BANK INDONESIA

PETUNJUK TEKNIS

TENTANG
PELAPORAN KEAMANAN SISTEM INFORMASI DAN KETAHANAN SIBER BAGI PENYELENGGARA SISTEM PEMBAYARAN, PELAKU PASAR UANG DAN PASAR VALUTA ASING, SERTA PIHAK LAIN YANG DIATUR DAN DIAWASI BANK INDONESIA (KKS)

BANK INDONESIA

2025

DAFTAR ISI

BAB I
KETENTUAN UMUM

A. Latar Belakang

Bank Indonesia telah menerbitkan Peraturan Bank Indonesia Nomor 2 Tahun 2024 tanggal 18 April 2024 (PBI KKS) dan Peraturan Anggota Dewan Gubernur Nomor 24 Tahun 2024 tanggal 30 Desember 2025 (PADG KKS) yang merupakan pengaturan penerapan dan pengawasan KKS bagi Penyelenggara Sistem Pembayaran, pelaku Pasar Uang dan Pasar Valuta Asing, serta pihak lain yang diatur dan diawasi oleh Bank Indonesia yang selanjutnya disebut Penyelenggara.

Penerbitan PBI KKS dan PADG KKS merupakan upaya mitigasi terhadap peningkatan risiko siber yang dapat menyebabkan kerugian keuangan dan mengganggu stabilitas Sistem Keuangan, melalui penguatan pengawasan dan kolaborasi dalam pencegahan serta penanganan insiden siber.

Penerapan KKS oleh Penyelenggara perlu dilaporkan kepada Bank Indonesia secara tahunan dan secara insidental pada saat terjadi insiden siber.

Petunjuk teknis Pelaporan Keamanan Sistem Informasi Dan Ketahanan Siber bagi Penyelenggara memuat pengaturan yang lebih spesifik dan teknis mengenai penyampaian laporan KKS dari Penyelenggara ke Bank Indonesia.

B. Dasar Hukum

Peraturan yang menjadi dasar hukum penerbitan petunjuk teknis adalah Peraturan Anggota Dewan Gubernur Nomor 24 Tahun 2024 tentang Keamanan Sistem Informasi dan Ketahanan Siber Bagi Penyelenggara Sistem Pembayaran, Pelaku Pasar Uang dan Pasar Valuta Asing, Serta Pihak Lain Yang Diatur dan Diawasi Bank Indonesia, dengan rincian sebagai berikut:

1. Berdasarkan Pasal 52 PADG KKS, Penyelenggara wajib menyampaikan data/informasi kepada Bank Indonesia meliputi area tata kelola, pencegahan, dan penanganan terkait penerapan KKS dalam bentuk dokumen, data mentah, dan/atau data olahan.
2. Berdasarkan Pasal 45 ayat (2) huruf b, ayat (3), dan ayat (4) PADG KKS diatur bahwa Penyelenggara wajib menyampaikan laporan insidental pada saat terjadi insiden siber kepada Bank Indonesia meliputi:
   a. Notifikasi awal insiden siber paling lama 1 (satu) jam setelah insiden siber diketahui oleh Penyelenggara.
   b. Laporan insiden siber paling lama 3 (tiga) hari kalender setelah insiden siber terjadi.
3. Berdasarkan Pasal 10 ayat (2), Pasal 17 ayat (4), Pasal 52 ayat (2) huruf b PADG KKS, diatur bahwa Penyelenggara wajib menyampaikan laporan tahunan kepada Bank Indonesia meliputi:
   a. Laporan tingkat kematangan KKS.
   b. Laporan hasil identifikasi Infrastruktur Informasi Vital (IIV).
4. Berdasarkan Pasal 53 ayat (4) PADG KKS, laporan tahunan sebagaimana dimaksud pada angka 3 wajib disampaikan Penyelenggara paling lambat tanggal 31 Januari untuk periode pelaporan tahun sebelumnya.
   Contoh: Laporan tahunan periode 2025 disampaikan paling lambat tanggal 31 Januari 2026.

5. Berdasarkan Pasal 53 ayat (6) PADG KKS, diatur bahwa dalam hal diperlukan Bank Indonesia sewaktu-waktu dapat meminta Penyelenggara untuk menyampaikan laporan tingkat kematangan KKS terkini.

C. Tujuan

Petunjuk teknis ini disusun dengan tujuan untuk:

1. Meningkatkan KKS Penyelenggara untuk mencegah dan menangani dampak Serangan Siber.
2. Meningkatkan manajemen Risiko Siber Penyelenggara.
3. Menguatkan pengawasan dan kolaborasi dalam pencegahan Insiden Siber dan/atau penanganan Insiden Siber yang terjadi pada Penyelenggara.

D. Definisi atau Batasan Pengertian

Dalam petunjuk teknis ini yang dimaksud dengan:

1. Penyelenggara adalah pihak yang diatur dan diawasi Bank Indonesia yang mempunyai risiko Siber baik secara sistemik maupun nonsistemik bagi Sistem Keuangan.
2. Kerentanan Siber adalah kelemahan, kerawanan, atau kekurangan yang terdapat pada Siber sehingga berdampak negatif terhadap bisnis dan/atau layanan operasional Penyelenggara.
3. Ancaman Siber adalah suatu keadaan yang berpotensi mengeksploitasi Kerentanan Siber.
4. Serangan Siber adalah upaya mengeksploitasi Kerentanan Siber.
5. Insiden Siber adalah Serangan Siber yang mengganggu kelancaran bisnis dan/atau layanan operasional Penyelenggara yang memerlukan respons dan/atau pemulihan.
6. Risiko Siber adalah kemungkinan terjadinya Insiden Siber dan dampak yang diakibatkan dari Insiden Siber.
7. Keamanan Sistem Informasi dan Ketahanan Siber yang selanjutnya disebut KKS adalah kondisi terjaganya kerahasiaan, keutuhan, serta ketersediaan informasi dan/atau Sistem Informasi Penyelenggara dari Serangan Siber dan terjaganya kelangsungan bisnis Penyelenggara melalui tindakan antisipatif, adaptif, dan proaktif terhadap Ancaman Siber serta kemampuan Penyelenggara untuk melakukan respons dan pemulihan dengan cepat terhadap Insiden Siber.
8. Sistem Informasi adalah keterpaduan antara komponen data, informasi, sistem aplikasi, infrastruktur teknologi informasi, proses, dan/atau manusia yang saling berinteraksi untuk mencapai suatu tujuan.
9. Siber adalah ruang yang bersifat virtual yang dibentuk dari Sistem Informasi.
10. Penyelenggara dengan Kewajiban Pelaporan Penuh adalah Penyelenggara yang memiliki layanan digitalisasi yang terhubung secara langsung dengan sistem aplikasi dan/atau infrastruktur teknologi informasi Bank Indonesia dan/atau sistem aplikasi dan/atau infrastruktur teknologi informasi Penyelenggara lain.
11. Penyelenggara dengan Kewajiban Pelaporan Sebagian adalah Penyelenggara yang menggunakan sistem aplikasi dan/atau infrastruktur teknologi informasi pihak lain (*client*) atau sistem aplikasi dan/atau infrastruktur teknologi informasi sendiri yang tidak terhubung secara langsung dengan sistem aplikasi dan/atau infrastruktur teknologi informasi Bank Indonesia dan/atau Penyelenggara lain.

12. Sistem Pelaporan KKS Bank Indonesia adalah Sistem Informasi untuk mendukung pengelolaan pelaporan dan pengawasan KKS.

E. Ruang Lingkup

Ruang lingkup pengaturan petunjuk teknis ini yaitu:

1. Jenis Laporan KKS.
2. Tata Cara Penyampaian Laporan KKS.

F. Objek Penerapan

Objek penerapan petunjuk teknis ini yaitu:

1. Petunjuk teknis ini berlaku bagi Penyelenggara dengan Kewajiban Pelaporan Penuh dan Penyelenggara dengan Kewajiban Pelaporan Sebagian.
2. Petunjuk teknis ini tidak berlaku bagi Penyelenggara yang menggunakan *end user device* atau perangkat *stand-alone* lainnya dan/atau perangkat analog.
3. Bank Indonesia menyampaikan melalui surat tertulis daftar Penyelenggara yang termasuk dalam Penyelenggara dengan Kewajiban Pelaporan Penuh dan Penyelenggara dengan Kewajiban Pelaporan Sebagian.

BAB II
JENIS LAPORAN KKS

A. Notifikasi Awal Insiden Siber

Penyelenggara dengan Kewajiban Pelaporan Penuh dan Penyelenggara dengan Kewajiban Pelaporan Sebagian menyampaikan notifikasi awal Insiden Siber yang paling sedikit memuat:

1. Informasi kontak pelapor yang terdiri dari nama Penyelenggara, alamat kantor pusat Penyelenggara, nomor telepon, nama narahubung, nomor telepon narahubung.
2. Informasi umum Insiden Siber yang terdiri dari tanggal dan waktu terjadinya Insiden Siber, tanggal dan waktu Insiden Siber diketahui, jenis Insiden Siber, titik serangan Insiden Siber, respons awal Penyelenggara pasca Insiden Siber.
3. Asesmen awal dampak Insiden Siber yang terdiri dari penilaian awal atas dampak Insiden Siber Penyelenggara.

Format notifikasi awal Insiden Siber sebagaimana **Lampiran 1**.

B. Laporan Insiden Siber

Penyelenggara dengan Kewajiban Pelaporan Penuh dan Penyelenggara dengan Kewajiban Pelaporan Sebagian menyampaikan laporan Insiden Siber yang paling sedikit memuat:

1. Informasi kontak pelapor yang terdiri dari nama Penyelenggara, alamat kantor pusat Penyelenggara, nomor telepon, nama narahubung, nomor telepon narahubung, tanggal penyampaian notifikasi awal.
2. Informasi umum Insiden Siber yang terdiri dari tanggal dan waktu terjadinya Insiden Siber, tanggal dan waktu Insiden Siber diketahui, jenis Insiden Siber, titik serangan Insiden Siber, respons awal Penyelenggara pasca Insiden Siber.
3. Analisis komprehensif dampak Insiden Siber yang terdiri dari penilaian dampak Insiden Siber terhadap:
    a. Ketersediaan dan operasional layanan Penyelenggara;
    b. Finansial Penyelenggara;
    c. Reputasi Penyelenggara;
    d. Aspek hukum dan kepatuhan Penyelenggara;
    e. Pihak ketiga; dan
    f. Dampak lainnya.
4. Forensik Insiden Siber yang terdiri dari durasi terjadinya Insiden Siber, langkah yang dilakukan yang meliputi eskalasi, penanggulangan, dan pemulihan, keterlibatan pihak ketiga, pihak yang menerima informasi Insiden Siber, informasi pendukung, sumber serangan, serta faktor penyebab Insiden Siber.
5. Kesimpulan dan tindak lanjut perbaikan yang terdiri dari kesimpulan, langkah perbaikan, dan target waktu penyelesaian Insiden Siber.

Format laporan Insiden Siber sebagaimana **Lampiran 2**.

C. Laporan Tingkat Kematangan KKS

Penyelenggara dengan Kewajiban Pelaporan Penuh dan Penyelenggara dengan Kewajiban Pelaporan Sebagian menyampaikan laporan tingkat kematangan KKS yang disusun berdasarkan hasil asesmen mandiri Penyelenggara terhadap penerapan KKS di area tata kelola, pencegahan, dan penanganan dengan memperhatikan:

1. Kategori Penyelenggara dengan Kewajiban Pelaporan Penuh atau Kewajiban Pelaporan sebagian.
2. Pernah atau tidaknya Penyelenggara mengalami Insiden Siber.

Dalam hal Penyelenggara mengalami lebih dari satu kali Insiden Siber pada periode laporan yang sama, maka asesmen laporan tingkat kematangan KKS menggunakan Insiden Siber dengan tingkat kerusakan (*severity)* Insiden Siber yang paling signifikan.

Cakupan asesmen mandiri penerapan KKS oleh Penyelenggara dilakukan dengan ketentuan:

1. Penyelenggara dengan **Kewajiban Pelaporan Penuh** dan **pernah mengalami Insiden Siber setelah diterbitkannya PADG KKS**, melakukan asesmen mandiri terhadap penerapan KKS meliputi **318 indikator** dengan rincian:

Area	Dimensi	Faktor	Total Indikator
Tata Kelola	Strategi dan Kebijakan	Rencana Strategis KKS	11
		Kebijakan, Standar, dan Prosedur	7
		Fungsi Organisasi	36
	Budaya KKS	Implementasi Program Budaya KKS	11
	Total Indikator Tata Kelola		65
Pencegahan	Identifikasi	Penyusunan Profil Risiko	37
		Penginian Profil Risiko	3
	Proteksi	Pembangunan Sistem Pertahanan	56
		Pelindungan Data dan/atau Informasi	18
	Deteksi	Pemantauan	27
		Analisis Hasil Pemantauan	4
		Analisis Serangan Siber	7
		Analisis *Malicious/Unauthorized Code*	6
		Pemeliharaan dan Pengujian Sistem Deteksi	4
	Total Indikator Pencegahan		162
Penanganan	Respons	Penyusunan Rencana Penanganan & Pemulihan Insiden Siber	26
		Pelaksanaan Simulasi dan Uji coba	11
		Penanganan Insiden Siber	22
		Komunikasi Tindakan Penanganan Insiden Siber	6
	Pemulihan	Pengembalian Layanan Sebagaimana Kondisi Normal	13
		Perbaikan Berkelanjutan	6
		Komunikasi Tindakan Pemulihan Insiden Siber	4

Area	Dimensi	Faktor	Total Indikator
		Evaluasi Penanganan	3
	Total Indikator Penanganan		91
Total Indikator			**318**

Format laporan tingkat kematangan KKS bagi Penyelenggara dengan Kewajiban Pelaporan Penuh dan pernah mengalami Insiden Siber sebagaimana **Lampiran 3.1.**

2. Penyelenggara dengan **Kewajiban Pelaporan Penuh** dan **belum pernah mengalami Insiden Siber setelah diterbitkannya PADG KKS** menyampaikan laporan tahunan tingkat kematangan KKS kepada Bank Indonesia, dengan cakupan asesmen mandiri terhadap penerapan KKS meliputi **267 indikator** dengan rincian:

Area	Dimensi	Faktor	Total Indikator
Tata Kelola	Strategi dan Kebijakan	Rencana Strategis KKS	11
		Kebijakan, Standar, dan Prosedur	7
		Fungsi Organisasi	36
	Budaya KKS	Implementasi Program Budaya KKS	11
	Total Indikator Tata Kelola		65
Pencegahan	Identifikasi	Penyusunan Profil Risiko	37
		Penginian Profil Risiko	3
	Proteksi	Pembangunan Sistem Pertahanan	56
		Pelindungan Data dan/atau Informasi	18
	Deteksi	Pemantauan	27
		Analisis Hasil Pemantauan	4
		Analisis Serangan Siber	7
		Analisis *Malicious/Unauthorized Code*	6
		Pemeliharaan dan Pengujian Sistem Deteksi	4
	Total Indikator Pencegahan		162
Penanganan	Respons	Penyusunan Rencana Penanganan & Pemulihan Insiden Siber	26
		Pelaksanaan Simulasi dan Uji coba	11
	Pemulihan	Evaluasi Penanganan	3
	Total Indikator Penanganan		40
Total Indikator			**267**

Format laporan tingkat kematangan KKS bagi Penyelenggara dengan Kewajiban Pelaporan Penuh dan belum pernah mengalami Insiden Siber sebagaimana **Lampiran 3.2.**

3. Penyelenggara dengan **Kewajiban Pelaporan Sebagian** dan **pernah mengalami Insiden Siber setelah diterbitkannya PADG KKS** menyampaikan laporan tahunan tingkat kematangan KKS kepada Bank Indonesia, dengan cakupan asesmen mandiri terhadap penerapan KKS meliputi **52 indikator** dengan rincian:

Area	Dimensi	Faktor	Total Indikator
Tata Kelola	Strategi dan Kebijakan	Kebijakan, Standar, dan Prosedur	5
		Fungsi Organisasi	3
	Budaya KKS	Implementasi Program Budaya KKS	1
	Total Indikator Tata Kelola		9
Pencegahan	Identifikasi	Penyusunan Profil Risiko	9
		Penginian Profil Risiko	1
	Proteksi	Pembangunan Sistem Pertahanan	14
		Pelindungan Data dan/atau Informasi	1
	Deteksi	Pemantauan	6
		Pemeliharaan dan Pengujian Sistem Deteksi	1
	Total Indikator Pencegahan		32
Penanganan	Respons	Penyusunan Rencana Penanganan & Pemulihan Insiden Siber	2
		Penanganan Insiden Siber	8
	Pemulihan	Perbaikan Berkelanjutan	1
	Total Indikator Penanganan		11
Total Indikator			**52**

Format laporan tingkat kematangan KKS bagi Penyelenggara dengan Kewajiban Pelaporan Sebagian dan Pernah mengalami Insiden Siber sebagaimana **Lampiran 3.3.**

4. Penyelenggara dengan **Kewajiban Pelaporan Sebagian** dan **belum pernah mengalami Insiden Siber setelah diterbitkannya PADG KKS** menyampaikan laporan tahunan tingkat kematangan KKS kepada Bank Indonesia, dengan cakupan asesmen mandiri terhadap penerapan KKS meliputi **43 indikator** dengan rincian:

Area	Dimensi	Faktor	Total Indikator
Tata Kelola	Strategi dan Kebijakan	Kebijakan, Standar, dan Prosedur	5
		Fungsi Organisasi	3
	Budaya KKS	Implementasi Program Budaya KKS	1
	Total Indikator Tata Kelola		9
Pencegahan	Identifikasi	Penyusunan Profil Risiko	9
		Penginian Profil Risiko	1
	Proteksi	Pembangunan Sistem Pertahanan	14
		Pelindungan Data dan/atau Informasi	1
	Deteksi	Pemantauan	6
		Pemeliharaan dan Pengujian Sistem Deteksi	1
	Total Indikator Pencegahan		32

Area	Dimensi	Faktor	Total Indikator
Penanganan	Respons	Penyusunan Rencana Penanganan & Pemulihan Insiden Siber	2
	Total Indikator Penanganan		2
Total Pernyataan			**43**

Format laporan tingkat kematangan KKS bagi Penyelenggara dengan Kewajiban Pelaporan Sebagian dan Belum Pernah mengalami Insiden Siber sebagaimana **Lampiran 3.4.**

5. Penyelenggara memberikan nilai untuk setiap indikator berdasarkan asesmen mandiri dengan ketentuan:
   a. Ya: Indikator pernyataan sesuai sepenuhnya dengan kondisi Penyelenggara.
   b. Parsial: Indikator pernyataan sesuai secara parsial dengan kondisi Penyelenggara.
   c. Tidak: Indikator pernyataan tidak sesuai dengan kondisi Penyelenggara.
6. Untuk setiap indikator dengan nilai "Ya" atau "Parsial", laporan tingkat kematangan KKS disertai dengan lampiran bukti pendukung dan penjelasan.
7. Lampiran bukti pendukung disusun secara terkonsolidasi menjadi 7 file yang mewakili setiap dimensi. Khusus untuk Penyelenggara dengan Kewajiban Pelaporan Sebagian dan belum pernah mengalami Insiden Siber, Lampiran bukti pendukung disusun secara terkonsolidasi menjadi 6 file.
8. Bank Indonesia akan melakukan verifikasi laporan tingkat kematangan KKS setidak-tidaknya berdasarkan lampiran bukti pendukung yang disampaikan oleh Penyelenggara.

D. Laporan Hasil Identifikasi Infrastruktur Informasi Vital (IIV)

Penyelenggara dengan Kewajiban Pelaporan Penuh dan Penyelenggara dengan Kewajiban Pelaporan Sebagian menyampaikan laporan hasil identifikasi Infrastruktur Informasi Vital (IIV) yang disusun berdasarkan hasil asesmen mandiri Penyelenggara dengan melakukan inventarisasi sistem aplikasi dan/atau infrastruktur teknologi informasi yang berdampak luas terhadap stabilitas Sistem Keuangan terkait pelaksanaan kegiatan Sistem Pembayaran, Pasar Uang dan Pasar Valuta Asing, dan/atau kegiatan usaha penukaran valuta asing bukan Bank. Format laporan hasil identifikasi Infrastruktur Informasi Vital (IIV) sebagaimana **Lampiran 4**.

BAB III
TATA CARA PENYAMPAIAN LAPORAN KKS

A. Waktu Penyampaian Laporan

1. Notifikasi Awal Insiden Siber

Penyelenggara dengan Kewajiban Pelaporan Penuh dan Penyelenggara dengan Kewajiban Pelaporan Sebagian menyampaikan notifikasi awal Insiden Siber paling lama 1 (satu) jam setelah Insiden Siber diketahui oleh Penyelenggara kepada Bank Indonesia.

2. Laporan Insiden Siber

Penyelenggara dengan Kewajiban Pelaporan Penuh dan Penyelenggara dengan Kewajiban Pelaporan Sebagian menyampaikan laporan Insiden Siber paling lama 3 (tiga) hari kalender setelah Insiden Siber terjadi kepada Bank Indonesia.

