**PERBANDINGAN FRAMEWORK COBIT 2019 DENGAN NIST *CYBERSECURITY FRAMEWORK* (CSF) DAN ISO/IEC 27001 DALAM TATA KELOLA DAN KEAMANAN INFORMASI**

**TUGAS UJIAN TENGAN SEMESTER (UTS)**

**MATA KULIAH AUDIT DAN TATA KELOLA IT**

****

**Disusun Oleh Kelompok IV:**

**Asep Ridwan Hidayat (231012050036)**

**Ilyas Wichaksono (231012050048)**

**Imam Satria Hanggara (231012050019)**

**Riski Sudarsono (231012050025)**

**PROGRAM STUDI TEKNIK INFORMATIKA S-2**

**PROGRAM PASCA SARJANA**

**UNIVERSITA PAMULANG**

**TANGERANG SELATAN**

**2024**

ABSTRAK

Dalam era digital saat ini, kebutuhan akan tata kelola dan manajemen keamanan informasi yang efektif semakin mendesak. Framework COBIT 2019 dan NIST *Cybersecurity Framework* (CSF) menjadi dua pendekatan yang banyak digunakan oleh organisasi dalam mencapai tujuan ini. COBIT 2019 adalah kerangka kerja tata kelola TI yang dirancang untuk membantu organisasi mencapai tujuan tata kelola perusahaan yang sejalan dengan strategi dan tujuan bisnis mereka. Sementara itu, NIST *Cybersecurity Framework* (CSF) adalah kerangka kerja keamanan yang berfokus pada manajemen risiko keamanan siber dan perlindungan informasi. Meskipun keduanya memiliki tujuan yang berbeda, terdapat kesamaan dalam beberapa aspek penting, seperti pengelolaan risiko, manajemen kepatuhan, dan perlindungan data.

Makalah ini bertujuan untuk membandingkan poin-poin yang sama dalam COBIT 2019 dengan NIST *Cybersecurity Framework* (CSF) dan ISO/IEC 27001, dengan fokus pada aspek-aspek utama yang berhubungan dengan tata kelola risiko, kontrol keamanan informasi, dan kepatuhan terhadap regulasi. sementara ISO/IEC 27001 didedikasikan untuk membangun Sistem Manajemen Keamanan Informasi (ISMS) yang terstruktur. Analisis dilakukan dengan mengeksplorasi struktur dan pendekatan masing-masing framework dalam hal identifikasi dan mitigasi risiko, pengelolaan keamanan teknis, dan peranannya dalam peningkatan kesadaran keamanan di tingkat pengguna. Hasil dari perbandingan ini menunjukkan bahwa meskipun COBIT 2019 lebih berfokus pada tata kelola TI secara menyeluruh, dan NIST *Cybersecurity Framework* (CSF) lebih pada keamanan siber, keduanya memiliki kesamaan dalam penerapan proses manajemen risiko yang efektif serta perlindungan informasi yang terpadu.

Dengan memahami perbandingan ini, organisasi dapat mengoptimalkan tata kelola dan keamanan informasi mereka dengan memilih framework yang paling sesuai dengan kebutuhan mereka atau bahkan mengintegrasikan elemen-elemen dari kedua kerangka kerja tersebut. Langkah ini membantu organisasi untuk mencapai tata kelola TI yang menyeluruh dan memperkuat keamanan informasi di berbagai aspek operasional.

Kata Kunci: COBIT 2019, NIST CSF, ISO/IEC 27001, keamanan informasi, manajemen risiko, Cyber Security

**DAFTAR ISI**

[Daftar Tabel 5](#_Toc181111761)

[Daftar Gambar 6](#_Toc181111762)

[BAB I 7](#_Toc181111763)

[PENDAHULUAN 7](#_Toc181111764)

[1.1 Pendahuluan 7](#_Toc181111765)

[1.2 Rumusan Masalah 8](#_Toc181111766)

[1.3 Tujuan Pengkajian 8](#_Toc181111767)

[1.4 Manfaat Pengakajian 9](#_Toc181111768)

[1.5 Ruang Lingkup Pengkajian 11](#_Toc181111769)

[BAB II 14](#_Toc181111770)

[TINJAUAN PUSTAKA 14](#_Toc181111771)

[2.1 Framework COBIT 2019 14](#_Toc181111772)

[2.2 Framework NIST Cybersecurity Framework (CSF) 15](#_Toc181111773)

[2.2.1 Definisi dan Tujuan NIST CSF 16](#_Toc181111774)

[BAB III 17](#_Toc181111775)

[METODE PENELITIAN 17](#_Toc181111776)

[3.1 Pendekatan Penelitian 17](#_Toc181111777)

[3.2 Pengumpulan Data 17](#_Toc181111778)

[3.3 Teknik Analisis Data 17](#_Toc181111779)

[BAB IV 19](#_Toc181111780)

[HASIL PENGKAJIAN DAN PEMBAHASAN 19](#_Toc181111781)

[4.1 Relevansi *framework* COBIT 2019 dan NIST *Cybersecurity Framework* (NIST CSF). 19](#_Toc181111782)

[4.1.1 Pengelolaan Risiko (Risk Management) 19](#_Toc181111783)

[4.1.2 Pengelolaan Sumber Daya TI (IT Resource Management) 20](#_Toc181111784)

[4.1.3 Keselarasan dengan Tujuan Bisnis (Business Alignment) 20](#_Toc181111785)

[4.2 Perbedaan *framework* COBIT 2019 dan NIST *Cybersecurity Framework* (NIST CSF) 24](#_Toc181111786)

[BAB V 27](#_Toc181111787)

[KESIMPULAN 27](#_Toc181111788)

[Persamaan 28](#_Toc181111789)

[Perbedaan 28](#_Toc181111790)

[DAFTAR PUSTAKA 29](#_Toc181111791)

# DAFTAR TABEL

[**Tabel 1. 1 Relevansi Cobit 2019 dan NIST CSF** 21](#_Toc181111690)

[**Tabel 1. 2 Relevansi Domain Cobit 2019 dengan Kontrol NIST CST** 23](#_Toc181111691)

[**Tabel 1. 3 framework COBIT 2019 dan NIST Cybersecurity Framework (NIST CSF)** 24](#_Toc181111692)

# Daftar Gambar

[**Gambar 1. 1 Core Components** 24](#_Toc181111576)

# BAB I

# PENDAHULUAN

## Pendahuluan

Seiring dengan meningkatnya ketergantungan organisasi terhadap teknologi informasi (TI), kebutuhan untuk memastikan tata kelola dan keamanan informasi yang efektif menjadi semakin penting. Teknologi informasi memainkan peran vital dalam mendukung operasional, pengambilan keputusan, serta pencapaian tujuan strategis bisnis. Oleh karena itu, manajemen risiko dan pengamanan informasi menjadi aspek krusial untuk menjaga integritas, kerahasiaan, dan ketersediaan data. Di tengah dinamika ancaman siber yang semakin kompleks, framework tata kelola TI dan keamanan informasi seperti COBIT 2019 dan NIST CSF menjadi pedoman yang banyak digunakan oleh organisasi untuk mencapai standar keamanan yang diharapkan serta menjaga kepatuhan terhadap regulasi industri yang berlaku (ISACA, 2019).

COBIT 2019, yang dikembangkan oleh ISACA, adalah salah satu framework utama yang dirancang untuk mendukung tata kelola TI secara komprehensif. Framework ini menyediakan panduan bagi organisasi dalam mengatur, mengelola, dan memantau seluruh aspek TI yang relevan dengan tujuan bisnis mereka. Di sisi lain, NIST *Cybersecurity Framework* (CSF), yang dipublikasikan oleh National Institute of Standards and Technology (NIST), lebih berfokus pada aspek keamanan siber dengan pendekatan yang berbasis manajemen risiko. NIST *Cybersecurity Framework* (CSF) dirancang untuk membantu organisasi meningkatkan kemampuan mereka dalam mencegah, mendeteksi, dan merespons ancaman keamanan siber yang semakin berkembang (NIST, 2020).

Sedangkan kerangka kerja ISO/IEC 27001 adalah standar yang diakui secara global untuk manajemen keamanan informasi. Diterbitkan oleh International Organization for Standardization (ISO) dan International Electrotechnical Commission (IEC), standar ini memberikan pendekatan sistematis untuk mengelola informasi sensitif, memastikan kerahasiaan, integritas, dan ketersediaan. ISO/IEC 27001 merupakan bagian dari keluarga standar ISO/IEC 27000, yang dirancang untuk membantu organisasi dalam membangun, mengimplementasikan, memelihara, dan terus meningkatkan Sistem Manajemen Keamanan Informasi (ISMS).

ISO/IEC 27000 adalah serangkaian standar internasional yang dirancang untuk membantu organisasi dalam mengelola keamanan informasi. Standar ini memberikan panduan sistematis untuk membangun, mengimplementasikan, memelihara, dan terus meningkatkan Sistem Manajemen Keamanan Informasi (ISMS). Dengan meningkatnya ketergantungan organisasi terhadap teknologi informasi dan ancaman yang semakin kompleks, penerapan ISO/IEC 27000 menjadi sangat relevan untuk memastikan bahwa informasi sensitif dikelola dengan baik dan dilindungi dari berbagai risiko.

