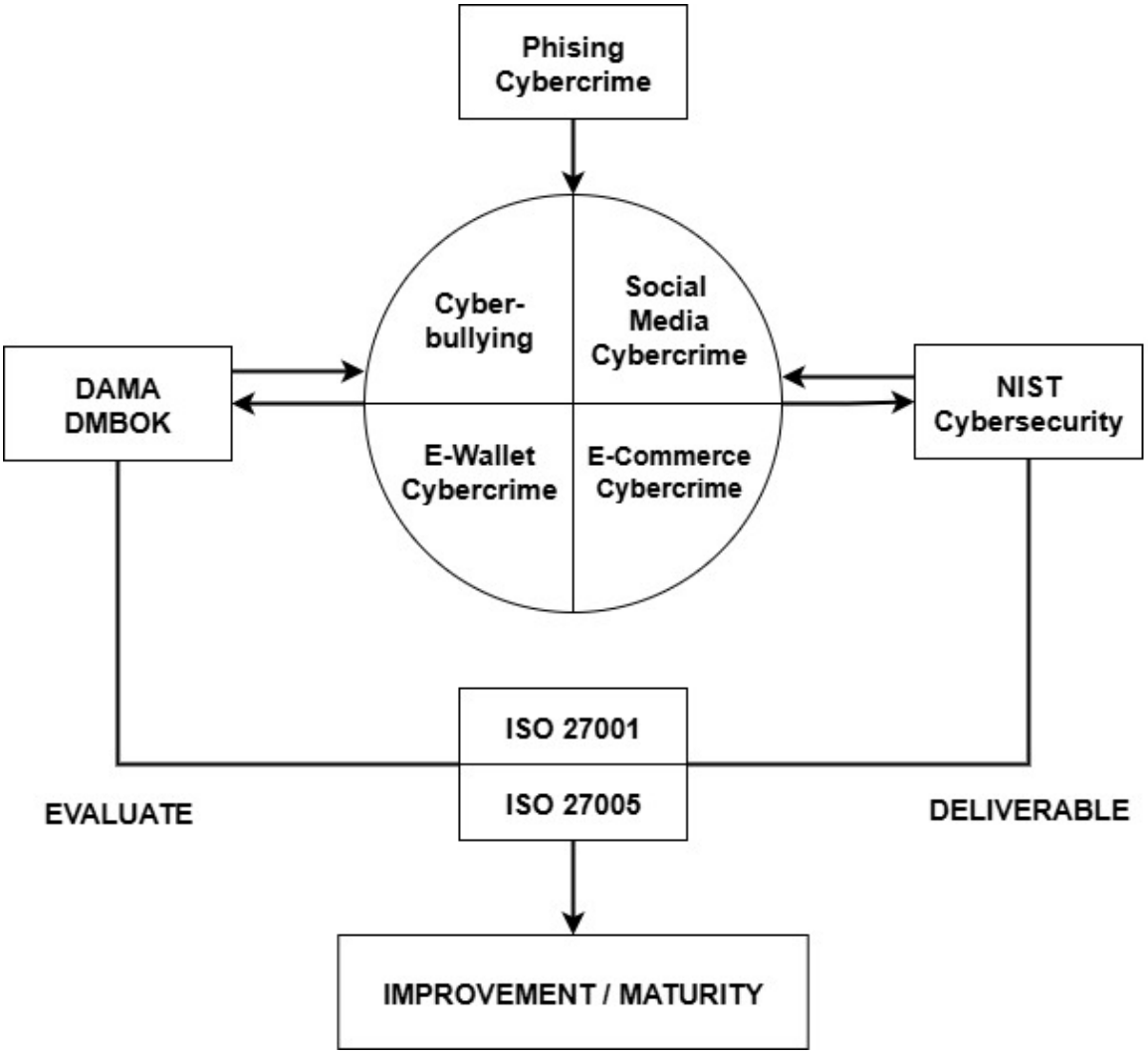

Figure 1 Model Implementasi Social Cybersecurity Awarness

Model yang diajukan adalah model implementasi social cybersecurity awareness yang dihadirkan sebagai website untuk membimbing praktik bermedia sosial/bertransaksi digital secara aman. Platform ini menyediakan asesmen mandiri, panduan dan aturan perilaku, serta materi pelatihan yang membenahi kebiasaan yang keliru sehingga memudahkan mitigasi risiko dan perlindungan data. Secara fungsional, model memetakan kategori kejahatan siber prioritas ke kerangka DAMA-DMBOK dan NIST, lalu dievaluasi siklik dengan ISO/IEC 27001/27005 (PDCA) guna menghasilkan deliverables terukur (kebijakan, SOP, kurikulum pelatihan, dan metrik kedewasaan) yang dapat diterapkan lintas institusi dan komunitas Asesmen Skor Maturitas kuesioner berbasis dimensi terukur (phishing, SMC, CB, EW, EC) menghasilkan profil risiko rekomendasi personal. Pelatihan Kontekstual modul mengikuti peran/fungsi (governance vs operasional) dan budaya

