BAB III

PELAKSANAAN KERJA MAGANG

3.1 Kedudukan dan Koordinasi

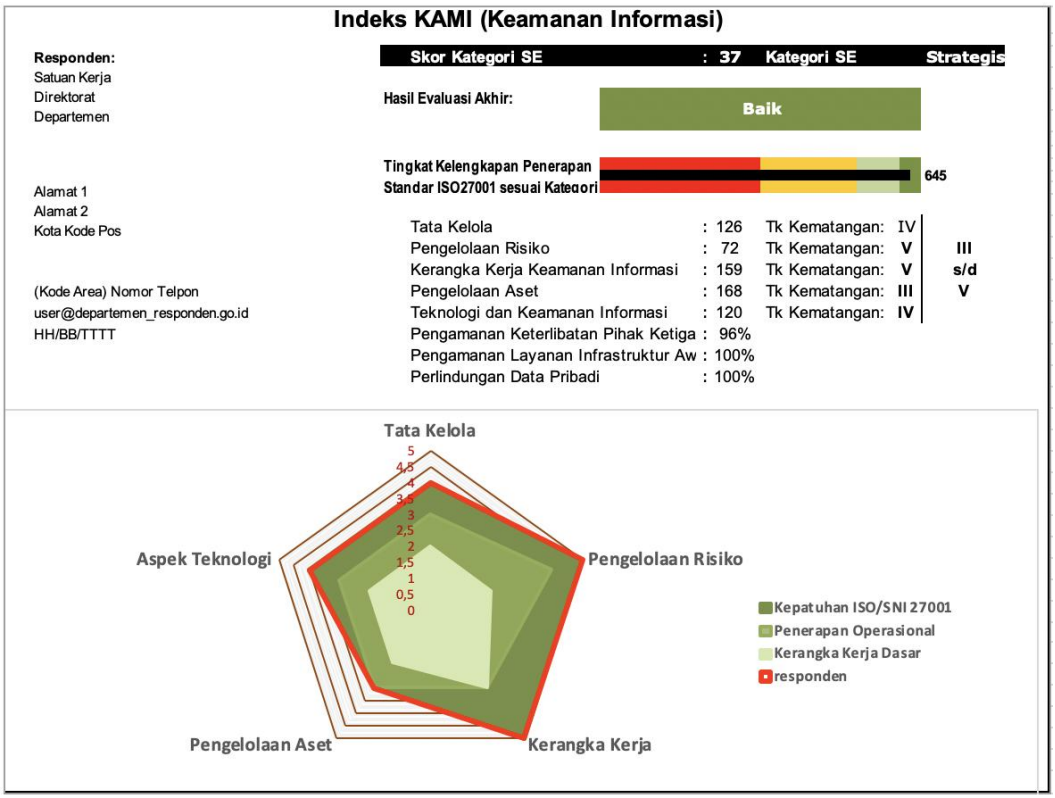
Dalam pelaksanaan program magang Merdeka Belajar Kampus Merdeka (MBKM), pemahaman terhadap kedudukan peserta magang dalam struktur organisasi serta alur koordinasi kerja menjadi aspek yang sangat penting dan harus dipahami secara menyeluruh. Hal ini bertujuan agar peserta magang tidak hanya menjadi pelaksana teknis, tetapi juga mampu memahami konteks kerja yang lebih luas, berkontribusi secara aktif dalam proses bisnis, serta menjalin komunikasi dan koordinasi yang efektif dengan berbagai pihak di dalam perusahaan. Mahasiswi magang tidak hanya menjalankan tugas administratif atau operasional semata, tetapi juga terlibat dalam berbagai kegiatan yang menuntut kemampuan analitis, kolaboratif, serta adaptasi terhadap budaya kerja profesional. Beberapa kegiatan tersebut antara lain adalah koordinasi lintas divisi, penyesuaian terhadap standar operasional prosedur (SOP) perusahaan, serta keterlibatan langsung dalam pengelolaan dokumentasi strategis terkait keamanan informasi yang menjadi bagian penting dari sistem tata kelola digital perusahaan.

Di PT Akebono Brake Astra Indonesia, Divisi IT memiliki struktur yang terbagi ke dalam beberapa sub-bagian atau section, masing-masing memiliki tanggung jawab spesifik dalam mendukung layanan teknologi informasi dan komunikasi (TIK) yang menunjang seluruh aktivitas bisnis perusahaan. Beberapa sub-bagian tersebut meliputi Infrastructure & Networking, Application Development, IT Governance & Compliance, serta Technical Support. Dalam konteks program magang ini, mahasiswi secara khusus ditempatkan pada Technical Support Section, yaitu sub-divisi yang memiliki cakupan kerja di bidang operasional harian IT, pengelolaan server dan jaringan, pelaksanaan audit internal sistem IT, risk assessment terhadap sistem informasi, serta pengembangan dan implementasi program cyber security, termasuk penerapan Information Security Management System (ISMS) yang mengacu pada standar internasional ISO/IEC 27001.

Sebagai bagian dari peran strategisnya selama magang, mahasiswi mendapatkan tugas khusus untuk membantu proses asesmen dan sertifikasi Indeks Keamanan Informasi (KAMI) yang merupakan standar penilaian tingkat keamanan informasi nasional yang disusun dan diterbitkan oleh Badan Siber dan Sandi Negara (BSSN). Keterlibatan dalam proyek ini memberikan pengalaman nyata dalam penerapan kebijakan keamanan informasi, pemetaan gap analisis terhadap standar nasional, serta penyusunan dokumentasi dan pelaporan yang diperlukan untuk proses sertifikasi. Dengan mengikuti seluruh tahapan asesmen ini, mahasiswi tidak hanya mengembangkan kompetensi teknis dan pemahaman mengenai tata kelola TI, tetapi juga memperoleh wawasan mendalam mengenai pentingnya integrasi antara manajemen risiko, perlindungan aset informasi, dan kesiapan organisasi dalam menghadapi ancaman siber di era digital industri 4.0.

Indeks Keamanan Informasi (KAMI) merupakan aplikasi yang digunakan sebagai alat bantu untuk melakukan asesmen dan evaluasi tingkat kesiapan (Kelengkapan dan Kematangan) penerapan keamanan informasi berdasarkan kriteria SNI ISO/IEC 27001. Proses evaluasi dilakukan melalui sejumlah pertanyaan di beberapa area berikut:

1. Kategori Sistem Elektronik yang digunakan
2. Tata Kelola Keamanan Informasi
3. Pengelolaan Risiko Keamanan Informasi
4. Kerangka Kerja Keamanan Informasi
5. Pengelolaan Aset Informasi
6. Teknologi dan Keamanan Informasi
7. Suplemen (Tambahan pengukuran dilakukan untuk aspek Pengamanan Keterlibatan Pihak Ketiga Penyedia Layanan, Pengamanan Layanan Infrastruktur Awan *(Cloud Service) dan* Perlindungan Data Pribadi.



Gambar 3. 1 Contoh hasil asesmen dan evaluasi tingkat kesiapan Indeks KAMI. [11]

Pada Gambar 3.1 ditampilkan contoh hasil asesmen dan evaluasi tingkat kesiapan keamanan informasi berdasarkan INDEKS KAMI yang dirancang oleh Badan Siber dan Sandi Negara (BSSN). Evaluasi ini memberikan skor kategori SE (Strategic Environment) sebesar 37 dengan hasil akhir evaluasi "Baik". Tingkat kelengkapan penerapan standar ISO 27001 mencapai 645 poin, mencerminkan pencapaian yang cukup tinggi terhadap elemen-elemen kontrol keamanan informasi[11].

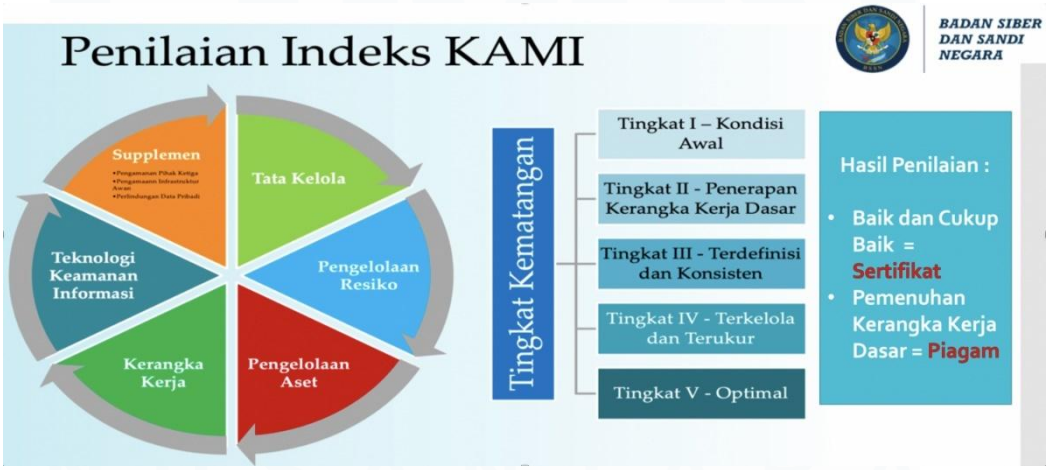
Asesmen ini mencakup enam domain utama, yaitu Tata Kelola, Pengelolaan Risiko, Kerangka Kerja Keamanan Informasi, Pengelolaan Aset, Aspek Teknologi, dan Teknologi dan Keamanan Informasi. Masing-masing domain dievaluasi tingkat kematangannya dari level I (inisial) hingga V (optimal), dengan hasil bervariasi mulai dari tingkat kematangan III hingga V. Visualisasi spider chart pada bagian bawah gambar menunjukkan perbandingan antara kepatuhan terhadap ISO 27001, penerapan operasional, kerangka kerja dasar, dan penilaian dari responden.

Hasil ini memberikan gambaran menyeluruh tentang sejauh mana organisasi telah memenuhi standar keamanan informasi dan area mana yang masih perlu diperbaiki atau ditingkatkan untuk mencapai kondisi ideal sesuai standar ISO/IEC 27001.

Pengelompokan kedua dilakukan berdasarkan **tingkat kematangan** penerapan pengamanan dengan kategorisasi yang mengacu kepada tingkatan kematangan yang digunakan oleh kerangka kerja COBIT atau CMMI. Tingkat kematangan ini nantinya akan digunakan sebagai alat untuk melaporkan pemetaan dan pemeringkatan kesiapan keamanan informasi di Kementerian / Lembaga. Untuk keperluan Indeks KAMI, tingkat kematangan tersebut didefinisikan sebagai:

a) Tingkat I – Kondisi Awal
b) Tingkat II – Penerapan Kerangka Kerja Dasar
c) Tingkat III – Terdefinisi dan Konsisten
d) Tingkat IV – Terkelola dan Terukur
e) Tingkat V – Optimal

Untuk membantu memberikan uraian yang lebih detil, tingkatan ini ditambah dengan tingkatan antara – I+, II+, III+, dan IV+, sehingga total terdapat 9 tingkatan kematangan . Sebagai awal, semua responden akan diberikan kategori kematangan Tingkat I. Sebagai padanan terhadap standar ISO/IEC 27001:2013, tingkat kematangan yang diharapkan untuk ambang batas minimum kesiapan sertifikasi adalah Tingkat III+.



