

**TATA KELOLA KEAMANAN SIBER PADA UNIVERSITAS
MUHAMMADIYAH PALEMBANG MENGGUNAKAN
*NIST CYBERSECURITY FRAMEWORK***



SKRIPSI

**Untuk Memenuhi Persyaratan Mencapai Gelar Sarjana Komputer
(S.Kom) Pada Program Studi Teknologi Informasi Fakultas Teknik
Universitas Muhammadiyah Palembang**

Oleh:

M.AIDIL HUTAMAM AJI

162022072

**PROGRAM STUDI TEKNOLOGI INFORMASI
FAKULTAS TEKNIK
UNIVERSITAS MUHAMMADIYAH PALEMBANG
2026**

HALAMAN PENGESAHAN

TATA KELOLA KEAMANAN SIBER PADA UNIVERSITAS MUHAMMADIYAH PALEMBANG MENGGUNAKAN *NIST CYBERSECURITY FRAMEWORK*



Oleh :

M.Aidil Hutamam Aji
162022072

Menyetujui,

Pembimbing Utama

Dedi Haryanto, S.Kom., M.Kom
NBM/NIDN: 1337459/0201089001

Pembimbing Pendamping

Assoc. Prof. Dr. Ir. Zulhipni R S Elsi, S.T., M.Kom
NBM/NIDN: 1338529/0205118002

Disetujui,
Bekas Fakultas Teknik



Ir. A. Junaldi, M.T
NBM/NIDN: 763050/0202026502

Program Studi Teknologi Informasi
Ketua Program Studi



Dr. Kurnadi, S. Kom., M. Kom
NBM/NIDN: 1088893/0210038202

HALAMAN PERSETUJUAN

Judul Skripsi : Tata Kelola Keamanan Siber Pada Universitas Muhammadiyah
Palembang Menggunakan *NIST Cybersecurity Framework*

Oleh M.Aidil Hutamam Aji NIM 162022072 Skripsi ini telah disetujui dan
disahkan oleh Tim Penguji Program Studi Teknologi Informasi Konsentrasi
Manajemen Tata Kelola Program Strata 1 Universitas Muhammadiyah Palembang
pada 22 Agustus 2026 dan telah Dinyatakan Lulus

Palembang, 22 Agustus 2026

Mengetahui,



Ketua Program Studi Teknologi Informasi
Universitas Muhammadiyah Palembang

Dr. Karnadi, S. Kom., M. Kom
NBM/NIDN: 1088893/0210038202

Tim Penguji
Ketua Penguji

Dedi Haryanto, S.Kom., M.Kom
NBM/NIDN: 1337459/0201089001

Penguji 1,

Dr. Karnadi, S. Kom., M. Kom
NBM/NIDN: 1088893/0210038202

Penguji 2,

Apriansyah, S. Kom., M. Kom
NBM/NIDN: 1339399/0204049001

HALAMAN PERNYATAAN

Yang bertanda tangan dibawah ini:

Nama : M.Aidil Hutamam Aji

NIM : 162022072

Fakultas/Prodi : Teknik / Teknologi Informasi

Judul Skripsi : Tata Kelola Keamanan Siber Pada Universitas Muhammadiyah
Palembang Menggunakan *NIST Cybersecurity Framework*

Menyatakan dengan sebenar-benarnya bahwa skripsi ini adalah benar-benar hasil karya asli saya sendiri dan bukan merupakan plagiarisme, pencurian hasil karya milik orang lain, hasil kerja orang lain untuk kepentingan saya karena hubungan material maupun non-material, ataupun segala kemungkinan lain yang pada hakekatnya bukan merupakan karya tulis skripsi saya secara orisinil dan otentik.

Bila dikemudian hari diduga kuat ada ketidaksesuaian antara fakta dengan kenyataan ini, saya bersedia diproses oleh tim Fakultas yang dibentuk untuk melakukan verifikasi, dengan sanksi terberat berupa pembatalan kelulusan/kesarjanaan.

Demikian surat pernyataan ini saya buat dengan kesadaran sendiri dan tidak atas tekanan ataupun paksaan dari pihak manapun demi menegakan integritas akademik di institusi ini.

Hormat Saya,

M.Aidil Hutamam Aji
162022072

MOTTO DAN PERSEMBAHAN

MOTTO

“Pada akhirnya, ini semua hanyalah permulaan”

- Nadin Amizah

PERSEMBAHAN

Dengan penuh rasa syukur atas segala nikmat dan kekuatan yang diberikan serta dengan segala kerendahan hati, izinkan penulis untuk mempersembahkan skripsi ini kepada:

1. Teristimewa, penulis mengucapkan terima kasih yang sebesar-besarnya kepada kedua orang tua, Ayah dan Ibu tercinta, yang selalu menjadi sumber kekuatan, semangat, dan alasan terbesar penulis untuk terus berjuang serta tidak pernah menyerah dalam menghadapi setiap proses kehidupan maupun penyusunan skripsi ini. Sebagai anak pertama, penulis menyadari adanya harapan dan tanggung jawab besar dalam keluarga, namun Ayah dan Ibu tidak pernah menuntut apa pun selain melihat anaknya hidup bahagia, menjadi pribadi yang baik, serta bertanggung jawab atas apa yang telah dimulai. Terima kasih atas segala cinta, doa yang tidak pernah putus, perhatian, dukungan moral maupun materi, serta pengorbanan tulus yang mungkin tidak akan pernah mampu terbalaskan sepenuhnya oleh penulis. Setiap langkah, perjuangan, dan pencapaian hingga berada pada titik ini tidak terlepas dari doa, kerja keras, dan kepercayaan yang selalu diberikan oleh kedua orang tua. Skripsi ini menjadi wujud kecil dari harapan dan impian yang telah kalian titipkan sejak awal. Penulis juga berharap dapat terus menjadi pribadi yang lebih baik, bertanggung jawab dalam setiap langkah kehidupan, serta mampu membanggakan dan membahagiakan Ayah dan Ibu. Semoga Allah SWT senantiasa memberikan kesehatan, kebahagiaan, umur panjang, serta balasan terbaik atas segala kasih sayang, doa, dan pengorbanan yang telah diberikan.

