PENERAPAN FRAMEWORK COBIT 5 PADADOMAIN DSS UNTUK MENGIDENTIFIKASI KEAMANAN TATA KELOLA WEBSITE UNIVERSITAS SWASTA DI SURAKARTA

Ilhaam Syafruddin Akbar [1)], Tining Haryanti[2]

[1)2)] Program Studi Teknik Informatika, Fakultas Teknik, Universitas Muhammadiyah Surabaya
Jl Sutorejo No. 59, Surabaya
Email: [1)], tiningharyanti@gmail.com[2)]

Abstrak

Pengelolaan keamanan website merupakan aspek penting dalam menghadapi tantangan keamanan siber yang terus berkembang. Dalam rangka meningkatkan kematangan tata kelola keamanan website, Universitas Muhammadiyah Surakarta memilih untuk menerapkan Framework COBIT 5.Penelitian ini bertujuan untuk mengidentifikasi kematangan tata kelola keamanan website universitas dengan menggunakan panduan dan prinsip COBIT 5. Metode yang digunakan dalam penelitian ini adalah studi kasus dengan melakukan audit tata kelola keamanan website universitas.bahwa penerapan Framework COBIT 5 memberikan panduan yang jelas dan komprehensif dalam mengidentifikasi kematangan tata kelola keamanan website. Hal ini meliputi peningkatan kebijakan keamanan, pelatihan dan kesadaran pengguna, implementasi kontrol keamanan yang sesuai, serta peningkatan pemantauan dan pelaporan keamanan.kontribusi yang signifikan dalam memperkuat tata kelola keamanan website universitas dan memberikan landasan bagi pengambilan keputusan yang lebih baik dalam menghadapi ancaman keamanan siber yang semakin kompleks. Dengan penerapan Framework COBIT 5, Universitas Muhammadiyah Surakarta dapat meningkatkan perlindungan data, meminimalkan risiko keamanan, dan memastikan keberlangsungan operasional website mereka.
Kata kunci: *Framework COBIT 5, tata teknologi informasi, website universitas, keamanan IT.*

Abstract

Website security management is an important aspect in facing the continuously evolving cybersecurity challenges. In order to enhance the maturity of website security governance, Universitas Muhammadiyah Surakarta has chosen to implement the COBIT 5 Framework. This research aims to identify the maturity of website security governance in the university using the guidance and principles of COBIT 5. The research methodology employed a case study approach by conducting an audit of the university's website security governance.The findings of the research indicate that the implementation of the COBIT 5 Framework provides clear and comprehensive guidance in identifying the maturity of website security governance. This includes improving security policies, user training and awareness, implementing appropriate security controls, as well as enhancing security monitoring and reporting.This research makes a significant contribution to strengthening the website security governance of the university and provides a foundation for better decision-making in facing increasingly complex cybersecurity threats. By implementing the COBIT 5 Framework, Universitas Muhammadiyah Surakarta can enhance data protection, minimize security risks, and ensure the continuity of their website operations.
Keywords : *COBIT 5 Framework,information technology governance, university website, IT security*

1. Pendahuluan

Di era digital saat ini, website perguruan tinggi swasta berperan sangat penting dalam menyampaikan informasi, berinteraksi dengan mahasiswa dan masyarakat, serta memfasilitasi pembelajaran. Namun, seiring perkembangan teknologi, tantangan keamanan dalam mengelola situs web universitas meningkat. Oleh karena itu, diperlukan pendekatan yang sistematis dan terstruktur untuk menentukan dan mengatur keamanan pengelolaan website universitas swasta.