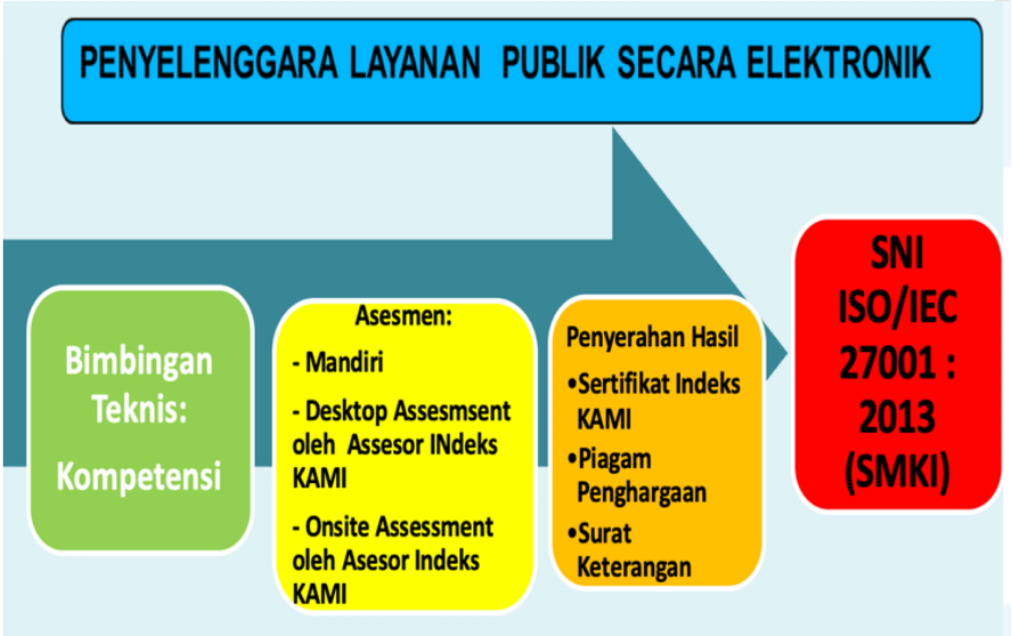
Gambar 3. 2 Penilaian Indeks KAMI berdasarkan tingkat kematangan [11]

Pada Gambar 3.2 ditampilkan skema penilaian INDEKS KAMI berdasarkan tingkat kematangan dalam lima domain utama, yaitu Tata Kelola, Pengelolaan Risiko, Kerangka Kerja, Pengelolaan Aset, dan Teknologi Keamanan Informasi. Penilaian ini bertujuan untuk memetakan sejauh mana kesiapan dan kematangan sistem keamanan informasi suatu instansi, bukan untuk menilai kelayakan atau efektivitas bentuk pengamanan yang digunakan[11].

Tingkat kematangan dinilai dari Tingkat I (Kondisi Awal) hingga Tingkat V (Optimal), yang menggambarkan progres penerapan mulai dari sekadar pengenalan kerangka kerja dasar hingga pada tahap yang terdokumentasi, terukur, dan terkelola secara optimal. Selain itu, hasil penilaian secara umum diklasifikasikan ke dalam kategori Baik dan Cukup Baik, yang berpotensi mendapatkan sertifikat, serta kategori Kurang dan Belum Memenuhi, yang membutuhkan perbaikan kerangka kerja dasar.

Melalui asesmen ini, PT Akebono Brake Astra Indonesia dapat memperoleh gambaran menyeluruh mengenai kesiapan keamanan informasi dan area mana yang perlu ditingkatkan. Proses pelaksanaan INDEKS KAMI dilakukan oleh BSSN melalui layanan bimbingan teknis, asesmen, dan konsultasi yang dilakukan secara elektronik.

INDEKS KAMI tidak ditujukan untuk menganalisis kelayakan atau efektivitas bentuk pengamanan yang ada, melainkan sebagai perangkat untuk memberikan gambaran kondisi kesiapan kerangka kerja keamanan informasi kepada Pimpinan Instansi. Implementasi Indeks KAMI dilakukan oleh penyelenggara layanan publik secara elektronik melalui Bimbingan Teknis, Asesmen, dan Konsultasi.



Gambar 3. 3 Tahapan Sertifikasi Indeks KAMI [11]

Target Pencapaian :

PT Akebono Brake Astra Indonesia saat ini sedang mempersiapkan diri untuk menjalani proses asesmen Indeks Keamanan Informasi (Indeks KAMI) yang disusun oleh Badan Siber dan Sandi Negara (BSSN). Asesmen ini menjadi salah satu target strategis perusahaan dalam penguatan sistem keamanan informasi nasional, sekaligus sebagai tahapan awal menuju implementasi dan sertifikasi ISO/IEC 27001:2022 secara internasional[11].

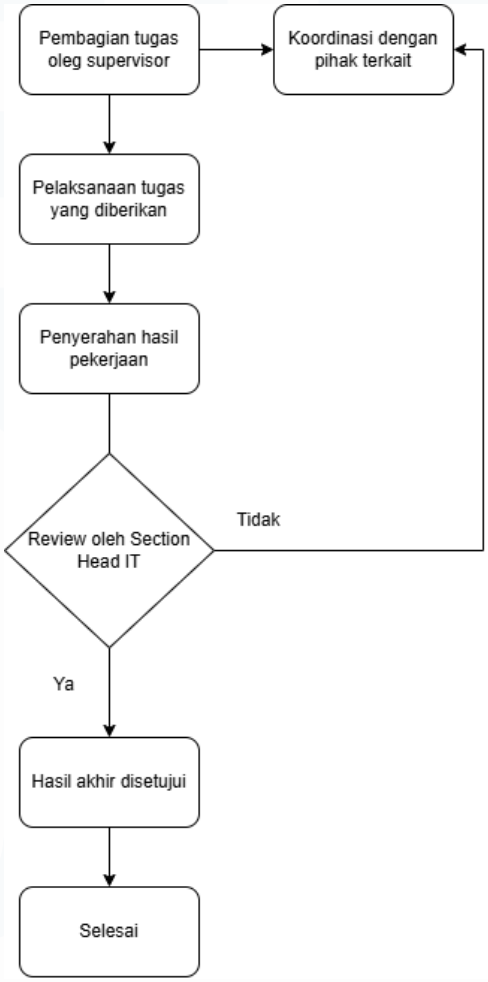
Target dari proses asesmen ini adalah agar PT Akebono Brake Astra Indonesia dapat memperoleh hasil evaluasi akhir dengan predikat “Baik” dan mencapai tingkat kematangan Level V (Optimal), yang mencerminkan sistem keamanan informasi yang tidak hanya berjalan sesuai standar, tetapi juga telah terdokumentasi dengan baik, dilaksanakan secara konsisten, serta dilakukan pemantauan dan peningkatan berkelanjutan.

Dengan hasil tersebut, perusahaan akan memiliki fondasi yang kuat dan kredibel untuk melanjutkan ke tahap sertifikasi ISO 27001, serta memperkuat posisi perusahaan dalam hal kepatuhan terhadap regulasi nasional dan daya saing global di tengah meningkatnya kompleksitas ancaman siber. Sertifikasi Indeks KAMI dari

BSSN nantinya juga akan menjadi bukti kesiapan PT Akebono Brake Astra Indonesia dalam menerapkan sistem manajemen keamanan informasi yang profesional, terintegrasi, dan sesuai dengan kebutuhan industri manufaktur otomotif modern.

3.2 Alur Kerja dan Koordinasi Magang

Dibawah ini merupakan alur kerja dan koordinasi magang mahasiswa pada PT Akebono Brake Astra Indonesia:



Gambar 3. 4 Flowchart alur kerja magang

Penjelasan alur kerja magang:

Gambar 3. 4 di atas merangkum proses kerja magang, dimulai dari penerimaan tugas hingga hasil akhir disetujui.

1. **Pembagian Tugas oleh Supervisor:** Alur kerja diawali dengan Supervisor atau Senior Staff IT Support yang memberikan tugas harian atau tugas proyek kepada mahasiswa magang.
2. **Pelaksanaan Tugas oleh Mahasiswa:** Mahasiswa mengerjakan tugas yang diberikan, seperti membuat dokumen (SOP, WI), mengumpulkan data, atau menyusun laporan.
3. **Koordinasi dengan Pihak Terkait:** Selama mengerjakan tugas, mahasiswa secara aktif berkoordinasi dengan berbagai pihak. Ini adalah proses yang berjalan paralel dengan pelaksanaan tugas. Pihak-pihak tersebut antara lain:
    a. **Supervisor/Senior Staff:** Untuk bimbingan teknis.
    b. **Section Head IT:** Untuk arahan strategis dan evaluasi.
    c. **Tim System Development:** Terkait dokumentasi sistem aplikasi.
    d. **Divisi HR:** Untuk pengumpulan data pendukung.

    Koordinasi ini dilakukan baik melalui meeting mingguan formal maupun komunikasi informal (seperti *WhatsApp Group)*.
4. **Penyerahan Hasil Pekerjaan:** Setelah selesai, hasil kerja diserahkan untuk ditinjau.
5. **Review & Validasi oleh Section Head IT**: Section Head IT, sebagai pembimbing utama, akan me-review hasil kerja untuk memastikan kesesuaian dengan standar perusahaan. Jika ada yang perlu diperbaiki, pekerjaan akan dikembalikan kepada mahasiswa.
6. **Hasil Akhir Disetujui:** Jika pekerjaan sudah sesuai, Section Head IT akan memberikan persetujuan.
7. **Selesai:** Hasil kerja yang telah disetujui siap untuk digunakan, baik untuk kebutuhan internal maupun untuk diserahkan ke pihak eksternal.

3.3 Tugas dan Uraian Kerja Magang

Adapun tugas dan uraian kerja magang peserta magang dalan mengerjakan sertifikasi INDEKS KAMI, yaitu seperti berikut:

3.3.1. Uraian Pekerjaan

Gambar 3. 5 Flow Persiapan Dokumen Assesment INDEKS KAMI

Penjelasan langkah-langkah persiapan dokumen INDEKS KAMI:

Bagan alur di atas menggambarkan langkah-langkah spesifik yang dilakukan oleh mahasiswa magang dalam membantu persiapan dokumen INDEKS KAMI:

1. **Pemahaman Kriteria Indeks KAMI:** Sebelum menyusun dokumen, tim harus memahami secara menyeluruh **struktur dan kriteria penilaian** dari Indeks KAMI. BSSN membagi penilaian ke dalam **5 domain utama**, yang masing-masing memiliki parameter dan indikator tertentu:
   a. **Tata Kelola**
      Fokus pada kebijakan, peran tanggung jawab, dan mekanisme pengawasan keamanan informasi dalam organisasi.
   b. **Manajemen Risiko**
      Menilai sejauh mana perusahaan mengidentifikasi, mengevaluasi, dan merespons risiko keamanan informasi.
   c. **Pengelolaan Aset**
      Meliputi identifikasi, klasifikasi, dan pengendalian terhadap aset informasi, termasuk perangkat keras, perangkat lunak, dan data.
   d. **Teknologi dan Keamanan Informasi**
      Mencakup perlindungan sistem, jaringan, aplikasi, serta penerapan teknologi keamanan seperti firewall, antivirus, dan enkripsi.
   e. **SDM dan Kesadaran Keamanan Informasi**
      Menilai kapasitas sumber daya manusia dalam memahami dan melaksanakan keamanan informasi, termasuk pelatihan dan kampanye kesadaran.

Pemahaman terhadap struktur ini penting agar **penyusunan dokumen dapat terarah**, setiap indikator dapat dipetakan dengan bukti nyata, dan tidak terjadi kesalahan interpretasi dalam proses asesmen.

