

**THE IMPLEMENTATION OF PERSONAL DATA PROTECTION
LAW ON INFORMATION SYSTEM SECURITY RISKS USING
OCTAVE-S**

TUGAS AKHIR

Diajukan Sebagai Salah Satu Syarat
untuk Memperoleh Gelar Sarjana Komputer pada
Program Studi Sistem Informasi

Oleh:

GITA NURUL AINI

11950320643



UIN SUSKA RIAU

UIN SUSKA RIAU

State Islamic University of Sultan Syarif Kasim Riau

UNIVERSITAS ISLAM NEGERI SULTAN SYARIF KASIM RIAU
PEKANBARU

2023

Hak Cipta Dilindungi Undang-Undang

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber:

a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penyusunan laporan, penulisan kritik atau tinjauan suatu masalah.
b. Pengutipan tidak merugikan kepentingan yang wajar UIN Suska Riau.

2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin UIN Suska Riau.

LEMBAR PERSETUJUAN

THE IMPLEMENTATION OF PERSONAL DATA PROTECTION LAW ON INFORMATION SYSTEM SECURITY RISKS USING OCTAVE-S

TUGAS AKHIR

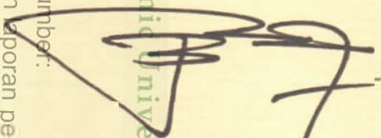
Oleh:

GITA NURUL AINI

11950320643

Telah diperiksa dan disetujui sebagai Laporan Tugas Akhir
di Pekanbaru, pada tanggal 04 Juli 2023

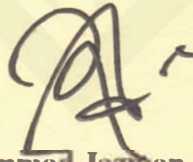
Ketua Program Studi



Eki Saputra, S.Kom., M.Kom.

NIP. 198307162011011008

Pembimbing



Muhammad Jazman, S.Kom., M.Infosys.

NIP. 198206042015031004

- Hak Cipta Dilindungi Undang-Undang
1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber:
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penyusunan laporan penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar UIN Suska Riau.
 2. Dilarang mengumunkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin UIN Suska Riau.

LEMBAR PENGESAHAN

THE IMPLEMENTATION OF PERSONAL DATA PROTECTION LAW ON INFORMATION SYSTEM SECURITY RISKS USING OCTAVE-S

TUGAS AKHIR

Oleh:

GITA NURUL AINI

11950320643

Telah dipertahankan di depan sidang dewan penguji
sebagai salah satu syarat untuk memperoleh gelar Sarjana Komputer
Fakultas Sains dan Teknologi Universitas Islam Negeri Sultan Syarif Kasim Riau
di Pekanbaru, pada tanggal 03 Juli 2023

Pekanbaru, 03 Juli 2023

Mengesahkan,

Ketua Program Studi



Eki Saputra, S.Kom., M.Kom.

NIP. 198307162011011008

Dekan

Dr. Hartono, M.Pd.

NIP. 196403011992031003

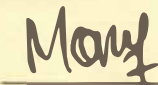
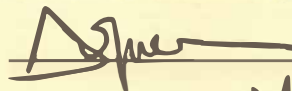
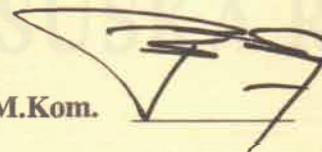
DEWAN PENGUJI:

Ketua : Eki Saputra, S.Kom., M.Kom.

Sekretaris : Muhammad Jazman, S.Kom., M.Infosys.

Anggota 1 : Dr. Angraini, S.Kom., M.Eng.

Anggota 2 : Mona Fronita, S.Kom., M.Kom.



- Hak Cipta Dilindungi Undang-Undang
1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber.
 2. Dilarang mengutip hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penyusunan laporan, penulisan kritik atau tinjauan suatu masalah.
 3. Dilarang tidak meragikan kepentingan yang wajar UIN Suska Riau.
 4. Dilarang mengemukakan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin UIN Suska Riau.

© Hak Cipta milik UIN Suska Riau

LEMBAR HAK ATAS KEKAYAAN INTELEKTUAL

Tugas Akhir yang tidak diterbitkan ini terdaftar dan tersedia di Perpustakaan Universitas Islam Negeri Sultan Syarif Kasim Riau adalah terbuka untuk umum, dengan ketentuan bahwa hak cipta ada pada penulis. Referensi kepustakaan diperkenankan dicatat, tetapi pengutipan atau ringkasan hanya dapat dilakukan atas izin penulis dan harus dilakukan mengikuti kaedah dan kebiasaan ilmiah serta menyebutkan sumbernya.

Penggandaan atau penerbitan sebagian atau seluruh Tugas Akhir ini harus memperoleh izin tertulis dari Dekan Fakultas Sains dan Teknologi Universitas Islam Negeri Sultan Syarif Kasim Riau. Perpustakaan dapat meminjamkan Tugas Akhir ini untuk anggotanya dengan mengisi nama, tanda peminjaman dan tanggal pinjam pada *form* peminjaman.

Hak Cipta Diindungi Undang-Undang

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber:
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penyusunan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar UIN Suska Riau.
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin UIN Suska Riau.

LEMBAR PERNYATAAN

Dengan ini saya menyatakan bahwa dalam Tugas Akhir ini tidak terdapat karya yang pernah diajukan untuk memperoleh gelar kesarjanaan di suatu Perguruan Tinggi, dan sepanjang pengetahuan saya juga tidak terdapat karya atau pendapat yang pernah ditulis atau diterbitkan oleh orang lain kecuali yang secara tertulis diadukan dalam naskah ini dan disebutkan di dalam daftar pustaka.

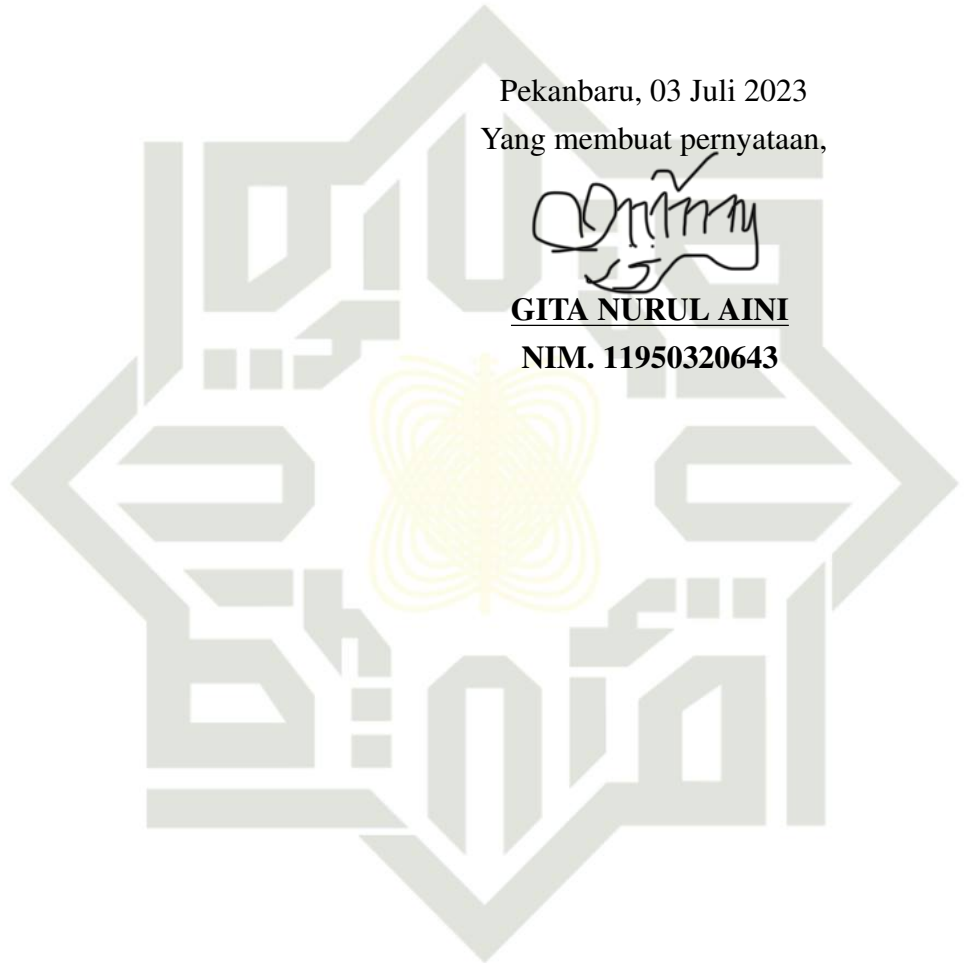
Pekanbaru, 03 Juli 2023

Yang membuat pernyataan,



GITA NURUL AINI

NIM. 11950320643



UIN SUSKA RIAU

Hak Cipta Dilindungi Undang-Undang

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber:
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penyusunan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar UIN Suska Riau.
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin UIN Suska Riau.

LEMBAR PERSEMBAHAN

بِسْمِ اللَّهِ الرَّحْمَنِ الرَّحِيمِ

Dengan menyebut nama Allah yang maha pengasih lagi maha penyayang

Assalamu'alaikum Warahmatullahi Wabarakaatuh.

Alhamdulillah Rabbil 'Alamin, segala puji bagi Allah Subhanahu Wa Ta'ala sebagai bentuk rasa syukur atas segala nikmat yang telah diberikan tanpa ada kekurangan sedikitpun. Shalawat beserta salam tak lupa pula kita ucapkan kepada Nabi Muhammad Shallallahu 'Alaihi Wa Sallam dengan mengucapkan Allahumma Sholli'ala Sayyidina Muhammad Wa'ala Ali Sayyidina Muhammad. Semoga kita semua selalu senantiasa mendapat syafa'at-Nya di dunia maupun di akhirat, aamiin ya rabbal'alaamiin.

