NIVEDITA
JOURNAL INFORMATICS
ISSN 3089-8366
(Media Online)

Vol. 01, No. 2, Juni 2025

AUDIT TATA KELOLA TEKONOLGI WEBSITE KKN UNIVERSITAS XYZ MENGGUNAKAN COBIT 5 APO12 & APO13

Afif Fathin[1], Muhammad Fauzan Khalid[2], Megawati[3]

[1,2,3,4] Sistem Informasi, Universitas Islam Negeri Sultan Syarif Kasim Riau, Pekanbaru, Indonesia

email: 12250311728@students.uin-suska.ac.id

Abstract

This study explores the implementation of risk and information security management within the digital service system of the KKN program at UIN Suska Riau, based on the COBIT 2019 framework. The evaluation concentrated on two essential domains: APO12 (Managed Risk) and APO13 (Managed Security). The assessment was conducted using capability level analysis, comparing the current process maturity with predetermined targets. The results revealed that APO12 achieved Capability Level 2, while APO13 remained at Level 1. These outcomes suggest that key processes are still underdeveloped, lack formal documentation, and are not yet backed by standardized policies. Accordingly, this research proposes several strategic actions, including policy formulation, risk documentation, security analysis, and enhancement of information protection mechanisms. These recommendations aim to strengthen the governance of IT-related risks and security while promoting sustainable digital service operations in accordance with COBIT 2019 guidelines.

Keywords: *COBIT 2019, Risk Management, Information Security, Capability Level, KKN System.*

Abstrak

Penelitian ini bertujuan untuk menelaah penerapan pengelolaan risiko dan keamanan teknologi informasi dalam sistem layanan digital Kuliah Kerja Nyata (KKN) di UIN Suska Riau, dengan mengacu pada kerangka kerja COBIT 2019. Fokus utama evaluasi berada pada dua domain: APO12 (Managed Risk) dan APO13 (Managed Security). Penilaian dilakukan melalui pendekatan capability level dengan membandingkan kondisi aktual terhadap target yang ditetapkan. Hasil evaluasi menunjukkan bahwa domain APO12 mencapai Level 2, sedangkan APO13 masih berada di Level 1. Temuan ini mengindikasikan bahwa pelaksanaan proses belum sepenuhnya berjalan optimal, minim dokumentasi formal, serta belum ditopang kebijakan standar. Oleh karena itu, penelitian ini memberikan sejumlah usulan strategis seperti penyusunan kebijakan, dokumentasi risiko, analisis keamanan, serta penguatan sistem perlindungan informasi. Langkah-langkah ini diharapkan dapat memperbaiki tata kelola risiko dan keamanan informasi, serta mendukung operasional layanan digital yang berkelanjutan sesuai prinsip COBIT 2019.

Kata kunci: COBIT 2019, Manajemen Risiko, Keamanan Informasi, Tingkat Kapabilitas, Sistem KKN.

Diajukan:13 Mei 2025; Direvisi: 29 Mei 2025; Diterima:1 Juni 2025

PENDAHULUAN

Transformasi digital di sektor publik, termasuk di institusi pendidikan tinggi, menjadi langkah strategis dalam meningkatkan efisiensi dan mutu layanan. Namun, proses implementasinya sering kali menghadapi tantangan, seperti ketergantungan pada jaringan internet, terbatasnya integrasi antar sistem, serta kelemahan dalam aspek manajemen risiko dan pengamanan informasi. Permasalahan serupa juga terjadi di Universitas XYZ, khususnya pada sistem informasi yang digunakan dalam pengelolaan kegiatan Kuliah Kerja Nyata (KKN), yang dinilai belum sepenuhnya mampu memenuhi tuntutan operasional secara menyeluruh [1].

