NIVEDITA JOURNAL INFORMATICS

Vol. 02, No. 1, December 2025
ISSN: 3089-8366 (Media Online)

EVALUASI RISIKO IMPLEMENTASI CHATBOT AI PADA MOBILE BANKING BANK XYZ DENGAN METODE OCTAVE ALLEGRO

Afif Fathin[1], Hadid[2], Angraini[3]
[123] Program Studi Sistem Informasi, Universitas Islam Negeri Sultan Syarif Kasim Riau, Kota Pekanbaru, Indonesia

Email: 12250311728@students.uin-suska.ac.id

Diajukan: 12 Juni 2025; Diterima: 31 Oktober 2025; DOI: doi.org/10.25078/nivedita.v2i1.5083

ABSTRACT *The chatbot AI SALMAH is implemented in the Mobile Banking service of Bank XYZ Pekanbaru Branch to improve customer service based on Islamic banking principles. The system aims to provide instant, accurate, and syariah-compliant assistance to customers. However, several risks are associated with this AI integration, including data security, regulatory compliance, and user adoption challenges. This study aims to identify potential threats, evaluate risks, and analyze their impact on banking operations using the High-level IT Risk Assessment framework supported by concepts from OCTAVE Allegro. The assessment revealed five key risk factors: syariah regulatory compliance, data security, customer adoption, industry competition, and rapid technological change. Mitigation strategies include strengthening data protection, customer education, system updates, and continuous monitoring. The highest risk was related to data security breaches and inaccurate chatbot responses. This research provides valuable insights for managing IT risks in syariah-based digital banking services and guides further improvements in AI implementation. Future studies may focus on comprehensive mitigation measures and effectiveness monitoring.*
Keywords: *Chatbot AI, Information Technology Risk, Mobile Banking, Islamic Banking, Risk Management*

ABSTRAK Chatbot AI SALMAH diimplementasikan dalam layanan Mobile Banking Bank XYZ Cabang Pekanbaru untuk meningkatkan pelayanan nasabah berbasis prinsip perbankan syariah. Sistem ini bertujuan memberikan bantuan cepat, akurat, dan sesuai syariah kepada nasabah. Namun, integrasi AI ini memiliki beberapa risiko, termasuk keamanan data, kepatuhan regulasi, serta tantangan adopsi pengguna. Penelitian ini bertujuan mengidentifikasi ancaman, mengevaluasi risiko, dan menganalisis dampaknya terhadap operasional perbankan menggunakan kerangka High-level IT Risk Assessment dengan dukungan konsep OCTAVE Allegro. Hasil penilaian mengungkap lima faktor risiko utama: kepatuhan regulasi syariah, keamanan data, adopsi nasabah, persaingan industri, dan perubahan teknologi yang cepat. Strategi mitigasi meliputi penguatan perlindungan data, edukasi nasabah, pembaruan sistem, dan pemantauan berkelanjutan. Risiko tertinggi terkait dengan kebocoran data dan informasi chatbot yang tidak akurat. Penelitian ini memberikan wawasan penting dalam pengelolaan risiko TI pada layanan perbankan digital berbasis syariah serta panduan pengembangan implementasi AI selanjutnya. Penelitian berikutnya dapat fokus pada penerapan mitigasi yang lebih komprehensif dan evaluasi efektivitasnya.
Kata Kunci: Chatbot AI, Risiko Teknologi Informasi, Mobile Banking, Perbankan Syariah, Manajemen Risiko

PENDAHULUAN

Teknologi informasi merupakan alat yang sangat penting saat ini, terutama dalam mendukung inovasi layanan di sektor perbankan syariah. Pemanfaatan teknologi informasi dalam perbankan, khususnya dalam layanan Mobile Banking berbasis kecerdasan buatan (AI), dapat meningkatkan efisiensi, efektivitas, dan akuntabilitas dalam pelayanan nasabah. Dalam perencanaan pengelolaan teknologi informasi, diperlukan tata kelola yang baik untuk menjamin bahwa tujuan organisasi dapat dicapai secara optimal melalui proses yang efisien dan aman [1]. Keberhasilan organisasi perbankan saat ini sering diukur dari seberapa baik tata kelola TI mendukung operasional dan inovasi layanan, termasuk integrasi AI dalam chatbot layanan pelanggan [3].