3. Laporan Tingkat Kematangan KKS

Penyelenggara dengan Kewajiban Pelaporan Penuh dan Penyelenggara dengan Kewajiban Pelaporan Sebagian menyampaikan laporan hasil tingkat kematangan KKS secara tahunan kepada Bank Indonesia, paling lambat tanggal 31 Januari untuk periode pelaporan tahun sebelumnya.

4. Laporan Hasil Identifikasi Infrastruktur Informasi Vital (IIV)

Penyelenggara dengan Kewajiban Pelaporan Penuh dan Penyelenggara dengan Kewajiban Pelaporan Sebagian menyampaikan laporan hasil identifikasi Infrastruktur Informasi Vital (IIV) secara tahunan kepada Bank Indonesia, paling lambat tanggal 31 Januari untuk periode pelaporan tahun sebelumnya.

B. Media Penyampaian Laporan

1. Sistem Pelaporan KKS Bank Indonesia

Penyelenggara dengan Kewajiban Pelaporan Penuh dan Penyelenggara dengan Kewajiban Pelaporan Sebagian menyampaikan laporan kepada Bank Indonesia melalui sistem pelaporan Bank Indonesia pada tautan https://pelaporan.bi.go.id.

Panduan penggunaan Sistem Pelaporan KKS Bank Indonesia sebagaimana **Lampiran 5**.

2. Surat Elektronik

Penyelenggara dengan Kewajiban Pelaporan Penuh dan Penyelenggara dengan Kewajiban Pelaporan Sebagian dapat menyampaikan laporan kepada Bank Indonesia dengan disampaikan menggunakan surat elektronik dalam hal terdapat kondisi:

a. Sistem Pelaporan KKS Bank Indonesia mengalami gangguan.
   Bank Indonesia menyampaikan adanya gangguan Sistem Pelaporan KKS Bank Indonesia melalui email atau kanal informasi lainnya.

b. Keadaan kahar (*Force Majeur*).
   Terjadi keadaan kahar yang berdampak terhadap Penyelenggara yang terjadi di luar kekuasaan dan kemampuan untuk mengatasinya, yang meliputi antara lain bencana alam, bencana nonalam, bencana sosial (antara lain huru hara, pemberontakan, perang, pemogokan), kebakaran yang bukan disebabkan oleh kelalaian Penyelenggara, dan perubahan peraturan perundang-undangan nasional, sebagaimana dinyatakan melalui keputusan bersama antara menteri terkait, dan/atau Peraturan Pemerintah. Penyelenggara harus memberitahukan keadaan kahar tersebut kepada Bank Indonesia disertai dengan bukti atau keterangan resmi dari pihak yang berwenang.

Penyampaian notifikasi awal Insiden Siber dapat menggunakan media komunikasi lainnya antara lain aplikasi pesan instan kepada Bank Indonesia dengan pertimbangan kecepatan waktu pelaporan. Informasi yang dimuat dalam pesan yang dikirimkan melalui pesan instan mengacu kepada **Lampiran 1** dan dapat berupa teks atau file dengan format tipe PDF.

C. Konvensi Penamaan dan Tipe File Laporan

Konvensi penamaan file dan tipe file untuk setiap jenis laporan KKS yang disampaikan Penyelenggara ke Bank Indonesia mengikuti ketentuan berikut:

1. Notifikasi Awal Insiden Siber

a. Konvensi penamaan file memuat:
   1) Tahun pelaporan.
   2) Kode laporan berupa NIS.
   3) Kode Sandi Pelapor.
   4) Nomor kejadian dalam periode pelaporan yang sama.

b. Tipe file PDF.

Contoh:

Penyelenggara XYZ mengalami Insiden Siber dan mengetahui Insiden Siber tersebut pada tanggal 6 Januari 2025 pukul 10.00 WIB, maka nama file yang harus disampaikan adalah **2025_NIS_Sandi Pelapor XYZ_01.pdf** dan disampaikan paling lambat pada tanggal 6 Januari 2025 pukul 11.00 WIB. Kemudian Penyelenggara XYZ mengalami Insiden Siber kembali dan mengetahui Insiden Siber tersebut pada tanggal 15 Januari 2025 pukul 14.00 WIB, maka nama file yang harus disampaikan adalah **2025_NIS_Sandi Pelapor XYZ_02.pdf** dan disampaikan paling lambat pada tanggal 15 Januari 2025 pukul 15.00 WIB.

2. Laporan Insiden Siber

a. Konvensi penamaan file memuat:
   1) Tahun pelaporan.
   2) Kode laporan berupa LIS.
   3) Kode Sandi Pelapor.
   4) Nomor kejadian dalam periode pelaporan yang sama.

b. Tipe file PDF.

Contoh:

Penyelenggara XYZ mengalami Insiden Siber dan mengetahui Insiden Siber tersebut pada tanggal 6 Januari 2025 pukul 10.00 WIB serta telah menyampaikan notifikasi awal Insiden Siber, maka nama file laporan Insiden Siber yang harus disampaikan adalah **2025_LIS_Sandi Pelapor XYZ_01.pdf** dan disampaikan paling lambat tanggal 9 Januari 2025. Kemudian Penyelenggara XYZ mengalami Insiden Siber kembali dan mengetahui Insiden Siber tersebut pada tanggal 15 Januari 2025 pukul 14.00 WIB, maka nama file yang harus disampaikan adalah **2025_LIS_Sandi Pelapor XYZ_02.pdf** dan disampaikan paling lambat tanggal 18 Januari 2025.

3. Laporan Tingkat Kematangan KKS

a. File Laporan Tingkat Kematangan KKS
   1) Konvensi penamaan file memuat:
      a) Tahun pelaporan.
      b) Kode laporan berupa TKS.
      c) Kode Sandi Pelapor.
      d) Nomor urutan laporan tingkat kematangan KKS.
   2) Tipe file .xls/.xlsx

   Contoh:

Penyelenggara XYZ akan melaporkan laporan tingkat kematangan KKS periode 2025 pada tanggal 25 Januari 2026 maka nama file laporan tingkat kematangan KKS yang harus disampaikan adalah **2025_TKS_Sandi Pelapor XYZ_01.xlsx**. Berdasarkan PADG Pasal 53 ayat (6), Bank Indonesia meminta kepada Penyelenggara XYZ untuk menyampaikan laporan tingkat kematangan KKS terkini pada bulan Juli 2026, maka nama file laporan tingkat kematangan KKS yang harus disampaikan adalah **2025_TKS_Sandi Pelapor XYZ_02.xlsx**. Kemudian pada bulan November 2026, Bank Indonesia meminta untuk menyampaikan kembali laporan tingkat kematangan KKS terkini maka nama file laporan tingkat kematangan KKS yang harus disampaikan adalah **2025_TKS_Sandi Pelapor XYZ_03.xlsx**.

b. File Bukti Pendukung
   1) Konvensi penamaan file memuat:
      a) Tahun pelaporan.
      b) Kode laporan berupa TKS.
      c) Kode Sandi Pelapor.
      d) Nomor urutan laporan tingkat kematangan KKS.
      e) Kode penyampaian bukti pendukung berupa BP.
      f) Dimensi KKS.
      2) Tipe file PDF.

Contoh:

Penyelenggara ABC yang merupakan Penyelenggara dengan **Kewajiban Pelaporan Penuh** dan **pernah mengalami Insiden Siber setelah diterbitkannya PADG KKS** melaporkan lampiran bukti pendukung yang disusun menjadi 7 file, mewakili setiap dimensi, dengan nama file:

Area	Dimensi	Nama File Bukti Pendukung
Tata Kelola	Strategi dan Kebijakan	**2025_TKS_Sandi Pelapor ABC_01_BP_Strategi Kebijakan.pdf**
	Budaya	**2025_TKS_Sandi Pelapor ABC_01_BP_Budaya.pdf**
Pencegahan	Identifikasi	**2025_TKS_Sandi Pelapor ABC_01_BP_Identifikasi.pdf**
	Proteksi	**2025_TKS_Sandi Pelapor ABC_01_BP_Proteksi.pdf**
	Deteksi	**2025_TKS_Sandi Pelapor ABC_01_BP_Deteksi.pdf**
Penanganan	Respons	**2025_TKS_Sandi Pelapor ABC_01_BP_Respons.pdf**
	Pemulihan	**2025_TKS_Sandi Pelapor ABC_01_BP_Pemulihan.pdf**

Penyelenggara XYZ yang merupakan Penyelenggara dengan **Kewajiban Pelaporan Sebagian** dan **belum pernah mengalami Insiden Siber setelah diterbitkannya PADG KKS** melaporkan lampiran bukti pendukung yang disusun menjadi 6 file, mewakili setiap dimensi, dengan nama file:

Area	Dimensi	Nama File Bukti Pendukung
Tata Kelola	Strategi dan Kebijakan	**2025_TKS_Sandi Pelapor XYZ_01_BP_Strategi Kebijakan.pdf**

Area	Dimensi	Nama File Bukti Pendukung
	Budaya	**2025_TKS_Sandi Pelapor XYZ_01_BP_Budaya.pdf**
Pencegahan	Identifikasi	**2025_TKS_Sandi Pelapor XYZ_01_BP_Identifikasi.pdf**
	Proteksi	**2025_TKS_Sandi Pelapor XYZ_01_BP_Proteksi.pdf**
	Deteksi	**2025_TKS_Sandi Pelapor XYZ_01_BP_Deteksi.pdf**
Penanganan	Respons	**2025_TKS_Sandi Pelapor XYZ_01_BP_Respons.pdf**

4. Laporan Hasil Identifikasi Infrastruktur Informasi Vital (IIV)

a. Konvensi penamaan file memuat:
   1) Tahun pelaporan.
   2) Kode laporan berupa IIV.
   3) Kode Sandi Pelapor.

b. Tipe file PDF.

Contoh:

Penyelenggara XYZ akan melaporkan laporan IIV periode pelaporan tahun 2025 pada tanggal 25 Januari 2026 maka nama file laporan IIV yang harus disampaikan adalah **2025_IIV_Sandi Pelapor XYZ.pdf**.

LAMPIRAN 1
Format Notifikasi Awal Insiden Siber

A. INFORMASI KONTAK PELAPOR
1. Nama Penyelenggara : .....
2. Alamat Kantor Pusat Penyelenggara : .....
3. Nomor Telepon : .....
4. Nama Narahubung : .....
5. Nomor Telepon Narahubung : .....

B. INFORMASI UMUM INSIDEN SIBER
1. Tanggal dan Waktu Terjadinya Insiden Siber: 1)
   ..../..../... ..... (dd/mm/yyyy), ... : .... (hh:mm)
2. Tanggal dan Waktu Insiden Siber Diketahui:
   ..../..../..... (dd/mm/yyyy), ... : .... (hh:mm)
3. Jenis Insiden Siber: ..... 2)
4. Titik Serangan Insiden Siber: ..... 3)
5. Respons Awal Pasca Insiden Siber:..... 4)

C. ASESMEN AWAL DAMPAK INSIDEN SIBER
Penilaian Awal atas Dampak Insiden Siber bagi Penyelenggara: ....5)

Keterangan:
1) Diisi dalam hal Penyelenggara telah mengidentifikasi tanggal dan waktu terjadinya Insiden Siber.
2) Memuat informasi mengenai jenis Insiden Siber antara lain: *malware*, *ransomware*, *web defacement*, dan *denial of services* (DoS)/*distributed denial of services* (DDoS).
3) Memuat informasi mengenai nama sistem dan/atau jaringan yang menjadi titik serangan.
4) Memuat informasi mengenai tindakan awal penanganan yang telah dilakukan oleh Penyelenggara setelah diketahui terjadinya Insiden Siber.
5) Diisi asesmen awal dampak terjadinya Insiden Siber pada aspek finansial dan non finansial.

LAMPIRAN 2
Format Laporan Insiden Siber

A. INFORMASI KONTAK PELAPOR
1. Nama Penyelenggara : .....
2. Alamat Kantor Pusat Penyelenggara : .....
3. Nomor Telepon : .....
4. Nama Narahubung : .....
5. Nomor Telepon Narahubung : .....
6. Tanggal Penyampaian Notifikasi Awal :
   ..../..../..... (dd/mm/yyyy)

B. INFORMASI UMUM INSIDEN SIBER[1)]
1. Tanggal dan Waktu Terjadinya Insiden Siber: [2)]
   ..../..../.... (dd/mm/yyyy), ... : .... (hh:mm)
2. Tanggal dan Waktu Insiden Siber Diketahui:
   ..../..../..... (dd/mm/yyyy), ... : .... (hh:mm)
3. Jenis Insiden Siber..... [3)]
4. Titik Serangan Insiden Siber ..... [4)]
5. Respons Awal Penyelenggara Pasca Insiden Siber ..... [5)]

C. ANALISIS KOMPREHENSIF DAMPAK INSIDEN SIBER[6)]
Penilaian Dampak Insiden Siber terhadap:
1. Ketersediaan dan Operasional Layanan Penyelenggara...[7)]
2. Finansial Penyelenggara.....[8)]
3. Reputasi Penyelenggara.....[9)]
4. Aspek Hukum dan Kepatuhan Penyelenggara.....[10)]
5. Pihak Eksternal.....[11)]
6. Dampak Lainnya.....

D. FORENSIK INSIDEN SIBER (ANALISIS LENGKAP)
1. Durasi terjadinya Insiden Siber.....
2. Langkah eskalasi Insiden Siber yang dilakukan.....
3. Langkah penanggulangan Insiden Siber yang dilakukan...
4. Langkah pemulihan Insiden Siber yang dilakukan.....
5. Keterlibatan pihak ketiga dalam penanganan dan pemulihan Insiden Siber.....
6. Pihak yang menerima informasi terkait Insiden Siber (pemangku kepentingan, contoh: otoritas, mitra layanan, dan nasabah) .....
7. Informasi pendukung yang digunakan untuk mengidentifikasi serangan siber, jika diketahui. (contoh: alamat IP yang mencurigakan, lalu lintas jaringan yang tidak biasa, tingkat kegagalan autentikasi yang tinggi, dan permintaan *file* secara berulang kali)
8. Sumber serangan siber:
   a. Pihak.....[12)]
   b. Negara Asal .....[13)]
   c. Motif Serangan .....[14)]
9. Faktor penyebab Insiden Siber .....[15)]

E. KESIMPULAN DAN TINDAK LANJUT PERBAIKAN

1. Kesimpulan.....
2. Langkah Perbaikan.....16)
3. Target Waktu Penyelesaian Insiden Siber: ..../..../... (dd/mm/yy)

Keterangan:

1) Berisi informasi yang sesuai dengan informasi yang telah disampaikan pada notifikasi awal, namun dapat ditambahkan atau disesuaikan dengan informasi tambahan jika ada.
2) Diisi dalam hal Penyelenggara telah mengidentifikasi tanggal dan waktu terjadinya Insiden Siber.
3) Memuat informasi mengenai jenis Insiden Siber antara lain: *malware*, *ransomware*, *web defacement*, dan *denial of services* (DoS)/*distributed denial of services* (DDoS).
4) Memuat informasi mengenai nama sistem atau jaringan yang diserang atau mengalami gangguan.
5) Memuat informasi mengenai tindakan awal penanganan yang telah dilakukan Penyelenggara setelah diketahui terjadinya Insiden Siber.
6) Pada bagian ini informasi yang diberikan berupa penjelasan tambahan dari penilaian awal yang sudah dilakukan oleh Penyelenggara saat pelaporan notifikasi awal Insiden Siber.
7) Diisi dalam hal terdapat dampak terhadap bisnis Penyelenggara, termasuk dalam kaitannya dengan ketersediaan dan operasional layanan Penyelenggara. Informasi paling sedikit memuat:
   a. jenis layanan dan/atau nama produk yang terdampak (contoh: layanan *treasury*, *trade finance*, *cash management*, dan layanan penyelenggaraan digital); dan
   b. penjelasan mengenai dampak yang terjadi (jika layanan dan/atau produk yang terdampak lebih dari 1 (satu), maka penjelasan diberikan untuk seluruh layanan dan produk yang terdampak).
8) Diisi dalam hal terdapat dampak finansial dari Insiden Siber. Informasi paling sedikit memuat:
   a. hal yang terdampak (contoh: nilai atau volume transaksi, penarikan dana, dan likuiditas Penyelenggara); dan
   b. penjelasan mengenai dampak yang terjadi (jika insiden memberikan dampak bagi lebih dari 1 (satu) hal maka penjelasan diberikan untuk seluruh hal yang terdampak).
9) Diisi dalam hal terdapat dampak terhadap reputasi Penyelenggara dari Insiden Siber (contoh: insiden dipublikasikan oleh media).
10) Diisi dalam hal terdapat dampak terhadap aspek hukum dan kepatuhan (contoh: pelanggaran ketentuan peraturan perundang-undangan dan adanya tuntutan hukum dari pihak terkait).
11) Diisi dalam hal terdapat dampak terhadap pihak ketiga dari Penyelenggara. Informasi paling sedikit memuat:
   a. kategori pihak eksternal (contoh: nasabah, pihak penyedia jasa, dan mitra kerja sama layanan); dan
   b. penjelasan mengenai dampak yang terjadi (jika insiden memberikan dampak bagi lebih dari 1 (satu) kategori mitra maka penjelasan diberikan untuk seluruh mitra terdampak).
12) Memuat informasi mengenai pihak yang melakukan serangan atau menjadi sumber serangan, antara lain: pihak internal, pihak eksternal atau pihak ketiga (jika diketahui).
13) Memuat informasi negara asal dari sumber serangan (jika diketahui).
14) Memuat informasi mengenai motif atau tujuan atas serangan yang dilakukan oleh pelaku (jika diketahui).

15) Memuat penjelasan lengkap dari faktor yang menyebabkan terjadinya Insiden Siber di Penyelenggara.
16) Memuat informasi mengenai langkah yang dilakukan Penyelenggara untuk mencegah insiden serupa terjadi di masa depan.

LAMPIRAN 3.1
Format Laporan Tingkat Kematangan KKS bagi Penyelenggara dengan Kewajiban Pelaporan Penuh dan Pernah Mengalami Insiden Siber

A. Informasi Pelapor

1. Nama Penyelenggara : .....
2. Alamat Kantor Pusat Penyelenggara : .....
3. Nomor Telepon : .....
4. Nama Narahubung : .....
5. Nomor Telepon Narahubung : .....
6. Tanggal Penyampaian Laporan : ..../..../..... (dd/mm/yyyy)
7. Periode Pelaporan : ..... (yyyy)

B. Hasil Asemen Mandiri Indikator Tingkat Kematangan KKS bagi Penyelenggara dengan Kewajiban Pelaporan Penuh dan Pernah Mengalami Insiden Siber

NO	INDIKATOR	NILAI
AREA: TATA KELOLA		
DIMENSI: STRATEGI DAN KEBIJAKAN KKS		
FAKTOR: RENCANA STRATEGIS KKS		
1	Arah strategis penguatan KKS disusun dengan mempertimbangkan arah dan rencana strategis bisnis, selera risiko (*risk appetite*), ketentuan peraturan perundang-undangan mengenai KKS, serta perkembangan tren teknologi, kerentanan siber, dan ancaman siber.	Ya/Parsial/Tidak
2	Peta jalan penguatan KKS disusun sesuai dengan arah strategis KKS.	Ya/Parsial/Tidak
3	Peta jalan penguatan KKS mencakup daftar program dan/atau proyek.	Ya/Parsial/Tidak
4	Peta jalan penguatan KKS mencakup daftar jadwal dan tahapan.	Ya/Parsial/Tidak
5	Peta jalan penguatan KKS mencakup hasil kerja.	Ya/Parsial/Tidak
6	Peta jalan penguatan KKS mencakup pelaksana proyek.	Ya/Parsial/Tidak
7	Perkiraan kebutuhan sumber daya untuk pelaksanaan peta jalan KKS mencakup perkiraan biaya.	Ya/Parsial/Tidak
8	Perkiraan kebutuhan sumber daya untuk pelaksanaan peta jalan KKS mencakup perkiraan sumber daya manusia.	Ya/Parsial/Tidak
9	Penetapan Rencana strategis KKS dilakukan secara formal dan ditetapkan oleh manajemen tertinggi.	Ya/Parsial/Tidak
10	Rencana strategis KKS dilakukan pemantauan pelaksanaannya dan persentase progres pencapaian hasil kerja program dan/atau proyek lebih dari 80% dari rencana jadwal dan tahapan.	Ya/Parsial/Tidak