Hasil penilaian sebelumnya terhadap sistem KKN menunjukkan tingkat efektivitas sebesar 54,5% berdasarkan model HOT-FIT, yang diklasifikasikan dalam kategori sedang. Capaian ini mengindikasikan perlunya perbaikan melalui tata kelola teknologi informasi yang lebih sistematis dan terstruktur [1]. Sejumlah kelemahan teknis juga ditemukan, di antaranya belum adanya mekanisme enkripsi data, lemahnya sistem autentikasi, tidak tersedianya prosedur pencadangan data yang baik, serta absennya dokumentasi formal seperti kebijakan teknis dan SOP terkait keamanan sistem.

Sebagai acuan, sektor industri telah menunjukkan keberhasilan dalam menerapkan kerangka kerja tata kelola TI seperti COBIT 5, khususnya pada domain APO12 (Managed Risk) dan APO13 (Managed

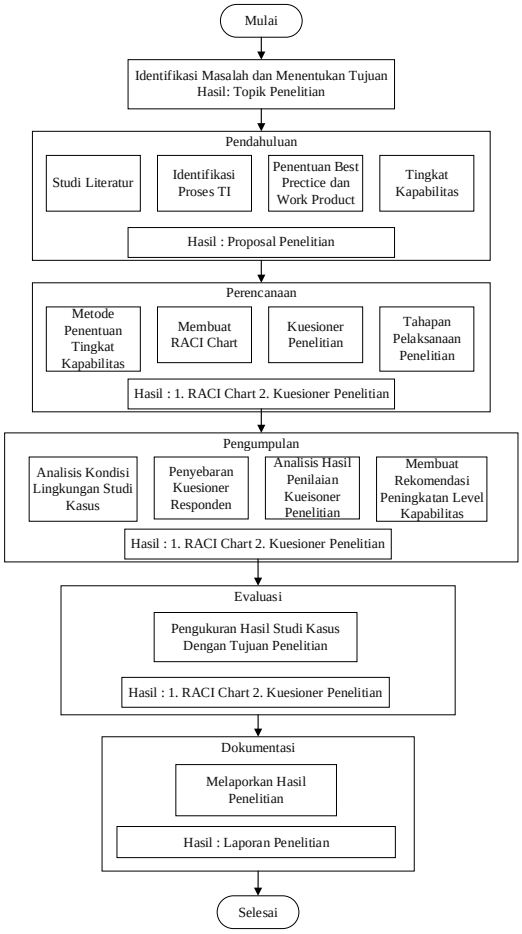
NIVEDITA JOURNAL INFORMATICS
ISSN 3089-8366
(Media Online)
Vol. 01, No. 2, Juni 2025

Security), yang terbukti efektif dalam menjamin kinerja dan keamanan sistem informasi [2]. Keberhasilan penerapan dua domain ini dapat dijadikan rujukan penting bagi perguruan tinggi dalam upaya meningkatkan kualitas tata kelola layanan digital.

Berdasarkan latar belakang tersebut, penelitian ini bertujuan untuk menilai tingkat kapabilitas pengelolaan risiko (APO12) dan keamanan informasi (APO13) pada sistem informasi KKN di Universitas XYZ. Penilaian dilakukan melalui pendekatan Process Assessment Model (PAM) dari COBIT 5, dan hasil evaluasinya akan digunakan sebagai dasar penyusunan rekomendasi strategis untuk meningkatkan kapabilitas proses serta keberlanjutan tata kelola teknologi informasi di lingkungan pendidikan tinggi.

METODE

Step-step yang dilakukan dalam penelitian ini disusun secara sistematis dan divisualisasikan melalui diagram alur pada Gambar 1. Proses penelitian dimulai dari tahap perencanaan awal hingga tahap akhir berupa dokumentasi hasil. Setiap tahapan dirancang untuk memastikan bahwa proses evaluasi terhadap tata kelola risiko dan keamanan informasi berjalan secara terstruktur dan terukur sesuai dengan standar kerangka kerja COBIT yang digunakan.