ISO/IEC 27000 pertama kali diterbitkan pada tahun 2005, dan sejak itu telah mengalami beberapa revisi untuk menyesuaikan dengan perkembangan teknologi dan kebutuhan industri. Keluarga standar ini mencakup berbagai aspek manajemen keamanan informasi, mulai dari kebijakan keamanan hingga kontrol teknis yang harus diterapkan oleh organisasi. Dengan lebih dari 30 standar dalam keluarga ini, ISO/IEC 27000 memberikan kerangka kerja yang komprehensif untuk melindungi data dan informasi organisasi.

ISO/IEC 27001 adalah standar utama dalam keluarga ini yang menetapkan persyaratan untuk mendirikan ISMS. Standar ini mencakup penilaian risiko, pengendalian keamanan, serta penetapan kebijakan dan prosedur yang diperlukan untuk menjaga kerahasiaan, integritas, dan ketersediaan informasi. Selain itu, ISO/IEC 27002 menyediakan panduan praktis tentang kontrol keamanan informasi yang dapat diterapkan oleh organisasi.

Penerapan standar ISO/IEC 27000 memberikan berbagai manfaat bagi organisasi, antara lain:

* Membantu organisasi dalam melindungi data sensitif dari akses yang tidak sah dan kebocoran informasi.
* Memfasilitasi kepatuhan terhadap regulasi dan persyaratan hukum terkait keamanan informasi yang berlaku di industri tertentu.
* Meningkatkan kepercayaan pelanggan dan mitra bisnis dengan menunjukkan komitmen terhadap keamanan informasi.
* Memberikan pendekatan sistematis dalam mengidentifikasi, mengevaluasi, dan mengelola risiko keamanan informasi.

Dalam konteks tata kelola TI dan keamanan informasi, ISO/IEC 27000 dapat diintegrasikan dengan framework lain seperti COBIT 2019 dan NIST CSF. Integrasi ini memungkinkan organisasi untuk menggabungkan praktik terbaik dari berbagai framework guna menciptakan pendekatan yang lebih holistik terhadap manajemen risiko dan keamanan informasi. Misalnya, COBIT 2019 menyediakan panduan untuk tata kelola TI secara keseluruhan, sementara NIST CSF fokus pada pengelolaan risiko siber. Dengan menggunakan ketiga framework ini secara bersamaan, organisasi dapat mencapai tujuan strategis mereka sekaligus memastikan bahwa mereka memiliki sistem manajemen keamanan informasi yang kuat.

Dengan demikian, penerapan ISO/IEC 27000 tidak hanya membantu organisasi dalam memenuhi standar keamanan informasi tetapi juga berkontribusi pada pencapaian tujuan bisnis secara keseluruhan.

Meskipun ketiga framework tersebut memiliki fokus dan pendekatan yang berbeda, ada sejumlah kesamaan dalam prinsip-prinsip inti yang mereka terapkan, terutama dalam hal pengelolaan risiko dan kepatuhan terhadap regulasi. Namun, implementasi framework ini juga menghadapi tantangan, seperti kebutuhan akan sumber daya, penyesuaian terhadap budaya organisasi, serta kesesuaian dengan regulasi lokal. Penelitian ini menjadi penting karena pemilihan framework yang tepat atau kombinasi antara keduanya dapat memberikan manfaat yang signifikan bagi organisasi dalam meningkatkan tata kelola TI dan keamanan informasi secara menyeluruh. Hasil dari penelitian ini diharapkan dapat menjadi panduan praktis bagi organisasi dalam menentukan atau mengintegrasikan framework yang paling sesuai dengan profil risiko dan tujuan bisnis mereka.

Dengan memahami dan membandingkan aspek-aspek yang sama antara COBIT 2019 dan NIST, organisasi dapat memaksimalkan efektivitas pengelolaan TI mereka dan meningkatkan perlindungan terhadap risiko-risiko siber yang mungkin dihadapi.

## Rumusan Masalah

Rumusan dari pembuatan makalah ini adalah sebagai berikut:

1. Bagaimana kesamaan dan perbedaan antara *framework* COBIT 2019 dengan NIST *Cybersecurity Framework* (CSF) dalam hal tata kelola TI dan manajemen keamanan informasi?
2. Bagaimana kesamaan dan perbedaan antara *framework* COBIT 2019 dan ISO/IEC 27001 dalam hal tata kelola TI dan manajemen keamanan informasi
3. Bagaimana kedua framework ini mendukung organisasi dalam mengelola risiko keamanan informasi secara efektif?
4. Apa saja kelebihan dan kekurangan dari penggunaan COBIT 2019 dengan NIST *Cybersecurity Framework* (CSF) dan ISO/IEC 27001 dalam konteks penerapan tata kelola dan keamanan informasi?

## Tujuan Pengkajian

Selain untuk pemenuhan tugas akhir,beberapa tujuan dari penelitian ini adalah sebagai berikut.

1. Bagaimana kesamaan dan perbedaan antara framework COBIT 2019 dengan NIST *Cybersecurity Framework* (CSF) dan ISO/IEC 27001 dalam aspek tata kelola TI dan manajemen keamanan informasi?
2. Bagaimana kesamaan dan perbedaan antara framework COBIT 2019 dengan NIST *Cybersecurity Framework* (CSF) dan ISO/IEC 27001 dalam aspek tata kelola TI dan manajemen keamanan informasi?
3. Sejauh mana kedua framework ini mendukung organisasi dalam mengidentifikasi, mengelola, dan memitigasi risiko keamanan informasi secara efektif?
4. Apa saja kelebihan dan kekurangan dari penerapan COBIT 2019 dengan NIST *Cybersecurity Framework* (CSF) dan ISO/IEC 27001 dalam konteks tata kelola TI dan keamanan informasi, serta bagaimana relevansinya terhadap kepatuhan regulasi industri?
5. Bagaimana kombinasi atau integrasi antara COBIT 2019 dengan NIST *Cybersecurity Framework* (CSF) dan ISO/IEC 27001 dapat memberikan nilai tambah dalam pengelolaan TI dan keamanan informasi organisasi?

## Manfaat Pengakajian

Manfaat yang dapat diperoleh dari pengkajian perbandingan antara framework NIST *Cybersecurity Framework* (CSF) dan ISO/IEC 27001 dalam konteks tata kelola dan keamanan informasi:

1. Panduan Pemilihan Framework yang Tepat Pengkajian ini membantu organisasi dalam menentukan framework yang paling sesuai dengan kebutuhan, profil risiko, dan tujuan bisnis mereka, apakah itu COBIT 2019 dengan NIST *Cybersecurity Framework* (CSF) dan ISO/IEC 27001, atau kombinasi keduanya.
2. Optimasi Tata Kelola dan Keamanan Informasi untuk memahami kelebihan dan kekurangan masing-masing framework, organisasi dapat mengoptimalkan tata kelola TI dan praktik keamanan informasi mereka untuk meningkatkan efisiensi, kepatuhan, dan perlindungan terhadap ancaman siber.
3. Peningkatan Manajemen Risiko ini memberi wawasan tentang pendekatan manajemen risiko dari kedua framework, sehingga organisasi dapat mengimplementasikan strategi yang lebih baik dalam mengidentifikasi, menilai, dan mengelola risiko keamanan informasi.
4. Peningkatan Kepatuhan terhadap Regulasi Analisis perbandingan ini juga dapat membantu organisasi memahami bagaimana setiap framework mendukung kepatuhan terhadap regulasi dan standar industri, sehingga mereka dapat memenuhi persyaratan hukum dan mengurangi risiko kepatuhan.
5. Nilai Tambah bagi Integrasi Framework Jika ada kebutuhan untuk menggabungkan elemen-elemen dari kedua framework, pengkajian ini menyediakan informasi yang berguna tentang cara terbaik untuk mengintegrasikan aspek-aspek penting dari COBIT 2019 dan NIST CSF agar lebih selaras dengan strategi organisasi.
6. Pengembangan Kebijakan Keamanan dan Kesadaran Pengguna: Hasil pengkajian ini dapat mendukung pengembangan kebijakan keamanan yang lebih komprehensif serta program kesadaran keamanan informasi bagi seluruh pemangku kepentingan di organisasi.

Pengkajian mengenai perbandingan *framework* **COBIT 2019** dengan **NIST *Cybersecurity Framework* (CSF)** dan *framework* **COBIT 2019 dengan ISO/IEC 27001** dalam konteks tata kelola dan keamanan informasi memiliki sejumlah manfaat penting yang dapat mendukung efektivitas organisasi dalam menghadapi tantangan keamanan siber dan tata kelola TI. Beberapa manfaat utama dari pengkajian ini adalah:

1. **Memberikan Pemahaman Komprehensif tentang Tata Kelola TI dan Keamanan Siber**

Pengkajian ini memberikan pemahaman yang mendalam mengenai pendekatan tata kelola TI dan keamanan siber dari dua framework utama yang diakui secara internasional. Hal ini memungkinkan organisasi untuk lebih memahami konsep, metodologi, dan praktik terbaik dalam mengelola aset informasi serta melindungi sistem dari ancaman siber.

