# PERANCANGAN DAN IMPLEMENTASI SISTEM ANALISIS RISIKO PRIVASI PADA PLATFORM DIGITAL MENGGUNAKAN *LIKELIHOOD–IMPACT ENGINE* BERBASIS *RULE-BASED AUTOMATION*

**SKRIPSI**

Diajukan untuk memenuhi salah satu syarat mencapai derajat Sarjana

Program Studi Teknik Komputer


disusun oleh

**MUNIF ARYAPUTRA**

**22.83.0787**


Kepada

**FAKULTAS ILMU KOMPUTER**

**UNIVERSITAS AMIKOM YOGYAKARTA**

**YOGYAKARTA**

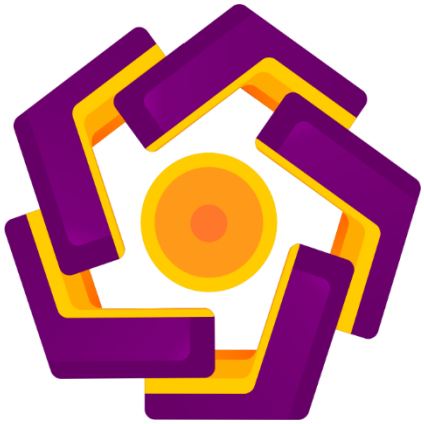
**2026**

# PERANCANGAN DAN IMPLEMENTASI SISTEM ANALISIS RISIKO PRIVASI PADA PLATFORM DIGITAL MENGGUNAKAN *LIKELIHOOD–IMPACT ENGINE* BERBASIS *RULE-BASED AUTOMATION*

**SKRIPSI**

untuk memenuhi salah satu syarat mencapai derajat Sarjana

Program Studi Teknik Komputer




disusun oleh

**MUNIF ARYAPUTRA**

**22.83.0787**


Kepada


**FAKULTAS ILMU KOMPUTER**

**UNIVERSITAS AMIKOM YOGYAKARTA**

**YOGYAKARTA**


**2026**

## HALAMAN PERSETUJUAN

**SKRIPSI**

**PERANCANGAN DAN IMPLEMENTASI SISTEM ANALISIS RISIKO PRIVASI PADA PLATFORM DIGITAL MENGGUNAKAN *LIKELIHOOD–IMPACT ENGINE* BERBASIS *RULE-BASED AUTOMATION***

yang disusun dan diajukan oleh

**Munif Aryaputra**

**22.83.0787**

telah disetujui oleh Dosen Pembimbing Skripsi
pada 18 Februari 2026

**Dosen Pembimbing,**

**Dr. Dony Ariyus, S.S., M.Kom.**
**NIK. 190302128**

## HALAMAN PENGESAHAN

**SKRIPSI**

**PERANCANGAN DAN IMPLEMENTASI SISTEM ANALISIS RISIKO PRIVASI PADA PLATFORM DIGITAL MENGGUNAKAN *LIKELIHOOD–IMPACT ENGINE* BERBASIS *RULE-BASED AUTOMATION***

yang disusun dan diajukan oleh

**Munif Aryaputra**

**22.83.0787**

Telah dipertahankan di depan Dewan Penguji
pada 18 Februari 2026

**Susunan Dewan Penguji**

| Nama Penguji | Tanda Tangan |
|---|---|
| **Jeki Kuswanto, S.Kom., M.Kom.**<br>**NIK. 190302456** | |
| **Melwin Syafrizal, S.Kom., M.Eng., Ph.D.**<br>**NIK. 190302105** | |
| **Dr. Dony Ariyus, S.S., M.Kom.**<br>**NIK. 190302128** | |

Skripsi ini telah diterima sebagai salah satu persyaratan
untuk memperoleh gelar Sarjana Komputer
18 Februari 2026

