Pelaksanaan Audit Keamanan Sistem Informasi Absensi Greatday Menggunakan Framework NIST

Nur Ayu Wulantari[1*], Tata Sutabri[2]
[1,2] Magister Teknologi Informatika, Universitas Bina Darma, Jln. Jendral Ahmad Yani No 3 Seberang Ulu I Palembang , Indonesia
Email : [*1]**wulantarinurayu@gmail.com**, tata.sutabri@gmail.com

Abstrak

Aplikasi sistem informasi absensi GreatDay adalah aplikasi absensi yang mempermudah pencatatan kehadiran karyawan secara otomatis dan real-time, baik dalam kondisi online maupun offline, dengan dukungan fitur seperti pengenalan wajah (Face Recognition). Penelitian ini bertujuan untuk mengevaluasi keamanan sistem informasi absensi GreatDay dengan menggunakan framework NIST, yang meliputi perencanaan audit, identifikasi sistem, penilaian risiko, implementasi kontrol keamanan, dan pengujian efektivitas kontrol. Untuk memastikan sistem ini berfungsi secara optimal dan aman, diperlukan audit keamanan sistem informasi menggunakan kerangka kerja NIST (National Institute of Standards and Technology). NIST memberikan panduan terkait audit keamanan sistem informasi untuk mengidentifikasi potensi risiko dan ancaman, serta untuk mengevaluasi penerapan kontrol keamanan yang tepat. Dari hasil penelitian ini dapat ditari kesimpulan bahwa Greatday Sistem Informasi sudah terdapat pada level 3, itu artinya prosedur dan control yang telah ditetapkan oleh pihak institusi sudah diterapkan. Level yang didapatkan merupakan hasil penilaian audit keamanan secara menyeluruh yang berada pada angka 3,7005 dari 5.

***Kata kunci**: Sistem Informasi Absensi, GreatDay, NIST, Keamanan Sistem, Audit, Face Recognition.*

.

Abstract

The GreatDay attendance information system application is an attendance app that facilitates the automatic and real-time recording of employee attendance, both online and offline, with support for features such as facial recognition (Face Recognition). This study aims to evaluate the security of the GreatDay attendance information system using the NIST framework, which includes audit planning, system identification, risk assessment, implementation of security controls, and testing the effectiveness of controls. To ensure that the system functions optimally and securely, an information system security audit is needed using the NIST (National Institute of Standards and Technology) framework. NIST provides guidelines for auditing information system security to identify potential risks and threats, as well as to evaluate the implementation of appropriate security controls. Based on the results of this study, it can be concluded that the attendance information system is at level 3, indicating that the procedures and controls set by the institution have been implemented. This conclusion is based on the overall security audit assessment, which scored 3.7005 out of 5.

***Keywords**: Attendance Information System, GreatDay, NIST, System Security, Audit, Face Recognition.*

1. PENDAHULUAN

Sistem informasi dibuat untuk membantu aktivitas dan proses bisnis agar lebih mudah, efektif dan efisien[1]. Begitupun dengan sistem informasi absensi yaitu suatu aplikasi berbasis teknologi informasi yang diciptakan agar membantu kinerja progres serta laporan dalam hal kehadiran atau absensi pegawai. Sistem aplikasi absensi adalah perangkat lunak yang digunakan untuk mencatat kehadiran karyawan atau siswa secara otomatis. Sistem ini sangat membantu dalam meningkatkan efisiensi administrasi dan mengurangi kesalahan manual dalam pencatatan kehadiran.

