan oleh ICASA (Nachrowi et al., 2020), Yani Nurhadyani, dan Heru Sukoco 2020). COBIT 2019 terdapat 5 domain utama dan 40 proses yang diterapkan dalam tata kelola TI perusahaan. 5 domain itu adalah EDM (*Evaluate, Direct and Monitor*), APO (*Align, Plan and Organize*), BAI (Build, Acquire and Implement), DSS (*Deliver, Service and Support*), dan MEA (*Monitor, Evaluate and Implement*) (ICASA *Governance and Management* 2019). Domain yang di gunakan pada penelitian ini berfokus dengan domain DSS (*Deliver, Services and Support*) khususnya sub domain DSS05 (*Manage security services*). Pemilihan subdomain DSS05 didasarkan pada manajemen keamanan dan proses pengelolaan, serta memvalidasi bahwa kebutuhan, keadaan dan preferensi pihak yang terlibat ditinjau untuk menetapkan target organisasi di masa depan (Baharuddin et al., 2019). Penelitian ini bertujuan untuk menganalisis penerapan kerangka kerja COBIT 2019 pada PT Perkebunan Nusantara V dalam konteks keamanan sistem informasi dengan focus utama untuk mengevaluasi sejau mana pengelolaan sistem di PTPN V dapat diukur menggunakan perhitungan tingkat *maturity level* yang ada dalam rangkaian kerja COBIT 2019. Tingkat *maturity level* ini diharapkan bisa menjadi titik acuan untuk dilakukannya perbaikan pada pengelolaan sistem informasi Sawit Rakyat Online (SRO).

Berdasarkan uraian tersebut maka diperlukan analisis keamanan sistem informasi menggunakan cobit 2019 pada sistem sawit rakyat online studi kasus PTPN V. Cobit 2019 berguna untuk mengetahui tingkat kematangan tata kelola TI terhadap pengelolaan dan untuk mengetahui tingkat keamanan sistem pada sistem informasi sawit rakyat online.

2. Landasan Teori

2.1 Tata kelola TI

Tata kelola TI adalah sistem interaksi dan prosedur yang memandu organisasi untuk mengendalikan dan mencapai tujuan bisnis dengan menciptakan nilai melalui penggunaan teknologi informasi (Ria & Budiman, 2021). Tata kelola TI harus memungkinkan organisasi mencapai tujuannya. Perusahaan perlu mengevaluasi tata kelola TI mereka (Muttaqin et al., 2020).

2.1 Keamanan Informasi

Keamanan informasi yakni proses perlindungan aspek kerahaasiaan (*Confidentiality)*, keutuhan (*Integrity)*, dan ketersediaan (*Availability)* pada suatu asset informasi.

Kerahasiaan, keutuhan, dan ketersediaan informasi atau umumnya disebut sebagai segitiga C.I.A. merupakan karakteristik yang penting atau kritis pada suatu informasi (Akraman et al., 2018). Berikut merupakan penjelasan karakteristik informasi:

1. *Confidentiality* (Kerahasiaan)
   Karakteristik informasi yang memungkinkan informasi untuk dilindungi dari penyebaran atau pengaksesan yang tidak terkendali baik oleh perseorangan atau sistem.
2. *Integrity* (Keutuhan)
   Integrity Di gunakan untuk informasi dijaga secara utuh, lengkap, dan tidak berkurang dari sebagaimana harusnya. Karakteristik keutuhan dijaga dengan cara melindungi informasi dari kemungkinan terjadinya perubahan, perusakan, pengurangan, penghancuran, atau jenis gangguan yang lain terhadap informasi yang mengubah informasi dari bentuk aslinya.
3. *Availability* (Ketersediaan)
   Availability merupakan karakteristik informasi yang memungkinkan informasi untuk dapat diakses oleh pengguna yang diperkenan, baik berupa perorangan maupun sistem. Pengaksesan tersebut dilakukan tanpa adanya gangguan atau halangan.

