

# Security Risk Analysis

---

A PRESENTATION BY  
KELOMPOK I SPM, DAREL PINEM,  
RAHMAT SITUMORANG.



# Content

---

1

ATTACK  
PATTERNS

2

RISK ANALYSIS

3

FOREST LEVEL  
VIEW

4

ARCHITECTURAL  
RISK ANALYSIS

# ATTACK PATTERNS

Attack Patterns merupakan katergorisasi teknik dan prosedur yang digunakan oleh penyerang saat ingin melakukan peretasan pada sebuah target.

Fungsi dari kategorisasi ini adalah untuk mempermudah mencatat dan menanggulangi jika ada kebocoran keamanan pada sebuah software.



# Possible pattern used

1

## File Content Injection

### Description:

Tipe serangan paling umum yang dilakukan, dimana penyerang akan melakukan serangan dengan memasukkan muatan berbahaya seperti malware ke dalam sebuah file seperti PDF, IMG dan file lainnya. Penyebaran file yang sudah dimodifikasi tersebut akan dilakukan dengan menggunakan email atau media penyebaran lainnya. Pada SPM IT Del, serangan dapat dilakukan dengan mengupload malware pada document management.

## CONTOH :

1. Memanfaatkan Formulir Input: Penyerang dapat memanfaatkan formulir input yang tidak divalidasi dengan benar oleh aplikasi web. Mereka bisa menyisipkan konten berbahaya seperti kode skrip atau perintah shell ke dalam bidang formulir, yang kemudian dieksekusi oleh sistem saat diproses.
1. Upload File: Serangan ini juga bisa terjadi melalui fitur unggah file di aplikasi web. Penyerang dapat mengunggah file yang berisi skrip berbahaya atau payload yang akan dieksekusi oleh server.

# Possible pattern used

2

Brute Force Attack (Serangan Brute Force):

Serangan Brute Force adalah teknik di mana penyerang mencoba semua kemungkinan kombinasi kata sandi atau kunci enkripsi untuk mendapatkan akses ke suatu sistem atau akun. Teknik ini menjadi lebih efektif saat kata sandi yang lemah atau tidak aman digunakan.

## CONTOH :

- 1.Pencarian Semua Kemungkinan: Penyerang menggunakan perangkat lunak khusus yang secara otomatis mencoba semua kemungkinan kombinasi kata sandi atau kunci enkripsi untuk mendapatkan akses ke suatu sistem atau akun.
- 2.Iterasi Berulang: Serangan ini melibatkan iterasi berulang dari upaya masuk ke sistem dengan mencoba kata sandi yang berbeda-beda setiap kali.
- 3.Dictionary Attack: Penyerang menggunakan daftar kata sandi yang umum atau "dictionary" untuk mencoba masuk ke sistem. Dictionary ini bisa berupa daftar kata sandi yang sering digunakan, kata-kata umum, atau kombinasi kata-kata yang mungkin digunakan oleh pengguna.
- 4.Penyusupan Akun: Penyerang juga dapat menggunakan brute force attack untuk mencoba masuk ke akun pengguna dengan mencoba kombinasi nama pengguna dan kata sandi yang berbeda.

# Possible pattern used

3

Phishing:

Phishing adalah upaya penipuan daring yang dilakukan dengan membuat situs web palsu atau mengirim email palsu yang meniru situs web asli untuk mencuri informasi pribadi pengguna, seperti nama pengguna, kata sandi, atau informasi keuangan. Situs phishing mungkin akan didesain sedemikian rupa agar terlihat serupa dengan situs asli Sistem Penjaminan Mutu IT Del.

## CONTOH :

1. Link atau Lampiran Berbahaya: Pesan phishing sering mengandung tautan yang mengarah ke situs web palsu yang dirancang untuk mencuri informasi pengguna atau mengandung lampiran berbahaya yang dapat menginstal malware atau virus pada komputer korban.
2. Domain dan Logo Tiruan: Penyerang sering membuat domain web atau alamat email yang menyerupai entitas yang ditiru, serta menggunakan logo dan citra merek palsu untuk meningkatkan kesan keaslian pesan.
3. Spoofing Alamat Email: Penyerang dapat menggunakan teknik spoofing untuk menyamar alamat email pengirim agar terlihat seperti berasal dari entitas tepercaya, meskipun sebenarnya berasal dari sumber yang tidak sah.