Salah satu pendekatan yang mungkin dilakukan adalah menerapkan kerangka COBIT 5 Domain for Security, Risk and Compliance (DSS) untuk menentukan keamanan manajemen situs web universitas swasta. COBIT (Control Objectives for Information and Related Technology) adalah kerangka referensi yang diakui secara internasional untuk manajemen dan administrasi TI. Area DSS COBIT 5 menangani aspek keamanan, risiko, dan kepatuhan. Dalam konteks situs web universitas swasta, domain ini digunakan untuk mengidentifikasi, menilai, dan mengatasi risiko keamanan yang mungkin terkait dengan administrasi situs web[1]. Saat mengimplementasikan framework COBIT 5 Domain DSS, beberapa

langkah dapat dilakukan untuk menentukan keamanan pengelolaan website universitas swasta:

Identifikasi kebijakan dan prosedur keamanan:

Mengidentifikasi dan mengembangkan kebijakan dan prosedur keamanan website Universitas Muhammadiyah Surakarta seperti: B. Kebijakan kontrol akses, kebijakan penggunaan informasi pribadi dan prosedur pemulihan bencana[2].

Informasi identifikasi aset informasi:

Mengidentifikasi sumber data penting dan sensitif di website universitas swasta, seperti B. data mahasiswa, data keuangan dan data penelitian. Tugas beresiko:

Melakukan penilaian risiko untuk mengidentifikasi ancaman yang dapat mempengaruhi keamanan website universitas swasta dan menentukan dampak dari ancaman tersebut. Pengaturan manajemen keamanan:

Terapkan kontrol keamanan yang sesuai untuk mengurangi risiko keamanan yang teridentifikasi. Misalnya, menggunakan autentikasi yang kuat, enkripsi data, firewall, dan pemantauan aktivitas mencurigakan[3]. Amati dan evaluasi:

Secara teratur memantau dan mengevaluasi keamanan administrasi situs web universitas swasta untuk mendeteksi kerentanan atau pelanggaran keamanan yang mungkin terjadi. Tujuan dari penelitian ini adalah untuk mengoptimalkan keamanan manajemen situs web untuk melindungi informasi sensitif, mencegah akses tidak sah dan mengurangi risiko kebocoran data[4].

Kerangka DSS Domain COBIT 5 memungkinkan Universitas Muhammadiyah Surakarta untuk mendapatkan pemahaman yang lebih baik tentang keamanan manajemen situs webnya. Dengan mengidentifikasi dan mengelola risiko keamanan dengan pendekatan terstruktur, perguruan tinggi swasta dapat memastikan bahwa situs web mereka aman, melindungi informasi sensitif, dan mematuhi peraturan yang berlaku.

2. Dasar teori

2.1 COBIT 5

COBIT 5 adalah framework yang dikembangkan oleh ISACA (Information Systems Audit and Control Association) untuk membantu organisasi mengelola dan mengontrol teknologi informasi mereka. COBIT 5 merupakan pengembangan dari COBIT 4.1 versi sebelumnya dan menawarkan pendekatan yang komprehensif dan terintegrasi untuk pengelolaan area manajemen TI. Tujuan COBIT 5 adalah untuk membantu organisasi mencapai tujuan strategis mereka melalui penggunaan teknologi informasi secara efektif. Kerangka kerja ini juga membantu organisasi mengidentifikasi dan memahami risiko terkait TI Memberikan panduan tentang cara mengendalikan dan mengelola risiko tersebut.[1]

Domain COBIT 5: COBIT 5 mencakup lima domain utama yang merupakan area fokus dalam pengelolaan dan pengendalian TI. Domain-domain tersebut adalah:

a. Mengevaluasi, Memahami, dan Mengendalikan: Memastikan pemahaman yang baik tentang risiko dan kontrol yang ada dalam organisasi.

b. Mengelola Investasi: Mengelola investasi teknologi informasi dengan memastikan nilai bisnis yang optimal.

c. Mengelola Kinerja dan Manajemen Proyek: Mengelola kinerja TI dan proyek-proyek TI secara efektif.

d. Mengelola Risiko: Mengelola risiko-risiko yang terkait dengan TI dan memastikan bahwa tindakan pencegahan yang tepat diambil.

e. Mengelola Perspektif Pemangku Kepentingan: Menjalin hubungan yang baik dengan pemangku kepentingan dan memastikan kepatuhan terhadap persyaratan dan peraturan yang berlaku.