Manfaat dari penggunaan teknologi informasi dalam layanan perbankan syariah adalah meningkatnya kecepatan layanan, kemudahan akses bagi nasabah, serta peningkatan transparansi dan kepatuhan terhadap

prinsip-prinsip syariah [4]. Namun demikian, beberapa institusi belum melakukan penilaian risiko secara sistematis terhadap sistem informasi digital yang digunakan, sehingga mengakibatkan ketidakmampuan mengidentifikasi dan mengelola risiko yang mungkin timbul. Masalah teknis seperti kebocoran data, kegagalan sistem, dan ketidaksesuaian regulasi dapat mengganggu kelancaran operasional dan menurunkan kepercayaan nasabah [6].

SALMAH merupakan chatbot layanan nasabah yang terintegrasi dalam aplikasi Mobile Banking Bank XYZ. Fungsinya meliputi tanya jawab FAQ produk dan kepatuhan syariah, alur terpandu (guided flow) untuk blokir kartu, reset PIN, dan pengecekan status transaksi, mekanisme handover ke petugas (live agent) ketika tingkat kepercayaan jawaban rendah, serta penyampaian notifikasi layanan.

Secara arsitektural, SALMAH terdiri atas modul pemahaman bahasa alami (NLU) dan pengelola dialog yang mengolah intent, entitas, dan confidence score sekaligus menyediakan fallback; gerbang API yang terhubung ke inti mobile banking dengan hak akses baca atas data non-sensitif, sedangkan operasi sensitif tetap dilakukan melalui antarmuka resmi dengan autentikasi multi-faktor; basis pengetahuan terkurasi (FAQ dan kebijakan syariah yang ditinjau Dewan Pengawas Syariah); lapis observability yang mencakup audit log, pelacakan sesi, anonimisasi PII, dan rate limiting; praktik model operations seperti versioning, uji A/B, dan human-in-the-loop untuk ujaran baru; pengamanan menyeluruh (TLS ujung ke ujung, secret management, WAF, sanitasi masukan, content filter, serta RBAC untuk akses admin); serta mekanisme keberlanjutan layanan berupa penskalaan otomatis, circuit breaker, dan graceful degradation ke FAQ statis saat jaringan terganggu. Rincian ini menjadi landasan identifikasi aset informasi dan penyusunan skenario ancaman dalam penilaian risiko.

Implementasi chatbot AI SALMAH pada Mobile Banking Bank XYZ Cabang Pekanbaru bertujuan meningkatkan kualitas layanan dengan memanfaatkan teknologi AI yang mampu memberikan informasi cepat dan akurat secara syariah-compliant. Seluruh sistem digital yang digunakan perlu dipelihara, diawasi, serta dikembangkan dengan manajemen risiko yang tepat agar potensi risiko dapat diminimalisasi dan tujuan pelayanan tercapai [1].

Penilaian risiko menjadi langkah penting bagi organisasi untuk menerapkan pengendalian yang bertujuan mengurangi efek negatif yang mungkin terjadi pada proses bisnis yang menggunakan sistem informasi. Risiko dalam sistem informasi dapat merugikan bisnis, terutama terkait reputasi, keuangan, kelancaran produktivitas, serta kepatuhan terhadap regulasi [1]. Untuk mencapai hasil yang optimal dan mengurangi ketidakpastian, organisasi melakukan manajemen risiko teknologi informasi [2].

Metode penilaian risiko yang digunakan dalam penelitian ini mengacu pada kerangka kerja *High-level IT Risk Assessment* berdasarkan *Risk IT Practitioner Guide*, dengan dukungan konsep dari metode OCTAVE Allegro. Metode OCTAVE Allegro fokus pada penilaian risiko terhadap aset informasi organisasi, memperhatikan penggunaan, penyimpanan, transportasi, serta potensi gangguan yang dapat terjadi [3]. Metode ini berbeda dari metode OCTAVE sebelumnya karena lebih menitikberatkan pada konteks bisnis dan penggunaan aset informasi secara menyeluruh [4][5]. Metode ini dipilih karena kemampuannya menghasilkan penilaian risiko yang komprehensif walau dalam kondisi sumber daya terbatas [6].