2. Untuk Adik tersayang, yang senantiasa memberikan doa dan semangat dalam setiap langkah perjalanan penulis.
3. Dosen pembimbing penulis, Bapak Dedi Haryanto, S.Kom., M.Kom selaku dosen pembimbing utama dan Bapak Assoc. Prof. Dr. Ir. Zulhipni Reno Saputra Elsi, S.T., M.Kom selaku dosen pembimbing pendamping, yang selalu memberikan arahan, bimbingan, masukan, serta ilmu yang sangat berharga sehingga skripsi ini dapat diselesaikan dengan baik.
4. Teman-teman seperjuangan angkatan 2022 Teknologi Informasi, yang telah kebersamai dalam suka, duka, dan berbagai cerita selama di bangku perkuliahan.
5. Almamater tercinta Universitas Muhammadiyah Palembang, yang telah menjadi tempat penulis tumbuh, belajar, dan meraih pengalaman berharga hingga mencapai tahap penyelesaian studi ini.
6. Terakhir, untuk diri sendiri, **M.Aidil Hutamam Aji**, terima kasih telah bertahan dan berjuang sejauh ini. Terima kasih karena tetap kuat di tengah rasa lelah, tidak menyerah saat keadaan terasa sulit, dan terus melangkah melewati setiap proses yang tidak mudah. Menjadi anak pertama dengan berbagai tanggung jawab memang bukan hal yang ringan, walaupun sebenarnya tidak pernah ada tuntutan apa pun dari orang tua selain melihat anaknya hidup bahagia, menjadi pribadi yang baik, serta bertanggung jawab atas apa yang telah dimulai. Namun, hal itulah yang menjadi alasan terbesar untuk terus berusaha memberikan yang terbaik. Segala perjuangan, kesabaran, doa, dan usaha yang telah dilalui akhirnya membuahkan hasil hingga skripsi ini dapat terselesaikan. Tidak semua proses berjalan sesuai harapan, tetapi diri ini tetap memilih untuk bangkit, bertahan, dan menyelesaikan apa yang telah dimulai. Seperti yang tertulis pada moto penulis, “Pada akhirnya, ini semua hanyalah permulaan,” semoga pencapaian ini menjadi awal dari perjalanan dan perjuangan yang lebih besar di masa depan.

ABSTRAK

Penelitian ini bertujuan untuk mengkaji tata kelola keamanan siber di Universitas Muhammadiyah Palembang menggunakan *NIST Cybersecurity Framework* sebagai dasar analisis. Penelitian menggunakan metode deskriptif evaluatif dengan pendekatan kualitatif deskriptif melalui studi dokumentasi, observasi sistem, wawancara, dan studi literatur. Analisis dilakukan berdasarkan lima fungsi utama *NIST Cybersecurity Framework*, yaitu *Identify*, *Protect*, *Detect*, *Respond*, dan *Recover*. Hasil penelitian menunjukkan bahwa Universitas Muhammadiyah Palembang telah menerapkan berbagai mekanisme tata kelola keamanan siber dalam mendukung layanan akademik dan operasional. Pada fungsi *Identify*, telah dilakukan pengelolaan layanan teknologi informasi dan identifikasi risiko. Pada fungsi *Protect*, telah diterapkan mekanisme autentikasi, pengaturan hak akses, dan perlindungan sistem. Pada fungsi *Detect*, terdapat mekanisme *monitoring* untuk mendukung deteksi gangguan dan aktivitas mencurigakan. Pada fungsi *Respond*, telah terdapat mekanisme penanganan gangguan dan tindakan perbaikan, sedangkan pada fungsi *Recover* telah diterapkan mekanisme *backup* dan pemulihan sistem. Secara keseluruhan, penerapan tata kelola keamanan siber telah mencakup lima fungsi *NIST Cybersecurity Framework*. Namun, masih terdapat beberapa area yang dapat ditingkatkan, terutama dokumentasi keamanan, pengelolaan akses, *monitoring*, evaluasi insiden, edukasi keamanan siber, serta dokumentasi dan pengujian pemulihan sistem.

Kata Kunci : Tata Kelola Keamanan Siber, *NIST Cybersecurity Framework*, Keamanan Informasi, Sistem Informasi, Layanan Digital.

ABSTRACT

This study aims to examine cybersecurity governance at Universitas Muhammadiyah Palembang using the NIST Cybersecurity Framework as the basis for analysis. This study employs a descriptive-evaluative method with a descriptive qualitative approach through document review, system observation, interviews, and literature review. The analysis is based on the five core functions of the NIST Cybersecurity Framework: Identify, Protect, Detect, Respond, and Recover. The results indicate that Universitas Muhammadiyah Palembang has implemented various cybersecurity governance mechanisms to support its academic and operational services. In the Identify function, information technology services and risks have been identified and managed. In the Protect function, authentication mechanisms, access control, and system protection have been implemented. In the Detect function, monitoring mechanisms are used to support the detection of disruptions and suspicious activities. In the Respond function, mechanisms for handling disruptions and implementing corrective actions have been established, while in the Recover function, backup and system recovery mechanisms have been implemented. Overall, cybersecurity governance practices have covered the five functions of the NIST Cybersecurity Framework. However, several areas still require improvement, particularly security documentation, access management, system monitoring, incident evaluation, cybersecurity education, as well as the documentation and testing of system recovery mechanisms.

Keywords: *Cybersecurity Governance, NIST Cybersecurity Framework, Information Security, Information Systems, Digital Services.*

KATA PENGANTAR

Alhamdulillahirabbil'alamin, Puji Syukur penulis panjatkan kehadiran Allah SWT yang telah memberikan rahmat hidayah dan karunia- Nya kepada kita, sehingga penyusunan Skripsi ini insyallah dapat diselesaikan dengan baik dan tepat pada waktu yang telah ditentukan. Skripsi ini disusun untuk memenuhi syarat kelulusan mahasiswa Program Studi Teknologi Informasi Universitas Muhammadiyah Palembang.

