# CCISO v4 *Overview*: Arah Strategis dan Kepemimpinan Keamanan Siber

**Yulian Sani**
*y.sani@aol.com*



*Certified Chief Information Security Officer* (CCISO) merupakan sertifikasi tingkat eksekutif yang dari EC-Council untuk mempersiapkan para profesional keamanan informasi agar mampu menjalankan peran strategis sebagai pemimpin keamanan siber di tingkat organisasi. Berbeda dengan sertifikasi teknis yang berfokus pada implementasi dan operasional keamanan, CCISO menitikberatkan pada kompetensi tata kelola, manajemen risiko, kepatuhan, kepemimpinan eksekutif, pengelolaan program keamanan, serta pengambilan keputusan strategis yang selaras dengan tujuan bisnis. Seiring dengan perkembangan ancaman siber, transformasi digital, dan kebutuhan organisasi terhadap kepemimpinan keamanan yang semakin berkembang, EC-Council melakukan penyempurnaan terhadap kerangka kompetensi CCISO melalui berbagai pembaruan kurikulum hingga saat ini mencapai versi keempat (CCISO v4).

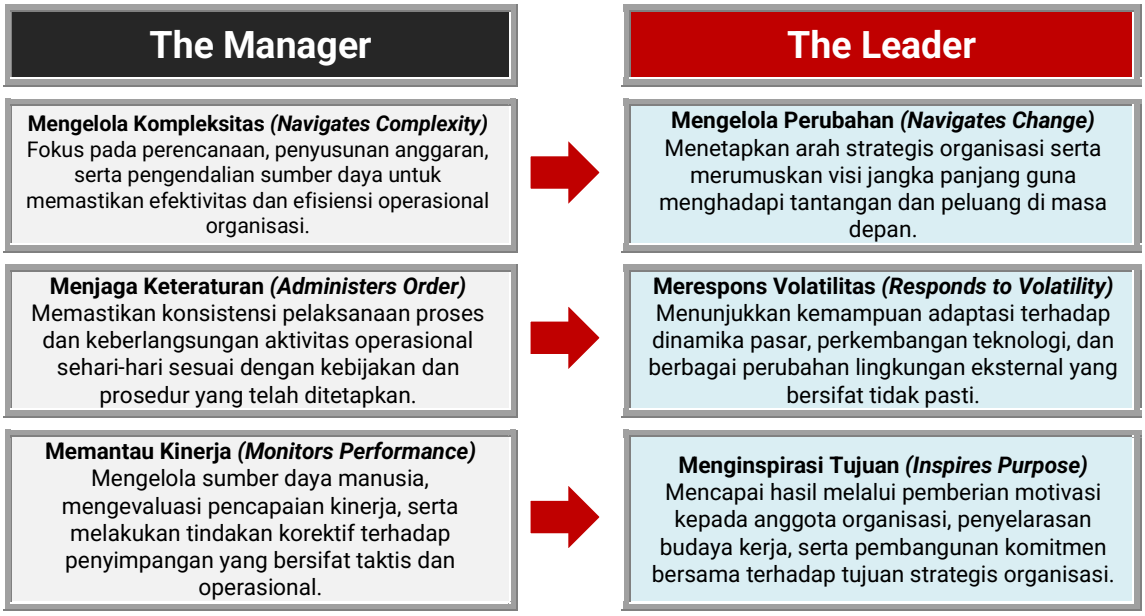
Pada CCISO v4 dijelaskan kerangka kompetensi yang dirancang untuk membentuk kapabilitas kepemimpinan keamanan siber di tingkat eksekutif. Materi ini menekankan transformasi peran seorang pemimpin keamanan informasi dari sekadar mengelola aspek teknis dan operasional keamanan menjadi penggerak strategi, tata kelola, serta visi keamanan organisasi melalui 5 (lima) domain kompetensi utama yang saling terintegrasi, yaitu *Governance*, *Risk* & *Compliance*; *Executive Leadership*; *Security Program Operations; Information Security Core Competencies*; dan *Strategic Vendor* & *Enterprise Management*.

Selain itu, pada versi ini dibahas mengenai integrasi aspek-aspek modern seperti pemanfaatan kecerdasan buatan (*Artificial Intelligence*), pengelolaan risiko pihak ketiga, keamanan lingkungan *cloud* dan *hybrid*, serta peningkatan ketahanan organisasi, sehingga memberikan peta jalan yang komprehensif bagi para eksekutif dalam membangun, mengelola, dan mengembangkan program keamanan informasi yang efektif dan berkelanjutan

# Transformasi Kepemimpinan Eksekutif Keamanan Informasi

Pemimpin keamanan informasi modern (*modern information security leader*) seperti CISO, berperan sebagai penggerak strategis organisasi yang tidak hanya mengelola operasi dan sumber daya keamanan, tetapi juga merumuskan visi dan arah strategis organisasi, memimpin transformasi, serta membangun budaya keamanan yang mendukung pencapaian sasaran bisnis dan ketahanan organisasi.

pergeseran paradigma dari manajer (*manager*) yang berorientasi pada pengelolaan operasional menuju pemimpin (*leader*) yang berorientasi pada kepemimpinan strategis. Perubahan ini menunjukkan bahwa keberhasilan organisasi modern tidak lagi hanya ditentukan oleh kemampuan mengelola sumber daya dan aktivitas operasional, tetapi juga oleh kemampuan untuk mengarahkan perubahan, mengantisipasi dinamika lingkungan, serta membangun komitmen organisasi terhadap tujuan jangka panjang.

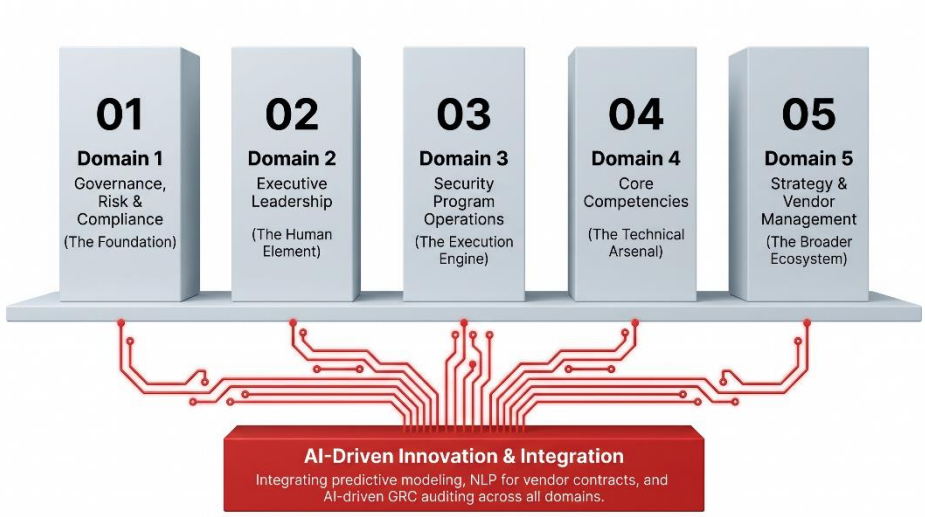



Manajemen dan kepemimpinan memiliki fokus yang berbeda namun saling melengkapi. Manajemen berorientasi pada stabilitas, efisiensi, dan pengendalian operasional, sedangkan kepemimpinan berorientasi pada visi, perubahan, adaptabilitas, dan inspirasi.

Dalam konteks organisasi modern, termasuk bidang keamanan siber dan keamanan informasi, seorang eksekutif tidak cukup hanya memiliki kompetensi manajerial, tetapi juga harus mampu menjalankan peran sebagai pemimpin strategis yang dapat mengarahkan organisasi menghadapi perubahan, ketidakpastian, dan tantangan masa depan.

## 5 Domain Kompetensi di Era *Artificial Intelligence*

Kerangka kompetensi CCISO v4 dirancang sebagai panduan pengembangan kapabilitas bagi profesional keamanan informasi yang dipersiapkan untuk memerankan posisi kepemimpinan strategis di tingkat eksekutif organisasi. Kerangka ini menegaskan bahwa peran *Chief Information Security Officer* (CISO) tidak lagi terbatas pada penguasaan aspek teknis keamanan siber, melainkan mencakup kompetensi yang lebih komprehensif dalam bidang tata kelola, manajemen risiko, kepatuhan, kepemimpinan strategis, operasional keamanan, serta pengelolaan hubungan dengan vendor dan pemangku kepentingan eksternal.