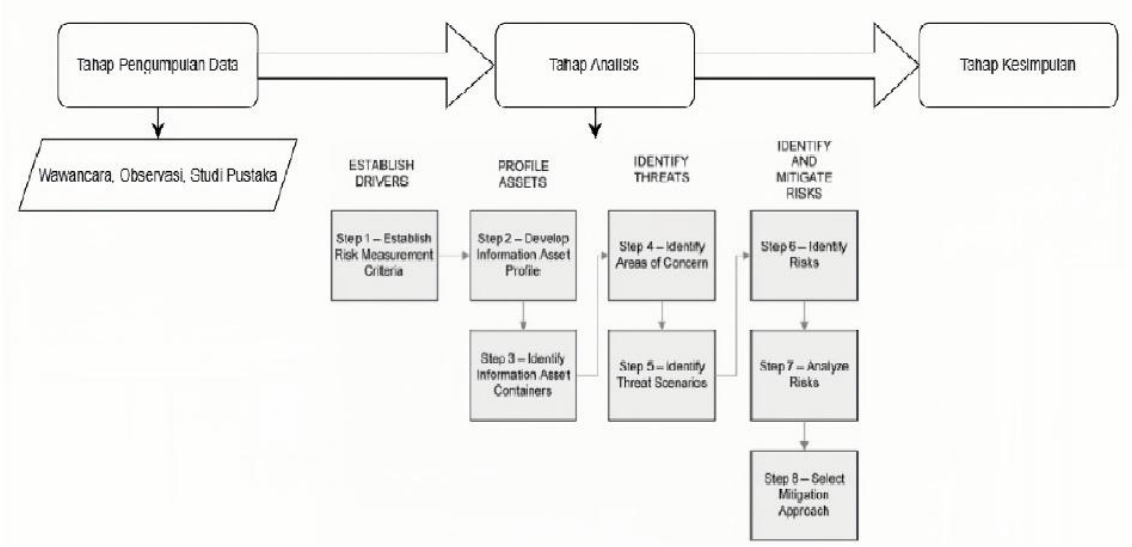
Tujuan dari penelitian ini adalah melakukan pengukuran risiko implementasi chatbot AI SALMAH pada layanan Mobile Banking Bank XYZ Cabang Pekanbaru. Penilaian risiko ini diharapkan dapat membantu mengidentifikasi ancaman yang mungkin terjadi, seperti kebocoran data, kesalahan informasi chatbot, dan tantangan adopsi pengguna, sehingga bank dapat mengambil tindakan mitigasi yang tepat untuk menjaga keamanan, kepatuhan, dan kualitas layanan.

METODE PENELITIAN

Penelitian ini mengadopsi metode penelitian kualitatif dengan hasil yang disajikan dalam bentuk deskriptif, serta menggunakan pendekatan khusus untuk penilaian risiko teknologi informasi, yakni High-level IT Risk Assessment berdasarkan Risk IT Practitioner Guide, dengan dukungan konsep dari metode OCTAVE Allegro. Pengumpulan data dilakukan melalui wawancara, observasi, dan studi pustaka untuk memperkuat pembahasan dan analisis.

A. Tahapan Penelitian

Gambar 1. di bawah ini menunjukkan tahapan penelitian yang mengikuti kerangka kerja *OCTAVE Allegro* dalam proses identifikasi dan mitigasi risiko TI.



Gambar 1. Tahapan Penelitian

1. **Tahap Pengumpulan Data.**

Data dikumpulkan melalui wawancara semi-terstruktur dengan staf IT dan manajemen risiko Bank XYZ Cabang Pekanbaru, observasi langsung kondisi implementasi chatbot AI SALMAH, serta studi literatur terkait manajemen risiko TI dan penerapan AI dalam perbankan syariah.

2. **Tahap Analisis/Pengolahan Data**

Data wawancara dan observasi yang terkumpul kemudian dianalisis dengan mengikuti langkah-langkah metode OCTAVE Allegro, yang meliputi:

a. Tahap pertama: Membangun Penggerak (*Establish Drivers*) Menetapkan kriteria dan standar penilaian risiko yang konsisten untuk evaluasi.
b. Tahap dua: profil aset (*Profile Assets*)
Mengembangkan profil aset informasi yang kritis, termasuk aplikasi chatbot, data nasabah, dan infrastruktur TI pendukung.
c. Tahap ketiga: Identifikasi Aset (*Identify Threats*)
Mengidentifikasi area perhatian (areas of concern) dan skenario ancaman (threat scenarios) yang berpotensi mengganggu aset informasi.
d. Tahap keempat: Identifikasi dan Pengurangan Risiko (*Identify And Mitigate Risk*) Meliputi identifikasi risiko spesifik, analisis dampak dan probabilitas risiko, serta pemilihan pendekatan mitigasi yang tepat.

