NIVEDITA JOURNAL INFORMATICS
e-ISSN : xxx-xxx
p-ISSN : xxx-xxx

Vol. 01, No. 1, Desember 2024

EVALUASI MANAJEMEN RISIKO TI PADA PERGURUAN TINGGI XYZ MENGGUNAKAN *FRAMEWORK* COBIT 2019 DOMAIN APO12 DAN APO13

Muhammad Nazaruddin Marpaung [1], Aditya Nugraha Yesa[2], Muhamad Nur Sarifudin[3], Megawati[4]

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

email: [1] 112150310030@students.uin-suska.ac.id, [2] l2150322141@students.uin-suska.ac.id, [3] l2150322141@students.uin-suska.ac.id, [4] megawati@uin-suska.ac.id

Abstract

Information technology risks can impact data security, privacy, and organizational operations, including at XYZ University, posing challenges in managing risks and ensuring the security of IT services. This study identifies issues related to IT risk management that are not systematically documented at the IT Service Unit (UPT TIK) of XYZ University. The COBIT 2019 framework was selected because it provides a structured approach to evaluating risk management (APO12) and information security (APO13). This framework is relevant for higher education institutions facing challenges in IT governance. This research aims to evaluate the implementation of IT risk management at the IT Service Unit of XYZ University using the COBIT 2019 framework, focusing on the APO12 (Manage Risk) and APO13 (Manage Security) domains. The research methodology includes observations, interviews, and questionnaires to assess the institution's readiness in identifying, managing, and mitigating IT risks. The evaluation results from the capability calculation show that the capability levels in the APO12 and APO13 domains are at level 1, where risk management and information security processes are still carried out ad-hoc without systematic documentation. To reach level 2, formal organization and documentation of related policies and procedures are required, along with the implementation of recommended strategic actions.

Keywords: *COBIT 2019, APO12, APO13, IT Risk Management*

Abstrak

Risiko teknologi informasi dapat berdampak pada keamanan data, privasi, dan operasional organisasi, termasuk di Perguruan Tinggi XYZ, menghadirkan tantangan dalam pengelolaan risiko dan keamanan layanan TI. Penelitian ini mengidentifikasi permasalahan terkait manajemen risiko TI yang tidak terdokumentasi secara sistematis di UPT TIK Perguruan Tinggi XYZ. *Framework* COBIT 2019 dipilih karena menyediakan pendekatan terstruktur untuk mengevaluasi pengelolaan risiko (APO12) dan keamanan informasi (APO13). Framework ini relevan untuk organisasi pendidikan tinggi yang menghadapi tantangan dalam tata kelola TI. Penelitian ini bertujuan mengevaluasi penerapan manajemen risiko TI di UPT TIK Perguruan Tinggi XYZ berdasarkan framework COBIT 2019, dengan fokus pada domain APO12 (*Manage Risk*) dan APO13 (*Manage Security*). Metodologi penelitian mencakup observasi, wawancara, dan penyebaran kuesioner untuk menilai tingkat kesiapan institusi dalam mengidentifikasi, mengelola, dan mengatasi risiko TI. Hasil evaluasi dari perhitungan *capability* menunjukkan bahwa tingkat kemampuan pada domain APO12 dan APO13 berada di level 1, di mana proses manajemen risiko dan keamanan informasi masih dilakukan secara ad-hoc tanpa dokumentasi yang sistematis. Untuk mencapai level 2, diperlukan pengorganisasian dan dokumentasi formal terhadap kebijakan dan prosedur terkait, serta implementasi langkah-langkah strategis yang direkomendasikan.

Kata kunci: COBIT 2019, APO12, APO13, *IT Risk Management*

Diajukan: 11 Desember 2024; Diterima: 27 Januari 2025;

PENDAHULUAN

Risiko teknologi informasi dapat berdampak pada keamanan data, privasi, dan operasional organisasi [1]. Di Perguruan Tinggi XYZ, untuk mengamankan akan hal ini diperlukan bagian khusus yang mengelolanya, peran ini dipegang oleh dan Pangkalan Data atau UPT TIK, yang bertanggung jawab memastikan bahwa infrastruktur TI dapat beroperasi dengan andal dan aman untuk mendukung kebutuhan seluruh pemangku kepentingan [2]. Namun, seiring dengan meningkatnya kompleksitas teknologi, risiko-

risiko yang dapat mempengaruhi efektivitas dan keberlanjutan layanan TI pun turut bertambah, seperti gangguan operasional, ancaman siber, dan kegagalan sistem. Maka dari itu penting untuk menerapkan manajemen risiko yang kuat agar dapat mengelola risiko yang mungkin muncul dan meminimalkan dampak negatif yang timbul [3].

