

PERBANDINGAN PENERAPAN ISO/IEC 27001 PADA CANVA FREE DAN PREMIUM**Ervina Kartika Sari¹, Novisca Indriani²**¹²Sistem Informasi, Teknik dan Ilmu Komputer, Universitas Islam Indragiri,Email: ervinakartikasari75@gmail.com¹, indrianinovisca@gmail.com²**ABSTRAK**

Pesatnya kemajuan teknologi digital mendorong semakin banyak individu dan organisasi memanfaatkan platform daring seperti Canva dalam memenuhi kebutuhan desain grafis. Namun, seiring meningkatnya penggunaan, muncul pula isu penting terkait keamanan informasi pengguna. Penelitian ini mengkaji sistem keamanan informasi pada layanan Canva dengan menggunakan pendekatan ISO/IEC 27001:2022. Fokus utama diarahkan pada perbandingan antara layanan gratis dan berbayar untuk menilai sejauh mana kontrol keamanan diterapkan. Hasil analisis menunjukkan bahwa layanan premium memiliki fitur pengamanan yang lebih lengkap, seperti autentikasi dua langkah dan pengelolaan peran pengguna. Sementara itu, versi gratis masih memiliki keterbatasan dalam hal kontrol keamanan. Berdasarkan temuan ini, direkomendasikan adanya peningkatan perlindungan data bagi semua pengguna dan pelaksanaan evaluasi rutin guna memastikan ketahanan sistem terhadap ancaman yang terus berkembang.

Kata Kunci: Canva, Keamanan Informasi, ISO/IEC 27001:2022, Audit, Layanan Gratis dan Premium.

ABSTRACT

The rapid advancement of digital technology has led to increased adoption of online platforms such as Canva by individuals and organizations to meet their graphic design needs. However, as usage continues to grow, concerns regarding user information security have also emerged. This study examines the information security system of Canva using the ISO/IEC 27001:2022 framework. The analysis focuses on comparing the free and premium services to evaluate the extent to which security controls are implemented. Findings indicate that the premium version offers more comprehensive security features, such as two-factor authentication and role-based access management. In contrast, the free version still lacks several key security controls. Based on these results, the study recommends enhancing data protection for all users and conducting regular evaluations to ensure the system remains resilient against evolving threats.

Keywords: Canva, Information Security, ISO/IEC 27001:2022, Audit, Free and Premium Services.

1 PENDAHULUAN

Perkembangan teknologi digital yang pesat dalam satu dekade terakhir telah memberikan dampak signifikan terhadap berbagai aspek kehidupan manusia, termasuk dalam cara bekerja, belajar, dan berkomunikasi. Salah satu bentuk transformasi digital tersebut terlihat pada meningkatnya penggunaan platform berbasis daring untuk mendukung berbagai aktivitas, salah satunya di bidang desain grafis. Canva merupakan salah satu platform desain grafis berbasis cloud yang saat ini banyak digunakan oleh masyarakat. Platform ini menawarkan kemudahan dalam pembuatan berbagai konten visual, seperti presentasi, poster, materi promosi, dan konten media sosial. Ketersediaan dalam dua versi, yaitu layanan gratis dan layanan berbayar (premium), menjadikan Canva dapat diakses secara luas oleh individu dari berbagai latar belakang, baik pelajar, tenaga pendidik, pelaku usaha, maupun instansi pemerintahan. Namun demikian, meningkatnya penggunaan platform Canva juga menimbulkan potensi risiko terhadap keamanan informasi, khususnya berkaitan dengan data pengguna yang tersimpan di dalam sistem. Data yang dimaksud tidak hanya terbatas pada hasil desain grafis, tetapi juga mencakup informasi pribadi, data akun, hingga akses tim dalam layanan premium. Keamanan informasi menjadi aspek yang sangat penting

untuk diperhatikan karena ancaman terhadap data dapat datang dari berbagai arah, baik berupa akses tidak sah, pencurian data, penyalahgunaan informasi, maupun gangguan terhadap integritas dan ketersediaan sistem.