2. **Identifikasi Dokumen yang Dibutuhkan:** Setelah memahami indikator penilaian, langkah selanjutnya adalah **menyusun daftar dokumen pendukung** yang dibutuhkan. Setiap indikator dalam Indeks KAMI harus ditopang oleh

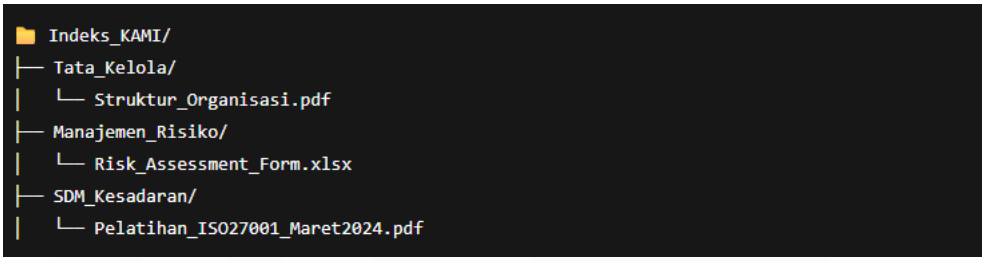
evidence-based documentation. Beberapa dokumen yang umum dibutuhkan antara lain:

a. **Kebijakan Keamanan Informasi (Information Security Policy)** Merupakan dokumen utama yang menjadi rujukan seluruh pengelolaan keamanan informasi perusahaan.
b. **SOP dan WI (Work Instruction)** terkait akses sistem, backup data, pengelolaan akun, dll.
c. **Struktur Organisasi** dan dokumen terkait tanggung jawab keamanan informasi.
d. **Hasil Audit Internal**, log keamanan sistem, rekaman insiden, dan hasil penanganan insiden.
e. **Bukti Pelatihan** atau sosialisasi keamanan informasi (materi, absensi, notulen).

a. Setiap dokumen yang diidentifikasi akan dihubungkan ke indikator tertentu. Disarankan untuk membuat **matrix pemetaan** antara indikator dan dokumen, agar tidak ada indikator yang terlewat.

3. **Pengumpulan dan Validasi Bukti:** Setelah daftar dokumen tersusun, tim mulai melakukan pengumpulan bukti dari masing-masing departemen atau unit kerja. Tahap ini tidak hanya sekadar mengumpulkan, tetapi juga mencakup **verifikasi dan validasi** bukti. Langkah-langkah penting dalam tahap ini meliputi:
   a. **Konsistensi** isi dokumen dengan kebutuhan indikator.
   b. **Keaslian dan keabsahan** dokumen, pastikan dokumen adalah versi terbaru.
   c. **Format penamaan** file harus konsisten (misal: `SOP_BackupData_v2_2024.pdf`).
   d. **Penyusunan struktur folder** digital yang sistematis berdasarkan domain.

   Contoh struktur folder:



Gambar 3. 6 Contoh Struktur Folder INDEKS KAMI

Dokumen yang tidak valid, kedaluwarsa, atau tidak sesuai indikator harus diperbarui atau diganti.

4. **Penyusunan Draft Jawaban Form Indeks KAMI:** Selanjutnya, tim mengisi formulir penilaian mandiri (self-assessment form) yang disediakan oleh BSSN. Proses ini mencakup:
   a. Menilai tingkat pencapaian terhadap setiap indikator (skor 0–4).
   b. Menyebutkan **referensi dokumen** sebagai bukti yang mendukung jawaban.
   c. Memberikan catatan tambahan jika diperlukan untuk menjelaskan konteks atau keterbatasan implementasi.

   Penyusunan ini tidak boleh dilakukan sembarangan, karena jawaban akan diuji saat proses **desktop assessment atau onsite assessment**. Penting untuk menjaga **konsistensi antara jawaban dan bukti** yang tersedia.
5. **Review Internal dan Perbaikan:** Setelah draft jawaban selesai, dilakukan proses **review internal**. Tahapan ini penting untuk:
   a. **Menemukan inkonsistensi** antara jawaban dan bukti.
   b. **Memperbaiki kesalahan** interpretasi terhadap indikator BSSN.
   c. **Simulasi audit**, di mana setiap bukti diuji apakah dapat ditampilkan, dijelaskan, dan memenuhi syarat.

   Review dilakukan oleh anggota tim yang tidak terlibat langsung dalam penulisan, atau oleh **komite ISMS** jika tersedia. Hasil review akan menjadi dasar untuk **revisi akhir** sebelum dokumen difinalisasi.
6. **Finalisasi Dokumen dan Bundling:** Tahap terakhir adalah mengemas seluruh dokumen dan hasil asesmen ke dalam satu paket yang siap dikirim ke BSSN atau disimpan untuk audit internal. Format pengemasan bisa berupa:

a. **Paket digital** (ZIP/RAR) berisi folder-folder yang telah ditata rapi.
b. **Upload ke sistem BSSN** jika diminta melalui platform digital.
c. **Dokumentasi internal** dalam sistem manajemen dokumen perusahaan (misal: SharePoint, Nextcloud, atau e-Document System).

Pada tahap ini penting untuk membuat **daftar isi atau index file** agar saat audit, semua dokumen dapat ditampilkan kembali dengan cepat dan mudah.

Melalui posisi ini, mahasiswi memperoleh pemahaman langsung tentang bagaimana sistem informasi tidak hanya digunakan untuk mendukung operasional teknis, tetapi juga sebagai sarana untuk membangun kerangka kerja keamanan informasi yang kokoh, yang mampu menjamin kerahasiaan, integritas, dan ketersediaan data perusahaan.

3.3.2. Timeline dan uraian kerja magang

Untuk mendukung kelancaran pelaksanaan kegiatan magang, disusunlah perencanaan kegiatan yang mencakup berbagai aktivitas utama sesuai dengan lingkup tugas yang telah ditetapkan. Perencanaan ini juga mencakup estimasi waktu pelaksanaan agar setiap kegiatan dapat berjalan secara terstruktur dan terukur. Berikut adalah tabel yang memuat timeline dan uraian kegiatan magang yang telah direalisasikan selama periode magang berlangsung:

Tabel 3. 1 Realisasi Rincian Kegiatan Magang

No	Tema Kegiatan	Kegiatan yang Dilakukan	Waktu Mulai	Waktu Selesai
1	Perkenalan dan Orientasi	Onboarding perusahaan, divisi IT, dan pemetaan jobdesc	06-01-2025	10-01-2025
2	Pemetaan Infrastruktur	Pendataan system, server, jaringan, aplikasi internal	13-01-2025	17-01-2025
3	Identifikasi Dokumen	Pengumpulan dan klasifikasi SOP, WI, PM	20-01-2025	21-01-2025

		terkait kemanan informasi		
4	Pre-Assesment ISO	Analisis kesenjangan dokumen terhadap standar ISO 27001	22-01-2025	24-01-2025
5	Kampanye Awareness	Desain dan pembuatan poster keamanan informasi untuk sosialisasi internal	26-01-2025	31-02-2025
6	Penyusunan Dokumen	Dreafting dokumen SOP/WI/PM berbasis ISO dan tamplate perusahaan	30-01-2025	05-02-2025
7	Struktur ISMS	Penyusunan scope ISMS, role & responsibilities, struktur keamanan informasi	03-02-2025	05-02-2025
8	Business Continuity Plan	Pembuatan dokumen BCP untuk mendukung control Annex ISO 27001	06-02-2025	14-02-2025
9	Review dan Revisi Dokumen	Revisi SOP dan WI berdasarkan feedback internal dan Akebono Jepang	17-02-2025	21-02-2025
10	Permintaan Data INDEKS KAMI	Pengerjaan permintaan data dan dokumen pendukung dari BSSN	28-02-2025	01-03-2025

11	Audit Internal	Pelaksanaan audit internal J-SOX dan asesmen resiko IT	04-03-2025	05-03-2025
12	Koordinasi BSSN	Meeting persiapan assessment dan koodinasi dengan tim BSSN	12-03-2025	17-03-2025
13	Validasi Struktur Keamanan	Finalisasi Struktur ISO 27002 dan subnet system	24-03-2025	24-03-2025
14	Finalisasi & Pemetaan Dokumen	Pengumpulan dokumen pemetaan control ke database	01-04-2025	12-04-2025
15	Pengisian IKAS	Mengisi intrumen evaluasi kemanan informasi dari BSSN	14-04-2025	21-04-2025
16	Revisi Akhir	Review dan penguatan dokumentasi ISO sebelum visitasi	22-05-2025	22-05-2025
17	Penyusunan Laporan	Menulis laporan akhir magang dan dokumentasi hasil kerja	03-06-2025	27-06-2025

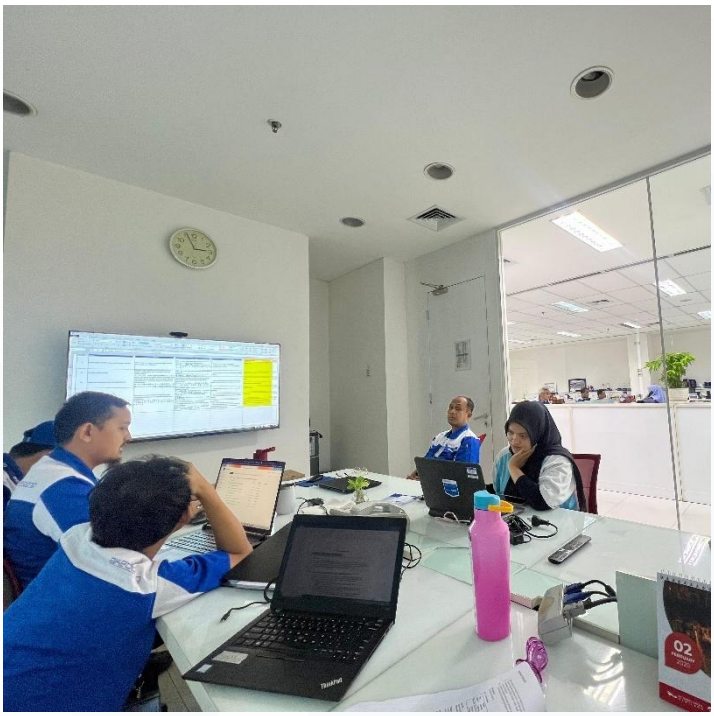
Tabel 3. 1 Realisasi Rincian Kegiatan Magang menampilkan rangkaian aktivitas yang dilakukan selama program magang berlangsung, mulai dari tanggal 6 Januari hingga 27 Juni 2025. Setiap kegiatan disusun berdasarkan tahapan kerja yang sudah direncanakan oleh Divisi IT PT Akebono Brake Astra Indonesia, dimulai dari orientasi dan pemahaman infrastruktur IT, lalu dilanjutkan dengan penyusunan dokumen, validasi, hingga keterlibatan langsung dalam asesmen keamanan informasi nasional melalui program INDEKS KAMI dari BSSN.

Tabel ini bukan hanya berfungsi sebagai catatan kegiatan, tapi juga menggambarkan peran aktif peserta magang dalam proyek-proyek yang nyata dan menantang, terutama di bidang keamanan informasi. Misalnya, kegiatan seperti penyusunan SOP, WI, dan PM, pengisian form asesmen, validasi struktur kontrol ISO 27001, serta koordinasi dengan berbagai unit di perusahaan menjadi pengalaman yang memperluas pemahaman peserta terhadap praktik keamanan informasi di industri.

