EVALUASI DAN PENINGKATAN KEAMANAN INSTAGRAM MELALUI AUDIT SISTEM INFORMASI

Salmiati[1], Novi Indriyani[2]
[12]Sistem Informasi, Fakultas Teknik dan Ilmu Komputer, Universitas Islam Indragiri,
Email: salmiayati353@gmail.com[1] , noviindriyani135@gmail.com[2]

ABSTRAK

Platform Instagram adalam media sosial yang digunakan banyak orang, apalagi diera teknologi yang sekarng ini yang semakin berkembang dan semakin maju zamannya. Akan tetapi, instagram bukan berarti dikatakan aman sesuai zamannya, karena semakin maju teknologi maka semakin berbahaya keamanannya. Oleh karena itu peneliti bertujuan untuk mengevaluasi dan menhingkatkan keamanan instagram melalui audit sistem informasi dengan menggunakan metode cobit 4.1 dan hasil yang di capai pada penelitian ini memberikan wawasan baru, serta peningkatan keamanannya bagaimana dengan memberikan penjelasan mengenai kelemahan yang ada pada keamanan instagram.

Kata Kunci: Evaluasi, Keamanan, Instagram, Cobit 4.1, Audit Sistem Informasi.

1 PENDAHULUAN

Dalam era digital saat ini, media sosial telah menjadi bagian integral dari kehidupan sehari-hari. Instagram, sebagai salah satu platform terkemuka, menyimpan banyak data sensitif pengguna yang rentan terhadap berbagai ancaman keamanan. Dengan jumlah pengguna aktif yang terus meningkat, risiko terhadap keamanan data juga semakin tinggi. Oleh karena itu, penting untuk melakukan evaluasi dan peningkatan keamanan melalui audit sistem informasi yang menyeluruh. Cobit 4.1 menyediakan kerangka kerja yang dapat membantu organisasi dalam memastikan tata kelola teknologi informasi yang efektif dan efisien[1].

Instagram telah menjadi salah satu platform media sosial paling populer di dunia, dengan lebih dari satu miliar pengguna aktif setiap bulannya. Platform ini digunakan untuk berbagi foto, video, dan cerita, serta berinteraksi dengan pengguna lain melalui pesan langsung dan komentar. Namun, popularitas Instagram juga menarik perhatian para peretas dan penjahat siber yang berusaha mencuri data pribadi pengguna atau merusak integritas platform.

Audit didefinisikan sebagai pemeriksaan yang dilakukan secara berkala dan dievaluasi secara formal dalam suatu organisasi. Tujuan dari audit adalah untuk meningkatkan dampak organisasi, baik positif maupun negatif. Audit juga membantu organisasi dalam melakukan pemeriksaan kebijakan agar dapat berkembang dengan memperoleh rekomendasi perbaikan yang dapat diterapkan oleh organisasi tersebut[2].

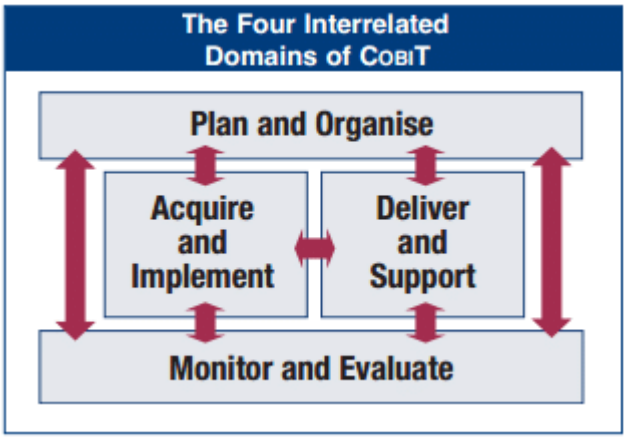
Dalam penelitian ini, peneliti melakukan perbandingan dengan peneliti-peneliti sebelumnya terkait metode dan beberapa kontek yang hampir sama. Adapun yang menyatakan dalam penelitiannya yang berjudul "Audit Keamanan Informasi pada Platform Media Sosial Menggunakan Cobit 4.1" menyoroti pentingnya melakukan audit keamanan informasi pada platform media 670indak yang banyak digunakan di Indonesia[3]. Penelitian ini dilakukan untuk mengevaluasi keamanan sistem informasi pada platform media sosial di Indonesia, seperti Facebook dan Instagram, dengan menggunakan kerangka kerja Cobit 4.1. Hidayat menemukan bahwa terdapat beberapa kelemahan dalam 670indaka akses dan pemantauan keamanan pada platform tersebut. Selain itu, kebijakan keamanan yang ada seringkali tidak diterapkan dengan baik oleh pengguna. Hidayat merekomendasikan peningkatan dalam kebijakan keamanan, akses yang lebih ketat, dan pemantauan keamanan yang lebih efektif untuk melindungi data pengguna.