3. **Tahap Kesimpulan**

Berdasarkan hasil analisis data dan penilaian risiko menggunakan metode OCTAVE Allegro serta High-level IT Risk Assessment, peneliti menarik kesimpulan dan memberikan rekomendasi strategis untuk pengelolaan risiko TI terkait implementasi chatbot AI SALMAH.

B. *RACI Model*

Dalam penelitian ini dibuat tabel *RACI* untuk mengidentifikasi peran dan tanggung jawab para narasumber dan pihak terkait dalam pelaksanaan aktivitas penelitian. RACI adalah singkatan dari empat peran dalam manajemen tugas yang menjelaskan keterlibatan masing-masing pihak, yaitu:

Tabel 1. Tabel *RACI Chart* Sistem Informasi Chatbot AI SALMAH

Aktivitas	Kepala IT Bank XYZ	Manajer Proyek IT	Tim Pengembang Chatbot	Manajemen Risiko Bank	Tim Pelatihan Nasabah	Nasabah
Pengumpulan Data Wawancara	I	A	C	C	I	I
Observasi Implementasi	I	A	R	C	I	I

Aktivitas	Kepala IT Bank XYZ	Manajer Proyek IT	Tim Pengembang Chatbot	Manajemen Risiko Bank	Tim Pelatihan Nasabah	Nasabah
Analisis Risiko	C	A	R	R	I	I
Penyusunan Strategi Mitigasi	I	A	C	R	C	I
Pelatihan dan Edukasi Nasabah	I	C	I	C	R	I
Monitoring dan Evaluasi	C	A	R	R	C	I

Untuk menentukan peran-peran responden, RACI Chart digunakan, dengan;
a. R (*Responsible*): Bertanggung jawab langsung melakukan aktivitas
b. A (*Accountable*): Memiliki otoritas dan keputusan akhir
c. C (*Consulted*): Diberi konsultasi dan masukan
d. I (*Informed*): Mendapatkan informasi terkait progres

HASIL DAN PEMBAHASAN

Hasil penelitian ini mencakup seluruh tahapan yang ada pada metode OCTAVE Allegro, yang digunakan dalam paduan lembar kerja penilaian risiko. Berikut adalah hasilnya:

1. Tahap Pertama: *Establish Drivers*

Pada tahap ini dilakukan pembangunan kriteria pengukuran risiko, yang bertujuan menetapkan standar dan skala prioritas untuk mengukur dampak risiko terhadap area penting. Kriteria pengukuran ini mencakup dampak pada beberapa area utama, yakni Reputasi dan Kepercayaan Pelanggan, Keuangan, Produktivitas, Keamanan. **Tabel 2.** berikut menggambarkan skala prioritas yang diberikan pada setiap area dampak berdasarkan hasil analisis dan wawancara dengan narasumber.

Tabel 2. Skala Prioritas Area Dampak Risiko

Prioritas	Area Dampak	Keterangan
1	Keamanan	Meliputi perlindungan data dan sistem TI
2	Keuangan	Dampak terhadap biaya dan pendapatan bank
3	Produktivitas	Pengaruh pada kelancaran operasional
4	Reputasi dan Kepercayaan Pelanggan	Pengaruh pada citra dan kepercayaan nasabah

2. Tahap kedua: *Profile Assets*

a. Kegiatan *Develop Information Asset Profile*

Pada tahap ini dilakukan identifikasi dan pengembangan profil aset informasi yang kritis dalam implementasi chatbot AI SALMAH pada layanan Mobile Banking Bank XYZ. Profil aset ini menjadi dasar untuk mengevaluasi risiko terhadap masing-masing aset dan menentukan prioritas pengamanan dan Profil aset yang lengkap ini memudahkan proses identifikasi ancaman dan mitigasi risiko yang tepat sesuai dengan karakteristik masing-masing asset dan berikut adalah Aset-aset penting meliputi:

Tabel 3. Profil Aset Informasi Kritis

Jenis Aset	Contoh Aset	Deskripsi / Fungsi	Pemilik Aset
Software	Chatbot AI SALMAH	Memberikan layanan bantuan otomatis pada nasabah	Tim Pengembang IT Bank
Hardware	Server dan perangkat jaringan	Menyimpan data dan menjalankan aplikasi chatbot	Departemen IT Bank
Sistem Informasi	Sistem Mobile Banking	Platform utama transaksi dan layanan nasabah	Divisi Operasional
Sumber Daya Manusia	Tim IT, Manajemen Risiko, Nasabah	Pengelola dan pengguna sistem	Bank XYZ

b. Kegiatan *Identify Information Asset Containers*

Pada tahap ini dilakukan identifikasi lokasi penyimpanan dan pengelolaan aset informasi yang terkait

dengan implementasi chatbot AI SALMAH. Tempat penyimpanan aset informasi ini dikelompokkan ke dalam tiga kategori utama, yaitu Physical Container, People Container, Technical Container.

Tabel 4. Peta Lingkungan Risiko Aset Informasi

Jenis Container	Deskripsi	Pemilik Aset
Physical Container	Server Bank XYZ Pekanbaru	Unit Infrastruktur TI Bank
Technical Container	Sistem Operasi, Chatbot AI SALMAH	Tim Pengembang dan IT Bank
Technical Container	Jaringan Internet dan Firewall	Departemen Keamanan TI Bank
People Container	Tim IT, Manajemen Risiko, Nasabah	Bank XYZ Cabang Pekanbaru

3. Tahap ketiga: *Identify Threats*

a.* Kegiatan *Identify Areas of Concern

Pada tahap ini dilakukan identifikasi area yang diamati (areas of concern), yaitu kondisi atau situasi yang sebenarnya terjadi dan memiliki potensi untuk mempengaruhi aset informasi penting pada implementasi chatbot AI SALMAH. Beberapa area perhatian utama yang ditemukan meliputi Penyebaran gangguan keamanan sistem, Ketidakstabilan koneksi internet, Keterbatasan kapasitas penyimpanan server, Identifikasi area perhatian ini menjadi dasar bagi langkah selanjutnya dalam mengembangkan skenario ancaman yang spesifik dan menyusun strategi mitigasi risiko yang tepat.

Tabel 5. Area yang diamati

Area yang Diamati	Jenis Gangguan / Ancaman	Dampak Potensial
Penyebaran gangguan keamanan sistem	Virus, serangan siber, akses tidak sah	Kehilangan data, gangguan operasional
Ketidakstabilan koneksi internet	Gangguan dari provider, bandwidth terbatas	Sistem tidak dapat diakses, layanan terganggu
Keterbatasan kapasitas penyimpanan server	Overload, kegagalan hardware	Data tidak lengkap, sistem lambat

b. Kegiatan *Identify Threat Scenarios*

Pada tahap ini, semua areas of concern yang telah diidentifikasi sebelumnya diubah menjadi threat scenarios yang menjelaskan bagaimana suatu masalah atau tindakan dapat menimbulkan ancaman terhadap aset informasi. Karakteristik ancaman diuraikan untuk memperjelas aktor, penyebab, motif, dampak, dan probabilitasnya.

Dengan mengidentifikasi skenario ancaman secara terperinci, bank dapat menentukan prioritas risiko yang harus ditangani dan menyiapkan langkah mitigasi yang tepat untuk menjaga keamanan dan stabilitas sistem chatbot AI SALMAH.

Tabel 6. Karakteristik Ancaman

Item	Keterangan
Gangguan Celah Keamanan Sistem	
Aktor	Virus, hacker, pihak internal yang tidak bertanggung jawab
Penyebab	Gangguan yang menyebabkan kegagalan software, pencurian data
Motif	Tidak sengaja atau tindakan kriminal
Hasil	Kerusakan sistem, gangguan layanan, pencurian data
Keamanan	Penerapan firewall dan update antivirus secara rutin
Probabilitas	Rendah
Kapasitas Ruang Penyimpanan	
Aktor	-
Penyebab	Sistem down karena kapasitas server tidak mencukupi
Motif	Tidak sengaja
Hasil	Modifikasi data, gangguan layanan
Keamanan	Penambahan kapasitas penyimpanan
Probabilitas	Rendah