Dengan ini peneliti persembahkan Tugas Akhir kepada kedua orang tua terhebat dan motivator terbesar dalam hidup peneliti, **Ayahanda Wangsul** dan **Ibunda Irawati**. Untuk Ibunda tercinta, terima kasih atas dukungan, nasihat, do'a, dan semangat yang Ibunda berikan kepada peneliti selama ini. Kasih sayang yang selalu diberikan setiap waktu membuat peneliti merasa kuat menghadapi segala tantangan dan rintangan dunia. Untuk Ayahanda tercinta, terima kasih atas kasih sayang yang berlimpah yang telah diberikan sampai detik ini kepada peneliti. Do'a dan dukungan selalu diberikan agar semua keinginan peneliti bisa terwujud. Peneliti akan melakukan yang terbaik untuk setiap kepercayaan yang Ayahanda dan Ibunda berikan. Semua jerih payah Ayahanda dan Ibunda tak bisa dinilai dengan apapun.

Terima kasih juga peneliti sampaikan pada kakak peneliti **Vivi Pratiwi** dan adek **Grananda Hafidzul** yang telah menemani peneliti sedari kecil hingga detik ini. Terima kasih untuk segala waktu berharga yang telah kita lalui bersama, do'a, dan dukungan yang tiada hentinya. Semoga kita menjadi pribadi yang baik dan dapat mengharumkan nama keluarga.

Tugas Akhir ini merupakan kado kecil dari peneliti untuk Ayahanda, Ibunda, Kakak dan Adek peneliti yang tidak pernah henti-hentinya memberikan peneliti do'a dan dukungan dalam menyelesaikan Tugas Akhir. Semoga kita semua selalu diberikan rahmat, karunia, hidayah, serta innayah-Nya. *Aamiin.*

Wassalamu'alaikum Warahmatullahi Wabarakaatuh.

KATA PENGANTAR

Alhamdulillah Rabbil 'Alamin, bersyukur kehadiran Allah *Subhanahu Wa Ta'ala* atas segala rahmat dan karunia-Nya sehingga peneliti dapat menyelesaikan Tugas Akhir ini dengan baik dan tepat waktu. Shalawat serta salam tidak lupa pula kita ucapkan kepada Nabi Muhammad *Shallallahu 'Alaihi Wa Sallam* dengan mengucapkan *Allahumma Sholli'Ala Sayyidina Muhammad Wa'Ala Ali Sayyidina Muhammad*. Tugas Akhir ini dibuat sebagai salah satu syarat untuk memperoleh gelar Sarjana Komputer di Program Studi Sistem Informasi Fakultas Sains dan Teknologi Universitas Islam Negeri Sultan Syarif Kasim Riau.

Pada Kesempatan ini peneliti ingin menyampaikan ucapan terimakasih kepada Allah *Subhanahu Wa Ta'ala* yang telah memberikan kesehatan dan kekuatan, serta ucapan terimakasih terkhususnya kepada Ayahanda Wangsul dan Ibunda Irawati yang telah mendo'akan dan mendukung yang terbaik kepada peneliti, serta menjadi penyemangat dalam hidup peneliti. Tidak lupa pula peneliti mengucapkan terima kasih dan do'a kepada:

1. Bapak Prof. Dr. Hairunas, M.Ag sebagai Rektor Universitas Islam Negeri Sultan Syarif Kasim Riau.
2. Bapak Dr. Hartono, M.Pd sebagai Dekan Fakultas Sains dan Teknologi.
3. Bapak Eki Saputra, S.Kom., M.Kom sebagai Ketua Program Studi Sistem Informasi sekaligus ketua sidang Tugas Akhir peneliti.
4. Ibu Siti Monalisa, ST., M.Kom sebagai Sekretaris Program Studi Sistem Informasi.
5. Bapak Tengku Khairil Ahsyar, S.Kom., M.Kom sebagai Kepala Laboratorium Program Studi Sistem Informasi.
6. Bapak Inggih Permana, ST., M.Kom sebagai Dosen Pembimbing Akademik peneliti yang telah banyak memberikan arahan, masukan, dan motivasi selama perkuliahan mulai dari Semester 1 hingga Semester 8 ini.
7. Bapak Muhammad Jazman, S.Kom., M.Infosys sebagai pembimbing Tugas Akhir yang telah banyak memberikan arahan, masukan, nasihat, serta motivasinya baik dalam penyelesaian Tugas Akhir, maupun juga dalam perkuliahan dan kehidupan sehari-hari. Setiap motivasi yang diberikan akan selalu peneliti ingat dan dijadikan sebagai pelajaran hidup.
8. Ibu Dr. Angraini, S.Kom., M.Eng dan Ibu Mona Fronita, S.Kom., M.Kom sebagai Penguji peneliti yang telah banyak memberikan arahan, nasihat, masukan, serta motivasinya baik dalam penyelesaian Tugas Akhir, maupun

Hak Cipta Dilindungi Undang-Undang

1. Diarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber:
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penyusunan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar UIN Suska Riau.
2. Diarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin UIN Suska Riau.

juga dalam perkuliahan dan kehidupan sehari-hari. Setiap motivasi yang diberikan akan selalu peneliti ingat dan dijadikan sebagai pelajaran hidup.

Seluruh Bapak dan Ibu Dosen Program Studi Sistem Informasi yang telah banyak memberikan ilmunya kepada peneliti. Semoga ilmu yang diberikan dapat peneliti amalkan dan menjadi amal jariyah.

Seluruh Pegawai dan Staff Fakultas Sains dan Teknologi Universitas Islam Negeri Sultan Syarif Kasim Riau yang telah membantu dan mempermudah proses administrasi selama perkuliahan ini.

Satria Ananda Pratama C.F, ST sebagai teknisi PTPN V yang telah memberikan bantuan, motivasi dan arahan, serta meluangkan waktu dalam setiap proses menyelesaikan Tugas Akhir.

Terkhusus kepada kakak dan adek peneliti tercinta Vivi Pratiwi dan Grananda Hafidzul yang selalu memberikan semangat dan dukungan.

Made Agus Rizky Prabawa Kurnia dan Alriwanda kakanda Prodi Sistem Informasi yang telah memberikan dukungan, arahan, dan materi dalam proses pengerjaan Tugas Akhir.

Teman-teman Sistem Informasi 2019 khususnya Kelas B yang telah menemani selama menuntut ilmu di kampus dan untuk sahabat(Lisa, Adel, dan Fidia) yang telah membantu mempersiapkan keperluan seminar dan sidang.

Teman-teman KKN Basilam Baru, Kota Dumai yang telah hadir dan juga memberikan motivasi dalam menyelesaikan Tugas Akhir.

Peneliti menyadari dalam laporan ini masih banyak kesalahan dan kekurangan. Oleh karena itu, kritik dan saran yang membangun sangat diharapkan untuk kesempurnaan Laporan ini. Akhir kata peneliti ucapkan terimakasih.

Pekanbaru, 04 Juli 2023

Peneliti,



GITA NURUL AINI

NIM. 11950320643

Hak Cipta Dilindungi Undang-Undang

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber:
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penyusunan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar UIN Suska Riau.
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin UIN Suska Riau.



KLIK: Kajian Ilmiah Informatika dan Komputer

ISSN 2723-3898 (media online)

Jalan Sisingamangaraja No. 338, Sumatera Utara, Medan

Website <https://djournals.com/klik> | Email: jurnal.klikbd@gmail.com

Publisher Universitas Budi Darma

Medan, 12 Juni 2023

No : 158/KLIK/LOA/VI/2023
Lamp :-
Hal : Surat Penerimaan Naskah Publikasi Jurnal

Kepada Yth,
Bapak/Ibu **Gita Nurul Aini**
Di Tempat

Terimakasih telah mengirimkan artikel ilmiah untuk diterbitkan pada **KLIK: Kajian Ilmiah Informatika dan Komputer** (ISSN 2723-3898 (media online)), dengan judul:

The Implementation of Personal Data Protection Law on Information System Security Risks Using OCTAVE-S

Penulis: **Gita Nurul Aini(*)**, **Muhammad Jazman**, **Angraini**, **Mona Fronita**

Berdasarkan hasil review, artikel tersebut dinyatakan DITERIMA untuk dipublikasikan pada **Volume 3, Nomor 6, Juni 2023**.

QR-Code di bawah merupakan kode digital sebagai penanda keaslian LOA yang telah dikeluarkan dan akan menuju pada link LOA yang telah dikeluarkan pada Jurnal KLIK.

Sebagai informasi tambahan, saat ini **KLIK: Kajian Ilmiah Informatika dan Komputer** (ISSN 2723-3898 (media online)) telah TERAKREDITASI dengan Peringkat SINTA 4 berdasarkan Surat Keputusan peringkat Akreditasi periode III 2022, dari Kementerian Pendidikan, Kebudayaan, Riset, dan Teknologi, Direktorat Jendral Pendidikan Tinggi, Riset dan, Teknologi No [225/E/KPT/2022](#), tanggal 7 Desember 2022.

Demikian surat ini kami sampaikan, atas perhatiannya kami ucapkan terimakasih.



Hormat Kami,

Surya Darma Nasution, M.Kom
Ketua Editor

Tembusan:

1. Peringgal
2. Author

ISSN 2723-3898 (Media Online)

KLIK: Kajian Ilmiah Informatika dan Komputer

Volume 3 No 6 Juni 2023

Dipublikasikan Oleh



STMIK BUDI DARMA

Jalan Sisingamangaraja No. 338
Sumatera Utara

Website <http://stmik-budidarma.ac.id/>

LAMPIRAN A

DAFTAR ISI

© Hak cipta milik UIN Suska Riau

State Islamic University of Sultan Syarif Kasim Riau

Hak Cipta Dilindungi Undang-Undang

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber:
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penyusunan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar UIN Suska Riau.
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin UIN Suska Riau.