Salah satu aplikasi sistem informasi absensi yang saat ini banyak digunakan di Perusahaan besar yaitu aplikasi GreatDay[2]. Aplikasi Greatday yaitu suatu Fitur Absensi yang dapat mencatat kehadiran online dan offline dengan pengenalan wajah, menyediakan riwayat absensi yang akurat dan terintegrasi dengan penggajian. Sistem aplikasi ini juga dapat memungkinkan pengajuan yang efisien dengan berbagai tipe fleksibel, menyediakan riwayat dan status pengajuan yang bisa dimonitor sendiri[3]. Fitur *Face Matching* dan *Face Recognition* menolak rekam kehadiran karyawan yang tidak sesuai wajah dan tidak dilakukan secara *real-time*. Sistem Informasi Absensi GreatDay ini dapat memastikan data yang terekam akurat dan *real-time*. Namun dalam penggunaanya aplikasi ini memiliki kendala jika terjadi kesalahan *input* data dan tidak terekam oleh sistem maka akan dilakukan pemotongan gaji otomatis pada saat akhir bulan. Karena pentingnya data pribadi yang diinput dan rekam dalam aplikasi ini maka perlu dilakukan evaluasi keamaanan sistem informasi ini terhadap kebocoran data, serangan siber dan gangguan lainnya yang dapat merugikan karyawan.

Framework NIST telah digunakan dalam beberapa jurnal ilmiah yang berhubungan dengan keamanan dari suatu sistem informasi. NIST merupakan sebuah kerangka kerja yang dipublikasikan oleh *National Institute of Standard Technology* (NIST)[5]. Proses ini sangat lengkap sehingga dapat meliputi semua kegiatan manajemen Risiko, mulai dari identifikasi ancaman, sampai rekomendasi kontrol [4] Penelitian ini menggunakan kerangka kerja NIST (*National Institute of Standard and Technology*) khusus untuk tipe data kualitatif serta dapat mengidentifikasi, mengevaluasi dan mengelola Risiko TI dalam sistem secara keseluruhan.

Beberapa penelitian yang berkaitan dengan Audit keamanan sistem informasi absensi menggunakan metode NIST telah dilakukan. Penelitian yang dilakukan oleh Rangga S mengenai audit keamaanan sistem informasi akademik pada Universitas Sangga Buana YPKB Bandung metode yang digunakan menggunakan tahapan dari *framework* NIST. Hasil yang didapatkan yaitu memperoleh skor 3,6005 dari 5. Merujuk pada tingkatan keamanan sistem informasi yang terdapat di dalam *framework* NIST SP 800-26 yang digunakan, Manajemen kontrol berada pada tingkat 3, yaitu *implemented procedures and controls*. Itu artinya, prosedur dan pengendalian yang direncanakan oleh pihak institusi secara keseluruhan sudah dijalankan.[6]

Penelitian yang dilakukan oleh Rizka NW dan teman-teman mengenai audit sistem informasi absensi juga dengan studi kasus pada PT. Metal Castindo Industritama dengan menggunakan *framework* Cobit 5. Hasil yang didapatkan sistem absensi sebagai alat untuk menjaga dan mengelola keamanan sistem informasi dan telah berada pada level 4 yakni *Predictable Process* dengan nilai *capability* sebesar 3,6.[7]

Penelitian yang dilakukan oleh Reynaldi G mengenai audit keamanan & manajemen resiko pada *e-learning* UNIB. Hasil yang didapatkan sebagai berikut : (1) Dampak sistem *e-Learning* terhadap manajemen kontrol sangat positif yaitu 85,04%. (2) *Operational control* 75,6% dan *technical control* 76,8% cukup baik, namun masih perlu pengembangan. (3) Keamanan sistem berada pada level 3 (*implemented procedures and control*) dengan nilai 79,14%. (4) Analisis OWASP ZAP menemukan 17 kriteria kerentanan pada website el.unibi.ac.id. (5) Rekomendasi: perbaikan program keamanan, kontrol berkala, analisis insiden rutin, penggunaan server khusus, dan dokumentasi aktivitas pengguna.[8]

Penelitian yang dilakukan oleh Mia NS & Besus MS yang dilakukan tentang audit sistem informasi absensi pada PT. Intan Salsabila, hasil dari Kesimpulan kuesioner yang telah disebar