1. **Membantu dalam Pemilihan *Framework* yang Tepat untuk Organisasi**

Dengan menganalisis dan membandingkan kelebihan dan kekurangan dari COBIT 2019 dengan NIST ***Cybersecurity Framework* (CSF)** dan ISO/IEC 27001, organisasi dapat menentukan framework yang paling sesuai dengan kebutuhan mereka. Kajian ini akan memberikan panduan dalam memilih framework yang optimal berdasarkan tujuan bisnis, kebutuhan keamanan, dan kompleksitas operasi organisasi.

1. **Meningkatkan Efisiensi Implementasi Tata Kelola dan Keamanan Informasi**

Pengkajian ini dapat membantu organisasi dalam mengintegrasikan elemen-elemen terbaik dari kedua framework untuk menciptakan tata kelola dan keamanan informasi yang lebih efektif. Hal ini memungkinkan penerapan kontrol keamanan yang lebih sesuai, pengelolaan risiko yang lebih baik, dan alokasi sumber daya yang lebih efisien.

1. **Mendukung Peningkatan Kepatuhan terhadap Standar dan Regulasi**

COBIT 2019 dengan ***Cybersecurity Framework* (CSF)** dan ISO 27001 sama-sama membantu organisasi dalam mencapai kepatuhan terhadap berbagai standar dan regulasi yang relevan, seperti, GDPR, dan regulasi lokal lainnya. Kajian ini akan membantu organisasi memahami bagaimana kedua framework tersebut mendukung pencapaian kepatuhan hukum dan standar keamanan informasi.

1. **Meningkatkan Kemampuan Manajemen Risiko Siber**

Perbandingan kedua framework akan mengungkap pendekatan yang lebih efektif dalam mengidentifikasi, mengevaluasi, dan mengelola risiko keamanan siber. Hal ini akan membantu organisasi mengembangkan strategi yang lebih proaktif dalam menghadapi ancaman keamanan informasi, serta meningkatkan ketahanan terhadap serangan siber.

1. **Mendukung Keberlanjutan Bisnis melalui Pengelolaan Keamanan yang Lebih Baik**

Implementasi framework yang tepat membantu memastikan keberlanjutan bisnis dengan melindungi aset informasi kritis dari ancaman yang terus berkembang. Pengkajian ini akan menunjukkan bagaimana pengelolaan tata kelola dan keamanan informasi yang kuat dapat meminimalkan potensi gangguan operasional akibat insiden siber.

1. **Memberikan Wawasan tentang Praktik Terbaik dalam Keamanan Informasi**

Kajian ini akan memberikan wawasan mengenai praktik terbaik dalam tata kelola TI dan keamanan informasi yang telah diimplementasikan oleh berbagai industri. Organisasi dapat menggunakan informasi ini sebagai acuan untuk mengadopsi pendekatan yang telah terbukti efektif dalam meningkatkan keamanan informasi.

## Ruang Lingkup Pengkajian

Ruang lingkup pengkajian ini mencakup beberapa aspek utama dalam perbandingan antara framework COBIT 2019 dengan NIST ***Cybersecurity Framework* (CSF)** dan framework COBIT 2019 dengan ISO/IEC 27001 dalam konteks tata kelola TI dan keamanan informasi, sebagai berikut:

1. Perbandingan Struktur dan Pendekatan Framework

Menganalisis elemen struktural dan pendekatan yang digunakan oleh COBIT 2019 dengan NIST ***Cybersecurity Framework* (CSF)** dan ISO/IEC 27001 dalam tata kelola dan manajemen risiko keamanan informasi.

1. Manajemen Risiko dan Keamanan Informasi

Mengkaji bagaimana masing-masing framework menangani proses identifikasi, mitigasi, dan respons terhadap risiko keamanan informasi, serta kemampuan dalam mengadaptasi strategi terhadap ancaman yang berkembang.

1. Dukungan terhadap Kepatuhan Regulasi

Menilai sejauh mana COBIT 2019 dengan NIST ***Cybersecurity Framework* (CSF)** dan ISO/IEC 27001 mendukung organisasi dalam memenuhi persyaratan regulasi dan standar industri yang relevan dengan tata kelola dan keamanan informasi.

1. Kelebihan dan Kekurangan Framework

Mengidentifikasi keunggulan dan keterbatasan dari kedua *framework* dalam penerapan nyata pada berbagai jenis organisasi, baik dalam hal efektivitas tata kelola, fleksibilitas, maupun sumber daya yang dibutuhkan.

1. Potensi Integrasi Framework

Mengkaji kemungkinan dan manfaat dari integrasi elemen-elemen COBIT 2019 dengan NIST ***Cybersecurity Framework* (CSF)** dan ISO/IEC 27001 untuk menciptakan solusi tata kelola dan keamanan informasi yang lebih terpadu.

1. Studi Kasus Implementasi (opsional)

Jika memungkinkan, membahas beberapa studi kasus atau contoh organisasi yang telah menerapkan COBIT 2019, NIST ***Cybersecurity Framework* (CSF)** dan ISO/IEC 27001, untuk memberikan gambaran nyata tentang keefektifan dan tantangan implementasi masing-masing framework dalam konteks operasional.

# BAB II

# TINJAUAN PUSTAKA

## *Framework* COBIT 2019

Framework COBIT 2019 (Control Objectives for Information and Related Technology) merupakan versi terbaru dari framework tata kelola dan manajemen TI yang dirancang untuk membantu organisasi mencapai tujuan bisnis melalui penggunaan teknologi informasi yang efektif. COBIT pertama kali dikembangkan oleh ISACA (Information Systems Audit and Control Association) dan terus diperbarui untuk menyesuaikan dengan perubahan teknologi dan kebutuhan bisnis yang berkembang.

COBIT 2019 bertujuan untuk memastikan bahwa TI mendukung pencapaian tujuan bisnis organisasi secara efektif dan efisien, dengan berfokus pada prinsip-prinsip utama seperti pemisahan antara tata kelola dan manajemen, serta pengelolaan TI berbasis nilai. Framework ini mencakup komponen-komponen utama seperti tujuan tata kelola, proses, prinsip, praktik terbaik, dan panduan implementasi, yang semuanya dirancang untuk membantu organisasi mengelola risiko TI dengan baik.

Framework ini juga mendukung pendekatan berbasis pemangku kepentingan, dengan mempertimbangkan kebutuhan dan ekspektasi berbagai pihak terkait untuk membantu mencapai keseimbangan antara manfaat, risiko, dan sumber daya TI. Selain itu, COBIT 2019 kompatibel dengan standar dan framework lain seperti ITIL, ISO/IEC 27001, dan NIST CSF, sehingga memungkinkan integrasi dengan pendekatan lain yang mungkin sudah diterapkan di organisasi.

COBIT 2019 menyediakan panduan implementasi yang fleksibel dan berbasis skala prioritas, memungkinkan organisasi dari berbagai ukuran dan industri untuk menyesuaikan framework ini sesuai kebutuhan spesifik mereka.

## Framework NIST Cybersecurity Framework (CSF)

**NIST *Cybersecurity Framework* (CSF) adalah sebuah kerangka kerja yang dikembangkan oleh *National Institute of Standards and Technology* (NIST), sebuah lembaga di bawah Departemen Perdagangan Amerika Serikat, yang berfokus pada peningkatan keamanan siber di sektor-sektor industri kritis. NIST CSF diperkenalkan pertama kali pada tahun 2014 sebagai panduan bagi organisasi untuk meningkatkan ketahanan terhadap ancaman siber dan telah diperbarui beberapa kali untuk menyesuaikan dengan perkembangan teknologi dan ancaman keamanan.**

**Tujuan utama NIST CSF adalah membantu organisasi mengelola dan mengurangi risiko keamanan siber, serta meningkatkan kemampuan mereka dalam mencegah, mendeteksi, merespons, dan memulihkan dari insiden siber. Framework ini terdiri dari lima fungsi utama atau Core Functions yang mencakup Identify, Protect, Detect, Respond, dan Recover. Kelima fungsi ini memberikan struktur yang sistematis dalam menangani ancaman siber, mulai dari identifikasi risiko hingga pemulihan dari insiden.**

**NIST CSF dirancang dengan pendekatan yang fleksibel dan terukur, sehingga dapat diterapkan oleh organisasi dari berbagai ukuran dan sektor. Framework ini juga memiliki keselarasan dengan standar keamanan internasional seperti ISO/IEC 27001, yang memungkinkan organisasi untuk mengintegrasikan NIST CSF dengan standar keamanan informasi lainnya.**

**Framework ini menggunakan Framework Profiles untuk membantu organisasi dalam mengevaluasi postur keamanan siber saat ini, membandingkannya dengan profil yang diinginkan, serta merencanakan langkah-langkah peningkatan. Dengan fleksibilitas ini, NIST CSF memungkinkan organisasi untuk menyesuaikan framework sesuai dengan kebutuhan spesifik dan profil risiko mereka.**

### 2.2.1 Definisi dan Tujuan ****NIST *Cybersecurity Framework* (CSF)****

NIST CSF merupakan sebuah panduan berbasis risiko yang menyediakan pendekatan sistematis dalam mengelola keamanan siber. Framework ini dirancang untuk digunakan oleh organisasi dari semua ukuran dan sektor, baik di sektor swasta maupun publik.

