Jurnal Penelitian Nusantara
Volume 2 ; Nomor 11 ; November 2026 ; Page 106-114
Doi : https://doi.org/10.59435/menulis.v2i11.1608
Website : https://jurnal.padangtekno.web.id/index.php/menulis
E-ISSN : 3088-988X

Audit TI Aplikasi Weverse: Evaluasi Kontrol Keamanan Menggunakan COBIT 2019 DSS05

Rifdha Aurelia[1], Viona Violetta[2], Nickytha Nunik Rindi Aryani[3], Ahkmad Sayuti[4]

[1]Program Studi Sistem Informasi, Fakultas Sains dan Teknologi, Universitas Islam Negeri Raden Fatah Palembang
[1]rifdhaaurelia77@gmail.com, [2]vionavioletta013@gmail.com, [3]nickyth4811@gmail.com, [4]akhmad.sayuti.mkom@gmail.com

Abstrak

Aplikasi Weverse menghubungkan artis dan penggemar serta terintegrasi dengan layanan perdagangan elektronik, sehingga pengelolaan identitas pengguna dan akses logis menjadi aspek keamanan yang penting. Penelitian ini bertujuan mengevaluasi aspek pengelolaan identitas pengguna dan akses logis pada aplikasi Weverse yang dapat diamati dari sisi pengguna dengan mengacu pada DSS05.04 (*Manage User Identity and Logical Access*) COBIT 2019. Penelitian menggunakan pendekatan kualitatif deskriptif dengan desain studi kasus. Data dikumpulkan melalui observasi langsung terstruktur dan studi dokumen, kemudian dianalisis dengan tujuh indikator dan empat status keteramatan. Hasil menunjukkan bahwa enam dari tujuh indikator dapat diamati: empat berstatus Memenuhi dan dua berstatus Sebagian, sedangkan satu indikator tentang aspek internal tidak teramati dari sisi pengguna. Ditemukan dua kesenjangan, yaitu keunikan identitas akun yang tidak dapat diverifikasi (risiko rendah) dan pengaturan autentikasi dua faktor yang tidak ditemukan pada halaman yang diamati (risiko sedang). Rekomendasi utama adalah menyediakan opsi autentikasi dua faktor dan memperjelas informasi identitas akun. Hasil ini bukan audit menyeluruh dan tidak menetapkan tingkat kapabilitas proses.

Kata Kunci: Audit TI, COBIT 2019, DSS05.04, Weverse, Keamanan Akses

PENDAHULUAN

Sistem informasi dan teknologi informasi (SI/TI) menjadi bagian penting dalam kegiatan organisasi dan layanan digital. Penerapan sistem informasi dapat membantu integrasi teknologi, meningkatkan efisiensi operasional, serta mendukung pengambilan keputusan. Abdi (2025), melalui kajian sistematis literatur, membahas penerapan sistem informasi dalam transformasi digital dan kaitannya dengan perubahan proses serta pemanfaatan teknologi dalam organisasi.

Weverse merupakan platform digital yang menghubungkan artis dan penggemar serta terintegrasi dengan layanan perdagangan elektronik Weverse Shop. Platform tersebut menyediakan komunitas penggemar, siaran langsung, pesan, dan pembelian produk. Bollmer & Tillerson (2025) membahas Weverse sebagai platform yang menggabungkan aktivitas komunitas penggemar dan aktivitas ekonomi dalam ekosistem digital. Penelitian ini membatasi perhatian pada pengelolaan identitas pengguna dan akses logis yang dapat diamati melalui aplikasi.

Ketergantungan terhadap layanan digital juga disertai risiko, seperti akses tidak sah, kebocoran data, penyalahgunaan informasi, dan kelemahan pengamanan antarmuka aplikasi. Risiko tersebut bukan hanya bersifat teoretis. Dalam pemberitahuan resmi pada September 2026, Weverse Company menyatakan telah mengonfirmasi kebocoran yang mencakup 422.584 kasus berdasarkan unit ID akun. Informasi yang terdampak mencakup pengenal internal dan sejumlah informasi transaksi, seperti jenis pembayaran, nama *payment gateway*, mata uang, jumlah pembelian atau pembatalan, waktu transaksi, status pembelian, serta waktu pengembalian dana. Perusahaan menyebutkan bahwa kerentanan berkaitan dengan API pemrosesan informasi pembayaran dan menyatakan telah memperkuat kendali akses serta menghapus pengenal internal dari informasi yang terekspos (Weverse Company, 2026). Informasi tersebut berasal dari pengumuman perusahaan sehingga bukan hasil pemeriksaan independen, dan digunakan sebagai konteks pentingnya pengelolaan keamanan akses, bukan sebagai bukti bahwa praktik tertentu dalam COBIT telah gagal.