# Risk Analysis



# Risk Analysis

1

## Authentication

Risiko: Jika verifikasi akun admin dan pengguna tidak dilakukan dengan benar, data dan dokumen pada website dapat diakses dan diedit oleh pihak yang tidak sah, mengancam keamanan dan integritas sistem.

Mitigasi: Implementasi mekanisme autentikasi yang kuat serta pemantauan aktif terhadap aktivitas masuk yang mencurigakan.

# Risk Analysis

2

## Authorization

Risiko: Tanpa pengaturan izin yang tepat, risiko akses tidak sah atau modifikasi data oleh akun admin dapat terjadi, mengancam keamanan dan validitas informasi.

Mitigasi: Penetapan model otorisasi yang ketat dan pemantauan aktivitas admin SPM IT Del secara berkala.

# Risk Analysis

3

## Auditing

Risiko: Kurangnya filterisasi data dan kurangnya proses checking dokumen dapat menyebabkan penyajian informasi yang tidak akurat, mengurangi integritas data dan kepercayaan pengguna terhadap sistem.

Mitigasi: Implementasi kontrol validasi data yang ketat dalam penginputan dokumen dan pemantauan aktivitas untuk mendeteksi anomali.

# Risk Analysis

4

## Integrity

Risiko: Kekurangan notifikasi untuk kesalahan input data dapat mengakibatkan kesalahan data yang tidak terdeteksi, mengurangi kualitas informasi dan efektivitas pengguna.

Mitigasi: Implementasi validasi data dan mekanisme notifikasi kesalahan untuk memastikan integritas data yang optimal.

# Risk Analysis

5

## Perubahan Proses Pengembangan

Risiko: Tanpa pemantauan yang tepat terhadap perubahan sistem, risiko kegagalan atau kerusakan sistem saat implementasi perubahan dapat meningkat.

Mitigasi: Melakukan uji coba secara berkala selama pengembangan website SPM IT Del dan pemantauan ketat selama perubahan sistem, serta memiliki rencana pemulihan yang solid jika diperlukan.

