PENILAIAN RESIKO KEAMANAN SIBER KAMPUS MENGGUNAKAN *NATIONAL INSTITUTE OF STANDARD AND TECHNOLOGY* (NIST) *CYBERSECURITY FRAMEWORK* (CSF) 2.0 DI UNIVERSITAS MUHAMMADIYAH LAMONGAN

SKRIPSI
untuk memenuhi Sebagian persyaratan
mencapai derajat Sarjana S-1 Program Studi
Teknik Komputer

Di Susun Oleh :

IQBAL PRAMUDITO
2103010048

PROGRAM STUDI S1 TEKNIK KOMPUTER
FAKULTAS SAINS, TEKNOLOGI DAN PENDIDIKAN
UNIVERSITAS MUHAMMADIYAH LAMONGAN

2025

KATA PEGANTAR

Alhamdulillah puji syukur kepada Allah SWT. Yang telah memberikan kemudahan dalam menyelesaikan skripsi ini. Sholawat dan salam dilimpahkan kepada junjungan kita Nabi Muhammad SAW. Dan semoga kita semua menerima syafaatnya di hari akhir, Aamiin. Dalam setiap langkah saya berusaha semaksimal mungkin untuk mewujudkan harapan-harapan yang saya impikan sebagai ungkapan terima kasih, saya ingin mempersembahkan skripsi ini untuk :

1. Bapak Eko Handoyo, S.Kom., M.Kom selaku Dosen Pembimbing I dan Dekan Fakultas Sains, Teknologi dan Pendidikan Universitas Muhammadiyah Lamongan.
2. Bapak Mufti Ari Bianto, S.Kom., M.Kom selaku Ketua Program Studi Teknik Komputer Universitas Muhammadiyah Lamongan.
3. Bapak Muhammad Nurul Ihsan, S.T., M.Kom selaku Dosen Pembimbing II Skripsi yang telah memberikan pengarahan kepada penulis sampai di titik ini.
4. Orang Tua saya yaitu Ibu Supriyatin dan Bapak Bambang yang selalu memberikan dukungan materi, moral, dan doa yang tak putus untuk penulis. Terima kasih untuk semua pengorbanan, perhatian, dan kasih sayang yang diberikan selama ini.
5. Kepada kedua saudara kandung saya, Muhammad Zaul Haq dan Alfitra Salam meski mengambil keputusan untuk tidak menempuh pemdidikan kuliah tapi, engkau telah menjadi satu alasan penulis untuk memperjuangkan Skripsi ini hingga selesai, semoga apapun yang engkau pilih selalu diberi kemudahan dimasa depan.
6. Kepada teman-teman saya semuanya, teman seperjuangan saya, teman yang ada disaat penulis merasa susah, teman semester 8 teknik komputer yang selalu membersamai dalam perjuangan ini, semoga kita nanti bisa kembali bertemu dengan senyuman dan kebahagiaan di masa depan.
7. Kepada diri saya sendiri, terima kasih sudah menyempatkan untuk berjuangan dan menanam pundi-pundi harapan, walau tak mudah kau mampu melewatinya dengan kobaran api di dadamu, selamat kau pernah berjuang.

8. Kepada seseorang yang menurut penulis tak kalah penting kehadiranya, Dhea Nur Savira terima kasih banyak telah menjadi bagian dari perjalanan hidup penulis. Sudah menyempatkan untuk mendukung dan meyakinkan penulis sampai penulis dapat menyelesaikan tugas akhir ini, namamu abadi di Skripsi ini terima kasih.
9. Seluruh pihak yang telah membantu dalam pelaksanaan dan penyusunan Skripsi yang tidak dapat disebutkan satu persatu.

Peneliti menyadari sepenuhnya atas keterbatasan yang ada, kemampuan, pengetahuan, waktu, pengalaman, maupun literatur yang tersedia maka tentunya semua ini jauh dari sempurna, oleh karena itu penulis mengharapkan kritik dan saran yang bersifat membangun dari pembaca sebagai perbaikan dimasa yang akan datang.