NO	INDIKATOR	NILAI
11	Pelaksanaan evaluasi rencana strategis KKS: a. dilakukan secara berkala minimal sekali dalam setahun dengan memperhatikan perkembangan risiko siber; b. melibatkan manajemen tertinggi penyelenggara; dan c. hasil evaluasi rencana strategis KKS digunakan sebagai perbaikan rencana strategis KKS ke depan.	Ya/Parsial/Tidak
FAKTOR: KEBIJAKAN STANDAR DAN PROSEDUR KKS		
12	Kebijakan pengamanan KKS paling sedikit terdiri atas pengamanan data, sistem aplikasi, infrastruktur teknologi informasi, pihak ketiga, serta pelindungan konsumen dan manajemen *fraud*.	Ya/Parsial/Tidak
13	Standar pengamanan KKS paling sedikit terdiri atas pengamanan data, sistem aplikasi, infrastruktur teknologi informasi, pihak ketiga, serta pelindungan konsumen dan manajemen *fraud*.	Ya/Parsial/Tidak
14	Prosedur pengamanan KKS paling sedikit terdiri atas pengamanan data, sistem aplikasi, infrastruktur teknologi informasi, pihak ketiga, serta pelindungan konsumen dan manajemen *fraud*.	Ya/Parsial/Tidak
15	Kebijakan, standar, dan prosedur KKS disusun dengan memperhatikan rencana strategis KKS, kompleksitas sistem informasi, dan profil risiko.	Ya/Parsial/Tidak
16	Penetapan Kebijakan KKS dilakukan secara formal dan ditetapkan oleh manajemen tertinggi.	Ya/Parsial/Tidak
17	Kebijakan, standar, dan prosedur KKS sudah diterapkan dan dikomunikasikan: a. kepada seluruh pihak internal dan/atau pihak ketiga yang terkait ketika pertama kali bekerja; b. secara tahunan; dan c. jika terdapat perubahan.	Ya/Parsial/Tidak
18	Pelaksanaan evaluasi kebijakan, standar, dan prosedur KKS dilakukan: a. secara berkala minimal sekali dalam setahun; b. melibatkan manajemen tertinggi penyelenggara; dan c. hasil evaluasi kebijakan, standar, dan prosedur KKS digunakan sebagai perbaikan kebijakan, standar, dan prosedur KKS ke depan.	Ya/Parsial/Tidak

NO	INDIKATOR	NILAI
	FAKTOR: FUNGSI ORGANISASI KKS	
19	Memiliki fungsi manajemen KKS, manajemen risiko KKS, dan audit KKS dalam struktur organisasi yang terpisah	Ya/Parsial/Tidak
20	Manajemen KKS memiliki visi dan misi yang jelas.	Ya/Parsial/Tidak
21	Manajemen KKS memiliki struktur organisasi dan struktur jabatan yang jelas.	Ya/Parsial/Tidak
22	Manajemen KKS memiliki tugas pokok dan produk pokok manajemen KKS yang jelas.	Ya/Parsial/Tidak
23	Manajemen KKS memiliki uraian tugas dan profil persyaratan jabatan yang jelas.	Ya/Parsial/Tidak
24	Manajemen KKS memiliki kapasitas SDM yang mencukupi terkait KKS.	Ya/Parsial/Tidak
25	Manajemen KKS memiliki kapabilitas SDM yang memadai terkait KKS.	Ya/Parsial/Tidak
26	Manajemen KKS memiliki program peningkatan kapabilitas SDM terkait manajemen KKS.	Ya/Parsial/Tidak
27	Penerapan manajemen KKS meliputi perencanaan strategis KKS, penyusunan kebijakan, standar, dan prosedur KKS, penerapan budaya KKS, serta pelaksanaan pencegahan dan penanganan KKS.	Ya/Parsial/Tidak
28	Manajemen KKS bertanggung jawab kepada manajemen tertinggi.	Ya/Parsial/Tidak
29	Pelaksanaan evaluasi manajemen KKS dilakukan: a. secara berkala minimal sekali dalam setahun b. melibatkan manajemen tertinggi penyelenggara; dan c. hasil evaluasi penerapan manajemen KKS digunakan sebagai perbaikan fungsi organisasi manajemen KKS.	Ya/Parsial/Tidak
30	Manajemen risiko siber memiliki visi dan misi yang jelas.	Ya/Parsial/Tidak
31	Manajemen risiko siber memiliki struktur organisasi dan struktur jabatan yang jelas.	Ya/Parsial/Tidak
32	Manajemen risiko siber memiliki tugas pokok dan produk pokok yang jelas.	Ya/Parsial/Tidak
33	Manajemen risiko siber memiliki uraian tugas dan profil persyaratan jabatan yang jelas.	Ya/Parsial/Tidak
34	Manajemen risiko siber memiliki kapasitas SDM yang mencukupi terkait manajemen risiko siber.	Ya/Parsial/Tidak
35	Manajemen risiko siber memiliki kapabilitas SDM yang memadai terkait manajemen risiko siber.	Ya/Parsial/Tidak

NO	INDIKATOR	NILAI
36	Manajemen risiko siber memiliki program peningkatan kapabilitas SDM terkait manajemen risiko siber.	Ya/Parsial/Tidak
37	Manajemen risiko siber terintegrasi ke dalam proses manajemen risiko penyelenggara.	Ya/Parsial/Tidak
38	Penerapan manajemen risiko siber meliputi identifikasi, asesmen, mitigasi, dan evaluasi risiko siber terhadap ancaman siber atau serangan siber.	Ya/Parsial/Tidak
39	Manajemen risiko siber bertanggung jawab kepada manajemen tertinggi.	Ya/Parsial/Tidak
40	Pelaksanaan evaluasi manajemen risiko siber dilakukan: a. secara berkala minimal sekali dalam setahun sesuai dengan perkembangan risiko siber; b. melibatkan manajemen tertinggi penyelenggara; dan c. hasil evaluasi penerapan manajemen risiko siber digunakan sebagai perbaikan fungsi organisasi manajemen risiko siber.	Ya/Parsial/Tidak
41	Audit KKS memiliki objektif yang jelas.	Ya/Parsial/Tidak
42	Audit KKS memiliki struktur organisasi dan struktur jabatan yang jelas.	Ya/Parsial/Tidak
43	Audit KKS memiliki tugas pokok dan produk pokok yang jelas.	Ya/Parsial/Tidak
44	Audit KKS memiliki mempunyai uraian tugas dan profil persyaratan jabatan yang jelas.	Ya/Parsial/Tidak
45	Audit KKS internal memiliki kapasitas SDM yang mencukupi terkait audit KKS.	Ya/Parsial/Tidak
46	Audit KKS internal memiliki kapabilitas SDM yang memadai terkait audit KKS.	Ya/Parsial/Tidak
47	Audit KKS memiliki program peningkatan kapabilitas SDM terkait audit KKS.	Ya/Parsial/Tidak
48	Audit KKS dilakukan oleh pihak eksternal yang merupakan auditor KKS independen yang terdaftar di SRO dan/atau otoritas lain.	Ya/Parsial/Tidak
49	Audit KKS bertanggung jawab kepada manajemen tertinggi.	Ya/Parsial/Tidak
50	Audit KKS dilakukan minimal 1 kali dalam 1 tahun.	Ya/Parsial/Tidak
51	Audit KKS mencakup tata kelola, pencegahan, dan penanganan	Ya/Parsial/Tidak
52	Memiliki sertifikasi audit KKS berstandar internasional antara lain ISO 27001 dan PCI-DSS.	Ya/Parsial/Tidak

NO	INDIKATOR	NILAI
53	Hasil audit KKS disampaikan kepada manajemen tertinggi dan digunakan untuk perbaikan tata kelola, pencegahan, dan penanganan.	Ya/Parsial/Tidak
54	Pelaksanaan evaluasi audit KKS dilakukan: a. secara berkala minimal sekali dalam setahun sesuai dengan perkembangan risiko siber; b. melibatkan manajemen tertinggi penyelenggara; dan c. hasil evaluasi penerapan manajemen risiko siber digunakan sebagai perbaikan fungsi organisasi audit KKS.	Ya/Parsial/Tidak
DIMENSI: BUDAYA KKS		
55	Program peningkatan budaya KKS berupa *awareness* diberikan secara berkala sesuai dengan kewenangan dan tanggung jawab personel internal.	Ya/Parsial/Tidak
56	Program peningkatan budaya KKS berupa pelatihan diberikan secara berkala sesuai dengan kewenangan dan tanggung jawab personel internal.	Ya/Parsial/Tidak
57	Program peningkatan budaya KKS berupa edukasi diberikan sesuai dengan kewenangan dan tanggung jawab personel internal.	Ya/Parsial/Tidak
58	Personel internal menjaga pengetahuan KKS tetap terbaru dengan menghadiri konferensi dan acara yang bertujuan untuk peningkatan teknis dan profesional.	Ya/Parsial/Tidak
59	Program peningkatan budaya KKS berupa *awareness* diberikan secara berkala sesuai dengan kewenangan dan tanggung jawab pihak ketiga.	Ya/Parsial/Tidak
60	Program peningkatan budaya KKS berupa pelatihan diberikan secara berkala sesuai dengan kewenangan dan tanggung jawab pihak ketiga.	Ya/Parsial/Tidak
61	Program peningkatan budaya KKS berupa *awareness* diberikan secara berkala sesuai dengan kewenangan dan tanggung jawab konsumen.	Ya/Parsial/Tidak
62	Pelaksanaan program peningkatan budaya KKS melibatkan manajemen tertinggi.	Ya/Parsial/Tidak
63	Program peningkatan budaya KKS dilakukan secara berkala paling sedikit 1 kali dalam 1 tahun.	Ya/Parsial/Tidak
64	Program peningkatan budaya KKS diselaraskan dengan rencana strategis KKS.	Ya/Parsial/Tidak

NO	INDIKATOR	NILAI
65	Pelaksanaan evaluasi program peningkatan budaya KKS dilakukan: a. secara berkala minimal sekali dalam setahun sesuai dengan perkembangan risiko siber; b. melibatkan manajemen tertinggi penyelenggara; dan c. hasil evaluasi program peningkatan budaya KKS digunakan sebagai perbaikan program peningkatan budaya KKS ke depan.	Ya/Parsial/Tidak
AREA: PENCEGAHAN		
DIMENSI: IDENTIFIKASI		
FAKTOR: PENYUSUNAN PROFIL RISIKO SIBER		
66	Identifikasi risiko siber dilakukan dengan memperhatikan kerentanan dan ancaman siber dari aspek manusia dengan memantau perkembangan siber terkini yang bersumber dari internal dan eksternal, antara lain ketidakcukupan kapasitas dan kapabilitas SDM.	Ya/Parsial/Tidak
67	Identifikasi risiko siber dilakukan dengan memperhatikan kerentanan dan ancaman siber dari aspek proses dengan memantau perkembangan siber terkini yang bersumber dari internal dan eksternal, antara lain ketidakcukupan kebijakan, standar, dan prosedur KKS.	Ya/Parsial/Tidak
68	Identifikasi risiko siber dilakukan dengan memperhatikan kerentanan dan ancaman siber dari aspek teknologi dengan memantau perkembangan siber terkini yang bersumber dari internal dan eksternal, antara lain *vulnerability* teknologi baru.	Ya/Parsial/Tidak
69	Identifikasi risiko siber dilakukan dengan memperhatikan objek yang akan dilindungi meliputi data yang dikelola oleh penyelenggara.	Ya/Parsial/Tidak
70	Identifikasi risiko siber dilakukan dengan memperhatikan objek yang akan dilindungi meliputi sistem aplikasi dan konfigurasinya yang dikelola oleh penyelenggara.	Ya/Parsial/Tidak
71	Identifikasi risiko siber dilakukan dengan memperhatikan objek yang akan dilindungi meliputi infrastruktur teknologi informasi dan konfigurasinya yang dikelola oleh penyelenggara.	Ya/Parsial/Tidak
72	Identifikasi risiko siber dilakukan dengan memperhatikan objek yang akan dilindungi meliputi Sistem Informasi yang dikelola oleh pihak ketiga.	Ya/Parsial/Tidak

NO	INDIKATOR	NILAI
73	Objek yang dilindungi diprioritisasi berdasarkan klasifikasi, kritikalitas, sumber daya, dan dampak terhadap bisnis.	Ya/Parsial/Tidak
74	Inventarisasi objek yang dilindungi dilakukan dengan menggunakan sistem/*tools*.	Ya/Parsial/Tidak
75	Memiliki konfigurasi keterhubungan antar objek yang dilindungi yang tersimpan dalam *configuration management system*.	Ya/Parsial/Tidak
76	Identifikasi risiko siber untuk informasi kerentanan siber dan ancaman siber didapatkan dari sarana pertukaran informasi yang dibentuk Bank Indonesia.	Ya/Parsial/Tidak
77	Identifikasi risiko siber untuk informasi kerentanan siber dan ancaman siber didapatkan dari sarana pertukaran informasi sesama penyelenggara.	Ya/Parsial/Tidak
78	Identifikasi risiko siber untuk informasi kerentanan siber dan ancaman siber didapatkan dari *cyber threat intelligence*.	Ya/Parsial/Tidak
79	Hasil identifikasi kerentanan siber dan ancaman siber didokumentasikan pada inventaris risiko siber (*cyber risk register*) pada level fungsi manajemen KKS.	Ya/Parsial/Tidak
80	Hasil identifikasi kerentanan siber dan ancaman siber didokumentasikan pada inventaris risiko siber (*cyber risk register*) pada level *enterprise risk management.*	Ya/Parsial/Tidak
81	Memiliki metodologi asesmen risiko siber yang mencakup penilaian dampak yang ditimbulkan dari risiko siber (*impact*) dan penilaian kemungkinan terjadinya risiko siber (*likelihood*).	Ya/Parsial/Tidak
82	Metodologi asesmen risiko siber selaras dengan metode asesmen *enterprise risk management* penyelenggara.	Ya/Parsial/Tidak
83	Metodologi asesmen risiko siber diuji dengan menggunakan sampling risiko siber untuk memastikan hasil asesmen risiko yang konsisten dan valid.	Ya/Parsial/Tidak
84	Melakukan penilaian dampak kerentanan siber dan ancaman siber berupa perkiraan kerugian sebagai akibat gangguan layanan (contoh: potensi kehilangan *revenue*).	Ya/Parsial/Tidak
85	Melakukan penilaian dampak kerentanan siber dan ancaman siber berupa dampak kerusakan (contoh: kerugian non-finansial antara lain reputasi, hukum, dan *compliance*).	Ya/Parsial/Tidak

NO	INDIKATOR	NILAI
86	Melakukan penilaian dampak kerentanan siber dan ancaman siber berupa biaya pemulihan yang harus dilakukan (biaya yang dikeluarkan untuk penanganan dan pemulihan atas insiden siber).	Ya/Parsial/Tidak
87	Daftar risiko siber dilakukan prioritisasi berdasarkan *impact* dan *likelihood*.	Ya/Parsial/Tidak
88	*Risk treatments* (*accept, mitigate, transfer, avoid*) dilakukan untuk daftar risiko yang telah diprioritisasi berdasarkan selera dan toleransi risiko siber.	Ya/Parsial/Tidak
89	Prioritasi mitigasi kerentanan siber dan ancaman siber dilakukan berdasarkan tingkat risiko siber, urgensi waktu pelaksanaan mitigasi risiko siber, dan urutan pelaksanaan mitigasi risiko siber.	Ya/Parsial/Tidak
90	Penilaian dampak bisnis dilakukan dengan menetapkan jenis dampak finansial dan non finansial.	Ya/Parsial/Tidak
91	Penilaian dampak bisnis dilakukan dengan menetapkan *Maximum Tolerable Period of Disruption* (MTPD) untuk setiap layanan.	Ya/Parsial/Tidak
92	Penetapan MTPD telah dianalisis dengan mempertimbangkan sasaran waktu pemulihan (*Recovery Time Objective* - RTO).	Ya/Parsial/Tidak
93	Penilaian dampak bisnis dilakukan dengan menetapkan sumber daya finansial untuk mendukung fungsi bisnis yang diprioritaskan.	Ya/Parsial/Tidak
94	Penilaian dampak bisnis dilakukan dengan menetapkan sumber daya manusia untuk mendukung fungsi bisnis yang diprioritaskan.	Ya/Parsial/Tidak
95	Analisis kritikalitas fungsi bisnis dan sistem informasi dilakukan dengan menetapkan sasaran waktu pemulihan (*Recovery Time Objective* - RTO).	Ya/Parsial/Tidak
96	Analisis kritikalitas fungsi bisnis dan sistem informasi dilakukan dengan menetapkan sasaran titik pemulihan (*Recovery Point Objective* - RPO).	Ya/Parsial/Tidak
97	Analisis kritikalitas fungsi bisnis dan sistem informasi dilakukan dengan menetapkan *service level* untuk sistem informasi.	Ya/Parsial/Tidak
98	Analisis kritikalitas fungsi bisnis dan sistem informasi dilakukan dengan menetapkan *maximum downtime* yang tidak terjadwal.	Ya/Parsial/Tidak
99	Analisis kritikalitas fungsi bisnis dan sistem informasi dilakukan dengan menetapkan *maximum downtime* yang terjadwal.	Ya/Parsial/Tidak

NO	INDIKATOR	NILAI
100	Memiliki inventaris sistem aplikasi dan infrastruktur teknologi informasi terkait pelaksanaan kegiatan sistem pembayaran, pasar uang dan pasar valuta asing, dan/atau kegiatan usaha penukaran valuta asing bukan bank yang berdampak luas terhadap stabilitas sistem keuangan.	Ya/Parsial/Tidak
101	Melakukan analisis sistem aplikasi dan infrastruktur teknologi informasi yang berdampak luas terhadap stabilitas sistem keuangan.	Ya/Parsial/Tidak
102	Melakukan implementasi penguatan KKS berdasarkan peta jalan penguatan Infrastruktur Informasi Vital (IIV) sektor keuangan.	Ya/Parsial/Tidak
FAKTOR: PENGINIAN PROFIL RISIKO SIBER		
103	Profil risiko siber dievaluasi dan dikinikan paling sedikit 1 kali dalam 1 tahun.	Ya/Parsial/Tidak
104	Profil risiko siber dikinikan setiap terjadi insiden siber.	Ya/Parsial/Tidak
105	Profil risiko siber ditetapkan oleh manajemen tertinggi.	Ya/Parsial/Tidak
DIMENSI: PROTEKSI		
FAKTOR: PEMBANGUNAN SISTEM PERTAHANAN		
106	Keamanan pihak internal dan pihak ketiga dipastikan dengan melakukan verifikasi latar belakang pihak internal dan/atau pihak ketiga yang akan dipekerjakan.	Ya/Parsial/Tidak
107	Verifikasi latar belakang dilakukan dengan memperhatikan ketentuan organisasi terkini, klasifikasi informasi yang diakses, dan risiko yang dihadapi.	Ya/Parsial/Tidak
108	Mengomunikasikan peran dan tanggung jawab KKS kepada personel pihak internal dan/atau pihak ketiga yang dipekerjakan.	Ya/Parsial/Tidak
109	Mewajibkan personel pihak internal dan/atau pihak ketiga telah menandatangani perjanjian atau surat pernyataan untuk menjaga kerahasiaan data dan/atau informasi dari pihak yang tidak berwenang.	Ya/Parsial/Tidak
110	Persyaratan perjanjian kerahasiaan dan *Non-Disclosure Agreement* (NDA) ditinjau secara berkala dan ketika terjadi perubahan yang mempengaruhi persyaratan ini.	Ya/Parsial/Tidak
111	Terdapat mekanisme sanksi terhadap pelanggaran kebijakan KKS.	Ya/Parsial/Tidak
112	Menerapkan pemisahan tugas yang dapat menimbulkan konflik kepentingan dalam pelaksanaan peran dan tanggung jawab personel pihak internal dan/atau pihak ketiga.	Ya/Parsial/Tidak

NO	INDIKATOR	NILAI
113	Melaksanakan alih pengetahuan dalam hal terdapat perpindahan tanggung jawab atau penonaktifan personel pihak internal dan/atau pihak ketiga.	Ya/Parsial/Tidak
114	Melakukan monitoring terhadap personel internal dan pihak ketiga untuk memastikan kerahasiaan data dan/atau informasi dari pihak yang tidak berwenang selama personel dipekerjakan, saat terjadi perpindahan tanggung jawab, dan saat dinonaktifkan.	Ya/Parsial/Tidak
115	Menerapkan manajemen akses antara lain standar penggunaan *password* yang meliputi kompleksitas *password*, limit upaya percobaan penggunaan *password*, dan penggantian *default password*.	Ya/Parsial/Tidak
116	Semua *password* dan akun *default* telah diubah sebelum implementasi sistem aplikasi dan infrastruktur teknologi informasi.	Ya/Parsial/Tidak
117	Menerapkan *zero trust architecture*.	Ya/Parsial/Tidak
118	Akses diberikan sesuai dengan kewenangan berdasarkan prinsip *least privilege* dan *segregation of duties*.	Ya/Parsial/Tidak
119	*User access matrix* dan daftar akses pengguna dievaluasi secara berkala (contoh: ketika ada pergantian peran atau personel yang keluar dari organisasi).	Ya/Parsial/Tidak
120	Menerapkan kontrol keamanan fisik berlapis antara lain personel *security*, CCTV, dan sistem alarm.	Ya/Parsial/Tidak
121	Memiliki prosedur pengawalan tamu, vendor, dan pihak ketiga lainnya di area kritikal antara lain ruang operator dan *data center*.	Ya/Parsial/Tidak
122	*User access review* dilakukan secara berkala untuk setiap sistem aplikasi dan infrastruktur teknologi informasi.	Ya/Parsial/Tidak
123	Setiap perubahan akses user ke level *administrator* akan memicu notifikasi ke manajemen KKS.	Ya/Parsial/Tidak
124	Setiap terdapat akses ke sistem aplikasi dan infrastruktur teknologi informasi yang tidak biasa, akan memicu notifikasi ke manajemen KKS.	Ya/Parsial/Tidak
125	Menerapkan proses manajemen perubahan konfigurasi sistem aplikasi dan infrastruktur teknologi informasi.	Ya/Parsial/Tidak
126	Konfigurasi untuk seluruh layanan kritikal dilakukan *monitoring* secara *realtime*.	Ya/Parsial/Tidak