**DEKAN FAKULTAS ILMU KOMPUTER**

**Prof. Dr. Kusrini, M.Kom.**
**NIK. 190302106**

# HALAMAN PERNYATAAN KEASLIAN SKRIPSI

Yang bertandatangan di bawah ini,

**Nama mahasiswa : Munif Aryaputra**
**NIM : 22.83.0787**

Menyatakan bahwa Skripsi dengan judul berikut:

**PERANCANGAN DAN IMPLEMENTASI SISTEM ANALISIS RISIKO PRIVASI PADA PLATFORM DIGITAL MENGGUNAKAN *LIKELIHOOD–IMPACT ENGINE* BERBASIS *RULE-BASED AUTOMATION***

Dosen Pembimbing : Dr. Dony Ariyus, S.S., M.Kom.

1. Karya tulis ini adalah benar-benar ASLI dan BELUM PERNAH diajukan untuk mendapatkan gelar akademik, baik di Universitas AMIKOM Yogyakarta maupun di Perguruan Tinggi lainnya.
2. Karya tulis ini merupakan gagasan, rumusan dan penelitian SAYA sendiri, tanpa bantuan pihak lain kecuali arahan dari Dosen Pembimbing.
3. Dalam karya tulis ini tidak terdapat karya atau pendapat orang lain, kecuali secara tertulis dengan jelas dicantumkan sebagai acuan dalam naskah dengan disebutkan nama pengarang dan disebutkan dalam Daftar Pustaka pada karya tulis ini.
4. Perangkat lunak yang digunakan dalam penelitian ini sepenuhnya menjadi tanggung jawab SAYA, bukan tanggung jawab Universitas AMIKOM Yogyakarta.
5. Pernyataan ini SAYA buat dengan sesungguhnya, apabila di kemudian hari terdapat penyimpangan dan ketidakbenaran dalam pernyataan ini, maka SAYA bersedia menerima SANKSI AKADEMIK dengan pencabutan gelar yang sudah diperoleh, serta sanksi lainnya sesuai dengan norma yang berlaku di Perguruan Tinggi.

Yogyakarta, 18 Februari 2026

Yang Menyatakan,


Munif Aryaputra

## HALAMAN PERSEMBAHAN

Karya tulis ini saya persembahkan sebagai wujud rasa syukur dan terima kasih kepada:

1. Allah SWT, atas segala rahmat, hidayah dan kekuatan yang diberikan sehingga saya dapat menyelesaikan skripsi ini.
2. Kedua Orang Tua dan Keluarga, yang senantiasa memberikan doa, kasih sayang, dukungan moril, serta materil yang tak terhingga selama proses studi saya.
3. Bapak Dr. Dony Ariyus, S.S., M.Kom., selaku Dosen Pembimbing yang telah meluangkan waktu, tenaga dan pikiran untuk memberikan bimbingan serta arahan terbaik hingga skripsi ini selesai.
4. Universitas Amikom Yogyakarta, almamater kebanggaan tempat saya menimba ilmu dan mengembangkan diri.
5. Masyarakat, organisasi, pengembang dan auditor internal untuk mengukur tingkat kepatuhan awal terhadap UU PDP 2022 dan *NIST CSF 2.0* secara mandiri (*self-assessment*) dengan biaya yang terjangkau (*low-cost*).

# KATA PENGANTAR

Puji syukur penulis panjatkan ke hadirat Allah Swt. atas rahmat dan karunia-Nya sehingga penulis dapat menyelesaikan penyusunan skripsi ini dengan baik. Skripsi ini disusun sebagai salah satu syarat untuk memperoleh gelar Sarjana Komputer di Universitas Amikom Yogyakarta. Dalam kesempatan ini, penulis menyampaikan ucapan terima kasih yang sebesar-besarnya kepada:

1. Bapak Dr. Dony Ariyus, S.S., M.Kom. selaku dosen pembimbing yang telah memberikan bimbingan, arahan, serta motivasi selama proses penyusunan skripsi ini.
2. Bapak Jeki Kuswanto, S.Kom., M.Kom. selaku dosen penguji I atas koreksi, saran dan masukan yang sangat berharga dalam penyempurnaan hasil penelitian ini.
3. Bapak Melwin Syafrizal, S.Kom., M.Eng., Ph.D. selaku dosen penguji II yang telah memberikan telaah kritis dan arahan demi kualitas penelitian yang lebih baik.
4. Seluruh dosen dan staf di Universitas Amikom Yogyakarta yang telah memberikan ilmu dan dukungan selama masa perkuliahan.
5. Ayah Sujoko Wahyono, S.E dan Bunda Purwanti, S.Psi., M.M atas doa, semangat, serta dukungan moral dan material yang tiada henti.
6. Teman-teman di Pentolan Fams (Ilham, Rama, Daffa, Acil, Bela, Fina, Liona, Kak Chika, Kak Rani, Kak Rifky, Kak Feby, Kak Putri, Kak Yongki dan Kak May) atas kekonyolan dan keseriusannya.
7. Alumni AMCC, juga para ANSEHIR (Anak Semester Akhir) yang sudah berbagi pengalaman dan memberikan informasi-informasi A1 terkait berita kampus.
8. Terakhir, teman-teman seperjuangan angkatan 22-S1TK dan sebagian eks pengurus HIMTEKK 2024/2025 yang semangatnya selalu menyala seperti api.

Penulis menyadari bahwa dalam penyusunan skripsi ini masih terdapat kekurangan. Oleh karena itu, penulis dengan senang hati menerima saran/masukan yang bersifat membangun demi kesempurnaan karya ini. Semoga skripsi ini dapat memberikan manfaat bagi pembaca dan pihak-pihak yang membutuhkan.

Yogyakarta, 18 Februari 2026

Penulis

# DAFTAR ISI

# DAFTAR TABEL

## DAFTAR GAMBAR

## DAFTAR LAMBANG DAN SINGKATAN

| | |
|---|---|
| AFPI | Asosiasi Fintech Pendanaan Bersama Indonesia |
| API | *Application Programming Interface* |
| CSS | *Cascading Style Sheets* |
| DOM | *Document Object Model* |
| GDPR | *General Data Protection Regulation* |
| HTML | *Hyper Text Markup Language* |
| JS | *JavaScript* |
| KYC | *Know Your Customer* |
| MFA | *Multi-Factor Authentication* |
| *NIST CSF 2.0* | *National Institute of Standards and Technology Cybersecurity Framework* |
| OJK | Otoritas Jasa Keuangan |
| PDP | Perlindungan Data Pribadi |
| *PRISMA COKRO* | *Privacy Risk Management System & Analysis - Compliance & Risk Override* |
| PSE | Penyelenggara Sistem Elektronik |
| SPA | *Single Page Application* |
| UU PDP 2022 | Undang - Undang Perlindungan Data Pribadi |
| *CIA Triad* | *Confidentiality, Integrity, Availability* |
| $L_{eff}$ | *Likelihood Effective*: Nilai kemungkinan akhir setelah penambahan penalti keamanan. |
| $I_{eff}$ | *Impact Effective*: Nilai dampak akhir setelah penambahan bobot sensitivitas data. |
| $L_{base}$ | Nilai konstanta dasar untuk kemungkinan (*Likelihood*), bernilai 3. |
| $I_{base}$ | Nilai konstanta dasar untuk dampak (*Impact*), bernilai 3. |
| Σ | *Sigma*: Notasi matematika untuk penjumlahan akumulatif (total). |
| $P_{sec}$ | *Security Penalty*: Nilai penalti akibat lemahnya kontrol keamanan. |
| $W_{sens}$ | *Sensitivity Weight*: Nilai bobot tambahan akibat jenis data spesifik. |
| $R_{tech}$ | *Technical Risk Score*: Skor risiko teknis murni sebelum validasi legalitas. |

| | |
|---|---|
| $R_{final}$ | *Final Risk Score*: Skor risiko akhir yang ditampilkan kepada pengguna. |
| DPA | *Data Processing Agreement* |
| LLM | *Large Language Model* |
| SOP | *Standard Operating Procedure* |
| SIEM | *Security Information and Event Management* |
| URI | *Uniform Resource Identifier* |
| GEN 1.0 | Generasi 1.0 / Generasi Pertama |