Dalam mengelola risiko-risiko tersebut, framework COBIT *(Control Objectives for Information and Related Technologies)* 2019 merupakan salah satu kerangka kerja yang sangat relevan dan komprehensif [3]. COBIT 2019 dirancang oleh ISACA sebagai panduan dalam tata kelola dan manajemen TI yang dapat membantu organisasi dalam mencapai tujuan strategisnya. Framework ini menyelaraskan aspek-aspek kontrol dan manajemen risiko TI sehingga dapat meningkatkan keandalan dan keamanan layanan TI. Di dalam *framework* COBIT 2019, domain-domain APO12 *(Manage Risk)* dan APO13 *(Manage Security)* adalah area yang berfokus pada manajemen risiko dan pengelolaan keamanan informai [1]. Domain APO12 memberikan pedoman dalam mengidentifikasi, menilai, dan menangani risiko TI, sementara APO13 lebih berfokus pada pengelolaan keamanan untuk melindungi sistem dari ancaman eksternal dan internal [4].

Manajemen risiko yang baik menjadi kunci dalam memastikan keberlangsungan layanan dan perlindungan terhadap informasi penting di dalam institusi [5]. Dengan implementasi yang tepat, *framework* COBIT 2019 dapat memberikan fondasi yang kokoh untuk meningkatkan kemampuan organisasi dalam merespon risiko dan ancaman terhadap sistem TI [3]. Penerapan yang efektif dari APO12 akan memungkinkan UPT TIK Perguruan Tinggi XYZ untuk mengidentifikasi risiko mengimplementasikan diperlukan. Sementara secara tindakan itu, proaktif mitigasi dan yang penerapan APO13 mendukung keamanan data serta informasi yang tersimpan pada suatu sistem, sehingga menekan potensi ancaman keamanan yang dapat membahayakan integritas data maupun reputasi institusi [6].

Melalui evaluasi ini, Penelitian ini bertujuan untuk menganalisis sejauh mana implementasi manajemen risiko TI di UPT TIK Perguruan Tinggi XYZ dilakukan telah sesuai dengan standar yang ada dalam COBIT 2019. Evaluasi ini mencakup penilaian terhadap kebijakan, prosedur, serta langkah-langkah manajemen risiko yang telah diambil oleh UPT TIK. Dengan fokus pada domain APO12 dan APO13, Penelitian ini diharapkan mampu memberikan pemahaman yang lebih mendalam tentang tingkat kesiapan UPT TIK Perguruan Tinggi XYZ dalam mengelola risiko-risiko yang mungkin timbul, serta identifikasi area yang memerlukan perbaikan dan penguatan [7].

Melalui evaluasi ini, penelitian ini bertujuan untuk menganalisis sejauh mana implementasi manajemen risiko TI di UPT TIK Perguruan Tinggi XYZ telah sesuai dengan standar yang ditetapkan dalam framework COBIT 2019. Evaluasi ini mencakup penilaian terhadap kebijakan, prosedur, serta langkah-langkah manajemen risiko yang telah diambil oleh UPT TIK. Dengan menitikberatkan pada domain APO12 dan APO13, penelitian ini diharapkan dapat memberikan wawasan yang lebih mendalam mengenai tingkat kesiapan UPT TIK Perguruan Tinggi XYZ dalam mengelola risiko-risiko yang mungkin muncul, serta mengidentifikasi area yang memerlukan perbaikan dan peningkatan. Pada penelitian Verdila et al. (2024) melakukan evaluasi manajemen risiko teknologi informasi di lingkungan perguruan tinggi menggunakan framework COBIT 2019 dengan fokus pada domain EDM03 dan APO12. Meskipun penelitian tersebut berfokus pada tata kelola teknologi informasi secara umum, aspek manajemen keamanan informasi yang terdapat pada domain APO13 belum menjadi perhatian utama. Selanjutnya, penelitian Rajjani et al. (2021) menganalisis manajemen risiko teknologi informasi pada sektor industri, yakni Department of ICT PT Semen Indonesia, dengan menggunakan domain EDM03 dan APO12. Namun, penelitian tersebut tidak mempertimbangkan konteks institusi pendidikan yang memiliki kebutuhan dan tantangan berbeda dibandingkan sektor industri.