Tujuan utama dari NIST CSF adalah memberikan panduan bagi organisasi untuk:

1. **Mengidentifikasi dan Mengelola Risiko Siber**

Membantu organisasi dalam mengidentifikasi, menilai, dan memahami risiko keamanan siber yang ada, serta membuat perencanaan mitigasi risiko yang sesuai.

1. **Meningkatkan Ketahanan terhadap Ancaman Siber**

Mengembangkan kemampuan organisasi untuk melindungi sistem, mendeteksi ancaman, merespons insiden siber, dan melakukan pemulihan pasca-insiden.

1. **Mendukung Kepatuhan dan Standardisasi**

Memberikan panduan yang selaras dengan standar keamanan internasional seperti ISO/IEC 27001, sehingga organisasi dapat lebih mudah memenuhi persyaratan regulasi dan standar yang berlaku.

1. **Memfasilitasi Peningkatan Berkelanjutan**

Framework ini memberikan dasar untuk organisasi secara berkala meninjau dan meningkatkan postur keamanan mereka melalui fungsi utama framework, yaitu *Identify*, *Protect*, *Detect*, *Respond*, dan *Recover*.

1. **Mendukung Fleksibilitas dan Penerapan yang Dapat Disesuaikan**

Dengan pendekatan berbasis profil (*Framework Profiles*), NIST CSF memungkinkan organisasi untuk menyesuaikan penerapan framework ini sesuai dengan kebutuhan, skala, dan karakteristik risiko yang mereka hadapi.

## *Framework* ISO/IEC 27001

Framework ISO/IEC 27001 adalah kerangka kerja yang memberikan panduan untuk mengelola keamanan informasi dalam organisasi secara sistematis. Framework ini berfungsi sebagai dasar untuk menerapkan, memelihara, dan meningkatkan Sistem Manajemen Keamanan Informasi (ISMS). Berikut adalah komponen utama dalam framework ISO/IEC 27001:

**--TOLONG TAMBAHKAN ---**

* + 1. **Definisi dan Tujuan ISO/IEC 27001**

#### ****Definisi ISO/IEC 27001****

ISO/IEC 27001 adalah standar internasional yang memberikan persyaratan untuk menetapkan, menerapkan, memelihara, dan terus meningkatkan Sistem Manajemen Keamanan Informasi (Information Security Management System atau ISMS). Standar ini diterbitkan oleh International Organization for Standardization (ISO) dan International Electrotechnical Commission (IEC) dan bertujuan untuk melindungi kerahasiaan, integritas, dan ketersediaan informasi dengan mengelola risiko keamanan informasi dalam organisasi.

ISO/IEC 27001 mendefinisikan berbagai persyaratan yang harus dipenuhi oleh organisasi yang ingin menerapkan ISMS, termasuk kebijakan, prosedur, kontrol teknis, dan proses manajemen untuk mengidentifikasi dan mengelola risiko terkait keamanan informasi.

#### ****Tujuan ISO/IEC 27001****

Tujuan utama dari ISO/IEC 27001 adalah membantu organisasi dalam menjaga keamanan informasi melalui penerapan praktik terbaik manajemen risiko dan kontrol keamanan. Berikut adalah beberapa tujuan utama dari penerapan ISO/IEC 27001:

* 1. **Menjaga Kerahasiaan Informasi**
* Melindungi informasi dari akses yang tidak sah, menjaga informasi tetap terbatas pada pihak-pihak yang berwenang.
  1. **Memastikan Integritas Data**
* Menjaga akurasi dan kelengkapan data, sehingga data tidak diubah tanpa izin atau secara tidak sah.
  1. **Memastikan Ketersediaan Informasi**
* Menjamin bahwa informasi dan sistem pendukungnya tersedia ketika dibutuhkan oleh pengguna yang berwenang.
  1. **Meningkatkan Manajemen Risiko Keamanan Informasi**
* Mengidentifikasi, menilai, dan mengelola risiko yang berkaitan dengan keamanan informasi melalui proses yang terstruktur, sehingga organisasi dapat mengambil langkah-langkah pencegahan yang efektif.
  1. **Kepatuhan Hukum dan Regulasi**
* Memastikan bahwa organisasi memenuhi persyaratan hukum, peraturan, dan kontrak yang berkaitan dengan keamanan informasi, seperti perlindungan data dan privasi.
  1. **Meningkatkan Kepercayaan Stakeholder**
* Meningkatkan kepercayaan dari pelanggan, mitra bisnis, dan pihak berkepentingan lainnya dengan menunjukkan komitmen terhadap keamanan informasi melalui penerapan standar internasional.
  1. **Peningkatan Berkelanjutan**
* Mendorong budaya peningkatan berkelanjutan dalam manajemen keamanan informasi, baik melalui audit internal maupun tinjauan manajemen yang teratur, untuk selalu menyesuaikan dengan perkembangan ancaman keamanan.

**--TOLONG TAMBAHKAN ---**

# BAB III

# METODE PENELITIAN

Penelitian ini menggunakan metode deskriptif kualitatif dengan pendekatan studi kepustakaan (literature review). Penelitian ini akan melakukan analisis komparatif antara Framework COBIT 2019 dan NIST *Cybersecurity Framework* (CSF) juga COBIT 2019 dengan ISO/IEC 27001 untuk mengidentifikasi kesamaan, perbedaan, dan keunggulan masing-masing dalam konteks tata kelola dan keamanan informasi.

## Pendekatan Penelitian

Pendekatan yang digunakan dalam penelitian ini adalah deskriptif kualitatif. Penelitian deskriptif bertujuan untuk memberikan gambaran mendetail mengenai karakteristik dari dua kerangka kerja yang dibandingkan, yaitu COBIT 2019 dan NIST CSF ) juga COBIT 2019 dengan ISO/IEC 27001. Dengan pendekatan ini, penelitian akan mengeksplorasi poin-poin persamaan dan perbedaan berdasarkan kajian pustaka dan literatur yang relevan.

## Pengumpulan Data

Pengumpulan data dilakukan melalui kajian pustaka, di mana berbagai sumber literatur yang relevan dengan framework COBIT 2019 dan NIST CSF juga juga COBIT 2019 dengan ISO/IEC 27001 akan dikaji. Sumber data mencakup:

1. Buku referensi terkait tata kelola TI dan keamanan informasi.
2. Jurnal ilmiah dan artikel penelitian yang membahas implementasi dan evaluasi COBIT 2019 dengan NIST CSF. Dan COBIT 2019 dengan ISO/IEC 27001
3. Dokumen resmi dari ISACA mengenai COBIT 2019, dokumen NIST CSF dari National Institute of Standards and Technology dan ISO/IEC 27001yang diterbitkan oleh *International Organization for Standardization* (ISO) dan *International Electrotechnical Commission* (IEC).

## Teknik Analisis Data

Analisis data dilakukan secara komparatif dengan tahapan sebagai berikut:

1. Tahap 1: Pengumpulan Informasi Dasar Pada tahap awal, data mengenai struktur dasar, tujuan, dan fokus utama dari COBIT 2019 dan NIST CSF juga COBIT 2019 dengan ISO/IEC 27001 dikumpulkan. Tujuan dari tahap ini adalah untuk memberikan pemahaman dasar mengenai bagaimana masing-masing framework bekerja, tujuan tata kelola dan keamanan yang diutamakan, serta ruang lingkup penerapannya.
2. Tahap 2: Identifikasi Poin-Poin Persamaan dan Perbedaan Data yang terkumpul kemudian dianalisis untuk mengidentifikasi poin-poin persamaan dan perbedaan antara COBIT 2019 dan NIST CSF juga COBIT 2019 dengan ISO/IEC 27001. Peneliti akan menguraikan kesamaan dalam hal manajemen risiko, keamanan informasi, kepatuhan terhadap regulasi, serta pengelolaan sumber daya TI.
3. Tahap 3: Analisis Kelebihan dan Kekurangan Masing-Masing Framework Setelah mengidentifikasi persamaan dan perbedaan, penelitian akan melakukan analisis untuk mengevaluasi kelebihan dan kekurangan masing-masing framework. COBIT 2019 lebih menekankan pada tata kelola yang menyeluruh, sedangkan NIST CSF berfokus pada aspek keamanan siber dan Fokus dari ISO/IEC 27001 adalah membangun, mengimplementasikan, memelihara, dan meningkatkan Sistem Manajemen Keamanan Informasi (Information Security Management System/ISMS). Dalam tahap ini, peneliti juga akan membahas fleksibilitas, kompleksitas penerapan, serta dukungan terhadap tujuan bisnis dan keamanan.

# BAB IV

# HASIL PENGKAJIAN DAN PEMBAHASAN

## Framework COBIT 2019 dan NIST NIST *Cybersecurity Framework* (NIST CSF).

Tahap pembahasan pertama yaitu mengkaji *framework* COBIT 2019 dan NIST *Cybersecurity Framework* (NIST CSF) untuk memahami kesamaan dan perbedaan keduanya dalam konteks tata kelola dan keamanan informasi. Melalui analisis mendetail terhadap poin-poin utama dalam kedua framework, beberapa kesamaan prinsip ditemukan, terutama dalam hal pengelolaan risiko, kepatuhan terhadap regulasi, dan pengelolaan sumber daya TI secara efisien.

