Abdi Jurnal Publikasi **ISSN : 2963-3486**
Vol. 1, No. 6, Juni 2023 (519-524)

SISTEM MANAJEMEN SEKURITI PADA PT TELKOM INDONESIA

Edy Soesanto[1], Kefas Kristian Telaumbanua[2], Muhammad Dzaky[3], Fransisca Nada Sherenika[4]

[1]Program Studi Teknik Perminyakan, Universitas Bhayangkara Jakarta Raya
e-mail: [1]*edy.soesanto@dsn.ubharajaya.ac.id*

[2,3,]4Ekonomi & Bisnis/Manajemen, Universitas Bhayangkara Jakarta Raya
e-mail: [2]*202010325205@mhs.ubharajaya.ac.id,* [3]*202010325162@mhs.ubharaja.ac.id,*
[4]*fransisca.nada.sherenika18@mhs.ubharajaya.ac.id*

Abstract

This journal aims to investigate the security management system implemented at PT Telkom Indonesia. Research was conducted with the aim of analyzing and implementing effective security measures to protect company systems, data and infrastructure. This study involves an in-depth analysis of relevant security aspects, including risk identification, vulnerability assessment, identity and access management, security monitoring, and response to security incidents. The methodology used is the literature review. The research results show that PT Telkom Indonesia has implemented various significant security measures to protect the company's systems and information. They have strong policies on identity and access management, as well as sophisticated monitoring systems to detect attacks and suspicious activity. The response to security incidents has also been strengthened through detailed disaster recovery plans.

Keywords: Security Management System; PT. Telcom Indonesia

Abstrak

Jurnal ini bertujuan untuk menyelidiki sistem manajemen keamanan yang diterapkan di PT Telkom Indonesia. Penelitian dilakukan dengan tujuan untuk menganalisis dan mengimplementasikan langkah-langkah keamanan yang efektif guna melindungi sistem, data, dan infrastruktur perusahaan. Studi ini melibatkan analisis mendalam terhadap aspek keamanan yang relevan, termasuk identifikasi risiko, penilaian kerentanan, pengelolaan identitas dan akses, pemantauan keamanan, dan respons terhadap insiden keamanan. Metodologi yang digunakan literatur review. Hasil penelitian menunjukkan bahwa PT Telkom Indonesia telah menerapkan berbagai langkah keamanan yang signifikan untuk melindungi sistem dan informasi perusahaan. Mereka memiliki kebijakan yang kuat dalam pengelolaan identitas dan akses, serta sistem pemantauan yang canggih untuk mendeteksi serangan dan aktivitas mencurigakan. Respons terhadap insiden keamanan juga telah diperkuat melalui rencana pemulihan bencana yang terperinci.

Kata Kunci: Sistem Manajemen Sekuriti; PT. Telkom Indonesia

1. PENDAHULUAN

PT Telkom Indonesia adalah perusahaan telekomunikasi terkemuka di Indonesia. Didirikan pada tahun 1856, perusahaan ini merupakan Badan Usaha Milik Negara (BUMN) yang bergerak dalam penyediaan layanan telekomunikasi dan informasi di Indonesia. PT Telkom Indonesia memiliki visi untuk menjadi perusahaan telekomunikasi terdepan di dunia yang memberikan kontribusi signifikan bagi kemajuan bangsa [1].

Sebagai perusahaan telekomunikasi terbesar di Indonesia, PT Telkom Indonesia menyediakan berbagai layanan yang mencakup telepon tetap, telepon seluler, internet, televisi kabel, dan jasa komunikasi data kepada pelanggan perorangan, bisnis, dan lembaga pemerintah. Perusahaan ini juga menyediakan layanan lain seperti telepon internasional, layanan cloud computing, solusi IT, dan integrasi sistem [2].