COBIT merupakan kerangka tata kelola dan manajemen informasi serta teknologi perusahaan yang dapat digunakan untuk menghubungkan kebutuhan pemangku kepentingan, tujuan organisasi, dan sasaran tata kelola maupun manajemen TI (ISACA, 2018). Penelitian ini memfokuskan pembahasan pada DSS05 (*Managed Security Services*) dan dibatasi pada aspek keamanan akses yang dapat diamati dari sisi pengguna melalui penggunaan aplikasi dan penelaahan informasi yang tersedia untuk umum. Kelompok tidak memeriksa konfigurasi server, kode sumber, basis data, atau API internal, tidak menguji kerentanan teknis, dan tidak menetapkan tingkat kapabilitas proses.

Penelitian terdahulu yang relevan antara lain Kurniawan et al. (2024), yang mengevaluasi tingkat kematangan keamanan layanan jaringan menggunakan COBIT 2019 pada domain DSS05 dan melaporkan DSS05.04 pada indeks 3,55 atau level 4. Arifin et al. (2024) menerapkan COBIT 2019 pada DSS05 untuk menganalisis keamanan Sistem Sawit Rakyat Online (SRO) di PTPN V dan melaporkan DSS05.04 berada pada level 4. Sementara itu, Putra et al. (2025) menggunakan COBIT 2019 untuk audit sistem informasi dengan fokus DSS05 dan melaporkan hasil keseluruhan pada level 1. Penelitian-penelitian

CC Attribution-ShareAlike 4.0 License.

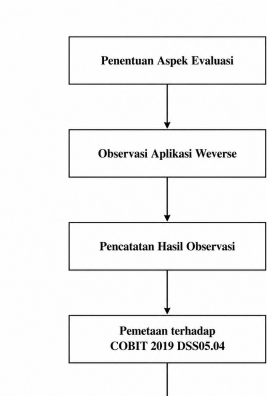
tersebut menjadi pembanding, tetapi objek, bukti, dan metode penilaiannya berbeda dari penelitian ini, yang membatasi evaluasi pada aspek DSS05.04 yang dapat diamati dari sisi pengguna.

Berdasarkan uraian tersebut, penelitian ini bertujuan (1) mengidentifikasi aspek pengelolaan identitas pengguna dan akses logis pada aplikasi Weverse yang dapat diamati dari sisi pengguna, (2) memetakan aspek yang diamati terhadap DSS05.04 COBIT 2019 tanpa mengklaim penilaian atas seluruh kontrol internal, dan (3) menyusun rekomendasi perbaikan berdasarkan temuan observasi dan informasi yang tersedia. Secara akademis, penelitian ini diharapkan menambah contoh penerapan COBIT 2019 pada aplikasi digital; secara praktis, hasilnya membantu memahami fitur autentikasi dan pengelolaan akun yang tersedia bagi pengguna.

METODE

Kerangka Pemikiran Evaluasi

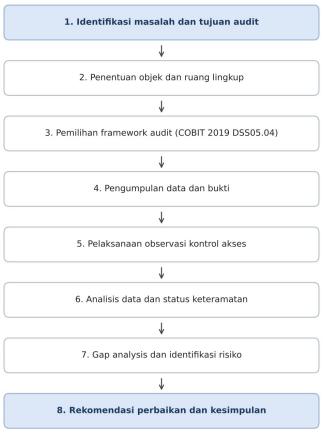
Kerangka pemikiran (Gambar 1) dimulai dari penentuan aspek pengelolaan identitas pengguna dan akses logis pada aplikasi Weverse. Kelompok mengamati proses *login*, opsi autentikasi tambahan, proses pemulihan akun, dan pengaturan akun yang berhubungan dengan akses; hasilnya dicatat beserta bukti, status keteramatan, dan keterbatasan, dipetakan terhadap DSS05.04, lalu digunakan menyusun rekomendasi yang sebanding dengan bukti.



Gambar 1. Kerangka Pemikiran Evaluasi

Tahapan Penelitian

Penelitian ini merupakan penelitian kualitatif deskriptif dengan desain studi kasus pada aplikasi Weverse. Pendekatan kualitatif dipilih karena data utama berupa hasil pengamatan terhadap fitur dan alur penggunaan, bukan data numerik (Creswell & Creswell, 2018). Dalam kerangka audit, kegiatan ini dilakukan sebagai evaluasi terbatas berbasis kriteria, yaitu proses sistematis untuk memperoleh bukti dan menilainya terhadap kriteria yang telah ditetapkan (International Organization for Standardization [ISO], 2018). Prosedur dilaksanakan dalam delapan tahap pada Gambar 2. Tahap 1 sampai 3 menyusun dasar audit (masalah dan tujuan, objek dan ruang lingkup, serta *framework*); tahap 4 dan 5 mengumpulkan bukti dan melaksanakan observasi kontrol akses; tahap 6 dan 7 menganalisis data, kesenjangan, dan risiko; tahap 8 merumuskan rekomendasi dan kesimpulan. Urutan ini mengikuti kegiatan audit pada umumnya, yaitu perencanaan, pengumpulan bukti, evaluasi terhadap kriteria, dan pelaporan (ISO, 2018).