2.2 Audit Sistem Informasi

Audit sistem informasi yakni tahapan penghimpunan dan pengujian bukti dalam menetapkan sistem informasi atau data yang diterapkan dengan kontrol internal apakah telah sesuai, serta apakah seluruh aset diproteksi dengan baik dan tidak disalahgunakan. Tujuan audit ini adalah untuk memastikan integritas, keandalan, efektivitas, dan efesiensi pengelolaan sistem informasi atau data berbasis computer (Azizah, 2017). Audit merupakam rangkaian yang terstruktur dan obyektif guna mengumpulkan dan menilai bukti mengenai tindakan ekonomi, dengan tujuan memberikan penjelasan atau asersi serta memeriksa sejauh mana langkah dari ekonomi sesuai kriteria yang berlaku, serta menginformasikan hasilnya pada pihak yang berkepentingan (Windasari et al., 2022).

2.3 Cobit

Control Objective for Information and Related Technology (COBIT) adalah rangkaian kerja untuk tata kelola teknologi informasi yang dikembangkan oleh ICASA dan ITGI sekitar tahun 1990. COBIT awal mula terbit tahun 1996, kemudian direvisi dan diterbitkan kembali pada tahun 1998, 2000, dan 2005. Kerangka kerja COBIT membantu organisasi dalam pengambilan keputusan terkait investasi teknologi informasi. Keberhasilan suatu organisasi dalam membangun TI yang efektif dapat dinilai dari sejauh mana organisasi tersebut memenuhi kriteria pengukuran informasi. COBIT adalah serangkaian panduan yang berguna sebagai referensi untuk menetapkan tahapan TI dan objektif control yang dibutuhkan dalam tata kelola TI (Natanael et al., 2018). COBIT memberikan tindakan umum dan praktik terbaik yang membantu perusahaan memanfaatkan TI sesuai target industry (Dharma et al., 2021).

2.4 Cobit 2019

COBIT 2019 adalah versi pembaruan dari panduan ISACA yang membicarakan pengelolaan dan manajemen TI. Kerangka kerja ini berdasarkan pengalaman lebih dari 24 tahun penggunaan COBIT oleh beragam perusahaan dan praktisi di bidang bisnis, teknologi informasi, risiko, asuransi

dan keamanan. COBIT 2019 membantu organisasi mencapai nilai baik TI dengan memelihara keseimbangan antara pencapaian keuntungan, optimalisasi pengelolaan risiko serta penggunaan sumber daya efektif (ISACA, 2019). COBIT 2019 adalah pembaruan terbaru setelah COBIT 5.0 yang dikembangkan oleh ISACA. Kerangka ini menyediakan panduan mengenai tata kelola dan manajemen TI dengan konteks alur bisnis organisasi. Perkembangan teknologi informasi dan era informasi yang dinamis di perusahaan menjadi faktor utama dalam mendukung pertumbuhan organisai (Pada 2023). Dalam COBIT 2019 masih terdapat 5 domain dan 2 area utama, yaitu *area governance* dan *area management. Area governance* umumnya dikelola pleh pimpinan atau dewa eksekutif perusahaan dan mencakup domain *Evaluate, Direct and Monitor* (EDM). Sementara itu, area management yang dikelola karyawan meliputi 4 domain yaitu *Align, Plan and Organize* (APO), *Build, Acquire and Implement* (BAI), *Deliver, Service and Support* (DSS) dan *Monitor, Evaluate and Assess* (MEA) (ISACA Governance and Manajement, 2019).