digital setempat. Policy/SOP Generator templat kebijakan SOP selaras NIST CSF dan kontrol ISO 27001, dilengkapi PDCA metrik efektivitas. Dashboard Organisasi/Komunitas ringkasan kepatuhan, insiden, dan tren perilaku untuk mendorong perbaikan berkelanjutan. Yang dimana model ini menggambarkan beberapa model yang tergabung diantaranya diantaranya dalam hal ini menjadi tiger diantaranya dalam konteks kejahatan dalam siber yang sering dilakukan dalam ranah sosial diantaranya :

- *Phishing Cybercrime*
- *social media cybercrime*
- *cyberbullying*
- *e-wallet cybercrime*
- *e-commerce cybercrime*.

Figure 2 Indonesia Cybersecurity Research Gaps

Yang dimana kemanan dalam Cybersecurity di Indonesia memberikan dampak yang sangat signifikan hal ini dapat memebrikan odel yag memberikan keaman sistem informasi menjadi wajib untuk di berikan impelementasi

Phising Cybercrime

Phishing Cybercrime adalah salah satu bentuk kejahatan siber yang bertujuan untuk menipu korban agar secara tidak sadar memberikan informasi sensitif seperti kata sandi, nomor kartu kredit, kode OTP, atau data pribadi lainnya. Modus utama dari phishing adalah menyamar sebagai pihak atau lembaga resmi—misalnya bank, marketplace, penyedia e-wallet, atau bahkan teman dekat—melalui media elektronik seperti email, pesan singkat, media sosial, maupun situs web tiruan.

Dalam praktiknya, pelaku biasanya mengirimkan tautan atau lampiran berbahaya yang dirancang menyerupai layanan sah agar korban percaya dan melakukan aksi tertentu, seperti mengklik tautan login palsu atau mengunduh file yang sudah disisipi malware. Konsekuensinya, data pribadi dapat dicuri, akun dapat diambil alih (account takeover), hingga memicu tindak kejahatan lanjutan seperti penipuan finansial, penyebaran malware, atau pemalsuan identitas. Dalam konteks Social Cybersecurity Awareness, phishing digolongkan sebagai ancaman payung karena dapat memicu berbagai insiden di empat domain utama lainnya—social media cybercrime, cyberbullying, e-wallet crime, dan e-commerce crime. Oleh karena itu, model ini menekankan pentingnya intervensi kebiasaan seperti berhati-hati terhadap tautan yang mencurigakan, mengaktifkan verifikasi dua langkah, menggunakan email/web filters, dan mengikuti pelatihan simulasi phishing untuk membentuk respons otomatis yang lebih aman.

Penjelasan bagian per bagian

1) Domain Risiko (lingkaran berkuadran + kotak *Phishing*)

- **Social Media Cybercrime**

KMO and Bartlett's Test

Kaiser-Meyer-Olkin Measure of Sampling Adequacy.		.587
Bartlett's Test of Sphericity	Approx. Chi-Square	71.940
	df	10
	Sig.	<,001

Hasil uji Kaiser-Meyer-Olkin (KMO) menunjukkan nilai 0,587, yang berarti data cukup memadai untuk analisis faktor karena melewati ambang batas 0,5. Uji Bartlett's Test of Sphericity juga signifikan (Chi-Square = 71,940; df = 10; $p < 0,001$), menandakan adanya korelasi antar item kuesioner sehingga layak dilakukan Analisis Komponen Utama (PCA). Dari hasil PCA diperoleh dua komponen utama dengan nilai eigen >1, yaitu 2,299 (45,98%) dan 1,251 (25,02%), yang secara kumulatif menjelaskan 70,99% variasi data. Rotasi faktor menunjukkan distribusi yang seimbang, dengan komponen pertama menjelaskan 44,74% dan komponen kedua 26,25%. Plot scree menguatkan bahwa jumlah faktor optimal adalah dua. Interpretasi item memperlihatkan bahwa faktor pertama berkaitan dengan paparan langsung phishing (frekuensi penerimaan tautan/OTP), sedangkan faktor kedua berkaitan dengan pengetahuan responden tentang phishing. Dengan demikian, pengalaman dan persepsi terkait kejahatan siber phishing dapat dirangkum menjadi dua dimensi utama: paparan dan pengetahuan. Dimensi ini juga terkait dengan ancaman nyata di ranah media sosial, yakni pengambilalihan akun, penipuan identitas, penyebaran tautan/malware, dan