PT Telkom Indonesia memiliki jaringan telekomunikasi yang luas dan canggih, termasuk infrastruktur serat optik dan jaringan seluler yang tersebar di seluruh Indonesia. Jaringan ini memungkinkan PT Telkom Indonesia untuk memberikan konektivitas yang handal dan

berkualitas tinggi kepada pelanggan di berbagai wilayah di Indonesia.

Selain itu, PT Telkom Indonesia juga berkomitmen untuk mengembangkan inovasi teknologi dan layanan yang relevan dengan perkembangan terkini. Perusahaan ini aktif dalam upaya penelitian dan pengembangan teknologi telekomunikasi, serta berinvestasi dalam pengembangan sumber daya manusia yang kompeten untuk menghadapi tantangan masa depan [3].

Sebagai BUMN, PT Telkom Indonesia juga berperan dalam mendukung pembangunan nasional dan inklusi digital di Indonesia. Perusahaan ini turut berpartisipasi dalam program pemerintah untuk meningkatkan konektivitas di daerah terpencil dan meningkatkan akses pendidikan dan pelayanan kesehatan melalui teknologi informasi dan telekomunikasi.

Dengan komitmen terhadap kualitas layanan, inovasi, dan kontribusi sosial, PT Telkom Indonesia terus menjaga posisinya sebagai pemimpin industri telekomunikasi di Indonesia dan berperan dalam mendorong transformasi digital dan kemajuan bangsa [4].

Keamanan dan keberlanjutan operasional merupakan aspek krusial dalam lingkungan bisnis yang semakin terhubung dan tergantung pada teknologi informasi. PT Telkom Indonesia, sebagai perusahaan telekomunikasi terkemuka di Indonesia, mengakui pentingnya manajemen keamanan atau keamanan sistem dalam menjaga integritas, kerahasiaan, dan ketersediaan informasi yang dikelola serta melindungi infrastruktur dan layanan yang ditawarkan.

Dalam era digital yang terus berkembang, PT Telkom Indonesia berperan penting dalam memenuhi kebutuhan komunikasi dan konektivitas pelanggan, baik dalam konteks bisnis maupun individu. Seiring dengan kemajuan teknologi, tantangan terkait keamanan dan perlindungan informasi semakin kompleks dan beragam. Ancaman serangan siber, penyalahgunaan data, dan gangguan layanan menjadi ancaman yang nyata dan berdampak luas dalam industri telekomunikasi.

Manajemen sekuriti atau keamanan sistem yang kuat adalah suatu keharusan bagi PT Telkom Indonesia. Tindakan yang proaktif dan holistik dalam mengelola risiko keamanan memastikan keandalan layanan, perlindungan data pelanggan, dan pematuhan terhadap regulasi yang berlaku. Dengan mengutamakan keamanan, PT Telkom Indonesia dapat membangun kepercayaan pelanggan, meminimalkan risiko serangan siber, dan menjaga reputasi sebagai penyedia jasa telekomunikasi yang andal.

Penelitian ini bertujuan untuk menyelidiki dan menganalisis sistem manajemen sekuriti yang diterapkan di PT Telkom Indonesia. Penelitian ini bertujuan untuk mengeksplorasi strategi, kebijakan, dan praktik terkait manajemen sekuriti yang digunakan oleh perusahaan. Dalam penelitian ini, kami akan menyoroti langkah-langkah yang diambil oleh PT Telkom Indonesia untuk melindungi aset informasi, mencegah serangan siber, dan memitigasi risiko keamanan yang dihadapi [5].

Dengan pemahaman yang lebih mendalam tentang manajemen sekuriti di PT Telkom Indonesia, diharapkan penelitian ini dapat memberikan wawasan yang berharga dalam menghadapi tantangan keamanan yang kompleks dan membantu perusahaan dalam meningkatkan keunggulan kompetitif dan keberlanjutan bisnisnya.