KLIK: KAJIAN ILMIAH INFORMATIKA DAN KOMPUTER
Register Login

HOME E-JOURNAL CURRENT ARCHIVES ABOUT EDITORIAL TEAM REVIEWER
SEARCH

HOME / ARCHIVES / Vol. 3 No. 6 (2023): Juni 2023

Vol. 3 No. 6 (2023): Juni 2023

DOI: <https://doi.org/10.30865/klik.v3i6.316>

PUBLISHED: 2023-06-24

ARTICLES

Implementasi Business Intelligence Menggunakan Tableau Untuk Visualisasi Data Dampak Bencana Banjir di Indonesia 586-594

- Dandie Triyanto (Universitas Muhammadiyah Prof. Dr. Hamka, Jakarta, Indonesia)
- Muchammad Sholeh (Universitas Muhammadiyah Prof. Dr. Hamka, Jakarta, Indonesia)
- Firman Noor Hasan (Universitas Muhammadiyah Prof. Dr. Hamka, Jakarta, Indonesia)

DOI: <https://doi.org/10.30865/klik.v3i6.769> Abstract View: 92 times PDF Download: 35 times

[PDF](#)

Cybersecurity Supply Chain Risk Management Using NIST SP 800-161r1 595-601

- Rahmi Aulia Astri (Universitas Islam Negeri Sultan Syarif Kasim Riau, Pekanbaru, Indonesia)
- Muhammad Jazman (Universitas Islam Negeri Sultan Syarif Kasim Riau, Pekanbaru, Indonesia)
- Syaifulah (Universitas Islam Negeri Sultan Syarif Kasim Riau, Pekanbaru, Indonesia)
- Eki Saputra (Universitas Islam Negeri Sultan Syarif Kasim Riau, Pekanbaru, Indonesia)

DOI: <https://doi.org/10.30865/klik.v3i6.799> Abstract View: 36 times PDF Download: 15 times

[PDF](#)

Analisis Usability Pada Sistem Informasi LAPORBUP Menggunakan Performance Measurement, Retrospective Think Aloud dan User Experience Questionnaire 754-764

- Mohamad Ariansidi (Universitas Pendidikan Ganesha, Singaraja, Indonesia)
- I Made Candiasa (Universitas Pendidikan Ganesha, Singaraja, Indonesia)
- I Made Gede Sunarya (Universitas Pendidikan Ganesha, Singaraja, Indonesia)

DOI: <https://doi.org/10.30865/klik.v3i6.807> Abstract View: 12 times PDF Download: 7 times

[PDF](#)

The Implementation of Personal Data Protection Law on Information System Security Risks Using OCTAVE-5 765-772

- Gita Nurul Aini (Universitas Islam Negeri Sultan Syarif Kasim, Pekanbaru, Indonesia)
- Muhammad Jazman (Universitas Islam Negeri Sultan Syarif Kasim Riau, Pekanbaru, Indonesia)
- Angraini (Universitas Islam Negeri Sultan Syarif Kasim Riau, Pekanbaru, Indonesia)
- Mona Fronita (Universitas Islam Negeri Sultan Syarif Kasim Riau, Pekanbaru, Indonesia)

DOI: <https://doi.org/10.30865/klik.v3i6.848> Abstract View: 16 times PDF Download: 12 times

[PDF](#)

Analisis Sentimen Ulasan Pelanggan Pada Aplikasi Fore Coffee Menggunakan Metode Naive Bayes 773-779

- Tia Anggia Sari (Universitas Muhammadiyah Prof. Dr. Hamka, Jakarta, Indonesia)
- Estu Sinduningrum (Universitas Muhammadiyah Prof. Dr. Hamka, Jakarta, Indonesia)
- Firman Noor Hasan (Universitas Muhammadiyah Prof. Dr. Hamka, Jakarta, Indonesia)

DOI: <https://doi.org/10.30865/klik.v3i6.884> Abstract View: 22 times PDF Download: 11 times

[PDF](#)

Pengaruh Distribusi dan Parameter terhadap Kinerja Sistem Antrian 780-785

- Mukarramah Yusuf (Universitas Hasanuddin, Makassar, Indonesia)

DOI: <https://doi.org/10.30865/klik.v3i6.878> Abstract View: 5 times PDF Download: 4 times

[PDF](#)

Klasifikasi Sentimen Masyarakat di Media Sosial Twitter terhadap Calon Presiden 2024 Prabowo Subianto dengan Metode K-NN 786-797

- Aivaldy Rahmat Rivita (Universitas Islam Negeri Sultan Syarif Kasim Riau, Pekanbaru, Indonesia)
- Yusra (Universitas Islam Negeri Sultan Syarif Kasim Riau, Pekanbaru, Indonesia)
- Muhammad Fikry (Universitas Islam Negeri Sultan Syarif Kasim Riau, Pekanbaru, Indonesia)

DOI: <https://doi.org/10.30865/klik.v3i6.890> Abstract View: 15 times PDF Download: 9 times

Accredited
SINTA 4

Ada Pertanyaan?
 Chat Via WhatsApp
SINERGI KLIK TOGA WA

Submit a Manuscript



Article
template
Indonesia



Article
template
English

Contact Us

Editorial Team

Reviewer

Hak Cipta Diindungi Undang-Undang

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber:
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penyusunan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar UIN Suska Riau.
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin UIN Suska Riau.

Analisis Usability Pada Sistem Informasi LAPORBUP Menggunakan Performance Measurement, Retrospective Think Aloud dan User Experience Questionnaire

- Mohamad Ariansidi (Universitas Pendidikan Ganesha, Singaraja, Indonesia)
- I Made Canelasa (Universitas Pendidikan Ganesha, Singaraja, Indonesia)
- I Made Gede Sunarya (Universitas Pendidikan Ganesha, Singaraja, Indonesia)

DOI: <https://doi.org/10.30865/iklik.v3i6.807> Abstract View: 12 times PDF Download: 7 times



The Implementation of Personal Data Protection Law on Information System Security Risks Using OCTAVE-S

- Gita Nuru Aini (Universitas Islam Negeri Sultan Syarif Kasim, Pekanbaru, Indonesia)
- Muhammad Jazman (Universitas Islam Negeri Sultan Syarif Kasim Riau, Pekanbaru, Indonesia)
- Angraini (Universitas Islam Negeri Sultan Syarif Kasim Riau, Pekanbaru, Indonesia)
- Mona Fronita (Universitas Islam Negeri Sultan Syarif Kasim Riau, Pekanbaru, Indonesia)

DOI: <https://doi.org/10.30865/iklik.v3i6.848> Abstract View: 16 times PDF Download: 12 times



Analisis Sentimen Ulasan Pelanggan Pada Aplikasi Fore Coffee Menggunakan Metode Naive Bayes

- Tia Anggita Sari (Universitas Muhammadiyah Prof. Dr. Hamka, Jakarta, Indonesia)
- Estu Simuningrum (Universitas Muhammadiyah Prof. Dr. Hamka, Jakarta, Indonesia)
- Firman Noor Hasan (Universitas Muhammadiyah Prof. Dr. Hamka, Jakarta, Indonesia)

DOI: <https://doi.org/10.30865/iklik.v3i6.884> Abstract View: 22 times PDF Download: 11 times



Pengaruh Distribusi dan Parameter terhadap Kinerja Sistem Antrian

- Mukarramah Yusuf (Universitas Hasanuddin, Makassar, Indonesia)

DOI: <https://doi.org/10.30865/iklik.v3i6.878> Abstract View: 5 times PDF Download: 4 times



Klasifikasi Sentimen Masyarakat di Media Sosial Twitter terhadap Calon Presiden 2024 Prabowo Subianto dengan Metode K-NN

- Avaldy Rahmat Rivita (Universitas Islam Negeri Sultan Syarif Kasim Riau, Pekanbaru, Indonesia)
- Yusra (Universitas Islam Negeri Sultan Syarif Kasim Riau, Pekanbaru, Indonesia)
- Muhammad Fikry (Universitas Islam Negeri Sultan Syarif Kasim Riau, Pekanbaru, Indonesia)

DOI: <https://doi.org/10.30865/iklik.v3i6.890> Abstract View: 15 times PDF Download: 9 times





Hak Cipta Dilindungi Undang-Undang

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber:
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penyusunan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar UIN Suska Riau.
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin UIN Suska Riau.

Lampiran Surat:

Nomor :

Tanggal : 03 Juli 2023

SURAT PERNYATAAN

Saya yang bertandatangan di bawah ini :

Nama : Gita Nurul Aini

NIM : 11950320643

Tempat/ Tgl. Lahir : Pelalawan, 05 Mei 2001

Fakultas/Pascasarjana : Sains dan Teknologi

Prodi : Sistem Informasi

Judul Disertasi/Thesis/Skripsi/Karya Ilmiah lainnya*:

The Implementation of Personal Data Protection Law
on Information System Security Risks Using OCTAVE-S

Menyatakan dengan sebenar-benarnya bahwa :

1. Penulisan Disertasi/Tesis/Skripsi/Karya Ilmiah lainnya* dengan judul sebagaimana tersebut di atas adalah hasil pemikiran dan penelitian saya sendiri.
2. Semua kutipan pada karya tulis saya ini sudah disebutkan sumbernya.
3. Oleh karena itu Disertasi/Tesis/Skripsi/Karya Ilmiah lainnya* saya ini, saya nyatakan bebas dari plagiat.
4. Apa bila dikemudian hari terbukti terdapat plagiat dalam penulisan Disertasi/Tesis/Skripsi/(Karya Ilmiah lainnya)* saya tersebut, maka saya bersedia menerima sanksi sesuai peraturan perundang-undangan.

Demikian Surat Pernyataan ini saya buat dengan penuh kesadaran dan tanpa paksaan dari pihak manapun juga.