2.2 Deliver,Service,Support(DSS)

Delivery, Service and Support (DSS) adalah salah satu dari lima domain dalam kerangka kerja COBIT 5 (Control Objectives for Information and Related Technology). Domain DS terdiri dari proses yang berkaitan dengan pengiriman, pengiriman layanan, dan dukungan TI untuk memenuhi kebutuhan bisnis[5].

Domain DSS mencakup proses yang diperlukan untuk menyediakan solusi TI dan layanan TI yang memenuhi kebutuhan bisnis, memastikan operasi TI yang stabil dan andal, serta memberikan dukungan dan layanan teknis kepada pengguna TI [6]. Domain DSS ada 6 yaitu:

1. DSS01 :Manage Operations TI
2. DSS02 :Manage Service Requests and Incident
3. DSS03 :Manage Problems
4. DSS04 :Manage Continuity
5. DSS05 :Manage Security Services
6. DSS06 :Manage business process controls

Mengapa menggunakan domain DSS? Karena domain DSS menjelaskan bagaimana proses penyampaian layanan bekerja di website yang dikembangkan oleh Universitas Muhammadiyah Surakarta. Penelitian ini hanya berfokus pada analisis keamanan website.

2.3 Keamanan Tata Kelola

Keamanan tata kelola (governance) merupakan elemen penting dalam mengelola informasi dan teknologi dengan fokus pada perlindungan aset informasi dan sistem teknologi dari risiko dan ancaman. Hal ini melibatkan kebijakan, prosedur, dan kontrol yang diterapkan untuk memastikan keamanan, integritas, kerahasiaan, ketersediaan, dan keandalan informasi dan sistem teknologi di organisasi.[7]

Aspek utama dalam keamanan tata kelola adalah:

1. Kebijakan Keamanan: Organisasi perlu memiliki kebijakan keamanan yang jelas dan komprehensif yang mengatur penggunaan, akses, penyimpanan, dan perlindungan informasi dan sistem teknologi.
2. Pengelolaan Risiko: Organisasi harus mengidentifikasi, mengevaluasi, dan mengelola risiko keamanan yang terkait dengan aset informasi dan sistem teknologi.
3. Perlindungan Fisik dan Logis: Keamanan tata kelola harus mencakup pengamanan fisik dan logis terhadap aset informasi dan sistem teknologi, termasuk pengendalian akses fisik, pengamanan jaringan, enkripsi data, dan pengelolaan kata sandi.
4. Kesadaran Keamanan: Organisasi perlu meningkatkan kesadaran keamanan di antara karyawan dan pengguna sistem melalui pelatihan dan edukasi mengenai kebijakan dan praktik keamanan.
5. Keamanan Pihak Ketiga: Jika menggunakan layanan pihak ketiga, organisasi perlu memastikan bahwa pihak ketiga tersebut memenuhi standar keamanan yang ditetapkan.
6. Pengawasan dan Pemantauan: Organisasi harus memiliki mekanisme pengawasan dan pemantauan yang efektif untuk memastikan penerapan kebijakan keamanan dan kinerja kontrol keamanan.
7. Tanggapan Keamanan: Organisasi harus memiliki rencana dan prosedur tanggap keamanan untuk menghadapi insiden keamanan yang mungkin terjadi.

Dengan menerapkan keamanan tata kelola yang baik, organisasi dapat mengurangi risiko keamanan informasi dan sistem teknologi serta melindungi aset mereka dengan baik.

2.4 Maturity Level

Model kematangan (maturity level) merupakan salah satu instrumen untuk mengukur efektivitas sistem teknologi informasi. Model ini digunakan dalam framework COBIT untuk mengontrol proses teknologi informasi. Dengan metode evaluasi atau evaluasi, tujuan utama organisasi adalah untuk mengetahui tingkat kematangan teknologi informasi saat ini dan terus berupaya untuk meningkatkannya hingga level tertinggi [8] dimana dapat menganalisis objek website universitas. Aspek yang mengatur TI harus bekerja dengan baik. Kemampuan penguasaan teknologi informasi dibagi menjadi beberapa tingkatan pada skala kematangan.