Penelitian ini berfokus terhadap implementasi manajemen risiko TI yang mencakup aspek keamanan informasi di lingkungan institusi pendidikan tinggi, khususnya di UPT TIK Perguruan Tinggi XYZ. Dengan menitikberatkan pada domain APO12 dan APO13, penelitian ini memberikan kontribusi yang signifikan dalam mengkaji implementasi tata kelola risiko TI dan keamanan informasi secara mendalam pada institusi pendidikan. Hal ini diharapkan dapat mendukung pengembangan tata kelola teknologi informasi yang lebih terstruktur dan terorganisasi sesuai dengan standar yang telah ditetapkan.

Hasil dari penelitian ini diharapkan mampu memberikan rekomendasi yang aplikatif pada UPT TIK Perguruan Tinggi XYZ dalam meningkatkan tata kelola dan manajemen risiko TI, sehingga mampu menghadapi tantangan ke depan dengan lebih efektif. Selain itu, penelitian ini juga dapat sebagai acuan bagi institusi pendidikan tinggi lainnya yang menghadapi tantangan serupa dalam manajemen risiko TI [3]. Dengan adanya evaluasi ini, UPT TIK Perguruan Tinggi XYZ dapat mengambil langkah langkah strategis untuk memperkuat keamanan informasi dan meningkatkan keandalan infrastruktur TI guna mendukung pencapaian tujuan akademik dan operasional yang lebih optimal [3].

METODE

Adapun langkah dan tahapan yang dilakukan pada penelitian ini dapat dilihat melalui skema alir pada Gambar. Tahapan dimulai dari perencanaan dan berakhir hingga dokumentasi.

Gambar 1 Metodologi Penelitian

1. Studi Pustaka

Studi pustaka merupakan aktivitas mengumpulkan, mempelajari, dan menganalisis berbagai literatur yang relevan dan terbaru. Tujuannya adalah memahami konsep, teori, serta temuan sebelumnya yang terkait dengan topik penelitian, sekaligus mengidentifikasi celah atau kelemahan dalam penelitian terdahulu.

2. Penentuan Domain

Domain dipilih berdasarkan topik penelitian. Pada penelitian kali ini domain pada framework COBIT 2019 yang dipilih yaitu APO12 *(Managed Risk)* dan APO13 *(Managed Security).* Kuesioner ditetapkan berdasarkan domain dan subdomain masing-masing.

2.1 APO12

Domain APO12, yang disebut *(Managed Risk)*, membahas tentang integrasi manajemen risiko terkait TI dengan manajemen risiko perusahaan secara keseluruhan (ERM). Domain ini juga menyoroti perlunya menyeimbangkan antara biaya dan manfaat dalam pengelolaan risiko TI perusahaan[3].

Tabel 1. APO12

Domain APO12 : Managed Risk	
APO12.01	Mengumpulkan data
APO12.02	Analisis risiko
APO12.03	Memepertahankan profil risiko
APO12.04	Mengartikulasikan risiko
APO12.05	Mendefinisikan portofolio tindakan manajemen risiko
APO12.06	Menanggapi risiko

2.2 APO13

Dalam framework COBIT 2019 adalah salah satu domain yang fokus pada pengelolaan keamanan informasi, yang disebut juga sebagai Manage Security [8]. Domain ini dirancang untuk membantu organisasi mengidentifikasi, mengelola, dan mengamankan aset informasi agar terlindung dari ancaman internal maupun eksternal [3].