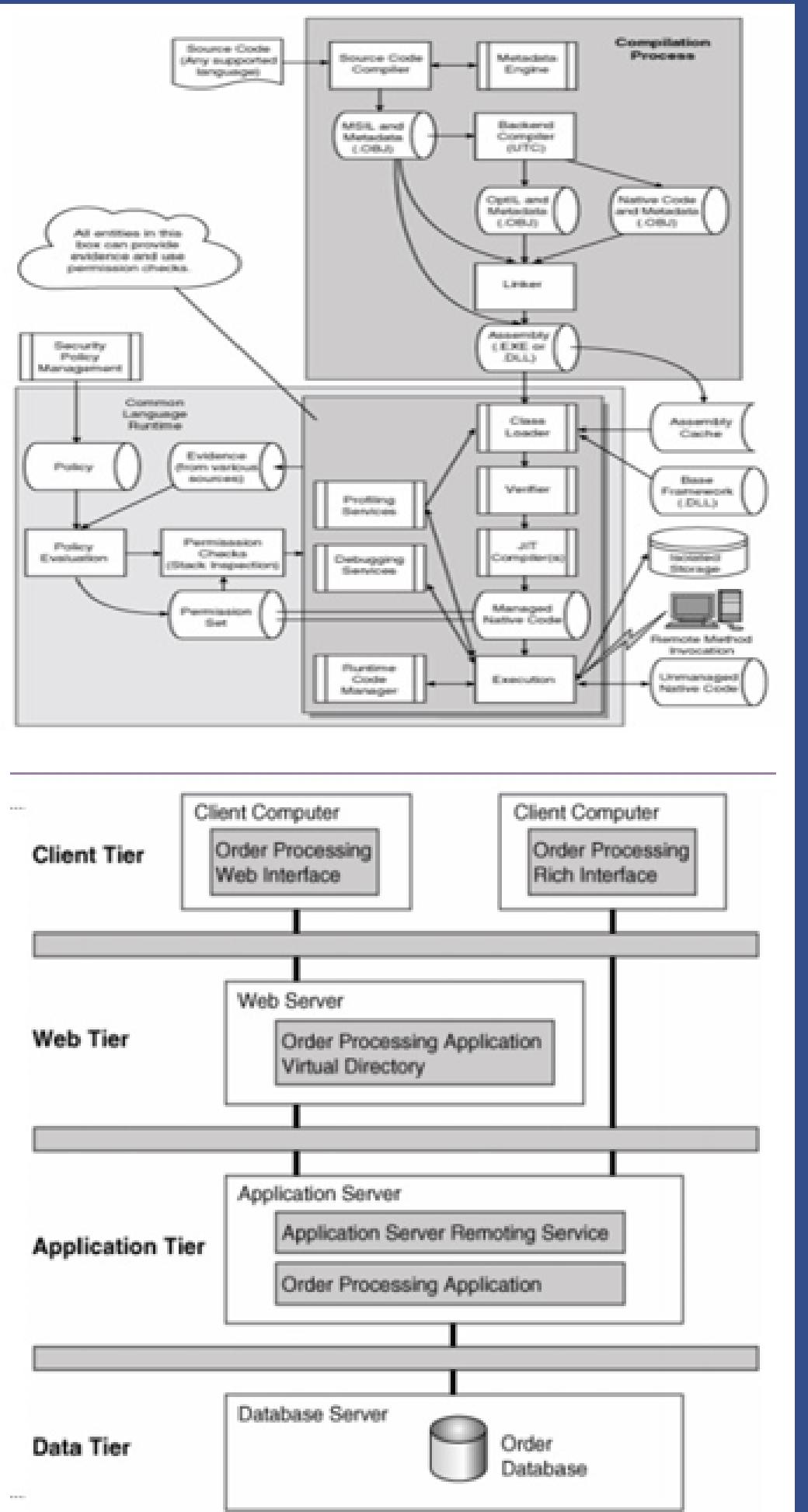
# Forest Level View



# Forest Level View

Forest level view adalah pandangan yang holistik terhadap semua aspek yang terlibat dalam suatu lingkungan atau sistem. Dalam konteks ini, forest level view akan mencakup semua aspek yang terkait dengan keamanan dan integritas sistem, termasuk autentikasi, otorisasi, auditing, integritas data, dan manajemen perubahan.





# FOREST LEVEL VIEW

## 1. AUTENTIKASI

- VERIFIKASI AKUN ADMIN DAN USER
- BATASI PERCOBAAN GAGAL SAAT LOGIN

## 2. OTORISASI

- AKSES DATA DIRI ADMIN
- AKSES INFORMASI PRIBADI ADMIN LAIN
- HANYA SUPER ADMIN YANG DAPAT MELIHAT DAN MENGEDIT INFORMASI PRIBADI ADMIN LAIN