Lebih dari sekadar daftar tugas, isi tabel ini juga merefleksikan proses pembelajaran yang berkelanjutan, di mana peserta mendapatkan kesempatan untuk mengembangkan keterampilan seperti penyusunan dokumentasi teknis, analisis risiko, manajemen aset informasi, hingga pemetaan struktur kontrol keamanan. Semua ini sejalan dengan standar dan praktik yang digunakan dalam sertifikasi ISO 27001 maupun penilaian kematangan keamanan informasi melalui INDEKS KAMI.

Seluruh kegiatan dijalankan secara bertahap dan kolaboratif—mulai dari tahap perencanaan, pelaksanaan teknis, validasi internal, hingga pembuatan laporan akhir. Proses ini menjadi pengalaman berharga yang menghubungkan antara ilmu yang dipelajari di bangku kuliah dengan realita kerja di dunia industri, khususnya di bidang teknologi informasi.

Dokumentasi berikut merupakan rangkaian kegiatan yang dilakukan selama program magang di PT Akebono Brake Astra Indonesia. Gambar-gambar ini mencerminkan aktivitas sehari-hari peserta magang, baik dalam hal teknis maupun koordinatif, serta memberikan gambaran umum tentang suasana dan lingkungan kerja di perusahaan.



Gambar 3. 7 Proses pengisian form assesmen mandiri Indeks KAMI, pengecekan dan pendataan kebutuhan dokumen serta evidence

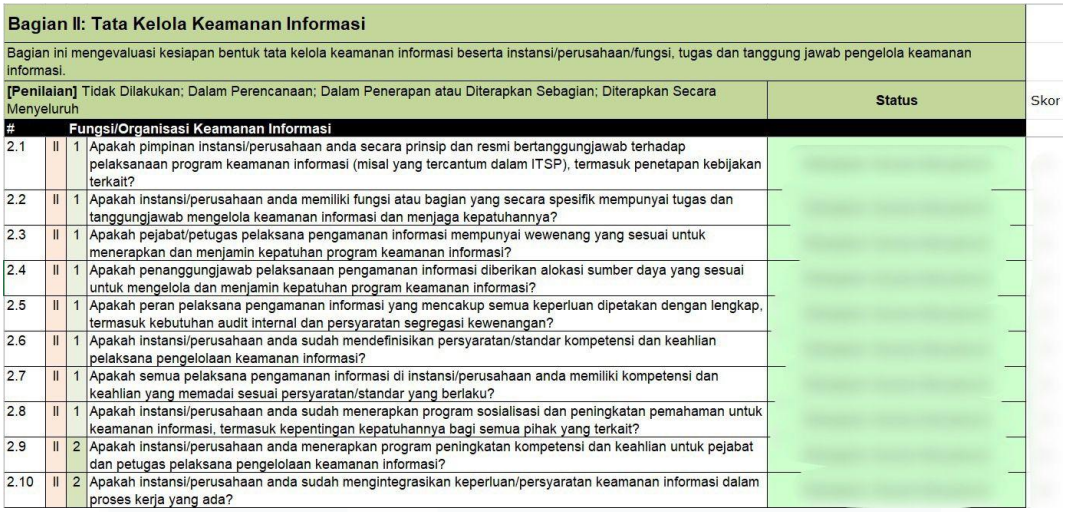
Gambar 3. 7 memperlihatkan proses pengisian formulir asesmen mandiri Indeks KAMI yang dilaksanakan secara kolaboratif oleh Tim IT dan Tim Audit Internal. Proses ini merupakan tahapan krusial dalam mempersiapkan organisasi menuju validasi resmi oleh Badan Siber dan Sandi Negara (BSSN). Pengisian formulir tidak dilakukan secara sembarangan, melainkan melalui tahapan yang terstruktur dan sistematis, diawali dengan pemetaan terhadap lima domain yang dinilai dalam Indeks KAMI, yaitu: Tata Kelola, Manajemen Risiko, Pengelolaan Aset, Teknologi dan Keamanan, serta Sumber Daya Manusia. Setiap domain memiliki sejumlah indikator yang harus diisi secara objektif dan didukung oleh bukti valid yang relevan.

Dalam pelaksanaannya, tim melakukan audit internal berbasis dokumen, yang mencakup peninjauan terhadap kebijakan keamanan informasi, prosedur kerja yang terdokumentasi, bukti pelatihan bagi sumber daya manusia, hingga catatan log sistem dan dokumentasi hasil pemantauan teknis. Mahasiswi magang terlibat secara aktif dalam proses identifikasi dan pengelompokan dokumen pendukung,

menyusun arsip digital, serta membuat direktori atau tautan referensi agar proses validasi nantinya dapat dilakukan secara efisien dan terstruktur. Proses ini juga disertai dengan penelaahan silang antaranggota tim guna memastikan bahwa tidak terdapat kekeliruan atau kekurangan pada dokumen yang disiapkan.

Diskusi internal menjadi bagian yang tidak terpisahkan, khususnya dalam mengisi indikator yang bersifat kualitatif dan memerlukan analisis mendalam. Sebagai contoh, untuk menilai sejauh mana perusahaan telah menerapkan mekanisme pengendalian risiko secara efektif dan terdokumentasi, diperlukan bukti berupa laporan evaluasi risiko, hasil pemantauan berkala, serta dokumen tindak lanjut terhadap temuan sebelumnya. Kegiatan ini turut mendorong terciptanya budaya kerja yang menjunjung tinggi prinsip akuntabilitas dan transparansi[15].

Lebih dari sekadar kontribusi terhadap hasil asesmen, keterlibatan mahasiswi magang dalam kegiatan ini juga memberikan pengalaman dan pembelajaran yang bermakna mengenai integrasi antara kebijakan manajemen, sistem teknologi informasi, dan proses audit internal dalam membangun tata kelola keamanan informasi yang selaras dengan standar nasional. Melalui kegiatan ini, peserta magang memperoleh pemahaman yang lebih dalam, tidak hanya mengenai aspek teknis pengamanan sistem informasi, tetapi juga keterampilan berpikir kritis, kemampuan bekerja dalam tim lintas fungsi, serta pemahaman terhadap pentingnya kepatuhan *(compliance)* dalam sistem manajemen yang lebih maju. Seluruh proses tersebut menjadi bagian yang tidak terpisahkan dari upaya PT Akebono Brake Astra Indonesia dalam mempersiapkan diri menuju sertifikasi ISO/IEC 27001, di manaasesmen Indeks KAMI menjadi fondasi awal yang strategis dan bernilai tinggi.



Bagian II: Tata Kelola Keamanan Informasi

Bagian ini mengevaluasi kesiapan bentuk tata kelola keamanan informasi beserta instansi/perusahaan/fungsi, tugas dan tanggung jawab pengelola keamanan informasi.

[Penilaian] Tidak Dilakukan; Dalam Perencanaan; Dalam Penerapan atau Diterapkan Sebagian; Diterapkan Secara Menyeluruh				**Status**	Skor
#			**Fungsi/Organisasi Keamanan Informasi**		
2.1	II	1	Apakah pimpinan instansi/perusahaan anda secara prinsip dan resmi bertanggungjawab terhadap pelaksanaan program keamanan informasi (misal yang tercantum dalam ITSP), termasuk penetapan kebijakan terkait?		
2.2	II	1	Apakah instansi/perusahaan anda memiliki fungsi atau bagian yang secara spesifik mempunyai tugas dan tanggungjawab mengelola keamanan informasi dan menjaga kepatuhannya?		
2.3	II	1	Apakah pejabat/petugas pelaksana pengamanan informasi mempunyai wewenang yang sesuai untuk menerapkan dan menjamin kepatuhan program keamanan informasi?		
2.4	II	1	Apakah penanggungjawab pelaksanaan pengamanan informasi diberikan alokasi sumber daya yang sesuai untuk mengelola dan menjamin kepatuhan program keamanan informasi?		
2.5	II	1	Apakah peran pelaksana pengamanan informasi yang mencakup semua keperluan dipetakan dengan lengkap, termasuk kebutuhan audit internal dan persyaratan segregasi kewenangan?		
2.6	II	1	Apakah instansi/perusahaan anda sudah mendefinisikan persyaratan/standar kompetensi dan keahlian pelaksana pengelolaan keamanan informasi?		
2.7	II	1	Apakah semua pelaksana pengamanan informasi di instansi/perusahaan anda memiliki kompetensi dan keahlian yang memadai sesuai persyaratan/standar yang berlaku?		
2.8	II	1	Apakah instansi/perusahaan anda sudah menerapkan program sosialisasi dan peningkatan pemahaman untuk keamanan informasi, termasuk kepentingan kepatuhannya bagi semua pihak yang terkait?		
2.9	II	2	Apakah instansi/perusahaan anda menerapkan program peningkatan kompetensi dan keahlian untuk pejabat dan petugas pelaksana pengelolaan keamanan informasi?		
2.10	II	2	Apakah instansi/perusahaan anda sudah mengintegrasikan keperluan/persyaratan keamanan informasi dalam proses kerja yang ada?		

Gambar 3. 8 Contoh Form Assesment INDEKS KAMI Untuk Bagian II: Tata Kelola Keamanan Informasi

Gambar 3.8 menunjukkan contoh form asesmen INDEKS KAMI pada Bagian II: Tata Kelola Keamanan Informasi, yang digunakan untuk mengevaluasi sejauh mana instansi atau perusahaan telah memiliki struktur tata kelola keamanan informasi yang baik dan terdokumentasi. Setiap butir dalam formulir ini berisi pertanyaan yang mengukur tanggung jawab, kewenangan, kompetensi, serta pelaksanaan program keamanan informasi di tingkat pimpinan hingga pelaksana teknis.

Formulir ini terdiri dari beberapa indikator, seperti keterlibatan pimpinan dalam menetapkan kebijakan keamanan, keberadaan peran dan tanggung jawab yang jelas, kecukupan sumber daya, hingga pemenuhan standar kompetensi dan pelatihan untuk personel terkait keamanan informasi. Penilaian dilakukan berdasarkan empat kategori status penerapan, yaitu Tidak Dilakukan, Dalam Perencanaan, Dalam Penerapan atau Diterapkan Sebagian, dan Diterapkan Secara Menyeluruh.

Hasil dari asesmen ini akan dikonversi menjadi skor yang menggambarkan tingkat kematangan dari aspek tata kelola, yang merupakan salah satu komponen

penting dalam evaluasi keseluruhan INDEKS KAMI sesuai standar keamanan informasi nasional dan internasional.

Bagian III: Pengelolaan Risiko Keamanan Informasi

Bagian ini mengevaluasi kesiapan penerapan pengelolaan risiko keamanan informasi sebagai dasar penerapan strategi keamanan informasi.