2. METODE

Penelitian ini menggunakan metode deskriptif dengan pendekatan kualitatif dengan berupa tinjauan Pustaka. Metode ini dilakukan berdasarkan sumber informasi yang relevan dengan topik penelitian. Sumber informasi ini berupa artikel jurnal, buku, laporan riset ataupun studi kasus yang memaparkan tentang sistem manajemen sekuriti di PT Telkom Indonesia [6].

3. PEMBAHASAN

Proteksi Sistem Manajemen Sekuriti PT Telkom Indonesia

PT Telkom Indonesia memiliki pendekatan yang komprehensif dalam melindungi keamanan sistem dan informasi. Berikut adalah beberapa langkah dan praktik yang dilakukan oleh PT Telkom Indonesia dalam proteksi manajemen keamanan:

a. Kebijakan dan Prosedur Keamanan
   PT Telkom Indonesia memiliki kebijakan dan prosedur yang jelas terkait keamanan sistem dan informasi. Ini mencakup pedoman untuk penggunaan yang aman, pengelolaan akses, kebijakan sandi yang kuat, dan tindakan keamanan lainnya.
b. Pengelolaan Identitas dan Akses
   PT Telkom Indonesia menerapkan sistem manajemen identitas dan akses yang ketat untuk memastikan bahwa hanya pengguna yang sah yang memiliki akses yang tepat ke sistem dan data yang sensitif. Ini termasuk penggunaan

autentikasi ganda, manajemen peran, dan pemeriksaan otorisasi.

c. Keamanan Jaringan
PT Telkom Indonesia menggunakan langkah-langkah keamanan jaringan yang canggih, seperti firewall, sistem deteksi intrusi, dan enkripsi data. Ini membantu melindungi jaringan perusahaan dari serangan siber dan upaya tidak sah lainnya.

d. Pemantauan Keamanan
PT Telkom Indonesia melakukan pemantauan keamanan secara terus-menerus untuk mendeteksi ancaman atau serangan potensial. Sistem pemantauan keamanan diterapkan untuk memonitor aktivitas jaringan, deteksi intrusi, dan peringatan dini terhadap potensi ancaman.

e. Pelatihan dan Kesadaran Keamanan
PT Telkom Indonesia menyadari pentingnya pelatihan dan kesadaran keamanan bagi karyawan. Pelatihan rutin diberikan untuk meningkatkan pemahaman tentang praktik keamanan yang baik, mengenali serangan siber, dan melaporkan insiden keamanan dengan cepat.

f. Pemulihan Bencana dan Manajemen Kejadian Keamanan
PT Telkom Indonesia memiliki rencana pemulihan bencana dan manajemen kejadian keamanan yang dirancang untuk menghadapi insiden keamanan atau bencana alam. Hal ini termasuk cadangan data, pemulihan sistem, dan respons yang terorganisir dalam situasi darurat.

g. Kepatuhan dan Audit
PT Telkom Indonesia memastikan kepatuhan terhadap regulasi keamanan dan standar industri yang berlaku. Audit keamanan dilakukan secara berkala untuk memverifikasi keefektifan langkah-langkah keamanan yang diimplementasikan dan mengidentifikasi area yang memerlukan perbaikan.

PT Telkom Indonesia terus berinovasi dan mengikuti perkembangan teknologi dan tren keamanan terkini untuk memastikan sistem dan informasi mereka tetap aman. Perusahaan ini memiliki tim keamanan yang berdedikasi untuk mengidentifikasi ancaman baru dan mengembangkan solusi keamanan yang lebih baik sesuai dengan perubahan lingkungan keamanan yang cepat.