Pekanbaru, 03 Juli 2023

Yang membuat pernyataan



Gita Nurul Aini

NIM : 11950320643

*pilih salah satu sesuai jenis karya tulis

The Implementation of Personal Data Protection Law on Information System Security Risks Using OCTAVE-S

Gita Nurul Aini*, Muhammad Jazman, Angraini, Mona Fronita

Fitri Kusumadewi Sains dan Teknologi, Program Studi Sistem Informasi, Universitas Islam Negeri Sultan Syarif Kasim, Pekanbaru, Indonesia
Email: ¹gitanurulaini005@gmail.com, ²jazman@uin-suska.ac.id, ³angraini@uin-suska.ac.id, ⁴monafronita@uin-suska.ac.id

Email Penulis Korespondensi: gitanurulaini005@gmail.com

Abstract—The research focuses on the risk assessment and mitigation of the Hitmi system, an information system used by PT Perkebunan Nusantara (PTPN V) for calculating employee premiums. The study aims to identify and evaluate the risks associated with the system's information technology assets and provide risk mitigation recommendations in accordance with information security practices and the Personal Data Protection Act. The research methodology includes several stages: Planning, Data Collection, Analysis and Data Processing, and Final Phase. In the Planning Stage, the problem is identified through observations and interviews, and the research purpose is defined. The Data Collection Phase involves literature studies, observations, interviews, and the use of OCTAVE-S to collect relevant data. The Analysis and Data Processing stage focuses on analyzing the collected data and processing it for conclusions and problem resolution. The OCTAVE-S framework is used to identify assets, vulnerabilities, and develop security strategies and plans. The results and discussion section presents the mapping of the OCTAVE-S analysis with the Personal Data Protection Act, identifying organizational information, and assessing organizational security practices. The risk impact assessment criteria are used to evaluate the risks, and the assets of the organization are identified. The assessment of security practices reveals areas of improvement and areas where good security practices are already implemented. Based on the findings, recommendations for mitigation are provided. These recommendations include security awareness and training programs for employees, improved resource allocation for security activities, regular updates to security policies, and the implementation of access control measures, incident management procedures, and encryption techniques. This research contributes to enhancing information security practices and reducing risks associated with the Hitmi system at PTPN V. The findings can guide the organization in implementing effective security controls, complying with the Personal Data Protection Act, and ensuring the confidentiality, integrity, and availability of sensitive data.

Keywords: Hitmi System; Information Technology Assets; OCTAVE-S; Personal Data Protection Act; Risk Assessment;

1. INTRODUCTION

Information systems generally investigate and discuss the processes in which the system itself is implemented and deployed to ensure that all relevant parties involved in the system can obtain the desired information effectively[1]. Information Systems in general, refers to hardware, digital applications, storage, communication systems, internet utilities, and almost all other aspects of business technology infrastructure, organizations, governments, schools, or other groups that shape the idea of big data[2], [3]. However, the use of information systems has various risks such as electrical failure due to natural factors, human error, system damage due to viruses, fire, data leakage due to hackers and others[4]. In recent times, there have been documented cases of unauthorized disclosure of personal data occurring within institutional and government settings, as well as in private companies, specifically in the realm of fintech start-ups[5].

The protection of personal data is a human right that needs to be given a legal basis to provide security over personal data. This is done to minimize the risk of data leakage on electronic systems. The Government has made the Law on the Protection of Personal Data in the Law of the Republic of Indonesia No.27 of 2022[6]. Information Systems and Information Technology (IT) plays an important role in risk management[7]. Risk management is the recurring process of analyzing, designing, implementing, controlling, supervising strategies and stages to implement security policies[8]. The purpose of risk management is to address a variety of problems such as the inadequacy of business processes, the company's reputation down, financial loss or bankruptcy of the company as well as the security of IT systems that store, process, or transmit information[8], [9]. In a company or organization, risk management refers to the CIA (Confidentiality, Integrity, Authentication) by identifying threats, classifying organization assets, and assessing system vulnerabilities so that effective security controls can be applied[10].

PT Perkebunan Nusantara (PTPN V) is located in Jl. Rambutan No.43, Sidomulyo East, Marpoyan Peace, Pekanbaru City, Riau 28294 is a company that operates in the palm and coconut planting sector in its management. PTPN V is a state-owned enterprise (BUMN) and the largest agribusiness and agro-industrial company of palm and rubber in Riau with the main purpose of serving the public or public interest[11]. In supporting the business processes in the company, PTPN V uses the information system. The information system used is the Hitungan Premi system (Hitmi System). The Hitmi system is a system for calculating employee premiums. The premium is an additional salary given to employees who work in the factory to process palm coconut. Before using the Hitmi System in PTPN V still use manual calculation, so there are some of the following problems: 1) High HPP, premium costs above the budget; 2) Frequently occurring calculation errors and the application of premium terms; 3) Difficult to monitor and evaluate premium calculations.

The development of digital technology transformation in PTPN V as tools supporting then implemented Hitmi system. In the operation of the hitmi system suffered barriers such as human error, where users often enter the data incorrectly. It will affect the instance. Hitmi systems load some sensitive information such as the personal data of employees and employee salary data so it is necessary to investigate so that there is no error input data that can affect the



results of salary calculation. In 2021, the hitmi system was hacked by hackers. the hacker entered the network and replaced index.php with an image resulting in the system being unusable. If the event is ignored by the company, it is concerned that the hacking and the theft of sensitive data will happen again. In order to reduce the occurrence of threats or technological risks, a risk assessment of the existing Hitmi system on PTPN V. The aim is to measure the level of awareness of risk and develop security controls to reduce losses and get maximum benefits for the agency, as well as to comply with the Personal Data Protection Act. It requires a framework to identify information security risks, such as the OCTAVE, FMEA, and ISO frameworks.

The development of digital technology transformation in PTPN V serves as a supporting tool for the implementation of the Hitmi system. However, the operation of the Hitmi system faces certain challenges, such as human error where users often input data incorrectly, leading to potential issues. The Hitmi system contains sensitive information, including personal employee data and salary information, making it essential to investigate and prevent any data input errors that could impact salary calculations. In 2021, the Hitmi system was hacked by hackers who gained unauthorized access to the network and replaced the index.php file with an image, rendering the system unusable. If this incident is disregarded by the company, there is a concern that hacking and theft of sensitive data could occur again. To mitigate the occurrence of threats and technological risks, a risk assessment of the existing Hitmi system in PTPN V is necessary. The objective is to assess the severity of risks and develop security controls to minimize losses and maximize benefits for the organization, while also aligning with the provisions of the Personal Data Protection Act. This requires the utilization of frameworks like OCTAVE, FMEA, and ISO to identify information security risks.

Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE) is a method used to identify and evaluate organizational risks that focus on strategic issues related to practices[12], [13]. OCTAVE-S is a simple methodology and supported by the Technology Insertion, Demonstration and Evaluation (TIDE) program at SEI, aimed at small organizations and assumes that such organizations have security involved in the process[14], [15]. OCTAVE-S is led by a small, interdisciplinary team (three to five people) of an organization's personnel who gather and analyze information, producing a protection strategy and mitigation plans based on the organization's unique operational security risks[16].

Some previous studies using the OCTAVE Framework research entitled "E-Procurement System Risk Analysis Using OCTAVE-S Method" with system security risk analysis obtained threats with yellow status where the agency needs to improve the security management system to prevent risks that have a major impact and interfere with operational activities[17]. The study entitled "Information Security Planning Based on Information Technology Risk Analysis Using OCTAVE Method and ISO 27001 (Case Study of the IT Field of the Banten Police Region)" was concluded after the analysis process carried out that there are 28 risks that may occur in the IT field of Banten police area with the highest RPN value of 240 to the lowest RPR value of 18. Risk mitigation recommendations can be made with 11 controls obtained in ISO 27001[18]. Research with the title IT Risk Management Analysis and Asset Security Using OCTAVE-S Method. The OCTAVE-S method has proven to identify risks and the results of the assessment have been concluded in a category that is very high, high, medium, low, very low. Very high, at this level the researchers had 4 risks with the highest RPN. The ISO 27001 standard can be used as a reference for recommendations for risk mitigation[19].

The following research, entitled Analysis, Evaluation, and Mitigation of Risk of Information Technology Assets Using the OCTAVE Framework and FMEA (Case Study: Unit of Management Technical Information Technology Fan Communication University XYZ) can be concluded that information security can be enhanced by analyzing the assets as well as the risks that occur on such assets using the Octave-S Frameworks. ISO 27001 helps in improving and improving information security in organizations[20]. Research entitled Security Risk Management Analysis System BMKGSOFT Using the OCTAVE-S Method concluded that the method for analyzing assets and risks can be done using the Octave method. Information security can be enhanced by analysing the assets used to manage such information as well as the risks that may occur on those assets[21].

In this study, the OCTAVE-S framework is used to identify the risks associated with the information technology assets used in the service, conduct risk assessments, and provide recommendations for risk mitigation in accordance with information security practices. Subsequently, the results of the OCTAVE-S analysis will be used in the data mapping process, aligning various data sources with the Personal Data Protection Act and integrating them into the main database to bridge any differences.

2. RESEARCH METHODOLOGY

The research methodology refers to the measures taken to achieve the research objectives. The steps involved in this study include: (1) the Planning Stage, (2) the Data Collection Phase, (3) the Data Analysis and Processing Phase, and (4) the Final Phase.