Di dalam model tersebut, terdapat 5 (lima) domain kompetensi utama yang saling terintegrasi.

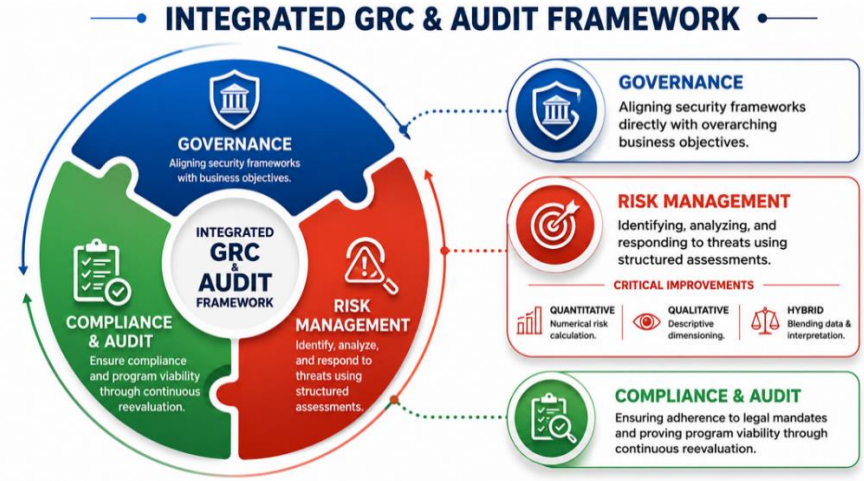
1) Domain pertama adalah *Governance*, Risk and Compliance (GRC) yang menjadi fondasi dalam memastikan bahwa strategi keamanan informasi selaras dengan tujuan bisnis organisasi. Domain ini membahas pengembangan kebijakan keamanan, pengelolaan risiko perusahaan, pemenuhan regulasi, serta penerapan mekanisme pengendalian yang efektif untuk melindungi aset informasi organisasi.
2) Domain kedua adalah *Executive Leadership*, yang menekankan kemampuan seorang pemimpin keamanan informasi dalam mengelola sumber daya manusia, membangun budaya keamanan, memengaruhi pengambilan keputusan strategis, serta berkomunikasi secara efektif dengan manajemen puncak dan/atau dewan direksi. Kompetensi kepemimpinan menjadi faktor penting karena keberhasilan program keamanan informasi sangat bergantung pada dukungan dan komitmen seluruh pemangku kepentingan organisasi.
3) Domain ketiga adalah *Security Program Operations*, yang berfokus pada kemampuan merancang, mengimplementasikan, mengoperasikan, serta mengevaluasi program keamanan informasi secara berkelanjutan. Domain ini mencakup pengelolaan insiden keamanan, pengembangan arsitektur keamanan, pengelolaan keamanan operasional, serta pemantauan efektivitas kontrol keamanan yang diterapkan dalam organisasi.

4) Domain keempat adalah *Core Competencies*, menjelaskan bahwa kompetensi teknis menjadi inti yang harus dimiliki oleh seorang pemimpin keamanan informasi. Kompetensi tersebut meliputi pemahaman mengenai ancaman siber, keamanan jaringan, keamanan aplikasi, keamanan cloud, forensik digital, manajemen kerentanan, serta berbagai aspek teknis lainnya yang menjadi dasar dalam pengambilan keputusan strategis terkait keamanan informasi.
5) Domain kelima adalah *Strategic Vendor and Enterprise Management*, yang menitikberatkan pada kemampuan mengelola hubungan dengan vendor, mitra bisnis, serta pihak ketiga yang memiliki akses terhadap aset informasi organisasi. Domain ini juga mencakup evaluasi risiko pihak ketiga, pengelolaan kontrak, pengawasan kinerja vendor, serta integrasi strategi keamanan ke dalam ekosistem bisnis yang lebih luas.
6) Selain lima domain utama tersebut, pada kerangka kompetensi CCISO v4 menekankan bahwa *AI-Driven Innovation & Integration* menjadi elemen yang mendukung seluruh domain, seperti *predictive modeling*, NLP untuk kontrak vendor, dan *AI-driven* GRC *auditing*.

Kerangka Kompetensi Domain CCISO v4 menekankan bahwa kompetensi seorang CCISO modern harus mencakup keseimbangan antara kemampuan teknis, manajerial, dan strategis. Melalui pemahaman terhadap lima domain kompetensi yang didukung oleh pemanfaatan teknologi AI, seorang pemimpin keamanan informasi diharapkan mampu berperan sebagai mitra strategis bisnis yang tidak hanya melindungi organisasi dari ancaman siber, tetapi juga mendukung pencapaian tujuan dan keberlanjutan organisasi secara menyeluruh.

## Domain 01: *Governance, Risk, and Compliance* (GRC)

Pada domain ini dijelaskan bahwa *Governance*, *Risk*, *and Compliance* (GRC) merupakan fondasi utama dalam membangun dan mengelola program keamanan informasi yang efektif di tingkat organisasi. Dalam kerangka CCISOv4, GRC ditempatkan sebagai domain pertama karena seluruh aktivitas keamanan informasi harus berlandaskan pada tata kelola yang baik, pengelolaan risiko yang terstruktur, serta kepatuhan terhadap peraturan dan standar yang berlaku.



Ketiga komponen tersebut digambarkan sebagai roda gigi (*gear*) yang saling terhubung, menunjukkan bahwa keberhasilan keamanan informasi hanya dapat dicapai apabila *governance*, *risk management*, dan *compliance* bekerja secara terintegrasi dan berkesinambungan.

1. Komponen pertama, yaitu Tata Kelola (*Governance*), berfungsi sebagai mekanisme untuk menyelaraskan strategi keamanan informasi dengan tujuan dan sasaran bisnis organisasi. Tata kelola memastikan bahwa seluruh kebijakan, standar, prosedur, serta investasi keamanan yang dilakukan organisasi memberikan nilai tambah bagi pencapaian tujuan bisnis. Dalam konteks ini, keamanan informasi tidak dipandang sebagai fungsi teknis semata, melainkan sebagai bagian dari strategi organisasi yang mendukung keberlangsungan operasional, perlindungan aset, serta penciptaan keunggulan kompetitif. Melalui tata kelola yang efektif, manajemen puncak dapat memastikan bahwa keputusan terkait keamanan informasi selaras dengan arah strategis perusahaan, toleransi risiko, dan kebutuhan para pemangku kepentingan.

2. Komponen kedua adalah Manajemen Risiko (*Risk Management*), yang berfokus pada proses identifikasi, analisis, evaluasi, dan penanganan risiko yang dapat memengaruhi keamanan informasi organisasi. Bagian ini menjelaskan bahwa proses penilaian risiko dapat dilakukan melalui tiga pendekatan utama, yaitu:
   a. Pendekatan kuantitatif (*quantitative assessment*) yang menggunakan data numerik dan metode perhitungan untuk mengukur tingkat risiko secara objektif. Pendekatan ini umumnya digunakan untuk menghitung potensi kerugian finansial, probabilitas terjadinya insiden, atau dampak bisnis yang mungkin timbul akibat suatu ancaman.
   b. Pendekatan kualitatif (*qualitative assessment*) yang menggunakan penilaian berbasis observasi, pengalaman, dan pertimbangan profesional untuk mengategorikan tingkat risiko ke dalam skala tertentu, seperti rendah, sedang, atau tinggi.
   c. Pendekatan hibrida (*hybrid assessment*) yang menggabungkan unsur kuantitatif dan kualitatif guna menghasilkan pemahaman risiko yang lebih komprehensif dan akurat. Pendekatan hibrida dianggap mampu memberikan gambaran yang lebih realistis mengenai kondisi risiko organisasi karena mempertimbangkan baik data objektif maupun konteks bisnis yang relevan.