Antisipasi Sistem Manajemen Sekuriti PT Telkom Indonesia

PT Telkom Indonesia mengadopsi berbagai tindakan antisipatif dalam manajemen sekuriti untuk melindungi sistem dan informasi perusahaan. Berikut adalah langkah-langkah antisipasi yang dilakukan oleh PT Telkom Indonesia:

a. Analisis Risiko
PT Telkom Indonesia melakukan analisis risiko secara teratur untuk mengidentifikasi potensi ancaman dan kerentanan dalam infrastruktur dan sistem mereka. Ini membantu dalam merencanakan tindakan pencegahan yang tepat dan mengalokasikan sumber daya dengan bijaksana.

b. Patching dan Pembaharuan Sistem
PT Telkom Indonesia secara teratur memperbarui dan memperbaiki kerentanan yang diketahui melalui penerapan patch keamanan dan pembaruan sistem. Hal ini penting untuk menjaga sistem mereka tetap aman dari serangan yang memanfaatkan kerentanan yang diketahui.

c. Manajemen Rentang Kontrol
PT Telkom Indonesia menerapkan prinsip manajemen rentang kontrol yang melibatkan penerapan langkah-langkah keamanan di seluruh rantai pasokan dan ekosistem perusahaan. Ini mencakup pemilihan vendor yang aman, pemantauan keamanan pihak ketiga, dan kerjasama dengan mitra untuk memastikan keamanan end-to-end.

d. Deteksi Dini dan Respon Cepat
PT Telkom Indonesia memiliki sistem pemantauan dan deteksi dini yang kuat untuk mendeteksi aktivitas mencurigakan, serangan siber, atau pelanggaran keamanan lainnya. Mereka juga memiliki tim respons keamanan yang siap untuk merespons insiden dengan cepat dan efektif.

e. Pelatihan Keamanan
PT Telkom Indonesia memberikan pelatihan keamanan yang berkala kepada karyawan mereka untuk meningkatkan kesadaran keamanan dan membekali mereka dengan pengetahuan dan keterampilan yang diperlukan untuk menghadapi ancaman keamanan. Hal ini membantu mencegah serangan melalui tindakan manusia yang tidak sengaja atau kelalaian.

f. Uji Penetrasi dan Audit Keamanan
PT Telkom Indonesia melakukan uji penetrasi secara berkala untuk menguji kekuatan dan kerentanan sistem mereka. Audit keamanan juga dilakukan untuk memverifikasi kepatuhan terhadap standar keamanan dan mengidentifikasi area yang perlu diperbaiki.

g. Keamanan Fisik dan Keamanan Data
PT Telkom Indonesia memastikan perlindungan keamanan fisik terhadap pusat data mereka, termasuk pengawasan akses fisik, pengamanan

perangkat keras, dan pemantauan lingkungan. Mereka juga menerapkan kebijakan dan teknologi yang tepat untuk melindungi integritas, kerahasiaan, dan ketersediaan data mereka.

Dengan mengadopsi langkah-langkah antisipatif ini, PT Telkom Indonesia dapat mengurangi risiko keamanan dan meningkatkan kemampuan mereka dalam melindungi sistem dan informasi dari ancaman yang mungkin timbul. Perusahaan ini selalu berupaya untuk mengikuti perkembangan terbaru dalam keamanan informasi dan teknologi guna menjaga tingkat keamanan yang tinggi [7].

Assesment Manajemen Sekuriti PT Telkom Indonesia

Dalam konteks menilai sistem keamanannya PT Telkom melakukan tindakan sebagai berikut:

a. Identifikasi Aktiva dan Ancaman
   Identifikasi semua aktiva informasi yang dimiliki oleh PT Telkom Indonesia, termasuk sistem, infrastruktur, dan data sensitif. Kemudian, identifikasi berbagai ancaman yang dapat mempengaruhi keamanan aktiva tersebut, seperti serangan siber, kegagalan perangkat keras, atau bencana alam.
b. Penilaian Resiko
   Melakukan penilaian risiko untuk mengidentifikasi kerentanan, ancaman, dan dampak potensial terhadap aktiva yang dimiliki. Evaluasi risiko membantu dalam menentukan prioritas dan langkah-langkah yang perlu diambil untuk mengurangi risiko yang ada.
c. Kebijakan dan Prosedur
   Melakukan peninjauan dan evaluasi kebijakan dan prosedur yang ada terkait keamanan. Memastikan bahwa kebijakan dan prosedur tersebut relevan, efektif, dan sesuai dengan standar keamanan yang berlaku.
d. Pengujian Keamanan
   Melakukan pengujian keamanan secara menyeluruh, termasuk uji penetrasi dan simulasi serangan untuk mengidentifikasi kerentanan yang mungkin ada dalam sistem dan infrastruktur. Hasil dari pengujian ini memberikan wawasan tentang kerentanan yang perlu diperbaiki.
e. Manajemen Identitas dan Akses
   Melakukan penilaian terhadap sistem manajemen identitas dan akses yang diterapkan. Memastikan bahwa kontrol akses yang memadai telah diterapkan, dan hanya pengguna yang sah yang memiliki akses yang tepat ke sistem dan data sensitif.
f. Pemantauan dan Deteksi
   Menilai sistem pemantauan dan deteksi yang digunakan untuk mendeteksi aktivitas yang mencurigakan atau serangan potensial. Memastikan bahwa sistem pemantauan yang memadai telah diterapkan untuk mendapatkan visibilitas terhadap ancaman keamanan.
g. Respons dan Pemulihan
   Menilai rencana respons keamanan dan pemulihan bencana yang ada. Memastikan bahwa rencana respons yang tepat telah dirancang dan dapat diimplementasikan dengan efektif dalam menghadapi insiden keamanan atau bencana.

Perlu diketahui penilaian sistem manajemen keamanan yang komprehensif biasanya melibatkan tim keamanan yang berpengalaman dan ahli dalam bidang keamanan informasi.

Risk Assesment Sistem Manajemen Sekuriti PT Telkom Indonesia

PT Telkom menghadapi banyak risiko kritis dalam kegiatan operasionalnya, baik internal maupun eksternal. Masalah ini karena PT Telkom merupakan perseroan terbatas yang berkedudukan di Indonesia, dimana sebagian besar operasi, aset dan pelanggannya berada di Indonesia. Akibatnya, kondisi politik, ekonomi, hukum, dan sosial Indonesia akan berubah di masa depan dan tindakan dan kebijakan tertentu yang diambil atau tidak diambil oleh pemerintah dapat berdampak negatif secara material terhadap bisnis, kondisi keuangan, dan hasil operasi dari PT Telkom.

Menurut PT Telkom, risiko operasional berarti risiko yang terkandung di dalamnya berhubungan langsung atau tidak langsung dengan operasi perusahaan sehari-hari hasil langsung dari proses internal yang tidak memadai atau rusak, orang dan sistem, atau Kejadian di luar kendali perusahaan, termasuk bencana alam. Risiko operasional ini termasuk misalnya:

a. Risiko Bisnis *(Business Risk)*
   yang meliputi adanya perubahan terhadap pangsa pasar perusahaan, konsumen atau produk, perubahan pada lingkungan ekonomi dan politik di mana perusahaan beroperasi seperti antara lain meliputi risiko kepuasan pelanggan *(customer satisfaction risk)*, pengadaan *(procurement risk)*, risiko pengembangan produk *(product development risk)*, risiko penurunan merek *(brand erosion)*, risiko perencanaan kapasitas bisnis *(business/capacity planning risk)*, dan risiko gangguan bisnis *(business interuption risk)* dan

risiko strategis *(strategic risk)* yang harus dihadapi perusahaan apabila rencana bisnis, sistem pendukung dan implementasinya akan mempengaruhi perusahaan, seperti antara lain meliputi risiko kompetisi *(competition risk)*, risiko regulasi/hukum/kebijakan internal *(regulation/legal/internal policy risk)*, risiko ketersediaan modal *(capital availability risk)*, risiko inovasi teknologi *(technological innovation risk)*, dan risiko tata kelola perusahaan *(corporate governance risk)*.