[Penilaian] Tidak Dilakukan; Dalam Perencanaan; Dalam Penerapan atau Diterapkan Sebagian; Diterapkan Secara Menyeluruh				**Status**
#			**Kajian Risiko Keamanan Informasi**	
3.1	II	1	Apakah instansi/perusahaan anda mempunyai program kerja pengelolaan risiko keamanan informasi yang terdokumentasi dan secara resmi digunakan?	
3.2	II	1	Apakah instansi/perusahaan anda sudah menetapkan penanggung jawab manajemen risiko dan eskalasi pelaporan status pengelolaan risiko keamanan informasi sampai ke tingkat pimpinan?	
3.3	II	1	Apakah instansi/perusahaan anda mempunyai kerangka kerja pengelolaan risiko keamanan informasi yang terdokumentasi dan secara resmi digunakan?	
3.4	II	1	Apakah kerangka kerja pengelolaan risiko ini mencakup definisi dan hubungan tingkat klasifikasi aset informasi, tingkat ancaman, kemungkinan terjadinya ancaman tersebut dan dampak kerugian terhadap instansi/perusahaan anda?	
3.5	II	1	Apakah instansi/perusahaan anda sudah menetapkan ambang batas tingkat risiko yang dapat diterima?	
3.6	II	1	Apakah instansi/perusahaan anda sudah mendefinisikan kepemilikan dan pihak pengelola *(custodian)* aset informasi yang ada, termasuk aset utama/penting dan proses kerja utama yang menggunakan aset tersebut?	
3.7	II	1	Apakah ancaman dan kelemahan yang terkait dengan aset informasi, terutama untuk setiap aset utama sudah teridentifikasi?	
3.8	II	1	Apakah dampak kerugian yang terkait dengan hilangnya/terganggunya fungsi aset utama sudah ditetapkan sesuai dengan definisi yang ada?	
3.9	II	1	Apakah instansi/perusahaan anda sudah menjalankan inisiatif analisa/kajian risiko keamanan informasi secara terstruktur terhadap aset informasi yang ada (untuk nantinya digunakan dalam mengidentifikasi langkah mitigasi atau penanggulangan yang menjadi bagian dari program pengelolaan keamanan informasi)?	

Gambar 3. 9 Contoh Form Assesment INDEKS KAMI Untuk Bagian III: Pengelolaan Risiko Keamanan Informasi

Gambar 3.9 menunjukkan contoh form asesmen INDEKS KAMI pada Bagian III: Pengelolaan Risiko Keamanan Informasi, yang digunakan untuk mengevaluasi sejauh mana instansi atau perusahaan telah menerapkan proses manajemen risiko terhadap aset informasi yang dimiliki. Formulir ini berisi sejumlah pertanyaan yang berkaitan dengan identifikasi, analisis, dan pengendalian risiko yang berdampak terhadap kerahasiaan, integritas, dan ketersediaan informasi.

Aspek yang dinilai mencakup keberadaan program pengelolaan risiko, penunjukan penanggung jawab, identifikasi aset dan kerentanannya, penilaian dampak dari ancaman yang mungkin terjadi, serta keberadaan strategi mitigasi risiko yang terdokumentasi. Penilaian dilakukan berdasarkan status implementasi: tidak dilakukan, dalam perencanaan, dalam penerapan sebagian, atau diterapkan secara menyeluruh.

Hasil dari asesmen ini memberikan gambaran tentang tingkat kematangan organisasi dalam mengelola risiko keamanan informasi. Evaluasi ini sangat penting untuk memastikan bahwa setiap ancaman potensial telah ditangani secara sistematis guna meminimalkan gangguan terhadap operasional bisnis dan menjaga kepercayaan pemangku kepentingan.

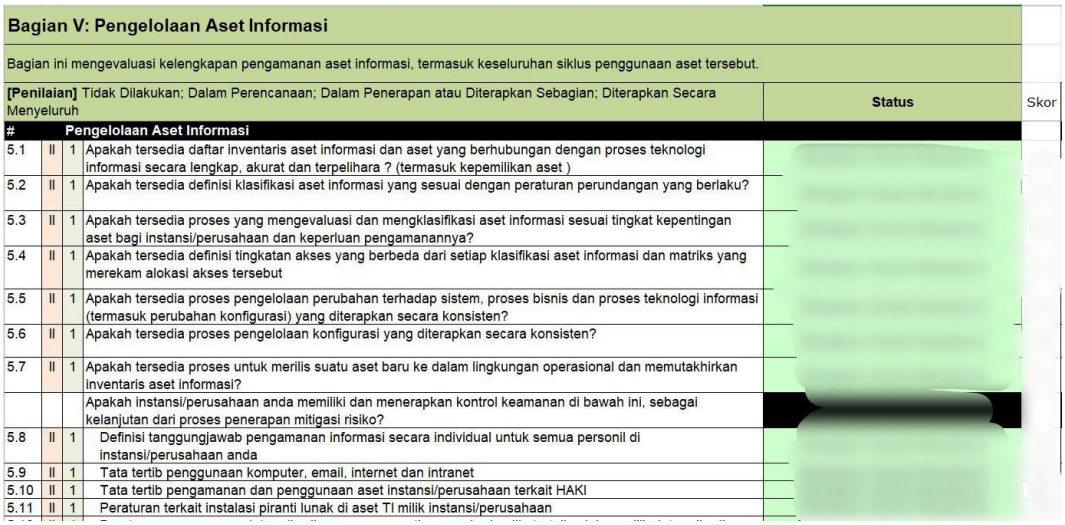
Bagian IV: Kerangka Kerja Pengelolaan Keamanan Informasi

Bagian ini mengevaluasi kelengkapan dan kesiapan kerangka kerja (kebijakan & prosedur) pengelolaan keamanan informasi dan strategi penerapannya.

[Penilaian] Tidak Dilakukan; Dalam Perencanaan; Dalam Penerapan atau Diterapkan Sebagian; Diterapkan Secara Menyeluruh				**Status**	Skor
4.3	II	1	Apakah tersedia mekanisme untuk mengelola dokumen kebijakan dan prosedur keamanan informasi, termasuk penggunaan daftar induk, distribusi, penarikan dari peredaran dan penyimpanannya?		
4.4	II	1	Apakah tersedia proses (mencakup pelaksana, mekanisme, jadwal, materi, dan sasarannya) untuk mengkomunikasikan kebijakan keamanan informasi (dan perubahannya) kepada semua pihak terkait, termasuk pihak ketiga?		
4.5	II	1	Apakah keseluruhan kebijakan dan prosedur keamanan informasi yang ada merefleksikan kebutuhan mitigasi dari hasil kajian risiko keamanan informasi, maupun sasaran/obyetif tertentu yang ditetapkan oleh pimpinan instansi/perusahaan?		
4.6	II	1	Apakah tersedia proses untuk mengidentifikasi kondisi yang membahayakan keamanan infomasi dan menetapkannya sebagai insiden keamanan informasi untuk ditindak lanjuti sesuai prosedur yang diberlakukan?		
4.7	II	1	Apakah aspek keamanan informasi yang mencakup pelaporan insiden, menjaga kerahasiaan, HAKI, tata tertib penggunaan dan pengamanan aset maupun layanan TIK tercantum dalam kontrak dengan pihak ketiga?		
4.8	II	2	Apakah konsekwensi dari pelanggaran kebijakan keamanan informasi sudah didefinisikan, dikomunikasikan dan ditegakkan?		
4.9	II	2	Apakah tersedia prosedur resmi untuk mengelola suatu pengecualian terhadap penerapan keamanan informasi, termasuk proses untuk menindak lanjuti konsekwensi dari kondisi ini?		
4.10	III	2	Apakah organisasi anda sudah menerapkan kebijakan dan prosedur operasional untuk mengelola implementasi *security patch*, alokasi tanggung jawab untuk memonitor adanya rilis *security patch* baru, memastikan pemasangannya dan melaporkannya?		
4.11	III	2	Apakah organisasi anda sudah membahas aspek keamanan informasi dalam manajemen proyek yang terkait dengan ruang lingkup?		

Gambar 3. 10 Contoh Form Assesment INDEKS KAMI Untuk Bagian IV: Kerangka Kerja Pengelolaan Keamanan Informasi

Gambar 3. 10 formulir asesmen INDEKS KAMI pada Bagian IV: Kerangka Kerja Pengelolaan Keamanan Informasi, yang berfungsi untuk mengevaluasi kelengkapan kebijakan dan prosedur dalam mengelola keamanan informasi di suatu organisasi. Penilaian dilakukan melalui serangkaian pertanyaan yang mencakup aspek dokumentasi kebijakan, komunikasi internal, mitigasi risiko, hingga kesiapan dalam merespons insiden keamanan. Setiap jawaban dikategorikan ke dalam empat status implementasi, yaitu: Tidak Dilakukan, Dalam Perencanaan, Dalam Penerapan Sebagian, dan Diterapkan Secara Menyeluruh. Hasil dari asesmen ini memberikan gambaran menyeluruh mengenai tingkat kematangan organisasi dalam membangun sistem tata kelola keamanan informasi yang efektif dan sesuai dengan kerangka kerja yang ditetapkan oleh BSSN.



Bagian V: Pengelolaan Aset Informasi

Bagian ini mengevaluasi kelengkapan pengamanan aset informasi, termasuk keseluruhan siklus penggunaan aset tersebut.

[Penilaian] Tidak Dilakukan; Dalam Perencanaan; Dalam Penerapan atau Diterapkan Sebagian; Diterapkan Secara Menyeluruh				**Status**	Skor
#			**Pengelolaan Aset Informasi**		
5.1	II	1	Apakah tersedia daftar inventaris aset informasi dan aset yang berhubungan dengan proses teknologi informasi secara lengkap, akurat dan terpelihara ? (termasuk kepemilikan aset)		
5.2	II	1	Apakah tersedia definisi klasifikasi aset informasi yang sesuai dengan peraturan perundangan yang berlaku?		
5.3	II	1	Apakah tersedia proses yang mengevaluasi dan mengklasifikasi aset informasi sesuai tingkat kepentingan aset bagi instansi/perusahaan dan keperluan pengamanannya?		
5.4	II	1	Apakah tersedia definisi tingkatan akses yang berbeda dari setiap klasifikasi aset informasi dan matriks yang merekam alokasi akses tersebut		
5.5	II	1	Apakah tersedia proses pengelolaan perubahan terhadap sistem, proses bisnis dan proses teknologi informasi (termasuk perubahan konfigurasi) yang diterapkan secara konsisten?		
5.6	II	1	Apakah tersedia proses pengelolaan konfigurasi yang diterapkan secara konsisten?		
5.7	II	1	Apakah tersedia proses untuk merilis suatu aset baru ke dalam lingkungan operasional dan memutakhirkan inventaris aset informasi?		
			Apakah instansi/perusahaan anda memiliki dan menerapkan kontrol keamanan di bawah ini, sebagai kelanjutan dari proses penerapan mitigasi risiko?		
5.8	II	1	Definisi tanggungjawab pengamanan informasi secara individual untuk semua personil di instansi/perusahaan anda		
5.9	II	1	Tata tertib penggunaan komputer, email, internet dan intranet		
5.10	II	1	Tata tertib pengamanan dan penggunaan aset instansi/perusahaan terkait HAKI		
5.11	II	1	Peraturan terkait instalasi piranti lunak di aset TI milik instansi/perusahaan		

Gambar 3. 11 Contoh Form Assesment INDEKS KAMI Untuk Bagian V: Pengelolaan Aset Informasi

Gambar 3.11 menunjukkan contoh form asesmen INDEKS KAMI pada Bagian V: Pengelolaan Aset Informasi, yang digunakan untuk mengevaluasi sejauh mana instansi atau perusahaan telah menerapkan pengamanan terhadap aset informasi yang dimiliki. Formulir ini memuat sejumlah pertanyaan yang berkaitan dengan pencatatan, klasifikasi, dan pengendalian aset informasi, termasuk perangkat keras, perangkat lunak, serta data yang digunakan dalam proses bisnis dan sistem teknologi informasi.

Aspek yang dinilai mencakup keberadaan daftar inventaris aset informasi, proses klasifikasi berdasarkan tingkat kepentingan dan kebutuhan pengamanan, penilaian hak akses terhadap aset, serta prosedur pengelolaan konfigurasi dan perbaruan aset. Selain itu, juga dinilai keberadaan aturan penggunaan perangkat teknologi seperti komputer, internet, dan email, serta kepatuhan terhadap kebijakan terkait hak kekayaan intelektual dan instalasi perangkat lunak resmi.