Beberapa studi terdahulu menegaskan bahwa sistem keamanan informasi harus dirancang untuk mampu menyesuaikan diri dengan dinamika ancaman digital yang terus berkembang serta menjadi bagian integral dalam kebijakan dan strategi organisasi[1] Kurangnya kesadaran terhadap risiko keamanan informasi juga sering menjadi salah satu penyebab utama munculnya kerentanan, sebagaimana ditemukan pada sistem informasi akademik yang tidak dilengkapi dengan kontrol keamanan memadai[2]. Dalam hal ini, penerapan standar internasional seperti ISO/IEC 27001 dipandang penting sebagai kerangka kerja dalam membangun dan mengevaluasi sistem manajemen keamanan informasi (SMKI) yang andal. Penelitian terbaru juga menunjukkan bahwa penerapan Indeks KAMI yang dipadukan dengan ISO/IEC 27001 dapat membantu organisasi, khususnya di sektor pemerintahan daerah, dalam menilai kesiapan dan tingkat kematangan keamanan informasi, sekaligus merumuskan rekomendasi untuk perbaikan[3]. Di sisi lain, dalam konteks pemerintahan daerah, ditemukan bahwa penerapan sistem keamanan informasi masih menghadapi berbagai kendala, terutama terkait dengan keterbatasan sumber daya manusia, kurangnya pelatihan, serta belum terbentuknya budaya keamanan yang kuat[4]. Selain itu, audit internal dan evaluasi terhadap tingkat kematangan sistem informasi merupakan langkah strategis dalam mengidentifikasi kelemahan sistem dan menyusun langkah perbaikan berkelanjutan. Penerapan pendekatan seperti siklus Plan-Do-Check-Act (PDCA) telah terbukti efektif dalam membantu organisasi meningkatkan tata kelola keamanan informasinya [5]. Di samping itu, metode penilaian risiko seperti Failure Mode and Effect Analysis (FMEA) juga dapat digunakan untuk mengidentifikasi titik-titik rawan dalam sistem dan menentukan prioritas pengendalian berbasis kontrol dalam ISO/IEC 27001:2022 [6]. Evaluasi semacam ini sangat relevan pula pada sektor layanan kesehatan, yang memerlukan sistem informasi dengan tingkat keandalan tinggi dalam menjaga kerahasiaan, integritas, dan ketersediaan data [7].

Berdasarkan latar belakang tersebut, penelitian ini bertujuan untuk melakukan evaluasi terhadap sistem keamanan informasi pada platform Canva dengan menggunakan pendekatan audit checklist berbasis standar ISO/IEC 27001:2022. Fokus kajian diarahkan pada perbandingan antara layanan gratis dan layanan premium untuk menilai sejauh mana kontrol keamanan telah diterapkan secara proporsional pada kedua jenis layanan tersebut. Melalui analisis ini, diharapkan dapat diperoleh gambaran mengenai tingkat kesesuaian kontrol keamanan Canva terhadap prinsip-prinsip ISO/IEC 27001, serta dirumuskan rekomendasi untuk perbaikan sistem guna meningkatkan perlindungan informasi pengguna secara menyeluruh.

2 TINJAUAN PUSTAKA

Penerapan standar ISO/IEC 27001 telah menjadi rujukan utama dalam membangun sistem manajemen keamanan informasi (SMKI) di berbagai sektor. Penelitian terdahulu menunjukkan bahwa integrasi kebijakan keamanan ke dalam proses bisnis melalui ISO/IEC 27001:2022 dapat meningkatkan postur keamanan organisasi secara keseluruhan, meskipun masih menghadapi tantangan seperti keterbatasan sumber daya dan minimnya dukungan manajemen[1]. Dalam konteks pendidikan, pendekatan serupa digunakan untuk mengatasi kelemahan pada sistem informasi akademik, seperti absennya backup data dan kurangnya firewall, yang dapat menyebabkan celah keamanan serius[2]. Audit internal di lembaga pendidikan seperti SMKN dan PEM Akamigas dilaksanakan secara berkala guna menjamin integritas, efesiensi operasional, serta kepatuhan terhadap berbagai standar yang berlaku.[8]