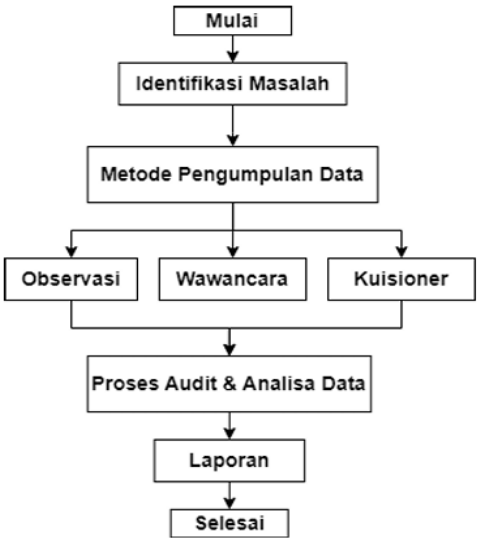
dengan urutan domain dengan nilai tertinggi yaitu domain DSS01.01 *Perform Operational Procedure* sehingga mendapatkan nilai *maturity level* 10. [9]

Setelah mengkaji beberapa penelitian terdahulu tersebut, penulis berusaha melakukan evaluasi aplikasi Greatday ini dengan menggunakan *framework* NIST karena terdapat beberapa persamaan dengan penelitian sebelumnya yaitu dengan mengumpulkan berbagai referensi audit sistem informasi mengenai Aplikasi Greatday dengan berbagai *framework* khususnya cobit 8 dan kami memberikan pandangan baru dengan melakukan penelitian ini karena dari beberapa penelitian belum ditemukan audit keamanan dari sistem informasi absensi *Greatday* sehingga penggunaan aplikasi ini dapat lebih optimal bagi perusahaan ataupun karyawan.

Dengan dilakukan pelaksanaan audit pada sistem aplikasi Greatday menggunakan framework NIST maka diharapkan dapat mengevaluasi dan memastikan keamanan sistem absensi *online* ini dalam penggunaanya memang benar melindungi data pribadi dan aman dari kebocoran sistem serta dapat membantu para karyawan perusaahaan dan berguna sebagaimana mestinya.

2. METODE PENELITIAN

Tahapan metode penelitian yang dilakukan dalam penelitian ini yaitu :



Gambar 1. Tahapan Metode Penelitian

Langkah awal yaitu melakukan analisa masalah pada aplikasi Greatday. Apa saja kendala yang terdapat pada aplikasi absensi Greatday tersebut. Adapun hasil identifikasi yang telah kami rumuskan dari penelitian ini adalah :

1. Pada Aplikasi Greatday Pengecekan arsip Log absensi tidak dapat dicek langsung pada Aplikasi.
2. Notifikasi peringatan untuk karyawan melakukan absensi kerja tidak otomatis tersimpan pada ponsel pengguna.

Terdapat beberapa metode pengumpulan data yang digunakan dalam penelitian ini, diantaranya:

2.1 Kuisioner

Pada penelitian ini digunakan kuesioner untuk mengumpulkan data dari pengguna sistem mengenai pengalaman mereka, kepuasan, dan kendala yang mereka temui. Penulis memberikan beberapa Pertanyaan Terstruktur (*Closed-Ended Questions*): Pertanyaan ini memberikan pilihan jawaban yang sudah ditentukan sebelumnya. Responden hanya perlu memilih jawaban yang paling sesuai. Kuisioner diberikan kepada 10 orang karyawan yang memang benar menggunakan sistem informasi absensi Greatday dalam pekerjaan sehari-hari.