b. Risiko Kejahatan (*Crime Risk)*
Yang meliputi pencurian, fraud dan pembajakan komputer *(computer hacking).*

c. Risiko Bencana *(Disaster Risk)*
Baik yang terjadi secara alami (gempa bumi, tsunami, dll) maupun yang terjadi akibat ulah manusia (banjir, kebakaran, dll), serta adanya aktivitas terorisme.

d. Risiko Teknologi Information *(Information Technology Risk)*
Meliputi adanya kebocoran data dan informasi, dan adanya akses ke perusahaan yang tidak diinginkan seperti antara lain meliputi risiko infrastruktur jaringan/IT *(IT/Network Infrastructure risk)* dan risiko integrasi informasi *(information integrity risk).*

e. Risiko Hukum *(Legal Risk)*
Meliputi peningkatan kerugian akibat adanya perubahan pada tindakan hukum yang tidak tepat dan adanya praktek dan dokumen hukum yang tidak terdeteksi.

f. Risiko Regulasi *(Regulatory Risk)*
Meliputi kurangnya perhatian terhadap peraturan yang telah ditetapkan.

g. Risiko Reputasi *(Reputational Risk)*
Timbul dari akibat adanya publikasi negatif terhadap kegiatan bisnis dan pengendalian intern yang dilakukan.

h. Risiko Sistem *(System Risk)*
Berupa kehilangan yang terjadi akibat dari adanya kegagalan oleh penghentian prosedur, proses atau sistem dan kontrol bisnis.

i. Risiko Kerjasama *(Partnering Risk)*
Meliputi aliansi, joint venture, afiliasi dan bentuk kerja sama lainnya dengan pihak ketiga yang tidak efektif atau tidak efisien dapat mempengaruhi kemampuan perusahaan dalam berkompetisi, ketidakpastian ini terjadi karena kesalahan dalam pemilihan mitra kerjasama, kesalahan dalam eksekusi, mengambil keuntungan yang berlebihan menyebabkan kehilangan mitra kerjasama.

j. Risiko Sumber Daya Manusia/Kepemimpinan *(Human Resource/Leadership Risk)*
Meliputi risiko tidak dapat untuk merekrut, mempertahankan dan mengelola sumber daya manusia perusahaan, termasuk didalamnya risiko tidak adanya komunikasi yang baik, kepemimpinan dan memotivasi karyawan sehingga menyebabkan kegagalan untuk memaksimalkan dan mempertahankan produktivitas dan efisiensi organisasi dan perusahaan.

k. Risiko Interkoneksi *(Inter-Carrier Risk)*
Terjadi akibat operasi yang tidak efisien dan efektif dalam melakukan kerjasama dengan operator lokal atau interlokal yang mengakibatkan buruknya penyediaan jasa komunikasi end-to-end untuk traffic atau jalur tertentu.

4. KESIMPULAN

Berdasarkan uraian hasil dan pembahasan di atas, penulis menyimpulkan bahwa:

a. PT Telkom Indonesia memiliki pendekatan yang komprehensif dalam melindungi sistem dan informasi perusahaan mereka. Mereka mengadopsi kebijakan, prosedur, dan praktik keamanan yang didukung oleh teknologi canggih untuk memastikan keamanan yang optimal.

b. PT Telkom Indonesia mengakui pentingnya manajemen keamanan dalam menjaga integritas, kerahasiaan, dan ketersediaan sistem dan informasi mereka. Mereka secara teratur melakukan analisis risiko, mengidentifikasi ancaman potensial, dan mengambil langkah-langkah yang diperlukan untuk mengurangi risiko yang ada.