Di sektor pemerintahan, pendekatan gabungan antara framework OCTAVE-S dan ISO/IEC 27001 digunakan untuk menganalisis risiko keamanan sistem informasi. Temuan dari penelitian tersebut menggarisbawahi pentingnya dokumentasi dan kebijakan keamanan yang terstruktur guna mengurangi risiko teknis dan operasional [3]. Sementara itu, dalam pemerintahan daerah, evaluasi kesiapan keamanan informasi menggunakan Indeks KAMI 4.2 yang dipadukan dengan standar ISO/IEC 27001 dapat membantu menilai tingkat kematangan sistem dan memberikan

rekomenisasi perbaikan untuk mengurangi celah risiko [4]. Dalam ranah pemerintahan, terutama dalam hal pengawasan terhadap anggaran pendidikan, pelaksanaan audit secara rutin merupakan elemen krusial dalam sistem pengawasan yang menyeluruh. Penerapan pendekatan yang terpadu yang mencakup pemantauan, audit, pelaporan yang transparan, serta evaluasi berdasarkan indikator capaian dapat memperkuat transparansi dan akuntabilitas penggunaan dana, sekaligus mendorong perbaikan kinerja sektor pendidikan secara menyeluruh[9].

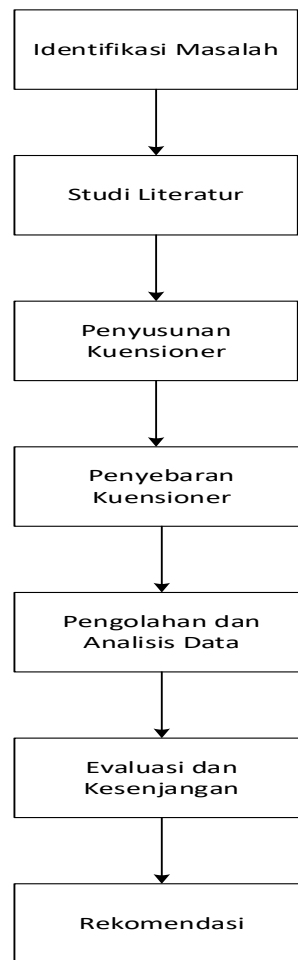
Sementara itu pada sektor kesehatan audit operasional dan audit internal di rumah sakit dan fasilitas kesehatan terbukti meningkatkan efektivitas pelayanan medis dan mutu perawatan pasien. Audit dilakukan secara berkala (6-12 bulan) dengan fokus pada kepatuhan prosedur, peningkatan kualitas perawatan, dan pengawasan biaya pelayanan kesehatan.[10]

Audit sistem informasi berbasis ISO/IEC 27001 juga telah banyak digunakan untuk menilai efektivitas kontrol keamanan. Studi menunjukkan bahwa sebagian besar organisasi berada pada level kematangan menengah, di mana kontrol telah diterapkan namun belum optimal [5]. Selain itu, metode FMEA mampu membantu dalam memprioritaskan risiko berdasarkan tingkat keparahan dan probabilitas kegagalan sistem [6]. Pada sektor kesehatan, audit berkala terhadap sistem informasi rumah sakit direkomendasikan untuk memastikan bahwa kontrol berjalan konsisten dan mampu merespons tantangan keamanan yang terus berkembang [7].

2 METODE PENELITIAN

Penelitian ini menggunakan metode deskriptif kuantitatif, yang bertujuan untuk mengukur dan mengevaluasi penerapan sistem keamanan informasi pada platform Canva, baik versi gratis maupun premium, dengan melibatkan persepsi pengguna secara langsung. Data dikumpulkan melalui penyebaran kuesioner kepada mahasiswa Universitas Islam Indragiri sebagai responden, serta didukung dengan studi literatur dan analisis dokumen pendukung yang relevan dengan standar ISO/IEC 27001:2022. Kuesioner yang digunakan disusun berdasarkan indikator kontrol keamanan informasi yang terdapat dalam Annex A ISO/IEC 27001:2022, seperti autentikasi pengguna, pengendalian akses, perlindungan data, dan manajemen insiden. Hasil kuesioner kemudian diolah untuk memperoleh gambaran tingkat penerapan kontrol keamanan informasi pada Canva.

Berikut adalah tahapan-tahapan yang dijalankan dalam penelitian ini:

**Gambar 1 Computer**

2.1 Identifikasi Masalah

Peneliti mengidentifikasi permasalahan terkait perlindungan informasi pada platform Canva, dengan fokus pada meningkatnya kebutuhan pengguna terhadap jaminan keamanan data pribadi di layanan desain grafis berbasis daring.