2.2 Wawancara

Wawancara adalah suatu percakapan langsung dengan tujuan-tujuan tertentu dengan menggunakan format tanya jawab[6]. Pada Penelitian ini wawancara dilakukan kepada pengguna sistem untuk memahami proses, kebijakan, dan kendala yang dihadapi dalam penggunaan sistem absensi. Pertanyaan yang diberikan berupa Pertanyaan Terstruktur yaitu Pertanyaan yang sudah ditentukan sebelumnya dan memiliki pilihan jawaban yang terbatas sehingga digunakan untuk mendapatkan data yang lebih terorganisir dan mudah dianalisis. Dalam proses penelitian ini wawancara dilakukan dengan 10 karyawan yang menggunakan sistem absensi Greatday. Berikut rangkuman hasil dari wawancara:

Tabel 1. Hasil Wawancara

No	Hasil Wawancara
1.	Sering terjadi data error mengakibatkan data absensi tidak tersimpan dan tidak dapat diperbaiki
2.	Kekhawatiran perlindungan data pribadi di setiap input data jika terjadi kegagalan *face recognition*
3.	Terdapat pemotongan gaji yang tidak sesuai
4.	Aplikasi rentan diretas dan data yang telah diinput sering hilang dan tidak tersimpan
5.	Beberapa karyawan merasa khawatir karena data yang diinput di sistem sangat berhubungan dengan gaji bulanan dan lembur bulanan sehingga dipertanyakan keamanannya.

2.3 NIST SP 800-26

Berikut ini merupakan tabel tipe kontrol dan sub kategori dari *framework* NIST SP 800-26 :

Tabel 2. Tipe kontrol NIST SP 800-26

No	Tipe Kontrol	17 Sub Kategori Kontrol
1	*Management Control*	*a. Authorize Processing* *b. Life Cycle* *c. Review of Security Control* *d. Risk Management*
2	*Operational Control*	*a. Physical Security* *b. Personnal Security* *c. Contingency Planning* *d.. Hardware and System Software Maintenance* *e. Documentation* *f. Data Integrity* *g.. Hardware and System Software Maintenance* *h. Production, Input and Output Control*
3	*Technical Control*	*a. Logical Access Control* *b. Audit Trails* *c. Identification and Authentication*

NIST SP 800-26 pun menyebutkan terdapat 5 tingkatan keamanan pada teknologi informasi, yaitu.

Tabel 3. Tingkatan Kebijakan dari NIST SP 900-26

No	Tingkatan	Keterangan
1	Tingkat 1	*Documented Policy* (Kebijakan Terdokumentasi)
2	Tingkat 2	*Documented Procedures* (Prosedur terdokumentasi)
3	Tingkat 3	*Implemented Procedures and Controls* (Prosedur pengendalian sudah dilakukan)
4	Tingkat 4	*Tested and Reviewed Procedures and Controls* (Prosedur dan pengendalian sudah diuji dan dikaji ulang)
5	Tingkat 5	*Fully Integrated Procedures and Controls* (Prosedur dan pengendalian sepenuhnya sudah terintegrasi)

Pelaksanaan audit sistem informasi absensi GreatDay menggunakan *framework* NIST melibatkan langkah-langkah sistematis untuk memastikan bahwa sistem tersebut aman, efektif, dan sesuai dengan standar yang ditetapkan. Berikut adalah langkah-langkah yang bisa diambil[10]:

1. Perencanaan Audit
   Langkah yang pertama yaitu menentukan tujuan audit sistem informasi. Tujuan audit sistem informasi absensi pegawai ini adalah menilai keamanan data absensi, kepatuhan terhadap kebijakan privasi, dan efektivitas kontrol akses. Ruang lingkup dari penelitian ini adalah untuk mengidentifikasi bagian sistem yang akan diaudit, termasuk modul absensi, penyimpanan data, dan antarmuka pengguna. [11]
2. Identifikasi dan Klasifikasi Sistem
   Mengidentifikasi komponen sistem absensi GreatDay yang mencakup aplikasi, basis data, dan infrastruktur. Mengklasifikasikan data yang dikumpulkan (misalnya, data pribadi karyawan) berdasarkan sensitivitasnya.
3. Penilaian Risiko
   Menggunakan NIST SP 800-30 untuk melakukan analisis risiko, termasuk identifikasi ancaman (misalnya, akses tidak sah, kehilangan data) dan kerentanan (misalnya, kelemahan dalam kontrol akses).
4. Implementasi Kontrol Keamanan
   Memeriksa penerapan kontrol keamanan berdasarkan NIST SP 800-53, seperti akses control yaitu nilai kebijakan kontrol akses dan autentikasi serta melakukan eknsripsi data dengan cara memeriksa penggunaan enkripsi untuk data yang disimpan dan dikirim serta Memastikan adanya log aktivitas pengguna dan pemantauan sistem. [7]
5. Pengujian dan Evaluasi Kontrol