a. Level 0 (Non existent)
   Pada tingkat ini, perusahaan tidak memberikan perhatian yang cukup terhadap pentingnya pengelolaan teknologi informasi oleh manajemen.
b. Level 1 (Initial)
   Pada tingkat ini, perusahaan secara proaktif menerapkan dan mengimplementasikan teknologi informasi sesuai dengan kebutuhan mendesak tanpa melakukan perencanaan sebelumnya.
c. Level 2 (Repeatable)
   Pada level ini, perusahaan telah memiliki pola yang berulangkali dilakukan dalam

manajemen aktivitas terkait dengan tata kelola teknologi, namun keberadaannya belum terdefinisi secara baik dan formal sehingga masih terjadi ketidak konsistenan.

d. Level 3 (Defined Process)
   Pada level ini, perusahaan telah memiliki prosedur baku formal dan tertulis yang telah di sosialisasikan ke segenap jajaran dan karyawan untuk dipatuhi dan dikerjakan dalam aktivitas sehari-hari.
e. Level 4 (Manage and Measurable)
   Pada level ini, perusahaan telah memiliki sejumlah indikator atau ukuran kuantitatif yang dijadikan sebagai sasaran maupun obyektif kinerja setiap penerapan aplikasi teknologi informasi yang ada.
f. Level 5 (Optimised)
   Pada level yang terakhir, perusahaan telah mengimplementasikan tata kelola teknologi informasi yang mengacu pada "best practice".

3. Metodologi Penelitian

3.1. Identifikasi Masalah

Tahap identifikasi masalah dilakukan setelah memilih topik penelitian dari beberapa pilihan yang tersedia. Tujuan dari tahap ini Universitas Muhammadiyah Surakarta mungkin tidak memiliki kebijakan keamanan yang jelas dan komprehensif untuk mengatur penggunaan, akses, penyimpanan, dan perlindungan informasi dan sistem teknologi pada website mereka[6]. Ini dapat menyebabkan celah keamanan yang dapat dimanfaatkan oleh pihak yang tidak berwenang.

3.2 Pengumpulan Data

Penelitian ini dilakukan melalui studi kasus di Universitas Muhammadiyah Surakarta untuk mengukur kematangan tata kelola teknologi informasi di website kampus tersebut menggunakan framework Cobit 5. Penelitian ini menggunakan metode observasi untuk mengumpulkan data.[9]

3.2. Analisis Data

Setelah data terkumpul, penulis melakukan analisis data yang terdiri dari analisis tingkat kematangan dan analisis kesenjangan. Pengolahan dan analisis hasil penelitian dilakukan menggunakan perangkat lunak komputer Microsoft Excel 2010.[2]

4. Pengujian dan Pembahasan

4.1. Observasi Identifikasi Masalah

Disini penulis mengelompokkan tujuan bisnis Universitas Muhammadiyah Surakarta dan tujuan bisnis COBIT 5 mengingat tujuan penelitian yaitu untuk meningkatkan informasi dan keamanan, sehingga penulis menempatkan tujuan tersebut pada bagian Managed Business Risk (Asset) COBIT 5 [2]. Tujuan bisnis Universitas Muhammadiyah Surakarta termasuk dalam kategori Managed Business Risk (perlindungan aset) karena Universitas Muhammadiyah Surakarta meningkatkan keamanan data dan informasi EMIS.

4.2. Identifikasi Proses COBIT 5

Tabel 2. Domain DSS

Process	Proses Name
DSS 01	Manage Operations TI
DSS 02	Manage Service Requests and Incident
DSS 03	Manage Problems
DSS 05	Manage Security Services

Identifikasi DSS Cobit 5 pada penelitian ini menggunakan DSS01, 02, 03 dan 05. Mengapa tidak menggunakan DSS04 dan DSS06? Karena DSS04 dan DSS06 hanya menjelaskan konten spesifik dari bisnis manajemen, fokus kajiannya hanya pada keamanan informasi yang diberikan.