Penilaian dilakukan berdasarkan status implementasi, yaitu: tidak dilakukan, dalam perencanaan, dalam penerapan sebagian, atau diterapkan secara menyeluruh. Hasil dari asesmen ini memberikan gambaran tentang tingkat kesiapan dan kematangan organisasi dalam melindungi aset informasinya. Evaluasi ini penting dilakukan untuk memastikan bahwa aset informasi dikelola secara

sistematis dan aman, guna mendukung kelangsungan operasional dan menjaga keandalan sistem informasi organisasi.

Bagian VI: Teknologi dan Keamanan Informasi

Bagian ini mengevaluasi kelengkapan, konsistensi dan efektifitas penggunaan teknologi dalam pengamanan aset informasi.

[Penilaian] Tidak Dilakukan; Dalam Perencanaan; Dalam Penerapan atau Diterapkan Sebagian; Diterapkan Secara Menyeluruh				**Status**	Skor
#			**Pengamanan Teknologi**		
6.1	II	1	Apakah layanan TIK (sistem komputer) yang menggunakan internet sudah dilindungi dengan lebih dari 1 lapis pengamanan?		
6.2	II	1	Apakah jaringan komunikasi disegmentasi sesuai dengan kepentingannya (pembagian instansi/perusahaan, kebutuhan aplikasi, jalur akses khusus, dll)?		
6.3	II	1	Apakah tersedia konfigurasi standar untuk keamanan sistem bagi keseluruhan aset jaringan, sistem dan aplikasi, yang dimutakhirkan sesuai perkembangan (standar industri yang berlaku) dan kebutuhan?		
6.4	II	1	Apakah instansi/perusahaan anda secara rutin menganalisa kepatuhan penerapan konfigurasi standar yang ada?		
6.5	II	1	Apakah jaringan, sistem dan aplikasi yang digunakan secara rutin dipindai untuk mengidentifikasi kemungkinan adanya celah kelemahan atau perubahan/keutuhan konfigurasi?		
6.6	II	1	Apakah keseluruhan infrastruktur jaringan, sistem dan aplikasi dirancang untuk memastikan ketersediaan (rancangan redundan) sesuai kebutuhan/persyaratan yang ada?		
6.7	II	1	Apakah keseluruhan infrastruktur jaringan, sistem dan aplikasi dimonitor untuk memastikan ketersediaan kapasitas yang cukup untuk kebutuhan yang ada?		
6.8	II	1	Apakah setiap perubahan dalam sistem informasi secara otomatis terekam di dalam log?		
6.9	II	1	Apakah upaya akses oleh yang tidak berhak secara otomatis terekam di dalam log?		
6.10	II	1	Apakah semua log dianalisa secara berkala untuk memastikan akurasi, validitas dan kelengkapan isinya (untuk kepentingan jejak audit dan forensik)?		
6.11	II	1	Apakah instansi/perusahaan anda menerapkan enkripsi untuk melindungi aset informasi penting sesuai kebijakan pengelolaan yang ada?		
6.12	III	2	Apakah instansi/perusahaan anda mempunyai standar dalam menggunakan enkripsi?		

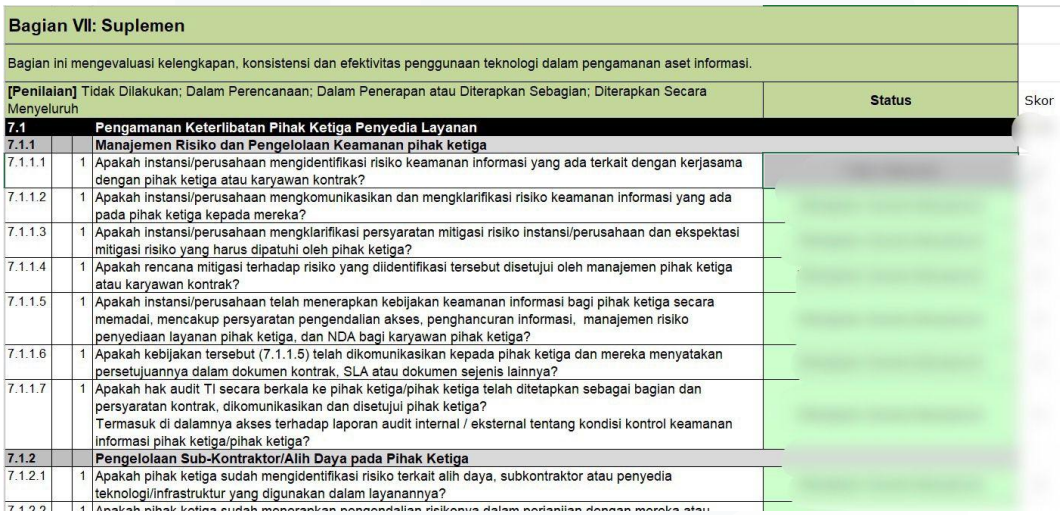
Gambar 3. 12 Contoh Form Assesment INDEKS KAMI Untuk Bagian VI: Teknologi dan Keamanan Informasi

Gambar 3.12 menunjukkan contoh form asesmen INDEKS KAMI pada Bagian VI: Teknologi dan Keamanan Informasi, yang digunakan untuk mengevaluasi sejauh mana instansi atau perusahaan telah menerapkan teknologi serta pengamanan yang memadai dalam mendukung perlindungan aset informasi. Formulir ini berisi pertanyaan-pertanyaan yang mengkaji aspek teknis dari sistem dan jaringan yang digunakan, serta efektivitas kontrol keamanan yang telah diterapkan.

Aspek yang dinilai dalam bagian ini mencakup perlindungan sistem terhadap akses tidak sah, standar keamanan terhadap jaringan dan aplikasi, pengelolaan konfigurasi sistem, serta pemantauan sistem secara rutin untuk memastikan ketersediaan dan keandalan layanan. Selain itu, formulir ini juga mengevaluasi keberadaan mekanisme audit, pengelolaan log akses, perlindungan informasi penting, serta penerapan enkripsi sebagai salah satu langkah teknis keamanan informasi.

Penilaian dilakukan berdasarkan tingkat implementasi, yaitu: tidak dilakukan, dalam perencanaan, dalam penerapan sebagian, atau diterapkan secara

menyeluruh. Hasil asesmen ini memberikan gambaran tentang kesiapan infrastruktur teknologi dan efektivitas sistem keamanan yang dimiliki oleh organisasi. Evaluasi ini penting untuk memastikan bahwa penggunaan teknologi dilakukan secara aman, konsisten, dan sesuai standar yang berlaku guna mencegah kebocoran data dan gangguan terhadap operasional perusahaan.



Bagian VII: Suplemen				
Bagian ini mengevaluasi kelengkapan, konsistensi dan efektivitas penggunaan teknologi dalam pengamanan aset informasi.				
[Penilaian] Tidak Dilakukan; Dalam Perencanaan; Dalam Penerapan atau Diterapkan Sebagian; Diterapkan Secara Menyeluruh			**Status**	Skor
7.1		**Pengamanan Keterlibatan Pihak Ketiga Penyedia Layanan**		
7.1.1		**Manajemen Risiko dan Pengelolaan Keamanan pihak ketiga**		
7.1.1.1	1	Apakah instansi/perusahaan mengidentifikasi risiko keamanan informasi yang ada terkait dengan kerjasama dengan pihak ketiga atau karyawan kontrak?		
7.1.1.2	1	Apakah instansi/perusahaan mengkomunikasikan dan mengklarifikasi risiko keamanan informasi yang ada pada pihak ketiga kepada mereka?		
7.1.1.3	1	Apakah instansi/perusahaan mengklarifikasi persyaratan mitigasi risiko instansi/perusahaan dan ekspektasi mitigasi risiko yang harus dipatuhi oleh pihak ketiga?		
7.1.1.4	1	Apakah rencana mitigasi terhadap risiko yang diidentifikasi tersebut disetujui oleh manajemen pihak ketiga atau karyawan kontrak?		
7.1.1.5	1	Apakah instansi/perusahaan telah menerapkan kebijakan keamanan informasi bagi pihak ketiga secara memadai, mencakup persyaratan pengendalian akses, penghancuran informasi, manajemen risiko penyediaan layanan pihak ketiga, dan NDA bagi karyawan pihak ketiga?		
7.1.1.6	1	Apakah kebijakan tersebut (7.1.1.5) telah dikomunikasikan kepada pihak ketiga dan mereka menyatakan persetujuannya dalam dokumen kontrak, SLA atau dokumen sejenis lainnya?		
7.1.1.7	1	Apakah hak audit TI secara berkala ke pihak ketiga/pihak ketiga telah ditetapkan sebagai bagian dan persyaratan kontrak, dikomunikasikan dan disetujui pihak ketiga? Termasuk di dalamnya akses terhadap laporan audit internal / eksternal tentang kondisi kontrol keamanan informasi pihak ketiga/pihak ketiga?		
7.1.2		**Pengelolaan Sub-Kontraktor/Alih Daya pada Pihak Ketiga**		
7.1.2.1	1	Apakah pihak ketiga sudah mengidentifikasi risiko terkait alih daya, subkontraktor atau penyedia teknologi/infrastruktur yang digunakan dalam layanannya?		
7.1.2.2	1	Apakah pihak ketiga sudah menerapkan pengendalian risikonya dalam perjanjian dengan mereka atau		

Gambar 3. 13 Contoh Form Assesment INDEKS KAMI Untuk Bagian VII: Suplemen

Gambar 3.13 menunjukkan contoh form asesmen INDEKS KAMI pada Bagian VII: Suplemen, yang difokuskan pada evaluasi pengelolaan keamanan informasi yang melibatkan pihak ketiga. Bagian ini bertujuan untuk memastikan bahwa instansi atau perusahaan memiliki prosedur dan kebijakan yang memadai dalam mengelola risiko keamanan informasi yang timbul dari kerja sama dengan pihak luar, seperti vendor, kontraktor, atau penyedia layanan.

Formulir ini mencakup sejumlah pertanyaan yang mengkaji bagaimana instansi mengidentifikasi risiko keamanan dari pihak ketiga, mengkomunikasikan ekspektasi keamanan, dan melakukan klarifikasi tanggung jawab serta mitigasi risiko kepada mitra eksternal. Selain itu, dievaluasi pula apakah ada dokumen tertulis seperti perjanjian atau kebijakan yang disepakati bersama pihak ketiga terkait perlindungan data, kerahasiaan, serta akses ke sistem informasi.

Aspek yang dinilai dalam bagian ini terbagi menjadi dua subbagian, yaitu Manajemen Risiko dan Pengelolaan Keamanan Pihak Ketiga serta Pengelolaan

Sub-Kontraktor/Alih Daya pada Pihak Ketiga. Penilaian dilakukan berdasarkan tingkat implementasi: tidak dilakukan, dalam perencanaan, dalam penerapan sebagian, atau diterapkan secara menyeluruh.

Melalui asesmen ini, instansi dapat mengevaluasi sejauh mana mereka telah memiliki kontrol dan perlindungan yang memadai terhadap risiko-risiko yang muncul dari keterlibatan pihak luar. Evaluasi ini sangat penting untuk menjaga integritas dan keamanan data organisasi ketika bekerja sama dengan pihak ketiga, terutama dalam era digital yang rentan terhadap kebocoran dan penyalahgunaan informasi.