# DAFTAR ISTILAH

| | |
|---|---|
| *Black -Box Testing* | Metode pengujian perangkat lunak yang berfokus pada fungsionalitas tanpa melihat struktur kode internal. |
| *Clamping* | Teknik dalam pemrograman untuk membatasi nilai variabel agar tetap berada dalam rentang minimum dan maksimum tertentu. |
| *Client-side* | Proses komputasi yang dijalankan pada sisi pengguna (*browser*), bukan pada *server*. |
| *Data Sovereignty* | Konsep bahwa data tunduk pada hukum dan peraturan negara tempat data tersebut secara fisik disimpan. |
| *Impact* | Tingkat dampak atau kerugian yang dihasilkan jika sebuah risiko terjadi. |
| *Institutional Trust* | Kepercayaan yang diberikan kepada suatu entitas karena adanya jaminan regulasi atau pengawasan otoritas. |
| *Legal Override* | Mekanisme dalam sistem ini di mana status legalitas layanan dapat menggantikan (menimpa) hasil perhitungan risiko teknis. |
| *Likelihood* | Probabilitas atau kemungkinan terjadinya suatu insiden risiko. |
| *Privacy Harm* | Dampak negatif atau kerugian yang dialami individu akibat pelanggaran privasi atau penyalahgunaan data pribadi. |
| *Residual Risk* | Risiko yang tersisa setelah upaya mitigasi atau kontrol keamanan diterapkan. |
| *Risk Engine* | Komponen perangkat lunak yang bertugas melakukan kalkulasi dan logika penilaian risiko. |
| *Rule-Based Automation* | Sistem otomatisasi yang bekerja berdasarkan serangkaian aturan logika *if-then* yang telah ditentukan sebelumnya. |
| *Client-Side Processing* | Metode pemrosesan data yang dilakukan sepenuhnya pada perangkat pengguna (*browser*) tanpa mengirimkan data input ke server eksternal, mendukung prinsip privasi. |
| *Institutional Trust Override* | Mekanisme logika dalam sistem yang memberikan pengecualian tingkat risiko rendah secara otomatis kepada entitas layanan yang terdaftar pada regulator resmi. |

| | |
|---|---|
| *Data Minimization* | Prinsip privasi untuk membatasi pengumpulan data hanya pada apa yang benar-benar diperlukan (diterapkan melalui arsitektur tanpa database pengguna). |
| *Rule-Based Mapping* | Metode pemetaan kepatuhan yang menggunakan aturan logika deterministik (*if-then*) untuk menghubungkan parameter input dengan pasal regulasi. |
| *High-Contrast UI* | Gaya antarmuka pengguna dengan kontras warna yang tinggi untuk memudahkan pembacaan informasi metrik keamanan. |
| *Likelihood-Impact Engine* | Mesin kalkulasi inti sistem yang menghitung besaran risiko berdasarkan perkalian antara faktor kemungkinan dan dampak. |
| *Crowdsourcing* | Metode pembaruan data yang mengandalkan partisipasi komunitas pengguna untuk melaporkan kesalahan atau data baru. |
| *Encrypted Local Persistence* | Mekanisme penyimpanan data sementara pada *browser* pengguna yang diamankan melalui teknik enkripsi atau *encoding*. |
| *Obfuscation* | Teknik mengaburkan data atau kode program (misalnya menggunakan *Base64*) agar tidak mudah dibaca secara kasat mata oleh manusia. |
| *Stateless* | Karakteristik aplikasi web yang tidak menyimpan status sesi pengguna di server, sehingga setiap permintaan diproses secara independen. |
| *Zero-Knowledge Architecture* | Model arsitektur sistem di mana penyedia layanan (*server*) tidak memiliki akses atau pengetahuan apa pun terhadap data yang diproses oleh pengguna. |
| *Feedback Loop* | Siklus umpan balik di mana output dari sistem atau pengguna dikembalikan sebagai input untuk perbaikan sistem di masa depan. |