Tabel 2. APO12

Domain APO13 : Managed Security	
APO13.01	Membangun dan memelihara sistemmanajemen keamanan informasi
APO13.02	Menentukan dan mengelola perawatanrisiko keamanan dan privasi keamanan dan privasi informasi
APO13.03	Memantau dan meninjau sistem manajemen keamanan informasi

3. Penentuan Responden

Jumlah responden ditentukan menggunakan RACI Chart. Berdasarkan ISACA (2018) dalam buku *COBIT 2019: Governance and Management Objectives*, RACI *(Responsible, Accountable, Consulted, Informed)* adalah matriks yang menjelaskan tingkat tanggung jawab, peran, dan akuntabilitas dalam struktur organisasi, baik untuk bisnis maupun TI. Responden yang memenuhi kriteria akan diberikan kuesioner penilaian. Berdasarkan RACI *chart* yang telah dirancang, kami mengambil Div. Server & Keamanan Data dan Div. Infrasytruktur & Jaringan sebagai responden untuk proses evaluasi dikarenakan perannya sebagai responsible.

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

Tabel 3. RACI *Chart* APO12

APO12	Kepala PTIPD	Div. Tata Kelola Layanan Umum	Div. Tata Kelola Manajemen Keuangan	Div. Pusat Layanan Umum & Helpdesk C3	Div. Aplikasi &Data	Div. Server & Keamanan Data	Div. Infrasytruktur &Jaringan
Mengidentifikasi dan mengumpulkan data yang relevan	A	I	C	I	C	R	R
Menganalisis resiko	A	I	C	I	C	R	R
Mempertahankan prodil risiko	A	I	C	I	C	R	R
Mengartikulasi risiko	A	I	C	I	C	R	R
Menentukan dan mengelola portofolio tindakan manajemen risiko	A	I	C	I	C	R	R
Menanggapi risiko	A	I	C	I	C	R	R

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

Tabel 4. RACI *Chart* APO13

APO12	Kepala PTIPD	Div. Tata Kelola Layanan Umum	Div. Tata Kelola Manajemen Keuangan	Div. Pusat Layanan Umum & Helpdesk C3	Div. Aplikasi &Data	Div. Server & Keamanan Data	Div. Infrasytruktur &Jaringan
Membangun dan memelihara system manajemen keamanan informasi	A	I	C	I	C	R	R
Menentukan dan mengelola perawatan risiko keamanan dan privasi keamanan dan privasi informasi	A	I	C	I	C	R	R
Memantau dan meninjau sistem manajemen keamanan informasi	A	I	C	I	C	R	R

4. Pengumpulan Data

Penelitian ini menggunakan dua jenis data, yaitu data primer dan data sekunder.

A. Data Primer

Data primer diperoleh langsung dari lapangan melalui observasi, wawancara, dan penyebaran kuesioner kepada UPT TIK. Berikut penjelasan tahapan pengumpulan data primer:

- Observasi

Observasi dilakukan di UPT TIK Perguruan Tinggi XYZ dengan pendekatan observasi *non*-partisipan, di mana peneliti hanya bertindak sebagai pengamat tanpa terlibat dalam aktivitas yang diamati.

- Wawancara
  Wawancara dilaksanakan dengan pertanyaan yang berfokus pada tugas, tanggung jawab, fungsi utama divisi, serta strategi dan tujuan perusahaan.
- Kuesioner
  Kuesioner berupa pertanyaan tertulis diberikan kepada responden. Pertanyaan disusun berdasarkan *framework* COBIT 2019, sesuai domain yang dibahas. Kuesioner mencakup berbagai aktivitas di setiap level, yang disusun sesuai panduan dalam buku COBIT 2019: *Governance and Management Objectives.*

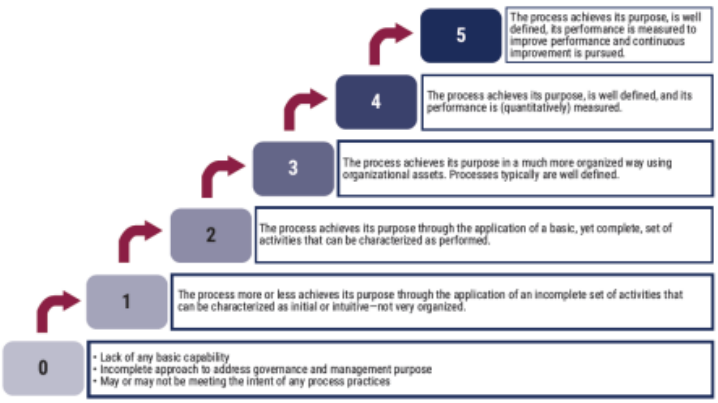
B. Data Sekunder

Data sekunder diperoleh melalui studi pustaka yang berkaitan dengan tata kelola teknologi informasi. Dalam penelitian ini, data sekunder berupa studi literatur.