3. Komponen ketiga adalah Compliance and Audit (Kepatuhan dan Audit) yang berperan dalam memastikan bahwa organisasi mematuhi berbagai persyaratan hukum, regulasi, standar industri, serta kebijakan internal yang berlaku. Kepatuhan menjadi aspek yang sangat penting karena kegagalan memenuhi ketentuan yang ditetapkan dapat mengakibatkan sanksi hukum, kerugian finansial, maupun penurunan reputasi organisasi. Selain memastikan kepatuhan, fungsi audit juga berperan dalam melakukan evaluasi secara berkala terhadap efektivitas program keamanan informasi yang telah diterapkan. Melalui audit yang berkesinambungan, organisasi dapat mengidentifikasi kelemahan pengendalian, mengukur tingkat kematangan keamanan informasi, serta memastikan bahwa program keamanan tetap relevan terhadap perubahan ancaman, teknologi, dan kebutuhan bisnis.

Selain 3 komponen utama tersebut, terdapat siklus *Audit Management* yang mengelilingi ketiga komponen utama GRC. Representasi tersebut menegaskan bahwa tata kelola, manajemen risiko, dan kepatuhan bukanlah aktivitas yang dilakukan satu kali, melainkan merupakan proses berkelanjutan yang harus dievaluasi dan ditingkatkan secara terus-menerus. Audit berfungsi sebagai mekanisme umpan balik (*feedback mechanism*) yang memungkinkan organisasi melakukan perbaikan berkelanjutan (*continuous improvement*) terhadap seluruh aspek keamanan informasi.

Domain ini menegaskan bahwa GRC merupakan fondasi strategis yang memungkinkan organisasi membangun program keamanan informasi yang selaras dengan tujuan bisnis, mampu mengelola risiko secara efektif, serta memenuhi seluruh kewajiban kepatuhan yang berlaku. Integrasi ketiga elemen tersebut menjadi faktor kunci dalam menciptakan ketahanan organisasi terhadap ancaman siber sekaligus mendukung keberlangsungan dan pertumbuhan bisnis dalam jangka panjang.

## Domain 02: Kepemimpinan & Pengaruh Strategis (*Executive Leadership)*

Pada domain ke-2 menjelaskan bahwa salah satu kompetensi utama yang harus dimiliki oleh seorang CISO adalah kemampuan dalam mengelola dan menerapkan berbagai bentuk kewenangan (*power*) serta pengaruh (*influence*) dalam lingkungan organisasi. Dalam konteks kepemimpinan eksekutif, keberhasilan program keamanan informasi tidak hanya ditentukan oleh kemampuan teknis dan pemahaman terhadap ancaman siber, tetapi juga oleh kemampuan seorang pemimpin untuk memengaruhi perilaku, keputusan, dan komitmen para pemangku kepentingan di seluruh tingkatan organisasi.


CISO berperan sebagai pusat pengaruh dalam organisasi yang memiliki akses terhadap berbagai sumber kewenangan yang dapat digunakan untuk mendukung pencapaian tujuan keamanan informasi. Hal tersebut menunjukkan bahwa efektivitas kepemimpinan seorang CISO bergantung pada kemampuan menyeimbangkan penggunaan berbagai jenis kewenangan atau otoritas secara tepat sesuai dengan situasi, budaya organisasi, dan tujuan yang ingin dicapai.

1. **Kewenangan yang sah (*Legitimate Power*)**, yaitu perintah yang berasal dari posisi formal seseorang dalam struktur organisasi. Sebagai pejabat yang bertanggung jawab atas keamanan informasi, seorang CISO memiliki kewenangan resmi untuk menetapkan kebijakan, mengarahkan implementasi kontrol keamanan, serta memastikan kepatuhan terhadap standar dan regulasi yang berlaku. Kewenangan legitimasi memberikan dasar hukum dan administratif bagi seorang pemimpin untuk mengambil keputusan serta mengoordinasikan aktivitas keamanan di seluruh unit organisasi.
2. **Kewenangan Ahli (*Expert Power*)** yang diperoleh melalui pengetahuan, keterampilan, pengalaman, dan kompetensi profesional yang dimiliki seseorang. Dalam bidang keamanan siber yang sangat kompleks dan dinamis, kewenangan keahlian sering kali menjadi sumber pengaruh yang paling penting bagi seorang CISO. Pemangku kepentingan cenderung mempercayai dan mengikuti arahan seorang pemimpin yang memiliki pemahaman mendalam mengenai ancaman siber, teknologi keamanan, manajemen risiko, dan praktik terbaik industri. Oleh karena itu, pengembangan kompetensi profesional secara berkelanjutan menjadi faktor penting dalam membangun kredibilitas kepemimpinan.
3. **Kewenangan Referensi (*Referent Power*)**, yaitu kewenangan yang muncul karena rasa hormat, kepercayaan, dan pengakuan yang diberikan oleh orang lain. Kekuasaan ini tidak berasal dari jabatan maupun keahlian teknis semata, melainkan dari karakter, integritas, dan kemampuan interpersonal seorang pemimpin. Seorang CISO yang mampu membangun hubungan positif dengan manajemen, karyawan, regulator, dan mitra bisnis akan lebih mudah memperoleh dukungan terhadap inisiatif keamanan informasi yang dijalankan. *Referent power* menjadi sangat penting dalam membangun budaya keamanan yang kuat karena mendorong keterlibatan sukarela dari seluruh anggota organisasi.
4. **Kewenangan Penghargaan (*Reward Power*)**, yaitu kemampuan untuk memberikan insentif, penghargaan, atau pengakuan kepada individu maupun kelompok yang menunjukkan perilaku sesuai dengan tujuan organisasi. Dalam konteks keamanan informasi, penghargaan dapat diberikan kepada unit kerja yang berhasil memenuhi target kepatuhan, menerapkan praktik keamanan terbaik, atau berkontribusi dalam peningkatan keamanan organisasi. Penggunaan reward power secara efektif dapat meningkatkan motivasi, partisipasi, dan kesadaran keamanan di seluruh organisasi.
5. **Kewenangan Koersif (*Coercive Power*)**, yaitu kemampuan untuk menerapkan sanksi, pembatasan, atau konsekuensi terhadap individu yang melanggar kebijakan dan ketentuan organisasi. Dalam keamanan informasi, kewenangan koersif dapat diwujudkan melalui tindakan disipliner, pembatasan akses, atau penerapan konsekuensi terhadap pelanggaran keamanan yang dilakukan oleh karyawan maupun pihak ketiga. Meskipun diperlukan dalam kondisi tertentu, penggunaan kewenangan koersif harus dilakukan secara proporsional dan hati-hati karena berpotensi menimbulkan resistensi, menurunkan motivasi, dan mengurangi kepercayaan apabila diterapkan secara berlebihan.

Selain menjelaskan berbagai bentuk kewenangan, bagian ini juga menekankan pentingnya Pengawasan Etis (*Ethical Oversight*) sebagai landasan dalam penggunaan kewenangan organisasi. Pengawasan etis berfungsi untuk memastikan bahwa seluruh bentuk pengaruh dan

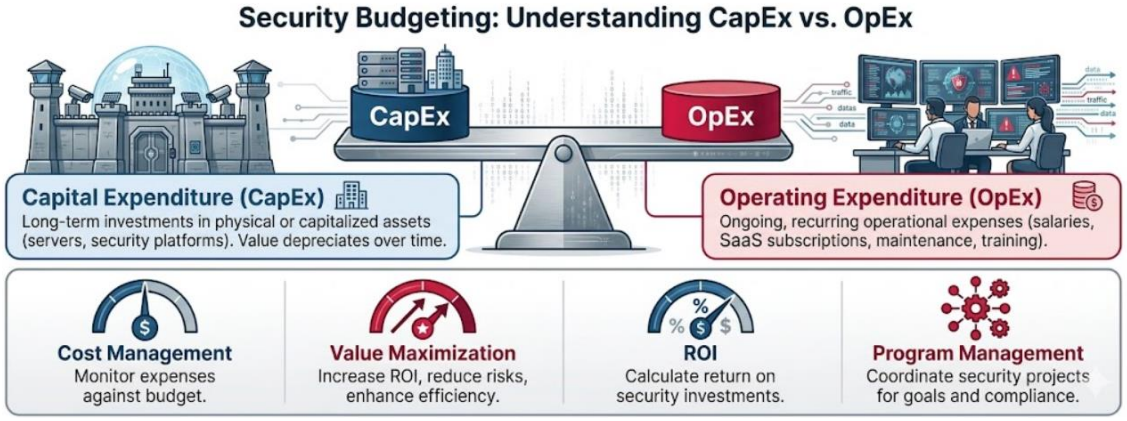
kewenangan digunakan secara transparan, bertanggung jawab, dan sesuai dengan prinsip-prinsip etika organisasi. Melalui pengawasan etis, organisasi dapat mencegah penyalahgunaan wewenang, praktik pemaksaan yang tidak proporsional, konflik kepentingan, serta perilaku yang dapat merusak kepercayaan pemangku kepentingan. Dengan demikian, penggunaan kewenangan tidak hanya bertujuan mencapai kepatuhan, tetapi juga membangun kepercayaan dan legitimasi jangka panjang.