Gambar 1 Metodologi Penelitian

1. Identifikasi Masalah

Untuk memulai penelitian ini, kami melihat masalah yang terjadi dengan sistem informasi Kuliah Kerja Nyata (KKN) di Universitas XYZ. Hasil dari observasi awal kami dan wawancara dengan tim pengelola sistem menunjukkan bahwa elemen manajemen risiko dan keamanan informasi masih diterapkan secara tidak sistematis dan tanpa dokumentasi formal yang memadai. Selain itu, tidak ada standar operasional prosedur (SOP) yang dimaksudkan untuk mengarahkan pelaksanaan teknis. Beberapa hambatan tambahan yang diidentifikasi termasuk kurangnya sistem enkripsi yang digunakan untuk melindungi data, kurangnya rencana pencadangan data yang terstruktur, sistem pencatatan log aktivitas, serta lemahnya fitur autentikasi untuk pengguna sistem [3], [4].

NIVEDITA JOURNAL INFORMATICS
ISSN 3089-8366
(Media Online)
Vol. 01, No. 2, Juni 2025

2. Pendahuluan

Setelah proses identifikasi masalah diselesaikan, langkah selanjutnya adalah melakukan kajian pustaka guna memperdalam pemahaman terkait tata kelola teknologi informasi, pengelolaan risiko, Selain itu, aspek proteksi sistem informasi juga dikaji dengan merujuk pada struktur kerangka kerja **COBIT 5**. Tinjauan literatur secara khusus difokuskan pada dua domain utama dalam kerangka tersebut, yaitu **APO12** yang berhubungan dengan pengelolaan risiko, serta **APO13** yang berfokus pada pengendalian dan keamanan informasi.. Studi ini berperan penting dalam membentuk landasan teoritis yang mendukung penelitian, sekaligus menjadi acuan dalam menyusun rancangan awal pelaksanaan studi. Pada tahap ini pula, disusun proposal penelitian yang mencakup tujuan, cakupan, metodologi yang akan diterapkan, serta penetapan tingkat kapabilitas proses yang akan menjadi objek evaluasi [5], [6].

2.1. APO12

Tujuan utama dari domain APO12 yaitu memastikan proses pengendalian risiko TI sejalan dan terkoordinasi dengan kebijakan manajemen risiko di tingkat organisasi secara luas. Domain ini juga menekankan perlunya mempertimbangkan secara proporsional antara potensi biaya dan manfaat yang ditimbulkan dalam setiap kegiatan pengelolaan risiko TI, guna mendukung pengambilan keputusan yang tepat dan efisien.

Tabel 1. APO12

Kode	Aktivitas
APO12.01	Mengumpulkan data
APO12.02	Melakukan analisis risiko
APO12.03	Mempertahankan profil risiko
APO12.04	Mengartikulasikan risiko
APO12.05	Mendefinisikan portofolio tindakan manajemen risiko
APO12.06	Menanggapi risiko

2.2. APO13

Dalam struktur kerangka kerja COBIT 2019, APO13 (Managed Security) merupakan salah satu domain kunci yang berfungsi untuk melindungi aset informasi organisasi. Fokus utamanya adalah membantu institusi dalam merancang, menerapkan, dan menjaga sistem keamanan informasi secara terpadu. Pendekatan ini dirancang agar organisasi dapat mengenali dan menangani berbagai risiko yang mungkin timbul, baik dari dalam organisasi maupun dari faktor luar organisasi.

Tabel 2. APO13

Kode	Aktivitas
APO13.01	Merancang dan memelihara sistem manajemen keamanan informasi
APO13.02	Menetapkan serta mengelola pengendalian terhadap risiko keamanan dan privasi informasi
APO13.03	Melakukan pemantauan dan evaluasi berkala terhadap sistem keamanan informasi

3. Perencanaan

Perencanaan penelitian mencakup penentuan metode pengumpulan data dan instrumen yang digunakan. Salah satu langkah penting dalam tahap ini adalah penyusunan RACI Chart, yaitu sebuah matriks yang digunakan untuk memperjelas peran dan tanggung jawab setiap pihak yang terlibat dalam suatu proses atau proyek. RACI merupakan akronim dari:

- Responsible : pihak yang bertanggung jawab langsung melaksanakan tugas,
- Accountable: pihak yang memegang kekuasaan utama serta bertanggung jawab penuh terhadap hasil akhir dari suatu aktivitas atau keputusan.
- Consulted : pihak yang dikonsultasikan sebelum pengambilan keputusan, dan
- Informed : pihak yang perlu mendapatkan informasi terkait keputusan atau hasil.