NO	INDIKATOR	NILAI
127	Memiliki *tools* untuk mengelola akses dan konfigurasi antara lain *identity management system* (IDMS) atau *identity access management* (IAM).	Ya/Parsial/Tidak
128	Penginian pengendalian keamanan dilakukan secara berkala untuk memastikan kecukupan kontrol keamanan.	Ya/Parsial/Tidak
129	Melakukan perencanaan dan *due diligence* untuk mengurangi risiko sebelum melakukan kerja sama dengan pihak ketiga.	Ya/Parsial/Tidak
130	Terdapat persyaratan keamanan siber untuk setiap kontrak/perjanjian antara Penyelenggara dengan pihak ketiga, termasuk menjaga kerahasiaan informasi.	Ya/Parsial/Tidak
131	Memiliki kebijakan untuk melakukan dokumentasi, pengujian, dan pemantauan model kecerdasan artifisial secara berkelanjutan dalam hal menggunakan sistem kecerdasan artifisial.	Ya/Parsial/Tidak
132	Menerapkan *defence in depth strategy*.	Ya/Parsial/Tidak
133	Menerapkan segmentasi jaringan antara lain internet, ekstranet, dan intranet.	Ya/Parsial/Tidak
134	Memiliki *network perimeter defence tools* antara lain *firewall.*	Ya/Parsial/Tidak
135	*Firewall* diimplementasikan pada setiap jaringan yang terhubung dengan internet serta antara *Demilitarised Zone* (DMZ) dan intranet.	Ya/Parsial/Tidak
136	*Firewall rules* diverifikasi secara berkala.	Ya/Parsial/Tidak
137	Memiliki IPS/IDS untuk mendeteksi atau membatasi percobaan serangan atau intrusi.	Ya/Parsial/Tidak
138	Menerapkan anti *spoofing* untuk mendeteksi dan membatasi *forged source* IP *address* yang masuk ke dalam jaringan.	Ya/Parsial/Tidak
139	Terdapat antivirus dan anti *malware* pada setiap sistem aplikasi dan infrastruktur teknologi informasi termasuk *end point devices*, antara lain *work station*, *laptop*, dan *mobile devices*.	Ya/Parsial/Tidak
140	*Antivirus* dan *anti-malware* yang terupdate secara otomatis.	Ya/Parsial/Tidak
141	Menerapkan kontrol dan pemindaian untuk setiap *attachment e-mail, malware,* situs *web* yang memiliki risiko siber.	Ya/Parsial/Tidak
142	Terdapat *centralized end-point management tools* yang mengintegrasikan managemen *patching*, konfigurasi, dan manajemen kerentanan yang terintegrasi penuh, serta dapat mendeteksi *malware*.	Ya/Parsial/Tidak

NO	INDIKATOR	NILAI
143	Menerapkan *whitelist* aplikasi untuk memastikan hanya perangkat lunak yang terotorisasi yang dapat dijalankan oleh sistem.	Ya/Parsial/Tidak
144	melindungi integritas dan keamanan data dengan menyimpan *master images* pada server yang telah dikonfigurasi dengan kontrol yang ketat.	Ya/Parsial/Tidak
145	Menerapkan *secure coding* pada pengembangan sistem aplikasi sesuai dengan standar industri.	Ya/Parsial/Tidak
146	Pengembangan sistem aplikasi dilakukan pada *environment development* yang terpisah dari *environment production*.	Ya/Parsial/Tidak
147	Pengembangan sistem aplikasi menggunakan *software*, dan/atau *libraries* yang berasal dari sumber yang kredibel.	Ya/Parsial/Tidak
148	Pengujian keamanan dilakukan pada tahapan *unit testing*, *system integration testing*, dan *user acceptance testing*.	Ya/Parsial/Tidak
149	Pengujian keamanan dilakukan sebelum *deployment* sistem aplikasi di *environment production* antara lain *code review* dan *penetration testing*.	Ya/Parsial/Tidak
150	Pengujian keamanan dilakukan pada *environment testing* yang terpisah dari *environment development* dan *environment production*.	Ya/Parsial/Tidak
151	Pengujian keamanan dilakukan sebelum *deployment* sistem aplikasi di *environment production* atau setelah terdapat perubahan signifikan pada sistem aplikasi berbasis web yang terhubung ke internet antara lain dengan *SQL injection*, *cross-site*, dan *buffer overflow*.	Ya/Parsial/Tidak
152	*Patching* dilakukan dengan menggunakan versi perangkat lunak terkini dan telah teruji untuk setiap sistem aplikasi dan infrastruktur teknologi informasi.	Ya/Parsial/Tidak
153	*Menerapkan tools untuk* monitoring status *patch* pada setiap sistem aplikasi dan infrastruktur teknologi informasi untuk mengidentifikasi *patch* yang belum *update*.	Ya/Parsial/Tidak
154	*Remote* akses dilengkapi dengan pengamanan, antara lain *Virtual Private Network* (VPN) dan *Multi-Factor Authentication* (MFA).	Ya/Parsial/Tidak
155	Memiliki *password management system* yang dapat melakukan *enforcement* penerapan kontrol akses penggunaan *password*.	Ya/Parsial/Tidak
156	Akses ke sistem menggunakan *single factor authentication* antara lain *Personal Identification Number* (PIN) atau *password*.	Ya/Parsial/Tidak

NO	INDIKATOR	NILAI
157	Akses ke sistem kritikal menggunakan *two factor authentication* antara lain *password* dan token.	Ya/Parsial/Tidak
158	Akses ke sistem kritikal menggunakan *multi-factor authentication* antara lain *password*, token, dan *biometric*.	Ya/Parsial/Tidak
159	Enkripsi diterapkan untuk setiap otentikasi dan transmisi data yang melewati *wireless network*.	Ya/Parsial/Tidak
160	Terdapat teknologi *cyber deception* (penerapan *decoy* dan/atau *traps*) untuk mendeteksi, mencegah, dan mengalihkan serangan siber, serta mendapatkan informasi tambahan dari pelaku insiden siber.	Ya/Parsial/Tidak
161	Terdapat sistem pertahanan untuk memitigasi *adversarial attack* pada model kecerdasan artifisial dalam hal menggunakan sistem kecerdasan artifisial.	Ya/Parsial/Tidak
FAKTOR: PENGAMANAN DATA DAN/ATAU INFORMASI		
162	Data dan/atau informasi diamankan sesuai dengan klasifikasi data dan/atau informasi penyelenggara.	Ya/Parsial/Tidak
163	Data dan/atau informasi yang disimpan telah dilakukan pengamanan antara lain enkripsi, *digital signature*, dan kriptografi untuk memastikan keamanan aspek *confidentiality, integrity*, dan *availability*.	Ya/Parsial/Tidak
164	*Backup* data dilakukan secara berkala.	Ya/Parsial/Tidak
165	*Backup* data dilakukan termasuk untuk data konfigurasi sistem antara lain *images server* dan konfigurasi *router*.	Ya/Parsial/Tidak
166	Pengujian *restore backup* data dilakukan secara berkala di *environment testing* paling sedikit 1 kali dalam 1 tahun.	Ya/Parsial/Tidak
167	Menyimpan *backup* dengan aman secara *offline* dan *offsite* sehingga tidak terdampak ketika terjadi insiden atau bencana.	Ya/Parsial/Tidak
168	Menerapkan pemisahan secara geografis dan pembatasan geolokasi untuk penyimpanan *backup* data.	Ya/Parsial/Tidak
169	Menerapkan *full disk encryption* untuk melindungi data yang disimpan pada *user endpoint*.	Ya/Parsial/Tidak
170	Membatasi penggunaan *removable media* untuk mencegah eksfiltrasi data.	Ya/Parsial/Tidak
171	Data dan/atau informasi yang ditransmisikan telah dilakukan pengamanan antara lain enkripsi, *digital signature*, dan kriptografi untuk memastikan keamanan aspek *confidentiality, integrity*, dan *availability*.	Ya/Parsial/Tidak

NO	INDIKATOR	NILAI
172	Menerapkan *tools data loss prevention* pada komunikasi *inbound* dan *outbound*, antara lain *email*, FTP, dan Telnet.	Ya/Parsial/Tidak
173	Secara otomatis mengenkripsi atau memblokir *email* keluar dan komunikasi lain yang berisi data sensitif yang tidak sesuai dengan klasifikasi data.	Ya/Parsial/Tidak
174	Membatasi penggunaan data sensitif dari *production enviroment* antara lain data konsumen pada *environment development*, *testing*, atau *non-production* lain.	Ya/Parsial/Tidak
175	Data sensitif dari *environment production* dilakukan *data masking* sebelum digunakan pada *environment development*, *testing*, atau *non-production* lain.	Ya/Parsial/Tidak
176	Menggunakan fitur *password*, PIN, dan/atau MFA dalam pengamanan data dan/atau informasi ketika akan digunakan.	Ya/Parsial/Tidak
177	Menggunakan fitur *password*, PIN, dan/atau MFA dalam pengamanan data dan/atau informasi ketika akan dimusnahkan oleh pengguna yang sah.	Ya/Parsial/Tidak
178	Memiliki kebijakan dan prosedur untuk pemusnahan data dengan memperhatikan retensi data.	Ya/Parsial/Tidak
179	Pengamanan dan pelindungan data dan/atau informasi dilakukan sesuai dengan ketentuan mengenai pelindungan data pribadi.	Ya/Parsial/Tidak
DIMENSI: DETEKSI		
FAKTOR: PEMANTAUAN		
180	Deteksi dilaksanakan secara terpusat untuk mempercepat proses deteksi dan respons kerentanan siber, serangan siber, dan/atau insiden siber antara lain dengan menerapkan fungsi *Security Operation Center* (SOC).	Ya/Parsial/Tidak
181	Fungsi SOC dilengkapi dengan *red team* dan *blue team*.	Ya/Parsial/Tidak
182	Fungsi SOC dilengkapi dengan *threat hunter*.	Ya/Parsial/Tidak
183	Memiliki sumber daya manusia yang kompeten untuk melakukan deteksi.	Ya/Parsial/Tidak
184	Memiliki standar dan prosedur pelaksanaan untuk melakukan deteksi.	Ya/Parsial/Tidak
185	Memiliki teknologi sebagai alat bantu untuk melakukan deteksi.	Ya/Parsial/Tidak

NO	INDIKATOR	NILAI
186	Memiliki sistem yang dapat mendeteksi upaya akses tidak sah melalui jaringan baik *wired* maupun *wireless*, antara lain upaya pengubahan DNS, upaya koneksi *endpoint* yang tidak sah, upaya perubahan konfigurasi jaringan/perangkat keras/perangkat lunak yang tidak sah, pencurian/perusakan data.	Ya/Parsial/Tidak
187	Sistem dapat memantau *log* tentang akses *logical* untuk mengetahui pola akses yang tidak biasa dan upaya akses yang gagal.	Ya/Parsial/Tidak
188	Sistem dapat mendeteksi dan memblokir akses *environment production* secara *remote* bagi pihak ketiga.	Ya/Parsial/Tidak
189	Sistem dapat memantau *wired* dan *wireless network* untuk koneksi yang berasal dari *unauthorized endpoints*.	Ya/Parsial/Tidak
190	*Monitoring* jaringan komunikasi dapat mengidentifikasi perubahan pada *security postures* untuk kebutuhan *zero trust*.	Ya/Parsial/Tidak
191	Sistem dapat mendeteksi anomali aktivitas yang dilakukan oleh nasabah/konsumen, memberikan notifikasi, dan mencegah transaksi tidak terjadi/terulang.	Ya/Parsial/Tidak
192	Memiliki sistem untuk mendeteksi akses fisik yang tidak sah dan/atau upaya akses gagal beberapa kali.	Ya/Parsial/Tidak
193	Sistem dapat memantau *log* dari sistem kontrol akses fisik antara lain *badge readers* untuk menemukan pola akses yang tidak biasa dan percobaan akses gagal.	Ya/Parsial/Tidak
194	Melakukan review dan *monitoring* catatan akses fisik antara lain *visitor registration* dan akses masuk perangkat.	Ya/Parsial/Tidak
195	Sistem dilengkapi oleh sistem *alarm*, kamera pemantau (CCTV) dan petugas keamanan pada area dan/atau objek kritikal atau vital.	Ya/Parsial/Tidak
196	Menerapkan *behaviour analytics software* untuk mendeteksi aktivitas pengguna yang tidak wajar guna memitigasi ancaman orang dalam.	Ya/Parsial/Tidak
197	Menerapkan *monitoring* untuk *remote* dan *onsite* aktivitas administrasi dan *maintenance* yang dilakukan oleh pihak ketiga.	Ya/Parsial/Tidak
198	Menerapkan *monitoring* aktivitas layanan *cloud*, *internet services providers*, dan penyedia layanan lain dari pola akses yang tidak biasa.	Ya/Parsial/Tidak
199	Seluruh *log* / rekaman akses logis dan fisik disimpan dan di*backup* dengan memperhatikan masa retensi.	Ya/Parsial/Tidak
200	Log/rekaman akses logis dan fisik dilakukan review secara berkala.	Ya/Parsial/Tidak

NO	INDIKATOR	NILAI
201	Perubahan terhadap akses logis dan fisik dilakukan dengan prinsip *segregation of duties* dan dikelola melalui prosedur manajemen perubahan.	Ya/Parsial/Tidak
202	Terdapat penetapan indikator ambang batas (*threshold)* sebagai pemicu aktivasi sistem peringatan dengan mengacu pada profil risiko siber.	Ya/Parsial/Tidak
203	Melakukan evaluasi efektivitas indikator ambang batas secara berkala.	Ya/Parsial/Tidak
204	Pemindaian kerentanan siber dilakukan pada setiap sistem aplikasi, infrastruktur teknologi informasi, dan data secara bergiliran dan terjadwal mengacu pada profil risiko siber.	Ya/Parsial/Tidak
205	Pemindaian kerentanan siber dilakukan dan dianalisis sebelum dilakukan *deployment* atau *re-deployment* terhadap terhadap sistem aplikasi dan/atau infrastruktur teknologi informasi baru atau eksisting.	Ya/Parsial/Tidak
206	Evaluasi terhadap pemindaian kerentanan siber dilakukan paling sedikit 1 kali dalam 1 tahun.	Ya/Parsial/Tidak
	FAKTOR: ANALISIS HASIL PEMANTAUAN	
207	Melakukan analisis hasil pemantauan untuk catatan aktivitas siber yang meliputi pola aktivitas siber yang tidak biasa dan korelasi catatan aktivitas siber dari seluruh sistem aplikasi dan infrastruktur teknologi informasi. Pola aktivitas siber yang tidak biasa antara lain upaya akses tidak sah, upaya peningkatan peran hak akses, perubahan konfigurasi yang mencurigakan dan upaya lain yang berpotensi menjadi serangan siber.	Ya/Parsial/Tidak
208	Melakukan analisis hasil pemantauan untuk kerentanan siber dan potensi serangan siber dengan memperhatikan integrasi informasi dari internal dan eksternal penyelenggara.	Ya/Parsial/Tidak
209	Mengintegrasikan *cyber threat intelligence* untuk analisis kerentanan siber dan potensi serangan siber.	Ya/Parsial/Tidak
210	Melakukan *sharing informasi* hasil analisis kerentanan siber dan potensi serangan siber pada sarana pertukaran informasi yang dibentuk Bank Indonesia atau sarana informasi lain.	Ya/Parsial/Tidak
	FAKTOR: ANALISIS SERANGAN SIBER	
211	Melakukan analisis serangan siber meliputi sumber serangan meliputi asal serangan (internal dan/atau eksternal), profil *threat actor* (individu, kelompok, dan/atau, negara), dan *Indicator of Compromise* (IOC).	Ya/Parsial/Tidak

NO	INDIKATOR	NILAI
212	Melakukan analisis serangan siber meliputi sumber serangan meliputi jenis serangan siber.	Ya/Parsial/Tidak
213	Melakukan analisis serangan siber meliputi sumber serangan meliputi waktu terjadinya serangan siber dan korelasi serangan siber dengan kejadian keamanan siber (*security event*) lain.	Ya/Parsial/Tidak
214	Melakukan analisis aktivitas *fraud* pada tingkat akun, aktivitas jaringan, dan transaksi.	Ya/Parsial/Tidak
215	Memiliki *fraud detection system* untuk analisis aktivitas *fraud*.	Ya/Parsial/Tidak
216	Memiliki *Security Information and Events Management* (SIEM) untuk mengkorelasikan catatan aktivitas siber dari seluruh sistem aplikasi dan infrastruktur teknologi informasi.	Ya/Parsial/Tidak
217	Terdapat prosedur eskalasi terhadap hasil deteksi apabila terdapat potensi terjadinya insiden siber.	Ya/Parsial/Tidak
FAKTOR: ANALISIS KODE JAHAT ATAU KODE TIDAK SAH		
218	Melakukan analisis kode jahat atau kode tidak sah yang berpotensi menimbulkan serangan siber meliputi klasifikasi kode jahat atau kode tidak sah berdasarkan tingkat risiko siber untuk memastikan penanganan yang sesuai dengan tingkat ancaman.	Ya/Parsial/Tidak
219	Melakukan analisis kode jahat atau kode tidak sah dalam lingkungan yang aman dan terisolasi untuk memahami karakteristik, tujuan, dan potensi dampak kode jahat atau kode tidak sah tanpa risiko penyebaran lebih lanjut.	Ya/Parsial/Tidak
220	Melakukan analisis kode jahat atau kode tidak sah yang berpotensi menimbulkan serangan siber meliputi pemindaian sistem aplikasi dan/atau infrastruktur teknologi informasi yang terdampak.	Ya/Parsial/Tidak
221	Melakukan analisis kode jahat atau kode tidak sah yang berpotensi menimbulkan serangan siber meliputi memastikan kode yang dieksekusi pada sistem aplikasi dan/atau infrastruktur teknologi informasi telah dilakukan otorisasi dan tidak disusupi.	Ya/Parsial/Tidak
222	Terdapat prosedur eskalasi tindak lanjut untuk memitigasi atau meminimalisir dampak dari kode jahat atau kode tidak sah yang terdeteksi.	Ya/Parsial/Tidak
223	Melakukan evaluasi deteksi kode jahat atau kode tidak sah untuk perbaikan sistem deteksi dan implementasi kontrol untuk mencegah eksekusi dari kode jahat atau kode tidak sah.	Ya/Parsial/Tidak

NO	INDIKATOR	NILAI
FAKTOR: PEMELIHARAAN DAN PENGUJIAN SISTEM DETEKSI		
224	Sistem pemantauan terpelihara dengan versi perangkat lunak terkini dan telah teruji sesuai standar yang berlaku di penyelenggara.	Ya/Parsial/Tidak
225	Pemeliharaan dan pengujian sistem deteksi dilakukan paling sedikit 1 kali dalam 1 tahun.	Ya/Parsial/Tidak
226	Keandalan sistem pemantauan dilakukan penilaian meliputi aspek akurasi sistem deteksi, kemampuan sistem deteksi dalam merespons ancaman siber dan serangan siber serta kemampuan sistem deteksi dalam memberikan notifikasi secara cepat.	Ya/Parsial/Tidak
227	Sistem pemantauan terkoneksi dengan *tools* manajemen insiden.	Ya/Parsial/Tidak
AREA: PENANGANAN		
DIMENSI: RESPONS		
FAKTOR: PENYUSUNAN RENCANA PENANGANAN DAN PEMULIHAN INSIDEN SIBER		
228	Rencana penanganan insiden siber memuat penetapan status insiden siber berdasarkan kriteria penetapan insiden siber.	Ya/Parsial/Tidak
229	Rencana penanganan insiden siber memuat penentuan kategori insiden siber beserta level manajemen koordinator per kategori insiden siber dengan memperhatikan dampak dan prioritas penanganan insiden siber.	Ya/Parsial/Tidak
230	Rencana penanganan insiden siber memuat prosedur respons insiden siber dengan memperhatikan sasaran waktu pemulihan (*Recovery Time Objective* - RTO) dan sasaran titik pemulihan (*Recovery Point Objective* - RPO).	Ya/Parsial/Tidak
231	Rencana penanganan insiden siber memuat prosedur respons insiden siber untuk menghilangkan sumber insiden siber (*eradication*).	Ya/Parsial/Tidak
232	Rencana penanganan insiden siber memuat prosedur respons insiden siber untuk eskalasi setiap kategori insiden siber.	Ya/Parsial/Tidak
233	Rencana penanganan insiden siber memuat daftar personel internal dan pihak ketiga berikut peran, tanggung jawab, dan kontak yang dapat dihubungi dalam penanganan insiden siber.	Ya/Parsial/Tidak
234	Daftar personel internal dan pihak ketiga beserta kontak yang dapat dihubungi dilakukan verifikasi dan diperbarui berkala.	Ya/Parsial/Tidak

