Perbandingan Keamanan Siber: Integrasi Strategi Proaktif untuk Meningkatkan Kesiapan Organisasi

1st Larasati
Departemen Sistem Informasi
Telkom University
Bandung, Indonesia
lrsati@student.telkomuniversity.ac.id

2nd Dhata Praditya
Departemen Sistem Informasi
Telkom University
Bandung, Indonesia
dhatap@telkomuniversity.ac.id

3rd Ari Fajar Santoso
Departemen Sistem Informasi
Telkom University
Bandung, Indonesia
arifajar@telkomuniversity.ac.id

Abstrak* — Keamanan siber menjadi tantangan utama di era digital, dengan ancaman yang terus berkembang seperti ransomware, serangan berbasis trojan, dan phishing. Berbagai framework seperti COBIT 2019, NIST Cybersecurity Framework (CSF), dan MITRE ATT&CK telah banyak diterapkan untuk membantu organisasi mengelola risiko dan melindungi aset digital mereka. Namun, setiap framework memiliki kekuatan dan kelemahan, sehingga integrasi elemen terbaik dari masing-masing framework menjadi penting untuk menciptakan kerangka kerja yang lebih efektif. Artikel ini membahas perbandingan dan integrasi framework-framework tersebut untuk membangun kerangka kerja keamanan siber yang proaktif dan holistik. Framework hasil integrasi ini mencakup empat aspek utama: Data Security, Application and Endpoint Security, Network and Perimeter Security, serta Human Layer. Integrasi ini memadukan tata kelola strategis dari COBIT 2019, modularitas dan fleksibilitas NIST CSF, serta pendekatan berbasis ancaman dari MITRE ATT&CK. Hasilnya adalah solusi komprehensif yang tidak hanya meningkatkan efisiensi manajemen risiko tetapi juga dapat disesuaikan dengan kebutuhan sektor pemerintahan, pendidikan, layanan keuangan, dan industri lainnya. Framework ini diharapkan mampu meningkatkan kesiapan keamanan siber organisasi secara signifikan, mengurangi kerentanan, memprioritaskan mitigasi risiko, serta merancang strategi perlindungan yang adaptif terhadap ancaman yang terus berkembang.

***Kata kunci*— Keamanan Siber, Framework Terintegrasi, Tingkat Kematangan, Framework Keamanan Siber**

I. PENDAHULUAN

Keamanan siber telah menjadi tantangan global yang mendesak, terutama dengan meningkatnya ketergantungan pada teknologi digital di berbagai sektor. Di Indonesia, ancaman keamanan siber terus meningkat, sebagaimana dilaporkan oleh [1], dengan lebih dari 403 juta serangan siber yang tercatat, termasuk insiden *ransomware* yang mengganggu layanan pemerintah. Serangan ini tidak hanya mengancam data dan infrastruktur, tetapi juga menimbulkan kerugian ekonomi yang signifikan.

Framework seperti COBIT 2019, NIST CSF, dan MITRE ATT&CK telah banyak digunakan untuk membantu organisasi mengelola risiko siber. Namun, setiap *framework* memiliki fokus dan pendekatan yang berbeda, sehingga organisasi sering menghadapi kesulitan dalam memilih *framework* yang paling sesuai dengan kebutuhan mereka. Oleh karena itu, diperlukan pendekatan integrasi yang menggabungkan kekuatan dari berbagai *framework* untuk menciptakan solusi yang lebih holistik dan adaptif.

II. KAJIAN TEORI

A. Keamanan Siber

Keamanan siber (*cybersecurity*) adalah disiplin ilmu yang berfokus pada perlindungan sistem informasi, jaringan, perangkat, dan data dari ancaman siber. Menurut [2] keamanan siber mencakup tindakan untuk mengidentifikasi, melindungi, mendeteksi, merespons, dan memulihkan sistem dari potensi ancaman. Dalam konteks organisasi, keamanan siber tidak hanya melibatkan aspek teknis tetapi juga tata kelola, budaya organisasi, dan kesiapan sumber daya manusia.

B. COBIT 2019

Control Objectives for Information and Related Technologies (COBIT 2019) adalah *framework* yang dirancang untuk tata kelola dan manajemen teknologi informasi (TI). *Framework* ini menyediakan panduan strategis bagi organisasi dalam mengelola risiko TI, termasuk keamanan siber. COBIT 2019 memiliki lima prinsip utama [3]:

1. Memenuhi kebutuhan pemangku kepentingan.
2. Mencakup keseluruhan organisasi.
3. Menerapkan kerangka kerja holistik.
4. Memperhitungkan tata kelola yang dinamis.
5. Mengintegrasikan tata kelola dan manajemen.
6. *Framework* ini sangat relevan untuk memastikan keamanan siber menjadi bagian dari tata kelola organisasi secara keseluruhan.