Gambar 2. Alur Metode Penelitian

Objek, Ruang Lingkup, dan Framework Audit

Objek penelitian adalah aplikasi Weverse, khususnya fitur akun dan akses yang dapat digunakan oleh pengguna biasa. Ruang lingkup dibatasi pada pengelolaan identitas pengguna dan akses logis yang dapat diamati dari sisi pengguna, yaitu proses masuk, autentikasi tambahan jika tersedia, pemulihan akun, dan pengaturan keamanan akun. Penelitian tidak memeriksa

CC Attribution-ShareAlike 4.0 License.

konfigurasi server, kode sumber, basis data, maupun API internal, tidak melakukan uji penetrasi, dan tidak mengakses data pengguna lain; observasi dilakukan menggunakan akun milik anggota kelompok sendiri. *Framework* yang digunakan adalah COBIT 2019 pada domain DSS (*Deliver, Service and Support*), dengan sasaran DSS05 dan praktik DSS05.04 (*Manage User Identity and Logical Access*) sebagai kriteria audit (ISACA, 2018). Pemilihan DSS05 juga memungkinkan hasil dibandingkan secara konseptual dengan penelitian terdahulu (Arifin et al., 2024; Kurniawan et al., 2024; Putra et al., 2025).

Teknik Pengumpulan Data dan Instrumen

Data dikumpulkan melalui observasi langsung terstruktur dan studi dokumen. Pada observasi, anggota kelompok menjalankan alur proses masuk, autentikasi tambahan, pemulihan akun, dan pengaturan keamanan akun, kemudian mencatat apa yang ditampilkan aplikasi dan menyimpannya sebagai tangkapan layar bertanggal (Creswell & Creswell, 2018). Studi dokumen memanfaatkan informasi publik seperti pusat bantuan, ketentuan layanan, kebijakan privasi, dan pemberitahuan resmi Weverse Company (2026), serta literatur COBIT dan penelitian terdahulu. Wawancara dan kuesioner tidak digunakan karena kelompok tidak memiliki akses kepada pengelola sistem, berbeda dari Arifin et al. (2024). Setiap bukti diberi kode agar mudah dirujuk.

Instrumen berupa lembar observasi yang memuat indikator, kode bukti, status keteramatan, dan catatan. Indikator merupakan penjabaran dari tema praktik DSS05.04 (ISACA, 2018) dan, untuk autentikasi serta pemulihan akun, dilengkapi pedoman autentikasi digital NIST sebagai pembanding (Temoshok et al., 2025). Setiap indikator diberi salah satu dari empat status: Memenuhi, Sebagian, Belum memenuhi, atau Tidak teramati dari sisi pengguna. Indikator disajikan pada Tabel 1.

Tabel 1. Indikator Observasi

Kode	Indikator yang diamati	Acuan
I-01	Identifikasi pengguna: akun terdaftar dapat dibedakan secara unik (email atau ID akun)	DSS05.04
I-02	Autentikasi: metode masuk yang tersedia dan mekanisme verifikasi saat masuk	DSS05.04; NIST SP 800-63B-4
I-03	Autentikasi tambahan: ketersediaan verifikasi lain di luar kata sandi	DSS05.04; NIST SP 800-63B-4
I-04	Pemulihan akun: alur pemulihan dan verifikasi identitas sebelum akses dipulihkan	DSS05.04; NIST SP 800-63B-4
I-05	Pengaturan keamanan akun: perubahan kata sandi, pengelolaan sesi/perangkat, notifikasi aktivitas	DSS05.04
I-06	Perubahan atau pencabutan akses: keluar dari perangkat, penonaktifan, atau penghapusan akun	DSS05.04
I-07	Aspek internal: persetujuan perubahan hak akses, akun istimewa, pencatatan aktivitas, peninjauan berkala (dicatat "tidak teramati dari sisi pengguna")	DSS05.04

Teknik Analisis Data, Kesenjangan, dan Risiko

Data dianalisis secara kualitatif deskriptif melalui reduksi data, penyajian data, dan penarikan kesimpulan (Miles et al., 2014). Bukti dipilah dan dikaitkan dengan indikator, disajikan dalam matriks indikator-bukti-status, dan kesimpulan ditarik per indikator dengan mempertimbangkan kecukupan bukti. Keabsahan data dijaga melalui triangulasi antara hasil observasi dan informasi publik serta pemeriksaan silang antaranggota kelompok. Indikator yang tidak dapat dibuktikan dicatat sebagai "tidak teramati dari sisi pengguna" dan tidak dihitung sebagai ketidaksesuaian. Analisis kesenjangan membandingkan kondisi teramati dengan harapan dan hanya ditetapkan untuk indikator berstatus Sebagian atau Belum memenuhi. Setiap kesenjangan dinilai risikonya secara kualitatif berdasarkan kemungkinan dan dampak dengan skala rendah, sedang, dan tinggi yang disederhanakan dari panduan NIST (Joint Task Force Transformation Initiative, 2012). Rekomendasi disusun untuk setiap kesenjangan dan diurutkan berdasarkan tingkat risiko; aspek yang tidak teramati hanya dicatat sebagai saran verifikasi pada penelitian lanjutan dengan izin resmi.

