Remik: Riset dan E-Jurnal Manajemen Informatika Komputer
Volume 10, Number 1, Januari 2026
http://doi.org/10.33395/remik.v10i1.15907
e-ISSN : 2541-1330
p-ISSN : 2541-1332

Implementasi Sistem Manajemen Keamanan Informasi Iso/Iec 27001:2022 pada Unit Teknologi Informasi Perguruan Tinggi

[1]Harry Eko Ujiantoro Adi Basuki*, [2]Aliyi Hafiz, [3]Sulfikar Sallu
[1]Politeknik Sampit, [2] Bisnis Digital ITBA Dian Cipta Cendikia, [3]FKIP Universitas Sulawesi Tenggara
Kendari Indonesia

[1]harryeko.2025@student.Uny.Ac.Id, [2]hafizauditor@Gmail.Com , [3]sulfikar.sallu@gmail.Com

*Penulis Korespondensi
Diajukan : 13/12/2025
Diterima : 20/12/2025
Dipublikasi : 05/01/2026

ABSTRAK
Peningkatan ketergantungan perguruan tinggi terhadap sistem teknologi informasi menuntut adanya pengelolaan keamanan informasi yang terstruktur, sistematis, dan berbasis standar internasional guna melindungi kerahasiaan, integritas, dan ketersediaan aset informasi. Penelitian ini bertujuan untuk menganalisis implementasi Sistem Manajemen Keamanan Informasi (SMKI) ISO/IEC 27001:2022 pada Unit Teknologi Informasi di lingkungan perguruan tinggi sebagai upaya peningkatan tata kelola keamanan informasi dan kesiapan menuju sertifikasi. Penelitian ini menggunakan pendekatan studi kasus dengan metode deskriptif kualitatif. Data diperoleh melalui studi dokumentasi SMKI, observasi pelaksanaan sistem, serta hasil audit internal yang dilaksanakan berdasarkan siklus Plan–Do–Check–Act (PDCA). Hasil penelitian menunjukkan bahwa secara dokumentasi, implementasi SMKI telah memenuhi seluruh klausul utama ISO/IEC 27001:2022 dan kontrol yang relevan pada Annex A. Namun demikian, hasil audit internal mengidentifikasi masih terdapat kesenjangan pada tahap implementasi operasional, yang ditunjukkan oleh temuan ketidaksesuaian mayor dan minor, khususnya terkait pengelolaan risiko, pengendalian akses, dan konsistensi pencatatan rekaman. Temuan ini mengindikasikan bahwa keberhasilan implementasi SMKI tidak hanya ditentukan oleh kelengkapan dokumen, tetapi juga oleh efektivitas penerapan dan pemeliharaan sistem secara berkelanjutan. Penelitian ini menyimpulkan bahwa penerapan ISO/IEC 27001:2022 pada unit teknologi informasi perguruan tinggi memerlukan penguatan pada aspek implementasi dan budaya keamanan informasi agar kesiapan sertifikasi dapat dicapai secara optimal.

Kata Kunci: ISO/IEC 27001:2022, keamanan informasi, SMKI, teknologi informasi, perguruan tinggi

I. PENDAHULUAN
Perkembangan teknologi informasi yang pesat telah mendorong perguruan tinggi untuk mengandalkan sistem digital dalam mendukung penyelenggaraan layanan akademik, administrasi, dan pengelolaan data institusi. Sistem informasi akademik, pusat data, layanan jaringan, serta berbagai aplikasi pendukung menjadi aset strategis yang berperan penting dalam menjaga keberlangsungan operasional perguruan tinggi (Ali et al., 2015). Namun, peningkatan ketergantungan terhadap teknologi informasi juga diiringi dengan meningkatnya risiko keamanan informasi, seperti kebocoran data, gangguan layanan, serta penyalahgunaan akses yang dapat berdampak pada reputasi dan kepercayaan pemangku kepentingan.
Keamanan informasi dalam lingkungan perguruan tinggi memiliki karakteristik yang kompleks karena melibatkan berbagai jenis data, mulai dari data pribadi mahasiswa dan dosen, data

e-ISSN : 2541-1330
p-ISSN : 2541-1332

akademik, hingga data penelitian dan kerja sama institusional (Arum et al., 2025). Kerentanan terhadap insiden keamanan informasi tidak hanya disebabkan oleh faktor teknis, tetapi juga oleh lemahnya tata kelola, rendahnya kesadaran sumber daya manusia, serta belum terintegrasinya kebijakan dan prosedur keamanan informasi secara menyeluruh. Oleh karena itu, diperlukan suatu pendekatan manajemen keamanan informasi yang terstandar, terukur, dan berorientasi pada pengelolaan risiko.

ISO/IEC 27001:2022 merupakan standar internasional yang menyediakan kerangka kerja sistematis untuk membangun, menerapkan, memelihara, dan meningkatkan Sistem Manajemen Keamanan Informasi (SMKI) secara berkelanjutan (Filany Cahya Arumdiya, 2025) (Hafiz, 2025). Standar ini menekankan pendekatan berbasis risiko melalui siklus Plan–Do–Check–Act (PDCA), sehingga organisasi mampu mengidentifikasi ancaman, menilai risiko, serta menerapkan kontrol keamanan yang sesuai dengan konteks dan kebutuhan operasional. Penerapan ISO/IEC 27001:2022 di lingkungan perguruan tinggi diharapkan dapat meningkatkan tata kelola teknologi informasi, memperkuat perlindungan aset informasi, serta meningkatkan kepercayaan pemangku kepentingan internal dan eksternal .

Meskipun penerapan ISO/IEC 27001 telah banyak dikaji dalam konteks organisasi bisnis dan sektor industri, penelitian yang mengkaji implementasi standar ini secara empiris di lingkungan perguruan tinggi masih relatif terbatas (Culot et al., 2021) (Kitsios et al., 2023), khususnya yang menitikberatkan pada evaluasi kesiapan implementasi dan hasil audit internal. Sebagian penelitian lebih berfokus pada pengembangan sistem informasi atau aspek teknis keamanan, tanpa mengkaji secara komprehensif keterkaitan antara kelengkapan dokumentasi, efektivitas implementasi, dan temuan audit internal sebagai indikator keberhasilan SMKI. Kondisi ini menunjukkan adanya kesenjangan penelitian yang perlu diisi, terutama dalam konteks institusi pendidikan tinggi yang memiliki struktur organisasi dan budaya kerja yang berbeda dengan organisasi komersial.
Implementasi SMKI ISO/IEC 27001:2022 pada unit teknologi informasi perguruan tinggi menghadapi tantangan tersendiri, antara lain dalam menyelaraskan kebijakan keamanan informasi dengan proses operasional yang telah berjalan, membangun budaya keamanan informasi di kalangan sivitas akademika (Hafiz, 2025), serta memastikan konsistensi penerapan prosedur dan pencatatan rekaman sebagai bukti implementasi. Audit internal menjadi instrumen penting untuk menilai tingkat kesesuaian dan efektivitas penerapan SMKI, sekaligus mengidentifikasi kesenjangan antara dokumen yang telah disusun dengan praktik yang terjadi di lapangan.