2.2 Studi Literatur

Peneliti melakukan penelusuran berbagai literatur, seperti jurnal, buku, artikel ilmiah, dan dokumen standar ISO/IEC 27001:2022, guna memperkuat kerangka teori dan memberikan landasan bagi penyusunan instrumen penelitian.

2.3 Penyusunan Kuensioner

Instrumen kuesioner disusun berdasarkan kontrol keamanan informasi yang terdapat dalam Annex A ISO/IEC 27001:2022. Setiap item pertanyaan diorientasikan untuk mengukur tingkat kesadaran, pemahaman, serta pengalaman pengguna terkait fitur keamanan di Canva.

2.4 Penyebaran Kuensioner

Kuesioner disebar kepada mahasiswa Universitas Islam Indragiri yang menggunakan platform Canva, baik versi gratis maupun premium. Penyebaran dilakukan secara daring melalui Google Form atau media serupa.

2.5 Pengolahan dan Analisis Data

Data hasil kuesioner dikumpulkan, kemudian dilakukan pengolahan dengan cara menghitung rata-rata skor setiap indikator menggunakan skala Likert 1–5. Selanjutnya, dilakukan perhitungan indeks untuk mengetahui tingkat kematangan kontrol keamanan informasi pada Canva.

2.6 Evaluasi & Kesenjangan

Hasil pengolahan data dibandingkan dengan standar yang diacu untuk mengetahui kesenjangan antara implementasi kontrol keamanan informasi pada Canva versi gratis dan premium.

2.7 Rekomendasi

Berdasarkan hasil evaluasi, peneliti menyusun rekomendasi perbaikan penerapan kontrol keamanan informasi, terutama untuk meningkatkan perlindungan bagi seluruh pengguna.

3 HASIL DAN PEMBAHASAN

3.1 Karakteristik Responden

Penelitian ini menggunakan metode survei melalui penyebaran kuesioner kepada 23 responden yang merupakan pengguna platform Canva, baik versi Gratis maupun Premium. Dari total responden, 18 orang (78%) menggunakan Canva Gratis, sedangkan 5 orang (22%) menggunakan Canva Premium. Hal ini menunjukkan bahwa mayoritas responden lebih memilih layanan gratis dibandingkan layanan berbayar.

3.2 Rekapitulasi Hasil Kuesioner

Tabel 1 Hasil Rekapitulasi Hasil Kuesioner Persepsi Keamanan Informasi Canva

Pertanyaan	STS	ST	N	S	SS	Total Skor	Rata-rata
Saya merasa akun Canva saya aman dari akses tidak sah			9	11	3	86	3,74
Fitur autentikasi dua faktor (2FA) tersedia dan mudah digunakan		2	13	18	5	75	3,26
Canva memberikan notifikasi jika terjadi aktivitas mencurigakan	1	1	8	12	1	80	3,48
Saya mengetahui adanya pengaturan keamanan akun di Canva		1	7	12	3	86	3,74
Canva memberikan informasi cukup tentang privasi dan			6	15	2	88	3,83

perlindungan data							
Data pribadi saya aman di dalam sistem Canva			6	15	2	88	3,83
Saya mengetahui cara mengatur peran anggota tim di Canva (premium)	1	2	9	10	1	77	3,35
Canva menyediakan fitur keamanan tambahan untuk pengguna premium	1		9	9	4	84	3,65
Saya merasa perlu adanya peningkatan fitur keamanan untuk pengguna Gratis			6	10	7	93	4,04
Secara keseluruhan saya puas dengan sistem keamanan informasi Canva			6	13	2	80	3,48
						837	3,64