Framework ini sangat relevan untuk memastikan keamanan siber menjadi bagian dari tata kelola organisasi secara keseluruhan.

C. NIST *Cybersecurity Framework*

NIST *Cybersecurity Framework* (CSF) adalah kerangka kerja modular yang dirancang untuk membantu organisasi mengelola risiko keamanan siber secara fleksibel. *Framework* ini terdiri dari lima fungsi utama [2]:

1. *Identify*: Mengidentifikasi aset, sistem, dan risiko yang memerlukan perlindungan.
2. *Protect*: Mengimplementasikan langkah-langkah untuk melindungi sistem.
3. *Detect*: Mendeteksi ancaman secara cepat.
4. *Respond*: Merespons insiden dengan prosedur yang telah dirancang.
5. *Recover*: Memulihkan operasional setelah insiden.

Framework ini menekankan pentingnya pendekatan siklus hidup dalam pengelolaan keamanan siber.

D. *Center for Internet Security*

Center for Internet Security (CIS) *Controls*, sebelumnya dikenal sebagai CIS *Critical Security Controls*, adalah rangkaian panduan praktis yang dirancang untuk membantu organisasi meningkatkan keamanan sibernya. *Framework* ini berfokus pada pengelolaan dan mitigasi ancaman siber yang paling umum melalui serangkaian kontrol yang diprioritaskan. CIS *Controls* terdiri dari 18 kontrol utama yang terbagi menjadi tiga kategori berdasarkan tingkat prioritas dan implementasi: *Basic*, *Foundational*, dan *Organizational* [4].

E. ISO 27001

ISO 27001 adalah standar internasional untuk sistem manajemen keamanan informasi (*Information Security Management System/ISMS*). Standar ini memberikan panduan sistematis untuk melindungi informasi sensitif dari ancaman internal maupun eksternal melalui pendekatan berbasis risiko. ISO 27001 mencakup beberapa elemen kunci, termasuk [5]:

1. Konteks Organisasi: Memahami kebutuhan dan ekspektasi pemangku kepentingan.
2. Kepemimpinan: Komitmen manajemen untuk menerapkan ISMS secara efektif.
3. Perencanaan: Identifikasi risiko keamanan informasi dan langkah mitigasinya.
4. Dukungan: Pengelolaan sumber daya, pelatihan, dan kesadaran keamanan.
5. Operasi: Pelaksanaan langkah-langkah keamanan yang terencana.
6. Evaluasi Kinerja: *Monitoring* dan pengukuran efektivitas ISMS.
7. Peningkatan Berkelanjutan: Memperbaiki ISMS berdasarkan temuan audit atau insiden.

ISO 27001 menekankan pentingnya pendekatan berkelanjutan untuk melindungi kerahasiaan, integritas, dan ketersediaan informasi. Standar ini juga kompatibel dengan berbagai *framework* lain seperti COBIT dan NIST, sehingga dapat diintegrasikan untuk menciptakan sistem keamanan informasi yang lebih komprehensif.

III. METODE

A. Pendekatan *Design Science Research* (DSR)

Design Science Research (DSR) adalah pendekatan penelitian yang berorientasi pada pengembangan solusi praktis untuk menyelesaikan masalah yang kompleks melalui pembuatan dan evaluasi artefak. Artefak dalam konteks ini dapat berupa model, *framework*, algoritma, atau sistem yang dirancang untuk memberikan kontribusi teoritis dan praktis [6].

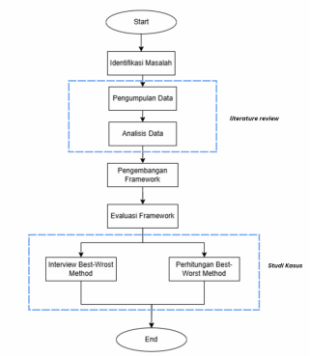
Pendekatan *Design Science Research* (DSR) digunakan dalam penelitian ini untuk mengembangkan dan mengevaluasi artefak berupa *framework* keamanan siber terintegrasi. Proses DSR terdiri dari tiga elemen utama:

1. *Environment* (Lingkungan)
   Memahami kebutuhan bisnis berdasarkan konteks organisasi yang beragam dan teknologi yang relevan, seperti 7 *Layers of Cybersecurity*. Lingkungan didefinisikan sebagai ruang masalah yang terdapat fenomena didalamnya.
2. *IS Research* (Penelitian Sistem Informasi)
   a. *Build*: Mengintegrasikan *Framework* keamanan siber, seperti COBIT 2019, NIST CSF, ISO 27001, dan CIS *Controls*, untuk menghasilkan kerangka kerja yang holistik dan adaptif.
   b. *Evaluate*: *Framework* diuji melalui wawancara, *desk research*, dan studi kasus untuk memastikan efektivitas, kelengkapan, dan kesesuaiannya dengan kebutuhan organisasi.
3. *Knowledge Base* (Dasar Pengetahuan)
   Landasan teori, seperti manajemen keamanan informasi dan keamanan siber, serta metodologi seperti *case study*, *literature review*, dan *Best Worst Method*, digunakan untuk memastikan bahwa *framework* memenuhi standar ilmiah (*rigor*) dan relevansi (*relevance*).

Proses iteratif ini menghasilkan *framework* yang tidak hanya relevan untuk aplikasi praktis, tetapi juga memberikan kontribusi teoretis pada bidang keamanan siber.

B. Sistematika Penelitian

Penelitian ini dilakukan secara sistematis dengan tahapan pada Gambar 1.



Gambar 1 Sistematika Penelitian

1. Identifikasi Masalah
   Penelitian dimulai dengan mengidentifikasi masalah utama dalam keamanan siber, yaitu kurangnya integrasi *framework* yang komprehensif untuk meningkatkan kesiapan keamanan organisasi. Masalah ini didasarkan pada kebutuhan organisasi untuk menghadapi ancaman siber yang terus berkembang.
2. Pengumpulan Data
   Tahap ini melibatkan pengumpulan data melalui kajian literatur (*literature review*), yang mencakup *framework* keamanan siber seperti COBIT 2019, NIST CSF, CIS *Controls*, dan ISO 27001. Data tambahan diperoleh melalui wawancara dengan praktisi keamanan siber.
3. Analisis Data
   Data yang dikumpulkan dianalisis untuk mengidentifikasi parameter kunci dari masing-masing *framework*. Analisis ini bertujuan untuk memahami kekuatan, kelemahan, dan relevansi *framework* dalam konteks organisasi.
4. Pengembangan *Framework*
   Framework keamanan siber terintegrasi dirancang berdasarkan hasil analisis data. *Framework* ini menggabungkan elemen terbaik dari *framework* yang dipelajari untuk menciptakan solusi yang lebih holistik dan relevan.

IV. HASIL DAN PEMBAHASAN

A. Hasil Penelitian

Penelitian ini menghasilkan sebuah *framework* keamanan siber terintegrasi yang dirancang berdasarkan pemetaan elemen-elemen utama dari COBIT 2019, NIST CSF, CIS *Controls*, dan ISO 27001. *Framework* ini bertujuan untuk meningkatkan kesiapan keamanan siber organisasi melalui pendekatan holistik yang mencakup empat aspek utama: *Data Security*, *Application and Endpoint Security*, *Network and Perimeter Security*, serta *Human Layer*. Pemetaan Parameter *framework* menunjukkan sejauh mana kontribusi setiap *framework* terhadap berbagai parameter keamanan siber. Hasil pemetaan disajikan dalam Tabel 1 berikut:

Tabel 1 Pemetaan Parameter Keamanan Siber

Parameter Keamanan	COBIT 2019	NIST CSF	CIS *Controls*	ISO 27001
Enkripsi Data	✓	✓	✓	✓
Manajemen Akses	✓	✓	✓	✓
Pemantauan *Endpoint*	✓	✓	✓	✗
Segmentasi Jaringan	✓	✓	✓	✓
Pelatihan Keamanan	✓	✓	✓	✓
Deteksi Ancaman	✗	✓	✓	✗
Respon Insiden	✓	✓	✗	✓
Kebijakan Tata Kelola	✓	✗	✗	✓

B. Analisis dan Interpretasi

Hasil analisis menunjukkan bahwa setiap *framework* memiliki fokus dan kekuatan yang saling melengkapi:

1. COBIT 2019 berfokus pada tata kelola strategis yang mencakup kebijakan, prosedur, dan pengelolaan risiko di tingkat manajemen.
2. NIST CSF memiliki pendekatan modular berbasis siklus hidup keamanan, yang sangat mendukung implementasi teknis dan respons insiden.
3. CIS *Controls* menekankan kontrol prioritas untuk mitigasi ancaman umum, seperti deteksi *malware*, autentikasi multifaktor, dan keamanan *endpoint*.
4. ISO 27001 menyediakan panduan berbasis risiko untuk pengelolaan keamanan informasi secara menyeluruh, termasuk kebijakan tata kelola dan pelatihan keamanan.