Berdasarkan permasalahan tersebut, penelitian ini bertujuan untuk menganalisis implementasi Sistem Manajemen Keamanan Informasi ISO/IEC 27001:2022 pada Unit Teknologi Informasi perguruan tinggi melalui pendekatan studi kasus. Fokus penelitian diarahkan pada evaluasi kesesuaian implementasi SMKI berdasarkan hasil audit internal, serta identifikasi kesenjangan yang terjadi pada tahap operasional. Hasil penelitian ini diharapkan dapat memberikan kontribusi akademik berupa pemahaman empiris mengenai penerapan ISO/IEC 27001:2022 di lingkungan perguruan tinggi, serta kontribusi praktis sebagai bahan evaluasi dan referensi bagi institusi pendidikan tinggi dalam meningkatkan kesiapan sertifikasi dan tata kelola keamanan informasi secara berkelanjutan.

II. STUDI LITERATUR

Penerapan sistem manajemen keamanan informasi telah menjadi perhatian penting seiring meningkatnya ancaman keamanan siber pada berbagai sektor organisasi, termasuk institusi pendidikan tinggi (Marhad et al., 2024). Sejumlah penelitian terdahulu menunjukkan bahwa keamanan informasi tidak hanya dipengaruhi oleh kecanggihan teknologi yang digunakan, tetapi juga oleh tata kelola, kebijakan, serta perilaku sumber daya manusia yang terlibat dalam pengelolaan sistem informasi. Oleh karena itu, pendekatan manajerial melalui penerapan standar internasional dipandang sebagai solusi strategis dalam mengendalikan risiko keamanan informasi secara menyeluruh.
Penelitian mengenai penerapan ISO/IEC 27001 di sektor organisasi telah banyak dilakukan, khususnya pada sektor industri dan lembaga keuangan (Nurbojatmiko et al., 2025). Beberapa studi menyimpulkan bahwa penerapan ISO/IEC 27001 mampu meningkatkan tingkat kepatuhan terhadap kebijakan keamanan informasi, memperbaiki pengelolaan risiko, serta meningkatkan

e-ISSN : 2541-1330
p-ISSN : 2541-1332

kepercayaan pemangku kepentingan (Magnusson et al., 2025). Namun, sebagian besar penelitian tersebut berfokus pada organisasi komersial yang memiliki struktur tata kelola dan budaya kerja yang relatif berbeda dengan institusi pendidikan tinggi. Hal ini menyebabkan hasil penelitian tersebut belum sepenuhnya dapat digeneralisasikan pada konteks perguruan tinggi.

Dalam konteks institusi pendidikan, sejumlah penelitian menyoroti bahwa perguruan tinggi memiliki tingkat kompleksitas keamanan informasi yang tinggi karena melibatkan berbagai jenis data dan pengguna dengan latar belakang yang beragam (Ulven & Wangen, 2021). Penelitian terdahulu menunjukkan bahwa kelemahan keamanan informasi di perguruan tinggi sering kali disebabkan oleh rendahnya kesadaran keamanan informasi, kurangnya pengendalian akses yang konsisten, serta lemahnya dokumentasi dan pencatatan rekaman keamanan. Kondisi ini mengindikasikan bahwa keberhasilan implementasi sistem manajemen keamanan informasi di perguruan tinggi memerlukan pendekatan yang tidak hanya teknis, tetapi juga organisatoris dan kultural.

Beberapa studi yang mengkaji penerapan ISO/IEC 27001 di lingkungan pendidikan tinggi menunjukkan bahwa proses implementasi sering kali menghadapi tantangan pada tahap operasional (López-Vasco et al., 2025) (Apriany & Wibowo, 2024). Meskipun dokumen kebijakan dan prosedur telah disusun sesuai standar, penerapan di lapangan belum sepenuhnya konsisten. Audit internal dalam penelitian-penelitian tersebut mengungkapkan adanya ketidaksesuaian minor hingga mayor yang berkaitan dengan manajemen risiko, pengendalian akses, serta pemeliharaan bukti implementasi. Temuan ini memperkuat pandangan bahwa audit internal merupakan instrumen penting dalam menilai efektivitas penerapan SMKI secara nyata.

Dari sisi teoretis, Sistem Manajemen Keamanan Informasi (SMKI) didefinisikan sebagai sekumpulan kebijakan, prosedur, pedoman, dan aktivitas yang dirancang untuk melindungi aset informasi organisasi dari berbagai ancaman. Prinsip utama SMKI adalah menjaga kerahasiaan, integritas, dan ketersediaan informasi sebagai fondasi keamanan informasi. ISO/IEC 27001:2022 mengadopsi pendekatan manajemen berbasis risiko yang terintegrasi dengan siklus Plan–Do–Check–Act (PDCA), sehingga organisasi dapat melakukan perencanaan, implementasi, evaluasi, dan perbaikan secara berkelanjutan (Muhdar Abdurahman1, Mudar Safi2, 2019)

Pendekatan PDCA dalam ISO/IEC 27001:2022 memberikan kerangka kerja sistematis bagi organisasi untuk memastikan bahwa pengendalian keamanan informasi tidak bersifat statis, melainkan terus disesuaikan dengan perubahan risiko dan kebutuhan organisasi (Tuazon, 2023). Tahap perencanaan berfokus pada penetapan konteks, penilaian risiko, serta penentuan kontrol yang relevan (Glind et al., 2025). Tahap implementasi menekankan penerapan kebijakan dan prosedur keamanan informasi. Tahap evaluasi dilakukan melalui pemantauan dan audit internal, sedangkan tahap tindakan korektif diarahkan pada perbaikan berkelanjutan berdasarkan hasil evaluasi (Ayu et al., 2025).