Domain 2 menekankan bahwa kepemimpinan keamanan informasi yang efektif membutuhkan kombinasi antara kewenangan formal, kompetensi profesional, kemampuan membangun hubungan, mekanisme penghargaan, dan penegakan disiplin yang didukung oleh prinsip-prinsip etika. Integrasi berbagai sumber kewenangan tersebut memungkinkan seorang CISO menjalankan perannya sebagai pemimpin strategis yang mampu memengaruhi organisasi secara positif dalam mencapai tujuan keamanan informasi dan bisnis.

## Domain 03: Operasi dan Investasi Keamanan Informasi

Domain ini menjelaskan bahwa salah satu tanggung jawab utama seorang CISO adalah dapat menjelaskan kebutuhan keamanan siber ke dalam perspektif finansial yang dapat dipahami dan diterima oleh manajemen serta pemangku kepentingan organisasi.

Dalam praktiknya, berbagai inisiatif keamanan informasi sering kali memerlukan investasi yang signifikan, sehingga seorang pemimpin keamanan harus mampu menunjukkan hubungan yang jelas antara kebutuhan keamanan, biaya yang dikeluarkan, risiko yang dapat dikurangi, serta manfaat bisnis yang diperoleh. Seorang CISO harus dapat mengukur peluang keberhasilan program keamanan informasi yang tidak hanya ditentukan oleh efektivitas kontrol keamanan yang diterapkan, tetapi juga oleh kemampuan untuk mengelola investasi, anggaran, dan nilai bisnis yang dihasilkan dari investasi tersebut.




Pada gambar di atas, digambarkan konsep keseimbangan antara *Capital Expenditure* (CapEx) dan *Operating Expenditure* (OpEx) sebagai dua kategori utama pengeluaran yang harus dikelola dalam program keamanan informasi. Keseimbangan tersebut menunjukkan bahwa pengelolaan keamanan informasi memerlukan kombinasi investasi jangka panjang dan biaya operasional berkelanjutan agar tujuan keamanan dan bisnis dapat tercapai secara optimal.

### 1. *Capital Expenditure* (CapEx)

*Capital Expenditure* (CapEx) merupakan pengeluaran yang digunakan untuk memperoleh, membangun, atau meningkatkan aset yang memiliki manfaat jangka panjang bagi organisasi. Dalam konteks keamanan informasi, CapEx biasanya mencakup investasi pada infrastruktur keamanan, perangkat keras, perangkat lunak strategis, pusat data, platform keamanan tingkat perusahaan, maupun proyek transformasi keamanan yang memiliki umur manfaat lebih dari satu periode akuntansi. Contoh pengeluaran CapEx terkait pekerjaan keamanan informasi meliputi:

- Implementasi *Security Information and Event Management* (SIEM);
- Pengadaan perangkat *firewall* generasi terbaru;
- Pembangunan *Security Operations Center* (SOC);
- Implementasi *Data Loss Prevention* (DLP);
- Pengembangan infrastruktur keamanan *cloud*;
- Modernisasi arsitektur keamanan perusahaan.

Karakteristik utama CapEx adalah bahwa investasi tersebut dicatat sebagai aset dan nilainya akan mengalami penyusutan (*depreciation*) selama masa manfaatnya. Oleh karena itu, keputusan terkait CapEx umumnya memerlukan analisis yang lebih mendalam karena melibatkan komitmen investasi jangka panjang dan alokasi dana yang relatif besar.

### 2. *Operating Expenditure* (OpEx)

*Operating Expenditure* (OpEx) merupakan biaya operasional yang dikeluarkan secara rutin untuk mendukung aktivitas organisasi sehari-hari. Berbeda dengan CapEx yang berorientasi pada aset jangka panjang, OpEx lebih berfokus pada biaya yang diperlukan untuk mempertahankan operasional keamanan secara berkelanjutan.

Beberapa contoh pengeluaran OpEx terkait pekerjaan keamanan informasi meliputi:

- Biaya lisensi perangkat lunak berbasis langganan (*subscription*);
- Layanan *Software as a Service* (SaaS);
- Gaji dan tunjangan personel keamanan informasi;
- Pelatihan dan pengembangan kompetensi pegawai;
- Kontrak pemeliharaan sistem keamanan;
- Managed Security Services;
- Biaya audit dan kepatuhan.

Pengeluaran OpEx bersifat berulang dan langsung dibebankan pada periode berjalan. Oleh karena itu, pengelolaan OpEx memerlukan pengawasan yang ketat untuk memastikan bahwa biaya yang dikeluarkan tetap sejalan dengan anggaran organisasi dan menghasilkan manfaat yang sepadan.

### 3. *Cost Management*

*Cost Management* mengacu pada proses perencanaan, pemantauan, pengendalian, dan evaluasi seluruh biaya yang terkait dengan program keamanan informasi. Dalam konteks ini, seorang CISO harus mampu:

- Menyusun anggaran keamanan informasi;
- Memprioritaskan investasi berdasarkan tingkat risiko;
- Mengendalikan pengeluaran agar tidak melebihi anggaran yang disetujui;
- Mengidentifikasi peluang efisiensi biaya;
- Menyeimbangkan kebutuhan keamanan dengan keterbatasan sumber daya organisasi.

*Cost management* menjadi penting karena organisasi umumnya memiliki sumber daya yang terbatas, sehingga setiap investasi keamanan harus dilakukan secara selektif dan berdasarkan pertimbangan risiko yang rasional.

### 4. *Value Maximization*

*Value Maximization* adalah upaya memaksimalkan nilai bisnis yang diperoleh dari setiap investasi keamanan informasi. Pendekatan ini menunjukkan bahwa tujuan utama investasi keamanan bukan sekadar membeli teknologi atau memenuhi kewajiban kepatuhan, melainkan menciptakan nilai yang nyata bagi organisasi.
Nilai tersebut dapat diwujudkan melalui:

- Pengurangan kemungkinan terjadinya insiden keamanan;
- Penurunan potensi kerugian finansial;
- Peningkatan efisiensi operasional;
- Perlindungan reputasi organisasi;
- Peningkatan kepercayaan pelanggan;
- Dukungan terhadap inovasi dan transformasi digital.

Dengan demikian, keberhasilan investasi keamanan tidak hanya diukur dari jumlah kontrol yang diterapkan, tetapi juga dari kontribusinya terhadap pencapaian tujuan bisnis organisasi.

### 5. *Return on Investment (*ROI)

*Return on Investment* (ROI) dilakukan untuk mengevaluasi sejauh mana investasi yang dilakukan mampu menghasilkan manfaat yang sebanding dengan biaya yang telah dikeluarkan. Dalam konteks keamanan siber, pengukuran ROI sering kali dilakukan melalui:

- Pengurangan potensi kerugian akibat insiden keamanan;
- Penurunan biaya pemulihan pasca-insiden;
- Efisiensi operasional yang dihasilkan oleh otomatisasi;
- Peningkatan produktivitas sumber daya manusia;
- Pengurangan risiko hukum dan regulasi.

Bagi seorang CISO, kemampuan menjelaskan ROI sangat penting karena keputusan investasi keamanan sering kali harus mendapatkan persetujuan dari manajemen puncak maupun dewan direksi yang lebih berorientasi pada perspektif bisnis dan finansial.