Item	Keterangan
Tidak Stabilnya Koneksi Internet	
Aktor	-
Penyebab	Ketidakmampuan provider memenuhi kebutuhan bandwidth
Motif	Tidak sengaja
Hasil	Modifikasi layanan, gangguan akses sistem
Keamanan	Penambahan bandwidth, pengelolaan manajemen jaringan
Probabilitas	Rendah

4. Tahap keeempat: *Identify and Mitigate Risk*

a. Kegiatan *Identify Risk*

Pada tahap ini, keadaan ancaman yang telah dicatat dalam laporan risiko aset informasi dianalisis untuk menentukan dampak yang dapat terjadi pada organisasi. Ancaman tersebut dihubungkan dengan potensi kerugian dan gangguan operasional yang mungkin diakibatkan pada implementasi chatbot AI SALMAH. Beberapa risiko yang diidentifikasi beserta dampaknya adalah sebagai berikut:

Tabel 7. Informasi Lembar Kerja Risiko Aset Identifikasi Risiko

Area yang Diamati	Dampak
Penyebaran gangguan keamanan sistem oleh pihak eksternal dan internal	Kehilangan data nasabah, terganggunya proses pelayanan, serta penurunan kepercayaan pelanggan
Keterbatasan kapasitas penyimpanan pada server	Data tidak lengkap, sistem berjalan lambat, dan gangguan akses layanan
Ketidakstabilan koneksi internet	Gangguan akses sistem, keterlambatan layanan, dan potensi kegagalan transaksi

b. Kegiatan *Analyze Risk*

Pada tahap ini dilakukan evaluasi terhadap situasi ancaman dan konsekuensi yang telah diidentifikasi sebelumnya, untuk menentukan dampaknya terhadap standar operasional saat ini. Proses evaluasi ini mempertimbangkan dampak terhadap beberapa area, yaitu reputasi & kepercayaan pelanggan, keuangan, produktivitas, dan keamanan.

Skala tingkat dampak menggunakan tiga level *(Low = 1, Medium = 2, High = 3)* dengan bobot per area sesuai prioritas Keamanan = 4, Keuangan = 3, Produktivitas = 2, dan Reputasi/Kepercayaan = 1. Nilai untuk tiap area dihitung sebagai level × bobot, lalu Total Nilai Risiko diperoleh dari penjumlahan seluruh area; tanpa memasukkan kemungkinan terjadinya (*likelihood*), total < 12 diklasifikasikan Rendah, 12–20 Sedang, dan >20 Tinggi. Bila organisasi ingin memasukkan *likelihood* (1–3), Skor Akhir dihitung sebagai Total × *likelihood*, dengan ambang klasifikasi mengikuti kebijakan risiko bank.

Menggunakan aturan ini, skenario gangguan keamanan sistem menghasilkan total 16 (Sedang)—Reputasi 3×1=3, Keuangan 1×3=3, Produktivitas 3×2=6, dan Keamanan 1×4=4. Skenario koneksi internet tidak stabil memberi total 22 (Tinggi) karena tiga area bernilai High dan Keamanan Low ((3×1)+(3×3)+(3×2)+(1×4)=3+9+6+4=22). Adapun kapasitas penyimpanan terbatas menghasilkan total 19 (Sedang) dari kombinasi *High, Medium, High*, dan *Low* (3+6+6+4=19).

Hasil ini tetap menempatkan "koneksi internet tidak stabil" sebagai risiko tertinggi dan menjadikan proses penilaian lebih transparan; rujukan metodologis untuk analisis dan perlakuan risiko merujuk pada ISO/IEC 27005.