Berdasarkan telaah penelitian terdahulu dan landasan teoretis tersebut, dapat disimpulkan bahwa masih terdapat kesenjangan penelitian terkait evaluasi implementasi ISO/IEC 27001:2022 di lingkungan perguruan tinggi, khususnya yang mengaitkan antara kelengkapan dokumentasi, hasil audit internal, dan efektivitas implementasi di tingkat operasional. Oleh karena itu, penelitian ini memposisikan diri untuk mengisi kesenjangan tersebut dengan menganalisis implementasi SMKI ISO/IEC 27001:2022 pada unit teknologi informasi perguruan tinggi melalui pendekatan studi kasus, sehingga diharapkan dapat memberikan kontribusi empiris bagi pengembangan tata kelola keamanan informasi di institusi pendidikan tinggi.

III. METODE

Penelitian ini menggunakan pendekatan **studi kasus** dengan metode **deskriptif kualitatif** untuk menganalisis implementasi Sistem Manajemen Keamanan Informasi (SMKI) ISO/IEC 27001:2022(Ulya et al., 2025) pada Unit Teknologi Informasi perguruan tinggi. Pendekatan studi kasus dipilih karena memungkinkan peneliti untuk melakukan pengamatan dan analisis secara mendalam terhadap penerapan SMKI dalam konteks organisasi yang nyata, sehingga mampu menggambarkan kondisi implementasi secara komprehensif dan kontekstual.

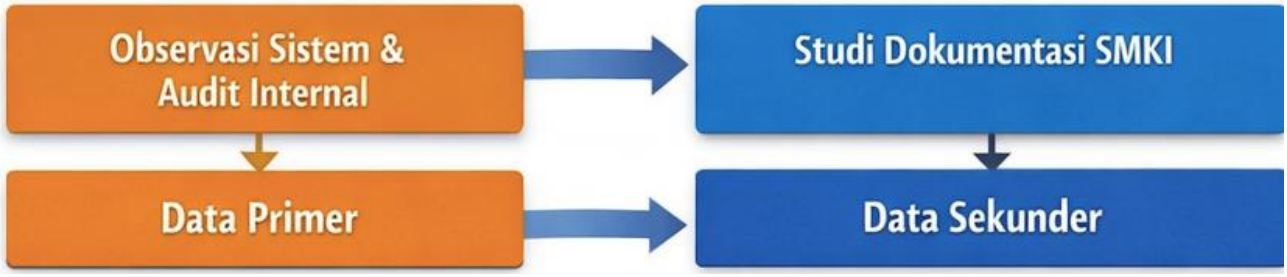
Objek penelitian adalah Unit Teknologi Informasi yang berperan sebagai pengelola layanan teknologi informasi dan aset informasi perguruan tinggi. Fokus penelitian diarahkan pada proses

Remik: Riset dan E-Jurnal Manajemen Informatika Komputer
Volume 10, Number 1, Januari 2026
http://doi.org/10.33395/remik.v10i1.15907
e-ISSN : 2541-1330
p-ISSN : 2541-1332

implementasi SMKI ISO/IEC 27001:2022, yang mencakup penyusunan dokumentasi, penerapan kontrol keamanan informasi, serta evaluasi efektivitas implementasi melalui audit internal. Penelitian ini tidak bertujuan untuk mengukur hubungan kausal antarvariabel, melainkan untuk mengevaluasi tingkat kesesuaian dan kesiapan implementasi SMKI berdasarkan standar yang berlaku.

Data penelitian diperoleh dari **data primer dan data sekunder**. Data primer dikumpulkan melalui observasi terhadap pelaksanaan sistem keamanan informasi dan proses audit internal yang dilaksanakan pada unit teknologi informasi. Data sekunder diperoleh melalui studi dokumentasi, yang meliputi kebijakan keamanan informasi, dokumen prosedur operasional standar (SOP), dokumen penilaian risiko, pernyataan penerapan kontrol (Statement of Applicability), serta laporan hasil audit internal SMKI ISO/IEC 27001:2022. Seluruh data yang digunakan merupakan data yang relevan dengan ruang lingkup implementasi SMKI pada unit yang diteliti.

Data diperoleh dari data primer ke data sekunder:



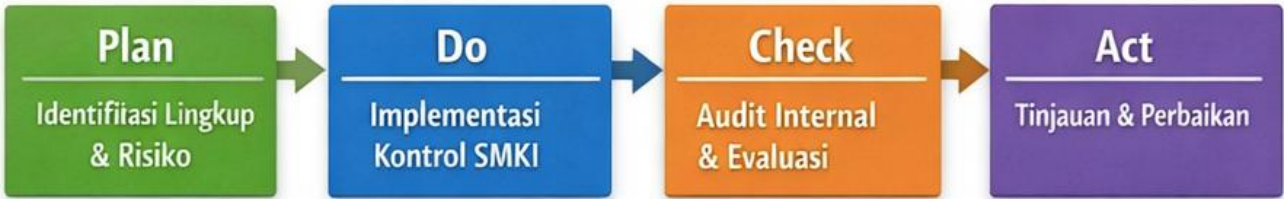
Gambar 1. Aliran Data Primer ke Sekunder

Gambar tersebut menggambarkan alur pengumpulan dan pengelompokan data penelitian dalam menganalisis implementasi Sistem Manajemen Keamanan Informasi (SMKI) ISO/IEC 27001:2022 pada unit teknologi informasi perguruan tinggi. Data primer diperoleh melalui observasi langsung terhadap sistem yang berjalan serta pelaksanaan audit internal SMKI. Observasi dan audit internal ini digunakan untuk menangkap kondisi nyata penerapan kebijakan, prosedur, dan kontrol keamanan informasi di tingkat operasional, termasuk praktik pengendalian akses, pengelolaan risiko, serta pencatatan bukti implementasi. Data primer ini mencerminkan tingkat kepatuhan aktual unit teknologi informasi terhadap persyaratan ISO/IEC 27001:2022.

Sementara itu, data sekunder diperoleh melalui studi dokumentasi SMKI yang meliputi kebijakan keamanan informasi, prosedur operasional standar, dokumen penilaian risiko, serta dokumen pendukung lainnya yang menjadi persyaratan standar. Hubungan antara data primer dan data sekunder pada gambar tersebut menunjukkan bahwa evaluasi implementasi SMKI tidak hanya bertumpu pada kelengkapan dokumen, tetapi juga pada kesesuaian antara dokumen yang disusun dengan praktik yang diterapkan di lapangan. Dengan mengintegrasikan kedua jenis data ini, penelitian mampu mengidentifikasi kesenjangan antara dokumentasi dan implementasi, sehingga memberikan gambaran yang lebih komprehensif mengenai tingkat kesiapan dan efektivitas penerapan ISO/IEC 27001:2022 pada unit teknologi informasi perguruan tinggi.