rekayasa sosial, yang dalam model berfungsi sebagai objek intervensi kebiasaan melalui aturan posting, pengaturan privasi, verifikasi dua langkah, serta peningkatan higienitas tauta

- **Cyberbullying**

KMO and Bartlett's Test

Kaiser-Meyer-Olkin Measure of Sampling Adequacy.		.606
Bartlett's Test of Sphericity	Approx. Chi-Square	129.025
	df	15
	Sig.	<,001

Berdasarkan uji Kaiser-Meyer-Olkin (KMO) sebesar 0,606, data dinilai memadai untuk analisis faktor karena sedikit di atas ambang batas minimum 0,6, meskipun hanya menunjukkan kecukupan sampel pada tingkat sedang. Uji Bartlett's Test of Sphericity menghasilkan nilai Chi-Square 129,025 dengan 15 derajat kebebasan (df) dan tingkat signifikansi <0,001, yang berarti korelasi antar variabel cukup kuat sehingga layak digunakan Analisis Komponen Utama (PCA). Hasil PCA menunjukkan dua komponen utama dengan nilai eigen >1, yaitu 2,664 (44,40%) dan 1,728 (28,80%), yang secara kumulatif menjelaskan 73,202% variasi total. Setelah rotasi, komponen pertama menjelaskan 43,74% dan komponen kedua 29,46%, dengan scree plot menegaskan adanya dua faktor utama. Interpretasi item kuesioner menunjukkan bahwa faktor pertama mewakili intensitas dan ketergantungan penggunaan media sosial (SMC2, SMC4, SMC5, SMC6), sedangkan faktor kedua berkaitan dengan perilaku berbagi informasi dan foto pribadi di media sosial (SMC1, SMC3). Temuan ini mengindikasikan bahwa risiko social media cybercrime dapat diringkas ke dalam dua dimensi utama: intensitas/ketergantungan penggunaan dan kebiasaan berbagi informasi pribadi. Dimensi ini terkait langsung dengan ancaman seperti perundungan, doxxing, dan pelecehan, yang dalam model berfungsi sebagai objek intervensi etika digital melalui pembentukan budaya penggunaan sehat, mekanisme pelaporan dan pemblokiran, kebijakan komunitas, serta pelatihan empati dan literasi budaya.

- **E-Wallet Cybercrime**

KMO and Bartlett's Test

Kaiser-Meyer-Olkin Measure of Sampling Adequacy.		.716
Bartlett's Test of Sphericity	Approx. Chi-Square	104.675
	df	3
	Sig.	<,001

Berdasarkan uji Kaiser-Meyer-Olkin (KMO) sebesar 0,716, data berada pada kategori sedang yang menunjukkan kualitas sampel cukup baik untuk analisis faktor. Uji Bartlett's Test of Sphericity menghasilkan nilai Chi-Square 104,675 dengan 3 derajat kebebasan (df) dan tingkat signifikansi <0,001, yang berarti korelasi antar item kuesioner memadai untuk dilakukan ekstraksi faktor. Hasil analisis eigenvalue menunjukkan hanya ada satu komponen utama dengan nilai >1, yakni 2,510, yang menjelaskan 83,678% dari variasi total. Nilai ini sangat tinggi, menandakan seluruh item (EWC1, EWC2, EWC3) mengukur dimensi yang sama, dan diperkuat oleh scree plot yang menampilkan penurunan tajam setelah komponen pertama, sehingga mendukung struktur faktor tunggal. Interpretasi menunjukkan faktor tunggal ini merepresentasikan tingkat penggunaan dan ketergantungan pada dompet digital, mencakup aspek penyimpanan dana pribadi, frekuensi transaksi, dan ketergantungan pengguna terhadap e-wallet. Dengan demikian, penggunaan yang berlebihan atau ceroboh dapat meningkatkan risiko e-wallet cybercrime, khususnya terkait ancaman seperti penipuan top-up, pengalihan OTP, aplikasi palsu, dan SIM swap, sehingga dalam model SCA faktor ini diposisikan sebagai objek intervensi kebiasaan aman bertransaksi, seperti verifikasi aplikasi resmi, tidak membagikan OTP, dan penggunaan transaction alert.