Melakukan pengujian untuk mengevaluasi efektivitas kontrol yang diterapkan, termasuk pengujian penetrasi untuk mengidentifikasi kerentanan dengan cara Wawancara dengan staf untuk memahami proses dan kepatuhan terhadap kebijakan.[12]

Dengan mengikuti langkah-langkah ini, audit sistem informasi absensi GreatDay dapat membantu memastikan bahwa sistem tersebut aman dan efektif dalam melindungi data kehadiran, serta memenuhi regulasi yang berlaku.

3. HASIL DAN PEMBAHASAN

Berikut ini hasil identifikasi ancaman-ancaman internal dan eksternal pada audit sistem informasi aplikasi Greatday:

Tabel 4. Identifikasi sumber ancaman dan jenis ancaman system informasi

No	Sumber Ancaman	Jenis Ancaman
1	Individu di luar organisasi	*Clickjacking, Spam, Network and Port Scanning, Denial Of Service, CSRF, Session fixation, cookie disclosure, Network Sniffing, malware, Virus dan Social Engineering, Information Disclosure, Blind SQL Injection*
2	Individu di dalam organisasi (pegawai)	*Network Sniffing, malware, Virus dan Social Engineering , CSRF, Session fixation, cookie disclosure, Clickjacking, Spam, Network and Port Scanning, Information Disclosure, Blind SQL Injection, Denial Of Service,*
3	Perlengkapan TI (media penyimpanan pada server)	Gagal fungsi media penyimpanan, seperti : *Error* atau disk full.
4	Perlengkapan TI (jaringan komunikasi data)	Gagal melakukan komunikasi dikarenakan terdapat Serangan *Flood/collusion , Wireless Jamming,* perusakan secara langsung perangkat atau jalur komunikasi data.
5	Pemprosesan data sistem informasi	Kegagalan sistem informasi
6	Bencana alam lainnya	Data hilang , Sistem mati, dan infrastruktur IT rusak

3.1 Hasil Penelitian

Penilaian penelitian ini berupa hasil dari data kuisioner dari 20 orang responden. Hasil penilaian tersebut telah diolah sehingga dapat mendapatkan hasil akhir penilaian.

Tabel 5. Penilaian *Management Control*

No	Kriteria	Rata-rata	Rata-rata akhir	Presentase
1	1.a	3,6125	3,5425	70,85
2	1.b	3,6500		
3	1.c	3,5750		
4	1.d	3,4000		
5	1.e	3,4750		

Berdasarkan hasil perhitungan dari data kuesioner, diperoleh nilai penilaian untuk manajemen kontrol sebesar 3,5425 dari 5. Mengacu pada tingkat keamanan sistem informasi dalam framework NIST SP 800-26 yang digunakan, manajemen kontrol berada pada tingkat 3, yaitu prosedur dan kontrol yang telah diterapkan. Ini menunjukkan bahwa prosedur dan pengendalian yang telah direncanakan oleh institusi terkait manajemen kontrol sudah dilaksanakan.

3.2 Penilaian Operational Control

Tabel 6. Penilaian Operational Control

No	Kriteria	Rata-rata	Rata-rata akhir	Presentasi
1	2.a	3,5375	3,5975	71,94
2	2.b	3,4750		
3	2.c	3,4500		
4	2.d	3,6250		
5	2.e	3,9250		
6	2.f	3,6375		
7	2.g	3,6000		
8	2.h	3,5875		
9	2.i	3,5375		

Berdasarkan perhitungan dari data kuesioner, hasil penilaian untuk manajemen kontrol adalah 3,5972 dari 5. Mengacu pada tingkat keamanan sistem informasi dalam framework NIST SP 800-26 yang digunakan, manajemen kontrol berada pada tingkat 3, yaitu prosedur dan kontrol yang telah diterapkan. Ini berarti bahwa prosedur dan pengendalian yang direncanakan oleh institusi terkait kontrol operasional sudah dilaksanakan.