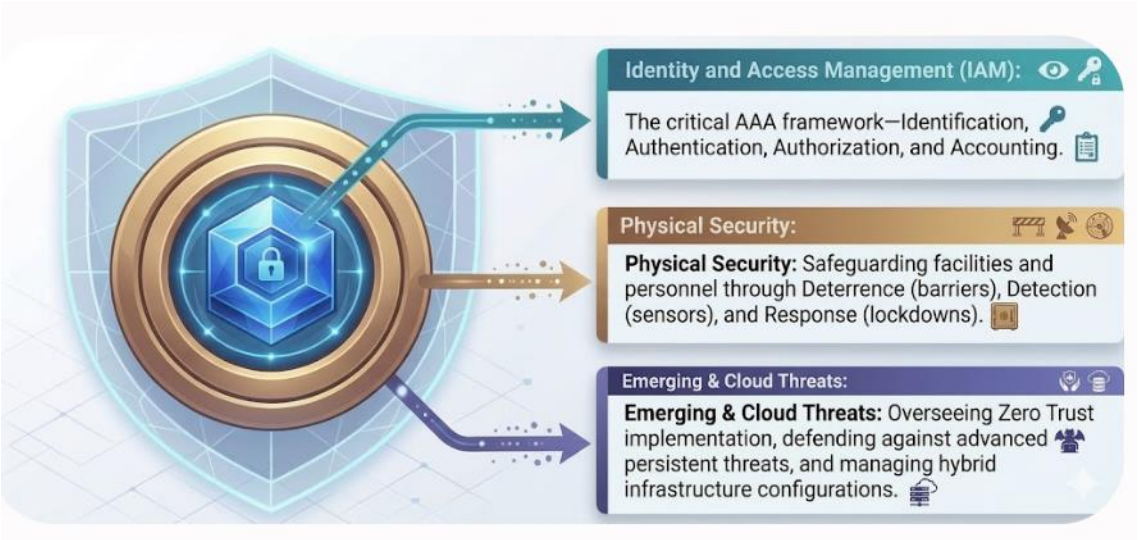
**6. Program Management**

*Program management* merupakan proses mengelola berbagai proyek keamanan yang saling terkait agar dapat mendukung pencapaian tujuan strategis organisasi secara terintegrasi. Berbeda dengan manajemen proyek yang berfokus pada satu inisiatif tertentu, program management berorientasi pada koordinasi beberapa proyek sekaligus untuk menghasilkan manfaat bisnis yang lebih besar. Dalam keamanan informasi, program management dapat mencakup pengelolaan berbagai inisiatif seperti implementasi *Zero Trust*, peningkatan keamanan *cloud*, modernisasi SOC, peningkatan kepatuhan regulasi, dan penguatan kesadaran keamanan pengguna.

Melalui pendekatan *program management*, organisasi dapat memastikan bahwa seluruh investasi keamanan berjalan secara selaras, menggunakan sumber daya secara efisien, serta tetap mematuhi batasan anggaran yang telah ditetapkan. Secara keseluruhan, halaman ini menegaskan bahwa seorang CISO modern harus memiliki kemampuan bisnis dan finansial yang kuat. Keamanan informasi tidak lagi dipandang sebagai fungsi teknis semata, tetapi sebagai investasi strategis yang harus mampu menghasilkan nilai, mendukung tujuan organisasi, mengurangi risiko, dan memberikan manfaat yang terukur bagi keberlangsungan bisnis.

## Domain 04: Kompetensi Keamanan Informasi

Domain keempat dalam kerangka CCISOv4 berfokus pada *Information Security Core* ***Competencies***, yaitu kompetensi utama yang menjadi fondasi bagi pengelolaan keamanan informasi organisasi. Berbeda dengan peran teknis operasional yang terlibat secara langsung dalam implementasi teknologi keamanan, seorang CISO diharapkan memiliki kemampuan untuk melakukan pengawasan strategis (*strategic oversight*) terhadap berbagai fungsi keamanan inti guna memastikan bahwa seluruh kontrol keamanan berjalan secara efektif dan selaras dengan kebutuhan bisnis.




Ilustrasi berbentuk perisai (*shield*) pada slide menggambarkan bahwa kompetensi utama keamanan informasi berfungsi sebagai lapisan perlindungan utama bagi organisasi. Perisai tersebut menunjukkan bahwa keamanan organisasi dibangun melalui berbagai lapisan kontrol

yang saling melengkapi, mulai dari pengelolaan identitas, perlindungan fisik, hingga pengamanan terhadap ancaman modern yang muncul akibat transformasi digital dan adopsi teknologi *cloud*. Pendekatan berlapis ini mencerminkan prinsip defense-in-depth yang menjadi salah satu konsep fundamental dalam keamanan informasi modern.

**1. *Identity and Access Management* (IAM)**

IAM merupakan salah satu komponen paling penting dalam keamanan informasi karena berfungsi untuk memastikan bahwa hanya individu yang berwenang yang dapat mengakses sumber daya organisasi sesuai dengan hak akses yang diberikan. IAM dibangun berdasarkan kerangka AAA (*Authentication*, *Authorization*, *and Accounting*) yang mencakup:

**a. *Identification***

*Identification* merupakan proses pengenalan identitas pengguna sebelum diberikan akses ke sistem atau sumber daya tertentu. Pada tahap ini, pengguna menyatakan identitasnya melalui username, nomor pegawai, alamat email, atau identitas digital lainnya.

**b. *Authentication***

*Authentication* merupakan proses verifikasi bahwa identitas yang diklaim oleh pengguna benar-benar sah. Proses ini dapat dilakukan menggunakan berbagai mekanisme seperti:

- *Password* atau *passphrase*;
- *Multi-Factor Authentication* (MFA);
- Biometrik (sidik jari, pengenalan wajah, iris mata);
- *Smart card* atau token keamanan;
- Sertifikat digital (*digital certificates*)

**c. *Authorization***

*Authorization* merupakan proses penentuan hak akses yang dimiliki pengguna setelah identitasnya berhasil diverifikasi. Prinsip yang umum digunakan adalah ***Least Privilege Principle***, yaitu memberikan hak akses minimum yang diperlukan untuk melaksanakan tugas pekerjaan. Melalui mekanisme ini organisasi dapat:

- Membatasi akses terhadap data sensitif;
- Mengurangi risiko insider threat;
- Mencegah penyalahgunaan hak akses;
- Mendukung kepatuhan terhadap regulasi keamanan informasi.

**d. *Accounting***

*Accounting* mengacu pada proses pencatatan dan Monitoring aktivitas pengguna dalam sistem. Aktivitas tersebut disimpan dalam bentuk *log* yang dapat digunakan untuk:

- Audit keamanan;
- Investigasi insiden;
- Pemantauan kepatuhan;
- Analisis perilaku pengguna;
- Forensik digital.

Dari perspektif strategis, CISO harus memastikan bahwa kebijakan IAM diterapkan secara konsisten di seluruh organisasi karena sebagian besar insiden keamanan modern berkaitan dengan penyalahgunaan atau kebocoran identitas digital.

**2. Keamanan Fisik (*Physical Security*)**

Kompetensi kedua yang dijelaskan adalah *Physical Security*, yaitu perlindungan terhadap fasilitas, aset fisik, infrastruktur teknologi informasi, dan personel organisasi dari ancaman fisik yang dapat mengganggu operasional bisnis. *Physical Security* dibangun berdasarkan 3 (tiga) komponen utama:

**a. Pencegahan (*Deterrence*)**

*Deterrence* bertujuan mencegah individu melakukan tindakan yang dapat mengancam keamanan organisasi. Bentuk kontrol *deterrence* meliputi:

- Pagar pengaman;
- Gerbang akses;
- Petugas keamanan;
- Kamera CCTV yang terlihat jelas;
- Tanda peringatan keamanan.

Kontrol ini berfungsi sebagai proteksi awal yang berfungsi untuk menghambat dan dapat mengurangi niat pelaku untuk melakukan pelanggaran.

**b. Deteksi (*Detection*)**

*Detection* bertujuan mengidentifikasi aktivitas yang mencurigakan atau tidak sah sesegera mungkin. Mekanisme deteksi dapat berupa:

- Sensor gerak;
- Alarm keamanan;
- Sistem pemantauan video;
- Sensor pintu dan jendela;
- Sistem pemantauan lingkungan pusat data.

Kemampuan deteksi yang cepat memungkinkan organisasi merespons ancaman sebelum menimbulkan dampak yang lebih besar.

**c. Respons (*Response*)**

Response merupakan tindakan yang dilakukan setelah ancaman terdeteksi. Contohnya meliputi:

- *Lockdown* area tertentu;
- Aktivasi prosedur tanggap darurat;
- Evakuasi personel;
- Intervensi petugas keamanan;
- Isolasi fasilitas yang terdampak.