Kemudian adapun yang menyatakan dalam penelitiannya yang berjudul "Evaluasi Keamanan Data Pengguna pada Platform Media Sosial di Indonesia" menggunakan pendekatan ISO/IEC 27001 untuk menilai risiko keamanan pada beberapa platform media sosial, termasuk Instagram. Permatasari menekankan pentingnya pengelolaan risiko yang baik untuk melindungi data pengguna dari ancaman yang semakin kompleks. Dalam penelitiannya, Permatasari mengidentifikasi bahwa salah satu masalah utama adalah kurangnya kesadaran pengguna tentang pentingnya keamanan instagram. Banyak pengguna yang tidak menggunakan fitur keamanan seperti autentikasi , yang meningkatkan risiko akses tidak sah. Permatasari menyarankan agar platform media sosial melakukan kampanye edukasi untuk meningkatkan kesadaran keamanan di kalangan pengguna, serta memperkuat mekanisme akses dan enkripsi data[4].

Penelitian-penelitian sebelumnya yang dilakukan oleh para peneliti Indonesia menunjukkan bahwa keamanan informasi pada platform media sosial di Indonesia masih perlu ditingkatkan. Dengan mempertimbangkan temuan-temuan dari penelitian sebelumnya, penelitian ini akan fokus pada evaluasi dan peningkatan keamanan Instagram menggunakan metode Cobit 4.1 untuk mengatasi isu-isu yang telah diidentifikasi.

2 METODE PENELITIAN

Penelitian ini menggunakan metode Cobit 4.1 untuk mengevaluasi dan meningkatkan keamanan sistem informasi Instagram. Metode ini terdiri dari empat domain utama: Planning and Organization, Acquisition and Implementation, Delivery and Support, serta Monitoring and Evaluation. Setiap domain menyediakan kerangka kerja yang komprehensif untuk mengelola dan mengawasi tata kelola teknologi informasi dalam organisasi. Berikut adalah langkah-langkah yang diambil dalam penelitian ini[3].



Gambar. 1 (tahapan cobit 4.1)

Cobit (Control Objectives for Information and related Technology) adalah kerangka kerja yang dikembangkan oleh ISACA (Information Systems Audit and Control Association) untuk tata kelola dan manajemen teknologi informasi. Versi 4.1 dari Cobit menyediakan panduan yang komprehensif bagi organisasi untuk mengelola dan mengawasi penggunaan teknologi informasi secara efektif dan efisien. Cobit 4.1 berfokus pada memastikan bahwa teknologi informasi mendukung tujuan bisnis, mengelola risiko TI, dan mengoptimalkan sumber daya TI[3][5].

Pada cobit 4.1 terdapat 4 tahapan utama, tahapan pertama ialah Planning and Organization (PO), tahapan ini mencakup perencanaan strategis, penetapan kebijakan, dan pengorganisasian

sumber daya TI untuk mendukung tujuan bisnis. Fokusnya adalah memastikan bahwa TI dikelola dengan baik, dengan perencanaan yang matang dan organisasi yang efisien.