# FOREST LEVEL VIEW

## 3. AUDIT

- FILTERISASI DATA YANG DIMASUKKAN

## 4. INTEGRITAS

- CHECKING DAN APPROVAL DOKUMEN

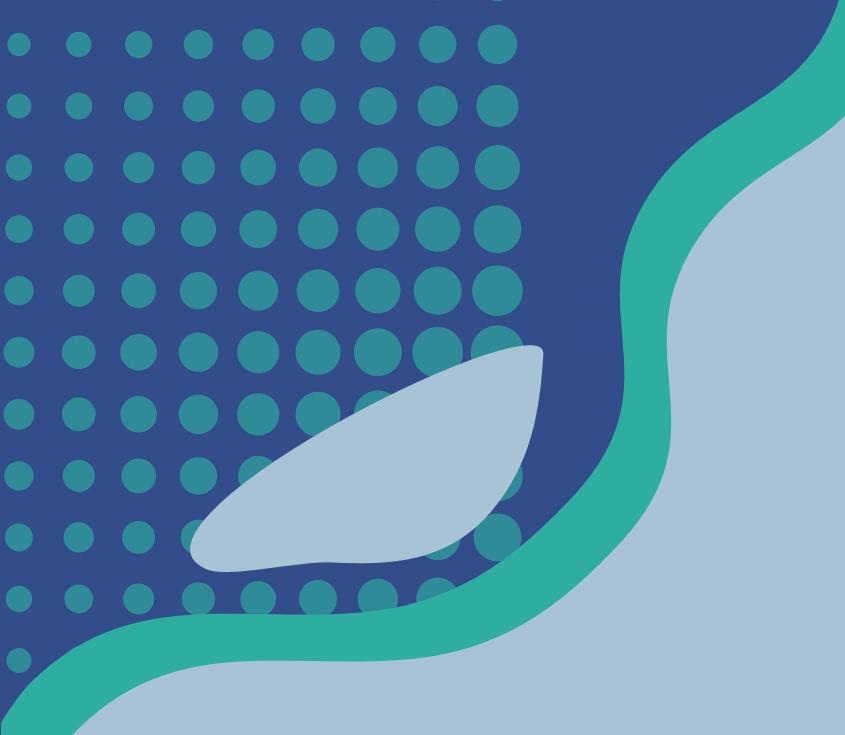
- MEMASTIKAN DATA USER TIDAK RUSAK

- SUPERADMIN DAPAT MELIHAT LOG AKTIVITAS

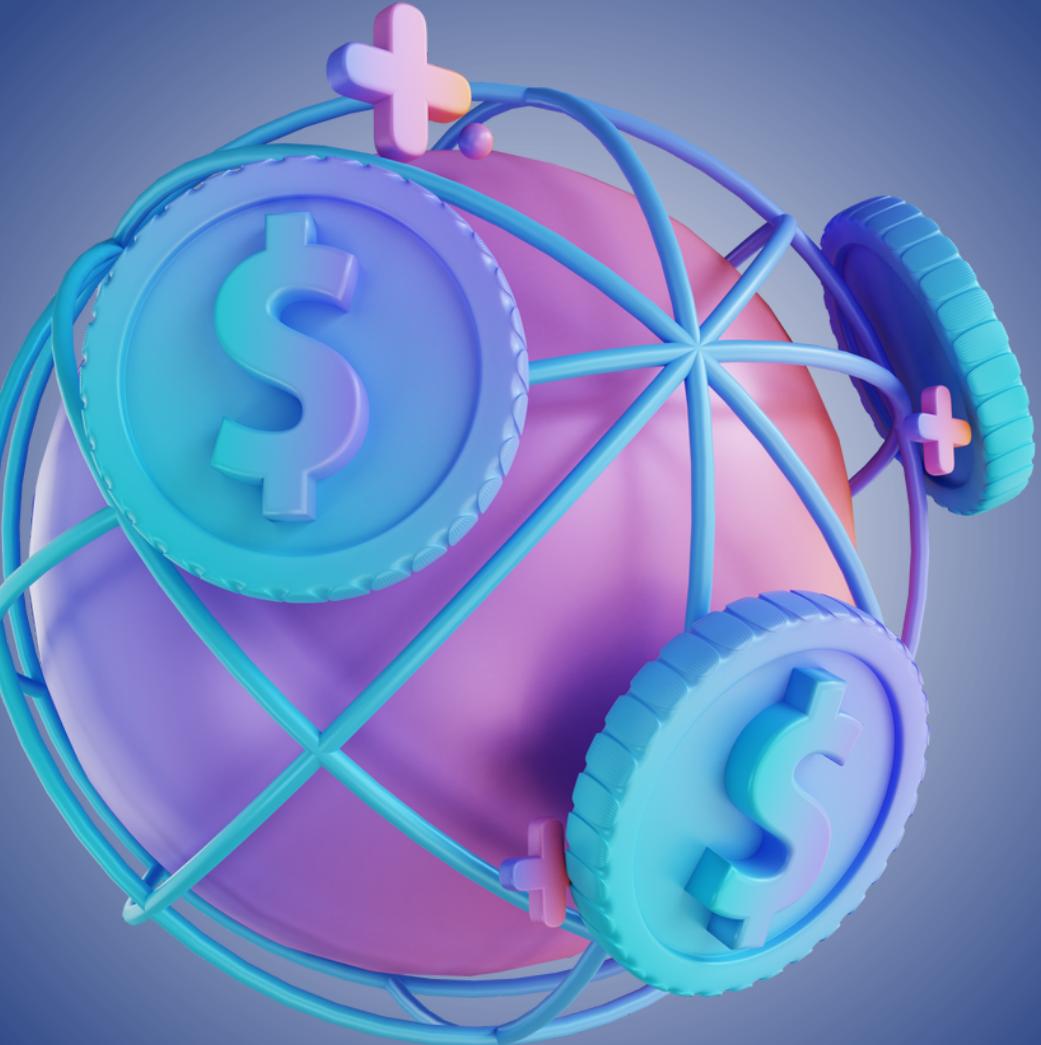
- NOTIFIKASI JIKA ADMIN SALAH MEMASUKKAN DATA

