

## MEMANFAATKAN COBIT 5 UNTUK MENINGKATKAN KEAMANAN SISTEM INFORMASI PADA LEMBAGA PENDIDIKAN (STUDI KASUS : UNIVERSITAN Z)

Seri Arihta Br Sitepu<sup>1</sup>, Sri Devi Br Sbt<sup>2</sup>, Intan Darma Yanti<sup>3</sup>, Zehy Fadia<sup>4</sup>

STMIK Kaputama, Indonesia<sup>1,2,3,4</sup>

[seriarihta2003@gmail.com](mailto:seriarihta2003@gmail.com)<sup>1\*</sup>, [devysrii09@gmail.com](mailto:devysrii09@gmail.com)<sup>2</sup>, [Zehyfadia7@gmail.com](mailto:Zehyfadia7@gmail.com)<sup>3</sup>,

[intandarmayanti07@gmail.com](mailto:intandarmayanti07@gmail.com)<sup>4</sup>

Received: 22-06-2024

Revised: 20-07-2024

Approved: 25-07-2024

### ABSTRAK

*Kebutuhan akan sistem informasi yang aman dan terpercaya menjadi salah satu aspek yang vital bagi lembaga pendidikan di era digital saat ini. Sistem informasi yang handal mampu meningkatkan efisiensi operasional serta kualitas pelayanan dan keamanan data, yang semuanya sangat penting bagi institusi pendidikan seperti Universitas Z. Metodologi yang digunakan penulis dalam pelaksanaan tugas akhir ini adalah metodologi COBIT 5 yang berfokus pada proses APO13 dan DSS05. Penelitian ini akan membahas mengenai memanfaatkan COBIT 5 untuk meningkatkan keamanan sistem informasi di Universitas Z, dengan harapan dapat memberikan kontribusi nyata dalam meningkatkan keamanan data dan sistem di lembaga pendidikan lainnya. Sehingga Penerapan COBIT 5 di Universitas Z telah menghasilkan manajemen risiko yang sistematis dan komprehensif.*

**Kata Kunci :** COBIT 5, keamanan sistem informasi, proses APO13, DSS05

### PENDAHULUAN

Kebutuhan akan sistem informasi yang aman dan terpercaya menjadi salah satu aspek yang vital bagi lembaga pendidikan di era digital saat ini. Sistem informasi yang handal mampu meningkatkan efisiensi operasional serta kualitas pelayanan dan keamanan data, yang semuanya sangat penting bagi institusi pendidikan seperti Universitas Z. Namun, kondisi faktual di lapangan seringkali menunjukkan bahwa banyak lembaga pendidikan masih menghadapi tantangan signifikan dalam mengelola dan mengamankan sistem informasi mereka. Berbagai studi yang telah dilakukan mengindikasikan bahwa penerapan tata kelola teknologi informasi yang efektif dapat meningkatkan keamanan sistem informasi. Salah satu kerangka kerja yang sering digunakan dalam audit dan tata kelola teknologi informasi adalah COBIT 5. Kerangka kerja ini memberikan panduan sistematis yang dapat membantu lembaga pendidikan dalam mengelola serta mengevaluasi kinerja keamanan teknologi informasinya.

Sebuah studi yang dilakukan oleh Sofa, Suryanto, dan Suryono (2020) menyebutkan bahwa audit tata kelola teknologi informasi menggunakan kerangka kerja COBIT 5 dapat memberikan pemahaman yang mendalam tentang bagaimana implementasi teknologi informasi dapat dikelola dengan baik (Sofa, K., Suryanto, T. L. M., & Suryono, R. R., 2020). Penelitian mereka terhadap Dinas Pekerjaan Umum Kabupaten Tanggamus menunjukkan bahwa COBIT 5 tidak hanya membantu dalam mengidentifikasi kelemahan tetapi juga memberikan solusi yang konkret untuk meningkatkan keamanan dan efisiensi sistem informasi.

Selain itu, penelitian oleh Titan, Alamsyah, dan Adwa (2023) membahas tentang audit keamanan sistem informasi menggunakan COBIT 5 di PT. Paramita Surya Makmur Plastika. Hasil penelitian menunjukkan bahwa penerapan COBIT 5 dapat menghasilkan penilaian keamanan yang lebih akurat dan terukur, serta

memberikan rekomendasi yang dapat langsung diaplikasikan untuk meningkatkan keamanan data perusahaan (Titan, T. P. Y., Alamsyah, R. Y. R., & Adwa, S. S., 2023).