Kemudian pada tahapan kedua ialah Acquisition and Implementation (AI), tahapan ini mencakup pengadaan dan implementasi 672indak TI yang memenuhi kebutuhan bisnis. Fokusnya adalah memastikan bahwa 672indak TI diimplementasikan dengan tepat waktu, sesuai anggaran, dan memenuhi persyaratan kualitas.

Pada tahapan ketiga yaitu Delivery and Support (DS), Dimana tahapan ini mencakup penyediaan layanan TI yang handal dan dukungan yang efektif kepada pengguna. Fokusnya adalah memastikan bahwa layanan TI memenuhi kebutuhan pengguna dan beroperasi dengan efisien.

Dalam tahapan yang keempat dan terakhir terdapat tahap Monitoring and Evaluation (ME), tahapan ini berupa pemantauan dan evaluasi kinerja TI serta kepatuhan terhadap kebijakan dan prosedur. Fokusnya adalah memastikan bahwa kinerja TI dievaluasi secara berkala dan 672indakan perbaikan diambil sesuai kebutuhan.

3 HASIL DAN PEMBAHASAN

Hasil dari audit sistem informasi menunjukkan beberapa kelemahan dalam keamanan Instagram. Berikut adalah deskripsi hasil temuan dan penjelasannya dalam bentuk tabel:

Tabel. 1 (*Planning and Organization*)

No	Domain	Hasil	Pembahasan
1	*Planning and Organization*	Kebijakan Keamanan, Kebijakan keamanan memadai, namun implementasinya belum optimal. Beberapa pengguna dan staf belum memahami dan menerapkan kebijakan tersebut. Perencanaan Keamanan, Perencanaan keamanan belum sepenuhnya mengantisipasi ancaman baru.	Kebijakan Keamanan, Diperlukan edukasi dan kampanye kesadaran keamanan secara kontinu untuk meningkatkan pemahaman dan penerapan kebijakan keamanan oleh pengguna dan staf. Perencanaan Keamanan, Perlu peninjauan berkala dan analisis risiko yang komprehensif untuk mengidentifikasi dan mengatasi ancaman baru. Memperbarui kebijakan keamanan dengan pedoman yang jelas dan mengedukasi pengguna serta staf tentang pentingnya menjaga kerahasiaan informasi pribadi.

Pada Tabel. 1 di atas menjelaskan mengenai planning and organization atau organisasi perencanaan yaitu kebijakan keamanan yang ada sudah memadai, tetapi belum sepenuhnya diterapkan dan dipahami oleh semua pengguna dan staf. Solusi yang diusulkan adalah melakukan edukasi dan kampanye kesadaran keamanan secara terus-menerus[6]. Perencanaan Keamanan adalah perencanaan saat ini belum memadai untuk mengantisipasi ancaman baru yang muncul. Diperlukan peninjauan dan analisis risiko secara berkala.

Tabel. 2 (*Acquisition and Implementation*)

No	Domain	Hasil	Pembahasan
1	*Acquisition and Implementation*	Sistem Otentikasi, Sistem otentikasi dua faktor (2FA) tersedia, namun belum diaktifkan oleh semua pengguna. Penggunaan kata sandi yang lemah masih menjadi masalah. Pembaruan Sistem, Pembaruan sistem dilakukan secara berkala, namun belum real-time.	Sistem Otentikasi, Kebijakan yang mendorong atau mewajibkan penggunaan 2FA dan kata sandi yang kuat perlu diterapkan. Panduan yang jelas harus disediakan untuk membantu pengguna. Pembaruan Sistem, Pembaruan sistem harus dioptimalkan agar bisa dilakukan secara real-time untuk menutup celah keamanan dengan cepat.