2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin UIN Suska Riau.

a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penyusunan laporan, penulisan kritik atau tinjauan suatu masalah.

b. Pengutipan tidak merugikan kepentingan yang wajar UIN Suska Riau.

c. Dilarang menggunakan ulang atau sebagian dari isi ini untuk tujuan komersial atau untuk merugikan UIN Suska Riau.

d. Dilarang menggunakan ulang atau sebagian dari isi ini untuk tujuan politik, agama, ras, atau golongan.

e. Dilarang menggunakan ulang atau sebagian dari isi ini untuk tujuan yang bertentangan dengan hukum, moral, atau nilai-nilai Pancasila.

f. Dilarang menggunakan ulang atau sebagian dari isi ini untuk tujuan yang melanggar hak-hak asasi manusia.

g. Dilarang menggunakan ulang atau sebagian dari isi ini untuk tujuan yang melanggar hak-hak kekayaan intelektual.

h. Dilarang menggunakan ulang atau sebagian dari isi ini untuk tujuan yang melanggar hak-hak paten.

i. Dilarang menggunakan ulang atau sebagian dari isi ini untuk tujuan yang melanggar hak-hak merek dagang.

j. Dilarang menggunakan ulang atau sebagian dari isi ini untuk tujuan yang melanggar hak-hak desain industri.

k. Dilarang menggunakan ulang atau sebagian dari isi ini untuk tujuan yang melanggar hak-hak rahasia dagang.

l. Dilarang menggunakan ulang atau sebagian dari isi ini untuk tujuan yang melanggar hak-hak informasi.

m. Dilarang menggunakan ulang atau sebagian dari isi ini untuk tujuan yang melanggar hak-hak privasi.

n. Dilarang menggunakan ulang atau sebagian dari isi ini untuk tujuan yang melanggar hak-hak kebebasan berekspresi.

o. Dilarang menggunakan ulang atau sebagian dari isi ini untuk tujuan yang melanggar hak-hak kebebasan beragama.

p. Dilarang menggunakan ulang atau sebagian dari isi ini untuk tujuan yang melanggar hak-hak kebebasan berpolitik.

q. Dilarang menggunakan ulang atau sebagian dari isi ini untuk tujuan yang melanggar hak-hak kebebasan berorganisasi.

r. Dilarang menggunakan ulang atau sebagian dari isi ini untuk tujuan yang melanggar hak-hak kebebasan berkeadilan.

s. Dilarang menggunakan ulang atau sebagian dari isi ini untuk tujuan yang melanggar hak-hak kebebasan berkeadilan.

t. Dilarang menggunakan ulang atau sebagian dari isi ini untuk tujuan yang melanggar hak-hak kebebasan berkeadilan.

u. Dilarang menggunakan ulang atau sebagian dari isi ini untuk tujuan yang melanggar hak-hak kebebasan berkeadilan.

v. Dilarang menggunakan ulang atau sebagian dari isi ini untuk tujuan yang melanggar hak-hak kebebasan berkeadilan.

w. Dilarang menggunakan ulang atau sebagian dari isi ini untuk tujuan yang melanggar hak-hak kebebasan berkeadilan.

x. Dilarang menggunakan ulang atau sebagian dari isi ini untuk tujuan yang melanggar hak-hak kebebasan berkeadilan.

y. Dilarang menggunakan ulang atau sebagian dari isi ini untuk tujuan yang melanggar hak-hak kebebasan berkeadilan.

z. Dilarang menggunakan ulang atau sebagian dari isi ini untuk tujuan yang melanggar hak-hak kebebasan berkeadilan.

aa. Dilarang menggunakan ulang atau sebagian dari isi ini untuk tujuan yang melanggar hak-hak kebebasan berkeadilan.

ab. Dilarang menggunakan ulang atau sebagian dari isi ini untuk tujuan yang melanggar hak-hak kebebasan berkeadilan.

ac. Dilarang menggunakan ulang atau sebagian dari isi ini untuk tujuan yang melanggar hak-hak kebebasan berkeadilan.

ad. Dilarang menggunakan ulang atau sebagian dari isi ini untuk tujuan yang melanggar hak-hak kebebasan berkeadilan.

ae. Dilarang menggunakan ulang atau sebagian dari isi ini untuk tujuan yang melanggar hak-hak kebebasan berkeadilan.

af. Dilarang menggunakan ulang atau sebagian dari isi ini untuk tujuan yang melanggar hak-hak kebebasan berkeadilan.

ag. Dilarang menggunakan ulang atau sebagian dari isi ini untuk tujuan yang melanggar hak-hak kebebasan berkeadilan.

ah. Dilarang menggunakan ulang atau sebagian dari isi ini untuk tujuan yang melanggar hak-hak kebebasan berkeadilan.

ai. Dilarang menggunakan ulang atau sebagian dari isi ini untuk tujuan yang melanggar hak-hak kebebasan berkeadilan.

aj. Dilarang menggunakan ulang atau sebagian dari isi ini untuk tujuan yang melanggar hak-hak kebebasan berkeadilan.

ak. Dilarang menggunakan ulang atau sebagian dari isi ini untuk tujuan yang melanggar hak-hak kebebasan berkeadilan.

al. Dilarang menggunakan ulang atau sebagian dari isi ini untuk tujuan yang melanggar hak-hak kebebasan berkeadilan.

am. Dilarang menggunakan ulang atau sebagian dari isi ini untuk tujuan yang melanggar hak-hak kebebasan berkeadilan.

an. Dilarang menggunakan ulang atau sebagian dari isi ini untuk tujuan yang melanggar hak-hak kebebasan berkeadilan.

ao. Dilarang menggunakan ulang atau sebagian dari isi ini untuk tujuan yang melanggar hak-hak kebebasan berkeadilan.

ap. Dilarang menggunakan ulang atau sebagian dari isi ini untuk tujuan yang melanggar hak-hak kebebasan berkeadilan.

aq. Dilarang menggunakan ulang atau sebagian dari isi ini untuk tujuan yang melanggar hak-hak kebebasan berkeadilan.



© Hak cipta milik UIN Suska Riau

Hak Cipta Dilindungi Undang-Undang

1. Diarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan sumbernya.
 a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penyusunan laporan, penulisan kritik atau tinjauan satu masalah.
 b. Pengutipan tidak merugikan kepentingan yang wajar UIN Suska Riau.
 2. Diarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin UIN Suska Riau.

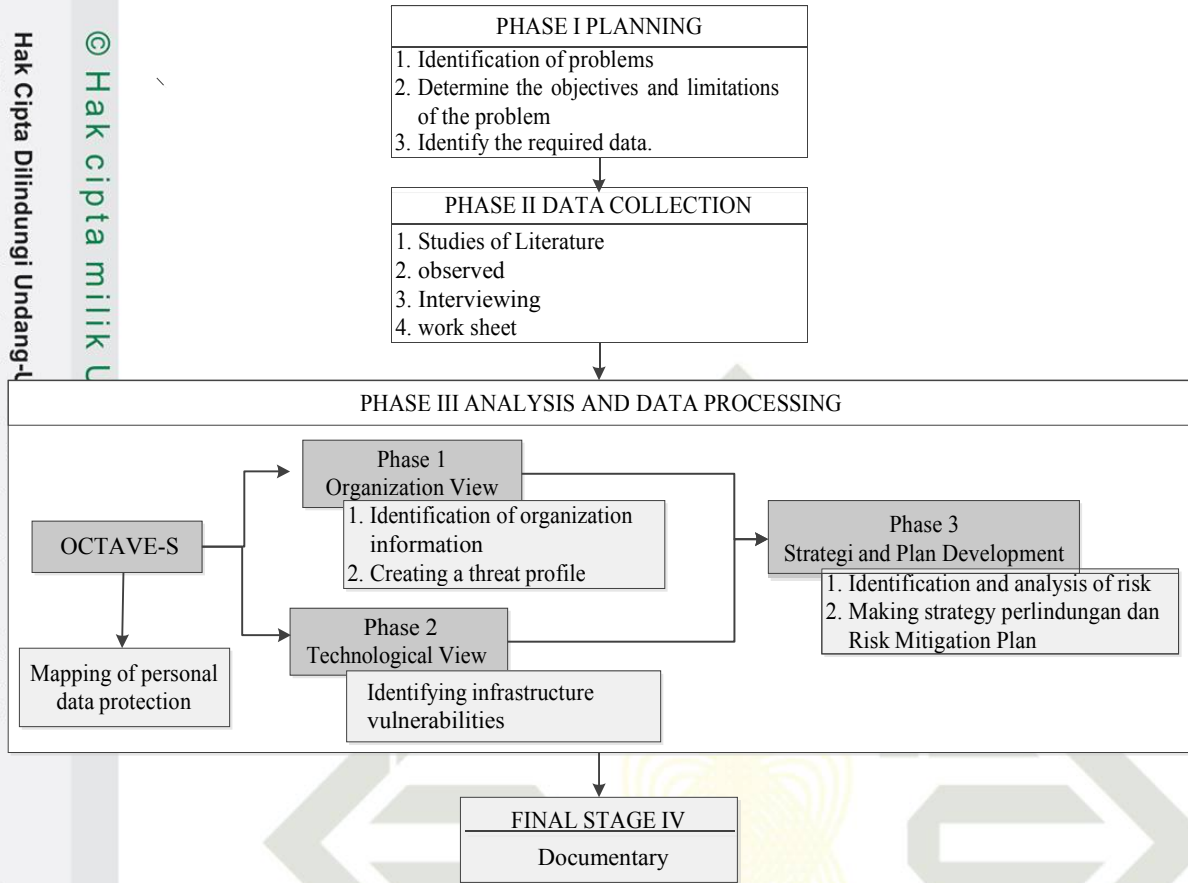


Figure 1. Methodology

2. The Planning Stage

The planning stage involves identifying the problem through observations and interviews conducted with PTPN V. Subsequently, the research purpose is determined, and the required data for this study is defined. The outcome of the initial stage is the interview protocol used to conduct a risk analysis on the Hitmi System.

2. Stage of Data Collection

The purpose of the data collection phase is to gain a better understanding of the problems to be investigated. There are four processes involved in data collection, including: (1) Literature studies, (2) Observations, (3) Interviews, (4) OCTAVE-S Sheets.