Gambar 3. 14 Review reguler membahas tindak lanjut kebutuhan dokumen dan evidence Indeks KAMI

Gambar 3. 14 menunjukkan kegiatan review yang dilakukan secara rutin oleh tim yang terlibat dalam proses asesmen Indeks KAMI. Kegiatan ini merupakan bagian penting dari mekanisme pengendalian internal yang bertujuan untuk memantau perkembangan, mengevaluasi kelengkapan, serta memastikan bahwa seluruh dokumen dan bukti (evidence) yang dibutuhkan dalam asesmen telah dipersiapkan secara tepat, akurat, dan sesuai dengan standar yang ditetapkan oleh Badan Siber dan Sandi Negara (BSSN).

Proses review ini dilakukan secara berkala, baik melalui pertemuan langsung (offline) maupun diskusi daring (online), dengan melibatkan anggota dari Tim IT, Tim Audit Internal, serta perwakilan dari Komite ISMS. Setiap sesi review dimanfaatkan untuk meninjau status masing-masing domain dalam Indeks KAMI, memverifikasi apakah seluruh indikator sudah terjawab dengan benar, dan mengecek keberadaan dokumen pendukung yang relevan. Jika ditemukan adanya kekurangan atau dokumen yang belum tersedia, maka tim segera menyusun rencana tindak lanjut, seperti melakukan koordinasi lintas divisi, meminta revisi kebijakan, atau mengumpulkan bukti teknis tambahan dari sistem IT.

Mahasiswi magang yang terlibat dalam kegiatan ini tidak hanya berperan sebagai pengamat, tetapi juga turut membantu dalam pencatatan hasil rapat, pembaruan status dokumentasi, serta penyusunan daftar checklist dokumen yang perlu dilengkapi. Melalui keterlibatan aktif dalam proses review, peserta magang memperoleh pemahaman mendalam mengenai pentingnya proses monitoring, validasi, dan verifikasi dalam siklus manajemen keamanan informasi.

Selain sebagai sarana evaluasi internal, kegiatan review juga menjadi media pembelajaran kolektif yang mendorong kesadaran seluruh anggota tim terhadap urgensi pengelolaan keamanan informasi secara terstruktur. Hal ini sangat penting untuk memastikan bahwa proses asesmen berjalan tidak hanya sebagai kegiatan administratif semata, tetapi sebagai bagian dari budaya tata kelola yang profesional dan berkelanjutan di lingkungan PT Akebono Brake Astra Indonesia. Dengan demikian, hasil asesmen Indeks KAMI nantinya benar-benar mencerminkan kondisi aktual dan kesiapan perusahaan dalam menghadapi proses sertifikasi ISO/IEC 27001 pada tahap selanjutnya.

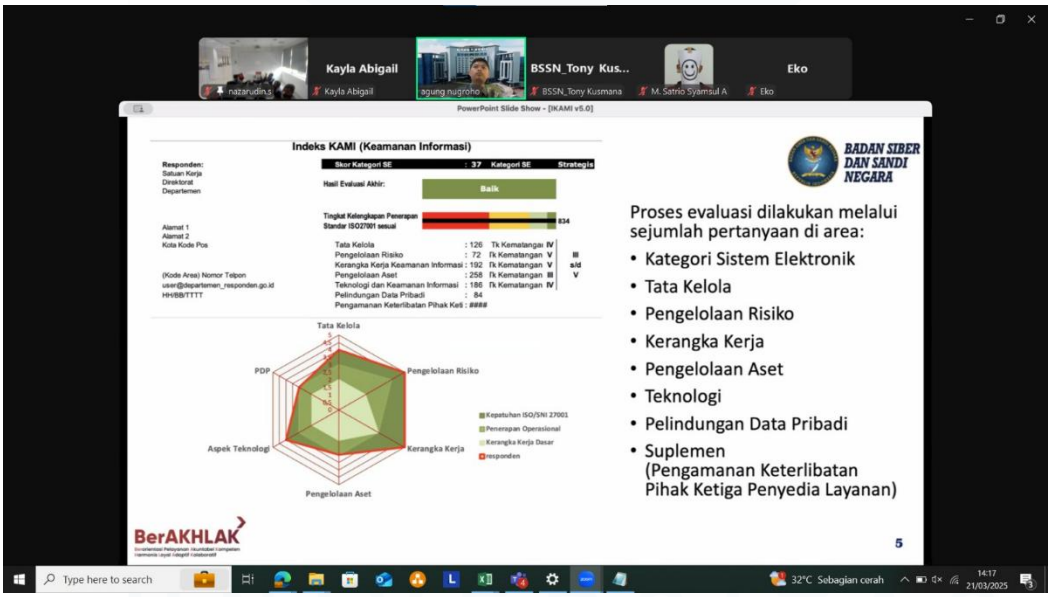
Gambar 3. 15 Desktop assesment oleh assesor Indeks KAMI dari BSSN secara online

Gambar 3. 15 memperlihatkan kegiatan desktop assessment yang dilaksanakan oleh asesor Indeks KAMI dari Badan Siber dan Sandi Negara (BSSN) secara daring (online). Kegiatan ini dilakukan sekitar satu minggu setelah PT Akebono Brake Astra Indonesia secara resmi mengirimkan atau men-submit formulir asesmen mandiri Indeks KAMI melalui sistem BSSN. Desktop assessment merupakan tahap awal dari proses validasi, di mana tim asesor dari BSSN melakukan peninjauan terhadap seluruh isian form asesmen mandiri yang telah diisi oleh pihak perusahaan, beserta dokumen pendukung yang telah dilampirkan.

Dalam sesi ini, asesor melakukan klarifikasi terhadap beberapa poin jawaban yang dinilai memerlukan penjelasan lebih lanjut, serta mencermati konsistensi antara pernyataan yang diisi pada form dengan bukti objektif yang disampaikan. Kegiatan ini menjadi forum penting bagi kedua belah pihak untuk saling berdiskusi secara terbuka dan profesional terkait status kematangan keamanan informasi yang telah dicapai oleh perusahaan. Tim dari PT Akebono Brake Astra Indonesia yang terdiri dari perwakilan IT, Audit Internal, dan Komite ISMS turut hadir secara lengkap untuk menjawab pertanyaan, memberikan penjelasan teknis, serta memaparkan alur pengelolaan keamanan informasi yang telah diterapkan di perusahaan.

Hasil dari kegiatan desktop assessment ini berupa feedback resmi dari asesor BSSN, yang berisi catatan penguatan, rekomendasi perbaikan, serta pernyataan awal mengenai tingkat kelengkapan dan kesiapan dokumen sebelum dilakukan validasi lapangan secara onsite. Dengan adanya tahapan ini, perusahaan mendapatkan gambaran awal mengenai sejauh mana hasil asesmen mandiri telah sesuai dengan standar yang diharapkan, serta memiliki waktu untuk melakukan penyempurnaan dokumen atau penguatan kontrol sebelum tahap akhir validasi di lokasi.

Kegiatan ini juga memberikan nilai tambah bagi mahasiswi magang, karena dapat menyaksikan secara langsung proses komunikasi formal antara perusahaan dan instansi pemerintah dalam konteks pemenuhan standar keamanan informasi nasional. Selain itu, mahasiswi juga memperoleh pengalaman praktis dalam memahami alur asesmen eksternal dan pentingnya dokumentasi yang akurat, relevan, dan terstruktur dalam proses tata kelola keamanan informasi modern.



Gambar 3. 16 Hasil assesmen mandiri Indeks KAMI PT. Akebono Brake Astra Indonesia

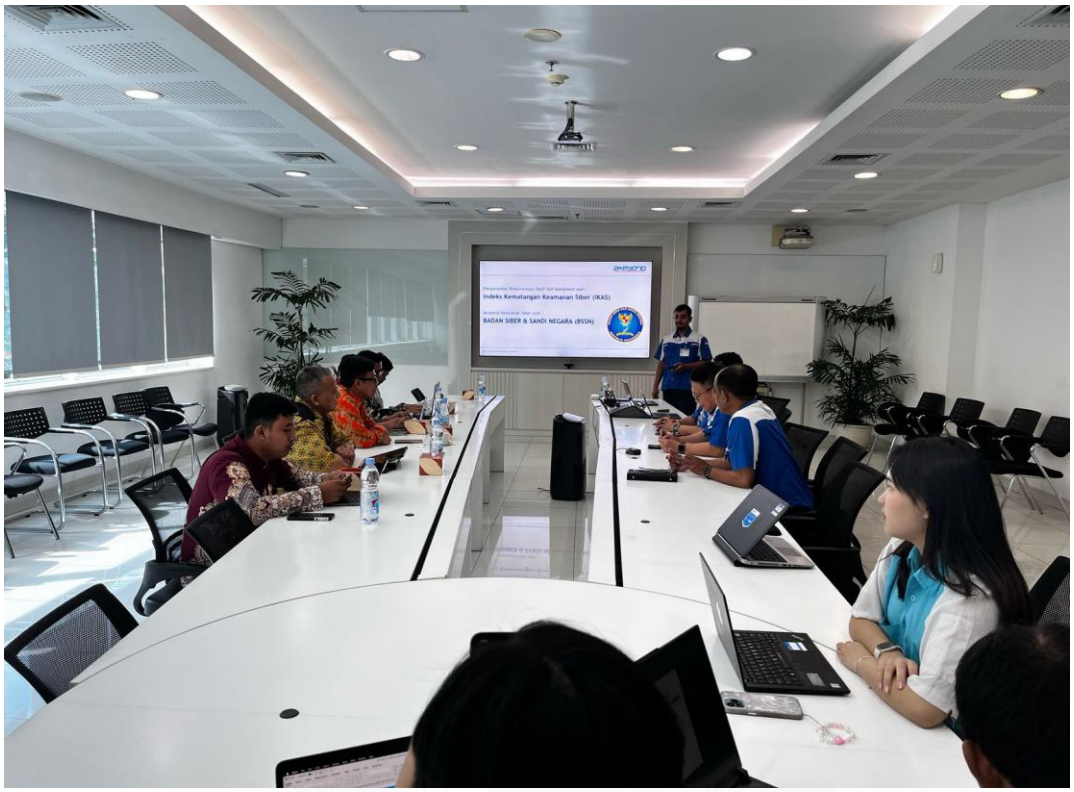
Gambar 3. 16 memperlihatkan hasil dari asesmen mandiri Indeks KAMI yang dilaksanakan oleh PT Akebono Brake Astra Indonesia. Hasil ini merupakan keluaran akhir dari rangkaian proses asesmen yang telah dilalui, mulai dari

pengisian formulir mandiri, pengumpulan bukti objektif, review internal, hingga validasi oleh pihak Badan Siber dan Sandi Negara (BSSN) melalui tahapan desktop assessment. Penilaian dilakukan berdasarkan lima domain utama yang menjadi fokus dalam Indeks KAMI, yaitu: Tata Kelola Keamanan Informasi, Manajemen Risiko, Pengelolaan Aset, Aspek Teknologi dan Keamanan, serta Sumber Daya Manusia.

Berdasarkan evaluasi yang dilakukan oleh tim asesor dari BSSN, tingkat kematangan keamanan informasi PT Akebono Brake Astra Indonesia secara keseluruhan berada pada Level IV (Terdefinisi dan Terkelola). Ini menunjukkan bahwa sebagian besar proses dan kebijakan yang berkaitan dengan keamanan informasi telah terdokumentasi dengan baik, dilaksanakan secara konsisten, dan diawasi melalui mekanisme evaluasi serta pengendalian internal yang memadai. Proses ini juga mencerminkan adanya koordinasi lintas fungsi yang berjalan efektif dalam menjaga keberlanjutan sistem keamanan informasi di lingkungan perusahaan.