Pada kesempatan ini penulis mengucapkan terima kasih kepada pihak pihak yang telah membantu dalam pelaksanaan dan penyusunan Skripsi diantaranya:

1. Bapak Prof. Dr. Abid Djazuli, S.E., M.M. selaku Rektor Universitas Muhammadiyah Palembang.
2. Bapak Ir. A. Junaidi, M.T. selaku Dekan Fakultas Teknik Universitas Muhammadiyah Palembang.
3. Bapak Dr. Karnadi, S.Kom., M.Kom. selaku Ketua Program Studi Teknologi Informasi sekaligus Dosen Pembimbing Akademik.
4. Bapak Dedi Haryanto, S.Kom., M.Kom. selaku Dosen Pembimbing Utama Skripsi.
5. Bapak Assoc. Prof. Dr. Ir. Zulhipni Reno Saputra Elsi, S.T., M.Kom. selaku Dosen Pembimbing Pendamping Skripsi.
6. Bapak / Ibu Dosen dan Staff Program Studi Teknologi Informasi.

Penulis menyadari keterbatasan kemampuan yang dimiliki, karena itu kritik dan saran yang membangun dari berbagai pihak sangat dibutuhkan untuk perbaikan dan kesempurnaan Skripsi ini.

Palembang, 30 April 2026



M.Aidil Hutamam Aji
162022072

DAFTAR ISI

HALAMAN JUDUL	i
HALAMAN PENGESAHAN	ii
HALAMAN PERSETUJUAN	iii
HALAMAN PERNYATAAN	iv
MOTTO DAN PERSEMBAHAN.....	v
ABSTRAK	vii
<i>ABSTRACT</i>	viii
KATA PENGANTAR.....	ix
DAFTAR ISI.....	x
DAFTAR GAMBAR.....	xiii
DAFTAR TABEL	xiv
BAB I PENDAHULUAN.....	1
1.1 Latar Belakang	1
1.2 Identifikasi Masalah	9
1.3 Rumusan Masalah	10
1.4 Batasan Penelitian	10
1.5 Tujuan Penelitian.....	11
1.6 Manfaat Penelitian.....	12
1.7 Sistematika Penulisan.....	12
BAB II TINJAUAN PUSTAKA.....	14
2.1 Tata Kelola Teknologi Informasi	14
2.2 Keamanan Informasi	15
2.3 Keamanan Siber (<i>Cybersecurity</i>)	16
2.4 Tata Kelola Keamanan Siber (<i>Cybersecurity Governance</i>).....	16
2.5 Sistem Informasi	17
2.6 Manajemen Risiko Keamanan Informasi	18
2.7 <i>National Institute of Standards and Technology (NIST)</i>	19
2.8 <i>NIST Cybersecurity Framework</i>	20
2.9 Fungsi <i>NIST Cybersecurity Framework</i>	23

2.9.1 <i>Identify</i>	24
2.9.2 <i>Protect</i>	24
2.9.3 <i>Detect</i>	25
2.9.4 <i>Respond</i>	26
2.9.5 <i>Recover</i>	26
2.10 <i>State Of The Art</i> dan Keterbaruan	28
2.10.1 Kebaruan (<i>Novelty</i>)	33
BAB III METODOLOGI PENELITIAN	35
3.1 Jenis Penelitian.....	35
3.2 Waktu dan Tempat Penelitian	37
3.2.1 Tempat Penelitian.....	37
3.2.2 Jadwal Penelitian.....	38
3.3 Kerangka Penelitian	41
3.4 Metode Pengumpulan Data	43
3.4.1 Studi Dokumentasi	44
3.4.2 Observasi Sistem	44
3.4.3 Wawancara	44
3.4.4 Studi Literatur	45
3.5 Metode Penelitian.....	45
3.6 Metode Analisis Data	48
3.6.1 Pengelompokan Data Berdasarkan <i>NIST CSF</i>	49
3.6.2 Analisis Berdasarkan <i>Framework Core</i>	49
3.6.3 Interpretasi Hasil Analisis	49
3.6.4 Identifikasi Area Peningkatan	50
3.7 Tahapan Penelitian	50
3.7.1 Identifikasi Masalah	50
3.7.2 Studi Literatur dan Pengumpulan Data	51
3.7.3 Analisis Menggunakan <i>NIST Cybersecurity Framework</i>	51
3.7.4 Interpretasi Hasil Analisis	51
3.7.5 Penyusunan Rekomendasi.....	52
BAB IV HASIL DAN PEMBAHASAN	53
4.1 Gambaran Umum Objek Penelitian	53

4.2 Hasil Analisis Berdasarkan <i>NIST Cybersecurity Framework</i>	57
4.2.1 <i>Identify</i> (Identifikasi)	57
4.2.2 <i>Protect</i> (Perlindungan)	64
4.2.3 <i>Detect</i> (Deteksi)	71
4.2.4 <i>Respond</i> (Respons)	75
4.2.5 <i>Recover</i> (Pemulihan)	78
4.3 Interpretasi Hasil Analisis	81
4.4 Identifikasi Area Peningkatan dan Rekomendasi	85
4.4.1 <i>Identify</i> (Identifikasi)	86
4.4.2 <i>Protect</i> (Perlindungan)	87
4.4.3 <i>Detect</i> (Deteksi)	88
4.4.4 <i>Respond</i> (Respons)	89
4.4.5 <i>Recover</i> (Pemulihan)	90
BAB V KESIMPULAN DAN SARAN	92
5.1 Kesimpulan	92
5.2 Saran	93
DAFTAR PUSTAKA	
LAMPIRAN	

DAFTAR GAMBAR

Gambar 2. 1 Fungsi Utama <i>NIST Cybersecurity Framework 2.0</i>	21
Gambar 2. 2 Struktur <i>Cybersecurity Framework Core</i>	22
Gambar 3. 1 Lokasi Penelitian	38
Gambar 3. 2 Kerangka Penelitian.....	42
Gambar 4. 1 Struktur Organisasi Biro Data dan Informasi UM-Palembang.....	56
Gambar 4. 2 Halaman <i>Login</i> Sistem Informasi Akademik (SIMAK).....	58
Gambar 4. 3 Halaman <i>Login E-Learning</i> UM-Palembang	58
Gambar 4. 4 Dokumentasi Identifikasi Risiko dan Rencana Aksi Sumber.....	59
Gambar 4. 5 Tampilan <i>Dashboard</i> Sistem Informasi Akademik (SIMAK)	65
Gambar 4. 6 Tampilan <i>Dashboard E-Learning</i> UM-Palembang	66
Gambar 4. 7 Dokumentasi Manual Prosedur Layanan Infrastruktur Jaringan	67