2. Analysis and Data Processing

The analysis is conducted to analyze the needs related to the raised problem and how to address it. The purpose of data processing is to transform the obtained raw material into processed information through the analysis process, making it easier to draw conclusions and find solutions to the research problems. The analysis of system security risks based on OCTAVE-S focuses on the initial phase of asset building, specifically the threat profile. This stage involves two processes: identifying organizational information and constructing the expected threat profiles. These activities assist in research and risk assessment, as well as support companies in establishing their vision and mission.

2.3.1 OCTAVE-S

OCTAVE-Ss based on three phases:

- a. Stage 1: Build Asset-Based Threat Profiles In this phase is the evaluation of organizational aspects. During this phase, the team of analysts defines the impact assessment criteria to be used to evaluate risk, identify the assets of the organization and evaluate the organization's security practices. Finally, the team defines security requirements and defines threat profiles for each critical asset.
- b. Phase 2: Identify infrastructure vulnerabilities At this stage is the identification of computing infrastructure, focusing on the extent to which security is considered by infrastructure maintenance. Analyze how people use computing infrastructure to access critical assets, generate key classes of components and who is responsible for configuring and using those components.
- c. Phase 3: Develop security strategies and plans The team creates protection strategies for the organization and risk mitigation plans to address risks to critical assets. The OCTAVE-S worksheet used during Phase 3 is highly structured



and closely connected to the OCTAVE practice catalog, enabling the linking of recommendations for improvements with the reference of received safety practices.

2. Final Phase

At this stage, the data obtained is collected and processed to become a report.

3. RESULT AND DISCUSSION

3.1 Mapping OCTAVE-S With the Personal Data Protection Act

The personal data protection law regulates a range of provisions, including the types of personal data, processing, and actions for misuse of personal data management. According to Article 39, paragraph (1) the controller of personal data is obligated to prevent unauthorized access to personal data. This prevention is supported by paragraph (2) which states that a security system must be implemented for processing personal data using electronic systems reliably, safely, and responsibly.

In Indonesia, there are 30 laws and regulations relating to the collection and management of personal data. Including a number of regulations on the privacy of citizens[22]. Then on 17 October 2022 the Law of the Republic of Indonesia Number 27 Year 2022 on the Protection of Personal Data was approved by the President of Indonesia

This section contains the results of mapping the Personal Data Protection Act and Hitmi System Risk Assessment using OCTAVE-S.

In the context of mapping between the security existing in the OCTAVE-S methodology and the data protection laws, there are some correlations and similarities between the two. Here are some examples of how security in OCTAVE-S can relate to the legal requirements of personal data protection:

Tabel 1. Mapping OCTAVE-S With the Personal Data Protection Act

SAFETY PRACTICE	OCTAVE-S	THE PERSONAL DATA PROTECTION ACT	ARTICLE
Security of Data	OCTAVE-S encourages the identification of critical assets and vulnerabilities to threats, including personal data.	Personal data protection laws also require adequate protection of personal data through appropriate safeguards, such as data encryption, access control, and protection against data leakage or misuse.	Chapter VI Duties of the controller of personal data and the processor in processing personal data: Article 32 paragraph 1 Chapter IV Article 12 Paragraph 1 on the right to Chapter VI Chapter 46,47 Chapter XIV Regulations Chapter VI Article 13, Article 24, Article 28, Chapter VI: Responsibilities of the controller and processor of personal data in the processing of data: Articles 35-39 on encryption
Regulation of access	OCTAVE-S analyzes existing access policies and controls within the organization, including access to personal data.	The law on the protection of personal data emphasizes the need to regulate appropriate access to personal data, including the exercise of access rights based on the principles of necessity and limitation of access.	Chapter XVI Transitional Provisions Articles 47 and 75
Network and system security	OCTAVE-S involves vulnerability assessments on infrastructure and systems, which include systems that manage and process personal data.	Personal data protection laws encourage the adoption of adequate network and system security measures to protect personal data from threats and attacks, such as network monitoring, intrusion detection, and protection against malware.	Chapter VI Obligations of Personal Data Controller and Personal Data Processor in Data Processing, Article 46 on Notification in the event of failure and incident response Chapter V: Data Processing: Article 16 Paragraph 2
Policy and Procedure	OCTAVE-S involves the evaluation of security-related organizational policies and procedures, including privacy and data security policies.	Personal data protection laws encourage the adoption of transparent and adequate policies and procedures to protect personal data, such as clear privacy policies, notification to individuals regarding data use, and effective incident response procedures.	

2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin UIN Suska Riau.

1. Dilarang mengutip, menyalin, atau memperbanyak sebagian atau seluruh karya tulis ini tanpa mengacukan sumber: a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penyusunan laporan, penulisan kritik atau tinjauan suatu masalah. b. Pengutipan tidak merugikan kepentingan yang wajar UIN Suska Riau.



5 Monitoring and Reviewing.

OCTAVE-S encourages periodic monitoring and review of existing security measures within the organization.

The Data Protection Act also emphasizes the importance of periodic monitoring and review to ensure compliance with the law and the effectiveness of the security measures implemented.

Chapter XVI Transitional Provisions Articles 74 and 75

It is important to note that the legal requirements for the protection of personal data may vary between countries or jurisdictions. Therefore, the mapping between OCTAVE-S and the data protection laws should be done specifically taking into account the legal requirements applicable in your jurisdiction.

3.2 Identification of Organizational Information

The risk assessment process starts with identifying information from the agency to determine the level of risk that may impact the agency's activities or survival. Data collection is conducted using worksheets.

3.2.1 Establish A Risk Impact Assessment

Data obtained as follows.

Table 2. Work Sheet Filling Data Identifying Risks from Organization Impact Assessment Criteria

No	Criteria of impact	Type / Impact	Level
1	Reputation and Loss of data	Reputation Damage to system	Low Low
2	financed Productivity	Operational costs Loss of income	Medium Low
3	Health / Safety	Working hours	Medium
4	Criteria of impact	Health and	Low

Based on Table 2, it can be observed that the System Reputation and Damage Indicators are at a low level. This is attributed to the positive reputation of the Hitmi System, as the existing systems and services are running smoothly. System damage on the Hitmi System occurs primarily during instances when service slows down and employee trust in agents is slightly diminished. As for the Financial Indicators, the impact of operating costs is assessed to be at a moderate level. This is due to the rise in hardware and system maintenance expenses. However, agents do not experience a significant decline in revenue, as indicated by the low risk level of revenue on the agent's criteria. The Productivity Hour indicator reveals that employees encounter a 10% to 30% increase during threats or incidents, placing them at a moderate risk level. In terms of employee health and safety indicators, the potential threats to employee well-being are considered low. Healthcare staff receive health insurance and tailored care based on the severity of their illness.

3.2.2 Identification of Organization Assets

Here is the data obtained from completing the work sheet. The second step involves identifying the assets of the organization as shown in Table 3, as follows:

Table 3. Data Assets of Human Resources

System	Information	Applications and Services	Other assets
Hitungan Premi System	Stable data premiums	CCTV	PHPstorm (text editor)
	Employee premiums / salary data every day	Milena	Server windows 2008
	Personal Data of Employees	Intank	MYSQL
	Data Delivery (permit, leave, and sick)	SAP	Code Igniter
	Data extension of the department/employee in other departments	Fossnirs	PKS Online

Table 4. Data Assets of Human Resources

Human Resource	
Departement Programming	Skilled Develop, manage, operate, and maintain enterprise system infrastructure, network, server, and database.

3.3 Assessment of Organizational Security Practices

To evaluate aspects of security practices based on the stolight status obtained from the results of filling the worksheet with the following descriptions:

2. Dilarang mengemukakan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin UIN Suska Riau.

Hak Cipta Dilindungi Undang-undang
1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan sumber atau dengan cara lain.
a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penyusunan laporan, penulisan kritik atau tinjauan suatu masalah.
b. Pengutipan tidak merugikan kepentingan yang wajar UIN Suska Riau.

© Hak cipta Sastra Islamik University of Sultan Syarif Kasim Riau



Table 5. Explanation of Assessment

Green	4 indicators very fulfilled
Yellow	3 indicators slightly fulfilled
Red	2 indicators are not met

As for the data obtained from Step 3 on the worksheet that has been filled out against the assessment of security practices that have been implemented by the Hitmi System as follows:

Table 6. Data filling work sheets of security practice agencies

NO	SAFETY PRACTICE	STOPLIGHT		
		RED	YELLOW	GREEN
1	Security Awareness and Training		✓	
2	Security Strategy			✓
3	Security management		✓	
4	Security Policy and Rules		✓	
5	Security and Collaboration Management			✓
6	Contingency Planning			✓
7	Control of physical access		✓	
8	Physical Safety Monitoring and Audit			✓
9	System and network management.		✓	
10	Monitoring and audit of security.		✓	
11	Verification and Authorization		✓	
12	Management of Vulnerability		✓	
13	Encrypted		✓	
14	Design and Security Architecture			✓
15	Management of incidents		✓	

Can be seen in the table 6, there are ten security practices are in the status of yellow stoplight which indicates that PTPN V has implemented the security practice but is not good enough and five security practice is in the state of green stoplight indicating that PTPN V has already implemented that security practice well.

3. Recommendations

The results of the risk assessment analysis are as follows:

Table 6. Risk Action List

No	Security Practice	Risk action
1	Security Awareness and Training	Training of employees will be the importance of the role and responsibility of employees. Routine training for PTPN V employees. Execute good resource allocation for PTPN V security activities
2	Security management	Responsibility for PTPN V employees Conduct a documented procedure. Management should be based on routine reports containing information related to security aspects.
3	Security Policy and Rules	Making policy documentation that is periodically updated Conduct a documented process to evaluate whether each employee of the company has the procedures in place.
4	Control of physical access.	Improve physical access control. Implement documented policies and procedures towards visitors. Implement security measures such as using an ID card and fingerprint scanner in accessing a room and using a password to any sensitive information access. Protect sensitive information in a secure place.
5	System and network management.	Make backup data on software and data staff of the company follow the procedure in making changes to username and password. Implement documented procedures to protect existing systems. Routine inspections of systems and networks.
6	Monitoring and audit of security.	Monitor and audit systems and networks within the company on a regular basis.
7	Verification and Authorization	Implementing Effective Controls in accordance with Existing Policies. Enforcing Access Restrictions for Hitmi System Users to prevent unauthorized access to sensitive data or information.
8	Management of Vulnerability	Conduct procedures to manage the level of vulnerability within the company. Evaluate the Hitmi System vulnerability periodically.