# INTISARI

Peningkatan pemrosesan data pribadi pada layanan digital menimbulkan kebutuhan mendesak terhadap mekanisme penilaian risiko privasi yang lebih terstruktur dan otomatis. Berbagai platform digital mengumpulkan data sensitif melalui proses registrasi hingga interaksi layanan, namun metode penilaian risiko yang ada saat ini masih didominasi oleh pendekatan manual yang subjektif dan lebih berfokus pada keamanan infrastruktur daripada privasi pengguna. Kondisi ini berdampak pada rendahnya transparansi serta lemahnya kemampuan pengendali data dalam mengidentifikasi potensi ancaman privasi secara akurat.

Penelitian ini merancang dan mengembangkan sistem analisis risiko privasi berbasis web statis dengan menggunakan model *Likelihood–Impact* dan pendekatan *rule-based automation*. Sistem bertindak sebagai jembatan antara kompleksitas regulasi dengan kebutuhan alat *self-assessment* praktis, menerima parameter teknis berupa jenis data pribadi dan aktivitas pemrosesan, kemudian mengolahnya melalui *privacy risk engine* berbasis *JavaScript* yang berjalan sepenuhnya di sisi klien (*client-side*). Engine ini dirancang berdasarkan prinsip manajemen risiko, Undang-Undang No. 27 Tahun 2022 tentang Perlindungan Data Pribadi (PDP) dan kerangka kerja *NIST Cybersecurity Framework 2.0*.

Hasil penelitian menunjukkan bahwa sistem mampu menghasilkan klasifikasi risiko, peta risiko, evaluasi kepatuhan dan rekomendasi otomatis secara konsisten. Sistem ini bermanfaat bagi pengembang aplikasi, auditor internal, regulator dan organisasi yang memerlukan penilaian risiko privasi yang otomatis, kuantitatif, mudah diakses dan mendukung implementasi cepat tanpa biaya infrastruktur tinggi. Ke depan, pengembangan lanjutan dapat diarahkan pada peningkatan cakupan aturan dan interoperabilitas dengan sistem manajemen keamanan informasi lainnya.

**Kata kunci:** Risiko Privasi, *Likelihood–Impact*, *Rule-Based Engine*, UU PDP 2022, *NIST CSF 2.0*.

## *ABSTRACT*

*The increasing processing of personal data in digital services has created an urgent need for a more structured and automated privacy risk assessment mechanism. Various digital platforms collect sensitive data throughout the registration process and service interactions, but current risk assessment methods are still dominated by subjective, manual approaches that focus more on infrastructure security than user privacy. This situation results in low transparency and weakens the ability of data controllers to accurately identify potential privacy threats.*

*This research designs and develops a static web-based privacy risk analysis system using the Likelihood–Impact model and a rule-based automation approach. The system acts as a bridge between regulatory complexity and the need for practical self-assessment tools. It accepts technical parameters such as personal data types and processing activities and processes them through a JavaScript-based privacy risk engine that runs entirely on the client side. This engine is designed based on risk management principles, Law No. 27 of 2022 concerning Personal Data Protection (PDP) and the NIST Cybersecurity Framework 2.0 framework.*

*The results demonstrate that the system is capable of consistently generating risk classifications, risk maps, compliance evaluations, and automated recommendations. This system is useful for application developers, internal auditors, regulators and organizations requiring automated, quantitative and easily accessible privacy risk assessments that support rapid implementation without high infrastructure costs. Future developments could focus on increasing rule coverage and interoperability with other information security management systems.*



***Keyword:*** *Privacy Risk, Likelihood–Impact, Rule-Based Engine, PDP Law, NIST CSF 2.0.*