Proses analisis data dilakukan dengan mengacu pada kerangka kerja **Plan–Do–Check–Act (PDCA)** sebagaimana diadopsi dalam ISO/IEC 27001:2022. Pada tahap *Plan*, dilakukan identifikasi konteks organisasi, ruang lingkup SMKI, serta penilaian risiko keamanan informasi berdasarkan dokumen yang tersedia. Tahap *Do* mencakup analisis penerapan kebijakan, prosedur, dan kontrol keamanan informasi yang telah diimplementasikan pada unit teknologi informasi. Tahap *Check* dilakukan melalui analisis hasil audit internal untuk menilai tingkat kesesuaian implementasi terhadap persyaratan standar ISO/IEC 27001:2022. Tahap *Act* difokuskan pada identifikasi kesenjangan implementasi dan evaluasi tindakan korektif yang direncanakan sebagai upaya perbaikan berkelanjutan.

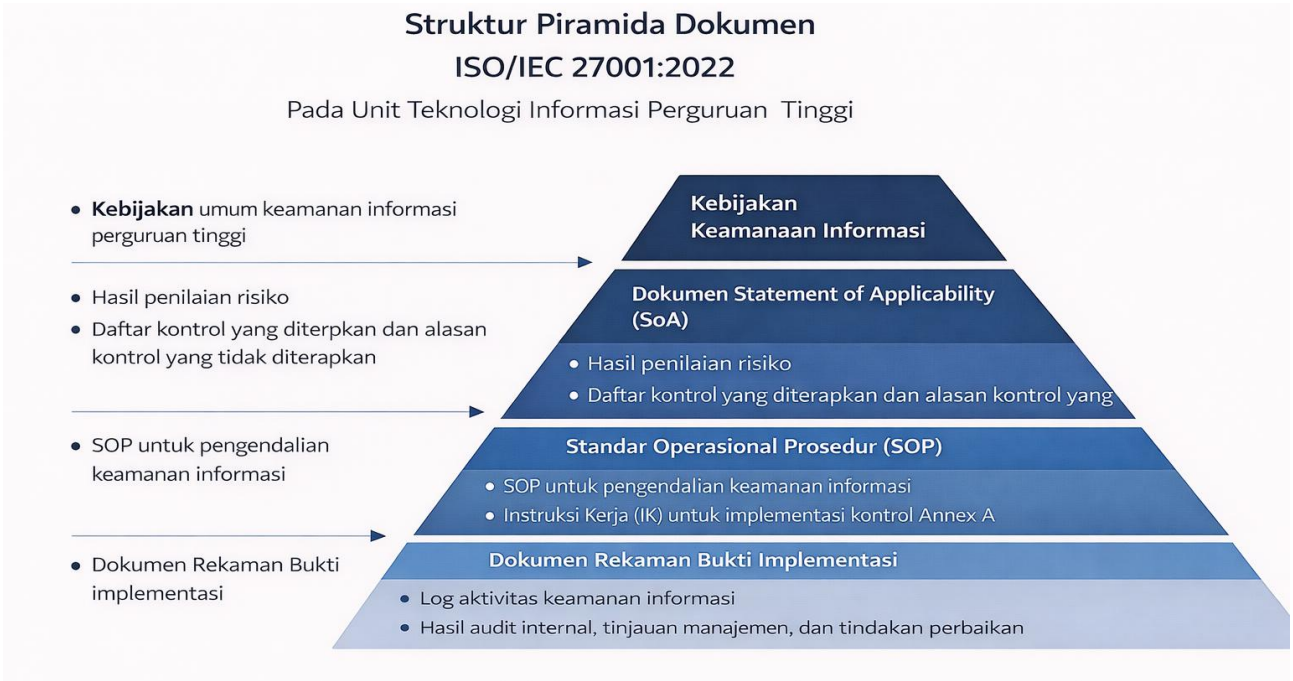
Remik: Riset dan E-Jurnal Manajemen Informatika Komputer
Volume 10, Number 1, Januari 2026
http://doi.org/10.33395/remik.v10i1.15907
e-ISSN : 2541-1330
p-ISSN : 2541-1332



Gambar 2. Kerangka PDCA

Gambar 2. Kerangka PDCA menunjukkan penerapan siklus Plan–Do–Check–Act (PDCA) sebagai kerangka kerja utama dalam implementasi Sistem Manajemen Keamanan Informasi (SMKI) ISO/IEC 27001:2022 pada unit teknologi informasi perguruan tinggi. Tahap *Plan* mencakup proses identifikasi ruang lingkup SMKI dan penilaian risiko keamanan informasi terhadap aset informasi yang dikelola, sehingga organisasi dapat menetapkan kebijakan, tujuan, serta kontrol keamanan yang relevan. Tahap ini menjadi fondasi penting dalam memastikan bahwa penerapan SMKI disesuaikan dengan konteks organisasi dan tingkat risiko yang dihadapi oleh unit teknologi informasi perguruan tinggi.

Tahap *Do* merepresentasikan implementasi kontrol keamanan informasi yang telah direncanakan, baik dalam bentuk kebijakan, prosedur, maupun pengendalian teknis dan administratif. Selanjutnya, tahap *Check* dilakukan melalui audit internal dan evaluasi kinerja SMKI untuk menilai tingkat kesesuaian penerapan kontrol terhadap persyaratan ISO/IEC 27001:2022 serta efektivitasnya dalam mengendalikan risiko. Tahap *Act* berfokus pada peninjauan manajemen dan perbaikan berkelanjutan berdasarkan hasil audit dan evaluasi, sehingga memungkinkan unit teknologi informasi perguruan tinggi untuk memperbaiki kelemahan yang ditemukan dan meningkatkan kematangan SMKI secara berkesinambungan. Siklus PDCA ini menegaskan bahwa implementasi SMKI bukan merupakan proses statis, melainkan proses dinamis yang terus berkembang seiring dengan perubahan risiko dan kebutuhan organisasi.