- **E-Commerce Cybercrime**

KMO and Bartlett's Test

Kaiser-Meyer-Olkin Measure of Sampling Adequacy.		.617
Bartlett's Test of Sphericity	Approx. Chi-Square	40.259
	df	3
	Sig.	<,001

Hasil uji Kaiser-Meyer-Olkin (KMO) sebesar 0,617 menunjukkan bahwa data berada pada kategori sedang namun tetap memadai untuk analisis faktor. Uji Bartlett's Test of Sphericity menghasilkan nilai Chi-Square 40,259 dengan 3 derajat kebebasan (df) dan tingkat signifikansi <0,001, yang berarti terdapat korelasi signifikan antar variabel sehingga memungkinkan dilakukan ekstraksi faktor. Analisis eigenvalue mengungkap hanya ada satu komponen utama dengan nilai >1, yaitu 1,974, yang menjelaskan

65,792% dari variasi total. Hasil ini menegaskan bahwa ketiga item (ECC1, ECC2, ECC3) secara konsisten mengukur dimensi yang sama, dan diperkuat oleh scree plot yang menunjukkan penurunan tajam setelah komponen pertama, sehingga mendukung struktur faktor tunggal. Interpretasi menunjukkan bahwa faktor tunggal ini merepresentasikan tingkat keterlibatan pengguna dalam aktivitas e-commerce, meliputi perilaku pembuatan akun, frekuensi transaksi, dan kecenderungan membagikan informasi pribadi di platform. Temuan ini menegaskan bahwa risiko e-commerce cybercrime dapat dikaitkan dengan ancaman seperti toko palsu, fake invoice, refund fraud, dan penyalahgunaan data pembayaran, yang dalam model SCA difungsikan sebagai objek intervensi kebiasaan aman, antara lain melalui verifikasi seller, tata kelola data kartu, edukasi penggunaan escrow, serta kebijakan pengembalian yang jelas.

- **Phishing (kotak atas, bersifat lintas domain)**

KMO and Bartlett's Test

Kaiser-Meyer-Olkin Measure of Sampling Adequacy.		.754
Bartlett's Test of Sphericity	Approx. Chi-Square	89.747
	df	21
	Sig.	<,001

Berdasarkan uji Kaiser-Meyer-Olkin (KMO) sebesar 0,754, data dikategorikan baik dan menunjukkan kualitas sampel cukup memadai untuk analisis faktor. Uji Bartlett's Test of Sphericity menghasilkan nilai Chi-Square 89,747 dengan df = 21 dan signifikansi <0,001, yang berarti terdapat korelasi signifikan antar variabel sehingga memungkinkan dilakukannya ekstraksi faktor. Analisis eigenvalue mengungkap adanya dua komponen utama dengan nilai >1, yaitu 2,944 (42,051%) dan 1,150 (16,426%), yang secara kumulatif menjelaskan 58,478% variasi total. Setelah rotasi, komponen pertama menjelaskan 33,261% dan komponen kedua 25,216%. Scree plot juga menunjukkan titik elbow pada komponen kedua, sehingga memperkuat keputusan untuk mempertahankan dua faktor utama. Interpretasi item kuesioner memperlihatkan bahwa faktor pertama merepresentasikan pengalaman langsung sebagai korban atau saksi cyberbullying (CB1–CB6), sedangkan faktor kedua menggambarkan pengetahuan dan kesadaran dalam menangani cyberbullying (CB7). Dengan demikian, fenomena cyberbullying dapat dipahami melalui dua dimensi besar: paparan terhadap perilaku perundungan daring dan kesadaran cara penanganannya. Dalam konteks model Social Cybersecurity Awareness, dimensi ini dipandang sebagai ancaman payung yang dapat memicu insiden di empat domain lainnya, sehingga model mengarusutamakan deteksi pesan/tautan mencurigakan,

penggunaan email/web filters, serta pelatihan phishing simulation sebagai bagian dari intervensi kebiasaan dan penguatan kesadaran digital.