*Physical Security* memiliki peran yang sangat penting karena kegagalan pengamanan fisik dapat mengakibatkan kompromi terhadap infrastruktur IT, sistem digital, perangkat keras, maupun data organisasi.

### 3. Ancaman Siber Terkini dan Ancaman Cloud (*Emerging and Cloud Threats*)

***Emerging and Cloud Threats*** merupakan kemampuan organisasi untuk menghadapi ancaman keamanan yang terus berkembang akibat kemajuan teknologi, transformasi digital, serta penggunaan lingkungan *cloud* dan *hybrid infrastructure*. Beberapa area utama yang menjadi bagian perhatian pada bagian ini misalnya:

#### a. Zero Trust Implementation

*Zero Trust* merupakan pendekatan keamanan modern yang didasarkan pada prinsip *"never trust, always verify"*. Model ini mengasumsikan bahwa tidak ada pengguna, perangkat, maupun sistem yang dapat dipercaya secara otomatis meskipun berada di dalam jaringan organisasi. Implementasi *Zero Trust* mencakup:

- Verifikasi identitas berkelanjutan;
- Segmentasi jaringan;
- Kontrol akses berbasis risiko;
- Monitoring aktivitas secara *real-time*.

#### b. *Advanced Persistent Threats* (APT)

APT merupakan serangan siber yang dilakukan secara terencana, tersembunyi, dan berjangka panjang oleh kelompok yang memiliki kemampuan tinggi. Tujuan APT umumnya adalah pencurian data, spionase, sabotase, atau akses jangka panjang ke lingkungan organisasi. Karakteristik APT meliputi:

- Persistensi yang tinggi;
- Teknik penghindaran deteksi;
- Pemanfaatan berbagai kerentanan secara berlapis;
- Target yang spesifik dan bernilai tinggi.

#### c. *Hybrid Infrastructure Security*

Banyak organisasi modern mengoperasikan kombinasi infrastruktur *on-premises* dan *cloud*. Lingkungan *hybrid* ini meningkatkan fleksibilitas bisnis, tetapi juga memperluas permukaan serangan (*attack surface*). Oleh karena itu, organisasi harus memastikan:

- Konfigurasi *cloud* yang aman;
- Integrasi kontrol keamanan lintas *platform*;
- Monitoring terpadu;
- Pengelolaan identitas yang konsisten;
- Kepatuhan terhadap regulasi keamanan data.

Dalam konteks ini, peran CISO bukan melakukan konfigurasi teknis secara langsung, melainkan memastikan bahwa strategi, kebijakan, sumber daya, dan investasi keamanan telah memadai untuk menghadapi ancaman yang terus berkembang.

Seorang CISO harus memiliki pemahaman strategis yang kuat terhadap kompetensi inti keamanan informasi, khususnya dalam pengelolaan identitas dan akses, perlindungan fisik, serta pengamanan terhadap ancaman modern dan lingkungan *cloud*. Penguasaan terhadap ketiga area tersebut memungkinkan organisasi membangun pertahanan keamanan yang komprehensif, berlapis, dan mampu beradaptasi terhadap dinamika ancaman siber yang semakin kompleks.

## Domain 05: Manajemen Vendor dan Enterprise Strategis

Domain ini menjelaskan bahwa salah satu tanggung jawab strategis seorang *Chief Information Security Officer* (CISO) adalah memastikan bahwa keamanan informasi diterapkan secara konsisten tidak hanya di dalam organisasi, tetapi juga pada seluruh pihak eksternal yang terlibat dalam rantai nilai bisnis. Dalam lingkungan bisnis digital saat ini, organisasi semakin bergantung pada vendor, penyedia layanan *cloud*, konsultan, mitra teknologi, dan berbagai pihak ketiga lainnya. Ketergantungan tersebut memberikan manfaat berupa efisiensi operasional dan percepatan inovasi, namun pada saat yang sama juga meningkatkan risiko keamanan informasi yang berasal dari luar organisasi.

Pada bagian ini dijelaskan hubungan antara 3 (tiga) komponen utama, yaitu *Enterprise Architecture* (EA), *Third-Party Attestation*, dan *Third-Party Vendors*.


Ketiga aspek tersebut membentuk suatu kerangka yang memungkinkan organisasi mengintegrasikan kebutuhan bisnis dengan pengendalian keamanan serta pengelolaan risiko pihak ketiga secara terstruktur.

### 1. *Enterprise Architecture* (EA)

Komponen pertama yang dijelaskan adalah *Enterprise Architecture* (EA). *Enterprise Architecture* merupakan kerangka yang digunakan untuk memetakan hubungan antara strategi bisnis, proses bisnis, aplikasi, data, teknologi, dan kontrol keamanan dalam suatu organisasi.

Dalam konteks tata kelola keamanan informasi, EA berperan dalam memetakan dan mengintegrasikan kontrol detektif ke dalam proses bisnis secara rinci sehingga keamanan dapat memberikan nilai tambah bagi organisasi melalui dukungan terhadap keberlangsungan operasional bisnis, bukan menjadi faktor yang menghambat inovasi maupun proses bisnis.

Dalam perspektif EA, keamanan informasi tidak ditempatkan sebagai fungsi yang berdiri sendiri, melainkan sebagai bagian yang terintegrasi pada seluruh proses bisnis organisasi. Oleh karena itu, setiap aktivitas bisnis harus memiliki kontrol keamanan yang sesuai dengan tingkat risiko yang dihadapi. Integrasi keamanan ke dalam EA memberikan beberapa manfaat penting, antara lain:

- Memastikan keselarasan antara strategi keamanan dan strategi bisnis;
- Mengurangi konflik antara kebutuhan operasional dan persyaratan keamanan;
- Mempermudah identifikasi titik risiko dalam proses bisnis;
- Mendukung pengambilan keputusan berbasis risiko;
- Memastikan keamanan diterapkan secara konsisten pada seluruh unit organisasi.

Dalam hal ini, pemahaman terhadap *Enterprise Architecture* menjadi sangat penting karena berbagai keputusan terkait teknologi, transformasi digital, migrasi *cloud*, dan integrasi sistem harus mempertimbangkan dampaknya terhadap keamanan informasi secara menyeluruh.

### 2. *Third-Party Attestation*

*Attestation* merupakan proses validasi atau pembuktian independen yang digunakan untuk menilai apakah suatu vendor telah menerapkan kontrol keamanan yang memadai. Dalam praktiknya, organisasi tidak dapat hanya mengandalkan pernyataan vendor mengenai tingkat keamanan yang dimilikinya. Diperlukan bukti objektif yang dapat diverifikasi untuk memastikan bahwa vendor benar-benar menerapkan pengendalian keamanan sesuai standar yang diharapkan. Oleh karena itu, dalam hal ini ditekankan pentingnya penggunaan berbagai bentuk verifikasi independen, misalnya:

#### a. SOC 2 *Report*

SOC 2 (*System and Organization Controls 2*) merupakan laporan audit independen yang mengevaluasi efektivitas kontrol keamanan, ketersediaan layanan, integritas pemrosesan, kerahasiaan, dan privasi suatu organisasi penyedia layanan.
Laporan SOC 2 sering digunakan sebagai dasar penilaian keamanan bagi vendor teknologi, penyedia *cloud*, maupun perusahaan yang mengelola data pelanggan.

#### b. ISO/IEC 27001 Certification

ISO/IEC 27001 merupakan standar internasional yang mengatur persyaratan Sistem Manajemen Keamanan Informasi (*Information Security Management System*/ISMS).
Sertifikasi ini menunjukkan bahwa organisasi telah menerapkan proses yang sistematis untuk:

- Mengidentifikasi risiko keamanan;
- Mengimplementasikan kontrol keamanan;
- Melakukan evaluasi berkala;
- Meningkatkan efektivitas keamanan secara berkelanjutan.

**c. PCI-DSS**

*Payment Card Industry Data Security Standard* (PCI-DSS) merupakan standar keamanan yang dirancang untuk melindungi data kartu pembayaran. Standar ini sangat penting bagi organisasi yang memproses, menyimpan, atau mentransmisikan data kartu kredit dan debit. Melalui berbagai mekanisme *attestation* tersebut, organisasi dapat memperoleh keyakinan yang lebih tinggi bahwa *vendor* telah menerapkan kontrol keamanan yang memadai dan sesuai dengan standar industri yang berlaku.

