**PERBANDINGAN FRAMEWORK COBIT 2019 DAN NIST *CYBERSECURITY FRAMEWORK* (CSF) 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**

**Imam Satria Hanggara**

**Riski**

Tolong isi nama dan NIM

**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 (National Institute of Standards and Technology) 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 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 yang penting, seperti pengelolaan risiko, manajemen kepatuhan, dan perlindungan data.

Makalah ini bertujuan untuk membandingkan poin-poin yang sama dalam COBIT 2019 dan NIST, dengan fokus pada aspek-aspek utama yang berhubungan dengan tata kelola dan keamanan informasi. Perbandingan dilakukan dengan menganalisis struktur dan pendekatan masing-masing framework dalam hal identifikasi risiko, respons risiko, pengelolaan keamanan, serta pencapaian kepatuhan terhadap regulasi. Hasil dari perbandingan ini menunjukkan bahwa meskipun COBIT 2019 lebih berfokus pada tata kelola TI secara umum, dan NIST lebih pada keamanan siber, keduanya memiliki kesamaan dalam penerapan proses manajemen risiko yang efektif dan perlindungan informasi yang terpadu. Dengan memahami perbandingan ini, organisasi dapat memilih framework yang paling sesuai dengan kebutuhan mereka atau bahkan mengkombinasikan elemen-elemen dari kedua kerangka kerja untuk mencapai pengelolaan TI yang lebih menyeluruh.

Kata Kunci: COBIT 2019, NIST, tata kelola TI, keamanan informasi, NIST, *Cyber Security*

**DAFTAR ISI**

[BAB I 4](#_Toc180430637)

[PENDAHULUAN 4](#_Toc180430638)

[1. Pendahuluan 4](#_Toc180430639)

[2. Rumusan Masalah 4](#_Toc180430640)

[3. Tujuan Pengkajian 5](#_Toc180430641)

[4. Manfaat Pengakajian 5](#_Toc180430642)

[5. Ruang Lingkup Pengkajian 5](#_Toc180430643)

[BAB II 6](#_Toc180430644)

[TINJAUAN PUSTAKA 6](#_Toc180430645)

[2.1 Framework COBIT 2019 6](#_Toc180430646)

[2.2 Framework NIST *Cybersecurity Framework* (CSF) 6](#_Toc180430647)

[Framework NIST *Cybersecurity Framework* (CSF) adalah 6](#_Toc180430648)

[BAB III 7](#_Toc180430649)

[METODE PENELITIAN 7](#_Toc180430650)

[3.1 Pendekatan Penelitian 7](#_Toc180430651)

[3.2 Pengumpulan Data 7](#_Toc180430652)

[3.3 Teknik Analisis Data 7](#_Toc180430653)

[BAB IV 9](#_Toc180430654)

[HASIL PENGKAJIAN DAN PEMBAHASAN 9](#_Toc180430655)

[4.1 Relevansi *framework* COBIT 2019 dan NIST *Cybersecurity Framework* (NIST CSF). 9](#_Toc180430656)

[4.2 Perbedaan *framework* COBIT 2019 dan NIST *Cybersecurity Framework* (NIST CSF) 13](#_Toc180430657)

[BAB V 17](#_Toc180430658)

[KESIMPULAN 17](#_Toc180430659)

[DAFTAR PUSTAKA 18](#_Toc180430660)

# 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. Dalam konteks ini, berbagai framework tata kelola TI dan keamanan informasi seperti COBIT 2019 dan NIST 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 CSF dirancang untuk membantu organisasi meningkatkan kemampuan mereka dalam mencegah, mendeteksi, dan merespons ancaman keamanan siber yang semakin berkembang (NIST, 2020).

Meskipun kedua 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. 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. 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 dan NIST dalam hal tata kelola TI dan manajemen keamanan informasi?
2. Bagaimana kedua framework ini mendukung organisasi dalam mengelola risiko keamanan informasi secara efektif?
3. Apa saja kelebihan dan kekurangan dari penggunaan COBIT 2019 dan NIST dalam konteks penerapan tata kelola dan keamanan informasi?

## Tujuan Pengkajian

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

1. Mengidentifikasi dan membandingkan aspek-aspek utama yang terdapat dalam framework COBIT 2019 dan NIST, terutama terkait tata kelola TI dan keamanan informasi.
2. Menganalisis bagaimana kedua framework ini membantu organisasi dalam mengelola risiko keamanan informasi dan memastikan kepatuhan terhadap regulasi.
3. Mengevaluasi kelebihan dan kekurangan dari kedua framework untuk memberikan rekomendasi kepada organisasi dalam memilih framework yang paling sesuai dengan kebutuhan mereka.