4.3. Perhitungan Tingkat Kematangan (Maturity Level)

Saat menghitung tingkat kematangan, hasil perhitungan dianalisis untuk setiap proses untuk

mengidentifikasi kemungkinan perbedaan (gap). [10] Pada website Universitas Muhammadiyah Surakarta, berdasarkan pencapaian target maturity level yang disesuaikan dengan kebutuhan sistem, diperoleh nilai 3,4 yang menunjukkan tingkat kematangan proses pada level proses yang telah didefinisikan. Hal ini menunjukkan bahwa tim TI Universitas Muhammadiyah Surakarta telah melaksanakan proses layanan informasi sesuai dengan standar dan prosedur yang telah ditetapkan, namun masih terdapat ruang untuk meningkatkan efisiensi manajemen keamanan ke tingkat yang optimal.

Tabel 3. Maturity Level

Process	Process Name	Maturity Level	Kondisi
DSS01	Manage Operations TI	3,4	Defined Process
DSS02	Manage Service Requests and Incident	3,3	Defined Process
DSS03	Manage Problems	3,4	Defined Process
DSS05	Manage Security Services	3,5	Manage and Measurabel
Average		3,4	Defined Process

Berdasarkan hasil perhitungan tingkat kematangan domain DSS pada Tabel 3, terlihat bahwa rata-rata tingkat kematangan proses DSS02 dan DSS04 adalah 3,4. Dari skor kematangan tersebut dapat disimpulkan bahwa pengelolaan TI website Universitas Muhammadiyah Surakarta berada pada level proses yang telah ditentukan, hal ini menunjukkan bahwa organisasi telah menerapkan keamanan sesuai dengan standar dan prosedur formal yang telah ditentukan [11]. Namun demikian, masih terdapat beberapa bidang yang belum mencapai tingkat optimal terutama dalam hal peningkatan integritas stakeholder kampus dan akreditasi program studi. Hal ini menunjukkan bahwa penerapan pengamanan di Universitas Muhammadiyah belum sepenuhnya sesuai dengan standar COBIT 5 yang seharusnya diterapkan untuk menarik mahasiswa baru. Tabel 4 lebih lanjut menggambarkan perbedaan antara tingkat kematangan saat ini dan tingkat kematangan yang diharapkan .

Tabel 4. Maturity Level

Process	Tingkat kematangan		
	Saat ini	Diharapkan	GAP
DSS01	3,4	4	0,6
DSS02	3,3	4	0,7
DSS03	3,4	4	0,6
DSS05	3,5	4	0,5
Average			0,6

Dari tabel tersebut dapat dilihat bahwa terdapat GAP sebesar 0,6 pada proses domain DSS01, DSS02,DSS03,dan DSS05 antara nilai kematangan saat ini dengan nilai kematangan yang diharapkan. Angka GAP tersebut bisa dibilang cukup signifikan, namun masih perlu dilakukan perbaikan agar dapat meningkatkan ketertarikan pada mahasiswa baru untuk bergabung di Universitas Muhammadiyah Surakarta.

5. Kesimpulan

Dari hasil evaluasi tata kelola keamanan pada website universitas swasta di Surakarta dengan melalui pendekatan tingkat kematangan dalam domain Deliver,Service,Support (DSS) di Cobit 5,ditemukan bahwa tingkat kematangan saat ini berada pada level 3,pada level ini,proses-proses TI telah dikelola dengan baik dan memperoleh nilai 3,4.Namun, terdapat kesenjangan sebesar 0,6 dari nilai yang diharapkan. Hasil im mengindisikan bahwa di level 3,universitas swasta di Surakarta sudah menjalankan memiliki prosedur baku formal dan tertulis yang telah di sosialisasikan ke segenap jajaran dan karyawan untuk dipatuhi dan dikerjakan dalam aktivitas sehari-hari.Alangkah baiknya pihak universitas swasta di Surakarta perlu perbaikan sejumlah indikator atau ukuran kuantitatif yang dijadikan sebagai sasaran maupun obyektif kinerja setiap penerapan aplikasi teknologi informasi yang ada.

Daftar Pustaka.