Gambar 3. Struktur Piramida Dokumen Sistem Manajemen Keamanan Informasi ISO/IEC 27001:2022 pada Unit Teknologi Informasi Perguruan Tinggi

Teknik analisis data dilakukan secara **deskriptif-analitis**, dengan cara membandingkan kondisi implementasi SMKI yang ditemukan di lapangan dengan persyaratan klausul ISO/IEC 27001:2022 dan kontrol yang relevan pada Annex A. Hasil audit internal dianalisis untuk mengidentifikasi jenis dan pola ketidaksesuaian, baik ketidaksesuaian mayor maupun minor, serta area yang memerlukan peningkatan. Analisis ini digunakan untuk menilai tingkat kesiapan implementasi SMKI dan efektivitas penerapannya pada unit teknologi informasi perguruan tinggi.

Remik: Riset dan E-Jurnal Manajemen Informatika Komputer
Volume 10, Number 1, Januari 2026 e-ISSN : 2541-1330
http://doi.org/10.33395/remik.v10i1.15907 p-ISSN : 2541-1332

IV. HASIL DAN PEMBAHASAN

Hasil penelitian menunjukkan bahwa implementasi Sistem Manajemen Keamanan Informasi (SMKI) ISO/IEC 27001:2022 pada unit teknologi informasi perguruan tinggi telah dilaksanakan secara terstruktur dan mengikuti kerangka kerja yang ditetapkan oleh standar. Pada tahap perencanaan, organisasi telah menetapkan ruang lingkup SMKI yang mencakup pengelolaan layanan teknologi informasi, pusat data, jaringan, serta aset informasi pendukung layanan akademik dan administrasi. Penilaian risiko keamanan informasi telah dilakukan sebagai dasar penentuan kontrol yang relevan, sehingga secara konseptual SMKI telah dirancang sesuai dengan prinsip manajemen risiko yang dianjurkan dalam ISO/IEC 27001:2022.

Dari sisi dokumentasi, hasil kajian menunjukkan bahwa unit teknologi informasi telah menyusun kebijakan keamanan informasi, prosedur operasional standar, dokumen penilaian risiko, serta pernyataan penerapan kontrol (Statement of Applicability) yang mencakup klausul utama dan kontrol Annex A ISO/IEC 27001:2022. Kelengkapan dokumen ini menunjukkan tingkat kepatuhan yang tinggi terhadap persyaratan formal standar. Dokumentasi SMKI juga telah dikendalikan melalui mekanisme pengendalian dokumen, sehingga perubahan dan distribusi dokumen dapat ditelusuri secara sistematis.

Namun demikian, hasil audit internal yang dilakukan pada tahap evaluasi mengungkapkan bahwa masih terdapat kesenjangan antara kelengkapan dokumentasi dan implementasi di tingkat operasional. Audit internal mengidentifikasi adanya ketidaksesuaian mayor dan minor, terutama yang berkaitan dengan konsistensi penerapan pengendalian akses, pengelolaan risiko yang belum sepenuhnya diperbarui, serta pencatatan rekaman sebagai bukti implementasi. Temuan ini menunjukkan bahwa meskipun kebijakan dan prosedur telah tersedia, penerapannya di lapangan belum sepenuhnya berjalan secara konsisten di seluruh unit kerja yang terlibat.

Temuan audit internal juga memperlihatkan bahwa sebagian besar ketidaksesuaian bersifat operasional, seperti belum optimalnya pemeliharaan log aktivitas, kurangnya bukti pelaksanaan prosedur tertentu, serta perbedaan pemahaman personel terhadap peran dan tanggung jawab dalam SMKI. Kondisi ini mengindikasikan bahwa faktor sumber daya manusia dan budaya keamanan informasi memiliki peran penting dalam menentukan efektivitas implementasi SMKI. Tanpa dukungan pemahaman dan kesadaran yang memadai, keberadaan dokumen dan kontrol formal belum tentu menjamin tercapainya tujuan keamanan informasi secara optimal.

Hasil penelitian ini sejalan dengan temuan penelitian terdahulu yang menyatakan bahwa keberhasilan penerapan ISO/IEC 27001 tidak hanya ditentukan oleh pemenuhan persyaratan dokumentasi, tetapi juga oleh efektivitas penerapan kontrol dan pemeliharaan sistem secara berkelanjutan. Dibandingkan dengan penelitian sebelumnya yang berfokus pada sektor industri atau organisasi komersial, hasil penelitian ini menunjukkan bahwa perguruan tinggi memiliki tantangan tambahan berupa kompleksitas pengguna dan variasi tingkat kepatuhan antarunit kerja. Oleh karena itu, audit internal dan siklus PDCA menjadi instrumen penting untuk memastikan bahwa SMKI dapat terus diperbaiki dan disesuaikan dengan dinamika organisasi.

Secara keseluruhan, hasil dan pembahasan menunjukkan bahwa implementasi SMKI ISO/IEC 27001:2022 pada unit teknologi informasi perguruan tinggi telah berada pada tahap implementasi yang baik dari sisi perencanaan dan dokumentasi, namun masih memerlukan penguatan pada aspek penerapan operasional dan konsistensi pelaksanaan kontrol. Temuan ini menegaskan pentingnya pendekatan perbaikan berkelanjutan melalui siklus PDCA, serta perlunya peningkatan kesadaran dan kompetensi sumber daya manusia sebagai bagian integral dari tata kelola keamanan informasi di perguruan tinggi.

Tabel 1. Hasil Evaluasi Implementasi SMKI ISO/IEC 27001:2022 pada Unit Teknologi Informasi Perguruan Tinggi