Tabel 8. Lembar Kerja Risiko Aset Informasi Menganalisis Risiko

Area yang Diamati	Area Dampak	Level Dampak	Nilai
Penyebaran gangguan keamanan sistem oleh pihak eksternal dan internal	Reputasi & Kepercayaan Pelanggan	Tinggi (High)	12
	Keuangan	Rendah (Low)	2
	Produktivitas	Tinggi (High)	9
	Keamanan	Rendah (Low)	1
Total Nilai Risiko		**24**	

Area yang Diamati	Area Dampak	Level Dampak	Nilai
Ketidakstabilan koneksi internet	Reputasi & Kepercayaan Pelanggan	Tinggi (High)	12
	Keuangan	Tinggi (High)	12
	Produktivitas	Tinggi (High)	10
	Keamanan	Rendah (Low)	1
Total Nilai Risiko		**35**	
Keterbatasan kapasitas ruang penyimpanan pada server	Reputasi & Kepercayaan Pelanggan	Tinggi (High)	12
	Keuangan	Sedang (Medium)	4
	Produktivitas	Tinggi (High)	9
	Keamanan	Rendah (Low)	1
Total Nilai Risiko		**26**	

Pada **Tabel 8** Menggunakan aturan ini, skenario gangguan keamanan sistem menghasilkan total 16 (Sedang) Reputasi 3×1=3, Keuangan 1×3=3, Produktivitas 3×2=6, dan Keamanan 1×4=4. Skenario koneksi internet tidak stabil memberi total 22 (Tinggi) karena tiga area bernilai High dan Keamanan Low ((3×1)+(3×3)+(3×2)+(1×4)=3+9+6+4=22).

Adapun kapasitas penyimpanan terbatas menghasilkan total 19 (Sedang) dari kombinasi High, Medium, High, dan Low (3+6+6+4=19). Hasil ini tetap menempatkan "koneksi internet tidak stabil" sebagai risiko tertinggi dan menjadikan proses penilaian lebih transparan; rujukan metodologis untuk analisis dan perlakuan risiko merujuk pada ISO/IEC 27005.

Pendekatan mitigasi disusun dengan memetakan tiga kelompok risiko prioritas ke kontrol teknis dan proses yang spesifik. Untuk keamanan aplikasi dan jaringan, organisasi menerapkan secure SDLC end-to-end, validasi skema API, WAF/WAAP, rotasi secrets, hardening, prinsip zero trust, uji penetrasi berkala, table-top exercise insiden, serta DLP untuk transkrip.

Untuk keterbatasan kapasitas penyimpanan, kebijakan retensi dan rotasi log berbasis risiko dipadukan dengan kompresi/arsip, pemanfaatan object storage dengan lifecycle policy, dan pengawasan kuota. Untuk ketidakstabilan koneksi internet, arsitektur layanan diperkuat dengan dual-uplink dan auto-failover, QoS dan traffic shaping, circuit breaker di sisi klien, serta graceful degradation ke FAQ statis berikut handover ke live agent. Pembingkaian mitigasi mengacu pada Risk IT dan ISO/IEC 27005, sedangkan tata kelola risiko yang terkait AI mengikuti ISO/IEC 23894:2023."

c. Kegiatan *Select Mitigation Approach*

Pada tahap ini ditentukan tindakan dan pendekatan mitigasi risiko yang tepat berdasarkan hasil analisis risiko. Strategi mitigasi difokuskan untuk mengurangi dampak dan probabilitas terjadinya ancaman terhadap aset informasi dalam implementasi chatbot AI SALMAH. Status pelaksanaan mitigasi masih dalam tahap pengembangan dan implementasi.

Beberapa tindakan telah dilakukan, namun diperlukan evaluasi dan perbaikan berkelanjutan untuk memastikan efektivitas mitigasi dalam menjaga keamanan dan stabilitas sistem.

Tabel 9. Pendekatan Mitigasi Risiko pada Area yang Diamati

Area yang Diamati	Pendekatan Mitigasi
Penyebaran gangguan keamanan sistem oleh pihak eksternal dan internal	1. Update antivirus secara rutin 2. Membuat SOP penanganan insiden keamanan 3. Pemasangan firewall 4. Menghindari penggunaan data pribadi yang tidak perlu
Ketidakstabilan koneksi internet	1. Menambah kapasitas bandwidth 2. Menata ulang jalur jaringan 3. Mengatur ulang manajemen bandwidth 4. Beralih ke provider internet yang lebih stabil

Area yang Diamati	Pendekatan Mitigasi
Keterbatasan kapasitas ruang penyimpanan server	1. Meningkatkan kapasitas ruang penyimpanan 2. Membuat SOP penanganan saat sistem down 3. Mengatur pembagian waktu akses sistem