- Studi Literatur
  Studi literatur dilakukan dengan mengkaji teori-teori yang relevan dengan evaluasi manajemen risiko dan tata kelola teknologi informasi, khususnya yang menggunakan kerangka kerja COBIT 2019. Sumber teori ini berasal dari buku, jurnal, *e-book*, serta penelitian-penelitian terdahulu yang mendukung penyusunan laporan ini.

5. Pengukuran Tingkat *Capability*

Untuk pengukuran pada penelitian ini mengguakan Tingkat kematangan atau *Capability Level* adalah alat yang digunakan untuk mengukur seberapa efektif manajemen risiko Teknologi Informasi diterapkan. Dengan menggunakan *capability*, kita dapat mengevaluasi posisi organisasi saat ini dan membandingkannya dengan posisi yang diinginkan di masa depan. [9].



Gambar 2. *Capability Level*

Dari kuesioner yang telah disebarkan, hasilnya kemudian dihitung untuk menganalisis *Capability Level* pada domain APO12 dan APO13. Penilaian *capability level* dibagi ke dalam empat kategori, yaitu:

1. N *(Not Achieved):* pencapaian antara 0% hingga 15%.
2. P *(Partially Achieved):* pencapaian lebih dari 15% hingga 50%.
3. L *(Largely Achieved):* pencapaian lebih dari 50% hingga 85%.
4. F *(Fully Achieved):* pencapaian lebih dari 85% hingga 100%.

6. Evaluasi dan Rekomendasi

Setelah pengukuran tingkat *capability* dilakukan, langkah berikutnya adalah melaksanakan evaluasi dan memberikan rekomendasi untuk UPT TIK Perguruan Tinggi XYZ. Hasil evaluasi dan rekomendasi ini diharapkan mampu membawa perubahan positif dan menghasilkan peningkatan yang signifikan untuk domain APO12 dan APO13 di Perguruan Tinggi XYZ. Implementasi rekomendasi tersebut menjadi tanggung jawab pihak-pihak terkait.

HASIL DAN PEMBAHASAN

Hasil evaluasi menunjukkan bahwa capability level pada APO12 dan APO13 masing-masing berada pada Level 1 dengan kategori, dengan aktivitas yang bersifat ad-hoc dan belum terdokumentasi. Evaluasi lebih lanjut mengungkapkan bahwa UPT TIK memerlukan peningkatan dalam dokumentasi dan implementasi kebijakan formal. Pada tahap metodologi, hasil tiap langkah dijabarkan sebagai berikut: Studi pustaka memberikan dasar teori yang kuat, penentuan domain memastikan fokus penelitian, dan analisis capability level menghasilkan rekomendasi yang terukur untuk peningkatan level kemampuan.

Berikut adalah hasil perhitungan kuesioner yang didapat dari 2 responden. Hasil ini berupa *capability level* pada tiap domain.

Tabel 5. Hasil Kuesioner Domain APO12

Domain APO12 Level 2						
Responden 1						
Pertanyaan	1	2	3	4	5	6
Kriteria Rentang	F	N				
Respoden 2						
Pertanyaan	1	2	3	4	5	6
Kriteria Rentang	F	N				

Hasil evaluasi menunjukkan bahwa aktivitas manajemen risiko di UPT TIK masih dilakukan secara ad-hoc, tanpa dokumentasi atau prosedur yang sistematis. Pada hasil kuesioner, responden 1 dan responden 2 menunjukkan distribusi nilai yang belum mencapai kategori "*Partially Achieved*" (P). Dengan demikian, domain APO12 berada pada Level 1, di mana aktivitas manajemen risiko TI hanya dilakukan secara intuitif dan belum terstruktur.

Tabel 6. Hasil Kuesioner Domain APO13

Domain APO13 Level 2			
Responden 1			
Pertanyaan	1	2	3
Kriteria Rentang	F	N	
Respoden 2			
Pertanyaan	1	2	3
Kriteria Rentang	F	N	

Hasil evaluasi pada domain APO13 mengungkapkan bahwa pengelolaan keamanan informasi juga bersifat ad-hoc, tanpa standar formal untuk mengelola risiko keamanan informasi. Hasil kuesioner dari kedua responden menunjukkan rentang nilai yang masih rendah, dengan sebagian besar aktivitas berada pada kategori "*Not Achieved*" (N). Hal ini menegaskan bahwa kemampuan pengelolaan keamanan informasi UPT TIK berada pada Level 1.