Tujuan utama dari penggunaan RACI Chart adalah untuk mencegah terjadinya tumpang tindih peran serta memberikan kejelasan dalam pelaksanaan tugas dan pengambilan keputusan selama proses penelitian berlangsung. Di samping itu, disusun pula instrumen kuesioner menggunakan Process Assessment Model (PAM) dari COBIT 5, yang mengacu pada indikator kapabilitas proses dalam domain APO12 dan APO13. Kuesioner disusun untuk masing-masing level kapabilitas dari Level 1 hingga Level 5[7].

NIVEDITA JOURNAL INFORMATICS
ISSN 3089-8366
(Media Online)
Vol. 01, No. 2, Juni 2025

A. *RACI Chart* untuk *Control Objective APO12*

Tabel 3. *RACI Chart APO12*

Aktivitas	Div. Aplikasi PTIPD	Div. Server PTIPD	Kepala LPPM	Kapus Pengabdian	Staf LPPM
APO12.01 – Mengumpulkan data risiko	R	R	A	C	I
APO12.02 – Menganalisis risiko	R	R	A	C	I
APO12.03 – Memelihara profil risiko	R	C	A	C	I
APO12.04 – Mengartikulasikan risiko	R	C	A	C	I
APO12.05 – Menentukan tindakan manajemen risiko	C	C	A	R	R
APO12.06 – Menanggapi risiko	R	R	A	C	I

B. *RACI Chart* untuk *Control Objective APO13*

Tabel 4. *RACI Chart APO13*

Aktivitas	Div. Aplikasi PTIPD	Div. Server PTIPD	Kepala LPPM	Kapus Pengabdian	Staf LPPM
APO13.01 – Membangun dan memelihara sistem manajemen keamanan informasi (ISMS)	R	R	A	C	I
APO13.02 – Menentukan dan mengelola rencana perlakuan risiko keamanan dan privasi	R	R	A	C	I
APO13.03 – Memantau dan meninjau sistem manajemen keamanan informasi (ISMS)	R	R	A	C	I

4. Pengumpulan

Pada tahap ini, dilakukan pengumpulan data melalui beberapa metode, yaitu observasi langsung di unit PTIPD dan LPPM Universitas XYZ, wawancara semi-terstruktur dengan pengelola sistem, serta distribusi survei kepada responden yang telah ditentukan menggunakan RACI Chart. Observasi bertujuan untuk memperoleh pemahaman mengenai pelaksanaan operasional sistem KKN di lapangan, sedangkan wawancara digunakan untuk mengeksplorasi aspek teknis dan kebijakan internal yang belum terdokumentasi secara formal. Adapun kuesioner dirancang untuk mengevaluasi tingkat pencapaian kapabilitas proses pada domain APO12 dan APO13 secara kuantitatif [8]

5. Evaluasi

Data hasil pengisian kuesioner selanjutnya dianalisis menggunakan pendekatan Process Assessment Model (PAM). Skor yang diperoleh diklasifikasikan ke dalam empat kategori pencapaian, yakni: Not Achieved (0–15%), Partially Achieved (15–50%), Largely Achieved (50–85%), dan Fully Achieved (85–100%). Persentase yang diperoleh selanjutnya dikonversikan ke dalam level kapabilitas proses saat ini. Untuk mengetahui selisih antara kondisi eksisting dan target yang diharapkan, dilakukan analisis kesenjangan atau GAP Analysis. Proses evaluasi ini difokuskan untuk menghasilkan penilaian yang obyektif atas kondisi aktual kematangan tata kelola TI, serta menyusun rekomendasi strategis yang mendukung perbaikan berkesinambungan. [9]

6. Dokumentasi

Tahap akhir dalam rangkaian penelitian ini adalah menyusun dokumentasi hasil evaluasi dalam bentuk laporan ilmiah. Laporan tersebut mencakup seluruh rangkaian aktivitas yang telah dilakukan, mulai

dari identifikasi permasalahan, perencanaan strategi, proses pengumpulan data, hingga analisis evaluatif dan penyusunan rekomendasi. Diharapkan dokumen ini dapat menjadi referensi utama bagi pihak kampus dalam merancang kebijakan pengembangan sistem informasi KKN secara lebih terarah, terstruktur, dan berkelanjutan.