**3. Vendor pihak ketiga *(Third-Party Vendors)***

Vendor pihak ketiga yaitu seluruh pihak eksternal yang menyediakan produk, layanan, infrastruktur, atau dukungan operasional bagi organisasi. Bagian ini menjelaskan bahwa pengelolaan vendor harus dilakukan melalui *Vendor Management Framework* yang mencakup:

- Pengawasan (*Oversight*);
- Kontrol kontraktual (*Contractual Controls*);
- Pemantauan berkelanjutan (*Continuous monitoring*).

**a. Pengawasan (*Oversight)***

*Oversight* mengacu pada proses pengawasan terhadap aktivitas vendor untuk memastikan bahwa layanan yang diberikan tetap memenuhi persyaratan keamanan dan kepatuhan yang telah disepakati. Pengawasan dapat dilakukan melalui:

- Audit vendor;
- Penilaian risiko berkala;
- Tinjauan kepatuhan;
- Evaluasi kinerja keamanan.

**b. Kontrol Kontraktual (*Contractual Controls*)**

Kontrol kontraktual merupakan mekanisme pengamanan yang dituangkan dalam perjanjian kerja sama antara organisasi dan vendor. Kontrol tersebut dapat mencakup:

- Persyaratan keamanan minimum;
- Kewajiban pelaporan insiden;
- Hak audit organisasi terhadap vendor;
- Persyaratan perlindungan data;
- Ketentuan kerahasiaan informasi;
- *Service Level Agreement* (SLA).

Melalui kontrak yang kuat, organisasi memiliki dasar hukum untuk memastikan vendor memenuhi ekspektasi keamanan yang ditetapkan.

**c. Pemantauan berkelanjutan (*Continuous monitoring*)**

Risiko vendor bersifat dinamis dan dapat berubah seiring waktu. Oleh karena itu, evaluasi keamanan tidak boleh dilakukan hanya pada saat proses pengadaan awal. *Continuous monitoring* memungkinkan organisasi untuk:

- Mengidentifikasi perubahan risiko secara cepat;
- Memantau kepatuhan vendor secara berkelanjutan;
- Menilai dampak perubahan teknologi vendor;
- Mengidentifikasi potensi ancaman baru yang muncul.

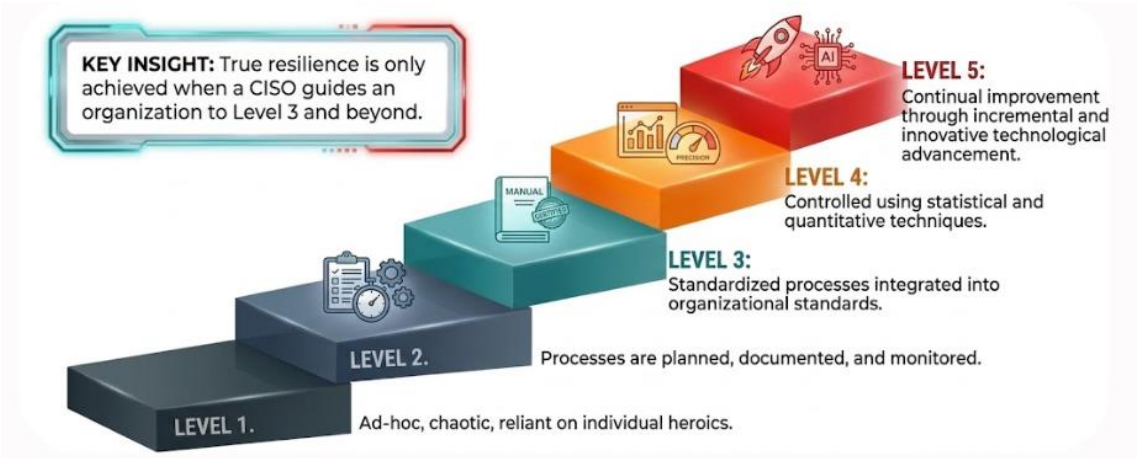
Pendekatan ini menjadi semakin penting karena banyak insiden keamanan siber modern berasal dari kompromi yang terjadi pada pihak ketiga yang memiliki akses terhadap sistem organisasi.

Domain ini menunjukkan bahwa seorang CISO harus mampu mengelola risiko yang berasal dari seluruh ekosistem bisnis, dan tidak hanya dari lingkungan internal organisasi. Keamanan informasi harus diperluas hingga mencakup rantai pasok digital (*digital supply chain*), vendor *cloud*, mitra bisnis, penyedia layanan teknologi, dan pihak eksternal lainnya.

## Asesmen Kematangan Keamanan Organisasi

Bagian ini menjelaskan bahwa tujuan akhir dari kepemimpinan keamanan informasi tidak hanya membangun kontrol keamanan atau memenuhi persyaratan kepatuhan, melainkan mendorong peningkatan tingkat kematangan keamanan organisasi secara menyeluruh. Konsep ini digambarkan melalui model kematangan (*maturity model*) yang terdiri dari 5 (lima) tingkatan perkembangan, mulai dari kondisi awal yang bersifat tidak terstruktur hingga kondisi optimal yang ditandai dengan perbaikan berkelanjutan dan inovasi.

Model kematangan keamanan informasi berfungsi sebagai instrumen untuk mengukur dan memetakan tingkat kapabilitas organisasi dalam menerapkan praktik keamanan informasi yang efektif. Pencapaian tingkat kematangan yang lebih tinggi mengindikasikan kemampuan organisasi yang semakin matang dalam mengelola risiko, meningkatkan ketahanan terhadap ancaman siber, serta menyelaraskan strategi keamanan informasi dengan tujuan bisnis dan keberlanjutan organisasi.



Berdasarkan model kematangan pada CCISO v4, ketahanan organisasi yang efektif baru dapat dicapai ketika organisasi telah mencapai tingkat kematangan keamanan minimal pada Level 3 (*Defined*), yaitu kondisi di mana proses, kebijakan, dan kontrol keamanan telah terdokumentasi, distandarisasi, serta diterapkan secara konsisten di seluruh organisasi. Sebelum mencapai tingkat tersebut, pengelolaan keamanan masih cenderung bersifat *ad hoc*, bergantung pada individu, dan berorientasi pada respons reaktif, sehingga belum mampu mendukung pengelolaan risiko dan ketahanan siber secara optimal.

**Level 1 – Initial**

*Initial*, yaitu kondisi awal di mana proses keamanan informasi masih bersifat *ad hoc*, tidak konsisten, dan sangat bergantung pada individu tertentu. Karakteristik utama pada level ini meliputi:

- Tidak adanya standar keamanan yang formal.
- Dokumentasi proses sangat terbatas atau bahkan tidak tersedia.
- Pengelolaan keamanan dilakukan secara reaktif setelah insiden terjadi.
- Keberhasilan keamanan sangat bergantung pada kemampuan individu tertentu.
- Tidak terdapat mekanisme pengukuran yang jelas.

Dalam kondisi ini, organisasi rentan terhadap berbagai ancaman karena kontrol keamanan belum diterapkan secara sistematis. Risiko operasional juga relatif tinggi karena hilangnya individu kunci dapat menyebabkan terganggunya proses keamanan organisasi. Pada level ini, keamanan informasi belum menjadi bagian integral dari tata kelola organisasi dan sering kali hanya dipandang sebagai kebutuhan teknis semata.

**Level 2 – *Managed***

*Managed* yaitu kondisi ketika proses keamanan mulai direncanakan, didokumentasikan, dan dipantau secara formal. Karakteristik level ini meliputi:

- Tersedianya kebijakan dan prosedur dasar.
- Adanya perencanaan aktivitas keamanan.
- Pelaksanaan monitoring terhadap proses keamanan.
- Penetapan tanggung jawab yang lebih jelas.
- Mulai diterapkannya kontrol keamanan secara konsisten.

Pada tahap ini organisasi mulai beralih dari pendekatan reaktif menuju pendekatan yang lebih terstruktur. Meskipun demikian, implementasi keamanan masih sering berbeda antar unit kerja dan belum sepenuhnya terintegrasi ke dalam proses bisnis organisasi. Keamanan mulai dilihat sebagai fungsi yang penting, tetapi masih berfokus pada pengendalian operasional dibandingkan pengelolaan strategis.