2) DAMA-DMBOK

Sehingga dilakukan proses penerapan dalam implementasi Kerangka Kerja yang memberi aturan tata kelola data dan kebiasaan digital, di antaranya terkait keamanan dalam bidang data meliputi: penetapan tujuan (mencegah akses tidak sah, memastikan autentikasi–otorisasi–akuntabilitas, dan pemenuhan regulasi), perumusan kebijakan & standar keamanan data, serta pengelolaan kontrol teknis dan prosedural yang terukur

- Peran/Fungsi: fondasi **governance data & kebiasaan** — klasifikasi data pribadi, hak akses, kualitas data, *data lifecycle*, peran pemilik/pengelola data.
- Keluaran: aturan tingkah laku bermedia (do/don't), standar privasi akun, *data handling policy*, *retention*, dan *consent management*.
- Interaksi: memberi "aturan main" ke domain risiko (panah ke lingkaran) dan menerima umpan balik dari insiden/temuan untuk penyempurnaan (panah balik).

3) NIST Cybersecurity Framework (kotak kanan)

- Peran/Fungsi: **praktik teknis & operasional**.
    - *Identify*: pemetaan aset akun/aplikasi & profil risiko pengguna.
    - *Protect*: MFA, kata sandi kuat, kebijakan perangkat, *content moderation*, *privacy settings*.
    - *Detect*: pemantauan anomali akun, *anti-phishing* filter, *brand monitoring*.
    - *Respond*: panduan tanggap insiden (ambil alih kembali akun, *take-down*, pelaporan).
    - *Recover*: pemulihan layanan, *post-incident review*, pemulihan reputasi.
- Keluaran: **DELIVERABLES** — kebijakan, SOP, *playbook*, modul pelatihan, *awareness content*, dan kontrol teknis.

4) ISO/IEC 27001 & ISO/IEC 27005 (kotak tengah-bawah)

- **ISO 27001 (ISMS)**: memastikan semua kebijakan/SOP berjalan dalam siklus **PDCA** (Plan-Do-Check-Act) dengan peran, bukti, dan audit.
- **ISO 27005 (Risk Management)**: metodologi identifikasi, analisis, penilaian, penanganan, dan penerimaan risiko untuk empat domain + phishing.

- Fungsi gabungan: **EVALUATE** efektivitas kontrol & kebiasaan, memutuskan perbaikan prioritas, dan mengukur kepatuhan.

5) Improvement / Maturity (kotak paling bawah)

- Peran/Fungsi: hasil akhir berupa **kenaikan tingkat kedewasaan** (individu, komunitas, organisasi).
- Indikator contoh:
    - Penurunan *click-rate* phishing, laju pelaporan meningkat.
    - Peningkatan adopsi MFA, kepatuhan kebijakan privasi.
    - Skor asesmen perilaku (pra-/pasca-pelatihan) membaik.
    - Jumlah insiden sosial/finansial turun.

Hubungan antarbagian (inti logika model)

- **Lingkaran risiko** = "apa yang harus diubah" (kebiasaan & paparan ancaman).
- **DAMA-DMBOK** = "aturan perilaku & pengelolaan data" (governance).
- **NIST CSF** = "cara teknis & operasional mengeksekusi" (kontrol & SOP).
- **ISO 27001/27005** = "bagaimana menguji & membuktikan" (evaluasi terstandar).
- **Improvement/Maturity** = "hasil yang terukur", lalu **diumpankan kembali** untuk memperbarui aturan, kontrol, dan materi pelatihan (siklus berulang).

Evaluate Terstandar ISO/IEC 27001

Implementasi dievaluasi dengan yang berfokus terhadap berfokus pada penerapan sistem manajemen keamanan informasi yang berbasis risiko, terdokumentasi, serta berjalan secara berkesinambungan. Dalam konteks Social Cybersecurity Awareness (SCA), implementasinya dimulai dari penetapan ruang lingkup dan konteks (Klausul 4) dengan mendefinisikan batas-batas ISMS seperti akun, data pribadi pengguna, modul asesmen, log, serta konten UGC, sekaligus mendokumentasikan pihak berkepentingan (user, moderator, PSP/e-wallet, marketplace, regulator). Selanjutnya pada kepemimpinan dan kebijakan (Klausul 5), organisasi diwajibkan menerbitkan Information Security Policy yang mencakup aturan penggunaan media sosial (AUP),