Pada Tabel. 2 menjelaskan *Acquisition and Implementation* sistem otentikasi, Meskipun 2FA tersedia, banyak pengguna belum mengaktifkannya. Kata sandi yang lemah juga menjadi masalah. Perlu ada kebijakan yang mendorong penggunaan 2FA dan kata sandi yang kuat, serta panduan yang jelas. **Pembaruan sistem**, Pembaruan sistem belum dilakukan secara real-time[7]. Ini penting untuk menutup celah keamanan dengan cepat, sehingga diperlukan optimalisasi dalam proses pembaruan.

Tabel. 3 (*Delivery and Support*)

No	Domain	Hasil	Pembahasan
1	*Delivery and Support*	Layanan Pengguna, Layanan dukungan pengguna dalam hal keamanan belum maksimal. Banyak pengguna tidak tahu cara melaporkan insiden keamanan atau mengatasi masalah keamanan. Pemantauan Keamanan, Pemantauan belum dilakukan secara real-time dan menyeluruh.	Layanan Pengguna, Layanan dukungan yang efektif perlu disediakan, termasuk panduan jelas tentang cara melaporkan insiden keamanan dan mendapatkan bantuan. Pemantauan Keamanan, Implementasi sistem pemantauan real-time diperlukan untuk deteksi dini dan respon cepat terhadap ancaman keamanan, dengan teknologi pemantauan otomatis untuk peringatan dini.

Adapun penjelasan pada Tabel. 3 adalah layanan pengguna, banyak pengguna tidak tahu bagaimana melaporkan insiden keamanan. Solusinya adalah menyediakan layanan dukungan yang efektif dan panduan yang jelas. Pemantauan keamanan, Pemantauan keamanan belum dilakukan secara real-time. Implementasi sistem pemantauan real-time diperlukan untuk mendeteksi dan merespons ancaman dengan cepat.

Tabel. 4 (*Monitoring and Evaluation*)

No	Domain	Hasil	Pembahasan
4	*Monitoring and Evaluation*	Audit Keamanan, Audit keamanan dilakukan, namun belum menyeluruh dan real-time. Beberapa ancaman mungkin tidak terdeteksi atau terlambat direspon.Evaluasi Kebijakan, Evaluasi kebijakan keamanan tidak dilakukan secara berkala.	Audit Keamanan, Audit keamanan real-time yang menyeluruh diperlukan untuk mendeteksi dan menanggapi ancaman dengan cepat. Penggunaan alat audit otomatis dapat membantu meningkatkan efisiensi dan efektivitas. Evaluasi Kebijakan, Evaluasi berkala dengan umpan balik dari pengguna dan staf diperlukan untuk memastikan kebijakan keamanan tetap relevan dan efektif.

Pada tahap terakhir yaitu pada Tabel. 4 mengenai *Monitoring and Evaluation* adalah Audit keamanan,Audit keamanan yang dilakukan belum menyeluruh dan real-time. Penggunaan alat audit otomatis dan audit real-time diperlukan. Evaluasi kebijakan, Evaluasi kebijakan keamanan tidak dilakukan secara berkala. Evaluasi berkala dengan umpan balik dari pengguna dan staf sangat diperlukan.

Kemudian pada hasil dan pembahasan di atas yang menjelaskan hasil setiap tahapan yang di lakukan adapun juga tahapan yang mendukung pada hasil ini akan dijelaskan dalam bentuk tabel berikut:

Tabel. 5 Peningkatan Kesadaran Keamanan

No	Domain	Hasil	Pembahasan
1	*Planning and Organization*	Peningkatan Kesadaran Keamanan, Banyak pengguna tidak menyadari pentingnya keamanan data pribadi.	Peningkatan Kesadaran Keamanan, Kampanye kesadaran dan pelatihan keamanan yang berkelanjutan penting untuk meningkatkan pemahaman pengguna mengenai pentingnya menjaga keamanan data pribadi dan cara melindungi diri dari ancaman siber.