- MEMASTIKAN SISTEM TIDAK RUSAK KETIKA ADA PERUBAHAN PROSES

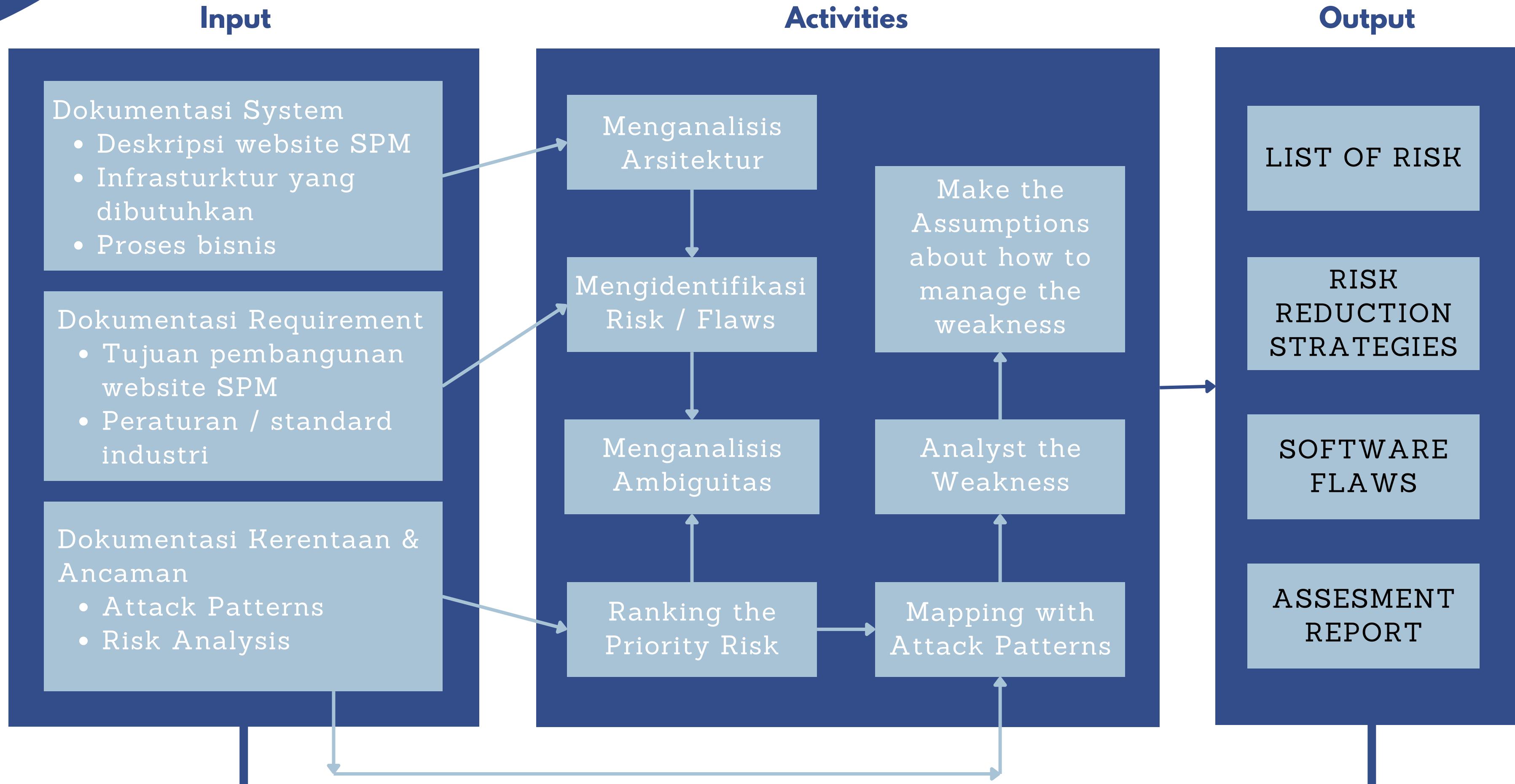
- PENGEMBANGAN



# Architecture Risk Analysis



# Architecture Risk Analysis





# Thank You

---