HASIL DAN PEMBAHASAN

Gambaran Umum Aplikasi Weverse

Weverse dikembangkan untuk menghubungkan artis dengan penggemarnya melalui layanan berbasis komunitas, antara lain komunitas penggemar, unggahan konten, komunikasi, siaran langsung (*live streaming*), dan layanan yang terintegrasi dengan Weverse Shop. Setiap pengguna perlu memiliki akun untuk mengakses layanan tersebut, sehingga informasi identitas, proses *login*, pengaturan keamanan, dan pengelolaan akses perangkat relevan untuk diamati. Pengamatan dibatasi pada fitur yang dapat diakses pengguna biasa, sedangkan aspek internal pengelolaan akses dicatat sebagai keterbatasan.

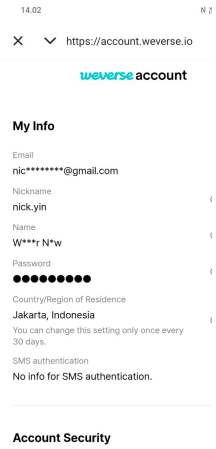
Hasil Observasi Aplikasi Weverse

Hasil observasi pada setiap indikator diuraikan pada subbab berikut. Bukti observasi B-01 sampai B-06 ditampilkan pada Gambar 3 sampai Gambar 8.

Identifikasi Pengguna (I-01)

Identifikasi pengguna merupakan salah satu aspek dalam pengelolaan identitas dan hak akses pengguna (*Manage User Identity and Logical Access*). Observasi dilakukan untuk mengetahui bagaimana aplikasi Weverse menyediakan informasi identitas yang dapat digunakan untuk mengenali dan membedakan setiap akun pengguna, melalui tampilan profil akun. Berdasarkan hasil observasi pada halaman *My Info* (Gambar 3), indikator identifikasi pengguna teramati melalui tersedianya informasi email, *nickname*, dan nama pengguna. Informasi email dan nama ditampilkan secara tersamarkan, sedangkan *nickname* ditampilkan secara langsung. Hal ini menunjukkan bahwa Weverse menyediakan informasi identitas akun pengguna. Namun, keunikan identitas akun belum dapat diverifikasi hanya melalui tampilan tersebut.

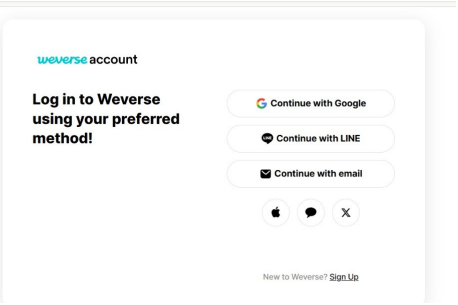
CC Attribution-ShareAlike 4.0 License.



Gambar 3. Halaman My Info (B-01)

Autentikasi (I-02)

Autentikasi merupakan aspek yang berkaitan dengan proses verifikasi identitas pengguna sebelum memperoleh akses ke dalam akun. Observasi dilakukan untuk mengetahui bagaimana aplikasi menerapkan proses autentikasi ketika pengguna melakukan *login*, termasuk metode autentikasi yang disediakan. Berdasarkan hasil observasi pada halaman *login* (Gambar 4), tersedia beberapa pilihan metode *login*, yaitu Google, LINE, email, Apple, dan metode lainnya. Dalam pengujian, peneliti menggunakan akun Google untuk masuk ke aplikasi Weverse dan berhasil diarahkan ke halaman utama. Hal ini menunjukkan bahwa Weverse menyediakan beberapa alternatif metode autentikasi, salah satunya melalui integrasi akun pihak ketiga seperti Google.

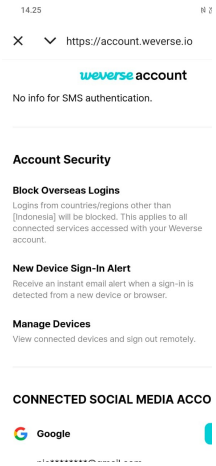


Gambar 4. Halaman Login Weverse (B-02)

Autentikasi Tambahan (I-03)

Autentikasi tambahan merupakan aspek yang berkaitan dengan mekanisme verifikasi identitas pengguna di luar proses autentikasi utama. Observasi dilakukan untuk mengetahui ketersediaan mekanisme verifikasi tambahan sebagai bentuk perlindungan terhadap akses akun. Berdasarkan hasil observasi pada halaman *Account Security* (Gambar 5), ditemukan fitur *New Device Sign-In Alert* yang memberikan notifikasi melalui email ketika terdapat aktivitas *login* dari perangkat atau *browser* baru. Selain itu, pada bagian *SMS Authentication* tertulis "No info for SMS authentication" dan belum ditemukan pengaturan autentikasi dua faktor (2FA) pada halaman yang diamati. Temuan ini menunjukkan bahwa Weverse menyediakan mekanisme pemberitahuan aktivitas *login* dari perangkat baru. Namun, penerapan mekanisme verifikasi tambahan untuk memastikan identitas pengguna belum dapat dibuktikan melalui observasi yang dilakukan.