Pada Tabel. 5 menjelaskan peningkatan kesadaran keamanan**,** banyak pengguna tidak menyadari pentingnya keamanan data pribadi. Kampanye kesadaran dan pelatihan keamanan yang berkelanjutan diperlukan untuk meningkatkan pemahaman ini.

Tabel. 6 Evaluasi Vendor Keamanan

No	Domain	Hasil	Pembahasan
2	*Acquisition and Implementation*	Evaluasi Vendor Keamanan, Evaluasi vendor keamanan tidak dilakukan secara menyeluruh.	Evaluasi Vendor Keamanan, Melakukan evaluasi menyeluruh terhadap vendor keamanan untuk memastikan mereka memenuhi standar keamanan yang tinggi dan dapat memberikan

			perlindungan yang memadai terhadap ancaman.

Dapat dijelaskan pada Tabel. 6 Evaluasi Vendor Keamanan**,** Evaluasi vendor keamanan yang dilakukan tidak menyeluruh. Evaluasi menyeluruh terhadap vendor diperlukan untuk memastikan standar keamanan yang tinggi.

Tabel. 7 Respon Insiden Keamanan

No	Domain	Hasil	Pembahasan
3	*Delivery and Support*	Respon Insiden Keamanan, Prosedur respon insiden belum optimal, menyebabkan keterlambatan dalam penanganan.	Respon Insiden Keamanan, Mengembangkan dan menguji prosedur respon insiden yang efektif dan cepat untuk memastikan bahwa setiap insiden keamanan dapat ditangani dengan tepat waktu, mengurangi dampak dari insiden tersebut.

Dapat dijelaskan pada Tabel. 7Respon Insiden Keamanan**,** Prosedur respon insiden yang ada belum optimal, menyebabkan keterlambatan dalam penanganan[8][9]. Prosedur respon insiden yang efektif dan cepat perlu dikembangkan dan diuji.

Tabel. 8 Pelaporan Insiden Keamanan

No	Domain	Hasil	Pembahasan
4	*Monitoring and Evaluation*	Pelaporan Insiden Keamana, Pelaporan insiden keamanan tidak dilakukan dengan cara yang terstruktur dan konsisten.	Pelaporan Insiden Keamanan, Mengimplementasikan sistem pelaporan insiden yang terstruktur dan konsisten untuk memastikan bahwa semua insiden dilaporkan dengan tepat dan ditangani sesuai dengan prosedur yang telah ditetapkan, serta digunakan untuk analisis lebih lanjut guna mencegah insiden serupa.

Pada Tabel. 8 Pelaporan Insiden Keamanan pada bagian Monitoring and Evaluation Pelaporan yaitu Insiden Keamanan**,** Pelaporan insiden keamanan tidak dilakukan dengan cara yang terstruktur dan konsisten[10]. Sistem pelaporan insiden yang terstruktur dan konsisten diperlukan untuk memastikan semua insiden dilaporkan dengan tepat dan ditangani sesuai prosedur.

Tabel-tabel di atas merangkum hasil dan rekomendasi untuk peningkatan keamanan Instagram berdasarkan metode Cobit 4.1, mencakup berbagai aspek yang perlu ditingkatkan untuk memastikan keamanan platform yang lebih baik.

4 KESIMPULAN

Dapat disimpulkan peneliti menggunakan metode cobit 4.1 untuk mengevaluasi dan meningkatkan keamanan instagram melalui audit sistem informasi. Pada metode ini melalui empat tahapan, dan empat tahapan tersebut sangat mendukung pada penyelesaian penelitian ini. Kemudian pada hasil dan pembahasan berisikan tentang 4 tahapan metode yang digunakan dalam bentuk tabel agar pembaca mudah memahaminya. Adapaun pada hasil dan pembahasan tahapan yang menyertai metode cobit 4.1 yaitu tabel pendukung sebagai penyempurnaan hasil akhir penelitian ini. Saran untuk penulis selanjutnya yaitu lebih memperbanyak refensi terbaru agar penelitian ini sesuai perkembang zaman.