Adapun hasil akhir yang diberikan oleh BSSN terhadap asesmen Indeks KAMI ini adalah dengan predikat **"BAIK"**, yang mengindikasikan bahwa perusahaan telah memiliki sistem keamanan informasi yang cukup matang dan siap untuk menghadapi tantangan serta risiko dunia siber, baik dalam konteks operasional sehari-hari maupun dalam persiapan menuju standar internasional seperti ISO/IEC 27001. Capaian ini juga menjadi dasar yang kuat bagi perusahaan untuk terus melanjutkan program peningkatan berkelanjutan di bidang tata kelola teknologi informasi dan keamanan siber.

Bagi mahasiswi magang, keterlibatan dalam seluruh tahapan asesmen hingga memperoleh hasil resmi dari BSSN ini menjadi pengalaman berharga. Mahasiswi tidak hanya memahami proses penilaian teknis dan administratif, tetapi juga memperoleh wawasan langsung mengenai pentingnya sinergi antara regulasi nasional, kepatuhan organisasi, serta penerapan kontrol keamanan yang berbasis risiko di dunia industri.



Gambar 3. 17 Onsite assesment Indeks KAMI oleh assesor dan Dirjen BSSN serta Board of Director PT. Akebono Brake Astra Indonesia

Gambar 3. 17 menampilkan proses asesmen lapangan (onsite assessment) Indeks KAMI yang dilaksanakan secara langsung oleh tim asesor dari Badan Siber dan Sandi Negara (BSSN) dan turut dihadiri oleh Direktur Jenderal BSSN serta Board of Director PT Akebono Brake Astra Indonesia. Kehadiran pihak manajemen puncak dalam kegiatan ini menunjukkan komitmen perusahaan yang tinggi terhadap tata kelola keamanan informasi serta kepatuhan terhadap standar nasional yang berlaku.

Dalam sesi onsite assessment ini, tim asesor melakukan validasi menyeluruh dan terperinci terhadap setiap item yang telah diisi dalam formulir asesmen mandiri. Proses validasi tidak hanya dilakukan melalui peninjauan dokumen, tetapi juga melalui verifikasi langsung terhadap bukti atau evidence yang mendukung pernyataan dalam asesmen, seperti SOP, laporan audit internal, hasil monitoring sistem, serta dokumentasi aktivitas keamanan informasi yang telah diterapkan oleh perusahaan.

Selain pemeriksaan dokumen, kegiatan ini juga mencakup survey lapangan ke area operasional dan infrastruktur teknologi informasi, termasuk ruang server, sistem kontrol akses, serta mekanisme backup dan pemulihan data. Tujuannya adalah untuk memastikan bahwa apa yang telah didokumentasikan dalam asesmen mandiri benar-benar diimplementasikan secara nyata di lapangan dan tidak hanya bersifat administratif.

Hasil dari onsite assessment ini menunjukkan bahwa terdapat kesesuaian antara data asesmen mandiri dan kondisi aktual di lapangan, yang mengindikasikan bahwa proses asesmen mandiri telah dilakukan secara jujur, obyektif, dan sesuai dengan pedoman yang ditetapkan oleh BSSN. Dengan demikian, tingkat kematangan keamanan informasi PT Akebono Brake Astra Indonesia tetap dinyatakan berada pada Level IV (Terdefinisi dan Terkelola), dan hasil akhir asesmen resmi ditetapkan dengan predikat **"BAIK".**

Bagi mahasiswi magang, keterlibatan dalam kegiatan onsite assessment ini memberikan pengalaman berharga karena dapat melihat secara langsung bagaimana proses audit eksternal dilakukan oleh instansi pemerintah, serta bagaimana perusahaan menyiapkan diri, berkomunikasi, dan mempresentasikan hasil kerjanya dalam forum resmi. Hal ini memperkuat pemahaman mahasiswi mengenai pentingnya sinergi antara dokumen, implementasi teknis, dan komitmen manajemen dalam membangun sistem keamanan informasi yang tangguh dan berkelanjutan.

Gambar 3. 18 Validasi dan survey lapangan terkait penerapan keamaan informasi PT Akebono Brake Astra Indonesia

Gambar 3.18 menunjukkan proses validasi dan survei lapangan yang dilakukan di area produksi PT Akebono Brake Astra Indonesia sebagai bagian dari penerapan dan penilaian keamanan informasi. Kegiatan ini melibatkan tim internal yang sedang melakukan observasi langsung terhadap fasilitas dan prosedur yang berkaitan dengan pengelolaan sistem informasi dan perlindungan aset digital perusahaan. Survei lapangan ini bertujuan untuk memastikan bahwa kebijakan keamanan informasi yang telah disusun benar-benar dijalankan di lingkungan operasional, sekaligus sebagai bentuk komitmen perusahaan terhadap keamanan data dan keberlangsungan sistem teknologi informasi.

3.4 Kendala yang Ditemukan

Selama pelaksanaan magang, beberapa kendala dan kesulitan yang ditemukan antara lain:

1. **Tingkat kematangan belum mencapai target**
   Hasil asesmen menunjukkan bahwa tingkat kematangan sistem keamanan informasi berada di Level IV, sedangkan target awal PT Akebono Brake Astra Indonesia adalah mencapai Level V.
2. **Aspek tata kelola belum optimal**
   Terdapat kekurangan dalam dokumentasi, struktur organisasi, serta kontrol dan monitoring tata kelola keamanan informasi secara menyeluruh.
3. **Perlindungan data pribadi masih lemah**
   Belum seluruh mekanisme dan prosedur perlindungan data pribadi (PDP) diimplementasikan sesuai standar, terutama dalam hal pengendalian akses dan kebijakan retensi data.
4. **Pengelolaan aset informasi belum lengkap**
   Inventarisasi aset belum sepenuhnya terdokumentasi, serta klasifikasi dan kontrol terhadap aset informasi masih terbatas.

3.5 Solusi atas Kendala yang Ditemukan

Untuk mengatasi berbagai kendala yang ditemukan selama proses kerja magang, beberapa langkah dan solusi proaktif telah diimplementasikan, antara lain:

1. **Peningkatan ke level kematangan V**
   Menyusun roadmap perbaikan dan peningkatan sistem keamanan informasi secara bertahap dan terstruktur untuk mencapai target Level V.

2. **Perbaikan tata kelola keamanan informasi**
   a. Menyusun ulang dan melengkapi kebijakan serta prosedur terkait tata kelola keamanan informasi.

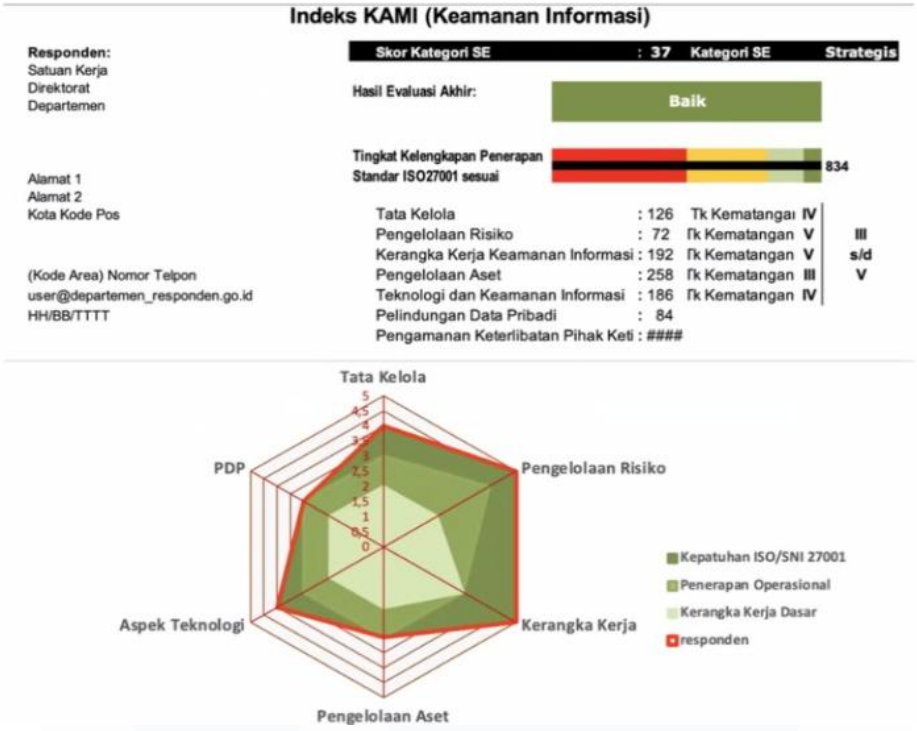
b. Menetapkan struktur tim keamanan informasi yang jelas, lengkap dengan tanggung jawab dan otoritasnya.
c. Melakukan audit internal secara berkala dan menindaklanjuti hasil temuan

3. Peningkatan Perlindungan Data Pribadi (PDP)

a. Menyusun dan mensosialisasikan kebijakan perlindungan data pribadi.
b. Menyediakan pelatihan kepada karyawan terkait pentingnya menjaga informasi pribadi.
c. Mengimplementasikan kontrol akses berbasis hak akses minimal dan monitoring aktivitas pengguna.

4. Penyempurnaan Pengelolaan Aset Informasi

a. Melakukan identifikasi dan pencatatan seluruh aset informasi (hardware, software, data).
b. Menerapkan klasifikasi aset berdasarkan nilai dan risiko.
c. Menyusun SOP terkait pemeliharaan dan penghapusan aset.



Gambar 3. 19 Laporan Hasil Evaluasi INDEKS KAMI (Keamanan Informasi) berdasarkan Tingkat Kematangan dan Kesesuaian dengan Standar ISO 27001

Gambar 3.19 menampilkan laporan hasil evaluasi INDEKS KAMI (Keamanan Informasi) yang digunakan untuk menilai sejauh mana penerapan keamanan informasi dalam suatu instansi atau unit kerja sesuai dengan standar ISO/IEC 27001. Pada bagian atas gambar ditunjukkan skor kategori SE sebesar 37, yang termasuk dalam kategori strategis, dengan hasil evaluasi akhir yang dinyatakan “Baik”. Penilaian ini juga menunjukkan bahwa tingkat kelengkapan penerapan terhadap standar ISO 27001 telah sesuai, ditandai dengan indikator warna hijau yang mendominasi grafik evaluasi.

Bagian tengah gambar mencantumkan hasil penilaian dari berbagai domain keamanan informasi, seperti tata kelola, pengelolaan risiko, kerangka kerja keamanan informasi, pengelolaan aset, teknologi dan keamanan informasi, serta perlindungan data pribadi. Masing-masing domain diberikan nilai dan tingkat kematangan, mulai dari tingkat kematangan III hingga V, yang menunjukkan kemajuan dan kesiapan implementasi keamanan informasi di berbagai aspek.

Domain pengamanan keterlibatan pihak ketiga belum diisi, kemungkinan karena masih dalam tahap awal evaluasi.

Di bagian bawah, ditampilkan diagram radar yang memperlihatkan pencapaian masing-masing domain dibandingkan dengan tiga kategori penerapan, yaitu kerangka dasar, penerapan operasional, dan kepatuhan terhadap ISO/SNI 27001. Area yang diarsir menunjukkan sejauh mana organisasi telah memenuhi indikator-indikator keamanan informasi, berdasarkan hasil isian dari responden. Secara keseluruhan, gambar ini memberikan gambaran visual dan kuantitatif mengenai kekuatan dan kelemahan penerapan keamanan informasi di instansi, serta menjadi dasar dalam merumuskan strategi peningkatan keamanan secara menyeluruh.