DAFTAR TABEL

Tabel 2. 1 <i>State of The Art</i>	28
Tabel 3. 1 Jadwal Penelitian.....	39
Tabel 3. 2 Metode Penelitian.....	47
Tabel 4. 1 Hasil Analisis Fungsi <i>Identify</i>	62
Tabel 4. 2 Hasil Analisis Fungsi <i>Protect</i>	69
Tabel 4. 3 Hasil Analisis Fungsi <i>Detect</i>	73
Tabel 4. 4 Hasil Analisis Fungsi <i>Respond</i>	76
Tabel 4. 5 Hasil Analisis Fungsi <i>Recover</i>	79

BAB I

PENDAHULUAN

1.1 Latar Belakang

Kemajuan teknologi informasi telah mengubah berbagai aspek kehidupan secara drastis, tak terkecuali institusi pendidikan tinggi yang kini makin mengandalkan platform digital untuk operasionalnya. Melalui teknologi ini, kegiatan akademik, pengelolaan tata usaha, pertukaran informasi, hingga manajemen data dapat berjalan dengan lebih tangkas dan optimal. Meski demikian, kemajuan ini turut memicu eskalasi risiko keamanan siber yang berpotensi menghambat kelancaran layanan di dalam organisasi tersebut. Berdasarkan laporan Badan Siber dan Sandi Negara (BSSN), sepanjang tahun 2023 terdeteksi ratusan juta anomali trafik siber di Indonesia yang didominasi oleh aktivitas *malware*, *trojan*, dan berbagai bentuk serangan lainnya [1]. Selain itu, pada tahun 2024 terjadi serangan *ransomware* terhadap Pusat Data Nasional Sementara (PDNS) yang menyebabkan terganggunya berbagai layanan publik di Indonesia [2]. Peristiwa tersebut menunjukkan bahwa ancaman keamanan siber dapat menyerang berbagai sektor dan menimbulkan dampak yang signifikan terhadap operasional organisasi. Serangan siber yang tidak ditangani dengan baik berpotensi menyebabkan kebocoran data, kerugian finansial, gangguan layanan, serta menurunnya kepercayaan pengguna. Oleh karena itu, keamanan siber menjadi salah satu aspek yang harus diperhatikan dalam pengelolaan teknologi informasi di setiap organisasi [3].

Sektor pendidikan tinggi sangat mengandalkan teknologi informasi untuk menunjang keberlangsungan operasionalnya, baik dalam aspek akademik maupun tata kelola administrasi. Berbagai layanan seperti sistem informasi akademik, pembelajaran daring, perpustakaan digital, sistem keuangan, dan layanan administrasi mahasiswa saat ini telah terintegrasi dengan teknologi digital. Selain itu, perguruan tinggi juga menyimpan berbagai aset informasi penting berupa data mahasiswa, dosen, tenaga kependidikan, hasil penelitian, serta dokumen institusi yang bersifat strategis dan rahasia. Banyaknya data yang dikelola menjadikan perguruan tinggi sebagai salah satu target potensial serangan siber [4]. Ancaman seperti *ransomware*, *phishing*, *malware*, pencurian data, penyalahgunaan akun, dan gangguan jaringan dapat menghambat proses akademik serta operasional institusi. Apabila keamanan siber tidak dikelola secara optimal, maka risiko kehilangan data dan gangguan layanan akan semakin meningkat. Oleh karena itu, perguruan tinggi memerlukan pengelolaan keamanan siber yang mampu melindungi seluruh aset informasi yang dimiliki. Dengan adanya tata kelola keamanan siber yang baik, keberlangsungan layanan digital dapat terjaga secara aman dan berkelanjutan [5].

Universitas Muhammadiyah Palembang merupakan salah satu perguruan tinggi yang telah memanfaatkan teknologi informasi dalam mendukung berbagai aktivitas akademik dan administrasi. Pemanfaatan teknologi tersebut diwujudkan melalui penggunaan Sistem Informasi Akademik (SIMAK), sistem penerimaan mahasiswa baru, website institusi, email resmi universitas, layanan administrasi daring, serta infrastruktur jaringan yang mendukung kegiatan civitas akademika. Selain itu, universitas juga mengelola berbagai aset informasi penting berupa data

mahasiswa, data dosen, data tenaga kependidikan, dokumen akademik, data keuangan, dan informasi institusi lainnya yang memiliki nilai strategis. Pemanfaatan teknologi informasi tersebut memberikan manfaat yang besar dalam meningkatkan efektivitas pelayanan dan pengelolaan informasi di lingkungan universitas. Namun, semakin banyaknya aset digital yang digunakan juga meningkatkan kompleksitas pengelolaan keamanan informasi yang harus dilakukan. Setiap aset teknologi informasi yang terhubung dengan jaringan memiliki potensi risiko berupa serangan siber, kebocoran data, penyalahgunaan akses, maupun gangguan layanan sistem. Risiko tersebut dapat memengaruhi keberlangsungan proses akademik dan administrasi apabila tidak dikelola secara baik. Oleh karena itu, keamanan siber menjadi aspek yang sangat penting dalam mendukung operasional Universitas Muhammadiyah Palembang.

Berdasarkan hasil observasi awal dan wawancara dengan pihak Pusat Teknologi Informasi Universitas Muhammadiyah Palembang, diketahui bahwa universitas telah memiliki berbagai layanan dan infrastruktur teknologi informasi yang digunakan untuk mendukung kegiatan organisasi. Meskipun demikian, hingga saat ini belum pernah dilakukan evaluasi atau pengukuran tingkat kesiapan keamanan siber menggunakan kerangka kerja standar internasional. Kondisi tersebut menyebabkan tingkat kesiapan keamanan siber universitas belum dapat diketahui secara objektif dan terukur. Selain itu, belum tersedia informasi yang menggambarkan sejauh mana pengelolaan identifikasi aset, perlindungan sistem, kemampuan deteksi ancaman, respons terhadap insiden keamanan, serta proses pemulihan layanan telah diterapkan secara optimal. Tidak adanya evaluasi yang

terstruktur juga dapat menyulitkan organisasi dalam mengidentifikasi kelemahan keamanan yang masih terdapat pada lingkungan teknologi informasi. Akibatnya, universitas berpotensi mengalami kesulitan dalam menentukan prioritas peningkatan keamanan yang diselaraskan dengan kebutuhan organisasi. Dengan demikian, evaluasi menyeluruh terhadap kondisi keamanan siber sangat diperlukan sebagai pijakan dalam merumuskan strategi peningkatan keamanan informasi.