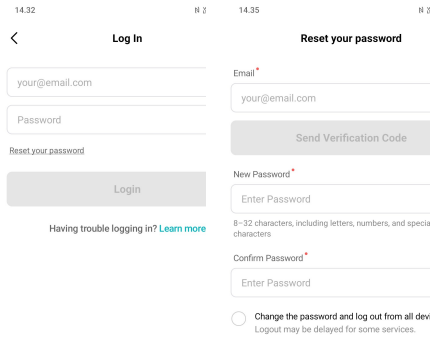
CC Attribution-ShareAlike 4.0 License.



Gambar 5. Halaman Account Security (B-03)

Pemulihan Akun (I-04)

Pemulihan akun merupakan aspek yang berkaitan dengan mekanisme memperoleh kembali akses akun ketika pengguna mengalami kendala dalam mengakses akunnya. Berdasarkan hasil observasi pada halaman *Reset your password* (Gambar 6), indikator pemulihan akun teramati melalui tersedianya mekanisme pengaturan ulang kata sandi. Pengguna diminta memasukkan alamat email untuk memperoleh kode verifikasi, kemudian membuat dan mengonfirmasi kata sandi baru. Selain itu, tersedia pilihan untuk mengeluarkan akun dari seluruh perangkat setelah perubahan kata sandi dilakukan. Hal ini menunjukkan bahwa Weverse menyediakan fasilitas pemulihan akun melalui verifikasi email.

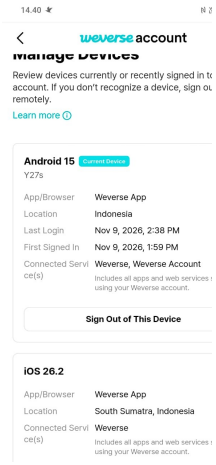


Gambar 6. Halaman Pemulihan Akun (B-04)

Pengaturan Keamanan Akun (I-05)

Pengaturan keamanan akun merupakan aspek yang berkaitan dengan fasilitas pengelolaan keamanan akun yang disediakan oleh aplikasi. Berdasarkan hasil observasi pada halaman *Account Security* dan *Manage Devices* (Gambar 7), indikator ini teramati melalui tersedianya fitur pengelolaan perangkat yang terhubung dengan akun Weverse. Pengguna dapat melihat informasi perangkat, sistem operasi, aplikasi yang digunakan, lokasi, serta riwayat waktu *login*. Selain itu, tersedia fitur *New Device Sign-In Alert*, *Block Overseas Logins*, dan pengaturan untuk mengeluarkan akun dari perangkat tertentu maupun seluruh perangkat. Fitur-fitur tersebut memberikan fasilitas bagi pengguna untuk memantau dan mengelola keamanan akses akun.

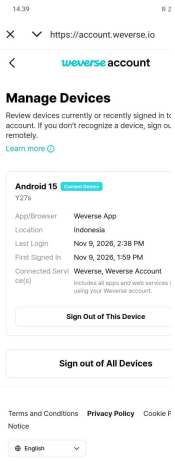
CC Attribution-ShareAlike 4.0 License.



Gambar 7. Halaman Manage Devices (B-05)

Perubahan dan Pencabutan Akses (I-06)

Perubahan dan pencabutan akses merupakan aspek yang berkaitan dengan pengelolaan akses pengguna terhadap akun. Berdasarkan hasil observasi pada halaman *Manage Devices* (Gambar 8), indikator ini teramati melalui tersedianya fitur *Sign Out of This Device* dan *Sign out of All Devices*. Fitur tersebut memungkinkan pengguna mengeluarkan akun dari perangkat tertentu maupun seluruh perangkat yang terhubung dengan akun Weverse. Dengan demikian, pengguna diberikan fasilitas untuk mengelola dan mencabut akses akun pada perangkat yang digunakan. Fitur penonaktifan atau penghapusan akun tidak diamati.



Gambar 8. Fitur Sign Out pada Manage Devices (B-06)

Aspek Internal Pengelolaan Akses (I-07)

Aspek internal pengelolaan akses berkaitan dengan mekanisme pengendalian identitas dan hak akses yang dilakukan oleh pihak pengelola sistem. Berdasarkan ruang lingkup observasi dari sisi pengguna, indikator ini tidak teramati. Proses persetujuan perubahan hak akses, pengelolaan akun istimewa, pencatatan aktivitas akses, dan peninjauan hak akses secara berkala merupakan aspek internal perusahaan yang tidak dapat diverifikasi melalui aplikasi Weverse. Oleh karena itu, aspek tersebut dicatat sebagai keterbatasan observasi dan tidak dinilai sebagai ketidaksesuaian.

Pemetaan terhadap COBIT 2019 DSS05.04

Pemetaan menjawab bagaimana aspek yang diamati dapat dipetakan terhadap DSS05.04 (ISACA, 2018). Setiap indikator pada Tabel 1 dikaitkan dengan tema praktik DSS05.04 dan dibandingkan dengan temuan observasi. Pemetaan hanya mencakup aspek yang dapat diamati dari sisi pengguna dan tidak digunakan untuk menetapkan tingkat kapabilitas proses (Tabel 2).