2.5 *Focus area maturity levels* COBIT 2019

Focus area Tingkat kematangan (*Maturity Level*) dapat digunakan untuk menentukan tujuan dan dikaitkan dengan area fokus. COBIT 2019 mendefinisikan tingkatan kematangan yang merupakan sekumpulan tingkat kemampuan sebagai ukuran kinerja di tingkat area fokus. Berikut ini adalah tingkat dalam mengukur kematangan:

1. Tingkat 0 Tidak Lengkap (*Incomplate*), Pekerjaan bisa atau tidak bisa terselesaikan untuk memperoleh target pengelolaan dan manajemen pada area fokus
2. Tingkat 1 Awal (*Initial*), Pekerjaan bisa terselesaikan, namun target keseluruhan dan rencana dari area belum dicapai sepenuhnya.
3. Tingkat 2 Dikelola (*Managed*), Perancangan dan perhitungan kinerja dilakukan, walaupun belum sepenuhnya memenuhi ketentuan.
4. Tingkat 3 Standardisasi (*Defined*), Standar keseluruhan perusahaan memberikan panduan yang merata.
5. Tingkat 4 Kuantitatif (*Quantitative*), Perusahaan berbasis data, dengan meningkatkan kinerja yang dapat diukur secara kuantitatif.
6. Tingakt 5 Mengoptimalkan (*Optimizing*), Perusahaan fokus pada peningkatan berkelanjutan.

2.6 Domain DSS (*Delivery, Service, Support*)

Pada domain DSS, terdapat Subdomain DSS05 yang merupakan focus utama pada keamanan informasi. Subdomain ini, yang dikenal dengan nama *manage security services* (mengelola layanan keamanan) yang terdiri dari 49 pernyataan yang dikelompokkan ke dalam 7 proses yang berbeda (Umar et al., 2020). Seperti pada tabel

Tabel 1 Praktik DSS05

Practice ID	Practice Name	Activity
DSS05.01.	*Protect against malware*	**6**
DSS05.02.	*Manage network and connectivity security*	9
DSS05.03.	*Manage endpoint security*	**9**
DSS05.04.	*Manage user identity and logical access*	**8**
DSS05.05.	*Manage physical access to IT assets*	**7**
DSS05.06.	*Manage sensitive documents and output devices*	**5**
DSS05.06.	*Monitor the infrastructure for security-related events*	**5**

Dalam DSS05, terdapat praktik sebagai berikut:

1. *Protect against malware* (DSS05.01)
   Pada langkah ini mengimplementasikan dan menjaga tindakan pencegahan, deteksi dan penyempurnaan (termasuk pembaruan keamanan dan control virus terbaru) diseluruh perusahaan guna memproteksi sistem informasi dan teknologi dari software berbahaya seperti virus, worm, spyware dan spam.
2. *Manage network and connectivity security* (DSS05.02)
   Pada langkah ini melibatkan tata cara keamanan dan tata cara manajemen yang relevan dalam memproteksi informasi dari berbagai metode konektivitas.
3. *Manage endpoint security* (DSS05.03)

Langkah ini menjamin bahwa titik akhir (seperti laptop, desktop, server, perangkat seluler dan jaringan seluler serta perangkat lunak lainnya) terjamin dengan tingkat keamanan sama atau lebih berdasarkan ketentuan yang diatur oleh informasi yang dikelola, diamankan atau dikirimkan

4. *Manage user identity and logical access* (DSS05.04)
   Langkah ini memastikan bahwa semua user mempunyai akses informasi tepat berdasarkan kepentingan bisnis mereka dan mengkoordinasikan pada bagian bisnis yang bertanggung jawab atas manajemen hak akses mereka dalam alur bisnis.
5. *Manage physical access to IT assets* (DSS05.05)
   Langkah tersebut melibatkan penetapan dan implementasi tata cara dalam memberikan, menghambat dan mencabut akses gedung, bangunan dan area tepat dengan kebutuhan bisnis termasuk dalam keadaan mendesak. Setiap akses ke gedung, bangunan dan area harus tersetujui, terverifikasi, tercatat dan terpantau. Kebijakan ini berlaku untuk seluruh individu yang masuk dilokasi tersebut termasuk staff, karyawan sementara, klien, vendor, pengunjung atau pihak ketiga lainnya.
6. *Manage sensitive documents and output devices* (DSS05.06)
   Langkah ini melibatkan pengaturan keamanan fisik, praktik akuntansi dan manajemen persediaan sesuai asset TI yang responsive seperti formulir khusus, instrument yang bisa disepakati, printer khusus atau token keamanan.
7. *Monitor the infrastructure for security-related events* (DSS05.07)
   Langkah ini melibatkan penggunaan alat pendeteksi intrusi untuk memonitor infrastruktur terhadap akses tidak sah, serta menjamin semua kegiatan terintegrasi dalam pantauan dan manajemen peristiwa secara umum.