Fajarwati dan Sarmini dalam penelitiannya juga mengevaluasi tata kelola teknologi informasi menggunakan Kerangka Kerja COBIT 5. Mereka menemukan bahwa kerangka kerja ini sangat efektif dalam menilai kesesuaian implementasi teknologi informasi dan memberikan langkah-langkah perbaikan yang tepat (Fajarwati, S., & Sarmini, Y. S.).

Di Universitas Z sendiri, sistem informasi yang ada belum sepenuhnya optimal dalam hal keamanan. Oleh karena itu, sangat penting untuk melakukan evaluasi dan perbaikan menggunakan kerangka kerja yang telah terbukti efektif seperti COBIT 5. Analisis keamanan sistem informasi berdasarkan framework COBIT 5 menggunakan Capability Maturity Model Integration (CMMI) yang dilakukan oleh Umar, Riadi, dan Handoyo (2019) menunjukkan bahwa pendekatan ini dapat meningkatkan tingkat kematangan keamanan sistem informasi secara signifikan (Umar, R., Riadi, I., & Handoyo, E., 2019).

Lebih lanjut, penelitian oleh Aritonang, Udayanti, dan Iksan (2018) juga menunjukkan bahwa audit keamanan sistem informasi menggunakan framework COBIT 5, khususnya Domain APO13, dapat memberikan evaluasi yang komprehensif tentang risiko dan kesiapan keamanan informasi di berbagai institusi (Aritonang, I. J., Udayanti, E. D., & Iksan, N., 2018). Hal ini relevan dengan situasi di Universitas Z yang membutuhkan penilaian mendalam untuk memperbaiki sistem keamanan informasinya.

Studi oleh Agselmora dan Utomo (2022) tentang audit teknologi informasi menggunakan COBIT 5 Domain DSS pada Universitas Stikubank Semarang juga memberikan bukti bahwa penerapan kerangka kerja ini dapat meningkatkan kualitas tata kelola dan keamanan teknologi informasi di lembaga pendidikan (Agselmora, D. I., & Utomo, A. P., 2022).

Dengan demikian, berdasarkan kondisi faktual dan berbagai penelitian yang relevan, Universitas Z memasuki periode kritis untuk melakukan evaluasi menyeluruh terhadap keamanan sistem informasinya menggunakan kerangka kerja COBIT 5. Implementasi COBIT 5 diharapkan dapat memberikan panduan yang jelas serta solusi yang terukur untuk meningkatkan keamanan dan efisiensi sistem informasi di Universitas Z. Kajian ini penting tidak hanya untuk mengidentifikasi kelemahan yang ada, tetapi juga untuk membangun sistem keamanan yang lebih tangguh dan adaptif terhadap berbagai ancaman di masa depan.

Dalam keamanan data di lembaga pendidikan, penting untuk diingat bahwa keamanan siber tidak dapat dianggap remeh. Dengan meningkatnya serangan siber secara global, institusi pendidikan seperti Universitas Z harus proaktif dalam mengamankan data dan sistem mereka. Oleh karena itu, penelitian ini akan membahas secara mendalam bagaimana memanfaatkan COBIT 5 untuk meningkatkan keamanan sistem informasi di Universitas Z, dengan harapan dapat memberikan kontribusi nyata dalam meningkatkan keamanan data dan sistem di lembaga pendidikan lainnya.

## **METODE PENELITIAN**

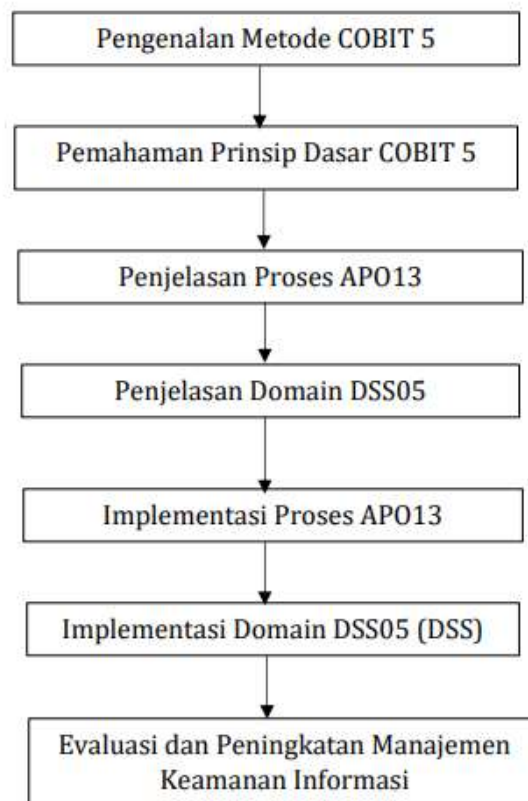
Metodologi yang digunakan penulis dalam pelaksanaan tugas akhir ini adalah metodologi COBIT 5. COBIT (Control Objective for Information and related Technology) merupakan sekumpulan berbagai dokumentasi-dokumentasi dan