Meningkatnya penggunaan teknologi informasi di lingkungan Universitas Muhammadiyah Palembang menuntut adanya pengelolaan keamanan siber yang efektif dan berkelanjutan. Namun, hingga saat ini tingkat kesiapan keamanan siber yang dimiliki universitas belum diketahui secara pasti karena belum pernah dilakukan pengukuran menggunakan *framework* keamanan siber yang terstandarisasi. Kondisi tersebut menyebabkan organisasi mengalami keterbatasan dalam mengidentifikasi tingkat kesiapan keamanan siber serta area yang memerlukan perbaikan. Selain itu, belum diketahui sejauh mana proses identifikasi aset dan risiko keamanan, perlindungan sistem dan data, deteksi ancaman, respons insiden, serta pemulihan layanan telah berjalan secara efektif. Apabila kondisi tersebut tidak dievaluasi secara berkala, maka potensi risiko terhadap aset informasi dan layanan digital dapat meningkat seiring berkembangnya ancaman keamanan siber. Kurangnya informasi mengenai kondisi keamanan siber juga dapat mempersulit organisasi dalam menyusun strategi pengelolaan risiko yang tepat. Oleh karena itu, diperlukan suatu pendekatan yang mampu memberikan gambaran kondisi keamanan siber secara sistematis, objektif, dan terukur [6]. Hasil evaluasi

tersebut diharapkan dapat menjadi dasar dalam meningkatkan keamanan informasi di lingkungan Universitas Muhammadiyah Palembang.

Salah satu kerangka kerja yang banyak digunakan dalam mengelola risiko keamanan siber adalah *NIST Cybersecurity Framework (NIST CSF)* yang dikembangkan oleh *National Institute of Standards and Technology*. *Framework* ini dirancang untuk membantu organisasi dalam memahami, mengelola, dan meningkatkan kemampuan keamanan siber secara sistematis. Pada versi terbaru yaitu *NIST Cybersecurity Framework 2.0* terdapat enam fungsi utama yang terdiri dari *Govern, Identify, Protect, Detect, Respond, dan Recover*. Namun, penelitian ini berfokus pada lima fungsi utama yaitu *Identify, Protect, Detect, Respond, dan Recover* karena kelima fungsi tersebut secara langsung berkaitan dengan pengelolaan keamanan siber operasional organisasi. Melalui fungsi-fungsi tersebut, organisasi dapat mengidentifikasi aset dan risiko keamanan, menerapkan perlindungan terhadap sistem dan data, mendeteksi ancaman yang muncul, merespons insiden keamanan, serta melakukan pemulihan layanan ketika terjadi gangguan. Kerangka kerja ini telah diadopsi secara luas berkat fleksibilitasnya, sehingga mampu diaplikasikan di bermacam jenis lembaga, tak terkecuali perguruan tinggi. Oleh karena itu, *NIST Cybersecurity Framework* dipilih sebagai metode evaluasi dalam penelitian ini [7].

Penelitian mengenai tata kelola keamanan siber menggunakan *NIST Cybersecurity Framework* telah banyak dilakukan pada berbagai organisasi, baik instansi pemerintah, perusahaan, maupun institusi pendidikan. Handoyo dan Nigrum melakukan penilaian risiko keamanan siber kampus menggunakan *NIST*

Cybersecurity Framework 1.1 dan menghasilkan rekomendasi peningkatan keamanan yang terstruktur [8]. Tan menerapkan *NIST Cybersecurity Framework* untuk manajemen risiko serangan siber dan menghasilkan rekomendasi kontrol keamanan yang sesuai dengan kebutuhan organisasi [9]. Nurochman menganalisis keamanan siber pada sistem informasi perpustakaan perguruan tinggi menggunakan *NIST Cybersecurity Framework* dan menemukan beberapa area yang memerlukan peningkatan keamanan [10]. Rofi'ah menunjukkan bahwa *NIST Cybersecurity Framework* dapat digunakan sebagai alat evaluasi keamanan siber yang efektif pada organisasi di Indonesia [11]. Sementara itu, Bernardo dkk. mengembangkan model penilaian kematangan keamanan siber yang selaras dengan *NIST Cybersecurity Framework* untuk mengukur tingkat kesiapan keamanan organisasi [12]. Hasil penelitian tersebut menunjukkan bahwa *NIST CSF* mampu membantu organisasi dalam mengidentifikasi kelemahan keamanan serta memberikan rekomendasi peningkatan yang sesuai dengan kebutuhan organisasi. Beberapa penelitian juga menunjukkan bahwa penerapan *NIST CSF* dapat meningkatkan efektivitas pengelolaan risiko keamanan siber dan mendukung proses pengambilan keputusan yang lebih baik. Selain itu, evaluasi menggunakan *framework* tersebut mampu memberikan gambaran mengenai tingkat kesiapan keamanan siber suatu organisasi secara sistematis dan terukur. Meskipun demikian, setiap organisasi memiliki karakteristik, kebutuhan, dan lingkungan teknologi yang berbeda sehingga hasil penelitian tidak dapat diterapkan secara langsung pada organisasi lainnya. Oleh karena itu, diperlukan penelitian yang disesuaikan dengan kondisi dan kebutuhan objek yang diteliti. Kajian terhadap studi-studi sebelumnya memegang peranan

krusial sebagai acuan dalam menetapkan pendekatan yang tepat untuk studi ini. Hal tersebut bertujuan untuk memastikan bahwa penelitian yang dilakukan berpijak pada fondasi teoretis maupun metodologis yang kokoh.