c. PT Telkom Indonesia menerapkan pengelolaan identitas dan akses yang ketat, dengan memastikan bahwa hanya pengguna yang sah yang memiliki akses yang tepat ke sistem dan data sensitif. Mereka juga menggunakan langkah-langkah keamanan jaringan, seperti firewall, sistem deteksi intrusi, dan enkripsi data, untuk melindungi jaringan perusahaan dari serangan.

d. PT Telkom Indonesia memiliki rencana pemulihan bencana dan manajemen kejadian keamanan yang dirancang untuk menghadapi insiden keamanan atau bencana alam. Hal ini termasuk cadangan data, pemulihan sistem, dan respons yang terorganisir dalam situasi darurat.

e. PT Telkom Indonesia secara teratur melakukan audit keamanan dan penilaian risiko untuk memverifikasi keefektifan langkah-langkah keamanan yang diimplementasikan dan

mengidentifikasi area yang memerlukan perbaikan.

Saran

a. Terus tingkatkan kesadaran keamanan di seluruh organisasi PT Telkom Indonesia. Melakukan pelatihan keamanan reguler kepada seluruh karyawan agar mereka memahami praktik keamanan yang baik dan mengenali tanda-tanda serangan siber atau pelanggaran keamanan lainnya.
b. Lakukan penilaian keamanan secara rutin untuk mengidentifikasi kerentanan dan memastikan bahwa langkah-langkah keamanan yang diterapkan masih efektif. Tinjau dan perbarui kebijakan, prosedur, dan kontrol keamanan sesuai dengan perkembangan teknologi dan ancaman keamanan terkini.

DAFTAR PUSTAKA

[1] R. G. Putra *Dkk.*, "Universitas Bhayangkara Jakarta Raya, Indonesia, Achmad.Fauzi@Dsn.Ubharajaya.Ac.Id 3. Universitas Bhayangkara Jakarta Raya, Indonesia, Ery.Teguh@Ubharajaya.Ac.Id 4," Vol. 2, No. 1, Doi: 10.38035/Jim.V2i1.

[2] Winarni, "Profil Pt Telkom Indonesia (Persero) Tbk," *Dataindonesia.Id*, 10 November 2021. Https://Dataindonesia.Id/Profil-Perusahaan/Detail/Profil-Pt-Telkom-Indonesia-Persero-Tbk (Diakses 8 Juni 2023).

[3] E. Lastyono Putra, B. Cahyo Hidayanto, Dan H. Maria Astuti, "Evaluasi Keamanan Informasi Pada Divisi Network Of Broadband Pt. Telekomunikasi Indonesia Tbk. Dengan Menggunakan Indeks Keamanan Informasi (Kami)," Vol. 3, No. 2, 2014.

[4] Edy Soesanto, Alifah Jiddal Masyruroh, Ganis Aliefiani Mulya Putri, Dan Srirahayu Putri Maharani, "Peranan Manajemen Sekuriti Dalam Mengamankan Dan Memecahkan Masalah Pt Sk Keris Indonesia," *Jurnal Manajemen Riset Inovasi*, Vol. 1, No. 3, Hlm. 46–57, Jun 2023, Doi: 10.55606/Mri.V1i3.1259.

[5] E. Lastyono Putra, B. Cahyo Hidayanto, Dan H. Maria Astuti, "Evaluasi Keamanan Informasi Pada Divisi Network Of Broadband Pt. Telekomunikasi Indonesia Tbk. Dengan Menggunakan Indeks Keamanan Informasi (Kami)," Vol. 3, No. 2, 2014.

[6] W. Agasia Dan S. Margaretha Kuway, "Analisis Proses Bisnis : Studi Kasus Bagian Customer Care Pada Pt. Telkom Indonesia Tbk Kandatel Pontianak," 2012.

[7] I. Santosa Dan D. Kuswanto, "Analisa Manajemen Resiko Keamanan Informasi Pada Kantor Pelayanan Pajak Pratama Xyz Analysis Of Information Security Risk Management In Tax Service Office Pratama Xyz".