2.7 *Responsible, Accountable, Consulted, Informed* (RACI) *Chart*

Dalam konteks perusahaan, RACI chart ialah alat yang berguna dalam pengambilan keputusan dan membantu manajemen dalam mengidentifikasi peran dan tanggung jawab karyawan. Pembagian tugas dengan jelas serta definisi peran dan tanggung jawab dapat membuat kebingungan, dan berakhir berkurangnya produktivitas kerja karyawan dalam perusahaan (Nurhuda et al., 2021)

COBIT 2019 menyajikan sebuah RACI chart dengan menggambarkan kegiatan serta tanggung jawab dan berperan penting pada proses pengambilan keputusan di dalam organisasi.

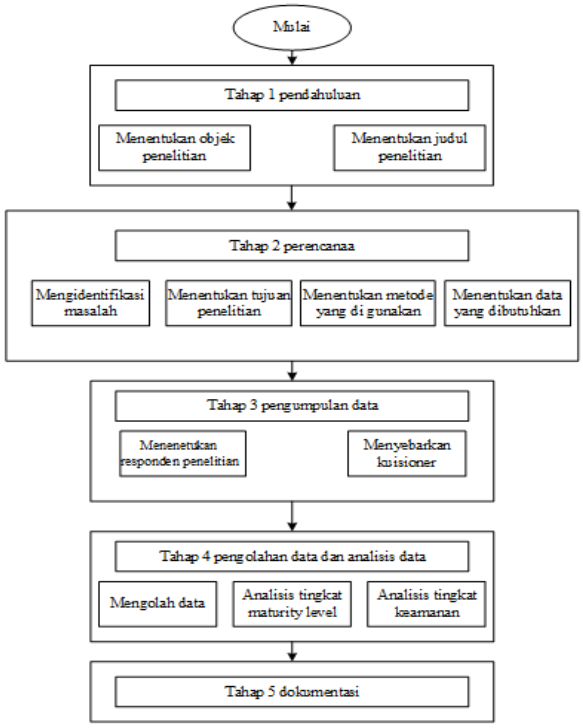
1. Responsible (R): Orang yang memiliki kewenangan untuk melaksanakan pekerjaan.
2. Accountable (A): Orang yang mempunyai otoritas dan kewenangan atas keputusan yang diambil saat ada persoalan pada perusahaan.
3. Consulted (C): Orang yang memberikan masukan mengenai kegiatan perusahaan
4. Informed (I): Orang yang akan memberi informasi atas keputusan yang diambil

2.8 Sistem Sawit Rakyat Online (SRO)

Sistem Sawit Rakyat Online (SRO) merupakan tempat sebagai transaksi jual beli bibit sawit secara online, Selain menjual bibit sawit, sistem ini juga ada fitur lainnya seperti berbagi informasi/berita tentang seputar sawit/bibit sawit khususnya untuk para petani dan masyarakat. Pada sistem Sawit Rakyat Online (SRO) ini dapat membantu petani mendapatkan informasi mengenai perkebunan kelapa sawit dengan lebih mudah, antara lain:

- Beli bibit Unggul N5
- Informasi tentang program kelapa sawit yang populer
- Testimoni pembelian benih N5 premium
- dan masih banyak lagi

3. Metodologi Penelitian



Gambar 1. Metodologi Penelitian

Pada gambar 1 dijelaskan alur penelitian ini dimulai dari tahapan pendahuluan dengan menentukan objek penelitian dan menentukan judul penelitian. Selanjutnya proses tahap perencanaan yang mencangkup pengidentifikasian masalah, penentuan tujuan penelitian, pemilihan metode yang digunakan, serta penentuan data yang diperlukan. Tahapan selanjutnya pengumpulan data dengan menentukan responden penelitian dan menyebarkan kuisioner. Kemudian tahap pemrosesan data dan analisis data dengan mengolah data, analisis tingkat *maturity level* dan, analisis tingkat keamanan.