No	Aspek Implementasi SMKI	Deskripsi Hasil Implementasi	Temuan Utama

e-ISSN : 2541-1330
p-ISSN : 2541-1332

1	Penetapan Ruang Lingkup	Ruang lingkup SMKI telah ditetapkan mencakup layanan teknologi informasi, pusat data, jaringan, serta aset informasi pendukung layanan akademik dan administrasi perguruan tinggi.	Ruang lingkup telah sesuai dengan konteks organisasi dan persyaratan ISO/IEC 27001:2022.
2	Penilaian Risiko Keamanan Informasi	Penilaian risiko telah dilakukan sebagai dasar penentuan kontrol keamanan informasi dan penyusunan Statement of Applicability (SoA).	Metodologi penilaian risiko tersedia, namun pembaruan risiko belum sepenuhnya konsisten.
3	Dokumentasi SMKI	Kebijakan keamanan informasi, SOP, dokumen penilaian risiko, dan SoA telah disusun sesuai klausul ISO/IEC 27001:2022 dan Annex A.	Dokumentasi dinilai lengkap dan memenuhi persyaratan formal standar.
4	Implementasi Kontrol Keamanan	Kontrol keamanan administratif dan teknis telah diterapkan berdasarkan dokumen yang disusun.	Implementasi belum sepenuhnya konsisten di seluruh unit kerja.
5	Audit Internal SMKI	Audit internal dilaksanakan untuk mengevaluasi kesesuaian implementasi SMKI terhadap persyaratan standar.	Ditemukan ketidaksesuaian mayor dan minor pada tingkat operasional.
6	Pengelolaan Rekaman dan Bukti Implementasi	Rekaman dan bukti implementasi disiapkan sebagai bagian dari pemenuhan persyaratan SMKI.	Sebagian rekaman belum terdokumentasi secara konsisten.
7	Peran dan Kesadaran SDM	Personel terlibat dalam penerapan SMKI sesuai peran dan tanggung jawab yang ditetapkan.	Masih terdapat perbedaan pemahaman terkait peran dan kewajiban SMKI.
8	Tinjauan dan Perbaikan	Tinjauan manajemen dan rencana tindakan korektif disusun berdasarkan hasil audit internal.	Proses perbaikan berkelanjutan telah direncanakan namun masih perlu penguatan implementasi.

Keterangan Tabel

Tabel 1 menunjukkan bahwa implementasi SMKI ISO/IEC 27001:2022 pada unit teknologi informasi perguruan tinggi telah memenuhi persyaratan standar dari sisi perencanaan dan dokumentasi. Namun demikian, hasil audit internal mengindikasikan adanya kesenjangan pada tahap implementasi operasional, khususnya terkait konsistensi penerapan kontrol dan pencatatan rekaman sebagai bukti implementasi.

Remik: Riset dan E-Jurnal Manajemen Informatika Komputer
Volume 10, Number 1, Januari 2026
http://doi.org/10.33395/remik.v10i1.15907
e-ISSN : 2541-1330
p-ISSN : 2541-1332

Tabel 2. Hasil Kuantitatif Evaluasi Implementasi SMKI ISO/IEC 27001:2022 pada Unit Teknologi Informasi Perguruan Tinggi

No	Aspek Evaluasi SMKI	Indikator Penilaian	Jumlah Temuan	Persentase (%)	Tingkat Kesesuaian
1	Perencanaan & Ruang Lingkup	Kesesuaian ruang lingkup dan konteks organisasi	2 Minor	1,8	Tinggi
2	Penilaian Risiko	Pembaruan risiko dan mitigasi	6 Minor, 4 Mayor	9,0	Sedang
3	Dokumentasi SMKI	Kelengkapan kebijakan, SOP, dan SoA	0	0,0	Sangat Tinggi
4	Implementasi Kontrol	Konsistensi penerapan kontrol Annex A	38 Minor, 9 Mayor	42,3	Rendah
5	Pengendalian Akses	Pengaturan hak akses dan otorisasi	14 Minor, 6 Mayor	18,0	Sedang
6	Pengelolaan Rekaman	Bukti implementasi dan pencatatan log	12 Minor	10,8	Sedang
7	Kesadaran & Peran SDM	Kepatuhan peran dan tanggung jawab	8 Minor	7,2	Sedang
8	Audit Internal & Evaluasi	Pelaksanaan audit dan tindak lanjut	2 Minor	1,8	Tinggi
–	**Total Temuan Audit Internal**	**Mayor + Minor + OFI**	**111 Temuan**	**100**	–

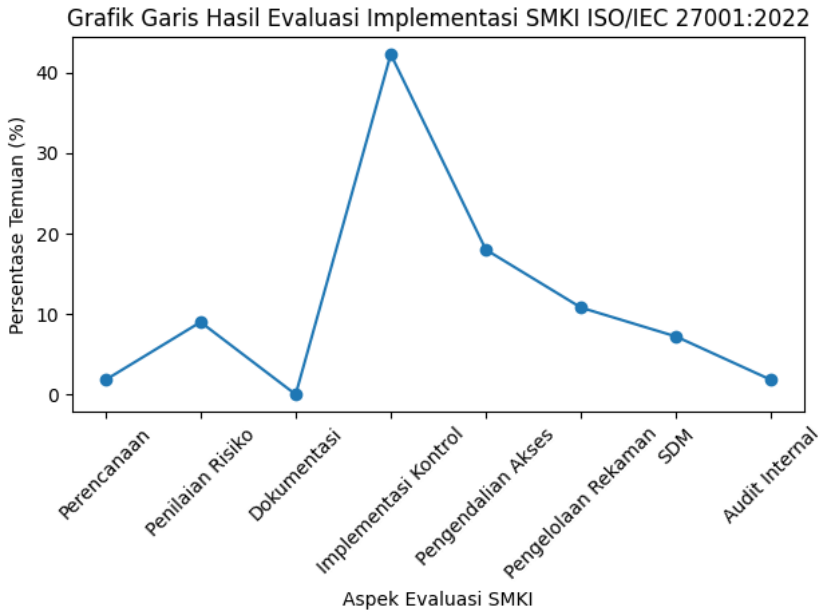
Keterangan Skala Tingkat Kesesuaian

A. **Sangat Tinggi** : 0–5% temuan
B. **Tinggi** : >5–10% temuan
C. **Sedang** : >10–20% temuan
D. **Rendah** : >20% temuan

Interpretasi Tabel

Berdasarkan Tabel 2, secara kuantitatif implementasi SMKI ISO/IEC 27001:2022 pada unit teknologi informasi perguruan tinggi menunjukkan tingkat kesesuaian yang **tinggi pada aspek perencanaan dan dokumentasi**, namun **menurun pada aspek implementasi kontrol dan pengendalian operasional**. Aspek implementasi kontrol keamanan informasi menjadi penyumbang temuan terbesar, yaitu lebih dari 40% dari total temuan audit internal, yang didominasi oleh ketidaksesuaian minor dan mayor. Hal ini menunjukkan bahwa tantangan utama implementasi SMKI terletak pada konsistensi penerapan kontrol dan pemeliharaan bukti implementasi, bukan pada ketersediaan dokumen.