3.3 Penilaian Technical Control

Tabel 7. Penilaian *Operational Control*

No	Kriteria	Rata-rata	Rata-rata akhir	Presentas (%)
1	3.a	3,6625	3,6917	73,83
2	3.b	3,6750		
3	3.c	3,7375		

Berdasarkan perhitungan dari data kuesioner, nilai penilaian untuk manajemen kontrol adalah 3,6917 dari 5. Mengacu pada tingkat keamanan sistem informasi dalam framework NIST SP 800-26 yang digunakan, manajemen kontrol berada pada tingkat 3, yaitu prosedur dan kontrol yang telah diterapkan. Hal ini menunjukkan bahwa prosedur dan pengendalian yang direncanakan oleh institusi terkait kontrol teknis sudah dilaksanakan.

3.4 Penilaian Keseluruhan

Tabel 8. Penilaian Keseluruhan

No	Kriteria	Rata-rata	Rata-rata akhir	Presentase (%)
1	1	3,5425	3,7005	72,43%
2	2	2,5972		
3	3	3,6917		

Berdasarkan perhitungan data kuesioner, nilai penilaian secara keseluruhan adalah 3,7005 dari 5. Mengacu pada tingkat keamanan sistem informasi dalam framework NIST SP 800-26 yang digunakan, manajemen kontrol berada pada tingkat 3, yaitu prosedur dan kontrol yang telah diterapkan. Ini berarti bahwa prosedur dan pengendalian yang direncanakan oleh institusi secara keseluruhan sudah dilaksanakan.

3.5 Validitas Data

Penentuan validitas data pada penelitian ini menggunakan rumus :

$$CVI = \frac{\text{Jumlah item yang disetujui oleh panel ahli}}{\text{Total jumlah item yang dievaluasi}}$$

Validitas konten menunjukkan sejauh mana item-item dalam kuisioner mencakup semua aspek dari konsep yang diukur.
CVI = Jumlah item yang disetujui oleh ahli
Jumlah total item
Jumlah item
Interpretasi : CVI yang lebih besar dari 0,8 menunjukkan validitas konten yang baik.

Validitas suatu alat ukur dapat diartikan sebagai sifat yang menunjukkan bahwa alat ukur tersebut dapat digunakan untuk mengukur karakter yang dimaksud. Validitas merujuk pada tingkat akurasi dari alat ukur tersebut. Alat ukur dianggap valid jika dapat menghasilkan pengukuran yang tepat untuk suatu masalah tertentu, namun tidak dapat digunakan untuk mengukur masalah lain. Alat ukur yang valid dan akurat memiliki tingkat validitas yang tinggi, sementara alat ukur yang kurang valid memiliki validitas yang rendah. Secara umum, validitas alat ukur bergantung pada faktor logika dan bukti statistik.[14]
Berikut adalah table dari hasil uji validitas data kuisioner yang telah dirangkum :

Tabel 9. Validitas Data Kusioner

No	Kriteria	Validitas
1	1.a	Valid
2	1.b	Valid
3	1.c	Valid
4	1.d	Valid
5	1.e	Valid
6	2.a	Valid
7	2.b	Valid
8	2.c	Valid
9	2.d	Valid
10	2.e	Valid
11	2.f	Valid
12	2.g	Valid
13	2.h	Valid
14	2.i	Valid
15	3.a	Valid
16	3.b	Valid
17	3.c	Valid