Berdasarkan hasil telaah terhadap berbagai penelitian terdahulu, sebagian besar penelitian keamanan siber menggunakan *NIST Cybersecurity Framework* dilakukan pada instansi pemerintah, perusahaan, dan beberapa perguruan tinggi di Indonesia. Fokus penelitian tersebut umumnya berada pada pengukuran tingkat kesiapan keamanan siber, analisis risiko, serta evaluasi keamanan informasi organisasi. Namun, hingga saat ini belum ditemukan penelitian yang secara khusus mengevaluasi keamanan siber di Universitas Muhammadiyah Palembang menggunakan *NIST Cybersecurity Framework*. Selain itu, sebagian penelitian terdahulu masih menggunakan *NIST CSF* versi 1.1 maupun *framework* lain seperti ISO 27001 dan COBIT sebagai dasar evaluasi keamanan informasi. Perbedaan objek penelitian dan *framework* yang digunakan menunjukkan adanya peluang penelitian yang masih dapat dikembangkan. Penelitian ini berupaya mengisi kesenjangan tersebut dengan melakukan evaluasi keamanan siber pada Universitas Muhammadiyah Palembang menggunakan *NIST Cybersecurity Framework*. Dengan demikian, penelitian ini memiliki kebaruan dari sisi objek penelitian dan penggunaan *framework* yang lebih mutakhir. Hasil penelitian diharapkan dapat memberikan kontribusi bagi pengembangan keamanan siber pada lingkungan perguruan tinggi.

Evaluasi keamanan siber menjadi penting untuk dilakukan karena dapat memberikan gambaran mengenai kondisi keamanan yang dimiliki organisasi saat

ini serta mengidentifikasi area yang masih memerlukan perbaikan. Hasil evaluasi tersebut dapat digunakan sebagai dasar dalam meningkatkan perlindungan aset informasi, memperkuat kemampuan deteksi ancaman, meningkatkan efektivitas respons insiden, dan mendukung proses pemulihan layanan ketika terjadi gangguan keamanan siber. Universitas Muhammadiyah Palembang sebagai institusi yang mengelola berbagai sistem dan data penting memerlukan informasi yang akurat mengenai kondisi keamanan siber yang dimiliki. Apabila tata kelola keamanan siber tidak dievaluasi secara berkala, maka potensi risiko seperti kebocoran data, gangguan layanan, dan penyalahgunaan akses dapat meningkat. Kondisi tersebut tidak hanya berdampak pada operasional universitas, tetapi juga dapat memengaruhi kepercayaan civitas akademika terhadap layanan yang diberikan. Oleh karena itu, penelitian ini penting dilakukan untuk memperoleh gambaran tingkat kesiapan keamanan siber universitas berdasarkan framework yang diakui secara internasional. Hasil penelitian diharapkan dapat dijadikan landasan dalam merumuskan strategi penguatan keamanan siber yang berdaya guna dan berkesinambungan. Oleh karena itu, universitas dapat meningkatkan kesiapan dalam menghadapi berbagai ancaman keamanan siber yang terus berkembang.

Berdasarkan perkembangan teknologi informasi yang diikuti oleh meningkatnya ancaman keamanan siber, perguruan tinggi dituntut untuk memiliki pengelolaan keamanan siber yang mampu melindungi aset informasi dan menjamin keberlangsungan layanan digital. Universitas Muhammadiyah Palembang sebagai institusi yang memanfaatkan berbagai sistem informasi dan infrastruktur teknologi juga menghadapi tantangan yang sama dalam mengelola risiko keamanan siber.

Hasil observasi awal menunjukkan bahwa hingga saat ini belum pernah dilakukan evaluasi tingkat kesiapan keamanan siber menggunakan kerangka kerja standar internasional sehingga kondisi keamanan siber universitas belum diketahui secara objektif dan terukur. Selain itu, hasil kajian penelitian terdahulu menunjukkan bahwa masih terdapat kesenjangan penelitian terkait penerapan *NIST Cybersecurity Framework* pada lingkungan Universitas Muhammadiyah Palembang. *NIST Cybersecurity Framework* dipilih karena menyediakan pendekatan yang sistematis dalam mengevaluasi aspek identifikasi, perlindungan, deteksi, respons, dan pemulihan keamanan siber. Melalui penerapan *framework* tersebut, kondisi keamanan siber universitas dapat diukur secara lebih terstruktur dan komprehensif. Penelitian ini diharapkan dapat memberikan rekomendasi yang mendukung penguatan keamanan informasi di lingkungan perguruan tinggi. Berdasarkan latar belakang tersebut, penelitian ini dilaksanakan dengan judul **“Tata Kelola Keamanan Siber pada Universitas Muhammadiyah Palembang Menggunakan *NIST Cybersecurity Framework*”**

1.2 Identifikasi Masalah

Berdasarkan pemaparan latar belakang tersebut, dapat diidentifikasi beberapa permasalahan sebagai berikut:

1. Belum terdapat kajian yang menggambarkan penerapan tata kelola keamanan siber di Universitas Muhammadiyah Palembang berdasarkan kerangka kerja *NIST Cybersecurity Framework*.

2. Informasi mengenai penerapan keamanan siber yang mencakup aspek identifikasi aset dan risiko, perlindungan sistem, deteksi ancaman, respons insiden, serta pemulihan layanan masih perlu dikaji secara terstruktur.
3. Pengelolaan keamanan siber di lingkungan Universitas Muhammadiyah Palembang perlu dianalisis untuk memperoleh gambaran kondisi penerapan keamanan siber berdasarkan fungsi-fungsi dalam *NIST Cybersecurity Framework*.
4. Belum terdapat gambaran yang terstruktur mengenai penerapan fungsi *Identify, Protect, Detect, Respond*, dan *Recover* dalam tata kelola keamanan siber di Universitas Muhammadiyah Palembang.

1.3 Rumusan Masalah

Berdasarkan uraian latar belakang dan identifikasi masalah yang telah dijelaskan, maka rumusan masalah dalam penelitian ini adalah Bagaimana penerapan tata kelola keamanan siber di Universitas Muhammadiyah Palembang berdasarkan fungsi *Identify, Protect, Detect, Respond*, dan *Recover* pada *NIST Cybersecurity Framework*?