Hak Cipta Dilindungi Undang-Undang
1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mengizinkan dan menyebutkan sumber.
a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penyusunan laporan, penulisan kritik atau tinjauan suatu masalah.
b. Pengutipan tidak merugikan kepentingan yang wajar UIN Suska Riau.
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin UIN Suska Riau.

© Hak cipta milik UIN Suska Riau

State Islamic University of Sultan Syarif Kasim Riau



Implementing Security Controls according to System Requirements.
Protected Sensitive Information.
Managing Systems, Routers, and Firewalls.
Conduct procedures documented by the company for the purpose of identifying, reporting, and processing the follow-up of suspected security incidents and breaches.

Encrypted

Management of incidents

Discussion

The research discussed the use of the OCTAVE-S framework to assess the risks and develop security controls for the Hitmi System used by PT Perkebunan Nusantara (PTPN V), a state-owned enterprise in Indonesia. The aim of the research is to identify and mitigate the risks associated with the system, particularly in relation to personal data protection.

The introduction highlighted the importance of information systems in effectively providing desired information to relevant parties. However, the use of information systems also comes with various risks, such as electrical failure, human error, system damage, and data leakage. To protect personal data, the Indonesian government has enacted the Law on the Protection of Personal Data. Information systems and information technology play a crucial role in risk management, addressing problems related to business processes, company reputation, financial loss, and IT system security.

PTPN V uses the Hitmi system for calculating employee premiums, replacing the previous manual calculation method. However, the system has faced challenges such as human errors in data entry and a hacking incident in 2021. Therefore, the research aims to assess the risks associated with the Hitmi system using the OCTAVE-S framework and develop security controls to prevent future incidents and comply with the Personal Data Protection Act.

The research methodology involves four stages: planning, data collection, analysis and data processing, and the final phase. In the planning stage, the problem was identified through observations and interviews with PTPN V, and the research purpose and data requirements were defined. The data collection phase involved literature studies, observations, interviews, and the use of OCTAVE-S worksheets to gather information about the system and its risks. The analysis and data processing stage focused on analyzing the collected data, assessing the risks using the OCTAVE-S framework, and developing security strategies and plans. Finally, the data obtained were processed to produce the research report.

The results and discussion section presents the mapping of the OCTAVE-S framework with the Personal Data Protection Act. It also includes the identification of organizational information, such as the impact assessment criteria and asset identification. The assessment of security practices implemented by the Hitmi System was also discussed, with some practices categorized as yellow (partially fulfilled) and others as green (fulfilled). Recommendations were provided to address the identified risks, including training employees on security awareness, allocating resources for security management, updating security policies, implementing physical access controls, and more.

Overall, this research provides insights into the risks associated with the Hitmi System used by PTPN V and offers recommendations to enhance information security and comply with the Personal Data Protection Act. By applying the OCTAVE-S framework, the study helps identify potential vulnerabilities, assess risks, and develop appropriate security controls. This research contributes to the field of information security and risk management, particularly in the context of organizations handling sensitive data.

4. CONCLUSION

This research focuses on the analysis and mitigation of risks in the Hitungan Premi system (Hitmi System) used by PT Perkebunan Nusantara (PTPN V), a state-owned enterprise operating in the palm and coconut planting sector. The study recognizes the risks associated with information systems, such as human error, system damage, and data leakage. The implementation of risk management, including the OCTAVE-S framework, is crucial to address these risks effectively. The OCTAVE-S framework helps in identifying and evaluating organizational risks, developing security strategies, and implementing risk mitigation plans. The research also emphasizes the importance of aligning the analysis with the Personal Data Protection Act to ensure compliance with data privacy regulations. Through the research methodology, including the planning stage, data collection phase, analysis and data processing, and the final phase, the study provides insights into the risks and security practices within PTPN V. The assessment reveals the impact criteria, organizational assets, and security practices, highlighting areas of improvement and recommendations for risk mitigation. Overall, this research contributes to enhancing information security and protecting personal data in the Hitmi System and provides valuable insights for organizations in similar contexts.

REFERENCES

[1] D. Berdik, S. Otoum, N. Schmidt, D. Porter, and Y. Jararweh, "A survey on blockchain for information systems management and security," *Information Processing & Management*, vol. 58, no. 1, p. 102397, 2021.

[2] W. J. Gordon and C. Catalini, "Blockchain Technology for Healthcare: Facilitating the Transition to Patient-Driven Interoperability," *Computational and Structural Biotechnology Journal*, vol. 16, pp. 224–230, 2018, doi: 10.1016/j.csbj.2018.06.003.

2. Dilarang mengemukakan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin UIN Suska Riau.

Hak Cipta Dilindungi Undang-Undang. 61. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mengutip sumber... 60. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mengutip sumber... 59. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mengutip sumber... 58. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mengutip sumber... 57. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mengutip sumber... 56. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mengutip sumber... 55. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mengutip sumber... 54. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mengutip sumber... 53. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mengutip sumber... 52. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mengutip sumber... 51. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mengutip sumber... 50. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mengutip sumber... 49. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mengutip sumber... 48. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mengutip sumber... 47. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mengutip sumber... 46. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mengutip sumber... 45. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mengutip sumber... 44. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mengutip sumber... 43. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mengutip sumber... 42. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mengutip sumber... 41. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mengutip sumber... 40. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mengutip sumber... 39. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mengutip sumber... 38. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mengutip sumber... 37. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mengutip sumber... 36. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mengutip sumber... 35. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mengutip sumber... 34. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mengutip sumber... 33. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mengutip sumber... 32. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mengutip sumber... 31. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mengutip sumber... 30. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mengutip sumber... 29. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mengutip sumber... 28. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mengutip sumber... 27. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mengutip sumber... 26. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mengutip sumber... 25. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mengutip sumber... 24. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mengutip sumber... 23. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mengutip sumber... 22. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mengutip sumber... 21. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mengutip sumber... 20. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mengutip sumber... 19. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mengutip sumber... 18. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mengutip sumber... 17. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mengutip sumber... 16. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mengutip sumber... 15. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mengutip sumber... 14. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mengutip sumber... 13. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mengutip sumber... 12. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mengutip sumber... 11. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mengutip sumber... 10. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mengutip sumber... 9. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mengutip sumber... 8. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mengutip sumber... 7. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mengutip sumber... 6. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mengutip sumber... 5. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mengutip sumber... 4. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mengutip sumber... 3. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mengutip sumber... 2. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mengutip sumber... 1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mengutip sumber...