REFERENSI

[1] F. V. Widiyanto and I. Ismail, "Audit Sistem Informasi Sas Pada Bpk Penabur Gading Serpong Menggunakan Kerangka Cobit 4.1," *J. Inform. dan Komputasi Media Bahasan, Anal. dan Apl.*, vol. 16, no. 01, pp. 12–17, 2022, doi: 10.56956/jiki.v16i01.97.

[2] S. K. PRATAMA, "Penerapan Perencanaan Dan Pengendalian Internal Audit Sistem Informasi," *J. Account. Tax. Audit.*, vol. 1, no. 2, pp. 1–10, 2020, doi: 10.57084/jata.v1i2.180.

[3] Fenny and J. F. Andry, "Audit Sistem Informasi Menggunakan Framework Cobit 4.1 Pada Pt. Aneka Solusi Teknologi," *Pros. Semnastek*, vol. Vol. 3, No, no. 0, pp. 1–2, 2017, [Online]. Available: https://jurnal.umj.ac.id/index.php/semnastek/article/view/2001

[4] T. P. Y. Titan, R. Y. Rakhman Alamsyah, and S. Silkillah Adwa, "Audit Keamanan Sistem Informasi Menggunakan Cobit 5 di PT. Paramita Surya Makmur Plastika," *J. Account. Inf. Syst.*, vol. 6, no. 1, pp. 75–88, 2023, doi: 10.32627/aims.v6i1.680.

[5] T. Kristiana, "Tata Kelola Teknologi Informasi Dengan Metode Cobit 4.1 (Studi Kasus: Rumah Sakit IMC Bintaro)," *Jln. RS.Fatmawati No*, vol. 87, no. 2, p. 7500282, 2017.

[6] A. L. Maryanto, M. N. Al Azam, and A. Nugroho, "Evaluasi Manajemen Keamanan Informasi Pada Perusahaan Pemula Berbasis Teknologi Menggunakan Indeks Kami," *J. Simantec*, vol. 11, no. 1, pp. 1–12, 2022, doi: 10.21107/simantec.v11i1.14099.

[7] A. Pandiangan and S. I. Shafa, "Audit Komunikasi Instagram @Jokowi Yang Dikelola Oleh Tim Komunikasi Digital Presiden," *J. Komun. dan Media*, vol. 1, no. 1, pp. 18–32, 2021, doi: 10.24167/jkm.v1i1.2846.

[8] D. Darwis and D. M. Pauristina, "Audit Sistem Informasi Menggunakan Framework Cobit 4.1 Sebagai Upaya Evaluasi Pengolahan Data Pada Smkk Bpk Penabur Bandar Lampung," *J. Ilm. Infrastruktur Teknol. Inf.*, vol. 1, no. 1, pp. 1–6, 2020, doi: 10.33365/jiiti.v1i1.254.

[9] Febryana Dewi Artati, Ficky Andrianto, Maria Ulfa, and Novi Khoiriawati, "Manajemen Resiko Teknologi Infor Manajemen Resiko Teknologi Informasi terhadap Audit Internal dan Dampak yang Ditimbulkan," *SAUJANA J. Perbank. Syariah dan Ekon. Syariah*, vol. 4, no. 02, pp. 12–24, 2022, doi: 10.59636/saujana.v4i02.73.

[10] A. A. Bakri, Y. Yusni, and N. Botutihe, "Analisis Efektivitas Penggunaan Teknologi Big Data dalam Proses Audit: Studi Kasus pada Kantor Akuntan Publik di Indonesia," *J. Akunt. Dan Keuang. West Sci.*, vol. 2, no. 03, pp. 179–186, 2023, doi: 10.58812/jakws.v2i03.641.