3.1 Pengumpulan Data

Tahap pengumpulan data, terlebih dahulu menentukan jenis data yang diperlukan untuk penelitian ini. Penelitian ini dilakukan setelah melakukan observasi langsung dan studi literatur untuk menentukan kebutuhan data. Penelitian ini menggunakan data primer.

Data primer adalah data yang berasal dari wawancara langsung dari narasumber yang tepat dan terpercaya dan menyebarkan kuisioner kepada pengguna sistem SRO. Dari hasil penyebaran kuesioner ini nantinya dapat menghasil penilaian pengguna tentang sistem SRO, kemudian hasil tersebut bisa jadi acuan untuk menentukan pengukuran tingkat kematangan dan tingkat keamanan sistem SRO.

3.2 Menentukan Responden Penelitian

Dalam penelitian ini, responden diidentifikasi berdasarkan RACI (*Responsible, Accountable, Consukted, and Informed*) Chart dalam Framework COBIT 19 yang sesuai dengan struktur organisasi PT. Perkebunan Nusantara V (PTPN V). Peneliti melakukan pemetaan RACI untuk mengidentifikasi pihak-pihak yang bertanggung jawab dalam mengelola keamanan sistem informasi Sawit Rakyat Online (SRO) di PTPN V dan siapa saja nantinya yang akan menerima kuisioner yang telah di tentukan berdasarkan RACI *Chart*. Berikut adalah responden pada masing-masing bidang yang dipilih, seperti yang ditunjukan Tabel 2.

Tabel 2. Responden Penelitian

NO	Jabatan	Deskripsi
1	Kepala Bagian Pengadaan, Logistik dan Pemasaran	*Chief Information Officer* adalah posisi senior di perusahaan yang mempunyai kewenangan atas penyelarasan TI dengan taktik bisnis dalam perancangan, alokasi sumber daya, dan tata kelola pengirim layanan serta solusi guna mendukung target TI perusahaan.
2	Tim Pengadaan 1 & 2	*Bussiness Process Owners* adalah seorang yang memiliki kewenangan atas hasil dari proses bisnis.
3	Ka. Su. Bag. Logistik & Pemasaran	*Privacy Officer* adalah seorang yang mempunyai kewenangan mengamati resiko dan dampak bisnis dari undang-undang privasi serta koordinasi pelaksana kebijakan dan kegiatan yang memastikan arahan privasi telah tercapai.
4	Kepala Bagian Perencanaan, Sustainability, & Teknologi Informasi	*Chief Information Security Officer* adalah kelompok eksekutif senior perusahaan yang mempunyai kewenangan terkait keamanan informasi perusahaan dari segala aspek.

NO	Jabatan	Deskripsi
5	Ka. Sub. Bag. Pengkajian, Perencanaan & Korporasi & Manajemen Kinerja	*Head IT Operations* adalah seorang senior yang bertugas mengenai lingkungan dan infrastruktur operasional TI.
6	Ka. Sub. Bag. Teknologi Informasi	*Information Security Manager* adalah seseorang yang berkewenangan menangani, merancang, memantau dan mengevaluasi keamanan informasi dalam perusahaan
7	GM Petani Mitra	*Head Development* adalah seorang senior yang memiliki kewenangan atas tahapan TI dan tahapan pengembangan solusi.

3.3 Penyebaran Kuisioner

Tahap penyebaran Kuisioner kepada responden yang merupakan pengguna sistem informasi, termasuk staff IT, dan pengguna IT, serta responden yang sudah ditentukan berdasarkan pemetaan RACI *Chart*. Kuisioner pada penelitian ini dibuat untuk mengevaluasi tingkat kematangan tata kelola teknologi dan informasi yang di implementasikan dengan mengumpulkan respon dari pengguna dan pembuat putusan mengenai penggunaan teknologi.