3.3 Analisis Hasil Kuensioner

Berdasarkan hasil rekapitulasi kuesioner pada Tabel 1, rata-rata persepsi responden terhadap sistem keamanan informasi pada platform Canva menunjukkan angka 3,64 pada skala Likert 1–5. Nilai ini mengindikasikan bahwa sebagian besar responden cenderung setuju bahwa Canva telah menyediakan fitur dan kebijakan keamanan informasi yang cukup baik, meskipun masih terdapat beberapa aspek yang perlu ditingkatkan. Pernyataan dengan rata-rata tertinggi terdapat pada

pernyataan ke-9, yaitu “Saya merasa perlu adanya peningkatan fitur keamanan untuk pengguna Canva versi gratis” dengan rata-rata 4,04, menandakan bahwa mayoritas pengguna masih mengharapkan perlindungan yang setara bagi pengguna versi gratis. Sementara itu, pernyataan dengan rata-rata terendah adalah terkait persepsi keamanan akun dari akses tidak sah (3,74) dan ketersediaan autentikasi dua faktor (3,26). Hal ini menunjukkan bahwa meskipun fitur 2FA sudah tersedia, masih banyak pengguna yang belum memanfaatkannya secara optimal atau belum mengetahuinya. Secara umum, distribusi jawaban responden menunjukkan persepsi yang positif, namun belum maksimal, sehingga hasil ini menjadi dasar untuk mengevaluasi tingkat kesiapan sistem keamanan informasi di Canva dengan pendekatan maturity level.

3.4 Penilaian Maturity Level

Penilaian tingkat kematangan (maturity level) dilakukan dengan menghitung indeks rata-rata berdasarkan skor kuesioner, kemudian dikonversikan ke skala 5 untuk disesuaikan dengan model CMMI.

Rumus Perhitungan: $\text{Indeks} = \frac{\text{Rata-rata Keseluruhan}}{\text{Skala Maksimum}}$

Skala Maksimum

Keterangan: a. Rata-rata Keseluruhan = 3,64

b. Skala Maksimum = 5

Maka: $\text{Indeks} = 3,64 / 5 = 0,728$

Tabel 2 Skala Maturity Level:

Indeks Skor	Level Maturity
0,00-0,20	Level 1 - Initial
0,21-0,40	Level 2 - Repeatable
0,41-0,60	Level 3 - Defined
0,61-0,80	Level 4 - Managed
0,81-1,00	Level 5 - Optimizing

Maka, nilai indeks 0,728 menempatkan sistem keamanan informasi Canva pada Level 4 – Managed, yang berarti pengendalian keamanan sudah dilaksanakan secara cukup baik, terdokumentasi, dan terpantau, namun masih memerlukan perbaikan berkelanjutan agar dapat mencapai tingkat Optimizing.

3.5 Implikasi dan Rekomendasi

Berdasarkan hasil analisis kuesioner dan penilaian maturity level, terdapat beberapa implikasi penting:

1. Pengguna Canva, terutama versi gratis, masih merasa perlu adanya penambahan fitur keamanan dasar, seperti autentikasi dua faktor yang lebih mudah diakses.
2. Tingkat kesadaran pengguna terhadap fitur-fitur keamanan masih bervariasi; hal ini menunjukkan perlunya edukasi keamanan siber yang berkelanjutan.
3. Pihak pengembang Canva disarankan untuk melakukan evaluasi rutin terhadap kebijakan keamanan informasi agar dapat mengantisipasi potensi ancaman digital yang terus berkembang.
4. Rekomendasi praktis yang dapat diterapkan adalah menyediakan panduan penggunaan fitur keamanan dalam bentuk video tutorial, pop-up reminder, atau notifikasi berkala bagi seluruh pengguna, baik gratis maupun premium.

Dengan demikian, diharapkan sistem keamanan informasi pada platform Canva dapat terus ditingkatkan menuju Level 5 – Optimizing, sehingga kepercayaan pengguna dapat terjaga secara berkelanjutan.