anti-bullying, anti-phishing, serta komitmen perbaikan berkelanjutan. Peran-peran utama seperti Owner ISMS, Information Security Manager, Data Steward, dan Moderator juga harus ditetapkan dengan jelas. Pada perencanaan (Klausul 6, 6.1.2–6.1.3), organisasi menyusun kriteria risiko untuk ancaman seperti phishing, SMC, CB, EW, maupun EC, melaksanakan penilaian risiko secara rutin, serta menyusun Risk Treatment Plan dan Statement of Applicability (SoA) berdasarkan kontrol Annex A, dengan persetujuan risk owner atas risiko residual. Selain itu, sasaran keamanan (6.2) diformulasikan dalam bentuk KPI seperti tingkat adopsi MFA, rasio klik phishing, TTD/MTTR sosial, dan kelulusan pelatihan keamanan. Dukungan (Klausul 7) menekankan kompetensi SDM, peningkatan awareness melalui pelatihan SCA, komunikasi internal-eksternal yang efektif, serta pengendalian dokumentasi (SOP, kebijakan, catatan pelatihan, dan log insiden).

- **Evaluate ISO/IEC 27005**

  memberikan proses terstruktur untuk mengelola risiko keamanan informasi secara menyeluruh, mulai dari penetapan konteks hingga pemantauan berkelanjutan, yang sangat relevan untuk domain Social Cybersecurity Awareness (SCA) seperti phishing, social media cybercrime, cyberbullying, e-wallet, dan e-commerce. Pada tahap Penetapan Konteks (Klausul 7), organisasi perlu mendefinisikan tujuan, kriteria evaluasi risiko (impact dan acceptance), ruang lingkup pada platform SCA, serta menetapkan peran dan relasinya dengan Enterprise Risk Management (ERM) dan kepatuhan seperti UU Perlindungan Data Pribadi. Selanjutnya, dalam Risk Assessment (Klausul 8) dilakukan identifikasi risiko dengan memetakan aset (akun, PII, konten, dompet digital, toko online), ancaman (phishing, impersonation, penipuan, ujaran kebencian), kontrol yang ada, hingga kerentanan (misalnya password reuse, setting privasi longgar, atau OTP sharing), lalu menganalisis risiko berdasarkan likelihood dan impact baik secara kualitatif maupun kuantitatif. Evaluasi risiko digunakan untuk memprioritaskan skenario yang masuk ke rencana penanganan melalui heatmap. Tahap berikutnya adalah Risk Treatment (Klausul 9), dengan opsi modify, avoid, share, atau retain, serta penyusunan kontrol seperti MFA, filter tautan berbahaya, moderasi konten, edukasi mikro-learning, hingga verifikasi merchant, beserta kendala dan rencana implementasinya. Setelah itu, Risk Acceptance (Klausul 10) menuntut dokumentasi residual risk yang diterima oleh risk owner, misalnya toleransi risiko pada fitur User Generated Content (UGC). Proses dilengkapi dengan Komunikasi dan Konsultasi (Klausul 11) melalui edukasi pengguna, notifikasi insiden, dan umpan balik komunitas, serta Monitoring dan Review (Klausul 12) untuk memantau efektivitas kontrol serta memperbarui tindakan bila tren risiko memburuk, seperti peningkatan click-rate phishing atau laporan

bullying. Dari seluruh siklus ini, artefak keluaran ISO/IEC 27005 berupa risk register yang berisi pemetaan aset-ancaman-kerentanan-kontrol, daftar skenario risiko dan tingkatannya, rencana treatment, bukti risk acceptance, serta laporan monitoring dan review yang mendukung peningkatan berkelanjutan dalam pengelolaan risiko SCA.

Evaluasi Terstandar. Implementasi dievaluasi dengan ISO/IEC 27001 yang berfokus pada pembentukan dan pengoperasian ISMS berbasis risiko (penetapan konteks & kebijakan, penilaian/penanganan risiko, pengendalian informasi terdokumentasi, monitoring–audit–tinjauan manajemen, serta perbaikan berkelanjutan) guna memastikan efektivitas kontrol SCA dapat diukur dan diaudit. ISO/IEC 27005 (manajemen risiko). Risiko pada domain SCA dikelola melalui tahapan penetapan konteks, identifikasi–analisis–evaluasi risiko, risk treatment (modify/avoid/share/retain), risk acceptance, komunikasi, serta pemantauan & review yang berulang, sehingga umpan balik implementasi SCA selalu kembali memperkuat kebijakan, SOP, dan pelatihan di platform

Label **EVALUATE** (kiri-bawah) menegaskan jalur umpan balik dari tata kelola ke evaluasi; **DELIVERABLE** (kanan-bawah) menegaskan keluaran praktis yang dihasilkan dari kerangka NIST.