3.6 Rekomendasi Tindaklanjut
Hasil penelitian uji validitas :

Tabel 10. Hasil Uji Validitas

No	Tipe Kontrol	Kriteria	Validitas	Rata-rata akhir	Presentasi (%)
1	*Management Control*	*a. Authorize Processing*	Valid	3,5425	72,43%
		b. Life Cycle	Valid		
		c. Review of Security Control	Valid		
		d. Risk Management	Valid		
2	*Operational Control*	*a. Physical Security*	Valid	2,5972	
		b. Personnal Security	Valid		
		c. Contingency Planning	Valid		
		d. Production, Input and Output Control	Valid		
		e. Hardware and System Software Maintenance	Valid		
		f. Documentation	Valid		
		g. Data Integrity	Valid		
3	*Technical Control*	*a. Identification and Authentication*	Valid	3,6917	
		b. Audit Trails	Valid		
		c. Logical Access Control	Valid		

Dari hasil riset yang telah dilakukan menggunakan Framework NIST dengan 3 tipe kontrol (1,2,3) dan 17 sub kategori tipe kontrol (a,b,c,d,e,f,g) rekomendasi dari penulis agar aplikasi dapat dipastikan aman, efektif, dan sesuai dengan kebijakan yang berlaku, serta dapat mendukung kebutuhan perusahaan dalam mengelola data kehadiran karyawan dengan lebih baik maka sistem informasi absensi Greatday ini harus melakukan perbaikan program keamanan, kontrol berkala, analisis insiden rutin, penggunaan server khusus, dan dokumentasi aktivitas pengguna Rekomendasi tindak lanjut untuk pihak manajemen yang diaudit terkait keamanan sistem informasi harus berfokus pada perbaikan yang dapat meningkatkan pertahanan terhadap ancaman siber, menjaga integritas data, serta memastikan kepatuhan terhadap standar dan peraturan yang berlaku.

4. KESIMPULAN

Berdasarkan hasil penilaian secara keseluruhan menggunakan Framework NIST dengan 3 kategori dan 17 subkategori, diperoleh hasil sebagai berikut: untuk Management Control, rata-rata nilai uji validitas adalah 3,55425; untuk Operational Control, nilai yang diperoleh adalah 2,5972; dan untuk Technical Control, nilai mencapai 3,6917. Rata-rata nilai kontrol secara keseluruhan adalah 3,7005 dari 5, yang setara dengan 72,43%. Berdasarkan hasil penilaian pelaksanaan audit keamanan terhadap sistem informasi absensi pada aplikasi Greatday, dapat disimpulkan bahwa sistem informasi absensi tersebut sudah berada pada tingkat 3, yang

menunjukkan bahwa prosedur dan pengendalian yang ditetapkan oleh pihak institusi sudah diterapkan. Kesimpulan ini diperoleh berdasarkan hasil penilaian audit keamanan secara keseluruhan dengan nilai 3,7005 dari 5.

DAFTAR PUSTAKA

[1] R. N. Wahidah, N. Lutfiyana, V. F. Ramadanti, P. Septiyo, and R. Drefiyanto, "AUDIT SISTEM INFORMASI ABSENSI MESIN FINGERPRINT PADA PT. METAL CASTINDO INDUSTRITAMA DENGAN MENGGUNAKAN FRAMEWORK COBIT 5". doi: 9827/klik.v4i2.1173.

[2] R. Kurnia Candra, I. Atastina, and Y. Firdaus, "Audit Teknologi Informasi menggunakan Framework COBIT 5 Pada Domain DSS (Delivery, Service, and Support) (Studi Kasus : iGracias Telkom University)." vol. 2, no. 8, pp. 18-19, 2023, Available : http://openjournal.unpam.ac.id/index.php/informatika

[3] R. Sekar, A. N. Afifah, and E. Zuraidah, "KLIK: Kajian Ilmiah Informatika dan Komputer Audit Sistem Informasi Aplikasi Absensi Greatday Menggunakan Framework Cobit 5," *Media Online)*, vol. 4, no. 2, pp. 926–936, 2023, doi: 10.30865/klik.v4i2.1173.