DAFTAR ISI

Halaman

DAFTAR GAMBAR

DAFTAR TABEL

DAFTAR LAMPIRAN

Penilaian Resiko Keamanan Siber Kampus Menggunakan *National Institute Of Standart and Technology (NIST) Cybersecurity Framework (CSF)* 2.0 di Universitas Muhammadiyah Lamongan

ABSTRAK

Meningkatnya kompleksitas ancaman siber di institusi pendidikan tinggi terjadi seiring adopsi teknologi digital dalam berbagai sistem informasi kampus. Lingkungan kampus harus merespons kondisi ini dengan penerapan kerangka kerja seperti NIST CSF 2.0 yang dinilai efektif dalam mengidentifikasi, melindungi, mendeteksi, merespons, dan memulihkan insiden siber, tercermin dalam skor rata-rata subkategori penilaian sebesar 4,01 dari 5. Penerapan kebijakan dan prosedur keamanan siber sudah cukup dipahami serta dijalankan oleh pengguna utama layanan teknologi informasi, walaupun masih diperlukan peningkatan pemantauan risiko pada manajemen rantai pasokan serta pembaruan kebijakan secara berkala mengikuti perkembangan ancaman. Evaluasi vendor teknologi secara ketat dan pembaruan kebijakan keamanan berdasarkan hasil audit menjadi prioritas penting, di samping memastikan partisipasi aktif seluruh sivitas kampus dalam menjaga keamanan informasi. Langkah ini dapat meminimalkan dampak insiden siber, mendukung kepatuhan regulasi, serta meningkatkan kepercayaan pemangku kepentingan terhadap tata kelola keamanan informasi di lingkungan pendidikan tinggi. Dengan semakin majunya teknologi dan bertambahnya jumlah perangkat yang terhubung, potensi kerentanan terhadap serangan siber juga meningkat. Oleh karena itu, keberlanjutan penerapan kerangka kerja yang adaptif dan integratif sangat penting untuk menghadapi dinamika ancaman yang terus berubah. Selain itu, pelatihan dan kesadaran keamanan siber bagi seluruh civitas akademika perlu diperkuat agar dapat berperan aktif dalam menjaga keamanan data dan informasi secara menyeluruh.

Kata Kunci: Keamanan Siber Kampus, *NIST CSF* 2.0, Manajemen Risiko, Tata Kelola Teknologi.

Cybersecurity Risk Assessment of Campus Using the National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF) 2.0 at Universitas Muhammadiyah Lamongan

ABSTRACT

The increasing complexity of cyber threats in higher education institutions has emerged in tandem with the adoption of digital technologies across various campus information systems. The campus environment must respond to these developments by implementing frameworks such as NIST CSF 2.0, which has proven effective in identifying, protecting, detecting, responding to, and recovering from cyber incidents, as reflected in an average subcategory score of 4.01 out of 5. Cybersecurity policies and procedures are generally well-understood and implemented by primary users of information technology services, although there remains a need to enhance risk monitoring in supply chain management and update policies regularly in line with the evolving threat landscape. Rigorous assessment of technology vendors and periodic updates to security policies based on audit results have become critical priorities, alongside ensuring the active participation of all campus members in maintaining information security. These measures can minimize the impact of cyber incidents, support regulatory compliance, and bolster stakeholder trust in information security governance within higher education. As technology continues to advance and the number of connected devices increases, the potential vulnerabilities to cyberattacks also rise. Therefore, the sustained implementation of adaptive and integrative frameworks is essential to address the ever-changing dynamics of cyber threats. In addition, cybersecurity training and awareness for all academic community members must be strengthened to foster active roles in safeguarding data and information comprehensively.

Keyword: *Campus Cybersecurity, NIST CSF 2.0, Information Risk Management, Technology Governance.*