Remik: Riset dan E-Jurnal Manajemen Informatika Komputer
Volume 10, Number 1, Januari 2026
http://doi.org/10.33395/remik.v10i1.15907
e-ISSN : 2541-1330
p-ISSN : 2541-1332



Grafik 1. Grafik Garis Hasil Evaluasi Implementasi SMKI ISO/IEC 27001:2022

Grafik garis tersebut menunjukkan distribusi persentase temuan audit internal pada setiap aspek evaluasi implementasi Sistem Manajemen Keamanan Informasi (SMKI) ISO/IEC 27001:2022 di unit teknologi informasi perguruan tinggi. Terlihat bahwa aspek *implementasi kontrol keamanan informasi* memiliki persentase temuan tertinggi, yaitu lebih dari 40%, yang mengindikasikan bahwa sebagian besar ketidaksesuaian terjadi pada tahap penerapan operasional kontrol Annex A. Kondisi ini menunjukkan bahwa meskipun kebijakan dan prosedur telah tersedia, penerapan kontrol di lapangan belum sepenuhnya berjalan secara konsisten.

Sebaliknya, aspek *dokumentasi SMKI* dan *audit internal* menunjukkan persentase temuan yang sangat rendah, mendekati nol, yang mencerminkan tingkat kepatuhan yang tinggi terhadap persyaratan formal standar. Aspek lain seperti *pengendalian akses*, *pengelolaan rekaman*, dan *kesadaran sumber daya manusia* berada pada tingkat temuan sedang, yang menandakan masih perlunya penguatan pada konsistensi implementasi dan budaya keamanan informasi. Secara keseluruhan, grafik ini menegaskan bahwa tantangan utama implementasi ISO/IEC 27001:2022 pada unit teknologi informasi perguruan tinggi terletak pada efektivitas penerapan operasional, bukan pada kelengkapan perencanaan dan dokumentasi sistem.

Hasil penelitian ini memperkuat temuan sejumlah penelitian terdahulu yang menyatakan bahwa penerapan ISO/IEC 27001 sering kali menunjukkan tingkat kepatuhan yang tinggi pada aspek dokumentasi, namun menghadapi tantangan pada tahap implementasi operasional. Penelitian-penelitian sebelumnya di sektor organisasi dan institusi publik menunjukkan bahwa keberadaan kebijakan dan prosedur keamanan informasi tidak secara otomatis menjamin efektivitas pengendalian risiko apabila tidak diikuti dengan penerapan yang konsisten di lapangan. Namun, sebagian besar studi terdahulu cenderung menilai keberhasilan implementasi ISO/IEC 27001 secara umum atau bersifat konseptual, tanpa menyajikan analisis kuantitatif yang mengaitkan distribusi temuan audit internal dengan aspek-aspek spesifik dalam siklus PDCA. Dalam konteks ini, hasil penelitian ini memberikan bukti empiris yang lebih terukur mengenai titik kritis implementasi SMKI, khususnya pada aspek implementasi kontrol dan pengendalian operasional.

Gambar struktur piramida dokumen ISO/IEC 27001:2022 menunjukkan bahwa implementasi Sistem Manajemen Keamanan Informasi (SMKI) pada unit teknologi informasi perguruan tinggi telah dibangun secara hierarkis dan terintegrasi mulai dari kebijakan hingga bukti implementasi. Pada tingkat tertinggi, kebijakan keamanan informasi berfungsi sebagai arah strategis dan komitmen manajemen, yang selanjutnya diterjemahkan ke dalam dokumen Statement of Applicability (SoA) sebagai dasar pemilihan kontrol keamanan berdasarkan hasil penilaian risiko. Tingkat berikutnya berupa standar operasional prosedur dan instruksi kerja menggambarkan proses

e-ISSN : 2541-1330
p-ISSN : 2541-1332

penerapan kontrol keamanan secara operasional, sedangkan lapisan terbawah berupa dokumen rekaman dan bukti implementasi mencerminkan realisasi kebijakan dan prosedur dalam praktik sehari-hari. Struktur piramida ini menegaskan bahwa meskipun dokumen kebijakan dan perencanaan telah tersusun dengan baik, efektivitas implementasi SMKI sangat ditentukan oleh konsistensi penerapan pada level operasional dan ketersediaan bukti implementasi, yang selaras dengan temuan audit internal pada penelitian ini.

Kontribusi ilmiah utama (novelty) dari penelitian ini terletak pada pendekatan evaluasi implementasi ISO/IEC 27001:2022 di lingkungan perguruan tinggi dengan mengintegrasikan hasil audit internal ke dalam analisis kuantitatif berbasis siklus PDCA. Berbeda dengan penelitian sebelumnya yang lebih menekankan pada kesiapan dokumen atau desain sistem keamanan informasi, penelitian ini menunjukkan bahwa tantangan terbesar implementasi SMKI pada unit teknologi informasi perguruan tinggi berada pada kesenjangan antara perencanaan dan pelaksanaan (*plan–do gap*). Temuan ini memperkaya khazanah keilmuan dengan memberikan perspektif bahwa keberhasilan ISO/IEC 27001 di institusi pendidikan tinggi sangat dipengaruhi oleh faktor operasional dan budaya keamanan informasi, bukan semata-mata oleh kepatuhan administratif. Dengan demikian, penelitian ini tidak hanya mengonfirmasi temuan sebelumnya, tetapi juga menawarkan sudut pandang baru yang relevan sebagai dasar pengembangan model evaluasi implementasi SMKI yang lebih kontekstual bagi perguruan tinggi.

V. UCAPAN TERIMA KASIH

Terima kasih disampaikan kepada PT. Bhakti Unggul Teknovasi (BUT) sebuah perusahaan berbasis teknologi yang berfokus pada solusi IT, konsultansi manajemen/teknologi, dan intermediasi hasil riset perguruan tinggi, terutama dari Telkom University. Didirikan di Bandung, BUT bertindak sebagai mitra strategis untuk Yayasan Pendidikan Telkom (YPT) dan industri umum, serta berkomitmen menjadi perusahaan transfer teknologi terkemuka pada tahun 2030 yang telah memberikan kesempatan kepada penulis untuk melakukan penelitian sejak dari awal pendampingan sampai selesai Audit Internal dengan durasi waktu 3 (tiga) bulan pada salah satu perguruan tinggi negeri di Indonesia.