**Level 3 – *Defined***

*Defined* yaitu kondisi ketika proses keamanan telah distandarisasi dan terintegrasi ke dalam standar organisasi. Pada tingkatan ini seluruh proses keamanan telah terdokumentasi dengan baik

dan diterapkan secara konsisten di seluruh organisasi.
Karakteristik utama level ini meliputi:

- Kebijakan keamanan yang formal dan terdokumentasi.
- Standar keamanan diterapkan di seluruh organisasi (*organization-wide*).
- Proses keamanan terintegrasi dengan proses bisnis.
- Tanggung jawab keamanan didefinisikan secara jelas.
- Program pelatihan dan kesadaran keamanan *(security awareness)* berjalan secara sistematis.
- Pengelolaan risiko dilakukan secara terstruktur.

Level ini dianggap sebagai titik penting dalam perjalanan kematangan organisasi karena keamanan tidak lagi bergantung pada individu tertentu, melainkan telah menjadi bagian dari budaya dan tata kelola organisasi. Pada tahap ini organisasi mulai memiliki kemampuan untuk mempertahankan konsistensi pengendalian keamanan meskipun terjadi perubahan personel, teknologi, maupun struktur organisasi.

**Level 4 – *Quantitatively Managed***

*Quantitatively Managed* yaitu kondisi ketika proses keamanan dikelola menggunakan pendekatan kuantitatif dan berbasis data. Pada tingkat kematangan ini, organisasi telah mengendalikan proses keamanan informasi melalui penerapan teknik statistik dan metode kuantitatif yang memungkinkan pengukuran kinerja secara objektif dan terstruktur. Pendekatan tersebut mendukung pemantauan efektivitas kontrol, pengelolaan risiko yang lebih akurat, serta pengambilan keputusan berbasis data guna meningkatkan efisiensi dan ketahanan organisasi.
Karakteristik level ini meliputi:

- Penggunaan metrik keamanan yang terukur.
- Pengembangan *Key Performance Indicators* (KPI).
- Penggunaan *Key Risk Indicators* (KRI).
- Analisis tren insiden keamanan.
- Pengukuran efektivitas kontrol keamanan.
- Pengambilan keputusan berbasis data.

Pada tahap ini organisasi tidak hanya mengetahui bahwa suatu kontrol telah diterapkan, tetapi juga mampu mengukur seberapa efektif kontrol tersebut dalam mengurangi risiko. Contohnya pengukuran tersebut meliputi:

- *Mean Time to Detect* (MTTD);
- *Mean Time to Respond* (MTTR);
- Tingkat keberhasilan *patch management*;
- Tingkat kepatuhan keamanan;
- Persentase mitigasi kerentanan kritis.

Pendekatan kuantitatif memungkinkan manajemen memperoleh gambaran yang lebih objektif mengenai kondisi keamanan organisasi dan mendukung proses pengambilan keputusan yang lebih akurat.

**Level 5 – *Optimizing***

*Optimizing* yaitu kondisi ketika organisasi telah menerapkan budaya perbaikan berkelanjutan (*continuous improvement*) serta memanfaatkan inovasi teknologi untuk meningkatkan keamanan secara proaktif.

Pernyataan tersebut mengindikasikan bahwa organisasi telah menerapkan budaya perbaikan berkelanjutan melalui penyempurnaan proses secara bertahap serta pemanfaatan inovasi teknologi. Pendekatan ini memungkinkan peningkatan efektivitas kontrol keamanan, penguatan ketahanan siber, dan peningkatan kapabilitas organisasi dalam menghadapi dinamika risiko dan perubahan teknologi yang terus berkembang. Karakteristik utama level ini meliputi:

- *Continuous improvement* sebagai budaya organisasi.
- Pemanfaatan otomatisasi keamanan.
- Integrasi *Artificial Intelligence* (AI) dan *Machine Learning*.
- Penerapan *threat intelligence* secara aktif.
- Adaptasi cepat terhadap ancaman baru.
- Inovasi berkelanjutan dalam pengelolaan keamanan.

Pada tahap ini organisasi tidak hanya mampu mengelola risiko yang ada, tetapi juga mampu mengantisipasi risiko yang akan muncul di masa depan. Keamanan informasi menjadi bagian dari strategi bisnis dan mendukung transformasi digital organisasi secara berkelanjutan. Organisasi yang berada pada level ini umumnya memiliki tingkat ketahanan siber yang tinggi, kemampuan respons yang cepat, serta kapasitas untuk beradaptasi terhadap perubahan lingkungan bisnis dan teknologi.

## Peran Strategis CISO

Model kematangan yang ditampilkan pada halaman ini menunjukkan bahwa peran utama seorang CISO bukan hanya mengelola teknologi keamanan, tetapi juga memimpin transformasi organisasi menuju tingkat kematangan yang lebih tinggi.
Untuk mencapai tujuan tersebut, CISO harus mampu:

- Mengembangkan tata kelola keamanan yang efektif.
- Menanamkan budaya keamanan di seluruh organisasi.
- Mengintegrasikan keamanan ke dalam proses bisnis.
- Mengembangkan metrik dan indikator kinerja keamanan.
- Mendorong inovasi dan perbaikan berkelanjutan.
- Memastikan investasi keamanan memberikan nilai bisnis yang terukur.

Keberhasilan seorang CISO dapat diukur dari kemampuannya meningkatkan tingkat kematangan keamanan organisasi sehingga organisasi mampu mencapai ketahanan siber yang berkelanjutan dan mendukung pencapaian tujuan strategis perusahaan.

# References

1. Ali, R. (2026). *Operationalising information security management: A procedural framework analysis of ISO/IEC 27001:2022 implementation in a financial-technology organisation*. arXiv. https://doi.org/10.48550/arXiv.2604.23230
2. Brunner, M., Sauerwein, C., Felderer, M., & Breu, R. (2020). *Risk management practices in information security: Exploring the status quo in the DACH region*. arXiv. https://doi.org/10.48550/arXiv.2003.07674
3. EC-Council. (2025). *Certified Chief Information Security Officer (CCISO) v4: Executive leadership program* [Training material].
4. EC-Council. (n.d.). *CCISO domain details*. https://ciso.eccouncil.org/cciso-certification/cciso-domain-details/
5. EC-Council. (n.d.). *Certified Chief Information Security Officer (CCISO)*. https://www.eccouncil.org/train-certify/certified-chief-information-security-officer-cciso/
6. International Organization for Standardization. (2018). *ISO 31000:2018 Risk management—Guidelines*. Author.
7. International Organization for Standardization. (2022). *ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection—Information security management systems—Requirements*. Author.
8. ISACA. (2019). *COBIT 2019 framework: Governance and management objectives*. ISACA.
9. National Institute of Standards and Technology. (2024). *Cybersecurity framework (CSF) 2.0*. U.S. Department of Commerce. https://doi.org/10.6028/NIST.CSWP.29
10. Onibere, M., Ahmad, A., & Maynard, S. B. (2021). *Dynamic information security management capability: Strategising for organisational performance*. arXiv. https://doi.org/10.48550/arXiv.2104.07141
11. TechRadar Pro. (2025). *The evolving CISO role: Bridging the gap between security and strategy*. https://www.techradar.com/pro/the-evolving-ciso-role-bridging-the-gap-between-security-and-strategy

## Biografi Penulis

**Yulian Sani**. Seorang *enthusiast* di bidang keamanan siber dan teknologi informasi dengan pengalaman di industri perbankan, manufaktur, dan konsultansi. Saat ini, berperan dalam fungsi *Internal Audit* dan *Data Analytics*, dengan kompetensi dalam keamanan siber, *penetration testing*, serta *software engineering*.

Meraih gelar Magister Administrasi Bisnis dari Institut Teknologi Telkom (Universitas Telkom). Sebelumnya juga, menyelesaikan Magister Teknik Informatika dengan fokus Keamanan Informasi dari Universitas Langlangbuana, serta Teknik Informatika dari Universitas Siliwangi. Saat ini memiliki beberapa sertifikasi profesional di bidang teknologi informasi, seperti CCISO, CEH, ECSA, dan CHFI.