Dari hasil rekapitulasi 2 responden, objektif APO 12 dan APO13 Berada pada level 1 berarti tujuan dari APO12 dan APO13 belum tercapai secara optimal, karena aktivitas yang dilakukan masih tidak lengkap dan terorganisir dengan baik, serta lebih bersifat sebagai langkah awal atau dilakukan secara intuitif.

1. Pembahasan Capability Level

A. Analisis Capability Level APO12

Domain APO12 yang bernama (*Managed Risk)* berfokus pada penilaian bagaimana manajemen risiko TI selaras dengan manajemen risiko perusahaan secara menyeluruh. (*Enterprise Risk Management* - ERM). Domain ini juga bertujuan untuk menyeimbangkan biaya *(cost)* dengan manfaat *(benefit)* dalam pengelolaan risiko TI [10].

Hasil penilaian *capability level* untuk domain APO12 adalah Level 1. Pada level ini, proses dalam domain telah mulai diterapkan, serta sejumlah aktivitas mendasar tang telah dilaksanakan untuk memenuhi tujuan dasar domain ini. Namun, aktivitas yang dilakukan belum terstruktur, terdokumentasi dengan baik, atau terorganisasi secara formal [11].

Tabel 7. *Gap Capability* APO12

Nama Domain	Level Saat ini	Level Target	Gap
APO12 *(Managed Risk)*	1	2	1

B. Analisis Capability Level APO13

Domain APO13 yang bernama (*Managed Security)* berfokus pada manajemen keamanan informasi untuk melindungi aset organisasi, memastikan integritas *(availability)* mencakup kerahasiaan *(integrity)*, dari informasi. pengelolaan *(confidentiality),* dan risiko ketersediaan Domain ini keamanan, pemantauan ancaman, serta penerapan langkah langkah pencegahan dan mitigasi [12].

Hasil penilaian capability level untuk domain APO13 adalah Level 1. Pada level ini, proses keamanan telah mulai dilakukan, dan serangkaian aktivitas dasar telah diterapkan. Namun, aktivitas tersebut masih bersifat ad-hoc, tidak terdokumentasi secara formal, dan belum dilakukan secara konsisten. Hal ini menunjukkan bahwa manajemen keamanan informasi belum sepenuhnya terintegrasi organisasi. ke dalam proses organisasi .

Tabel 8. *Gap Capability* APO13

Nama Domain	Level Saat ini	Level Target	Gap
APO13 *(Managed Security)*	1	2	1

2. Rekomendasi

Berdasarkan hasil evaluasi manajemen risiko teknologi informasi di Perguruan Tinggi XYZ menggunakan analisis *capability level*, disusun beberapa rekomendasi untuk mengembangkan dan memperbaiki penerapan manajemen risiko TI serta mengurangi risiko yang mungkin terjadi. Berikut adalah rekomendasi yang telah disusun berdasarkan masing-masing objektif yang akan disampaikan kepada UPT. TIK Perguruan Tinggi XYZ.

A. APO12 *(Managed Risk)*

1. UPT TIK Perguruan Tinggi XYZ diharapkan mampu mengidentifikasi dan mendokumentasikan secara menyeluruh berbagai sumber risiko TI di Perguruan Tinggi XYZ, sehingga mampu mendukung keberhasilan operasional keberlanjutan layanan serta teknologi informasi.
2. UPT TIK Perguruan Tinggi XYZ disarankan menyusun dokumen skema identifikasi dan analisis risiko TI yang terbagi menurut ruang lingkup internal dan eksternal. Dokumen ini dapat memberikan gambaran yang lebih jelas dalam mengelola risiko dan menentukan langkah mitigasi yang tepat.
3. UPT TIK Perguruan Tinggi XYZ diharapkan untuk mengembangkan infrastruktur TI yang diperlukan untuk memahami tingkat kerentanan serta kemampuan layanan komponen infrastruktur dari TI setiap guna mendukung penyelesaian permasalahan yang muncul.
4. UPT TIK Perguruan Tinggi XYZ disarankan untuk melakukan pemetaan skenario terkait potensi ancaman risiko TI. Hal ini bertujuan untuk meningkatkan kesiapan Perguruan Tinggi XYZ dalam menghadapi risiko yang mungkin terjadi di masa depan.
5. UPT TIK Perguruan Tinggi XYZ didorong untuk melakukan evaluasi berkala terhadap risiko-risiko yang teridentifikasi serta dampaknya pada proses bisnis dan layanan, sehingga tindakan mitigasi dapat disesuaikan secara dinamis.