4. Hasil dan Pembahasan

4.1 Analisis Tingkat Kematangan (*Maturity Level*)

Berdasarkan perhitungan secara keseluruhan tingkat kematangan untuk domain DSS05 (*managed security services*) yang didalamnya terdapat 7 subdomain proses COBIT 2019 yang akan digunakan dalam pengukuran tingkat kematangan. Hasil dari jawaban kuisioner akan di hitung penilaian tingkat kematangan setiap domain prosessnya. Berikut ini adalah tabel tingkat kematangan (*Maturity level).*

Tabel 3. Hasil Pengukuran Tingkat Kematangan Semua Proses TI pada Domain DSS05 (*managed security services*)

Control Proses TI	Rata-Rata Proses TI	Tingkat *Maturity Level*
DSS05.01 (*Protect against malware*)	4.57	Mengoptimalkan proses
DS005.02 (*Manage network and connectivity security*)	4.6	Mengoptimalkan proses
DS005.03 (*Manage endpoint security*)	4.17	Proses yang dapat diprediksi
DS005.04 (*Manage user identity and logical access*)	4.22	Proses yang dapat diprediksi
DS005.05 (*Manage physical access to IT assets*)	4.62	Mengoptimalkan proses
DS005.06 (*Manage sensitive documents and output devices*)	3.74	Proses yang dapat diprediksi
DS005.07 (*Monitor the infrastructure for security-related events*)	4.42	Proses yang dapat diprediksi

Berdasarkan Tabel 3 di atas hasil rekapitulasi jawaban kuesioner di setiap proses domain DSS05 dapat disimpulkan bahwa nilai DSS05.01 dengan presentase 4.57 berada pada tingkat "mengoptimalkan proses". Teknologi informasi yang telah terintegrasi dapat mengotomatisasi proses kerja di perusahaan, selain itu kemampuan beradaptasi dapat meningkatkan kualitas dan efektivitas pada suatu perusahaan. Selanjutnya nilai DSS05.02 sebesar 4.6 menunjukkan bahwa proses tersebut telah mencapai tingkat "mengoptimalkan proses".

Selanjutnya DSS05.03 dengan presentase 4.17 berada pada tingkat "proses yang dapat diprediksi". Proyek mengendalikan produk dan teknik untuk meminimalkan variasi kinerja proses sehingga batasan bisa diterima. Selanjutnya DSS05.04 dengan presentase 4.22 berada pada tingkat "proses yang dapat diprediksi". Proyek mengendalikan produk dan teknik untuk meminimalkan variasi kinerja proses sehingga batasan bisa diterima Selanjutnya DSS05.05 dengan presentase 4.62 berada pada tingkat "mengoptimalkan Proses". Teknologi Informasi yang telah terintegrasi dapat mengotomatisasi proses kerja di perusahaan, selain itu kemampuan beradaptasi dapat meningkatkan kualitas dan efektivitas pada suatu perusahaan. Kemudian DSS05.06 dengan presentase 3.74 berada pada tingkat "proses yang dapat diprediksi". Proyek mengendalikan produk dan teknik untuk meminimalkan variasi kinerja proses sehingga batasan bisa diterima. Dan yang terakhir DSS05.07 dengan presentase 4.42 berada pada tingkat "proses

yang dapat diprediksi". Proyek mengendalikan produk dan teknik untuk meminimalkan variasi kinerja proses sehingga batasan bisa diterima.

4.2 Analisis Tingkat Keamanan

Selanjutnya tingkat keamanan dapat ditentukan berdasarkan hasil perhitungan tingkat *maturity level* keseluruhan aktivitas yang disebutkan sebelumnya.