Tabel 2. Pemetaan Indikator terhadap DSS05.04

Indikator	Tema DSS05.04	Temuan ringkas	Status	Bukti
I-01 Identifikasi pengguna	Identifikasi pengguna secara unik	Email, nickname, nama tampil di My Info (tersamarkan); keunikan akun tidak dapat diverifikasi	Sebagian	B-01
I-02 Autentikasi	Autentikasi akses	Login via Google, LINE, email, Apple, dan lainnya; login Google berhasil	Memenuhi	B-02
I-03 Autentikasi tambahan	Autentikasi akses	New Device Sign-In Alert tersedia; SMS Authentication "No info"; 2FA tidak ditemukan	Sebagian	B-03

CC Attribution-ShareAlike 4.0 License.

Indikator	Tema DSS05.04	Temuan ringkas	Status	Bukti
I-04 Pemulihan akun	Autentikasi dan perubahan akses	Reset kata sandi via kode verifikasi email; opsi keluar dari seluruh perangkat	Memenuhi	B-04
I-05 Pengaturan keamanan akun	Pengelolaan hak akses dan perubahan akses	Manage Devices (perangkat, OS, lokasi, riwayat login); New Device Sign-In Alert; Block Overseas Logins	Memenuhi	B-05
I-06 Perubahan/pencabutan akses	Pengelolaan perubahan akses	Sign Out of This Device dan Sign out of All Devices	Memenuhi	B-06
I-07 Aspek internal	Persetujuan hak akses, akun istimewa, pencatatan, peninjauan berkala	Tidak dapat diverifikasi melalui aplikasi	Tidak teramati	-

Secara keseluruhan, dari tujuh indikator terdapat enam indikator yang dapat diamati dan satu indikator (I-07) yang tidak teramati dari sisi pengguna. Pada enam indikator yang teramati, empat berstatus Memenuhi, dua berstatus Sebagian, dan tidak ada yang berstatus Belum memenuhi. Status Sebagian pada I-01 mencerminkan keterbatasan bukti, bukan kegagalan kontrol. Indikator I-03 berstatus Sebagian karena aplikasi memberi notifikasi *login* perangkat baru, tetapi pengaturan 2FA tidak ditemukan; pedoman NIST menempatkan autentikasi sebagai bagian penting keamanan akun (Temoshok et al., 2025), sehingga ketiadaan opsi verifikasi tambahan yang dapat diatur pengguna dicatat sebagai kesenjangan. Pada *login* melalui akun pihak ketiga seperti Google, perlindungan tambahan dapat diatur pada penyedia akun tersebut, yang berada di luar pengamatan ini.

Analisis Kesenjangan dan Risiko

Kesenjangan hanya ditetapkan untuk indikator berstatus Sebagian atau Belum memenuhi, sehingga I-07 tidak dianalisis. Harapan disusun dari tema DSS05.04 (ISACA, 2018) dan, untuk autentikasi serta pemulihan akun, dibandingkan dengan pedoman NIST (Temoshok et al., 2025). Hasilnya disajikan pada Tabel 3.

Tabel 3. Analisis Kesenjangan

Indikator	Harapan	Kondisi teramati	Kesenjangan
I-01 Identifikasi pengguna	Akun terdaftar dapat dibedakan secara unik	Informasi identitas ditampilkan, keunikan tidak dapat diverifikasi	Ada (G-01)
I-02 Autentikasi	Terdapat verifikasi identitas saat masuk	Tersedia beberapa metode login	Tidak ada
I-03 Autentikasi tambahan	Tersedia verifikasi lain di luar kata sandi	Hanya notifikasi login perangkat baru; 2FA tidak ditemukan	Ada (G-02)
I-04 Pemulihan akun	Pemulihan disertai verifikasi identitas	Pemulihan melalui kode verifikasi email	Tidak ada
I-05 Pengaturan keamanan akun	Tersedia pengaturan keamanan yang dapat dikelola pengguna	Manage Devices, notifikasi perangkat baru, Block Overseas Logins	Tidak ada
I-06 Perubahan/pencabutan akses	Tersedia fitur untuk mengakhiri akses	Sign Out of This Device dan Sign out of All Devices	Tidak ada

Ditemukan dua kesenjangan. **G-01** (I-01): halaman *My Info* menampilkan email, *nickname*, dan nama (B-01), tetapi keunikan identitas tidak dapat dipastikan dari tampilan, sehingga lebih bersifat keterbatasan verifikasi daripada kelemahan sistem. **G-02** (I-03): *Account Security* menyediakan *New Device Sign-In Alert*, tetapi *SMS Authentication* tertulis "No info" dan pengaturan 2FA tidak ditemukan (B-03). Penilaian ini terbatas pada halaman yang diamati, sehingga fitur serupa di tempat lain atau pada penyedia akun pihak ketiga tidak tercakup.

Risiko dinilai secara kualitatif dari kemungkinan dan dampak menggunakan matriks pada Tabel 4, dan hasil penilaian disajikan pada Tabel 5. Penilaian ini merupakan perkiraan berdasarkan bukti dari sisi pengguna, bukan pengukuran kerentanan teknis.