2. Dilarang mengemukakan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin UIN Suska Riau.

- [3] S. Otoum, B. Kantarci, and H. Mouftah, "Empowering Reinforcement Learning on Big Sensed Data for Intrusion Detection," in *ICC 2019 - 2019 IEEE International Conference on Communications (ICC)*, Shanghai, China: IEEE, May 2019, pp. 1–7. doi: 10.1109/ICC.2019.8761575.
1. Diarangi mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan sumber:
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penyusunan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan atau seluruh karya tulis ini dalam bentuk apapun tanpa izin UIN Suska Riau.
2. Dilarang mengemukakan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin UIN Suska Riau.
- Setiawan, A. R. Sekarini, R. Waluyo, and F. N. Afiana, "Manajemen Risiko Sistem Informasi Menggunakan ISO 31000 dan Standar Pengendalian ISO/EIC 27001 di Tripio Purwokerto," *MATRIK: Jurnal Manajemen, Teknik Informatika dan Rekayasa Komputer*, vol. 20, no. 2, pp. 389–396, 2021.
- Susanto, "URGENSI PENGATURAN DATA DIGITAL/ELEKTRONIK PRIBADI," *Bureaucracy Journal: Indonesia Journal of Law and Social-Political Governance*, vol. 2, no. 3, pp. 1140–1148, 2022.
- Peraturan Menteri Dalam Negeri Republik Indonesia Nomor 27 Tahun 2022. Accessed: Nov. 24, 2022. [Online]. Available: <https://peraturan.bpk.go.id/Home/Details/229798/uu-no-27-tahun-2022>
- He, J. Zhang, and W. Li, "Information technology solutions, challenges, and suggestions for tackling the COVID-19 pandemic," *International journal of information management*, vol. 57, p. 102287, 2021.
- Hom B. Anong, K. B. Rii, L. K. Choi, and K. Zelina, "The Octave Allegro Method in Risk Management Assessment of Educational Institutions," *Aptisi Transactions on Technopreneurship (ATT)*, vol. 2, no. 2, pp. 167–179, 2020.
- Stoneburner, A. Goguen, and A. Feringa, "Risk management guide for information technology systems," *Nist special publication*, vol. 800, no. 30, pp. 800–30, 2002.
- L. K. Koz and R. D. Vines, *The CISSP prep guide: mastering the ten domains of computer security*. New York: Wiley, 2001.
- R. Rosmala, "Fungsi komunikasi korporat Humas PT. Perkebunan Nusantara V Pekanbaru," *PROfesi Humas*, vol. 5, no. 2, pp. 143–162, 2021.
- C. Alberts, A. Dorofee, J. Stevens, and C. Woody, "Introduction to the OCTAVE Approach," *Carnegie-Mellon Univ Pittsburgh Pa Software Engineering Inst*, 2003.
- J. S. Suroso and M. A. Fakhrozi, "Assessment of information system risk management with octave allegro at education institution," *Procedia Computer Science*, vol. 135, pp. 202–213, 2018.
- R. A. Calli, J. F. Stevens, L. R. Young, and W. R. Wilson, "Introducing octave allegro: Improving the information security risk assessment process," *Carnegie-Mellon Univ Pittsburgh PA Software Engineering Inst*, 2007.
- C. Woody, J. Coleman, M. Fancher, C. Myers, and L. Young, "Applying OCTAVE: Practitioners Report," *CARNEGIE-MELLON UNIV PITTSBURGH PA SOFTWARE ENGINEERING INST*, 2006.
- C. Alberts, A. Dorofee, J. Stevens, and C. Woody, "OCTAVE-S implementation guide, Version 1.0," *Manuel électronique*. Pittsburg, PA,: Software Engineering Institute, Carbegie Mellon university, 2005.
- J. P. SARI, "ANALISIS RESIKO KEAMANAN SISTEM E-PROCUREMENT MENGGUNAKAN METODE OCTAVE-S (Studi Kasus: Unit Layanan Pengadaan Provinsi Riau)," skripsi, Universitas Islam Negeri Sultan Syarif Kasim Riau, 2018. doi: 10.10.10.20BAB%20V_2018267SIF.pdf.
- F. A. Anshori and A. R. P. Suprpto, "Perencanaan Keamanan Informasi Berdasarkan Analisis Risiko Teknologi Informasi Menggunakan Metode OCTAVE dan ISO 27001 (Studi Kasus Bidang IT Kepolisian Daerah Banten)," *Jurnal Pengembangan Teknologi Informasi dan Ilmu Komputer e-ISSN*, vol. 2548, p. 964X, 2019.
- A. F. Rohman, A. Ambarwati, and E. Setiawan, "Analisis Manajemen Risiko IT dan Keamanan Aset Menggunakan Metode Octave-S," *INTECOMS: Journal of Information Technology and Computer Science*, vol. 3, no. 2, pp. 298–310, 2020.
- R. J. Gagah, I. Syah, and F. Febryanto, "ANALISIS, EVALUASI, DAN MITIGASI RISIKO ASET TEKNOLOGI INFORMASI MENGGUNAKAN FRAMEWORK OCTAVE DAN FMEA (STUDI KASUS: UNIT PENGELOLA TEKNIS TEKNOLOGI INFORMASI DAN KOMUNIKASI UNIVERSITAS XYZ)," *Jurnal Khatulistiwa Informatika*, vol. 9, no. 2, 2021.
- M. Megawati and M. L. Hamzah, "Analisis Manajemen Risiko Keamanan Sistem BMKGSoft Menggunakan Metode OCTAVE-S," *Jurnal Ilmiah Rekayasa dan Manajemen Sistem Informasi*, vol. 8, no. 1, pp. 62–67.
- Lintang Setianti, "Urgensi Regulasi Perlindungan Data Pribadi di Indonesia - Analisis - www.indonesiana.id," <https://www.indonesiana.id/profil/read/68772/urgensi-regulasi-perlindungan-data-pribadi-di-indonesia>, Apr. 27, 2019. <https://www.indonesiana.id/read/68772/urgensi-regulasi-perlindungan-data-pribadi-di-indonesia> (accessed Nov. 24, 2022).

Hak Cipta Dilindungi Undang-Undang

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber:
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penyusunan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar UIN Suska Riau.
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin UIN Suska Riau.

LAMPIRAN B

LEMBAR TRANSKIP WAWANCARA

TRANSKIP WAWANCARA

STUDI KASUS : PTPN V KOTA PEKANBARU (Sistem Hit Mi)

Transkrip wawancara berikut merupakan data yang berhasil dikumpulkan melalui proses wawancara yang dilakukan pada pegawai di PT Perkebunan Nusantara V Kota Pekanbaru.

Informasi Pelaksanaan Interview	
Interviewer	: Gita Nurul Aini
Narasumber	: Satria Ananda Pratama, S.T
Bagian	: Teknisi
Hari, Tanggal	: Sabtu, 10 Desember 2022
Pukul	: 15.30 s.d 16.00

Pekanbaru, 12 Januari 2023



Satria Ananda Pratama, S.T

LAMPIRAN C

LEMBAR KERJA OCTAVE-S

LEMBAR KERJA MEMILIH ASET KRITIS

Langkah 5-9			
Aset Kritis	Alasan Pemilihan	Deskripsi	Aset Terkait
Sistem apa yang memiliki status kritis ?	Mengapa sistem ini penting bagi instansi?	Siapa saja yang menggunakan sistem ini ?	Aset (Informasi, layanan/aplikasi, lainnya) apa saja yang berkaitan dengan sistem ini ?
HITM1	Karena sistem HITM1 adalah sistem untuk monitoring dan evaluasi pertumbuhan premi karyawan.	1. Bagian Inputan (Unit). 2. Bagian Approval (Manajer Unit). 3. Bagian Monitoring (KEL, SPI, Stakeholder lainnya). 4. Bagian Admin (TEP).	- Milena (Aplikasi monitoring) - Mitey - SAP - Vossmirs - Pkt online - Server asin 2008 - PHPStorm (Client editor). - Database MySQL

Hak Cipta Dilindungi Undang-Undang

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber:
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penyusunan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar UIN Suska Riau.
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin UIN Suska Riau.

LEMBAR KERJA IDENTIFIKASI ASET ORGANISASI

Langkah 2

Sistem, Informasi, Aplikasi dan Layanan			
Sistem	Informasi	Aplikasi/Layanan	Aset Lainnya
Sistem apa yang memiliki status kritis pada instansi ?	Informasi apa yang diperlukan pegawai dari adanya sistem tersebut ?	Aplikasi apa yang mendukung aset kritis ?	apa saja aset lain yang terkait oleh aset kritis ?
Hitung	<ul style="list-style-type: none"> - Data Premis tetap - Data premi / gaji karyawan setiap hari - Data pribadi karyawan - Data pengajuan (i, s, dan cuti) - Data ekstensi bagian / karyawan lain 	<ul style="list-style-type: none"> - CCTV - Mikena - Integ - Sdp - PHP - Vassnirs - Server Win 2008 - MySQL 	<ul style="list-style-type: none"> - PHP storm - Code Igniter - PkS Online
Sumber Daya Manusia			
Jabatan		Keahlian	
Programmer / Teknisi Li PTPN V		<ul style="list-style-type: none"> - Mengembangkan, mengoperasikan sistem / Aplikasi - Memelihara infrastruktur sistem jaringan - Memelihara server dan database 	

Hak Cipta Dilindungi Undang-Undang

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber:
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penyusunan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar UIN Suska Riau.
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin UIN Suska Riau.

Hak Cipta Dilindungi Undang-Undang

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber:
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penyusunan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar UIN Suska Riau.
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin UIN Suska Riau.

LEMBAR KERJA KEBUTUHAN KEAMANAN UNTUK ASET KRITIS

Langkah 10-11	
Kebutuhan Keamanan	Kebutuhan Keamanan Paling Penting
Apa kebutuhan keamanan untuk sistem ini? (Petunjuk : fokus pada kebutuhan keamanan apa yang seharusnya ada untuk sistem ini, bukan apa yang sekarang ada)	Kebutuhan keamanan mana yang paling penting untuk sistem ini?
<input checked="" type="checkbox"/> Kerahasiaan sistem <input checked="" type="checkbox"/> Integritas data <input checked="" type="checkbox"/> Ketersediaan informasi	<input checked="" type="checkbox"/> Kerahasiaan <input checked="" type="checkbox"/> Integritas <input checked="" type="checkbox"/> Ketersediaan

LAMPIRAN D DOKUMENTASI



© Hak cipta milik UIN Suska Riau

State Islamic University of Sultan Syarif Kasim Riau

Hak Cipta Diindungi Undang-Undang

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber:
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penyusunan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar UIN Suska Riau.
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin UIN Suska Riau.

DAFTAR RIWAYAT HIDUP

Gita Nurul Aini lahir di Pelalawan, 05 Mei 2001 sebagai anak kedua dari tiga bersaudara dari Ayahanda Wangsul dan Ibunda Irawati yang beralamatkan di Desa Harapan Jaya, Kec. Pangkalan Kuras, Kab. Pelalawan, Riau, *Email* gitanutrulaini005@gmail.com. Riwayat Pendidikan dimulai dari SD Negeri 022 Desa Harapan Jaya dari tahun 2007 sampai 2013. Kemudian peneliti melanjutkan pendidikan di SMP Negeri 2 Pangkalan Kuras dari tahun 2013 sampai 2016. Tahun 2016, peneliti melanjutkan pendidikan di SMA Negeri 1 Pangkalan Kerinci dengan mengambil jurusan Ilmu Pengetahuan Alam (IPA) pada tahun 2016 sampai 2019. Pada tahun 2019, peneliti melanjutkan pendidikan di Perguruan Tinggi Negeri jalur PBUD 2019 dengan mengambil jurusan Sistem Informasi Fakultas Sains dan Teknologi Universitas Islam Negeri Sultan Syarif Kasim Riau dan menamatkan pendidikan pada pertengahan tahun 2023. Selama menjalani masa perkuliahan, peneliti aktif pada organisasi kampus yaitu Himpunan Mahasiswa Sistem Informasi (HIMASI) dan ISOC Research. Pada tahun 2021, peneliti melakukan Kerja Praktek pada Pusat Pengembangan Bahasa (P2B) UIN Sultan Syarif Kasim Riau dengan mengambil projek mini berupa studi kelayakan sistem informasi tes bahasa berbasis website pada Pusat Pengembangan Bahasa (P2B) UIN Sultan Syarif Kasim Riau Menggunakan Metode TELOS.



© Ha

Suska Riau

State Islamic University of Sultan Syarif Kasim Riau

Hak Cipta Diindungi Undang-Undang

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber:
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penyusunan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar UIN Suska Riau.
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin UIN Suska Riau.