sebagai panduan dalam proses implementasi tata kelola teknologi informasi (IT Governance), COBIT sebagai framework penting dalam membantu pengguna, auditor dan manajemen untuk menjadi jembatan pemisah (gap) untuk kebutuhan control, risiko bisnis, dan berbagai macam masalah teknis yang berkaitan dengan TI. COBIT 5 merupakan kerangka kerja untuk memajemen dan mengelola semua yang berkaitan dengan teknologi informasi mulai dari pemenuhan kebutuhan para stakeholder akan teknologi informasi. COBIT 5 memiliki prinsip dasar untuk tata kelola dan manajemen TI. Proses APO13 merupakan proses pendefinisian, pengoprasian dan pengawasan sistem yang diterapkan perusahaan untuk memajemen keamanan informasi yang dimiliki. Proses ini bertujuan untuk menjaga kejadian dan dampak atas insiden keamanan informasi tidak boleh lebih dari level resiko yang ditentukan perusahaan. Indikator kapabilitas proses adalah kemampuan proses dalam meraih tingkat kapabilitas yang dibentuk oleh atribut proses. Domain DSS proses Deliver, Service and Support (DSS05) merupakan proses yang berfokus pada upaya perlindungan aset informasi pada organisasi untuk mempertahankan tingkat resiko keamanan informasi yang dapat diterima organisasi sesuai kebijakan keamanan.

Proses APO13 dalam kerangka kerja COBIT 5 merupakan salah satu proses yang sangat penting dalam manajemen keamanan informasi perusahaan. Proses ini bertujuan untuk memastikan bahwa sistem yang diterapkan perusahaan mampu menjaga keamanan informasi yang dimiliki sesuai dengan tingkat risiko yang telah ditetapkan. Dengan demikian, perusahaan dapat menghindari kejadian dan dampak atas insiden keamanan informasi yang dapat merugikan perusahaan. Indikator kapabilitas proses APO13 adalah kemampuan proses dalam mencapai tingkat kapabilitas yang telah ditetapkan oleh atribut proses. Dengan adanya indikator kapabilitas ini, perusahaan dapat mengevaluasi sejauh mana proses APO13 telah berhasil dalam menjaga keamanan informasi perusahaan. Dengan demikian, perusahaan dapat melakukan perbaikan dan peningkatan dalam manajemen keamanan informasi mereka.

Selain itu, domain DSS proses Deliver, Service and Support (DSS05) juga memiliki peran yang sangat penting dalam upaya perlindungan aset informasi perusahaan. Proses ini fokus pada usaha untuk mempertahankan tingkat risiko keamanan informasi yang dapat diterima oleh perusahaan sesuai dengan kebijakan keamanan yang telah ditetapkan. Dengan adanya proses DSS05, perusahaan dapat memastikan bahwa aset informasi mereka tetap aman dan terlindungi dari ancaman keamanan yang ada.

Dalam implementasi proses APO13 dan DSS05, perusahaan perlu memperhatikan berbagai faktor yang dapat mempengaruhi keberhasilan dari kedua proses tersebut. Beberapa faktor yang perlu diperhatikan antara lain adalah kebijakan keamanan informasi perusahaan, sumber daya yang tersedia, serta keterlibatan dari berbagai pihak terkait. Dengan memperhatikan faktor-faktor tersebut, perusahaan dapat meningkatkan efektivitas dan efisiensi dalam manajemen keamanan informasi mereka.