B APO13 *(Managed Security)*

1. UPT TIK Perguruan Tinggi XYZ disarankan untuk menyusun kebijakan keamanan informasi yang berbasis standar internasional, seperti ISO/IEC 27001, agar tata kelola keamanan informasi dapat dilaksanakan secara efektif dan konsisten.
2. UPT TIK Perguruan Tinggi XYZ diharapkan melakukan identifikasi dan penilaian terhadap potensi ancaman keamanan informasi, termasuk serangan siber, akses tidak sah, dan kebocoran data. Hasil penilaian ini dapat digunakan sebagai dasar perencanaan mitigasi risiko keamanan.
3. UPT TIK Perguruan Tinggi XYZ disarankan untuk mengimplementasikan kontrol akses berbasis peran *(role-based access control)* dan enkripsi data untuk melindungi aset informasi penting dari ancaman internal maupun eksternal.
4. UPT TIK Perguruan Tinggi XYZ diharapkan untuk mengembangkan program edukasi keamanan informasi yang ditujukan kepada staf dan mahasiswa agar kesadaran terhadap pentingnya keamanan informasi dapat meningkat.
5. UPT TIK Perguruan Tinggi XYZ disarankan untuk mengadopsi sistem pemantauan keamanan secara real-time, seperti SIEM *(Security Information and Event Management),* guna mendeteksi dan merespons ancaman keamanan secara cepat dan efektif.

KESIMPULAN

Berdasarkan hasil penelitian evaluasi manajemen risiko teknologi informasi di UPT TIK Perguruan Tinggi XYZ, diperoleh kesimpulan bahwa Hasil evaluasi menunjukkan bahwa implementasi manajemen risiko TI di UPT TIK Perguruan Tinggi XYZ belum sepenuhnya sesuai dengan standar yang ada dalam framework COBIT 2019 yaitu, pertama APO12 (*Managed Risk*) berada pada level 1, di mana aktivitas manajemen risiko TI masih dilakukan secara intuitif, tidak terdokumentasi secara sistematis, dan proses identifikasi, analisis, serta mitigasi risiko dilakukan secara insidental tanpa standar yang jelas. Kedua APO13 (*Managed Security*) juga berada pada level 1, di mana langkah-langkah pengelolaan keamanan informasi bersifat ad hoc, tidak terorganisasi dengan baik, dan tidak terdokumentasi secara formal.

Berdasarkan evaluasi kebijakan, prosedur, serta langkah-langkah yang diambil oleh UPT TIK, penelitian ini menemukan bahwa tingkat kemampuan yang diharapkan pada domain APO12 dan APO13 adalah level 2. Pada level tersebut, manajemen risiko TI dan keamanan informasi harus terdokumentasi, terorganisasi, dan dilaksanakan secara konsisten berdasarkan standar serta prosedur yang jelas.

Penelitian ini berhasil mengidentifikasi beberapa area yang memerlukan perbaikan dan penguatan, termasuk Penyusunan kebijakan dan prosedur formal yang relevan dengan manajemen risiko TI dan keamanan informasi, Pendokumentasian risiko dan potensi ancaman secara sistematis untuk mendukung proses analisis dan mitigasi risiko serta Pemantauan risiko secara berkala serta peningkatan kesadaran akan pentingnya keamanan informasi di lingkungan UPT TIK.

Dengan rekomendasi yang telah diberikan, UPT TIK Perguruan Tinggi XYZ diharapkan dapat meningkatkan kesiapan institusional dalam mengelola risiko TI secara lebih efektif dan mencapai level kemampuan yang lebih tinggi pada domain APO12 dan APO13, sehingga mendukung keberlanjutan tata kelola teknologi informasi sesuai dengan standar COBIT 2019.