## Relevansi *framework* COBIT 2019 dan NIST *Cybersecurity Framework* (CSF).

Fokus utama Cobit 2019 adalah pada tata kelola TI secara menyeluruh, termasuk manajemen risiko, kinerja, dan kepatuhan, sedangkan NIST *Cybersecurity Framework* (NIST CSF) Fokus pada keamanan siber, dengan pendekatan berbasis risiko yang berfokus pada perlindungan aset.

Dari sini dapat NIST *Cybersecurity Framework* (CSF) itu sangat focus pada cyber security, akan tetapi framework COBIT 2019 lebih menyeluruh. Cyber Security sudah menjadi bagian dari framework COBIT 2019. Tetapi dari penerapan konsep kedua framework ini menerapkan hal yang sama yaitu menjadi fokusnya ke management resiko.

Jika diklasifikasikan relevansi dari framework COBIT 2019 dengan NIST *Cybersecurity Framework* (NIST CSF) ada beberapa klasifikasi

### Pengelolaan Risiko (Risk Management)

Baik COBIT 2019 maupun NIST *Cybersecurity Framework* (CSF) memiliki fokus yang kuat pada pengelolaan risiko, meskipun pendekatannya berbeda. COBIT 2019 mengintegrasikan pengelolaan risiko ke dalam tata kelola TI secara menyeluruh, menjadikannya sebagai bagian dari proses manajemen strategis untuk mendukung tujuan bisnis. COBIT 2019 mengarahkan organisasi untuk mengidentifikasi, mengevaluasi, dan merespons risiko TI yang berpotensi menghambat pencapaian tujuan bisnis. Framework ini juga memberikan panduan praktis dalam membangun sistem kontrol dan mitigasi risiko melalui domain pengelolaan risiko TI (ISACA, 2019).

NIST *Cybersecurity Framework* (NIST CSF), di sisi lain, berfokus pada manajemen risiko keamanan siber dengan pendekatan yang lebih teknis. NIST CSF menawarkan pendekatan berbasis siklus hidup untuk mengidentifikasi, melindungi, mendeteksi, merespons, dan memulihkan dari insiden keamanan siber (NIST, 2020). Sama seperti COBIT, NIST CSF menekankan pentingnya mitigasi risiko, tetapi dengan orientasi yang lebih kuat pada perlindungan infrastruktur kritis dan data sensitif.

### Pengelolaan Sumber Daya TI (IT *Resource Management*)

COBIT 2019 menyediakan panduan yang lebih komprehensif dalam pengelolaan sumber daya TI secara keseluruhan, termasuk infrastruktur, aplikasi, dan informasi. COBIT menekankan pentingnya memaksimalkan nilai dari sumber daya TI yang tersedia serta menyeimbangkan antara investasi, manfaat, dan risiko (ISACA, 2019). Framework ini menekankan pada manajemen siklus hidup sumber daya TI, dari perencanaan hingga pengawasan penggunaan, serta menjaga keselarasan antara sumber daya TI dan kebutuhan bisnis.

Sementara itu, NIST lebih berfokus pada perlindungan aset dan infrastruktur informasi. NIST menyediakan pedoman untuk melindungi perangkat keras, perangkat lunak, dan data dari ancaman keamanan siber. Selain itu, NIST juga menekankan pentingnya pemantauan berkelanjutan terhadap ancaman untuk memastikan kesiapan dalam menghadapi serangan siber.

### Keselarasan dengan Tujuan Bisnis (Business Alignment)

COBIT 2019 secara eksplisit dirancang untuk memastikan bahwa pengelolaan TI selalu sejalan dengan tujuan strategis organisasi. Framework ini menyediakan mekanisme untuk menyelaraskan proses TI dengan tujuan bisnis, serta mendorong kolaborasi antara manajemen dan departemen TI agar tujuan organisasi dapat dicapai secara lebih efektif (ISACA, 2019).

NIST *Cybersecurity Framework* (NIST CSF) juga mengakui pentingnya keselarasan ini, tetapi lebih pada aspek perlindungan terhadap risiko keamanan yang dapat menghambat pencapaian tujuan bisnis. NIST berupaya membantu organisasi meminimalkan dampak risiko keamanan siber yang dapat mengganggu operasional dan reputasi bisnis (NIST, 2020).

Dari beberapa penjelasan diatas bisa lebih terperinci pada tabel dibawah ini.

**Tabel 1. 1 Relevansi Cobit 2019 dan NIST CSF**

|  |  |  |
| --- | --- | --- |
| **Item**  **COBIT 2019** | **Deskripsi**  **COBIT** | **Relevansi dengan**  **NIST CSF** |
| Tujuan Tata Kelola dan Manajemen (EDM, APO, DSS, MEA) | COBIT 2019 mendefinisikan 40 tujuan tata kelola dan manajemen yang mencakup berbagai proses TI, termasuk tata kelola (EDM), strategi (APO), pengiriman (DSS), dan pemantauan (MEA). | NIST CSF berfokus pada manajemen risiko dan keamanan operasional, sejalan dengan tata kelola dan pemantauan (misalnya, Identify, Protect, Detect, Respond, Recover). |
| Optimalisasi Risiko (EDM03) | Berfokus pada memastikan bahwa risiko terkait TI tidak melebihi toleransi risiko organisasi dan dikelola untuk menciptakan nilai. | NIST memiliki fokus khusus pada manajemen risiko keamanan siber, terutama melalui fungsi "Identify" dan "Respond". |
| Penyelarasan Tujuan TI dan Bisnis (APO02) | Memastikan bahwa strategi TI dan bisnis selaras dan mendukung satu sama lain dalam mencapai tujuan organisasi. | NIST CSF secara tidak langsung mendukung ini melalui integrasi manajemen risiko ke dalam tujuan bisnis, tetapi COBIT lebih eksplisit dalam mengaitkan TI dengan tujuan bisnis. |
| Pengelolaan Keamanan TI (APO13) | Berfokus pada membangun dan memelihara sistem manajemen untuk memastikan keamanan informasi, infrastruktur, aplikasi, dan layanan. | Secara langsung sebanding dengan fungsi "Protect" dalam NIST, yang bertujuan melindungi infrastruktur kritis dan informasi sensitif. |
| Pengelolaan Risiko (APO12) | Mengidentifikasi dan mengelola risiko terhadap tujuan organisasi, memastikan bahwa risiko terkait TI diminimalkan. | Fungsi "Identify" NIST sejalan di sini dengan mensyaratkan organisasi untuk memahami dan mengelola risiko keamanan siber terhadap sistem, aset, dan data. |
| Pengukuran Kinerja (MEA01) | Mengukur kinerja proses TI untuk memastikan bahwa mereka memenuhi tujuan bisnis dan tata kelola. | NIST CSF mencakup metrik kinerja sebagai bagian dari fungsi "Recover" dan pendekatan perbaikan berkelanjutan, tetapi lebih sedikit detail dibandingkan COBIT dalam area ini. |
| Kepatuhan terhadap Persyaratan Eksternal (APO08) | Memastikan bahwa kebijakan dan prosedur TI mematuhi peraturan eksternal dan undang-undang. | Ini sangat sejalan dengan tujuan terkait kepatuhan dalam NIST, terutama ketika digunakan bersama dengan ISO/IEC 27001 untuk kerangka kerja kepatuhan regulasi. |
| Manajemen Insiden (DSS02) | Mengelola insiden TI untuk meminimalkan dampak bisnis, termasuk deteksi, respons, dan penyelesaian insiden. | Fungsi "Detect" dan "Respond" dari NIST CSF memberikan panduan terperinci tentang cara mengidentifikasi dan merespons insiden keamanan. |
| Pemantauan Keamanan Informasi (MEA03) | Memantau dan menilai kinerja keamanan informasi secara berkelanjutan untuk memastikan manajemen risiko dan kepatuhan yang berkelanjutan. | Fungsi "Detect" dalam NIST CSF mencakup kegiatan pemantauan dan deteksi untuk kejadian-kejadian keamanan siber yang potensial. |
| Manajemen Risiko Keamanan Siber | Berfokus pada integrasi keamanan siber dalam proses manajemen risiko dan struktur tata kelola yang lebih luas. | Ini merupakan inti dari NIST CSF, di mana manajemen risiko ancaman keamanan siber diintegrasikan ke seluruh proses organisasi. |

Relevansi Untuk domain framework COBIT 2019 dengan NIST *Cybersecurity Framework* (NIST CSF) sebagai berikut.