Tabel 4. Matriks Tingkat Risiko

Kemungkinan \ Dampak	Rendah	Sedang	Tinggi
Rendah	Rendah	Rendah	Sedang
Sedang	Rendah	Sedang	Tinggi
Tinggi	Sedang	Tinggi	Tinggi

Tabel 5. Penilaian Risiko

Kode	Kesenjangan	Kemungkinan	Dampak	Tingkat risiko
G-01	Keunikan identitas akun tidak dapat diverifikasi dari tampilan (I-01)	Rendah	Rendah	Rendah
G-02	Pengaturan 2FA tidak ditemukan pada halaman yang diamati (I-03)	Sedang	Sedang	Sedang

Pada G-01, kemungkinan dan dampak dinilai rendah karena kesenjangan muncul dari keterbatasan verifikasi, informasi email dan nama ditampilkan tersamarkan, dan tidak ada indikasi penyalahgunaan identitas. Pada G-02, kemungkinan dinilai sedang karena akun yang masuk dengan email dan kata sandi bergantung pada kekuatan kata sandi bila tidak ada verifikasi tambahan, meskipun notifikasi perangkat baru, pengelolaan perangkat, dan *Block Overseas Logins* membantu pengguna membatasi akses yang tidak dikenal. Dampak dinilai sedang karena akun terhubung dengan layanan komunitas dan Weverse Shop sehingga pengambilalihan akun dapat memengaruhi data akun dan informasi transaksi. Dari dua kesenjangan, tidak ada

CC Attribution-ShareAlike 4.0 License.

yang berisiko tinggi, satu berisiko sedang, dan satu berisiko rendah. Insiden yang diumumkan Weverse Company (2026) hanya menjadi konteks pentingnya keamanan akses; penelitian ini tidak memiliki bukti teknis mengenai penyebabnya sehingga tidak menyimpulkan hubungan sebab-akibat dengan kesenjangan yang ditemukan.

Pembahasan

Hasil observasi menunjukkan bahwa Weverse menyediakan fitur dasar pengelolaan identitas dan akses yang dapat diamati pengguna, mencakup beberapa metode *login*, pemulihan akun melalui kode verifikasi, pengelolaan perangkat, dan pencabutan akses dari perangkat. Empat dari enam indikator teramati berstatus Memenuhi, dan aspek yang perlu perhatian lebih terutama berada pada autentikasi tambahan. Jika dikaitkan dengan DSS05.04 (ISACA, 2018), tema autentikasi dan perubahan akses dapat diamati dari antarmuka, sedangkan persetujuan hak akses, akun istimewa, pencatatan aktivitas, dan peninjauan berkala tidak dapat dinilai tanpa bukti internal, sehingga evaluasi dari sisi pengguna hanya menggambarkan sebagian DSS05.04.

Putra et al. (2025) melaporkan hasil keseluruhan level 1 untuk sistem akademik sekolah, Arifin et al. (2024) melaporkan level 4 dengan nilai 4,33 untuk SRO di PTPN V, dan Kurniawan et al. (2024) melaporkan DSS05.04 pada indeks 3,55 atau level 4 untuk layanan jaringan. Hasil penelitian ini tidak dapat dibandingkan secara angka karena memakai status keteramatan, bukan tingkat kapabilitas, dan hanya bertumpu pada bukti dari sisi pengguna. Namun, perbedaan hasil di antara penelitian terdahulu memperkuat pandangan bahwa hasil evaluasi bergantung pada objek, bukti, dan pendekatan penilaian. Penelitian ini melengkapinya dengan contoh evaluasi aplikasi publik yang dibatasi pada bukti yang dapat diamati.

Penelitian ini memiliki tiga keterbatasan. Pertama, observasi hanya dari sisi pengguna sehingga aspek internal DSS05.04 tidak teramati. Kedua, observasi dilakukan pada akun anggota kelompok sendiri dan pada kondisi aplikasi saat pengamatan, sehingga hasilnya dapat berubah mengikuti pembaruan aplikasi. Ketiga, penelitian tidak menguji kerentanan teknis dan tidak menetapkan tingkat kapabilitas proses, sehingga hasilnya tidak dapat digeneralisasi sebagai penilaian menyeluruh atas keamanan Weverse.

Rekomendasi Perbaikan

Rekomendasi diurutkan berdasarkan tingkat risiko dan sebanding dengan bukti. Aspek yang tidak teramati hanya berupa saran verifikasi lanjutan karena belum ada bukti ketidaksesuaian (Tabel 6).