[4] B. A. Nugraha, A. R. Perdanakusuma, and A. Rachmadi, "Analisa Manajemen Risiko pada Sistem Informasi Tata Naskah Dinas Elektronik dengan Kerangka Kerja NIST 800-30 pada Dinas Komunikasi dan Informatika Provinsi Jawa Timur," 2020. [Online]. Available: http://j-ptiik.ub.ac.id

[5] K. Ananta Wijaya and I. Wayan Septa Malan Vergantara, "Audit Tata Kelola Sistem Informasi Rekam Medis Primary Care dengan Framework Cobit 5 pada Puskesmas I Denpasar Barat Primary Care Medical Record Information System Governance Audit with Cobit 5 Framework at Puskesmas I Denpasar Barat." [Online]. Available: https://ejournal.politeknikkesehatankartinibali.ac.id/index.php/pkm/

[6] R. S. Perdana, "AUDIT KEAMANAN SISTEM INFORMASI AKADEMIK MENGGUNAKAN FRAMEWORK NIST SP 800-26 (Studi Kasus : Universitas Sangga Buana YPKP Bandung)," *Jurnal Infotronik*, vol. 3, no. 1, 2018. Available : Available : http://openjournal.unpam.ac.id/index.php/informatika

[7] R. N. Wahidah, N. Lutfiyana, V. F. Ramadanti, P. Septiyo, and R. Drefiyanto, "AUDIT SISTEM INFORMASI ABSENSI MESIN FINGERPRINT PADA PT. METAL CASTINDO INDUSTRITAMA DENGAN MENGGUNAKAN FRAMEWORK COBIT 5". doi: doi: klik.v4i2.187.

[8] R. Gimnastiar and R. Nursyanti, "SEMINAR NASIONAL CORISINDO Audit Keamanan Dan Manajemen Risiko Dengan Menggunakan Framework NIST (Studi Kasus : E-Learning UNIBI)." doi: 10.30865/klik.v4i2.1173.

[9] S. Alya Shafa and A. Muchayan, "Penerapan Metode Design Thinking dalam Perancangan Aplikasi Layanan Pengaduan Hukum Berbasis Mobile". doi: 90/klik.v4i2.1567.

[10] F. Mahardika, "Manajemen Risiko Keamanan Informasi Menggunakan Framework NIST SP 800-30 Revisi 1 (Studi Kasus: STMIK Sumedang)," vol. 02, no. 02, 2017. Available : http://openjournal.unpam.ac.id/index.php/informatika.

[11] Tata Sutabri, *Pengantar Sistem Informasi*, VI., vol. 1. Yogyakarta: Penerbit ANDI, 2016.

[12] H. Budi, S. : Manajemen, R. Pada, H. B. Santoso, and L. Ernawati, "Manajemen Risiko Pada Pusat Data Perguruan Tinggi Dengan Kerangka Kerja NIST 800-30 (Studi Kasus: Universitas Kristen Duta Wacana)," *8 JUISI*, vol. 03, no. 02, 2017. doi: /klik.v4i2.90.

[13] S. Alya Shafa and A. Muchayan, "Penerapan Metode Design Thinking dalam Perancangan Aplikasi Layanan Pengaduan Hukum Berbasis Mobile". vol. 4, no. 2, pp. 926–936, 2023, doi: 10.30865/klik.v4i2.1173.

[14] N. Sasongko, J. Akuntansi, F. Ekonomi, U. Jenderal, and A. Yani, "PENGUJIAN KEAMANAN TRANSAKSI CLOUD COMPUTING PADA LAYANAN SOFTWARE AS A SERVICE (SaaS)

MENGGUNAKAN KERANGKA KERJA NIST SP800-53A (Studi Kasus pada PT. X di Bandung),” 2011. vol. 4, no. 2, pp. 926–936, 2023, Available : http://openjournal.unpam.ac.id/index.php/informatika

[15] Nur Ayuwulantari, Tata Sutabri, “Optimalisasi Manajemen Layanan RSUD Besemah Dengan Framework Cobit 5 Untuk Meningkatkan Efisiensi dan Keamanan”. Available : http://jurnal.polsri.ac.id/index.php/jupiter