DAFTAR PUSTAKA

[1] J. S. A. Rajjani, B. T. Hanggara, dan Y. T. Musityo, "Evaluasi Manajemen Risiko Teknologi Informasi pada Department of ICT PT Semen Indonesia (Perseo) Tbk menggunakan Framework COBIT 2019 dengan Domain EDM03 dan APO12," *Jurnal Pengembangan Teknologi Informasi Dan Ilmu Komputer*, vol. 5, no. 5, hlm. 1734–1744, 2021.

[2] A. Fajri dan M. Affandes, "Analisis Manajemen Risiko TI Menggunakan Framework COBIT 5 Domain APO12 dan EDM03," *KLIK: Kajian Ilmiah Informatika dan Komputer*, vol. 4, no. 3, hlm. 1523–1530, 2023.

[3] C. Isaca, "Implementation Guide: Implementing and Optimizing an Information and Technology Governance Solution. 2018," 2019.

[4] A. Della Ariesta, S. Suprapto, dan A. R. Perdanakusuma, "Evaluasi Tata Kelola dan Manajemen Risiko Teknologi Informasi pada PT. MyECO Teknologi Nusantara menggunakan Framework COBIT 2019 Proses EDM03 dan APO12," *Jurnal Pengembangan Teknologi Informasi Dan Ilmu Komputer*, vol. 6, no. 12, hlm. 5736–5745, 2022.

[5] T. Alisya, H. Handayani, S. N. Auliani, L. Khairani, dan M. Megawati, "Audit Tata Kelola Universitas Islam Negara Sultan Syarif Kasim Riau Repository System Menggunakan COBIT 2019," *Jurnal Testing dan Implementasi Sistem Informasi*, vol. 2, no. 1, hlm. 1–9, 2024.

[6] A. A. Yantama, A. M. Putri, dan S. A. Wulandari, "Audit Keamanan Sistem Informasi PERJADIN BKKBN Provinsi Riau Menggunakan COBIT 19: APO12 dan APO13," dalam *Prosiding Seminar Nasional Amikom Surakarta*, 2023, hlm. 801–816.

[7] A. Nisiri, "Evaluasi Tingkat Kapabilitas Keamanan Sistem Informasi Menggunakan Kerangka Kerja Cobit 2019," *Jurnal Tata Kelola Dan Kerangka Kerja Teknologi Informasi*, vol. 9, no. 1, hlm. 34–41, 2023.

[8] V. Verdila, H. J. Setyadi, V. Z. Kamila, dan H. Muttaqien, "Evaluasi Manajemen Risiko Teknologi Informasi pada Perguruan Tinggi XYZ Menggunakan Objective EDM03 dan APO12 COBIT 2019," dalam *Prosiding Seminar Nasional Informatika*, 2024, hlm. 10–18.

[9] I. G. W. Aditya, I. G. P. K. Juliharta, dan I. G. A. P. D. Putri, "PENERAPAN FRAMEWORK COBIT 2019 DALAM AUDIT TATA KELOLA SISTEM INFORMASI PADA LPD DESA BERABAN," *JATI (Jurnal Mahasiswa Teknik Informatika)*, vol. 7, no. 4, hlm. 2592–2599, 2023.

[10] H. Herianto dan W. Wasilah, "Assessment Capability Level dan Maturity Level Tata Kelola TI pada Kantor Kementerian Agama Kabupaten Pesawaran Provinsi Lampung Menggunakan Framework COBIT 2019," *KONSTELASI: Konvergensi Teknologi dan Sistem Informasi*, vol. 2, no. 2, hlm. 229–240, 2022.

[11] I. A. A. Padmi, D. P. Githa, dan A. A. N. H. Susila, "Audit Tata Kelola Teknologi Informasi Rumah Sakit Umum X Menggunakan Framework Cobit 2019," *Jurnal Ilmiah Teknologi dan Komputer*, vol. 3, no. 1, hlm. 894–901, 2022.

[12] Y. T. Sepis, "Analisa keamanan sistem informasi menggunakan framework cobit 5 dengan domain dss05 dan apo13 di pt xyz," *TeIKa*, vol. 12, no. 01, hlm. 35–42, 2022.