NO	INDIKATOR	NILAI
235	Rencana penanganan insiden siber memuat daftar sistem aplikasi termasuk aplikasi pendukung (*surrounding application*), infrastruktur TI, dan sumber daya lainnya yang diperlukan dalam penanganan Insiden Siber.	Ya/Parsial/Tidak
236	Rencana penanganan insiden siber memuat prosedur pembatasan dampak insiden siber di internal penyelenggara (*containment*).	Ya/Parsial/Tidak
237	Rencana penanganan insiden siber memuat prosedur koordinasi pembatasan dampak insiden siber dengan otoritas, lembaga, dan/atau penyelenggara lain.	Ya/Parsial/Tidak
238	Rencana pemulihan insiden siber memuat prosedur pemulihan untuk setiap kategori insiden siber dengan memperhatikan sasaran titik pemulihan (*Recovery Point Objective* - RPO).	Ya/Parsial/Tidak
239	Rencana pemulihan insiden siber memuat daftar personel pihak internal atau pihak ketiga berikut peran, tanggung jawab, dan kontak yang dapat dihubungi dalam pemulihan insiden siber.	Ya/Parsial/Tidak
240	Rencana pemulihan insiden siber memuat daftar sistem aplikasi termasuk aplikasi pendukung (*surrounding application*), infrastruktur TI, dan sumber daya yang diperlukan dalam pemulihan insiden siber.	Ya/Parsial/Tidak
241	Rencana penanganan dan pemulihan insiden siber menjadi bagian dari rencana keberlangsungan bisnis penyelenggara.	Ya/Parsial/Tidak
242	Rencana penanganan dan pemulihan insiden siber didistribusikan atau dapat diakses oleh seluruh pihak terkait.	Ya/Parsial/Tidak
243	Rencana penanganan dan pemulihan insiden siber paling sedikit meliputi *malware attacks*, *phishing and social engineering*, *Distributed Denial of Service* (DDoS), *data breach*, dan *insider threats*.	Ya/Parsial/Tidak
244	Penetapan rencana penanganan dan pemulihan insiden siber dilakukan secara formal dan ditetapkan oleh manajemen tertinggi.	Ya/Parsial/Tidak
245	Pelaksanaan evaluasi rencana penanganan dan pemulihan insiden siber dilakukan: a. secara berkala minimal sekali dalam setahun sesuai dengan perkembangan risiko siber; b. melibatkan manajemen tertinggi penyelenggara; dan c. hasil evaluasi rencana penanganan dan pemulihan insiden siber digunakan sebagai perbaikan rencana penanganan dan pemulihan insiden siber kedepan.	Ya/Parsial/Tidak

NO	INDIKATOR	NILAI
246	Memiliki struktur Tim Tanggap Insiden Siber (TTIS) level organisasi.	Ya/Parsial/Tidak
247	Memiliki kejelasan peran dan tanggung jawab TTIS level organisasi.	Ya/Parsial/Tidak
248	Memiliki kriteria pengaktifan TTIS.	Ya/Parsial/Tidak
249	Memiliki kecukupan kapasitas SDM untuk melakukan penanganan dan pemulihan insiden siber.	Ya/Parsial/Tidak
250	Memiliki kecukupan kapabilitas SDM untuk melakukan penanganan dan pemulihan insiden siber.	Ya/Parsial/Tidak
251	TTIS melibatkan personel lintas departemen, unit kerja, dan bagian yang paling sedikit meliputi fungsi manajemen KKS, manajemen risiko, hukum, dan komunikasi.	Ya/Parsial/Tidak
252	Struktur dan susunan keanggotaan TTIS dilaporkan kepada di Bank Indonesia untuk koordinasi penanganan dan pemulihan insiden siber.	Ya/Parsial/Tidak
253	TTIS level organisasi bertanggung jawab kepada manajemen tertinggi.	Ya/Parsial/Tidak
	FAKTOR: PELAKSANAAN SIMULASI & UJICOBA PENANGANAN DAN PEMULIHAN INSIDEN SIBER	
254	Simulasi dan uji coba penanganan dan pemulihan Insiden siber dilakukan dengan mengacu pada profil risiko siber dan kritikalitas fungsi bisnis dan sistem informasi.	Ya/Parsial/Tidak
255	Terdapat skenario simulasi dan uji coba yang disusun berdasarkan hasil identifikasi kerentanan dan ancaman siber.	Ya/Parsial/Tidak
256	Skenario simulasi dan uji coba penanganan serta pemulihan insiden siber mencakup deteksi ancaman siber, eskalasi insiden siber, koordinasi antar tim, eskalasi, respons teknis, komunikasi dengan pemangku kepentingan, serta pemulihan layanan hingga evaluasi pasca-insiden.	Ya/Parsial/Tidak
257	Skenario simulasi dan uji coba penanganan serta pemulihan insiden siber mencakup skenario serangan dari dalam dan luar organisasi Penyelenggara antara lain serangan *malware*, DDoS, *phishing* atau *social engineering*, kegagalan sistem aplikasi dan/atau infrastruktur teknologi informasi, dan *insider threat*.	Ya/Parsial/Tidak
258	*Backup* data diuji secara berkala untuk memastikan integritas dan ketersediaannya dalam proses pemulihan.	Ya/Parsial/Tidak

NO	INDIKATOR	NILAI
259	Pelaksanaan simulasi dan uji coba harus dipastikan kelancaran operasional dan/atau layanan bisnis tetap terjaga, dengan adanya *environment testing*.	Ya/Parsial/Tidak
260	Pelaksanaan simulasi dan uji coba tidak berdampak terhadap terganggunya kelancaran operasional dan/atau layanan bisnis.	Ya/Parsial/Tidak
261	Simulasi dan uji coba penanganan dan pemulihan insiden siber dilakukan dengan melibatkan pemangku kepentingan terkait dan/atau pihak ketiga.	Ya/Parsial/Tidak
262	Berkontribusi aktif dalam simulasi dan uji coba penanganan dan pemulihan insiden siber yang diselenggarakan oleh otoritas sektor keuangan.	Ya/Parsial/Tidak
263	Hasil simulasi dan uji coba dilaporkan kepada manajemen tertinggi.	Ya/Parsial/Tidak
264	Hasil simulasi dan uji coba penanganan dan pemulihan insiden siber dijadikan umpan balik dalam proses peningkatan penanganan dan pemulihan insiden siber.	Ya/Parsial/Tidak
FAKTOR: PENANGANAN INSIDEN SIBER		
265	Penanganan insiden siber level organisasi dikoordinasikan oleh CISO.	Ya/Parsial/Tidak
266	Insiden siber ditetapkan berdasarkan kriteria penetapan insiden siber dan dikategorisasikan berdasarkan rencana penanganan insiden siber.	Ya/Parsial/Tidak
267	Pencatatan insiden siber dilakukan menggunakan *tools* antara lain *ticketing tools* untuk memudahkan manajemen insiden, termasuk melihat progress penanganan dan pemulihan, PIC yang sedang menangani, dan automasi notifikasi informasi dan status penanganan insiden siber.	Ya/Parsial/Tidak
268	Penanganan insiden siber yang berdampak pada ketersediaan layanan dilakukan sesuai dengan target RTO dan RPO.	Ya/Parsial/Tidak
269	Aktivasi TTIS di level organisasi dilakukan mengacu kepada kriteria pengaktifan TTIS yang telah ditetapkan.	Ya/Parsial/Tidak
270	Penyampaian notifikasi awal untuk setiap insiden siber kepada Bank Indonesia dilakukan paling lama 1 (satu) jam setelah insiden siber diketahui oleh Penyelenggara.	Ya/Parsial/Tidak
271	Penyampaian laporan insiden siber untuk setiap insiden siber kepada Bank Indonesia dilakukan paling lama 3 (tiga) hari kalender setelah insiden siber terjadi.	Ya/Parsial/Tidak
272	Pendalaman insiden siber dilakukan dengan memastikan catatan aktivitas siber tercatat dan terjaga integritasnya saat insiden terjadi.	Ya/Parsial/Tidak

NO	INDIKATOR	NILAI
273	Pendalaman insiden siber dilakukan dengan melakukan analisis dampak bisnis dan dampak teknis yang disebabkan insiden siber.	Ya/Parsial/Tidak
274	Analisis dampak bisnis meliputi paling sedikit dampak finansial, reputasi, dan kepatuhan terhadap regulasi.	Ya/Parsial/Tidak
275	Analisis dampak teknis meliputi paling sedikit dampak kerusakan sistem dan kehilangan data.	Ya/Parsial/Tidak
276	Pendalaman insiden siber dilakukan dengan melakukan analisis terhadap akar permasalahan insiden siber.	Ya/Parsial/Tidak
277	Analisis akar permasalahan insiden meliputi analisis forensik dari seluruh sistem terkait yang terdampak.	Ya/Parsial/Tidak
278	Analisis forensik dilakukan paling sedikit meliputi proses *collection*, *examination*, *analysis*, dan *reporting*.	Ya/Parsial/Tidak
279	Analisis forensik dilakukan dengan menggunakan bantuan *tools* forensik.	Ya/Parsial/Tidak
280	Mitigasi insiden siber dilakukan dengan memastikan sumber insiden siber telah dihilangkan (*eradication*) menggunakan *tools*.	Ya/Parsial/Tidak
281	Mitigasi insiden siber dilakukan dengan melakukan isolasi dampak insiden siber (*containment*).	Ya/Parsial/Tidak
282	Mitigasi insiden siber dilakukan dengan melakukan koordinasi penanganan isolasi dampak insiden siber dengan otoritas, lembaga, dan/atau penyelenggara lain yang terhubung dengan sistem penyelenggara.	Ya/Parsial/Tidak
283	Eskalasi penanganan insiden siber dilakukan berdasarkan rencana penanganan insiden siber.	Ya/Parsial/Tidak
284	Eskalasi atau aktivasi manajemen keberlangsungan bisnis dilakukan untuk setiap insiden siber yang berdampak terhadap bisnis penyelenggara.	Ya/Parsial/Tidak
285	Dalam hal penyelenggara melaksanakan penanganan insiden menggunakan sumber daya eskternal, penyelenggara memiliki perjanjian atau kontrak dengan pihak ketiga untuk mendukung penanganan insiden siber.	Ya/Parsial/Tidak
286	Perjanjian atau kontrak dengan pihak ketiga mencakup kerahasiaan data dan/atau informasi oleh pihak ketiga serta *service level agreement* terkait penanganan insiden siber.	Ya/Parsial/Tidak

NO	INDIKATOR	NILAI
	FAKTOR: PELAKSANAAN KOMUNIKASI TINDAKAN PENANGANAN INSIDEN SIBER	
287	Terdapat strategi dan metode komunikasi dalam penanganan dan pemulihan insiden siber, yang meliputi cakupan informasi, waktu yang tepat untuk penyampaian informasi, target penerima informasi/pemangku kepentingan, dan jalur/kanal komunikasi.	Ya/Parsial/Tidak
288	Komunikasi penanganan insiden siber dilakukan sesuai strategi dan metode komunikasi yang telah disusun.	Ya/Parsial/Tidak
289	Komunikasi penanganan insiden siber dilakukan dengan memperhatikan prinsip berorientasi pada piihak yang berkepentingan yang ditargetkan secara spesifik, berkelanjutan dan konsisten, waktu yang tepat, dan kehati-hatian.	Ya/Parsial/Tidak
290	Komunikasi penanganan insiden siber dilakukan antara lain kepada manajemen tertinggi, pihak ketiga, pelanggan, dan otoritas berdasarkan strategi dan metode komunikasi penanganan insiden siber yang telah disusun.	Ya/Parsial/Tidak
291	Komunikasi kemajuan penanganan insiden siber dilakukan dalam hal terdapat perubahan yang signifikan dalam penanganan insiden siber paling sedikit 1 kali dalam 1 hari.	Ya/Parsial/Tidak
292	Penyampaian dan/atau *sharing* informasi penanganan insiden siber dilakukan pada *sharing platform* yang disediakan oleh otoritas.	Ya/Parsial/Tidak
	DIMENSI: PEMULIHAN	
	FAKTOR: PENGEMBALIAN LAYANAN SEBAGAIMANA KONDISI NORMAL	
293	Memiliki lokasi kerja alternatif dalam hal lokasi kerja utama tidak dapat beroperasi sebagai akibat insiden siber.	Ya/Parsial/Tidak
294	Lokasi kerja alternatif sudah dilengkapi dengan berbagai perangkat siap kerja antara lain PC, printer, dan perangkat komunikasi.	Ya/Parsial/Tidak
295	Lokasi kerja alternatif terdapat di lokasi dengan jarak untuk mengantisipasi gangguan pada level bencana (*disaster*) pada lokasi kerja utama.	Ya/Parsial/Tidak
296	Memiliki pusat data alternatif yang terpisah dari pusat data utama.	Ya/Parsial/Tidak
297	Memiliki pusat data alternatif dengan konfigurasi aktif-aktif dengan pusat data utama, sesuai dengan analisis dampak bisnis dan setidaknya untuk sistem dengan tingkat kritikalitas tinggi dan/atau tingkat risiko tinggi.	Ya/Parsial/Tidak

NO	INDIKATOR	NILAI
298	Lokasi pusat data alternatif terdapat di lokasi dengan jarak untuk mengantisipasi gangguan pada level bencana (*disaster*) pada pusat data utama.	Ya/Parsial/Tidak
299	Memiliki sertifikasi pusat data dengan keseluruhan minimal *rating* / *tier* 3.	Ya/Parsial/Tidak
300	Memilki jaringan komunikasi data alternatif yang terpisah dari jaringan komunikasi data utama dan disediakan oleh *provider* yang berbeda.	Ya/Parsial/Tidak
301	Memiliki fitur *load balancing* dan/atau *auto network connection* dalam hal terjadi gangguan pada jaringan komunikasi data utama.	Ya/Parsial/Tidak
302	Pengembalian layanan sebagaimana kondisi normal dilakukan berdasarkan hasil analisis dampak bisnis dan dampak teknis, rencana pemulihan insiden siber, dan kritikalitas fungsi bisnis.	Ya/Parsial/Tidak
303	Pemulihan data dilakukan menggunakan data *backup* yang telah dilakukan *verifikasi integritas bersifat immutable, dan terkini.*	Ya/Parsial/Tidak
304	Keberhasilan pemulihan layanan berdasarkan kriteria keberhasilan pemulihan layanan yang telah ditetapkan penyelenggara.	Ya/Parsial/Tidak
305	Terdapat laporan pemulihan layanan penyelenggara yang diketahui oleh manajemen tertinggi penyelenggara.	Ya/Parsial/Tidak
	FAKTOR: PERBAIKAN BERKELANJUTAN	
306	Evaluasi efektivitas dan perbaikan rencana penanganan dan pemulihan insiden siber dilakukan atas dasar penanganan dan pemulihan insiden siber yang telah dilakukan.	Ya/Parsial/Tidak
307	*Root cause analysis dilakukan* untuk memastikan penyebab insiden siber diketahui.	Ya/Parsial/Tidak
308	*Root cause* ditemukan untuk setiap insiden siber.	Ya/Parsial/Tidak
309	Solusi permanen disusun untuk setiap *root cause* yang ditemukan.	Ya/Parsial/Tidak
310	Solusi permanen diimplementasikan untuk mencegah insiden siber serupa.	Ya/Parsial/Tidak
311	*Lesson learned* didokumentasikan untuk penguatan KKS.	Ya/Parsial/Tidak
	FAKTOR: PELAKSANAAN KOMUNIKASI PEMULIHAN INSIDEN SIBER	
312	Komunikasi pemulihan insiden siber dilakukan sesuai strategi dan metode komunikasi yang telah disusun.	Ya/Parsial/Tidak

NO	INDIKATOR	NILAI
313	Komunikasi pemulihan insiden siber dilakukan dengan memperhatikan prinsip berorientasi pada piihak yang berkepentingan yang ditargetkan secara spesifik, berkelanjutan dan konsisten, waktu yang tepat, dan kehati-hatian.	Ya/Parsial/Tidak
314	Komunikasi pemulihan insiden siber dilakukan antara lain kepada manajemen tertinggi, pihak ketiga, pelanggan, dan otoritas berdasarkan strategi dan metode komunikasi penanganan insiden siber yang telah disusun.	Ya/Parsial/Tidak
315	Komunikasi kemajuan pemulihan insiden siber dilakukan dalam hal terdapat perubahan yang signifikan dalam penanganan insiden siber.	Ya/Parsial/Tidak
	FAKTOR: EVALUASI PENANGANAN	
316	Evaluasi penanganan dilakukan paling sedikit 1 kali dalam 1 tahun.	Ya/Parsial/Tidak
317	Evaluasi penanganan dilakukan dengan memperhatikan profil risiko siber,tren perkembangan siber, hasil respons insiden siber, dan/atau hasil pemulihan insiden siber.	Ya/Parsial/Tidak
318	Hasil evaluasi penanganan disampaikan kepada manajemen tertinggi penyelenggara.	Ya/Parsial/Tidak

LAMPIRAN 3.2
Format Laporan Tingkat Kematangan KKS bagi Penyelenggara dengan Kewajiban Pelaporan Penuh dan Belum Pernah Mengalami Insiden Siber

A. Informasi Pelapor

1. Nama Penyelenggara : .....
2. Alamat Kantor Pusat Penyelenggara : .....
3. Nomor Telepon : .....
4. Nama Narahubung : .....
5. Nomor Telepon Narahubung : .....
6. Tanggal Penyampaian Laporan : .../..../.....(dd/mm/yyyy)
7. Periode Pelaporan : ..... (yyyy)

B. Hasil Asemen Mandiri Indikator Tingkat Kematangan KKS bagi Penyelenggara dengan Kewajiban Pelaporan Penuh dan Belum Pernah Mengalami Insiden Siber

NO	INDIKATOR	NILAI
AREA: TATA KELOLA		
DIMENSI: STRATEGI DAN KEBIJAKAN KKS		
FAKTOR: RENCANA STRATEGIS KKS		
1	Arah strategis penguatan KKS disusun dengan mempertimbangkan arah dan rencana strategis bisnis, selera risiko (*risk appetite*), ketentuan peraturan perundang-undangan mengenai KKS, serta perkembangan tren teknologi, kerentanan siber, dan ancaman siber.	Ya/Parsial/Tidak
2	Peta jalan penguatan KKS disusun sesuai dengan arah strategis KKS.	Ya/Parsial/Tidak
3	Peta jalan penguatan KKS mencakup daftar program dan/atau proyek.	Ya/Parsial/Tidak
4	Peta jalan penguatan KKS mencakup daftar jadwal dan tahapan.	Ya/Parsial/Tidak
5	Peta jalan penguatan KKS mencakup hasil kerja.	Ya/Parsial/Tidak
6	Peta jalan penguatan KKS mencakup pelaksana proyek.	Ya/Parsial/Tidak
7	Perkiraan kebutuhan sumber daya untuk pelaksanaan peta jalan KKS mencakup perkiraan biaya.	Ya/Parsial/Tidak
8	Perkiraan kebutuhan sumber daya untuk pelaksanaan peta jalan KKS mencakup perkiraan sumber daya manusia.	Ya/Parsial/Tidak
9	Penetapan Rencana strategis KKS dilakukan secara formal dan ditetapkan oleh manajemen tertinggi.	Ya/Parsial/Tidak
10	Rencana strategis KKS dilakukan pemantauan pelaksanaannya dan persentase progres pencapaian hasil kerja program dan/atau proyek lebih dari 80% dari rencana jadwal dan tahapan.	Ya/Parsial/Tidak

NO	INDIKATOR	NILAI
11	Pelaksanaan evaluasi rencana strategis KKS: a. dilakukan secara berkala minimal sekali dalam setahun dengan memperhatikan perkembangan risiko siber; b. melibatkan manajemen tertinggi penyelenggara; dan c. hasil evaluasi rencana strategis KKS digunakan sebagai perbaikan rencana strategis KKS ke depan.	Ya/Parsial/Tidak
FAKTOR: KEBIJAKAN STANDAR DAN PROSEDUR KKS		
12	Kebijakan pengamanan KKS paling sedikit terdiri atas pengamanan data, sistem aplikasi, infrastruktur teknologi informasi, pihak ketiga, serta pelindungan konsumen dan manajemen *fraud*.	Ya/Parsial/Tidak
13	Standar pengamanan KKS paling sedikit terdiri atas pengamanan data, sistem aplikasi, infrastruktur teknologi informasi, pihak ketiga, serta pelindungan konsumen dan manajemen *fraud*.	Ya/Parsial/Tidak
14	Prosedur pengamanan KKS paling sedikit terdiri atas pengamanan data, sistem aplikasi, infrastruktur teknologi informasi, pihak ketiga, serta pelindungan konsumen dan manajemen *fraud*.	Ya/Parsial/Tidak
15	Kebijakan, standar, dan prosedur KKS disusun dengan memperhatikan rencana strategis KKS, kompleksitas sistem informasi, dan profil risiko.	Ya/Parsial/Tidak
16	Penetapan Kebijakan KKS dilakukan secara formal dan ditetapkan oleh manajemen tertinggi.	Ya/Parsial/Tidak
17	Kebijakan, standar, dan prosedur KKS sudah diterapkan dan dikomunikasikan: a. kepada seluruh pihak internal dan/atau pihak ketiga yang terkait ketika pertama kali bekerja; b. secara tahunan; dan c. jika terdapat perubahan.	Ya/Parsial/Tidak
18	Pelaksanaan evaluasi kebijakan, standar, dan prosedur KKS dilakukan: a. secara berkala minimal sekali dalam setahun; b. melibatkan manajemen tertinggi penyelenggara; dan c. hasil evaluasi kebijakan, standar, dan prosedur KKS digunakan sebagai perbaikan kebijakan, standar, dan prosedur KKS ke depan.	Ya/Parsial/Tidak
FAKTOR: FUNGSI ORGANISASI KKS		
19	Memiliki fungsi manajemen KKS, manajemen risiko KKS, dan audit KKS dalam struktur organisasi yang terpisah.	Ya/Parsial/Tidak