Tabel 6. Rekomendasi Perbaikan

Kode	Rekomendasi	Prioritas
G-02	Menyediakan opsi autentikasi dua faktor yang dapat diaktifkan pengguna pada halaman Account Security, misalnya melalui aplikasi autentikator atau kode verifikasi, serta memperjelas keterangan SMS Authentication yang tertulis "No info for SMS authentication" (ISACA, 2018; Temoshok et al., 2025).	Prioritas 1 (risiko sedang)
G-01	Menampilkan penjelasan atau pengenal akun yang jelas pada halaman informasi akun dan menjelaskan di pusat bantuan cara identitas akun dikelola.	Prioritas 2 (risiko rendah)
I-07	Memverifikasi persetujuan perubahan hak akses, akun istimewa, pencatatan aktivitas akses, dan peninjauan berkala melalui wawancara atau bukti internal dengan izin resmi.	Verifikasi lanjutan

Bagi pengguna, fitur yang dapat dimanfaatkan segera adalah mengaktifkan *New Device Sign-In Alert* dan *Block Overseas Logins*, meninjau daftar perangkat pada *Manage Devices* secara berkala, mengeluarkan akun dari perangkat yang tidak dikenal, dan menggunakan kata sandi yang unik, guna mengurangi risiko selama opsi 2FA belum tersedia pada halaman yang diamati.

KESIMPULAN

Berdasarkan hasil observasi dari sisi pengguna, aplikasi Weverse menyediakan identifikasi akun, beberapa metode *login*, notifikasi *login* dari perangkat baru, pemulihan akun melalui kode verifikasi email, pengelolaan perangkat, serta fitur keluar dari perangkat. Enam dari tujuh indikator dapat diamati dan dipetakan terhadap DSS05.04, dengan empat indikator berstatus Memenuhi dan dua berstatus Sebagian. Aspek internal (I-07) tidak teramati dari sisi pengguna sehingga dicatat sebagai keterbatasan, bukan ketidaksesuaian.

Ditemukan dua kesenjangan, yaitu keunikan identitas akun yang tidak dapat diverifikasi dengan risiko rendah dan autentikasi dua faktor yang tidak ditemukan pada halaman yang diamati dengan risiko sedang. Rekomendasi utama adalah menyediakan opsi autentikasi dua faktor dan memperjelas keterangan *SMS Authentication*, kemudian memperjelas informasi identitas akun serta menganjurkan pengguna mengaktifkan fitur keamanan yang tersedia. Hasil penelitian ini hanya menggambarkan kondisi yang teramati dari sisi pengguna saat observasi, bukan audit menyeluruh, dan tidak menetapkan tingkat kapabilitas DSS05.04. Penelitian selanjutnya disarankan memperluas observasi pada lebih banyak perangkat, sistem operasi, dan metode *login*, serta memverifikasi aspek internal DSS05.04 melalui wawancara atau bukti internal dengan izin resmi.

DAFTAR PUSTAKA

Abdi, N. S. (2025). Analisis sistematis literatur tentang penerapan sistem informasi dalam transformasi digital. *Simtek: Jurnal Sistem Informasi dan Teknik Komputer, 10*(1), 58–62. https://doi.org/10.51876/SIMTEK.V10I1.1477

Arifin, H., Angraini, A., Ahsyar, T. K., & Syaifullah, S. (2024). Analisis keamanan sistem informasi menggunakan COBIT 2019 pada Sistem Sawit Rakyat Online (SRO) studi kasus PTPN V. *Jurnal Teknologi Sistem Informasi dan Aplikasi, 7*(3), 903–911. https://doi.org/10.32493/JTSI.V7I3.39650

Bollmer, G., & Tillerson, B. (2025). Platform fandom: Weverse and the technological domestication of fan community. *Social Media and Society, 11*(1). https://doi.org/10.1177/20563051251326689

CC Attribution-ShareAlike 4.0 License.

Creswell, J. W., & Creswell, J. D. (2018). *Research design: Qualitative, quantitative, and mixed methods approaches* (5th ed.). SAGE Publications.

International Organization for Standardization. (2018). *ISO 19011:2018 Guidelines for auditing management systems* (3rd ed.). ISO.

ISACA. (2018). *COBIT 2019 framework: Governance and management objectives*. ISACA.

Joint Task Force Transformation Initiative. (2012). *Guide for conducting risk assessments* (NIST Special Publication 800-30 Rev. 1). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-30r1

Kurniawan, D. A., Aprillya, M. R., & Handoyo, E. (2024). Analysis of network service security maturity level using COBIT 2019 framework. *Indonesian Journal of Engineering, Science and Technology, 1*(1), 1–13. https://doi.org/10.38040/IJENSET.V1I1.716

Miles, M. B., Huberman, A. M., & Saldaña, J. (2014). *Qualitative data analysis: A methods sourcebook* (3rd ed.). SAGE Publications.

Putra, B. A., Christian, D. R., & Daniati, E. (2025). Audit sistem informasi menggunakan kerangka COBIT 2019 DSS05. *Prosiding SEMNAS INOTEK*. https://proceeding.unpkediri.ac.id/index.php/inotek/article/download/7796/5142/30488

Temoshok, D., Fenton, J., Choong, Y.-Y., Lefkovitz, N., Regenscheid, A., Galluzzo, R., & Richer, J. (2025). *Digital identity guidelines: Authentication and authenticator management* (NIST Special Publication 800-63B-4). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-63b-4

Weverse Company. (2026, September). *Notice to our Weverse customers*. Weverse Shop. https://shop.weverse.io/en/notices/14265

CC Attribution-ShareAlike 4.0 License.