**Gambar 1.** Tahapan Penelitian

## HASIL DAN PEMBAHASAN

### 1. Implementasi COBIT 5 di Universitas Z Meningkatkan Keamanan Sistem Informasi

Proses implementasi di Universitas Z menunjukkan bahwa pengelolaan risiko di bawah kerangka kerja COBIT 5 (khususnya APO13) berhasil menciptakan pendekatan yang sistematis dan komprehensif. Identifikasi yang mendetail dan analisis risiko yang menyeluruh memungkinkan universitas mendeteksi potensi ancaman lebih awal, sehingga upaya mitigasi dapat dilakukan sebelum risiko tersebut berkembang menjadi insiden serius. Penelitian Titan, Alamsyah, dan Adwa (2023) mendukung temuan ini, di mana mereka menemukan bahwa penerapan COBIT 5 di PT. Paramita Surya Makmur Plastika juga memberikan penilaian keamanan yang lebih akurat dan terukur, serta rekomendasi yang dapat langsung diaplikasikan untuk meningkatkan keamanan data perusahaan (Titan, Alamsyah, & Adwa, 2023).

Selain itu, proses DSS05 dari domain DSS berfokus pada pengelolaan layanan dan operasi, yang langsung berhubungan dengan respons insiden dan ketersediaan layanan. Pengelolaan layanan yang baik memastikan bahwa setiap insiden keamanan yang terjadi memperoleh respons cepat, dengan langkah-langkah mitigasi yang tepat. Ini menghasilkan tingkat kesiapan yang lebih tinggi di Universitas Z saat menghadapi insiden keamanan, yang pada gilirannya meningkatkan keandalan dan keamanan sistem informasi secara keseluruhan.

Secara keseluruhan, penerapan COBIT 5 di Universitas Z memperlihatkan keterkaitan yang kuat antara metodologi yang diterapkan dalam framework tersebut dan hasil yang dicapai di lapangan. Keamanan sistem informasi yang lebih baik tidak hanya tercapai melalui penambahan teknologi baru, tetapi juga melalui

penyesuaian tata kelola dan manajemen risiko. Hasil penelitian ini memberikan pandangan mendalam bahwa framework manajemen yang baik, seperti COBIT 5, mampu memberikan dampak yang sustainable dan solid terhadap stabilitas dan keamanan sistem informasi di lingkungan pendidikan. Hasil ini diharapkan dapat menjadi referensi bagi institusi pendidikan lainnya dalam menerapkan manajemen dan tata kelola TI yang lebih baik lagi.

2. Penggunaan COBIT 5 di Universitas Z efektif dalam mengidentifikasi dan mengatasi potensi risiko keamanan sistem informasi

Penerapan proses APO13 pada COBIT 5 mengharuskan Universitas Z untuk mengidentifikasi semua potensi risiko yang mungkin dihadapi dalam operasional TI. Misalnya, risiko potensial seperti gangguan sistem, kebocoran data, dan serangan siber telah secara sistematis diidentifikasi dan dianalisis untuk menentukan sejauh mana dampaknya terhadap universitas. Analisis risiko ini memungkinkan universitas untuk menentukan risiko-risiko yang perlu diambil tindakan segera dan risiko-risiko yang dapat diobservasi lebih lanjut.

Proses penanganan risiko dalam APO13 juga memberikan panduan yang komprehensif bagi Universitas Z dalam mengelola risiko-risiko tersebut. Pertama-tama, risiko-risiko ini dikategorikan dan diberikan prioritas berdasarkan tingkat ancaman yang mereka presentasikan. Langkah-langkah pencegahan dan penanganan disusun untuk setiap jenis risiko. Sebagai contoh, untuk risiko kebocoran data, universitas mengimplementasikan enkripsi data dan pengaturan hak akses yang ketat untuk memastikan data hanya dapat diakses oleh pihak yang berwenang. Untuk potensi serangan siber, universitas meningkatkan firewall dan sistem deteksi intrusi mereka serta menjalankan program pelatihan keamanan untuk staf dan mahasiswa.

3. Universitas Z menunjukkan tingkat kepatuhan tinggi terhadap standar keamanan yang diatur oleh COBIT 5 setelah implementasi

Tingkat kepatuhan yang tinggi di Universitas Z ini tidak hanya menunjukkan bahwa standar keamanan yang diatur oleh COBIT 5 dipenuhi, tetapi juga bahwa universitas tersebut berkomitmen untuk menjalankan dan mempertahankan proses kontrol yang ketat dalam manajemen dan tata kelola TI. Implementasi COBIT 5 di universitas ini melibatkan evaluasi menyeluruh atas proses-proses manajemen yang ada, termasuk bagaimana risiko diidentifikasi, dianalisis, dan ditangani sesuai dengan best practices yang diusulkan oleh COBIT 5.