NO	INDIKATOR	NILAI
20	Manajemen KKS memiliki visi dan misi yang jelas.	Ya/Parsial/Tidak
21	Manajemen KKS memiliki struktur organisasi dan struktur jabatan yang jelas.	Ya/Parsial/Tidak
22	Manajemen KKS memiliki tugas pokok dan produk pokok manajemen KKS yang jelas.	Ya/Parsial/Tidak
23	Manajemen KKS memiliki uraian tugas dan profil persyaratan jabatan yang jelas.	Ya/Parsial/Tidak
24	Manajemen KKS memiliki kapasitas SDM yang mencukupi terkait KKS.	Ya/Parsial/Tidak
25	Manajemen KKS memiliki kapabilitas SDM yang memadai terkait KKS.	Ya/Parsial/Tidak
26	Manajemen KKS memiliki program peningkatan kapabilitas SDM terkait manajemen KKS.	Ya/Parsial/Tidak
27	Penerapan manajemen KKS meliputi perencanaan strategis KKS, penyusunan kebijakan, standar, dan prosedur KKS, penerapan budaya KKS, serta pelaksanaan pencegahan dan penanganan KKS.	Ya/Parsial/Tidak
28	Manajemen KKS bertanggung jawab kepada manajemen tertinggi.	Ya/Parsial/Tidak
29	Pelaksanaan evaluasi manajemen KKS dilakukan: a. secara berkala minimal sekali dalam setahun b. melibatkan manajemen tertinggi penyelenggara; dan c. hasil evaluasi penerapan manajemen KKS digunakan sebagai perbaikan fungsi organisasi manajemen KKS.	Ya/Parsial/Tidak
30	Manajemen risiko siber memiliki visi dan misi yang jelas.	Ya/Parsial/Tidak
31	Manajemen risiko siber memiliki struktur organisasi dan struktur jabatan yang jelas.	Ya/Parsial/Tidak
32	Manajemen risiko siber memiliki tugas pokok dan produk pokok yang jelas.	Ya/Parsial/Tidak
33	Manajemen risiko siber memiliki uraian tugas dan profil persyaratan jabatan yang jelas.	Ya/Parsial/Tidak
34	Manajemen risiko siber memiliki kapasitas SDM yang mencukupi terkait manajemen risiko siber.	Ya/Parsial/Tidak
35	Manajemen risiko siber memiliki kapabilitas SDM yang memadai terkait manajemen risiko siber.	Ya/Parsial/Tidak
36	Manajemen risiko siber memiliki program peningkatan kapabilitas SDM terkait manajemen risiko siber.	Ya/Parsial/Tidak
37	Manajemen risiko siber terintegrasi ke dalam proses manajemen risiko penyelenggara.	Ya/Parsial/Tidak

NO	INDIKATOR	NILAI
38	Penerapan manajemen risiko siber meliputi identifikasi, asesmen, mitigasi, dan evaluasi risiko siber terhadap ancaman siber atau serangan siber.	Ya/Parsial/Tidak
39	Manajemen risiko siber bertanggung jawab kepada manajemen tertinggi.	Ya/Parsial/Tidak
40	Pelaksanaan evaluasi manajemen risiko siber dilakukan: a. secara berkala minimal sekali dalam setahun sesuai dengan perkembangan risiko siber; b. melibatkan manajemen tertinggi penyelenggara; dan c. hasil evaluasi penerapan manajemen risiko siber digunakan sebagai perbaikan fungsi organisasi manajemen risiko siber.	Ya/Parsial/Tidak
41	Audit KKS memiliki objektif yang jelas.	Ya/Parsial/Tidak
42	Audit KKS memiliki struktur organisasi dan struktur jabatan yang jelas.	Ya/Parsial/Tidak
43	Audit KKS memiliki tugas pokok dan produk pokok yang jelas.	Ya/Parsial/Tidak
44	Audit KKS memiliki mempunyai uraian tugas dan profil persyaratan jabatan yang jelas.	Ya/Parsial/Tidak
45	Audit KKS internal memiliki kapasitas SDM yang mencukupi terkait audit KKS.	Ya/Parsial/Tidak
46	Audit KKS internal memiliki kapabilitas SDM yang memadai terkait audit KKS.	Ya/Parsial/Tidak
47	Audit KKS memiliki program peningkatan kapabilitas SDM terkait audit KKS.	Ya/Parsial/Tidak
48	Audit KKS dilakukan oleh pihak eksternal yang merupakan auditor KKS independen yang terdaftar di SRO dan/atau otoritas lain.	Ya/Parsial/Tidak
49	Audit KKS bertanggung jawab kepada manajemen tertinggi.	Ya/Parsial/Tidak
50	Audit KKS dilakukan minimal 1 kali dalam 1 tahun.	Ya/Parsial/Tidak
51	Audit KKS mencakup tata kelola, pencegahan, dan penanganan	Ya/Parsial/Tidak
52	Memiliki sertifikasi audit KKS berstandar internasional antara lain ISO 27001 dan PCI-DSS.	Ya/Parsial/Tidak
53	Hasil audit KKS disampaikan kepada manajemen tertinggi dan digunakan untuk perbaikan tata kelola, pencegahan, dan penanganan.	Ya/Parsial/Tidak

NO	INDIKATOR	NILAI
54	Pelaksanaan evaluasi audit KKS dilakukan: a. secara berkala minimal sekali dalam setahun sesuai dengan perkembangan risiko siber; b. melibatkan manajemen tertinggi penyelenggara; dan c. hasil evaluasi penerapan manajemen risiko siber digunakan sebagai perbaikan fungsi organisasi audit KKS.	Ya/Parsial/Tidak
DIMENSI: BUDAYA KKS		
55	Program peningkatan budaya KKS berupa *awareness* diberikan secara berkala sesuai dengan kewenangan dan tanggung jawab personel internal.	Ya/Parsial/Tidak
56	Program peningkatan budaya KKS berupa pelatihan diberikan secara berkala sesuai dengan kewenangan dan tanggung jawab personel internal.	Ya/Parsial/Tidak
57	Program peningkatan budaya KKS berupa edukasi diberikan sesuai dengan kewenangan dan tanggung jawab personel internal.	Ya/Parsial/Tidak
58	Personel internal menjaga pengetahuan KKS tetap terbaru dengan menghadiri konferensi dan acara yang bertujuan untuk peningkatan teknis dan profesional.	Ya/Parsial/Tidak
59	Program peningkatan budaya KKS berupa *awareness* diberikan secara berkala sesuai dengan kewenangan dan tanggung jawab pihak ketiga.	Ya/Parsial/Tidak
60	Program peningkatan budaya KKS berupa pelatihan diberikan secara berkala sesuai dengan kewenangan dan tanggung jawab pihak ketiga.	Ya/Parsial/Tidak
61	Program peningkatan budaya KKS berupa *awareness* diberikan secara berkala sesuai dengan kewenangan dan tanggung jawab konsumen.	Ya/Parsial/Tidak
62	Pelaksanaan program peningkatan budaya KKS melibatkan manajemen tertinggi.	Ya/Parsial/Tidak
63	Program peningkatan budaya KKS dilakukan secara berkala paling sedikit 1 kali dalam 1 tahun.	Ya/Parsial/Tidak
64	Program peningkatan budaya KKS diselaraskan dengan rencana strategis KKS.	Ya/Parsial/Tidak

NO	INDIKATOR	NILAI
65	Pelaksanaan evaluasi program peningkatan budaya KKS dilakukan: a. secara berkala minimal sekali dalam setahun sesuai dengan perkembangan risiko siber; b. melibatkan manajemen tertinggi penyelenggara; dan c. hasil evaluasi program peningkatan budaya KKS digunakan sebagai perbaikan program peningkatan budaya KKS ke depan.	Ya/Parsial/Tidak
AREA: PENCEGAHAN		
DIMENSI: IDENTIFIKASI		
FAKTOR: PENYUSUNAN PROFIL RISIKO SIBER		
66	Identifikasi risiko siber dilakukan dengan memperhatikan kerentanan dan ancaman siber dari aspek manusia dengan memantau perkembangan siber terkini yang bersumber dari internal dan eksternal, antara lain ketidakcukupan kapasitas dan kapabilitas SDM.	Ya/Parsial/Tidak
67	Identifikasi risiko siber dilakukan dengan memperhatikan kerentanan dan ancaman siber dari aspek proses dengan memantau perkembangan siber terkini yang bersumber dari internal dan eksternal, antara lain ketidakcukupan kebijakan, standar, dan prosedur KKS.	Ya/Parsial/Tidak
68	Identifikasi risiko siber dilakukan dengan memperhatikan kerentanan dan ancaman siber dari aspek teknologi dengan memantau perkembangan siber terkini yang bersumber dari internal dan eksternal, antara lain *vulnerability* teknologi baru.	Ya/Parsial/Tidak
69	Identifikasi risiko siber dilakukan dengan memperhatikan objek yang akan dilindungi meliputi data yang dikelola oleh penyelenggara.	Ya/Parsial/Tidak
70	Identifikasi risiko siber dilakukan dengan memperhatikan objek yang akan dilindungi meliputi sistem aplikasi dan konfigurasinya yang dikelola oleh penyelenggara.	Ya/Parsial/Tidak
71	Identifikasi risiko siber dilakukan dengan memperhatikan objek yang akan dilindungi meliputi infrastruktur teknologi informasi dan konfigurasinya yang dikelola oleh penyelenggara.	Ya/Parsial/Tidak
72	Identifikasi risiko siber dilakukan dengan memperhatikan objek yang akan dilindungi meliputi Sistem Informasi yang dikelola oleh pihak ketiga.	Ya/Parsial/Tidak
73	Objek yang dilindungi diprioritisasi berdasarkan klasifikasi, kritikalitas, sumber daya, dan dampak terhadap bisnis.	Ya/Parsial/Tidak

NO	INDIKATOR	NILAI
74	Inventarisasi objek yang dilindungi dilakukan dengan menggunakan sistem/*tools*.	Ya/Parsial/Tidak
75	Memiliki konfigurasi keterhubungan antar objek yang dilindungi yang tersimpan dalam *configuration management system*.	Ya/Parsial/Tidak
76	Identifikasi risiko siber untuk informasi kerentanan siber dan ancaman siber didapatkan dari sarana pertukaran informasi yang dibentuk Bank Indonesia.	Ya/Parsial/Tidak
77	Identifikasi risiko siber untuk informasi kerentanan siber dan ancaman siber didapatkan dari sarana pertukaran informasi sesama penyelenggara.	Ya/Parsial/Tidak
78	Identifikasi risiko siber untuk informasi kerentanan siber dan ancaman siber didapatkan dari *cyber threat intelligence*.	Ya/Parsial/Tidak
79	Hasil identifikasi kerentanan siber dan ancaman siber didokumentasikan pada inventaris risiko siber (*cyber risk register*) pada level fungsi manajemen KKS.	Ya/Parsial/Tidak
80	Hasil identifikasi kerentanan siber dan ancaman siber didokumentasikan pada inventaris risiko siber (*cyber risk register*) pada level *enterprise risk management.*	Ya/Parsial/Tidak
81	Memiliki metodologi asesmen risiko siber yang mencakup penilaian dampak yang ditimbulkan dari risiko siber (*impact*) dan penilaian kemungkinan terjadinya risiko siber (*likelihood*).	Ya/Parsial/Tidak
82	Metodologi asesmen risiko siber selaras dengan metode asesmen *enterprise risk management* penyelenggara.	Ya/Parsial/Tidak
83	Metodologi asesmen risiko siber diuji dengan menggunakan sampling risiko siber untuk memastikan hasil asesmen risiko yang konsisten dan valid.	Ya/Parsial/Tidak
84	Melakukan penilaian dampak kerentanan siber dan ancaman siber berupa perkiraan kerugian sebagai akibat gangguan layanan (contoh: potensi kehilangan *revenue*).	Ya/Parsial/Tidak
85	Melakukan penilaian dampak kerentanan siber dan ancaman siber berupa dampak kerusakan (contoh: kerugian non-finansial antara lain reputasi, hukum, dan *compliance*).	Ya/Parsial/Tidak
86	Melakukan penilaian dampak kerentanan siber dan ancaman siber berupa biaya pemulihan yang harus dilakukan (biaya yang dikeluarkan untuk penanganan dan pemulihan atas Insiden Siber).	Ya/Parsial/Tidak
87	Daftar risiko siber dilakukan prioritisasi berdasarkan *impact* dan *likelihood*.	Ya/Parsial/Tidak

NO	INDIKATOR	NILAI
88	*Risk treatments* (*accept, mitigate, transfer, avoid*) dilakukan untuk daftar risiko yang telah diprioritisasi berdasarkan selera dan toleransi risiko siber.	Ya/Parsial/Tidak
89	Prioritasi mitigasi kerentanan siber dan ancaman siber dilakukan berdasarkan tingkat risiko siber, urgensi waktu pelaksanaan mitigasi risiko siber, dan urutan pelaksanaan mitigasi risiko siber.	Ya/Parsial/Tidak
90	Penilaian dampak bisnis dilakukan dengan menetapkan jenis dampak finansial dan non finansial.	Ya/Parsial/Tidak
91	Penilaian dampak bisnis dilakukan dengan menetapkan *Maximum Tolerable Period of Disruption* (MTPD) untuk setiap layanan.	Ya/Parsial/Tidak
92	Penetapan MTPD telah dianalisis dengan mempertimbangkan sasaran waktu pemulihan (*Recovery Time Objective* - RTO).	Ya/Parsial/Tidak
93	Penilaian dampak bisnis dilakukan dengan menetapkan sumber daya finansial untuk mendukung fungsi bisnis yang diprioritaskan.	Ya/Parsial/Tidak
94	Penilaian dampak bisnis dilakukan dengan menetapkan sumber daya manusia untuk mendukung fungsi bisnis yang diprioritaskan.	Ya/Parsial/Tidak
95	Analisis kritikalitas fungsi bisnis dan sistem informasi dilakukan dengan menetapkan sasaran waktu pemulihan (*Recovery Time Objective* - RTO).	Ya/Parsial/Tidak
96	Analisis kritikalitas fungsi bisnis dan sistem informasi dilakukan dengan menetapkan sasaran titik pemulihan (*Recovery Point Objective* - RPO).	Ya/Parsial/Tidak
97	Analisis kritikalitas fungsi bisnis dan sistem informasi dilakukan dengan menetapkan *service level* untuk sistem informasi.	Ya/Parsial/Tidak
98	Analisis kritikalitas fungsi bisnis dan sistem informasi dilakukan dengan menetapkan *maximum downtime* yang tidak terjadwal.	Ya/Parsial/Tidak
99	Analisis kritikalitas fungsi bisnis dan sistem informasi dilakukan dengan menetapkan *maximum downtime* yang terjadwal.	Ya/Parsial/Tidak
100	Memiliki inventaris sistem aplikasi dan infrastruktur teknologi informasi terkait pelaksanaan kegiatan sistem pembayaran, pasar uang dan pasar valuta asing, dan/atau kegiatan usaha penukaran valuta asing bukan bank yang berdampak luas terhadap stabilitas sistem keuangan.	Ya/Parsial/Tidak
101	Melakukan analisis sistem aplikasi dan infrastruktur teknologi informasi yang berdampak luas terhadap stabilitas sistem keuangan.	Ya/Parsial/Tidak

NO	INDIKATOR	NILAI
102	Melakukan implementasi penguatan KKS berdasarkan peta jalan penguatan Infrastruktur Informasi Vital (IIV) sektor keuangan.	Ya/Parsial/Tidak
	FAKTOR: PENGINIAN PROFIL RISIKO SIBER	
103	Profil risiko siber dievaluasi dan dikinikan paling sedikit 1 kali dalam 1 tahun.	Ya/Parsial/Tidak
104	Profil risiko siber dikinikan setiap terjadi insiden siber.	Ya/Parsial/Tidak
105	Profil risiko siber ditetapkan oleh manajemen tertinggi.	Ya/Parsial/Tidak
	DIMENSI: PROTEKSI	
	FAKTOR: PEMBANGUNAN SISTEM PERTAHANAN	
106	Keamanan pihak internal dan pihak ketiga dipastikan dengan melakukan verifikasi latar belakang pihak internal dan/atau pihak ketiga yang akan dipekerjakan.	Ya/Parsial/Tidak
107	Verifikasi latar belakang dilakukan dengan memperhatikan ketentuan organisasi terkini, klasifikasi informasi yang diakses, dan risiko yang dihadapi.	Ya/Parsial/Tidak
108	Mengomunikasikan peran dan tanggung jawab KKS kepada personel pihak internal dan/atau pihak ketiga yang dipekerjakan.	Ya/Parsial/Tidak
109	Mewajibkan personel pihak internal dan/atau pihak ketiga telah menandatangani perjanjian atau surat pernyataan untuk menjaga kerahasiaan data dan/atau informasi dari pihak yang tidak berwenang.	Ya/Parsial/Tidak
110	Persyaratan perjanjian kerahasiaan dan *Non-Disclosure Agreement* (NDA) ditinjau secara berkala dan ketika terjadi perubahan yang mempengaruhi persyaratan ini.	Ya/Parsial/Tidak
111	Terdapat mekanisme sanksi terhadap pelanggaran kebijakan KKS.	Ya/Parsial/Tidak
112	Menerapkan pemisahan tugas yang dapat menimbulkan konflik kepentingan dalam pelaksanaan peran dan tanggung jawab personel pihak internal dan/atau pihak ketiga.	Ya/Parsial/Tidak
113	Melaksanakan alih pengetahuan dalam hal terdapat perpindahan tanggung jawab atau penonaktifan personel pihak internal dan/atau pihak ketiga.	Ya/Parsial/Tidak
114	Melakukan monitoring terhadap personel internal dan pihak ketiga untuk memastikan kerahasiaan data dan/atau informasi dari pihak yang tidak berwenang selama personel dipekerjakan, saat terjadi perpindahan tanggung jawab, dan saat dinonaktifkan.	Ya/Parsial/Tidak

NO	INDIKATOR	NILAI
115	Menerapkan manajemen akses antara lain standar penggunaan *password* yang meliputi kompleksitas *password*, limit upaya percobaan penggunaan *password*, dan penggantian *default password*.	Ya/Parsial/Tidak
116	Semua *password* dan akun *default* telah diubah sebelum implementasi sistem aplikasi dan infrastruktur teknologi informasi.	Ya/Parsial/Tidak
117	Menerapkan *zero trust architecture*.	Ya/Parsial/Tidak
118	Akses diberikan sesuai dengan kewenangan berdasarkan prinsip *least privilege* dan *segregation of duties*.	Ya/Parsial/Tidak
119	*User access matrix* dan daftar akses pengguna dievaluasi secara berkala (contoh: ketika ada pergantian peran atau personel yang keluar dari organisasi).	Ya/Parsial/Tidak
120	Menerapkan kontrol keamanan fisik berlapis antara lain personel *security*, CCTV, dan sistem alarm.	Ya/Parsial/Tidak
121	Memiliki prosedur pengawalan tamu, vendor, dan pihak ketiga lainnya di area kritikal antara lain ruang operator dan *data center*.	Ya/Parsial/Tidak
122	*User access review* dilakukan secara berkala untuk setiap sistem aplikasi dan infrastruktur teknologi informasi.	Ya/Parsial/Tidak
123	Setiap perubahan akses user ke level *administrator* akan memicu notifikasi ke manajemen KKS.	Ya/Parsial/Tidak
124	Setiap terdapat akses ke sistem aplikasi dan infrastruktur teknologi informasi yang tidak biasa, akan memicu notifikasi ke manajemen KKS.	Ya/Parsial/Tidak
125	Menerapkan proses manajemen perubahan konfigurasi sistem aplikasi dan infrastruktur teknologi informasi.	Ya/Parsial/Tidak
126	Konfigurasi untuk seluruh layanan kritikal dilakukan *monitoring* secara *realtime*.	Ya/Parsial/Tidak
127	Memiliki *tools* untuk mengelola akses dan konfigurasi antara lain *identity management system* (IDMS) atau *identity access management* (IAM).	Ya/Parsial/Tidak
128	Penginian pengendalian keamanan dilakukan secara berkala untuk memastikan kecukupan kontrol keamanan.	Ya/Parsial/Tidak
129	Melakukan perencanaan dan *due diligence* untuk mengurangi risiko sebelum melakukan kerja sama dengan pihak ketiga.	Ya/Parsial/Tidak