Dari hasil pemetaan, dapat disimpulkan bahwa integrasi elemen-elemen terbaik dari keempat *framework* ini dapat menghasilkan kerangka kerja keamanan siber yang lebih holistik dan relevan untuk berbagai sektor industri.

V. KESIMPULAN

Penelitian ini berhasil mengidentifikasi dan memetakan kontribusi dari empat *framework* utama dalam keamanan siber, yaitu COBIT 2019, NIST *Cybersecurity Framework* (CSF), CIS *Controls*, dan ISO 27001, terhadap delapan parameter utama keamanan siber. Hasil penelitian menunjukkan bahwa masing-masing *framework* memiliki keunggulan yang unik dan saling melengkapi. COBIT 2019 unggul dalam aspek kebijakan tata kelola dan manajemen risiko di tingkat strategis, memberikan panduan untuk mengembangkan budaya keamanan yang terstruktur. NIST CSF menonjol pada aspek teknis, seperti deteksi ancaman, pemantauan *endpoint*, dan respons insiden, yang dirancang untuk fleksibilitas dalam implementasi. Sementara itu, CIS *Controls* berfokus pada kontrol teknis praktis, seperti segmentasi jaringan dan pengamanan *endpoint*, yang mudah diterapkan oleh organisasi. ISO 27001, di sisi lain, menawarkan pendekatan berbasis risiko yang komprehensif, dengan kekuatan dalam kebijakan tata kelola, pelatihan keamanan, dan pengelolaan informasi sensitif.

Integrasi elemen terbaik dari keempat *framework* ini menghasilkan kerangka kerja keamanan siber yang holistik, mencakup aspek strategis dan teknis. Kerangka kerja ini relevan untuk diterapkan di berbagai sektor industri, seperti

pemerintahan, pendidikan, dan layanan keuangan, guna meningkatkan kesiapan organisasi dalam menghadapi ancaman siber yang terus berkembang. Penelitian ini juga memberikan kontribusi teoretis dengan mengidentifikasi parameter kunci keamanan siber dan kontribusi *framework* terhadap parameter tersebut, serta kontribusi praktis berupa panduan integrasi *framework* yang dapat disesuaikan dengan kebutuhan spesifik organisasi. Dengan menggabungkan pendekatan strategis dan teknis, kerangka kerja yang diusulkan diharapkan dapat membantu organisasi dalam mengelola ancaman siber secara lebih efektif dan berkelanjutan.

Selain itu, penelitian ini membuka peluang untuk pengembangan lebih lanjut, seperti pengujian *framework* pada skala yang lebih luas di berbagai sektor, integrasi teknologi mutakhir seperti *Artificial Intelligence* (AI) dan *Machine Learning* (ML) untuk mendukung otomatisasi deteksi ancaman, serta pengembangan metode evaluasi kuantitatif untuk mengukur efektivitas *framework* secara lebih objektif. Dengan demikian, kerangka kerja ini diharapkan dapat menjadi fondasi yang kokoh untuk pengelolaan keamanan siber yang adaptif, relevan, dan inovatif**.**

REFERENSI

[1] Badan Siber dan Sandi Negara Republik Indonesia, "LANSKAP KEAMANAN SIBER INDONESIA," 2023.

[2] NIST, "The NIST Cybersecurity Framework (CSF) 2.0," Feb 2024. doi: 10.6028/NIST.CSWP.29.

[3] Information Systems Audit and Control Association., *COBIT 2019 Framework Governance and Management Objectives*.

[4] CIS Control, "CIS Critical Security Controls®," 2024. [Daring]. Tersedia pada: http://www.cisecurity.org/controls/

[5] International Standard, "ISOIEC 270022022 Information security, cybersecurity and privacy protection — Information security co".

[6] D. Arnott dan G. Pervan, "Design science in decision support systems research: An assessment using the hevner, march, park, and ram guidelines," *J Assoc Inf Syst*, vol. 13, no. 11, hlm. 923–949, 2012, doi: 10.17705/1jais.00315.