VI. KESIMPULAN

Implementasi Sistem Manajemen Keamanan Informasi (SMKI) ISO/IEC 27001:2022 pada unit teknologi informasi perguruan tinggi telah memenuhi persyaratan standar dari sisi perencanaan dan kelengkapan dokumentasi, namun masih menghadapi tantangan pada tahap implementasi operasional kontrol keamanan informasi. Hasil audit internal menunjukkan bahwa kesenjangan utama terjadi pada konsistensi penerapan kontrol, pengelolaan rekaman, serta keterlibatan sumber daya manusia dalam menjalankan peran dan tanggung jawab keamanan informasi. Temuan ini menegaskan bahwa keberhasilan penerapan ISO/IEC 27001:2022 tidak hanya ditentukan oleh kepatuhan administratif, tetapi sangat bergantung pada efektivitas implementasi dan perbaikan berkelanjutan melalui siklus Plan–Do–Check–Act (PDCA). Penelitian ini memberikan kontribusi empiris dengan menunjukkan bahwa evaluasi berbasis audit internal dan analisis kuantitatif mampu mengidentifikasi titik kritis implementasi SMKI di lingkungan perguruan tinggi, sehingga dapat menjadi dasar penguatan tata kelola keamanan informasi dan peningkatan kesiapan sertifikasi secara berkelanjutan.

VII. REFERENSI

Ali, E., Susandri, & Rahmaddeni. (2015). Sistem Informasi Akademik (SIAKAD) untuk Solusi Kompleksitas Manajemen Data dan Informasi di Perguruan Tinggi. *Sains Dan Teknologi Informasi*, *1*(1), 63–68.

Apriany, A., & Wibowo, A. (2024). Analysis of the Implementation of ISO 27001: 2022 and KAMI Index in Enhancing the Information Security Management System in Consulting Firms. *IJCCS (Indonesian Journal of Computing and Cybernetics Systems)*, *18*(4), 417–428. https://doi.org/10.22146/ijccs.100385

Arum, S. F., Zubaidi, A., & Huwae, R. B. (2025). Pengukuran Tingkat Kesadaran Keamanan Informasi Menggunakan HAIS-Q: Mengungkap Kesenjangan antara Sikap dan Pengetahuan

Mahasiswa Measuring Information Security Awareness Using HAIS-Q: Revealing the Gap between Students' Attitudes and Knowledge. *Jurnal Bumigora Information Technology (BITe)*, *7*(2), 83–94. https://doi.org/10.30812/bite.v7i2.5430

Ayu, D., Faroqi, A., & Wulansari, A. (2025). Evaluation of Information Security Management Capability Level with COBIT 5. *Bit-Tech*, *8*, 726–737. https://doi.org/10.32877/bt.v8i1.2682

Culot, G., Nassimbeni, G., Podrecca, M., & Sartor, M. (2021). The ISO/IEC 27001 information security management standard: literature review and theory-based research agenda. *The TQM Journal*, *33*(7), 76–105. https://doi.org/https://doi.org/10.1108/TQM-09-2020-0202

Filany Cahya Arumdiya, C. R. (2025). Implementasi ISO 27001:2022 dalam Manajemen Risiko Keamanan Informasi. *Jurnal PETISI*, *6*(2), 167–186.

Glind, I. van de, Mulder, R., Akkerman, A., van der Biezen, M., Bootsma, J., Finnema, E., Heerma van Voss, L., Mouter, N., van Rooij, J., & van de Ven, G. (2025). Mapping the Literature on Job Evaluation: A Scoping Review. *Compensation and Benefits Review*, *57*(1), 24–46. https://doi.org/10.1177/08863687241279592

Hafiz, A. (2025). Tren Implementasi Iso 27001 Sistem Manajemen Keamanan Informasi Pada Perguruan Tinggi (Literature Review). *Jurnal Informasi Dan Komputer*, *13*(02), 159–163. https://doi.org/10.35959/jik.v13i02.782

Kitsios, F., Chatzidimitriou, E., & Kamariotou, M. (2023). The ISO/IEC 27001 Information Security Management Standard: How to Extract Value from Data in the IT Sector. In *Sustainability* (Vol. 15, Issue 7, p. 5828). https://doi.org/10.3390/su15075828

López-Vasco, F., Angulo, M., Zuñiga, D., Moromenacho, E., & Ortiz, N. (2025). Application of ISO/IEC 27,001 in Higher Education Technological Institutes: Case-Control Study. *International Conference of Research Apllied to Defense and Security*, 179–189. https://doi.org/10.1007/978-981-96-0235-3_15

Magnusson, L., Iqbal, S., Elm, P., & Dalipi, F. (2025). Information security governance in the public sector: investigations, approaches, measures, and trends. *International Journal of Information Security*, *24*(4). https://doi.org/10.1007/s10207-025-01097-x

Marhad, S., Goni, S., & Sani, M. (2024). Implementation of Information Security Management Systems for Data Protection in Organizations: A systematic literature review. *Environment-Behaviour Proceedings Journal*, *9*, 197–203. https://doi.org/10.21834/e-bpj.v9iSI18.5483

Muhdar Abdurahman1, Mudar Safi2, M. H. A. (2019). IJIS Indonesian Journal on Information System ISSN 2548-6438. *IJIS-Indonesia Journal on Information System*, *4*(April), 69–76. https://media.neliti.com/media/publications/260171-sistem-informasi-pengolahan-data-pembeli-e5ea5a2b.pdf

Nurbojatmiko, N., Karimiyah, M. S. K., Asnadi, N. M., & Anisyah, R. (2025). ISO 27001 As Information Security Solution In Society 5.0 Era: Systematic Literature Review. *Sinkron*, *9*(1), 484–492. https://doi.org/10.33395/sinkron.v9i1.14448

Tuazon, G. (2023). ISO 27001 and the PDCA Cycle: A Roadmap to Information Security. *GCC | Global Compliance Certification*, 1–5. https://gccertification.com/iso-27001-and-the-pdca-cycle-a-roadmap-to-information-security/

Ulven, J., & Wangen, G. B. (2021). A Systematic Review of Cybersecurity Risks in Higher Education. *Future Internet*, *13*. https://doi.org/10.3390/fi13020039

Ulya, A., Karima, A., Sukiman, T. S. A., Zulfia, A., & Rahmawati, R. (2025). Information Security Risk Analysis Using ISO 31000:2018 and ISO 27001:2022. *Brilliance: Research of Artificial Intelligence*, *5*(2), 843–853. https://jurnal.itscience.org/index.php/brilliance/article/view/6564