4 KESIMPULAN

Berdasarkan hasil penelitian yang telah dilakukan, dapat disimpulkan bahwa sistem keamanan informasi pada platform Canva, baik versi Gratis maupun Premium, telah menerapkan sebagian besar kontrol yang sesuai dengan standar ISO/IEC 27001:2022. Hasil audit checklist menunjukkan bahwa pada versi Premium, hampir seluruh kontrol penting telah diterapkan dengan baik, sedangkan pada versi Gratis masih terdapat beberapa kontrol yang belum diimplementasikan secara optimal, terutama pada aspek kontrol teknis dan administratif. Hasil kuesioner yang disebarkan kepada 23 responden mahasiswa Universitas Islam Indragiri juga menunjukkan bahwa persepsi pengguna terhadap keamanan informasi Canva berada pada kategori cukup baik, dengan rata-rata skor 3,64 yang jika dikonversikan ke indeks maturity level menghasilkan skor 0,728. Berdasarkan konversi skala, nilai ini termasuk ke dalam Level 4 – Managed, yang berarti pengendalian keamanan informasi sudah dikelola dan dipantau, tetapi masih memerlukan evaluasi dan peningkatan berkelanjutan agar dapat mencapai tingkat kematangan tertinggi. Secara keseluruhan, dapat disimpulkan bahwa Canva telah berupaya menjaga keamanan informasi penggunanya, terutama untuk layanan Premium, tetapi masih diperlukan upaya tambahan untuk meminimalkan kesenjangan perlindungan bagi pengguna layanan Gratis. Hal ini sejalan dengan harapan sebagian besar responden yang menginginkan peningkatan fitur keamanan dasar pada layanan Gratis, serta perlunya edukasi berkelanjutan terkait pemanfaatan fitur-fitur keamanan yang telah disediakan.

REFERENSI

- [1] R. Sinaga and F. Taan, "Penerapan ISO/IEC 27001:2022 dalam Tata Kelola Keamanan Sistem Informasi: Evaluasi Proses dan Kendala," *Nuansa Inform.*, vol. 18, no. 2, pp. 46–54, 2024, doi: 10.25134/ilkom.v18i2.205.
- [2] E. Ardius and D. Syamsuar, "Assessment Risk Terhadap Penggunaan Sistem Informasi Akademik Universitas Ea Menggunakan Metode Iso 27001," *J. Teknol. Inf. Mura*, vol. 15, no. 1, pp. 1–13, 2023, doi: 10.32767/jti.v15i1.1948.
- [3] D. R. Nurfadilah, W. N. H. Putra, and A. Rachmadi, "Analisis Manajemen Risiko Keamanan Sistem Informasi pada BKPSDM Kota Batu menggunakan Kerangka Kerja OCTAVE-S dan ISO 27001 : 2013 (Studi Kasus : Aplikasi E-Kinerja)," *J. Pengemb. Teknol. Inf. dan Ilmu Komputer, Univ. Brawijaya*, vol. 4, no. 9, pp. 3014–3020, 2020.
- [4] D. I. Khamil, "Evaluasi Tingkat Kesiapan Keamanan Informasi Menggunakan Indeks Kami 4.2 dan ISO/IEC 27001:2013 (Studi Kasus : Diskominfo Kabupaten Gianyar)," *JATISI (Jurnal Tek. Inform. dan Sist. Informasi)*, vol. 9, no. 3, pp. 1948–1960, 2022, doi: 10.35957/jatisi.v9i3.2310.
- [5] M. J. Budiman and Fanny Jouke Doringin, "Jurnal Ilmu Komputer," *Biomaterials*, vol. 07, no. 12, pp. 85–90, 2023.
- [6] T. Lavanya, N. | Malarvizhi, "Analisis dan manajemen risiko," *3 Maret*, vol. 14, no. 1, 2008, [Online]. Available: <https://www.pmi.org/learning/library/risk-analysis-project-management-7070#>
- [7] R. N. Akmal, D. D. Susilo, and E. H. Rouf, "Evaluasi Keamanan Sistem Informasi Rumah Sakit : Metode Pengujian ISO 27001 di RS Khusus Mata Purwokerto Abstrak," vol. 6, no. 1, pp. 560–569, 2025.
- [8] S. Y. Rakhmawati, "Hubungan Antara Audit Internal Dan Kualitas Laporan Keuangan Di SMKN 1 Surabaya," *Dewantara J. Pendidik. Sos. Hum.*, vol. 2, no. 2, pp. 168–176, 2023, [Online]. Available: <https://jurnaluniv45sby.ac.id/index.php/Dewantara/article/view/1034>
- [9] P. Anggaran, P. Dari, and K. Hingga, "Jurnal Riset dan Pengetahuan Nusantara Jurnal Riset dan Pengetahuan Nusantara," vol. 6, no. 1, 2025.

- [10] J. A. Haryadi, A. Setiawan, and M. R. Maengkom, "Studi Literatur terhadap Peran dan Manfaat Audit Operasional terhadap Efektivitas Pelayanan Kesehatan di Rumah Sakit," vol. 4, no. 1, pp. 553–563, 2024.