HASIL DAN PEMBAHASAN

Setelah proses pengukuran kapabilitas dilakukan, langkah selanjutnya adalah menganalisis hasil yang diperoleh serta merumuskan rekomendasi strategis yang dapat diimplementasikan oleh pengelola sistem informasi di Universitas XYZ. Evaluasi ini bertujuan untuk mengidentifikasi aspek-aspek yang menjadi kekuatan maupun kelemahan dalam praktik manajemen risiko dan keamanan informasi, khususnya pada domain APO12 dan APO13. Temuan evaluasi ini harapannya menjadi dasar perbaikan yang berkelanjutan guna meningkatkan kualitas tata kelola teknologi informasi. Pelaksanaan rekomendasi menjadi tanggung jawab unit-unit terkait, terutama bagian pengelola sistem seperti PTIPD dan LPPM.

Adapun hasil pengukuran pada domain APO12 (Managed Risk) menunjukkan bahwa Level 1 dan Level 2 masuk dalam kategori *Partially Achieved*, masing-masing dengan capaian sebesar 21,88% dan 22,50%. Sementara itu, level kapabilitas 3 hingga 5 belum tercapai karena hanya memperoleh skor 17,36%, 14,58%, dan 12,50% secara berurutan. Hasil ini menunjukkan bahwa sebagian aktivitas pengelolaan risiko telah dijalankan, namun belum terdokumentasi secara formal dan masih belum mengacu pada prosedur standar yang terstruktur. Dengan demikian, proses manajemen risiko yang berjalan selama ini masih bersifat intuitif dan belum sistematis sepenuhnya.

Tabel 5. Hasil Kuesioner Domain APO12

Process Name	**APO12 (Manage Risk)**				
Level	**Level 1**	**Level 2**	**Level 3**	**Level 4**	**Level 5**
Rating By Percentage	21,88	22,50	17,36	14,58	12,50
Rating by Criteria	P	P	N	N	N
Capability Level Percentage Achieved	21,88	22,50	17,36	1X4,58	12,50
Status	Tercapai Sebagian	Tercapai Sebagian	Tidak Tercapai	Tidak Tercapai	Tidak Tercapai

Pada domain APO13 (Managed Security), hanya Level 1 yang berada dalam kategori *Partially Achieved* dengan skor 16,67%. Sementara itu, level kapabilitas 2 hingga 5 belum tercapai, dengan persentase berturut-turut sebesar 14,50%, 14,67%, 13,58%, dan 9,50%. Hasil ini mencerminkan bahwa penerapan pengelolaan keamanan informasi di lingkungan sistem KKN masih dilakukan secara tidak terstruktur dan cenderung bersifat insidental. Belum terdapat kebijakan keamanan formal maupun sistem perlindungan informasi yang diimplementasikan secara komprehensif. Selain itu, dokumentasi terkait kontrol keamanan serta evaluasi risiko keamanan juga belum tersedia, yang mengindikasikan lemahnya tata kelola dalam aspek proteksi informasi digital.