**Tabel 1. 2 Relevansi Domain Cobit 2019 dengan Kontrol NIST CST**

|  |  |  |
| --- | --- | --- |
| Domain Cobit 2019 | Kontrol NIST CST | Relevansi |
| MEM01: Mengidentifikasi dan Mengelola Risiko | ICS1: Inventarisasi Aset yang Sah, ACS1: Manajemen Kerentanan Berkelanjutan | Kedua proses ini berfokus pada identifikasi aset dan risiko yang terkait. MEM01 secara umum, sedangkan ICS1 lebih spesifik pada aset fisik dan ACS1 pada kerentanan sistem. Baik MEM02 dan IR8 menekankan pentingnya mengelola perubahan dengan cara yang terkendali untuk mencegah dampak negatif pada keamanan. |
| MEM02: Mengelola Perubahan | IR8: Manajemen Perubahan | Baik MEM02 dan IR8 menekankan pentingnya mengelola perubahan dengan cara yang terkendali untuk mencegah dampak negatif pada keamanan. |
| MEM03: Mengelola Kinerja | DCS-1: Penggunaan Software yang Aman | MEM03 berfokus pada pengukuran kinerja, sedangkan DCS-1 memastikan penggunaan software yang aman. Namun, keduanya terkait karena penggunaan software yang tidak aman dapat berdampak negatif pada kinerja sistem. |

## Perbedaan *framework* COBIT 2019 dan NIST *Cybersecurity Framework* (CSF)

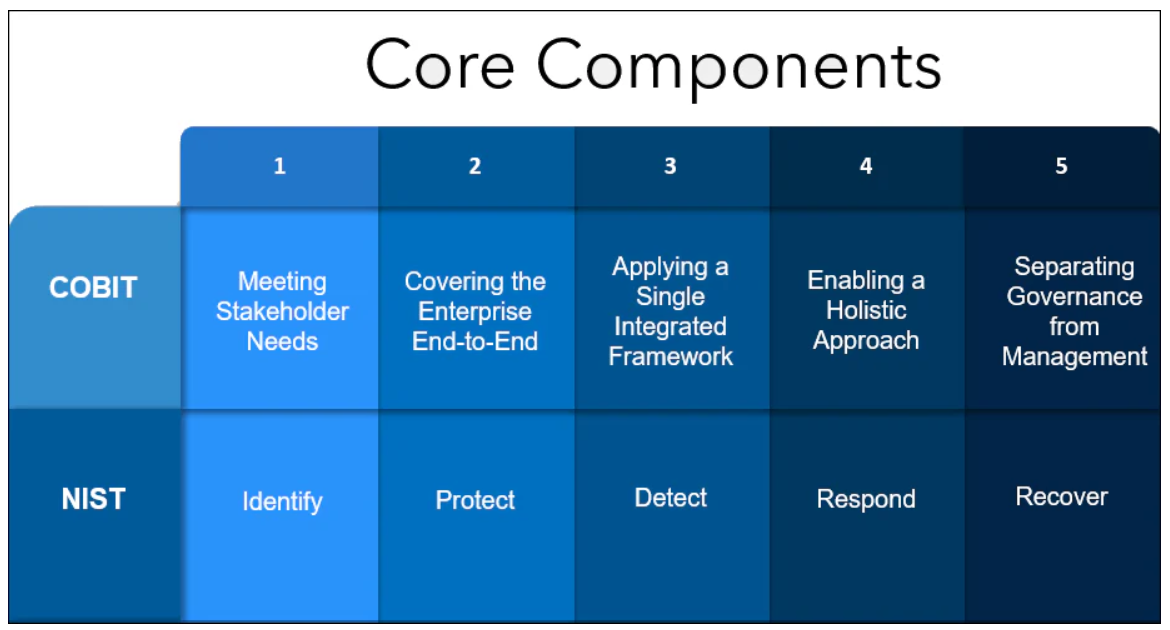
Dari segi landasan framework mempunyai lima landasan. Diantaranya:

1. Meeting Stakeholder Needs
2. Covering the Enterprise End-to-End
3. Applying a Single Integrated Framework
4. Enabling a Holistic Approach
5. Separating Governance from Management

Untuk *framework* NIST *Cybersecurity Framework* (CSF) seperti dibawah ini:

1. Identify
2. Protect
3. Detect
4. Respond

**Gambar 1. 1 Core Components**



Ada beberapa perbedaan signifikan dari framework COBIT 2019 dan NIST Cybersecurity Framework (CSF) bisa dilihat dari list berikut

**Tabel 1. 3 framework COBIT 2019 dan NIST Cybersecurity Framework (CSF)**

|  |  |  |
| --- | --- | --- |
| **Aspek** | **COBIT 2019** | **NIST CSF** |
| Tujuan Utama | Fokus pada tata kelola TI secara menyeluruh, termasuk manajemen risiko, kinerja, dan kepatuhan. | Fokus pada keamanan siber, dengan pendekatan berbasis risiko yang berfokus pada perlindungan aset. |
| Struktur Framework | Terdiri dari 40 tujuan tata kelola dan manajemen (Governance & Management Objectives) yang mencakup berbagai aspek TI. | Terbagi menjadi lima fungsi utama: Identify, Protect, Detect, Respond, Recover (ID.RPR). |
| Fungsi Utama | Menyediakan panduan untuk mengelola, mengontrol, dan mengawasi TI dalam organisasi untuk mendukung tujuan bisnis. | Membangun kemampuan untuk mengidentifikasi, melindungi, mendeteksi, merespons, dan memulihkan dari ancaman keamanan siber. |
| Fokus Manajemen Risiko | Mengintegrasikan manajemen risiko dalam semua proses TI untuk memastikan bahwa risiko yang dihadapi TI sesuai dengan toleransi risiko organisasi. | Secara eksplisit berfokus pada manajemen risiko keamanan siber dengan pendekatan berbasis siklus hidup: identifikasi, perlindungan, deteksi, respons, dan pemulihan. |
| Kepatuhan Terhadap Regulasi | Menyediakan panduan untuk mematuhi peraturan eksternal, seperti GDPR, HIPAA, PCI DSS. | Membantu organisasi untuk mematuhi regulasi yang relevan melalui integrasi kontrol keamanan siber berbasis standar. |
| Pendekatan terhadap Keamanan Informasi | Menekankan pentingnya mengelola risiko keamanan informasi sebagai bagian dari manajemen TI secara keseluruhan. | Menyediakan kerangka kerja yang sangat rinci untuk menangani aspek keamanan informasi dan ancaman siber. |
| Keamanan Teknologi dan Infrastruktur | Berfokus pada pengelolaan dan perlindungan infrastruktur TI dan data organisasi untuk mendukung tujuan bisnis. | Fokus pada melindungi aset kritis, termasuk perangkat keras, perangkat lunak, data, dan sistem informasi dari ancaman siber. |
| Pemantauan dan Evaluasi | Menyediakan panduan untuk memantau dan mengevaluasi kinerja, serta efektivitas kontrol dan risiko dalam organisasi. | Mencakup fungsi deteksi dan pemantauan berkelanjutan untuk mengidentifikasi potensi insiden keamanan siber. |
| Keselarasan dengan Tujuan Bisnis | Menyelaraskan TI dengan tujuan bisnis secara keseluruhan untuk mendukung pencapaian tujuan strategis organisasi. | Meskipun berfokus pada keamanan, NIST juga memastikan bahwa keamanan siber tidak menghambat pencapaian tujuan bisnis yang lebih besar. |
| Fleksibilitas dan Skalabilitas | Dapat diterapkan di berbagai jenis organisasi dan industri dengan fleksibilitas dalam penyesuaian tujuan dan kontrol. | Fleksibel dan dapat diadaptasi sesuai dengan ukuran dan kompleksitas organisasi serta kebutuhan keamanan sibernya. |
| Keterlibatan Stakeholder | Menekankan pentingnya keterlibatan pemangku kepentingan, dari tingkat eksekutif hingga operasional. | Fokus pada kolaborasi antara berbagai pemangku kepentingan dalam organisasi, termasuk pihak eksternal untuk memastikan keamanan yang holistik. |
| Dokumentasi dan Referensi | Dokumentasi yang komprehensif yang mencakup panduan untuk implementasi serta evaluasi kinerja tata kelola. | Memberikan panduan teknis yang jelas dan praktis, serta referensi untuk mengintegrasikan kontrol keamanan berdasarkan standar industri. |

secara garis besar COBIT 2019 lebih berfokus pada tata kelola TI secara keseluruhan, dengan menekankan integrasi TI dalam proses bisnis dan manajemen risiko yang lebih luas. COBIT menawarkan pendekatan yang lebih luas untuk mengelola TI dalam mendukung tujuan strategis organisasi.sedangkan NIST CSF sangat terfokus pada keamanan siber dengan pendekatan berbasis risiko yang lebih rinci dan praktis untuk mengelola ancaman dan insiden keamanan siber. Framework ini lebih cocok bagi organisasi yang mencari pedoman yang lebih spesifik terkait dengan ancaman siber dan kesiapan terhadap insiden.

## Framework COBIT 2019 dengan ISO/IEC 27001

Tahap pembahasan kedua yaitu mengkaji *framework* COBIT 2019 dengan ISO/IEC 27001, untuk memahami kesamaan dan perbedaan keduanya dalam konteks tata kelola, manajemen risiko, keamanan, kontrol akses, hubungan pemasok dan lain-lainnya.