NO	INDIKATOR	NILAI
130	Terdapat persyaratan keamanan siber untuk setiap kontrak/perjanjian antara Penyelenggara dengan pihak ketiga, termasuk menjaga kerahasiaan informasi.	Ya/Parsial/Tidak
131	Memiliki kebijakan untuk melakukan dokumentasi, pengujian, dan pemantauan model kecerdasan artifisial secara berkelanjutan dalam hal menggunakan sistem kecerdasan artifisial.	Ya/Parsial/Tidak
132	Menerapkan *defence in depth strategy*.	Ya/Parsial/Tidak
133	Menerapkan segmentasi jaringan antara lain internet, ekstranet, dan intranet.	Ya/Parsial/Tidak
134	Memiliki *network perimeter defence tools* antara lain *firewall.*	Ya/Parsial/Tidak
135	*Firewall* diimplementasikan pada setiap jaringan yang terhubung dengan internet serta antara *Demilitarised Zone* (DMZ) dan intranet.	Ya/Parsial/Tidak
136	*Firewall rules* diverifikasi secara berkala.	Ya/Parsial/Tidak
137	Memiliki IPS/IDS untuk mendeteksi atau membatasi percobaan serangan atau intrusi.	Ya/Parsial/Tidak
138	Menerapkan anti *spoofing* untuk mendeteksi dan membatasi *forged source* IP *address* yang masuk ke dalam jaringan.	Ya/Parsial/Tidak
139	Terdapat antivirus dan anti *malware* pada setiap sistem aplikasi dan infrastruktur teknologi informasi termasuk *end point devices*, antara lain *work station*, *laptop*, dan *mobile devices*.	Ya/Parsial/Tidak
140	*Antivirus* dan *anti-malware* yang terupdate secara otomatis.	Ya/Parsial/Tidak
141	Menerapkan kontrol dan pemindaian untuk setiap *attachment e-mail, malware,* situs *web* yang memiliki risiko siber.	Ya/Parsial/Tidak
142	Terdapat *centralized end-point management tools* yang mengintegrasikan managemen *patching*, konfigurasi, dan manajemen kerentanan yang terintegrasi penuh, serta dapat mendeteksi *malware*.	Ya/Parsial/Tidak
143	Menerapkan *whitelist* aplikasi untuk memastikan hanya perangkat lunak yang terotorisasi yang dapat dijalankan oleh sistem.	Ya/Parsial/Tidak
144	melindungi integritas dan keamanan data dengan menyimpan *master images* pada server yang telah dikonfigurasi dengan kontrol yang ketat.	Ya/Parsial/Tidak
145	Menerapkan *secure coding* pada pengembangan sistem aplikasi sesuai dengan standar industri.	Ya/Parsial/Tidak
146	Pengembangan sistem aplikasi dilakukan pada *environment development* yang terpisah dari *environment production*.	Ya/Parsial/Tidak

NO	INDIKATOR	NILAI
147	Pengembangan sistem aplikasi menggunakan *software*, dan/atau *libraries* yang berasal dari sumber yang kredibel.	Ya/Parsial/Tidak
148	Pengujian keamanan dilakukan pada tahapan *unit testing*, *system integration testing*, dan *user acceptance testing*.	Ya/Parsial/Tidak
149	Pengujian keamanan dilakukan sebelum *deployment* sistem aplikasi di *environment production* antara lain *code review* dan *penetration testing*.	Ya/Parsial/Tidak
150	Pengujian keamanan dilakukan pada *environment testing* yang terpisah dari *environment development* dan *environment production*.	Ya/Parsial/Tidak
151	Pengujian keamanan dilakukan sebelum *deployment* sistem aplikasi di *environment production* atau setelah terdapat perubahan signifikan pada sistem aplikasi berbasis web yang terhubung ke internet antara lain dengan *SQL injection*, *cross-site*, dan *buffer overflow*.	Ya/Parsial/Tidak
152	*Patching* dilakukan dengan menggunakan versi perangkat lunak terkini dan telah teruji untuk setiap sistem aplikasi dan infrastruktur teknologi informasi.	Ya/Parsial/Tidak
153	*Menerapkan tools untuk* monitoring status *patch* pada setiap sistem aplikasi dan infrastruktur teknologi informasi untuk mengidentifikasi *patch* yang belum *update*.	Ya/Parsial/Tidak
154	*Remote* akses dilengkapi dengan pengamanan, antara lain *Virtual Private Network* (VPN) dan *Multi-Factor Authentication* (MFA).	Ya/Parsial/Tidak
155	Memiliki *password management system* yang dapat melakukan *enforcement* penerapan kontrol akses penggunaan *password*.	Ya/Parsial/Tidak
156	Akses ke sistem menggunakan *single factor authentication* antara lain *Personal Identification Number* (PIN) atau *password*.	Ya/Parsial/Tidak
157	Akses ke sistem kritikal menggunakan *two factor authentication* antara lain *password* dan token.	Ya/Parsial/Tidak
158	Akses ke sistem kritikal menggunakan *multi-factor authentication* antara lain *password*, token, dan *biometric*.	Ya/Parsial/Tidak
159	Enkripsi diterapkan untuk setiap otentikasi dan transmisi data yang melewati *wireless network*.	Ya/Parsial/Tidak
160	Terdapat teknologi *cyber deception* (penerapan *decoy* dan/atau *traps*) untuk mendeteksi, mencegah, dan mengalihkan serangan siber, serta mendapatkan informasi tambahan dari pelaku insiden siber.	Ya/Parsial/Tidak

NO	INDIKATOR	NILAI
161	Terdapat sistem pertahanan untuk memitigasi *adversarial attack* pada model kecerdasan artifisial dalam hal menggunakan sistem kecerdasan artifisial.	Ya/Parsial/Tidak
FAKTOR: PENGAMANAN DATA DAN/ATAU INFORMASI		
162	Data dan/atau informasi diamankan sesuai dengan klasifikasi data dan/atau informasi penyelenggara.	Ya/Parsial/Tidak
163	Data dan/atau informasi yang disimpan telah dilakukan pengamanan antara lain enkripsi, *digital signature*, dan kriptografi untuk memastikan keamanan aspek *confidentiality, integrity,* dan *availability*.	Ya/Parsial/Tidak
164	*Backup* data dilakukan secara berkala.	Ya/Parsial/Tidak
165	*Backup* data dilakukan termasuk untuk data konfigurasi sistem antara lain *images server* dan konfigurasi *router*.	Ya/Parsial/Tidak
166	Pengujian *restore backup* data dilakukan secara berkala di *environment testing* paling sedikit 1 kali dalam 1 tahun.	Ya/Parsial/Tidak
167	Menyimpan *backup* dengan aman secara *offline* dan *offsite* sehingga tidak terdampak ketika terjadi insiden atau bencana.	Ya/Parsial/Tidak
168	Menerapkan pemisahan secara geografis dan pembatasan geolokasi untuk penyimpanan *backup* data.	Ya/Parsial/Tidak
169	Menerapkan *full disk encryption* untuk melindungi data yang disimpan pada *user endpoint*.	Ya/Parsial/Tidak
170	Membatasi penggunaan *removable media* untuk mencegah eksfiltrasi data.	Ya/Parsial/Tidak
171	Data dan/atau informasi yang ditransmisikan telah dilakukan pengamanan antara lain enkripsi, *digital signature*, dan kriptografi untuk memastikan keamanan aspek *confidentiality, integrity,* dan *availability*.	Ya/Parsial/Tidak
172	Menerapkan *tools data loss prevention* pada komunikasi *inbound* dan *outbound*, antara lain *email*, FTP, dan Telnet.	Ya/Parsial/Tidak
173	Secara otomatis mengenkripsi atau memblokir *email* keluar dan komunikasi lain yang berisi data sensitif yang tidak sesuai dengan klasifikasi data.	Ya/Parsial/Tidak
174	Membatasi penggunaan data sensitif dari *production enviroment* antara lain data konsumen pada *environment development*, *testing*, atau *non-production* lain.	Ya/Parsial/Tidak

NO	INDIKATOR	NILAI
175	Data sensitif dari *environment production* dilakukan *data masking* sebelum digunakan pada *environment development*, *testing*, atau *non-production* lain.	Ya/Parsial/Tidak
176	Menggunakan fitur *password*, PIN, dan/atau MFA dalam pengamanan data dan/atau informasi ketika akan digunakan.	Ya/Parsial/Tidak
177	Menggunakan fitur *password*, PIN, dan/atau MFA dalam pengamanan data dan/atau informasi ketika akan dimusnahkan oleh pengguna yang sah.	Ya/Parsial/Tidak
178	Memiliki kebijakan dan prosedur untuk pemusnahan data dengan memperhatikan retensi data.	Ya/Parsial/Tidak
179	Pengamanan dan pelindungan data dan/atau informasi dilakukan sesuai dengan ketentuan mengenai pelindungan data pribadi.	Ya/Parsial/Tidak
DIMENSI: DETEKSI		
FAKTOR: PEMANTAUAN		
180	Deteksi dilaksanakan secara terpusat untuk mempercepat proses deteksi dan respons kerentanan siber, serangan siber, dan/atau insiden siber antara lain dengan menerapkan fungsi *Security Operation Center* (SOC).	Ya/Parsial/Tidak
181	Fungsi SOC dilengkapi dengan *red team* dan *blue team*.	Ya/Parsial/Tidak
182	Fungsi SOC dilengkapi dengan *threat hunter*.	Ya/Parsial/Tidak
183	Memiliki sumber daya manusia yang kompeten untuk melakukan deteksi.	Ya/Parsial/Tidak
184	Memiliki standar dan prosedur pelaksanaan untuk melakukan deteksi.	Ya/Parsial/Tidak
185	Memiliki teknologi sebagai alat bantu untuk melakukan deteksi.	Ya/Parsial/Tidak
186	Memiliki sistem yang dapat mendeteksi upaya akses tidak sah melalui jaringan baik *wired* maupun *wireless*, antara lain upaya pengubahan DNS, upaya koneksi *endpoint* yang tidak sah, upaya perubahan konfigurasi jaringan/perangkat keras/perangkat lunak yang tidak sah, pencurian/perusakan data.	Ya/Parsial/Tidak
187	Sistem dapat memantau *log* tentang akses *logical* untuk mengetahui pola akses yang tidak biasa dan upaya akses yang gagal.	Ya/Parsial/Tidak
188	Sistem dapat mendeteksi dan memblokir akses *environment production* secara *remote* bagi pihak ketiga.	Ya/Parsial/Tidak
189	Sistem dapat memantau *wired* dan *wireless network* untuk koneksi yang berasal dari *unauthorized endpoints*.	Ya/Parsial/Tidak

NO	INDIKATOR	NILAI
190	*Monitoring* jaringan komunikasi dapat mengidentifikasi perubahan pada *security postures* untuk kebutuhan *zero trust*.	Ya/Parsial/Tidak
191	Sistem dapat mendeteksi anomali aktivitas yang dilakukan oleh nasabah/konsumen, memberikan notifikasi, dan mencegah transaksi tidak terjadi/terulang.	Ya/Parsial/Tidak
192	Memiliki sistem untuk mendeteksi akses fisik yang tidak sah dan/atau upaya akses gagal beberapa kali.	Ya/Parsial/Tidak
193	Sistem dapat memantau *log* dari sistem kontrol akses fisik antara lain *badge readers* untuk menemukan pola akses yang tidak biasa dan percobaan akses gagal.	Ya/Parsial/Tidak
194	Melakukan review dan *monitoring* catatan akses fisik antara lain *visitor registration* dan akses masuk perangkat.	Ya/Parsial/Tidak
195	Sistem dilengkapi oleh sistem *alarm*, kamera pemantau (CCTV) dan petugas keamanan pada area dan/atau objek kritikal atau vital.	Ya/Parsial/Tidak
196	Menerapkan *behaviour analytics software* untuk mendeteksi aktivitas pengguna yang tidak wajar guna memitigasi ancaman orang dalam.	Ya/Parsial/Tidak
197	Menerapkan *monitoring* untuk *remote* dan *onsite* aktivitas administrasi dan *maintenance* yang dilakukan oleh pihak ketiga.	Ya/Parsial/Tidak
198	Menerapkan *monitoring* aktivitas layanan *cloud*, *internet services providers*, dan penyedia layanan lain dari pola akses yang tidak biasa.	Ya/Parsial/Tidak
199	Seluruh *log* / rekaman akses logis dan fisik disimpan dan di*backup* dengan memperhatikan masa retensi.	Ya/Parsial/Tidak
200	Log/rekaman akses logis dan fisik dilakukan review secara berkala.	Ya/Parsial/Tidak
201	Perubahan terhadap akses logis dan fisik dilakukan dengan prinsip *segregation of duties* dan dikelola melalui prosedur manajemen perubahan.	Ya/Parsial/Tidak
202	Terdapat penetapan indikator ambang batas (*threshold)* sebagai pemicu aktivasi sistem peringatan dengan mengacu pada profil risiko siber.	Ya/Parsial/Tidak
203	Melakukan evaluasi efektivitas indikator ambang batas secara berkala.	Ya/Parsial/Tidak
204	Pemindaian kerentanan siber dilakukan pada setiap sistem aplikasi, infrastruktur teknologi informasi, dan data secara bergiliran dan terjadwal mengacu pada profil risiko siber.	Ya/Parsial/Tidak

NO	INDIKATOR	NILAI
205	Pemindaian kerentanan siber dilakukan dan dianalisis sebelum dilakukan *deployment* atau *re-deployment* terhadap terhadap sistem aplikasi dan/atau infrastruktur teknologi informasi baru atau eksisting.	Ya/Parsial/Tidak
206	Evaluasi terhadap pemindaian kerentanan siber dilakukan paling sedikit 1 kali dalam 1 tahun.	Ya/Parsial/Tidak
	FAKTOR: ANALISIS HASIL PEMANTAUAN	
207	Melakukan analisis hasil pemantauan untuk catatan aktivitas siber yang meliputi pola aktivitas siber yang tidak biasa dan korelasi catatan aktivitas siber dari seluruh sistem aplikasi dan infrastruktur teknologi informasi. Pola aktivitas siber yang tidak biasa antara lain upaya akses tidak sah, upaya peningkatan peran hak akses, perubahan konfigurasi yang mencurigakan dan upaya lain yang berpotensi menjadi serangan siber.	Ya/Parsial/Tidak
208	Melakukan analisis hasil pemantauan untuk kerentanan siber dan potensi serangan siber dengan memperhatikan integrasi informasi dari internal dan eksternal penyelenggara.	Ya/Parsial/Tidak
209	Mengintegrasikan *cyber threat intelligence* untuk analisis kerentanan siber dan potensi serangan siber.	Ya/Parsial/Tidak
210	Melakukan *sharing informasi* hasil analisis kerentanan siber dan potensi serangan siber pada sarana pertukaran informasi yang dibentuk Bank Indonesia atau sarana informasi lain.	Ya/Parsial/Tidak
	FAKTOR: ANALISIS SERANGAN SIBER	
211	Melakukan analisis serangan siber meliputi sumber serangan meliputi asal serangan (internal dan/atau eksternal), profil *threat actor* (individu, kelompok, dan/atau, negara), dan *Indicator of Compromise* (IOC).	Ya/Parsial/Tidak
212	Melakukan analisis serangan siber meliputi sumber serangan meliputi jenis serangan siber.	Ya/Parsial/Tidak
213	Melakukan analisis serangan siber meliputi sumber serangan meliputi waktu terjadinya serangan siber dan korelasi serangan siber dengan kejadian keamanan siber (*security event*) lain.	Ya/Parsial/Tidak
214	Melakukan analisis aktivitas *fraud* pada tingkat akun, aktivitas jaringan, dan transaksi.	Ya/Parsial/Tidak
215	Memiliki *fraud detection system* untuk analisis aktivitas *fraud*.	Ya/Parsial/Tidak
216	Memiliki *Security Information and Events Management* (SIEM) untuk mengkorelasikan catatan aktivitas siber dari seluruh sistem aplikasi dan infrastruktur teknologi informasi.	Ya/Parsial/Tidak

NO	INDIKATOR	NILAI
217	Terdapat prosedur eskalasi terhadap hasil deteksi apabila terdapat potensi terjadinya insiden siber.	Ya/Parsial/Tidak
FAKTOR: ANALISIS KODE JAHAT ATAU KODE TIDAK SAH		
218	Melakukan analisis kode jahat atau kode tidak sah yang berpotensi menimbulkan serangan siber meliputi klasifikasi kode jahat atau kode tidak sah berdasarkan tingkat risiko siber untuk memastikan penanganan yang sesuai dengan tingkat ancaman.	Ya/Parsial/Tidak
219	Melakukan analisis kode jahat atau kode tidak sah dalam lingkungan yang aman dan terisolasi untuk memahami karakteristik, tujuan, dan potensi dampak kode jahat atau kode tidak sah tanpa risiko penyebaran lebih lanjut.	Ya/Parsial/Tidak
220	Melakukan analisis kode jahat atau kode tidak sah yang berpotensi menimbulkan serangan siber meliputi pemindaian sistem aplikasi dan/atau infrastruktur teknologi informasi yang terdampak.	Ya/Parsial/Tidak
221	Melakukan analisis kode jahat atau kode tidak sah yang berpotensi menimbulkan serangan siber meliputi memastikan kode yang dieksekusi pada sistem aplikasi dan/atau infrastruktur teknologi informasi telah dilakukan otorisasi dan tidak disusupi.	Ya/Parsial/Tidak
222	Terdapat prosedur eskalasi tindak lanjut untuk memitigasi atau meminimalisir dampak dari kode jahat atau kode tidak sah yang terdeteksi.	Ya/Parsial/Tidak
223	Melakukan evaluasi deteksi kode jahat atau kode tidak sah untuk perbaikan sistem deteksi dan implementasi kontrol untuk mencegah eksekusi dari kode jahat atau kode tidak sah.	Ya/Parsial/Tidak
FAKTOR: PEMELIHARAAN DAN PENGUJIAN SISTEM DETEKSI		
224	Sistem pemantauan terpelihara dengan versi perangkat lunak terkini dan telah teruji sesuai standar yang berlaku di penyelenggara.	Ya/Parsial/Tidak
225	Pemeliharaan dan pengujian sistem deteksi dilakukan paling sedikit 1 kali dalam 1 tahun.	Ya/Parsial/Tidak
226	Keandalan sistem pemantauan dilakukan penilaian meliputi aspek akurasi sistem deteksi, kemampuan sistem deteksi dalam merespons ancaman siber dan serangan siber serta kemampuan sistem deteksi dalam memberikan notifikasi secara cepat.	Ya/Parsial/Tidak
227	Sistem pemantauan terkoneksi dengan *tools* manajemen insiden.	Ya/Parsial/Tidak

NO	INDIKATOR	NILAI
AREA: PENANGANAN		
DIMENSI: RESPONS		
FAKTOR: PENYUSUNAN RENCANA PENANGANAN DAN PEMULIHAN INSIDEN SIBER		
228	Rencana penanganan insiden siber memuat penetapan status insiden siber berdasarkan kriteria penetapan insiden siber.	Ya/Parsial/Tidak
229	Rencana penanganan insiden siber memuat penentuan kategori insiden siber beserta level manajemen koordinator per kategori insiden siber dengan memperhatikan dampak dan prioritas penanganan insiden siber.	Ya/Parsial/Tidak
230	Rencana penanganan insiden siber memuat prosedur respons insiden siber dengan memperhatikan sasaran waktu pemulihan (*Recovery Time Objective* - RTO) dan sasaran titik pemulihan (*Recovery Point Objective* - RPO).	Ya/Parsial/Tidak
231	Rencana penanganan insiden siber memuat prosedur respons insiden siber untuk menghilangkan sumber insiden siber (*eradication*).	Ya/Parsial/Tidak
232	Rencana penanganan insiden siber memuat prosedur respons insiden siber untuk eskalasi setiap kategori insiden siber.	Ya/Parsial/Tidak
233	Rencana penanganan insiden siber memuat daftar personel internal dan pihak ketiga berikut peran, tanggung jawab, dan kontak yang dapat dihubungi dalam penanganan insiden siber.	Ya/Parsial/Tidak
234	Daftar personel internal dan pihak ketiga beserta kontak yang dapat dihubungi dilakukan verifikasi dan diperbarui berkala.	Ya/Parsial/Tidak
235	Rencana penanganan insiden siber memuat daftar sistem aplikasi termasuk aplikasi pendukung (*surrounding application*), infrastruktur TI, dan sumber daya lainnya yang diperlukan dalam penanganan Insiden Siber.	Ya/Parsial/Tidak
236	Rencana penanganan insiden siber memuat prosedur pembatasan dampak insiden siber di internal penyelenggara (*containment*).	Ya/Parsial/Tidak
237	Rencana penanganan insiden siber memuat prosedur koordinasi pembatasan dampak insiden siber dengan otoritas, lembaga, dan/atau penyelenggara lain.	Ya/Parsial/Tidak
238	Rencana pemulihan insiden siber memuat prosedur pemulihan untuk setiap kategori insiden siber dengan memperhatikan sasaran titik pemulihan (*Recovery Point Objective* - RPO).	Ya/Parsial/Tidak