Tabel 6. Hasil Kuesioner Domain APO13

Process Name	**APO13 (Manage Risk)**				
Level	**Level 1**	**Level 2**	**Level 3**	**Level 4**	**Level 5**
Rating By Percentage	16,67	14,50	14,67	13,58	9,50
Rating by Criteria	P	N	N	N	N
Capability Level Percentage Achieved	16,67	14,50	14,67	13,58	9,50

NIVEDITA JOURNAL INFORMATICS
ISSN 3089-8366
(Media Online)
Vol. 01, No. 2, Juni 2025

Process Name	APO13 (Manage Risk)				
Level	**Level 1**	**Level 2**	**Level 3**	**Level 4**	**Level 5**
Status	Tercapai Sebagian	Tidak Tercapai	Tidak Tercapai	Tidak Tercapai	Tidak Tercapai

Evaluasi dilakukan melalui serangkaian tahapan metodologis yang saling mendukung dan berkesinambungan. Kajian literatur menjadi dasar utama dalam merancang instrumen evaluasi yang digunakan dalam penelitian ini. Fokus penelitian diarahkan secara spesifik pada domain APO12 dan APO13, guna memastikan bahwa kajian tetap relevan terhadap isu manajemen risiko dan keamanan data. Penilaian kapabilitas mengacu pada model PAM, dimana hasilnya berupa data numerik yang dipakai untuk membandingkan kondisi sekarang dengan tingkat kapabilitas yang diinginkan.

Evaluasi ini memanfaatkan data yang dikumpulkan melalui kuesioner, yang diisi oleh dua perwakilan dari PTIPD—yakni dari Divisi Aplikasi dan Divisi Server—yang berperan langsung dalam operasional sistem KKN.

1. Pembahasan Capality Level

A. Analisis Capablity Level APO12

Domain APO12 (Manage Risk) memiliki peran penting dalam memastikan bahwa pengelolaan risiko teknologi informasi terintegrasi secara optimal dengan sistem manajemen risiko organisasi secara keseluruhan atau dikenal sebagai Enterprise Risk Management. Berdasarkan hasil evaluasi, domain ini mencapai Level 2 dalam kapabilitas proses, sementara target yang ditetapkan adalah Level 3, sehingga terdapat gap sebesar satu tingkat antara kondisi aktual dan yang diharapkan.Temuan ini menunjukkan bahwa sebagian proses pengelolaan risiko telah diimplementasikan, namun belum terdokumentasi secara resmi dan belum mengacu pada sistem klasifikasi risiko yang standar. Selain itu, belum tersedia skenario risiko yang dapat dijadikan pedoman dalam pengambilan keputusan manajerial. Minimnya dokumentasi dan ketidakteraturan dalam penerapan proses berisiko menurunkan efektivitas pengelolaan risiko dalam sistem informasi [10]

Tabel 7. GAP Capability Level APO12

Nama Domain	Level Saat Ini	Level Target	GAP
APO12 (Managed Risk)	2	3	1

B. Analisis Capablity Level APO13

Domain APO13 (Managed Security) memiliki fokus utama pada perlindungan aset informasi melalui penerapan kebijakan, pengendalian, dan prosedur keamanan yang terstruktur. Berdasarkan hasil evaluasi, kapabilitas yang dicapai oleh domain ini berada pada Level 1, sedangkan level yang ditargetkan adalah Level 2, sehingga terdapat GAP sebesar satu tingkat. Meskipun beberapa inisiatif pengelolaan keamanan informasi telah dilakukan secara mendasar, namun masih belum tersedia kebijakan formal yang mendokumentasikan praktik tersebut. Ruang lingkup sistem juga belum terdefinisi secara jelas, dan belum terdapat mekanisme komunikasi yang resmi terkait kontrol keamanan yang diterapkan. Ketiadaan dokumentasi serta kurangnya sosialisasi terhadap aspek keamanan informasi menjadi faktor utama yang menghambat peningkatan kapabilitas pada domain ini [11].

Tabel 8. GAP Capability Level APO13

Nama Domain	Level Saat Ini	Level Target	GAP
APO13 (Managed Security)	1	2	1

2. Rekomendasi

Menurut hasil dari evaluasi capability level pada domain APO12 dan APO13, berikut ini disusun rekomendasi yang dapat digunakan oleh sistem KKN Universitas XYZ untuk meningkatkan tingkat kapabilitas sistem pengelolaan risiko dan keamanan informasi:

Berdasarkan hasil evaluasi terhadap tingkat kapabilitas proses dalam domain APO12 dan APO13, berikut dirumuskan sejumlah rekomendasi strategis yang dapat diterapkan oleh pengelola sistem informasi KKN Universitas XYZ untuk meningkatkan efektivitas tata kelola risiko dan keamanan informasi:

A. *APO12 – Managed Risk*

1. Melakukan pemetaan menyeluruh terhadap berbagai potensi risiko TI yang dapat memengaruhi operasional layanan digital KKN.
2. Menyusun dokumen resmi terkait prosedur identifikasi dan analisis risiko, baik yang berasal dari internal sistem (Divisi Aplikasi dan Server) maupun dari sisi pengguna eksternal.
3. Menyediakan dokumentasi standar yang memuat skenario risiko utama beserta strategi mitigasi dan rencana kesinambungan layanan apabila gangguan terjadi.
4. Meningkatkan kapasitas dan ketahanan infrastruktur TI untuk mendukung sistem deteksi dini terhadap ancaman dan kerentanan yang bersifat berulang.
5. Melaksanakan penilaian risiko secara periodik yang dikaitkan dengan proses bisnis KKN, dengan melibatkan pemangku kepentingan internal maupun pengguna sistem.

B. *APO13 – Managed Security*

1. Merancang dan menerapkan kebijakan keamanan informasi secara formal dengan mengacu pada standar internasional seperti ISO/IEC 27001.
2. Mengidentifikasi dan memetakan berbagai jenis ancaman terhadap keamanan informasi, baik dari sumber eksternal seperti serangan siber, maupun dari risiko internal seperti *insider threats* dan kebocoran data.
3. Menerapkan sistem pengendalian akses berbasis otorisasi serta penggunaan enkripsi guna menjaga kerahasiaan dan integritas data pengguna.
4. Menyelenggarakan program pelatihan dan peningkatan kapasitas di bidang keamanan informasi secara rutin bagi seluruh pihak yang terlibat dalam pengelolaan maupun penggunaan sistem.
5. Mengimplementasikan sistem manajemen informasi dan kejadian secara real-time, seperti SIEM (Security Information and Event Management), untuk meningkatkan responsivitas terhadap insiden keamanan yang terjadi.

KESIMPULAN

Berdasarkan hasil analisis penerapan pengelolaan risiko dan keamanan informasi pada sistem KKN Universitas XYZ menggunakan kerangka kerja COBIT 2019, diketahui bahwa implementasi kedua domain yang dievaluasi belum sepenuhnya mencapai tingkat kapabilitas yang ditargetkan. Pada domain APO12 (Managed Risk), tingkat pencapaian berada di Level 2 dengan status *partially achieved*, yang mengindikasikan bahwa proses manajemen risiko telah dijalankan, namun masih kekurangan dokumentasi pendukung secara menyeluruh. Belum menggunakan klasifikasi risiko yang sistematis, dan belum memiliki skenario mitigasi risiko sebagai pedoman operasional.

Sementara itu, domain APO13 (Managed Security) hanya mencapai Level 1, yang mencerminkan bahwa pengelolaan keamanan informasi masih bersifat tidak sistematis, belum memiliki dokumentasi formal, serta belum dilengkapi dengan mekanisme pemantauan yang berjalan secara konsisten. Pencapaian ini masih berada di bawah target kapabilitas yang telah ditentukan, yaitu Level 3 untuk APO12 dan Level 2 untuk APO13. Untuk mencapai tingkat yang diharapkan tersebut, diperlukan penerapan proses yang terdokumentasi dengan baik, distandarkan, serta dilaksanakan secara berkesinambungan dengan dukungan dari kebijakan dan prosedur formal yang jelas.

Penelitian ini juga mengidentifikasi beberapa area yang perlu ditingkatkan, di antaranya: penyusunan kebijakan formal terkait pengelolaan risiko dan keamanan informasi, penyusunan dokumentasi risiko dan ancaman secara sistematis, perancangan skenario mitigasi risiko, serta pelaksanaan proses pemantauan risiko secara berkala.