Berikut adalah perhitungan tingkat keamanan yang dilakukan dalam DSS05 sebagai berikut:

$$\textit{Maturity Level}\ \text{DSS05} = \frac{Maturity\ Level}{Banyak\ Proses}$$
$$= \frac{4.57+4.6+4.17+4.22+4.62+3.74+4.42}{7} = 4.33$$

Jadi hasil dari penilaian secara keseluruhan di atas menghasilkan skor 4.33 ini menunjukkan tingkat keamanan berada pada level 4 yaitu *Quantitative*. Yang mana Level ini berarti institusi telah melaksanakan proses yang telah ditetapkan dan semua tim memahami bagaimana proses seharusnya berlangsung. Menggunakan ketentuan organisasi dan menyesuaikannya dengan karakteristik proyek dan pekerjaan dengan fokus mencapai target proyek dan meningkatkan kinerja organisasi.

5. Kesimpulan

Bedasarkan hasil penelitian ini, dapat disimpulkan bahwa:

1. Analisis keamanan sistem informasi Sawit Rakyat Online (SRO) pada PT Perkebunan Nusantara V (PTPN V) telah memenuhi standar keamanan yang telah diukur menggunakan kerangka kerja sub domain DSS05 pada *framework* COBIT 2019. Keamanan sistem informasi pada level ini telah memadai, akan tetapi masih memerlukan inovasi dan pengembangan agar dapat responsive, cepat dan efektif dalam menghadapi ancaman keamanan. Berdasarkan evaluasi terhadap kerangka kerja COBIT 2019, ditemukan bahwa beberapa area perlu diperbaiki untuk meningkatkan keamanan sistem. Rekomendasi yang diberikan termasuk implementasi proses otomatisasi untuk monitoring keamanan secara terus-menerus, penguatan kebijakan akses dan manajemen identitas, serta peningkatan dalam pemantauan dan respons terhadap ancaman keamanan secara proaktif.
2. Berdasarkan hasil analisis tingkat kematangan menggunakan *framework* COBIT 2019 dengan *maturity level* pada sistem informasi Sawit rakyat Online (SRO) PT Perkebunan Nusantara V (PTPN V) telah diukur berdasarkan sub domain DSS05 sub domain DSS05.01 dengan hasil indeks 4,57 menunjukkan pada level 5 yaitu *Optimizing*, DSS05.02 dengan hasil indeks 4,6 menunjukkan pada level 5 yaitu *Optimizing*, DSS05.03 dengan hasil indeks 4,17 menunjukkan pada level 4 yaitu *Quantitative*, DSS05.04 dengan hasil indeks 4,22 menunjukkan pada level 4 yaitu *Quantitative* DSS05.05 dengan hasil indeks 4,62 menunjukkan pada level 5 yaitu *Optimizing*, DSS05.06 dengan hasil indeks 3,74 menunjukkan pada level 4 yaitu *Quantitative*, dan DSS05.07 dengan hasil indeks 4,42 menunjukkan pada level 4 yaitu *Quantitative*.
3. Berdasarkan hasil analisis tingkat keamanan yang di dapat berdasarkan dengan tingkatan *maturity level* semua aktifitas yang dikerjakan DSS05 dengan hasil 4,33 menunjukkan tingkat keamanan berada pada *Quantitative*. Pada tingkat ini institusi telah melaksanakan proses-proses yang telah ditetapkan dan semua tim telah memahami bagaimana proses tersebut seharusnya berlangsung. Menggunakan ketentuan organisasi dan menyesuaikannya dengan karakteristik proyek dan pekerjaan dengan fokus mencapai rujuan proyek dan kinerja organisasi.