## 5.2.1 Relevansi Framework COBIT 2019 dengan ISO/IEC 27001

COBIT 2019 dan ISO/IEC 27001 memiliki beberapa persamaan dalam fokus mereka, terutama terkait dengan tata kelola TI dan manajemen keamanan informasi. Meskipun COBIT 2019 lebih luas dalam mencakup keseluruhan tata kelola dan manajemen TI, sementara ISO/IEC 27001 berfokus pada keamanan informasi, keduanya memiliki elemen fokus yang serupa, antara lain:

1. **Manajemen Risiko**

Keduanya menekankan pentingnya mengidentifikasi, menilai, dan mengelola risiko. ISO/IEC 27001 berfokus pada risiko keamanan informasi, sedangkan COBIT 2019 memiliki pendekatan risiko yang lebih luas, termasuk risiko operasional dan strategis dalam tata kelola TI.

1. **Kepatuhan dan Regulasi**

Keduanya bertujuan untuk memastikan kepatuhan terhadap hukum dan regulasi. ISO/IEC 27001 memastikan organisasi mematuhi standar keamanan informasi, sedangkan COBIT 2019 mencakup kepatuhan TI secara keseluruhan, termasuk keamanan, privasi, dan regulasi operasional lainnya.

1. **Kontrol Keamanan dan Proses**

Kedua kerangka kerja ini menekankan pentingnya kontrol dan proses yang terdefinisi dengan baik untuk melindungi informasi organisasi. ISO/IEC 27001 mencakup kontrol teknis dan prosedural untuk keamanan informasi, sementara COBIT 2019 memiliki kontrol dan proses untuk tata kelola yang mencakup keamanan, operasional, dan pengelolaan layanan TI.

1. **Perbaikan Berkelanjutan**

Keduanya menggunakan pendekatan yang mendorong perbaikan berkelanjutan. ISO/IEC 27001 menerapkan siklus Plan-Do-Check-Act (PDCA), sedangkan COBIT 2019 juga mendorong penilaian dan perbaikan berkelanjutan dalam tata kelola TI untuk meningkatkan kualitas layanan dan keamanan.

1. **Keterlibatan Pemangku Kepentingan dan Kepemimpinan**

Kedua kerangka kerja menekankan pentingnya peran manajemen puncak dan keterlibatan pemangku kepentingan. ISO/IEC 27001 membutuhkan komitmen kepemimpinan dalam ISMS, dan COBIT 2019 menyoroti peran pemangku kepentingan dalam mendukung tata kelola dan pengambilan keputusan terkait TI.

1. **Pengelolaan Aset Informasi**

Baik COBIT 2019 maupun ISO/IEC 27001 mengakui pentingnya mengelola aset informasi secara efektif untuk memastikan integritas, kerahasiaan, dan ketersediaan data. Meskipun ISO/IEC 27001 lebih terfokus pada keamanan informasi, prinsip dasar pengelolaan aset yang aman juga tercakup dalam tujuan COBIT 2019.

Persamaan ini menjadikan COBIT 2019 dan ISO/IEC 27001 kompatibel satu sama lain. Banyak organisasi menggabungkan kedua kerangka ini untuk mencapai tata kelola TI yang kuat dan manajemen keamanan informasi yang efektif.

Secara lebih terperinci relevansi COBIT 2019 dan ISO/IEC 27001 dapat dilihat dari tabel matrik berikut ini.

**Tabel 1. 4 framework COBIT 2019 dan ISO/IEC 27001**

|  |  |  |
| --- | --- | --- |
| **Kategori** | **COBIT 2019** | **ISO/IEC 27001** |
| Kerangka Kerja Tata Kelola | EDM01: Pengaturan & Pemeliharaan Kerangka Tata Kelola | Klausa 5.1: Kepemimpinan dan Komitmen |
| Manajemen Risiko | APO12: Kelola Risiko | Klausa 6.1.2: Penilaian Risiko |
| Manajemen Keamanan | APO13: Kelola Keamanan | A.5–A.18: Kebijakan Keamanan Informasi |
| Kontrol Akses | DSS05: Kelola Layanan Keamanan | A.9: Kontrol Akses |
| Hubungan Pemasok | APO10: Kelola Pemasok | A.15: Hubungan Pemasok |
| Keberlanjutan Bisnis | DSS04: Kelola Keberlanjutan | A.17: Keberlanjutan Bisnis |
| Kepatuhan | MEA03: Kepatuhan terhadap Persyaratan Eksternal | Klausa 9.2: Audit Internal |
| Manajemen Insiden | DSS02: Kelola Insiden | A.16: Manajemen Insiden |
| Keamanan SDM | APO07: Kelola Sumber Daya Manusia | A.7: Keamanan SDM |
| Evaluasi Kinerja | MEA01: Kinerja dan Kepatuhan | Klausa 9: Evaluasi Kinerja |
| Manajemen Aset | BAI09: Kelola Aset | A.8: Manajemen Aset |

## 5.2.2 Perbedaan Framework COBIT 2019 dengan ISO/IEC 27001

Perbedaan signifikan antara COBIT 2019 dan ISO/IEC 27001 terletak pada cakupan, fokus utama, dan pendekatan yang diambil oleh masing-masing framework. Berikut adalah beberapa perbedaan utama:

1. **Cakupan dan Tujuan Utama**

COBIT 2019 dirancang untuk tata kelola dan manajemen teknologi informasi secara keseluruhan dalam suatu organisasi. Tujuannya adalah untuk mengoptimalkan nilai TI dengan memperhatikan semua aspek tata kelola TI, termasuk pengelolaan risiko, sumber daya, dan kepatuhan. Fokusnya mencakup strategi, pengambilan keputusan, kinerja, dan perbaikan operasional TI.

ISO/IEC 27001 berfokus khusus pada manajemen keamanan informasi dengan tujuan melindungi informasi yang sensitif melalui penerapan Sistem Manajemen Keamanan Informasi (ISMS). Standar ini mengarahkan organisasi dalam mengidentifikasi, mengelola, dan mengurangi risiko keamanan informasi secara sistematis.

1. **Pendekatan Berbasis Risiko**

COBIT 2019 Menggunakan tujuan tata kelola dan manajemen yang disesuaikan untuk semua aspek pengelolaan TI, dengan model yang lebih fleksibel dan dapat disesuaikan menurut kebutuhan organisasi. COBIT 2019 menyediakan domain dan proses yang lebih luas, termasuk komponen tata kelola TI seperti kebijakan, budaya, sumber daya, dan kerangka kerja.

ISO/IEC 27001 memiliki struktur yang lebih sistematis dalam sepuluh klausa dan lampiran Annex A yang berisi kontrol keamanan spesifik untuk ISMS. Annex A mengarahkan organisasi dalam menentukan langkah-langkah kontrol teknis dan operasional keamanan.

1. **Pengguna dan Aplikasi Utama**

COBIT 2019 Didesain untuk eksekutif TI, pemangku kepentingan tata kelola TI, dan manajemen tingkat atas untuk memastikan bahwa TI mendukung dan sejalan dengan tujuan bisnis. COBIT cocok untuk organisasi yang membutuhkan pendekatan holistik dalam mengelola TI.

ISO/IEC 27001 Biasanya digunakan oleh tim keamanan informasi, manajer risiko, dan profesional keamanan. Ini cocok untuk organisasi yang ingin mengembangkan sistem keamanan informasi yang sesuai dengan standar internasional dan mengatasi persyaratan kepatuhan.

1. **Sertifikasi**

COBIT tidak menyediakan sertifikasi formal untuk ISMS atau sistem tata kelola TI; namun, organisasi dapat menggunakan framework ini sebagai panduan.

ISO/IEC 27001 Memiliki proses sertifikasi resmi yang memungkinkan organisasi memperoleh sertifikat ISO/IEC 27001 dari auditor independen yang terakreditasi. Sertifikasi ini menunjukkan bahwa organisasi telah memenuhi standar internasional untuk keamanan informasi.

1. **Pendekatan Perbaikan Berkelanjutan**

COBIT 2019 Menggunakan prinsip-prinsip *Governance* Syst*em Design* dan *Components of a Governance System* untuk mendorong perbaikan berkelanjutan dalam tata kelola TI.

ISO/IEC 27001 Menggunakan siklus Plan-Do-Check-Act (PDCA) untuk memastikan bahwa ISMS terus ditinjau dan ditingkatkan.

Secara keseluruhan, COBIT 2019 lebih luas dalam konteks tata kelola TI dan manajemen yang mencakup semua aspek operasi TI, sedangkan ISO/IEC 27001 secara khusus mengarahkan organisasi untuk mengelola keamanan informasi secara sistematis dan efektif.

# BAB V

# KESIMPULAN

Perbandingan antara COBIT 2019 dan NIST Cybersecurity Framework (CSF) menunjukkan bahwa kedua framework ini memiliki fokus dan pendekatan yang berbeda namun saling melengkapi dalam konteks tata kelola dan keamanan informasi. COBIT 2019 berorientasi pada tata kelola TI secara keseluruhan, membantu organisasi dalam mengelola dan mengatur semua aspek teknologi informasi agar sejalan dengan tujuan bisnis. Sementara itu, NIST CSF lebih menekankan pada keamanan siber, memberikan panduan untuk mengelola risiko yang berkaitan dengan ancaman siber dan pemulihan dari insiden.