Dengan menerapkan rekomendasi yang telah disusun sebelumnya, sistem KKN di Universitas XYZ diharapkan dapat meningkatkan efektivitas pengelolaan risiko dan keamanan informasi. Ini juga akan mendukung pencapaian tingkat kapabilitas yang lebih optimal dan memperkuat keberlangsungan layanan digital secara profesional, aman, dan berorientasi jangka panjang, sesuai dengan prinsip-prinsip tata kelola teknologi informasi yang ada di COBIT 2019.

DAFTAR PUSTAKA

[1] M. Rahmawita Munzir, N. Khaira, P. Studi Sistem Informasi, F. H. Sains dan Teknologi UIN Suska Riau Jl Soebrantas KM, and P. Pekanbaru -Riau, "EVALUASI KEBERHASILAN IMPLEMENTASI SISTEM INFORMASI MANAJEMEN KULIAH KERJA NYATA MENGGUNAKAN METODE HOT FIT," *Jurnal Ilmiah Rekayasa dan Manajemen Sistem Informasi*, vol. 6, no. 1, pp. 100–108, 2020.

[2] D. Darmawan and A. F. Wijaya, "Analisis dan Desain Tata Kelola Teknologi Informasi Menggunakan Framework COBIT 2019 pada PT. XYZ," 2022. [Online]. Available: https://journal-computing.org/index.php/journal-cisa/index

[3] I. Malah *et al.*, "PERANCANGAN SISTEM ABSENSI, TRACKING GURU DAN SISWA DI SEKOLAH MENENGAH KEJURUAN," 2022.

[4] L. N. Amali, M. R. Katili, and S. Suhada, "Core model of information technology governance system design in local government," *Telkomnika (Telecommunication Computing Electronics and Control)*, vol. 21, no. 4, pp. 750–761, Aug. 2023, doi: 10.12928/TELKOMNIKA.v21i4.24287.

[5] A. Tantiono and D. Legowo, "Information System Governance in Higher Education Foundation using COBIT 5 Framework," *International Journal of Recent Technology and Engineering (IJRTE)*, vol. 8, pp. 2798–2811, Mar. 2020, doi: 10.35940/ijrte.F8192.038620.

[6] ISACA, *COBIT 2019 Framework Governance and Management Objectives*. 2019.

[7] Siti Aminah, Munirul Ula, and Mutammimul Ula, "PENGUKURAN TINGKAT KEMAMPUAN (CAPABILITY LEVEL) TATA KELOLA TEKNOLOGI INFORMASI PADA PERPUSTAKAAN UNIVERSITAS MALIKUSSALEH MENGGUNAKAN FRAMEWORK COBIT 5 DOMAIN APO (ALIGN, PLAN AND ORGANIZE)," 2020.

[8] A. Andri Yantama, A. Mesha Putri, S. Arum Wulandari, and P. Studi Sistem Informasi, "SEMINAR NASIONAL AMIKOM SURAKARTA (SEMNASA) 2023 Audit Keamanan Sistem Informasi PERJADIN BKKBN Provinsi Riau Menggunakan COBIT 19: APO12 dan APO13".

[9] C. Wijaya, M. Sukamto, and R. Yunis, "Audit Tata Kelola TI Menggunakan COBIT 2019 Domain APO-12 Pada Universitas Mikroskil," *Jurnal Sifo Mikroskil (JSM)*, vol. 24, no. 2, pp. 1–5, doi: 10.55601/jsm.24i2.pg.

[10] M. Audrilia and A. Budiman, "Perancangan Sistem Informasi Manajemen Bengkel Berbasis Web (Studi Kasus : Bengkel Anugrah)," *Jurnal Madani : Ilmu Pengetahuan, Teknologi, dan Humaniora*, vol. 3, no. 1, pp. 1–12, Mar. 2020, doi: 10.33753/madani.v3i1.78.

[11] A. Fitri, K. Parinduri, and J. Hartono, "Evaluasi Penerapan Tata Kelola Teknologi Informasi (TI) Menggunakan Framework Cobit 2019 (Studi Kasus pada Perguruan Tinggi Harapan Maju)," 2023.