References

Akraman, R., Candiwan, C., & Priyadi, Y. (2018). Pengukuran Kesadaran Keamanan Informasi Dan Privasi Pada Pengguna Smartphone Android Di Indonesia. *Jurnal Sistem Informasi Bisnis*, *8*(2), 115. https://doi.org/10.21456/vol8iss2pp115-122

Azizah, N. (2017). Audit Sistem Informasi Menggunakan Framework Cobit 4.1 Pada E-Learning Unisnu Jepara. *Simetris: Jurnal Teknik Mesin, Elektro Dan Ilmu Komputer*, *8*(1), 377–382. https://doi.org/10.24176/simet.v8i1.1024

Baharuddin, A. F., Suprapto, & Perdanakusuma, A. R. (2019). Evaluasi Tata Kelola Teknologi Informasi Menggunakan Framework COBIT 5 Domain DSS (Deliver , Service , Support) (

Studi Kasus : PT . PLN (Persero) Kantor Pusat). *Jurnal Teknoinfo*, *3*(9), 8866–8873.

Dharma, I. G. M., Sasmita, G. M., & Putra, I. M. (2021). Evaluasi Dan Implementasi Tata Kelola TI Menggunakan COBIT 2019 (Studi Kasus Pada Dinas Kependudukan Dan Pencatatan Sipil Kabupaten Tabanan). *JITTER : Jurnal Ilmiah Teknologi Dan Komputer*, *2*(2), 354–365.

ISACA. (2019). COBIT 2019 Framework - Introduction and Methodology. In *www.icasa.org/COBITuse*.

ISACA Governance and Manajement. (2019). *COBIT 2019 Governance and Management Objectives (ISACA)*.

Muttaqin, F., Idhom, M., Akbar, F. A., Swari, M. H. P., & Putri, E. D. (2020). Measurement of the IT Helpdesk Capability Level Using the COBIT 5 Framework. *Journal of Physics: Conference Series*, *1569*(2), 39–46. https://doi.org/10.1088/1742-6596/1569/2/022039

Nachrowi, E., Nurhadryani, Y., & Sukoco, H. (2020). Evaluation of Governance and Management of Information Technology Services Using Cobit 2019 and ITIL 4. *Jurnal RESTI (Rekayasa Sistem Dan Teknologi Informasi)*, *4*(4), 764–774. https://doi.org/10.29207/resti.v4i4.2265

Natanael, T., Santoso, L. W., & Noertjahyana, A. (2018). Analisa Keamanan Sistem Informasi RSUD Dr . Soetomo Dengan Framework COBIT. *Jurnal INFRA*, *6*(2), 1–4.

Nurhuda, A. M., Philipus, E., & Gunawan, I. (2021). Audit Sistem Pendataan Keluarga Menggunakan Pendekatan Framework COBIT 5 Pada Domain DSS (Studi Kasus: BKKBN Propinsi Jawa Barat). *Teknika*, *10*(1), 78–87. https://doi.org/10.34148/teknika.v10i1.324

Nurul, S., Shynta Anggrainy, & Siska Aprelyani. (2022). Faktor-Faktor Yang Mempengaruhi Keamanan Sistem Informasi: Keamanan Informasi, Teknologi Informasi Dan Network (Literature Review Sim). *Jurnal Ekonomi Manajemen Sistem Informasi*, *3*(5), 564–573. https://doi.org/10.31933/jemsi.v3i5.992

Ria, M. D., & Budiman, A. (2021). *Perancangan sistem informasi tata kelola teknologi informasi perpustakaan*. *2*(1), 122–133.

Setiawan, R. A., & Wasilah, W. (2022). Evaluasi Tata Kelola Dan Manajemen Teknologi Informasi Menggunakan Framework Cobit 2019 Pada Dinas Komunikasi Dan Informatika Kabupaten Lampung …. *Prosiding Seminar Nasional …*, 8–15.

Umar, R., Riadi, I., & Handoyo, E. (2020). Manage Security Services (Dss05) Dan Nist Sp 800-55. *Tahun*, *10*(1), 2087–4685.

Windasari, I. P., Rochim, A. F., Alfiani, S. N., & Kamalia, A. (2022). Audit Tata Kelola Teknologi Informasi Domain Monitor, Evaluate, and Asses dan Deliver, Service, Support Berdasarkan Framework COBIT 2019. *J. Sistem Info. Bisnis*, *11*(2), 131–138. https://doi.org/10.21456/vol11iss2pp131-138