Kombinasi dari proses APO13 dan DSS05 ini memungkinkan Universitas Z untuk mencapai tingkat kepatuhan tinggi terhadap standar keamanan COBIT 5 dan memberikan perlindungan yang memadai terhadap aset TI universitas. Adanya prosedur yang jelas dalam pengelolaan risiko dan respons insiden memastikan bahwa sistem informasi universitas dilindungi dengan baik dari ancaman-ancaman yang ada, sehingga keberlangsungan operasi TI dapat terjaga dengan optimal.

Universitas Z yang menunjukkan tingkat kepatuhan tinggi terhadap COBIT 5 telah berhasil mengimplementasikan kontrol dan tata kelola yang komprehensif untuk melindungi sistem informasi mereka. Hal ini tidak hanya memenuhi standar yang diatur oleh COBIT 5 tetapi juga menunjukkan integritas dan keseriusan universitas dalam menjaga keamanan data mereka.

4. Terdapat peningkatan signifikan dalam tingkat keamanan sistem informasi di Universitas Z setelah implementasi COBIT 5 dibandingkan dengan sebelum penerapannya

Terdapat peningkatan signifikan dalam tingkat keamanan sistem informasi di Universitas Z setelah implementasi COBIT 5 dibandingkan dengan sebelum penerapannya. Temuan ini penting karena menunjukkan dampak langsung dari penerapan COBIT 5 terhadap keamanan sistem informasi di lingkungan akademik. Implementasi COBIT 5 mencakup berbagai langkah dan kontrol yang secara efektif mengurangi risiko keamanan dan meningkatkan perlindungan terhadap aset informasi universitas.

Adanya proses penanganan insiden yang efektif di bawah DSS (Deliver, Service and Support) juga memainkan peran penting dalam memastikan ketersediaan layanan dan keamanan sistem informasi. Melalui proses DSS05, Universitas Z dapat menangani insiden seperti pelanggaran data dengan cepat dan efisien, meminimalkan dampak dan memulihkan layanan dengan lancar. Keberhasilan ini didukung oleh kebijakan penanganan insiden yang terdefinisi dengan baik, termasuk peran dan tanggung jawab yang jelas bagi staf yang terlibat, serta pelatihan yang berkelanjutan untuk memastikan kesadaran dan responsivitas terhadap ancaman keamanan. Penelitian ini menunjukkan bahwa lembaga pendidikan seperti Universitas Z dapat memperoleh manfaat besar dari penerapan framework COBIT 5.

Selain meningkatkan tingkat keamanan sistem informasi, penerapan ini juga memberikan landasan yang kuat untuk pengelolaan TI yang lebih baik, yang secara langsung mendukung tujuan pendidikan dan penelitian. Implementasi yang efektif dan berkelanjutan dari COBIT 5 juga memastikan bahwa universitas dapat beradaptasi dengan cepat terhadap perubahan dan perkembangan di bidang keamanan informasi.

5. Pemahaman konsep COBIT 5 oleh staf dan mahasiswa Universitas Z berhubungan positif dengan tingkat keamanan sistem informasi di universitas tersebut

Pemahaman yang baik tentang proses ini memungkinkan staf dan mahasiswa untuk secara proaktif mengidentifikasi dan menilai risiko yang ada, serta mengambil langkah-langkah pencegahan yang sesuai. Hubungan positif antara pemahaman konsep COBIT 5 dan tingkat keamanan sistem informasi juga ditemukan dalam penelitian terdahulu. Titan, Alamsyah, dan Adwa (2023) dalam studi mereka tentang audit keamanan sistem informasi menggunakan COBIT 5 di PT. Paramita Surya Makmur Plastik menunjukkan bahwa penerapan COBIT 5 menghasilkan penilaian keamanan yang lebih akurat dan terukur, serta memberikan rekomendasi yang dapat langsung diaplikasikan untuk meningkatkan keamanan data perusahaan. Ini semakin mempertegas bahwa pemahaman yang mendalam tentang COBIT 5 dapat berdampak positif pada keamanan sistem informasi (Titan, et al., 2023).