## Manfaat Pengakajian

Tolong disi DISISI

## Ruang Lingkup Pengkajian

Silahkan Disi

# BAB II

# TINJAUAN PUSTAKA

## Framework COBIT 2019

tambahkan

### Framework NIST *Cybersecurity Framework* (CSF)

### Framework NIST *Cybersecurity Framework* (CSF) adalah

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) 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. 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 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 dan NIST.
3. Dokumen resmi dari ISACA mengenai COBIT 2019 dan dokumen NIST CSF dari National Institute of Standards and Technology.

### 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 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. 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. Dalam tahap ini, peneliti juga akan membahas fleksibilitas, kompleksitas penerapan, serta dukungan terhadap tujuan bisnis dan keamanan.

# BAB IV

# HASIL PENGKAJIAN DAN PEMBAHASAN

Penelitian ini 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* (NIST 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* (NIST 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

Jika dibuatkan list secara relevansinya kedua framework ini seperti ini dibawah ini.

* + 1. **Pengelolaan Risiko (Risk Management)**

Baik COBIT 2019 maupun NIST 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.

* + 1. **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.

* + 1. **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.

|  |  |  |
| --- | --- | --- |
| **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. |

Tabel 1.1 Relevansi Cobit 2019 dan NIST CSF

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

|  |  |  |
| --- | --- | --- |
| 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. |

Tabel 1.2 Relevansi Domain Cobit 2019 dengan Kontrol NIST CST

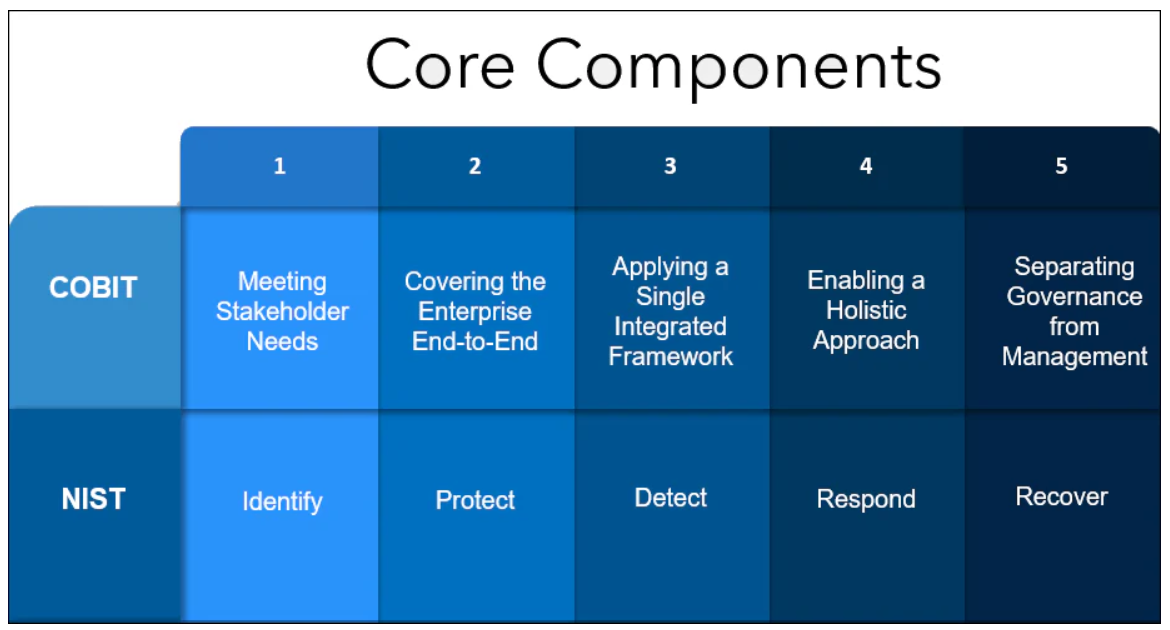
### Perbedaan *framework* COBIT 2019 dan NIST *Cybersecurity Framework* (NIST CSF)

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* (NIST CSF) seperti dibawah ini:

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



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

|  |  |  |
| --- | --- | --- |
| **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. |

Tabel 1.3 framework COBIT 2019 dan NIST Cybersecurity Framework (NIST CSF)

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.

# BAB V

# KESIMPULAN

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

Persamaan

1. MEM01: Mengidentifikasi dan Mengelola Risiko pada NIST ICS1: Inventarisasi Aset yang Sah dan ACS1: Manajemen Kerentanan Berkelanjutan.
2. MEM02: Mengelola Perubahan dengan IR8: Manajemen Perubahan.MEM03: Mengelola Kinerja dengan DCS-1: Penggunaan Software yang Aman

Perbedaan

Tolong ditambahkan

# DAFTAR PUSTAKA

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

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

Jurnal ilmiah dan buku referensi terkait tata kelola TI dan keamanan siber.

Tolong ditambahkan