1.4 Batasan Penelitian

Adapun batasan penelitian ini dirumuskan sebagai berikut:

1. Penelitian difokuskan pada tata kelola keamanan siber di lingkungan Universitas Muhammadiyah Palembang tanpa mengkaji secara mendalam pada satu sistem tertentu, melainkan pada pengelolaan keamanan siber secara umum di tingkat universitas.

2. Analisis dilakukan dengan mengacu pada *NIST Cybersecurity Framework* yang mencakup fungsi *Identify, Protect, Detect, Respond*, dan *Recover*, tanpa membahas fungsi *Govern*.
3. Data penelitian diperoleh melalui studi dokumentasi, observasi terhadap sistem informasi yang dapat diakses sesuai hak akses pengguna, serta wawancara dengan pihak yang berwenang dalam pengelolaan teknologi informasi di Universitas Muhammadiyah Palembang.
4. Penelitian menggunakan pendekatan deskriptif evaluatif dan tidak mencakup pengujian teknis keamanan sistem seperti *penetration testing, vulnerability assessment, digital forensic*, maupun pengembangan sistem.

1.5 Tujuan Penelitian

Tujuan dari penelitian ini dijabarkan sebagai berikut:

1. Mengkaji kondisi tata kelola keamanan siber di Universitas Muhammadiyah Palembang.
2. Menganalisis penerapan tata kelola keamanan siber berdasarkan fungsi *Identify, Protect, Detect, Respond*, dan *Recover* pada *NIST Cybersecurity Framework*.
3. Memberikan gambaran mengenai aspek-aspek keamanan siber yang telah diterapkan di Universitas Muhammadiyah Palembang berdasarkan *NIST Cybersecurity Framework*.
4. Menyusun rekomendasi yang dapat dijadikan bahan pertimbangan dalam upaya peningkatan tata kelola keamanan siber di Universitas Muhammadiyah Palembang.

1.6 Manfaat Penelitian

Hasil penelitian ini diharapkan memberikan kontribusi dan manfaat sebagai berikut:

1. Memberikan gambaran mengenai kondisi penerapan tata kelola keamanan siber di Universitas Muhammadiyah Palembang berdasarkan *NIST Cybersecurity Framework*.
2. Menambah pemahaman mengenai penerapan *NIST Cybersecurity Framework* dalam kajian tata kelola keamanan siber pada lingkungan perguruan tinggi.
3. Menjadi sumber informasi mengenai aspek-aspek keamanan siber yang telah diterapkan di Universitas Muhammadiyah Palembang.
4. Menjadi bahan pertimbangan bagi Universitas Muhammadiyah Palembang dalam upaya meningkatkan tata kelola keamanan siber dan keamanan informasi di lingkungan universitas.

1.7 Sistematika Penulisan

Sistematika penulisan ini disusun guna memberikan gambaran menyeluruh terkait pembahasan pada masing-masing bab. Adapun susunan penulisan dalam penelitian ini adalah sebagai berikut:

BAB I PENDAHULUAN

Bab ini mencakup latar belakang, identifikasi masalah, rumusan masalah, batasan masalah, tujuan dan manfaat penelitian, serta sistematika penulisan.

BAB II TINJAUAN PUSTAKA

Bab ini berisi teori-teori yang mendukung penelitian, meliputi konsep keamanan siber, tata kelola keamanan siber, *NIST Cybersecurity Framework*, serta penelitian terdahulu yang relevan sebagai landasan dalam pelaksanaan penelitian..

BAB III METODE PENELITIAN

Bab ini menguraikan metodologi yang diterapkan dalam studi ini, yang mencakup kerangka pemikiran, jenis dan pendekatan, lokasi serta waktu pelaksanaan, objek kajian, sumber data, hingga prosedur pengumpulan data, teknik pengumpulan data, instrumen penelitian, serta tahapan analisis berdasarkan fungsi *Identify*, *Protect*, *Detect*, *Respond*, dan *Recover* pada *NIST Cybersecurity Framework*.

BAB IV HASIL DAN PEMBAHASAN

Bab ini menyajikan hasil penelitian dan pembahasan mengenai penerapan tata kelola keamanan siber di Universitas Muhammadiyah Palembang berdasarkan *NIST Cybersecurity Framework*. Selain itu, bab ini juga membahas temuan-temuan yang diperoleh selama penelitian serta analisis terhadap kondisi keamanan siber yang diterapkan.

BAB V PENUTUP

Bab ini berisi kesimpulan yang diperoleh berdasarkan hasil penelitian serta saran yang dapat dijadikan sebagai bahan pertimbangan dalam upaya peningkatan tata kelola keamanan siber di Universitas Muhammadiyah Palembang.

DAFTAR PUSTAKA

- [1] Badan Siber dan Sandi Negara (BSSN), *Lanskap Keamanan Siber Indonesia 2023*. Jakarta, Indonesia: BSSN, 2024. [Online]. Available: <https://csirt.kemenkeu.go.id/in/post/lanskap-keamanan-siber-indonesia-2023>
- [2] Badan Siber dan Sandi Negara (BSSN), *Lanskap Keamanan Siber Indonesia 2024*. Jakarta, Indonesia: BSSN, 2025. [Online]. Available: <https://alika.pesisirbaratkab.go.id/files/272/E-BOOK/262/Lanskap-Keamanan-Siber-Indonesia-2024--BSSN.pdf>
- [3] R. von Solms and J. van Niekerk, "From Information Security to Cyber Security," *Computers & Security*, vol. 38, pp. 97–102, 2013, doi: 10.1016/j.cose.2013.04.004.
- [4] B. Sayres, "Secure Your College with *NIST* 's Cybersecurity Framework 2.0," CampusWorks, 2024. [Online]. Available: [https://www.campusworksinc.com/securing-your-college-or-university-NIST s-cybersecurity-framework-2-0/](https://www.campusworksinc.com/securing-your-college-or-university-NIST-s-cybersecurity-framework-2-0/)
- [5] R. M. Fazri, "Adoption of Cyber Security Maturity Framework for Data Protection in Higher Education," *Jurnal Media Computer Science*, vol. 5, no. 1, pp. 245–258, 2026.
- [6] J. L. Salas-Riega, Y. Riega-Virú, M. Ninaquispe-Soto, and J. M. Salas-Riega, "Cybersecurity and the *NIST* Framework: A Systematic Review of its Implementation and Effectiveness Against Cyber Threats," *International Journal of Advanced Computer Science and Applications (IJACSA)*, vol. 16, no. 6, pp. 723–735, 2025.
- [7] National Institute of Standards and Technology (*NIST*), *The NIST Cybersecurity Framework (CSF) 2.0*. Gaithersburg, MD, USA: *NIST*, Feb. 2024. doi: 10.6028/*NIST*.CSWP.29.
- [8] E. Handoyo and I. E. Nigrum, "Penilaian Risiko Keamanan Siber Kampus Menggunakan Framework Cybersecurity *NIST* 1.1," *Jurnal CoSciTech (Computer Science and Information Technology)*, vol. 4, no. 3, pp. 677–685, 2024.
- [9] T. Tan, "Manajemen Risiko Serangan Siber Menggunakan Framework *NIST* Cybersecurity," *JISAMAR (Journal of Information System, Applied, Management, Accounting and Research)*, vol. 6, no. 2, 2022.