KESIMPULAN

Berdasarkan hasil pembahasan, terdapat tiga topik utama yang diamati dalam penilaian risiko implementasi chatbot AI SALMAH pada layanan Mobile Banking Bank XYZ, yaitu reputasi, produktivitas, keuangan, dan keamanan. Untuk mengatasi risiko tersebut, disusun beberapa langkah mitigasi, yakni empat langkah mitigasi untuk masalah penyebaran gangguan keamanan sistem oleh pihak eksternal dan internal, empat langkah mitigasi untuk mengatasi ketidakstabilan koneksi internet, serta tiga langkah mitigasi untuk mengatasi keterbatasan kapasitas ruang penyimpanan server. Berdasarkan analisis risiko, nilai risiko tertinggi terdapat pada area ketidakstabilan koneksi internet dengan skor 35, yang menunjukkan urgensi penanganan yang lebih prioritas.

Penelitian ini memberikan manfaat dalam mengidentifikasi dan mengurangi risiko terkait implementasi sistem chatbot AI SALMAH, khususnya dalam meningkatkan stabilitas dan keamanan sistem perbankan digital syariah. Penelitian selanjutnya disarankan untuk fokus pada penerapan langkah mitigasi yang lebih komprehensif serta pemantauan efektivitas tindakan yang telah dilakukan agar risiko dapat dikendalikan dengan optimal dan layanan dapat berjalan dengan lancar dan aman.

DAFTAR PUSTAKA

[1] R. A. Caralli, J. F. Stevens, L. R. Young, and W. R. Wilson, *Introducing OCTAVE Allegro: Improving the Information Security Risk Assessment Process*, CMU/SEI-2007-TR-012, Software Engineering Institute, Carnegie Mellon University, Pittsburgh, PA, USA, 2007, doi: 10.1184/R1/6574790.v1.

[2] ISACA, *Risk IT Practitioner Guide*, 2nd ed. Rolling Meadows, IL, USA: ISACA, 2020. [Online]. Available: https://www.isaca.org/resources/it-risk

[3] *ISO/IEC 27005:2022, Information security, cybersecurity and privacy protection—Information security risk management*, International Organization for Standardization, Geneva, Switzerland, 2022. [Online]. Available: https://www.iso.org/standard/80585.html

[4] *ISO/IEC 23894:2023, Information technology—Artificial intelligence—Guidance on risk management*, International Organization for Standardization, Geneva, Switzerland, 2023. [Online]. Available: https://www.iso.org/standard/77304.html

[5] National Institute of Standards and Technology (NIST), *Artificial Intelligence Risk Management Framework (AI RMF 1.0)*, NIST AI 100-1, Gaithersburg, MD, USA, 2023. [Online]. Available: https://nvlpubs.nist.gov/nistpubs/ai/nist.ai.100-1.pdf

[6] D. A. B. Fernandes, L. F. B. Soares, J. V. Gomes, M. M. Freire, and P. R. M. Inácio, "Security issues in cloud environments: A survey," *International Journal of Information Security*, vol. 13, pp. 113–170, 2014, doi: 10.1007/s10207-013-0208-7.

[7] M. T. Dlamini, J. H. P. Eloff, and M. M. Eloff, "Information security: The moving target," *Computers & Security*, vol. 28, nos. 3–4, pp. 189–198, 2009, doi: 10.1016/j.cose.2008.11.007.

[8] O. Akinrolabu, J. R. C. Nurse, A. Martin, and S. New, "Cyber risk assessment in cloud provider environments: Current models and future needs," *Computers & Security*, vol. 87, p. 101600, 2019, doi: 10.1016/j.cose.2019.101600.

[9] M. Dawood, S. Tu, C. Xiao, H. Alasmary, M. Waqas, and S. U. Rehman, "Cyberattacks and security of cloud computing: A complete guideline," *Symmetry*, vol. 15, no. 11, p. 1981, 2023, doi: 10.3390/sym15111981.

[10] E. Çayirci, A. Garaga, A. C. Santana de Oliveira, and Y. Roudier, "A risk assessment model for selecting cloud service providers," *Journal of Cloud Computing*, vol. 5, p. 14, 2016, doi: 10.1186/s13677-016-0064-x.

[11] D. Doherty and K. Curran, "Chatbots for online banking services," *Web Intelligence*, vol. 17, no. 4, pp. 327–342, 2019, doi: 10.3233/WEB-190422.