Kedua framework ini memiliki kesamaan dalam hal manajemen risiko dan kepatuhan terhadap regulasi. Masing-masing memberikan pendekatan sistematis untuk mengidentifikasi, mengevaluasi, dan mengatasi risiko yang dihadapi organisasi. Selain itu, keduanya mendukung penerapan praktik terbaik dan peningkatan berkelanjutan dalam pengelolaan TI dan keamanan informasi.

Kelebihan dari COBIT 2019 terletak pada pendekatan holistiknya terhadap tata kelola TI, yang mencakup manajemen sumber daya, proses, dan kinerja organisasi. Di sisi lain, NIST CSF menawarkan fleksibilitas dan pendekatan berbasis risiko yang dapat disesuaikan dengan kebutuhan spesifik organisasi, serta fokus yang kuat pada aspek keamanan siber.

Organisasi dapat mengambil manfaat dari kombinasi kedua framework ini untuk mencapai pengelolaan TI yang lebih komprehensif dan meningkatkan ketahanan terhadap ancaman siber. Dengan demikian, pemilihan framework yang tepat atau integrasi elemen-elemen dari COBIT 2019 dan NIST CSF dapat memberikan nilai tambah yang signifikan dalam meningkatkan efektivitas tata kelola TI dan keamanan informasi, serta memastikan kepatuhan terhadap regulasi yang berlaku.

Dengan pemahaman yang mendalam tentang kekuatan dan kelemahan masing-masing framework, organisasi akan lebih siap menghadapi tantangan yang terus berkembang dalam lingkungan teknologi yang semakin kompleks.

Beberapa Persamaan detail Domain Framework Cobit 2019 dengan NIST CSF yaitu:

### Persamaan

1. **MEM01**: Mengidentifikasi dan Mengelola Risiko di COBIT 2019 berkaitan dengan **ICS1**: Inventarisasi Aset yang Sah dan **ACS1**: Manajemen Kerentanan Berkelanjutan pada NIST CSF. Kedua elemen ini menekankan pentingnya pengelolaan aset dan kerentanan untuk menjaga keamanan dan integritas sistem informasi. Inventarisasi aset yang tepat memungkinkan organisasi untuk mengidentifikasi dan mengelola risiko yang terkait dengan aset tersebut secara lebih efektif.
2. **MEM02**: Mengelola Perubahan dalam COBIT 2019 terkait dengan **IR8**: Manajemen Perubahan pada NIST CSF. Proses manajemen perubahan yang terstruktur sangat penting untuk memastikan bahwa perubahan dalam sistem TI tidak menimbulkan risiko baru bagi organisasi.
3. **MEM03**: Mengelola Kinerja dalam COBIT 2019 berhubungan dengan **DCS-1**: Penggunaan Software yang Aman pada NIST CSF. Pengelolaan kinerja yang baik membantu memastikan bahwa perangkat lunak yang digunakan dalam organisasi tidak hanya memenuhi kriteria kinerja tetapi juga aman dari potensi ancaman siber.

### Perbedaan

1. **Pendekatan**: COBIT 2019 berfokus pada tata kelola TI yang lebih holistik dan menyeluruh, sementara NIST CSF lebih berorientasi pada keamanan siber dengan pendekatan berbasis risiko yang spesifik. COBIT 2019 mencakup domain yang lebih luas, termasuk pengelolaan sumber daya, sedangkan NIST CSF fokus pada aspek perlindungan informasi.
2. **Ruang Lingkup**: COBIT 2019 mencakup berbagai aspek dari tata kelola TI dan pengelolaan kinerja, sedangkan NIST CSF lebih terarah pada keamanan siber dan pemulihan dari insiden siber. Ini menciptakan perbedaan dalam cara organisasi menerapkan dan mengadaptasi masing-masing framework sesuai dengan kebutuhan mereka.
3. **Kesesuaian dengan Regulasi**: COBIT 2019 mendukung kepatuhan secara keseluruhan terhadap berbagai regulasi yang berkaitan dengan TI, sementara NIST CSF lebih terfokus pada kepatuhan terhadap standar keamanan siber yang spesifik. Hal ini memungkinkan organisasi untuk memilih pendekatan yang paling sesuai dengan lingkungan regulasi yang mereka hadapi.

Framework COBIT 2019 dan NIST Cybersecurity Framework (CSF) memiliki kesamaan dalam menyediakan panduan untuk tata kelola TI dan keamanan informasi, tetapi dengan fokus yang berbeda. COBIT 2019 dirancang untuk mendukung tata kelola TI secara menyeluruh dengan menyelaraskan tujuan teknologi dengan tujuan bisnis organisasi. Di sisi lain, NIST CSF memiliki fokus utama pada keamanan siber, menggunakan pendekatan berbasis manajemen risiko yang berfungsi untuk mencegah, mendeteksi, dan merespons ancaman siber. Oleh karena itu, meskipun keduanya bertujuan mendukung organisasi dalam menjaga keamanan informasi, mereka dapat dipilih atau dikombinasikan sesuai kebutuhan organisasi, baik dalam tata kelola TI yang luas maupun dalam manajemen risiko keamanan siber yang spesifik.

Kesamaan dan perbedaan juga ditemukan antara framework COBIT 2019 dan ISO/IEC 27001. Keduanya mendukung aspek tata kelola TI dan keamanan informasi, tetapi memiliki pendekatan berbeda. ISO/IEC 27001 mengutamakan pembentukan Sistem Manajemen Keamanan Informasi (ISMS) dengan pendekatan berbasis standar yang berfokus pada kerahasiaan, integritas, dan ketersediaan informasi. Di sisi lain, COBIT 2019 memberikan fleksibilitas yang memungkinkan organisasi menyesuaikan kontrol dan kebijakan keamanan dengan tujuan strategis bisnis. Dengan kata lain, ISO/IEC 27001 lebih sistematis dalam manajemen keamanan, sementara COBIT 2019 menyediakan kerangka yang lebih fleksibel dan menyeluruh untuk pengelolaan TI.

Dalam hal pengelolaan risiko keamanan informasi, framework COBIT 2019, NIST CSF, dan ISO/IEC 27001 memiliki peran signifikan bagi organisasi. Ketiganya menawarkan pendekatan terstruktur untuk mengenali, mengevaluasi, dan mengurangi risiko keamanan. Dengan bantuan framework ini, organisasi dapat lebih proaktif dalam melindungi informasi mereka dari ancaman internal dan eksternal serta mencapai kepatuhan terhadap regulasi yang berlaku. Penggunaan ketiga framework ini membantu organisasi membangun sistem keamanan informasi yang lebih kuat dan efisien.

Masing-masing framework memiliki kelebihan dan kekurangan yang unik dan sesuai untuk berbagai jenis organisasi. COBIT 2019 menawarkan fleksibilitas dan keterhubungan antara teknologi dan tujuan bisnis, namun memerlukan dukungan tambahan untuk aspek keamanan spesifik. NIST CSF cocok bagi organisasi yang ingin fokus pada keamanan siber karena kemudahan implementasinya, namun cakupannya tidak sekomprehensif COBIT dalam tata kelola TI secara keseluruhan. Di sisi lain, ISO/IEC 27001 memberikan pendekatan yang sistematis dan standar untuk organisasi yang mengutamakan kepatuhan dan kontrol keamanan yang ketat, meskipun bagi beberapa organisasi, sifatnya yang formal dapat terasa terlalu kaku. Secara keseluruhan, kombinasi framework ini dapat memberikan pendekatan tata kelola dan keamanan informasi yang lebih lengkap bagi or

# DAFTAR PUSTAKA

ISACA. (2019). COBIT 2019 Framework: Introduction and Methodology. ISACA.

National Institute of Standards and Technology (NIST). (2020). Framework for Improving Critical Infrastructure Cybersecurity Version 1.1. NIST.

Calder, A. (2019). IT Governance: An International Guide to Data Security and ISO27001/ISO27002. Kogan Page Publishers.

Kaarst-Brown, M. L., & Robey, D. (2016). "The Role of IT Governance in Improving IT Governance." Journal of Information Technology, 31(2), 93-104.

Peltier, T. R. (2016). Information Security Policies, Procedures, and Standards: A Practitioner's Guide. Auerbach Publications.

Rittinghouse, J. W., & Ransome, J. F. (2017). Cloud Computing: Implementation, Management, and Security. CRC Press.

Stallings, W., & Brown, L. (2019). Computer Security: Principles and Practice (4th ed.). Pearson.

Whitten, J. L., & Bentley, L. D. (2018). Systems Analysis and Design (10th ed.). Cengage Learning.

Zhang, R., & Yan, D. (2021). "A Survey on Cybersecurity Frameworks." IEEE Access, 9, 4581-4596. DOI: 10.1109/ACCESS.2020.3034567.

Zeng, J., & Huang, K. (2020). "IT Governance, Risk, and Compliance: A Review." Journal of Information Technology, 35(3), 263-287. DOI: 10.1177/0268396219830956..

Calder, A., & Watkins, S. (2015). *ISO 27001/ISO 27002: A Pocket Guide* (3rd ed.). IT Governance Publishing.

International Organization for Standardization. (2013). *ISO/IEC 27001:2013 Information technology – Security techniques – Information security management systems – Requirements*. ISO