- [10] A. Nurochman, "Analisis Keamanan Siber Sistem Informasi Perpustakaan di Perpustakaan Universitas Jenderal Soedirman Menggunakan *NIST* Cybersecurity Framework," *BACA: Jurnal Dokumentasi dan Informasi*, vol. 45, no. 2, 2024.
- [11] D. M. Rofi'ah, "*NIST* Cybersecurity Framework in the Lens of Indonesian Internal Auditors," *Indonesian Interdisciplinary Journal of Sharia Economics*, vol. 8, no. 1, 2025.
- [12] L. Bernardo, S. Malta, and J. Magalhães, "An Evaluation Framework for Cybersecurity Maturity Assessment Aligned with *NIST* Cybersecurity Framework," *Electronics*, vol. 14, no. 7, 2025.
- [13] ISACA, *COBIT 2019 Framework: Governance and Management Objectives*. Schaumburg, IL, USA: ISACA, 2018.
- [14] M. Ikhsan, A. P. Widodo, and K. Adi, "Systematic literature review on corporate information technology governance in Indonesia using COBIT 2019," *Prisma Sains: Jurnal Pengkajian Ilmu dan Pembelajaran Matematika dan IPA IKIP Mataram*, vol. 9, no. 2, pp. 354–364, 2021, doi: 10.33394/j-ps.v9i2.4370.
- [15] M. E. Whitman and H. J. Mattord, *Principles of Information Security*, 7th ed. Boston, MA, USA: Cengage Learning, 2021.
- [16] V. I. Sugara, H. Syahril, and M. Syafrullah, "Sistem pemeriksa keamanan informasi menggunakan National Institute of Standards and Technology (*NIST*) Cybersecurity Framework," *Komputasi: Jurnal Ilmiah Ilmu Komputer dan Matematika*, vol. 16, no. 1, pp. 203–212, 2019, doi: 10.33751/komputasi.v16i1.1591.
- [17] C. Pascoe, S. Quinn, and K. Scarfone, *The NIST Cybersecurity Framework (CSF) 2.0, NIST CSWP 29*. Gaithersburg, MD, USA: National Institute of Standards and Technology, 2024, doi: 10.6028/NIST.CSWP.29.
- [18] S. Y. Bela and A. Hafeez-Baig, "A conceptual model for cybersecurity governance," *Journal of Applied Security Research*, vol. 16, no. 4, pp. 490–513, 2021, doi: 10.1080/19361610.2021.1918995.
- [19] K. C. Laudon and J. P. Laudon, *Management Information Systems: Managing the Digital Firm*, 16th ed. Harlow, U.K.: Pearson, 2020.
- [20] N. Ramadhanty, "Implementasi Kerangka Keamanan *NIST* Dan ISO/IEC 27001 Dalam Menghadapi Ancaman Risiko Siber," *Journal of Indonesian Management*, vol. 4, no. 4, Nov. 2024, doi: 10.53697/jim.v4i4.1973.
- [21] E. Handoyo and Izza Eka Nigrum, "Penilaian risiko keamanan siber kampus menggunakan framework cybersecurity *NIST* 1.1," *Jurnal CoSciTech*

- (*Computer Science and Information Technology*), vol. 4, no. 3, pp. 677–685, Jan. 2024, doi: 10.37859/coscitech.v4i3.5628.
- [22] T. Tan and B. Soewito, "Manajemen Risiko Serangan Siber Menggunakan Framework *NIST* Cybersecurity", *JISAMAR*, vol. 6, no. 2, pp. 411–422, 2022.
 - [23] D. Amanda, N. Mutiah, and S. Rahmayudha, "Analisis Tingkat Kematangan Keamanan Informasi Menggunakan *NIST* Cybersecurity Framework dan CMMI [1]," 2022.
 - [24] A. Sigit Julianto, I. R. Hikmah, and R. N. Yasa, "Cyber-Risk Management Menggunakan *NIST* Cybersecurity Framework (CSF) dan COBIT 2019 pada Instansi XYZ," 2024.
 - [25] F. Ferdynandus, J. Natu Prihanto, and W. Winarno, "Implementing *NIST* Framework and the People, Process, Technology approach in Indonesian Financial Services," *International Journal of Engineering Continuity*, vol. 3, no. 1, pp. 172–182, Jul. 2024, doi: 10.58291/ijec.v3i1.265.
 - [26] B. Panjaitan, M. Hendayun, and A. I. Suryana, "Tata Kelola Pengamanan Informasi pada Sistem Hybrid Lending dengan *NIST* Cybersecurity Framework (Studi kasus: PT. Amarta Mikro Fintek)," 2021.
 - [27] J. L. Salas-Riega, Y. Riega-Virú, M. Ninaquispe-Soto, and J. M. Salas-Riega, "Cybersecurity and the *NIST* Framework: A Systematic Review of its Implementation and Effectiveness Against Cyber Threats," *International Journal of Advanced Computer Science and Applications*, vol. 16, no. 6, pp. 723–735, 2025, doi: 10.14569/IJACSA.2025.0160672.
 - [28] S. Balafif, "Penyesuaian Model Ketahanan Siber UMKM di Indonesia Dengan *NIST* Cybersecurity Framework," vol. 8, no. 3, 2023.