[1] D. Darwis, N. Y. Solehah, and Dartono, "Penerapan Framework COBIT 5 untuk audit tata kelola keamanan informasi pada Kantor Wilayah Kementerian Agama Provinsi Lampung," *TELEFORTECH J. Telemat. Inf. Technol.*, vol. 1, no. 2, pp. 38–45, 2021.

[2] D. Pasha, A. thyo Priandika, and Y. Indonesian, "Analisis Tata Kelola It Dengan Domain Dss Pada Instansi Xyz Menggunakan Cobit 5," *J. Ilm. Infrastruktur Teknol. Inf.*, vol. 1, no. 1, pp. 7–12, 2020, doi: 10.33365/jiiti.v1i1.268.

[3] F. S. Sulaeman, "Audit Sistem Informasi Framework Cobit 5," *Media J. Inform.*, vol. 7, no. 2, pp. 37–42, 2020, [Online]. Available: https://jurnal.unsur.ac.id/mjinformatika/article/download/139/78

[4] A. Nuratmojo, E. Darwiyanto, and G. Wisudiawan, "Penerapan COBIT 5 Domain DSS (Deliver, Service, Support) untuk Audit Infrastruktur Teknologi Informasi FMS PT Grand Indonesia," *e-Proceeding Eng.*, vol. 2, no. 2, pp. 6499–6506, 2018.

[5] U. Cahyani, I. Aknuranda, and A. R. Perdanakusuma, "Evaluasi Layanan BPJSTK Mobile Dengan Menggunakan Domain Deliver, Service and Support Berdasarkan Framework COBIT 5 (Studi Kasus : BPJS Ketenagakerjaan Cabang Mataram)," *J. Pengemb. Teknol. Inf. dan Ilmu Komput.*, vol. 2, no. 8, pp. 2382–2391, 2018.

[6] N. Lediwara, "Analisis IT Governance Menggunakan Framework Cobit 5 Domain DSS, MEA dan BAI," *Pseudocode*, vol. 7, no. 2, pp. 97–104, 2020, doi: 10.33369/pseudocode.7.2.97-104.

[7] H. T. Sihotang and J. R. Sagala, "Penerapan Tata Kelola Teknologi Informasi Dan Komunikasi Pada Domain Align, Plan and Organise (Apo) Dan Monitor, Evaluate and Assess (Mea) Dengan Menggunakan Framework Cobit 5 Studi Kasus: Stmik Pelita Nusantara Medan," *J. Mantik Penusa Desember*, vol. 18, no. 2, pp. 2088–3943, 2015.

[8] M. Saleh, I. Yusuf, and H. Sujaini, "Penerapan Framework COBIT 2019 pada Audit Teknologi Informasi di Politeknik Sambas," *J. Edukasi dan Penelit. Inform.*, vol. 7, no. 2, p. 204, 2021, doi: 10.26418/jp.v7i2.48228.

[9] N. S. FARERA MESSAKH, "Analisis Sistem Informasi Berbasis Cobit 5 (Studi Kasus : LTC UKSW)," *JATISI (Jurnal Tek. Inform. dan Sist. Informasi)*, vol. 8, no. 1, pp. 388–400, 2021, doi: 10.35957/jatisi.v8i1.654.

[10] A. Sekarwati, T. Gantini, and S. K. Yefta, "Penerapan Domain DSS Cobit 5 pada Analisis GAP dan Kecukupan Layanan Teknologi Informasi," *J. Tek. Inform. dan Sist. Inf.*, vol. 3, no. 3, pp. 609–617, 2017, doi: 10.28932/jutisi.v3i3.703.

[11] M. A. Erizal, R. Fauzi, and R. A. Nugraha, "PERANCANGAN TATA KELOLA TEKNOLOGI INFORMASI di BUMN PT. ANGKASA PURA II MENGGUNAKAN framework COBIT 5 PADA DOMAIN DSS THE DESIGN OF INFORMATION TECHNOLOGY GOVERNANCE IN BUMN PT. ANGKASA PURA II USING COBIT 5 FRAMEWORK ON DSS DOMAIN," vol. 8, no. 5, pp. 9646–9663, 2021.