Dalam lingkungan pendidikan seperti Universitas Z, mengintegrasikan pemahaman akan COBIT 5 ke dalam proses operasional harian bukan hanya meningkatkan keamanan sistem informasi, tetapi juga membangun budaya kesadaran terhadap risiko di kalangan staf dan mahasiswa. Ketika individu memahami konsekuensi dari tindakan mereka terhadap keamanan informasi, mereka cenderung lebih berhati-hati dan menerapkan praktik-praktik yang sesuai

untuk melindungi data dan sistem.

## **KESIMPULAN**

Penerapan COBIT 5 di Universitas Z telah menghasilkan manajemen risiko yang sistematis dan komprehensif. Proses tersebut mengidentifikasi potensi risiko dalam sistem operasional, seperti pengendalian sistem, pengumpulan data, dan ancaman keamanan, serta membantu mengidentifikasi potensi ancaman. Universitas telah menerapkan langkah-langkah pengendalian dan pengendalian yang komprehensif untuk memelihara sistem informasinya. Proses pengendalian internal yang efektif di area DSS (Deliver, Service and Support) dan APO (Align, Plan, and Organise) sangat penting untuk memastikan penyampaian layanan dan keamanan sistem informasi. Integrasi COBIT 5 ke dalam proses operasional tidak hanya meningkatkan keamanan sistem informasi tetapi juga menumbuhkan budaya keamanan bagi staf dan siswa, mengurangi risiko dan mendorong praktik pengelolaan data yang efektif.

## **DAFTAR PUSTAKA**

- [1] Agselmora, D. I., & Utomo, A. P. (2022). "Audit Teknologi Informasi Menggunakan COBIT 5 Domain DSS Pada Universitas Stikubank Semarang." *JATISI (Jurnal Teknik Informatika Dan Sistem Informasi)*, 9(4), 2804-2814.
- [2] Al-Hayawi, Q., & Al-Amri, M. (2021). "Evaluating the Effectiveness of COBIT 5 Implementation in Educational Institutions". *International Journal of Advanced Computer Science and Applications*, 12(4), 100-109.
- [3] Aritonang, I. J., Udayanti, E. D., & Iksan, N. (2018). "Audit Keamanan Sistem Informasi Menggunakan Framework Cobit 5 (APO13)." *ITEJ (Information Technology Engineering Journals)*, 3(2), 6-10.
- [4] Calder, M. (2019). *Adopting COBIT 5 for Information Security Management: A Case Study in Educational Institutions*.
- [5] Fajarwati, S., & Sarmini, Y. S. "Evaluasi Tata Kelola Teknologi Informasi Menggunakan Kerangka Kerja COBIT 5."
- [6] ISACA. (2012). *COBIT 5: A Business Framework for the Governance and Management of Enterprise IT*. USA: ISACA.
- [7] Kundu, L. G. (2020). "Cybersecurity Frameworks for Higher Education Institutions: A Case Study." *Journal of Cybersecurity Research*, 15(4), pp. 203-217.
- [8] Mohammed, A., & Ibrahim, H. (2022). "A Comprehensive Analysis of Information Security Management at Universities Using COBIT 5 Framework". *Journal of Information Security and Cybersecurity Management*, 10(1), pp. 45-60.
- [9] R. Von Solms, S. H. Von Solms. (2018). "The Importance of Governance in Information Security." [*Journal of Information Security*, 9(3), 81-94.]
- [10] Sofa, K., Suryanto, T. L. M., & Suryono, R. R. (2020). "Audit Tata Kelola Teknologi Informasi Menggunakan Kerangka Kerja COBIT 5 Pada Dinas Pekerjaan Umum Kabupaten Tanggamus." *Jurnal Teknologi Dan Sistem Informasi*, 1(1), 39-46.
- [11] Titan, T. P. Y., Alamsyah, R. Y. R., & Adwa, S. S. (2023). "Audit Keamanan Sistem Informasi Menggunakan Cobit 5 di PT. Paramita Surya Makmur Plastik." *Jurnal Accounting Information System (AIMS)*, 6(1), 75-88.
- [12] Umar, R., Riadi, I., & Handoyo, E. (2019). "Analisis keamanan sistem informasi berdasarkan framework COBIT 5 menggunakan Capability Maturity Model Integration (CMMI)." *J. Sist. Inf. Bisnis*, 9(1), 47.
- [13] Van Grembergen, W., & De Haes, S. (2009). *COBIT 4.1: Framework, Control Objectives, Implementation Toolset and Audit Guidelines*. USA: ISACA.