NO	INDIKATOR	NILAI
239	Rencana pemulihan insiden siber memuat daftar personel pihak internal atau pihak ketiga berikut peran, tanggung jawab, dan kontak yang dapat dihubungi dalam pemulihan insiden siber.	Ya/Parsial/Tidak
240	Rencana pemulihan insiden siber memuat daftar sistem aplikasi termasuk aplikasi pendukung (*surrounding application*), infrastruktur TI, dan sumber daya yang diperlukan dalam pemulihan insiden siber.	Ya/Parsial/Tidak
241	Rencana penanganan dan pemulihan insiden siber menjadi bagian dari rencana keberlangsungan bisnis penyelenggara.	Ya/Parsial/Tidak
242	Rencana penanganan dan pemulihan insiden siber didistribusikan atau dapat diakses oleh seluruh pihak terkait.	Ya/Parsial/Tidak
243	Rencana penanganan dan pemulihan insiden siber paling sedikit meliputi *malware attacks*, *phishing and social engineering*, *Distributed Denial of Service* (DDoS), *data breach*, dan *insider threats*.	Ya/Parsial/Tidak
244	Penetapan rencana penanganan dan pemulihan insiden siber dilakukan secara formal dan ditetapkan oleh manajemen tertinggi.	Ya/Parsial/Tidak
245	Pelaksanaan evaluasi rencana penanganan dan pemulihan insiden siber dilakukan: a. secara berkala minimal sekali dalam setahun sesuai dengan perkembangan risiko siber; b. melibatkan manajemen tertinggi penyelenggara; dan c. hasil evaluasi rencana penanganan dan pemulihan insiden siber digunakan sebagai perbaikan rencana penanganan dan pemulihan insiden siber kedepan.	Ya/Parsial/Tidak
246	Memiliki struktur Tim Tanggap Insiden Siber (TTIS) level organisasi.	Ya/Parsial/Tidak
247	Memiliki kejelasan peran dan tanggung jawab TTIS level organisasi.	Ya/Parsial/Tidak
248	Memiliki kriteria pengaktifan TTIS.	Ya/Parsial/Tidak
249	Memiliki kecukupan kapasitas SDM untuk melakukan penanganan dan pemulihan insiden siber.	Ya/Parsial/Tidak
250	Memiliki kecukupan kapabilitas SDM untuk melakukan penanganan dan pemulihan insiden siber.	Ya/Parsial/Tidak
251	TTIS melibatkan personel lintas departemen, unit kerja, dan bagian yang paling sedikit meliputi fungsi manajemen KKS, manajemen risiko, hukum, dan komunikasi.	Ya/Parsial/Tidak

NO	INDIKATOR	NILAI
252	Struktur dan susunan keanggotaan TTIS dilaporkan kepada di Bank Indonesia untuk koordinasi penanganan dan pemulihan insiden siber.	Ya/Parsial/Tidak
253	TTIS level organisasi bertanggung jawab kepada manajemen tertinggi.	Ya/Parsial/Tidak
	FAKTOR: PELAKSANAAN SIMULASI & UJICOBA PENANGANAN DAN PEMULIHAN INSIDEN SIBER	
254	Simulasi dan uji coba penanganan dan pemulihan Insiden siber dilakukan dengan mengacu pada profil risiko siber dan kritikalitas fungsi bisnis dan sistem informasi.	Ya/Parsial/Tidak
255	Terdapat skenario simulasi dan uji coba yang disusun berdasarkan hasil identifikasi kerentanan dan ancaman siber.	Ya/Parsial/Tidak
256	Skenario simulasi dan uji coba penanganan serta pemulihan insiden siber mencakup deteksi ancaman siber, eskalasi insiden siber, koordinasi antar tim, eskalasi, respons teknis, komunikasi dengan pemangku kepentingan, serta pemulihan layanan hingga evaluasi pasca-insiden.	Ya/Parsial/Tidak
257	Skenario simulasi dan uji coba penanganan serta pemulihan insiden siber mencakup skenario serangan dari dalam dan luar organisasi Penyelenggara antara lain serangan *malware*, DDoS, *phishing* atau *social engineering*, kegagalan sistem aplikasi dan/atau infrastruktur teknologi informasi, dan *insider threat*.	Ya/Parsial/Tidak
258	*Backup* data diuji secara berkala untuk memastikan integritas dan ketersediaannya dalam proses pemulihan.	Ya/Parsial/Tidak
259	Pelaksanaan simulasi dan uji coba harus dipastikan kelancaran operasional dan/atau layanan bisnis tetap terjaga, dengan adanya *environment testing*.	Ya/Parsial/Tidak
260	Pelaksanaan simulasi dan uji coba tidak berdampak terhadap terganggunya kelancaran operasional dan/atau layanan bisnis.	Ya/Parsial/Tidak
261	Simulasi dan uji coba penanganan dan pemulihan insiden siber dilakukan dengan melibatkan pemangku kepentingan terkait dan/atau pihak ketiga.	Ya/Parsial/Tidak
262	Berkontribusi aktif dalam simulasi dan uji coba penanganan dan pemulihan insiden siber yang diselenggarakan oleh otoritas sektor keuangan.	Ya/Parsial/Tidak
263	Hasil simulasi dan uji coba dilaporkan kepada manajemen tertinggi.	Ya/Parsial/Tidak

NO	INDIKATOR	NILAI
264	Hasil simulasi dan uji coba penanganan dan pemulihan insiden siber dijadikan umpan balik dalam proses peningkatan penanganan dan pemulihan insiden siber.	Ya/Parsial/Tidak
	FAKTOR: EVALUASI PENANGANAN	
265	Evaluasi penanganan dilakukan paling sedikit 1 kali dalam 1 tahun.	Ya/Parsial/Tidak
266	Evaluasi penanganan dilakukan dengan memperhatikan profil risiko siber,tren perkembangan siber, hasil respons insiden siber, dan/atau hasil pemulihan insiden siber.	Ya/Parsial/Tidak
267	Hasil evaluasi penanganan disampaikan kepada manajemen tertinggi penyelenggara.	Ya/Parsial/Tidak

LAMPIRAN 3.3
Format Laporan Tingkat Kematangan KKS bagi Penyelenggara dengan Kewajiban Pelaporan Sebagian dan Pernah Mengalami Insiden Siber

A. Informasi Pelapor

1. Nama Penyelenggara : .....
2. Alamat Kantor Pusat Penyelenggara : .....
3. Nomor Telepon : .....
4. Nama Narahubung : .....
5. Nomor Telepon Narahubung : .....
6. Tanggal Penyampaian Laporan : .../..../.....(dd/mm/yyyy)
7. Periode Pelaporan : ..... (yyyy)

B. Hasil Asemen Mandiri Indikator Tingkat Kematangan KKS bagi Penyelenggara dengan Kewajiban Pelaporan Sebagian dan Pernah Mengalami Insiden Siber

NO	INDIKATOR	NILAI
AREA: TATA KELOLA		
DIMENSI: STRATEGI DAN KEBIJAKAN KKS		
FAKTOR: KEBIJAKAN STANDAR DAN PROSEDUR KKS		
1	Kebijakan pengamanan KKS paling sedikit terdiri atas pengamanan data, sistem aplikasi, infrastruktur teknologi informasi, pihak ketiga, serta pelindungan konsumen dan manajemen *fraud*.	Ya/Parsial/Tidak
2	Standar pengamanan KKS paling sedikit terdiri atas pengamanan data, sistem aplikasi, infrastruktur teknologi informasi, pihak ketiga, serta pelindungan konsumen dan manajemen *fraud*.	Ya/Parsial/Tidak
3	Prosedur pengamanan KKS paling sedikit terdiri atas pengamanan data, sistem aplikasi, infrastruktur teknologi informasi, pihak ketiga, serta pelindungan konsumen dan manajemen *fraud*.	Ya/Parsial/Tidak
4	Penetapan Kebijakan KKS dilakukan secara formal dan ditetapkan oleh manajemen tertinggi.	Ya/Parsial/Tidak
5	Kebijakan, standar, dan prosedur KKS sudah diterapkan dan dikomunikasikan: a. kepada seluruh pihak internal dan/atau pihak ketiga yang terkait ketika pertama kali bekerja; b. secara tahunan; dan c. jika terdapat perubahan.	Ya/Parsial/Tidak
FAKTOR: FUNGSI ORGANISASI KKS		
6	Penerapan manajemen KKS meliputi perencanaan strategis KKS, penyusunan kebijakan, standar, dan prosedur KKS, penerapan budaya KKS, serta pelaksanaan pencegahan dan penanganan KKS.	Ya/Parsial/Tidak
7	Audit KKS dilakukan minimal 1 kali dalam 1 tahun.	Ya/Parsial/Tidak

NO	INDIKATOR	NILAI
8	Audit KKS mencakup tata kelola, pencegahan, dan penanganan	Ya/Parsial/Tidak
DIMENSI: BUDAYA KKS		
9	Program peningkatan budaya KKS berupa *awareness* diberikan secara berkala sesuai dengan kewenangan dan tanggung jawab personel internal.	Ya/Parsial/Tidak
AREA: PENCEGAHAN		
DIMENSI: IDENTIFIKASI		
FAKTOR: PENYUSUNAN PROFIL RISIKO SIBER		
10	Identifikasi risiko siber dilakukan dengan memperhatikan kerentanan dan ancaman siber dari aspek manusia dengan memantau perkembangan siber terkini yang bersumber dari internal dan eksternal, antara lain ketidakcukupan kapasitas dan kapabilitas SDM.	Ya/Parsial/Tidak
11	Identifikasi risiko siber dilakukan dengan memperhatikan kerentanan dan ancaman siber dari aspek proses dengan memantau perkembangan siber terkini yang bersumber dari internal dan eksternal, antara lain ketidakcukupan kebijakan, standar, dan prosedur KKS.	Ya/Parsial/Tidak
12	Identifikasi risiko siber dilakukan dengan memperhatikan kerentanan dan ancaman siber dari aspek teknologi dengan memantau perkembangan siber terkini yang bersumber dari internal dan eksternal, antara lain *vulnerability* teknologi baru.	Ya/Parsial/Tidak
13	Identifikasi risiko siber dilakukan dengan memperhatikan objek yang akan dilindungi meliputi data yang dikelola oleh penyelenggara.	Ya/Parsial/Tidak
14	Identifikasi risiko siber dilakukan dengan memperhatikan objek yang akan dilindungi meliputi sistem aplikasi dan konfigurasinya yang dikelola oleh penyelenggara.	Ya/Parsial/Tidak
15	Identifikasi risiko siber dilakukan dengan memperhatikan objek yang akan dilindungi meliputi infrastruktur teknologi informasi dan konfigurasinya yang dikelola oleh penyelenggara.	Ya/Parsial/Tidak
16	Memiliki konfigurasi keterhubungan antar objek yang dilindungi yang tersimpan dalam *configuration management system*.	Ya/Parsial/Tidak
17	Hasil identifikasi kerentanan siber dan ancaman siber didokumentasikan pada inventaris risiko siber (*cyber risk register*) pada level fungsi manajemen KKS.	Ya/Parsial/Tidak

NO	INDIKATOR	NILAI
18	Hasil identifikasi kerentanan siber dan ancaman siber didokumentasikan pada inventaris risiko siber (*cyber risk register*) pada level *enterprise risk management.*	Ya/Parsial/Tidak
	FAKTOR: PENGINIAN PROFIL RISIKO SIBER	
19	Profil risiko siber dievaluasi dan dikinikan paling sedikit 1 kali dalam 1 tahun.	Ya/Parsial/Tidak
DIMENSI: PROTEKSI		
	FAKTOR: PEMBANGUNAN SISTEM PERTAHANAN	
20	Keamanan pihak internal dan pihak ketiga dipastikan dengan melakukan verifikasi latar belakang pihak internal dan/atau pihak ketiga yang akan dipekerjakan.	Ya/Parsial/Tidak
21	Verifikasi latar belakang dilakukan dengan memperhatikan ketentuan organisasi terkini, klasifikasi informasi yang diakses, dan risiko yang dihadapi.	Ya/Parsial/Tidak
22	Mewajibkan personel pihak internal dan/atau pihak ketiga telah menandatangani perjanjian atau surat pernyataan untuk menjaga kerahasiaan data dan/atau informasi dari pihak yang tidak berwenang.	Ya/Parsial/Tidak
23	Persyaratan perjanjian kerahasiaan dan *Non-Disclosure Agreement* (NDA) ditinjau secara berkala dan ketika terjadi perubahan yang mempengaruhi persyaratan ini.	Ya/Parsial/Tidak
24	Terdapat mekanisme sanksi terhadap pelanggaran kebijakan KKS.	Ya/Parsial/Tidak
25	Menerapkan manajemen akses antara lain standar penggunaan *password* yang meliputi kompleksitas *password*, limit upaya percobaan penggunaan *password*, dan penggantian *default password*.	Ya/Parsial/Tidak
26	Semua *password* dan akun *default* telah diubah sebelum implementasi sistem aplikasi dan infrastruktur teknologi informasi.	Ya/Parsial/Tidak
27	*User access matrix* dan daftar akses pengguna dievaluasi secara berkala (contoh: ketika ada pergantian peran atau personel yang keluar dari organisasi).	Ya/Parsial/Tidak
28	Menerapkan kontrol keamanan fisik berlapis antara lain personel *security*, CCTV, dan sistem alarm.	Ya/Parsial/Tidak
29	Memiliki prosedur pengawalan tamu, vendor, dan pihak ketiga lainnya di area kritikal antara lain ruang operator dan *data center*.	Ya/Parsial/Tidak
30	*User access review* dilakukan secara berkala untuk setiap sistem aplikasi dan infrastruktur teknologi informasi.	Ya/Parsial/Tidak

NO	INDIKATOR	NILAI
31	Melakukan perencanaan dan *due diligence* untuk mengurangi risiko sebelum melakukan kerja sama dengan pihak ketiga.	Ya/Parsial/Tidak
32	Terdapat persyaratan keamanan siber untuk setiap kontrak/perjanjian antara Penyelenggara dengan pihak ketiga, termasuk menjaga kerahasiaan informasi.	Ya/Parsial/Tidak
33	Akses ke sistem menggunakan *single factor authentication* antara lain *Personal Identification Number* (PIN) atau *password*.	Ya/Parsial/Tidak
	FAKTOR: PENGAMANAN DATA DAN/ATAU INFORMASI	
34	Pengamanan dan pelindungan data dan/atau informasi dilakukan sesuai dengan ketentuan mengenai pelindungan data pribadi.	Ya/Parsial/Tidak
DIMENSI: DETEKSI		
	FAKTOR: PEMANTAUAN	
35	Sistem dilengkapi oleh sistem *alarm*, kamera pemantau (CCTV) dan petugas keamanan pada area dan/atau objek kritikal atau vital.	Ya/Parsial/Tidak
36	Seluruh *log* / rekaman akses logis dan fisik disimpan dan di*backup* dengan memperhatikan masa retensi.	Ya/Parsial/Tidak
37	*Log* / rekaman akses logis dan fisik dilakukan review secara berkala.	Ya/Parsial/Tidak
38	Perubahan terhadap akses logis dan fisik dilakukan dengan prinsip *segregation of duties* dan dikelola melalui prosedur manajemen perubahan.	Ya/Parsial/Tidak
39	Pemindaian kerentanan siber dilakukan pada setiap sistem aplikasi, infrastruktur teknologi informasi, dan data secara bergiliran dan terjadwal mengacu pada profil risiko siber.	Ya/Parsial/Tidak
40	Pemindaian kerentanan siber dilakukan dan dianalisis sebelum dilakukan *deployment* atau *re-deployment* terhadap terhadap sistem aplikasi dan/atau infrastruktur teknologi informasi baru atau eksisting.	Ya/Parsial/Tidak
	FAKTOR: PEMELIHARAAN DAN PENGUJIAN SISTEM DETEKSI	
41	Sistem pemantauan terpelihara dengan versi perangkat lunak terkini dan telah teruji sesuai standar yang berlaku di penyelenggara.	Ya/Parsial/Tidak
AREA: PENANGANAN		
DIMENSI: RESPONS		
	FAKTOR: PENYUSUNAN RENCANA PENANGANAN DAN PEMULIHAN INSIDEN SIBER	
42	Rencana penanganan insiden siber memuat penetapan status insiden siber berdasarkan kriteria penetapan insiden siber.	Ya/Parsial/Tidak

NO	INDIKATOR	NILAI
43	Daftar personel internal dan pihak ketiga beserta kontak yang dapat dihubungi dilakukan verifikasi dan diperbarui berkala.	Ya/Parsial/Tidak
	FAKTOR: PENANGANAN INSIDEN SIBER	
44	Insiden siber ditetapkan berdasarkan kriteria penetapan insiden siber dan dikategorisasikan berdasarkan rencana penanganan insiden siber.	Ya/Parsial/Tidak
45	Pencatatan insiden siber dilakukan menggunakan *tools* antara lain *ticketing tools* untuk memudahkan manajemen insiden, termasuk melihat progress penanganan dan pemulihan, PIC yang sedang menangani, dan automasi notifikasi informasi dan status penanganan insiden siber.	Ya/Parsial/Tidak
46	Penyampaian notifikasi awal untuk setiap insiden siber kepada Bank Indonesia dilakukan paling lama 1 (satu) jam setelah insiden siber diketahui oleh Penyelenggara.	Ya/Parsial/Tidak
47	Penyampaian laporan insiden siber untuk setiap insiden siber kepada Bank Indonesia dilakukan paling lama 3 (tiga) hari kalender setelah insiden siber terjadi.	Ya/Parsial/Tidak
48	Mitigasi insiden siber dilakukan dengan memastikan sumber insiden siber telah dihilangkan (*eradication*) menggunakan *tools*.	Ya/Parsial/Tidak
49	Mitigasi insiden siber dilakukan dengan melakukan isolasi dampak insiden siber (*containment*).	Ya/Parsial/Tidak
50	Dalam hal penyelenggara melaksanakan penanganan insiden menggunakan sumber daya eskternal, penyelenggara memiliki perjanjian atau kontrak dengan pihak ketiga untuk mendukung penanganan insiden siber.	Ya/Parsial/Tidak
51	Perjanjian atau kontrak dengan pihak ketiga mencakup kerahasiaan data dan/atau informasi oleh pihak ketiga serta *service level agreement* terkait penanganan insiden siber.	Ya/Parsial/Tidak
DIMENSI: PEMULIHAN		
	FAKTOR: PERBAIKAN BERKELANJUTAN	
52	Evaluasi efektivitas dan perbaikan rencana penanganan dan pemulihan insiden siber dilakukan atas dasar penanganan dan pemulihan insiden siber yang telah dilakukan.	Ya/Parsial/Tidak

LAMPIRAN 3.4
Format Laporan Tingkat Kematangan KKS bagi Penyelenggara dengan Kewajiban Pelaporan Sebagian dan Belum Pernah Mengalami Insiden Siber

A. Informasi Pelapor

1. Nama Penyelenggara : .....
2. Alamat Kantor Pusat Penyelenggara : .....
3. Nomor Telepon : .....
4. Nama Narahubung : .....
5. Nomor Telepon Narahubung : .....
6. Tanggal Penyampaian Laporan : .../..../.....(dd/mm/yyyy)
7. Periode Pelaporan : ..... (yyyy)

B. Hasil Asemen Mandiri Indikator Tingkat Kematangan KKS bagi Penyelenggara dengan Kewajiban Pelaporan Sebagian dan Belum Pernah Mengalami Insiden Siber

NO	INDIKATOR	NILAI
AREA: TATA KELOLA		
DIMENSI: STRATEGI DAN KEBIJAKAN KKS		
FAKTOR: KEBIJAKAN STANDAR DAN PROSEDUR KKS		
1	Kebijakan pengamanan KKS paling sedikit terdiri atas pengamanan data, sistem aplikasi, infrastruktur teknologi informasi, pihak ketiga, serta pelindungan konsumen dan manajemen *fraud*.	Ya/Parsial/Tidak
2	Standar pengamanan KKS paling sedikit terdiri atas pengamanan data, sistem aplikasi, infrastruktur teknologi informasi, pihak ketiga, serta pelindungan konsumen dan manajemen *fraud*.	Ya/Parsial/Tidak
3	Prosedur pengamanan KKS paling sedikit terdiri atas pengamanan data, sistem aplikasi, infrastruktur teknologi informasi, pihak ketiga, serta pelindungan konsumen dan manajemen *fraud*.	Ya/Parsial/Tidak
4	Penetapan Kebijakan KKS dilakukan secara formal dan ditetapkan oleh manajemen tertinggi.	Ya/Parsial/Tidak
5	Kebijakan, standar, dan prosedur KKS sudah diterapkan dan dikomunikasikan: a. kepada seluruh pihak internal dan/atau pihak ketiga yang terkait ketika pertama kali bekerja; b. secara tahunan; dan c. jika terdapat perubahan.	Ya/Parsial/Tidak
FAKTOR: FUNGSI ORGANISASI KKS		
6	Penerapan manajemen KKS meliputi perencanaan strategis KKS, penyusunan kebijakan, standar, dan prosedur KKS, penerapan budaya KKS, serta pelaksanaan pencegahan dan penanganan KKS.	Ya/Parsial/Tidak

NO	INDIKATOR	NILAI
7	Audit KKS dilakukan minimal 1 kali dalam 1 tahun.	Ya/Parsial/Tidak
8	Audit KKS mencakup tata kelola, pencegahan, dan penanganan	Ya/Parsial/Tidak
DIMENSI: BUDAYA KKS		
9	Program peningkatan budaya KKS berupa *awareness* diberikan secara berkala sesuai dengan kewenangan dan tanggung jawab personel internal.	Ya/Parsial/Tidak
AREA: PENCEGAHAN		
DIMENSI: IDENTIFIKASI		
FAKTOR: PENYUSUNAN PROFIL RISIKO SIBER		
10	Identifikasi risiko siber dilakukan dengan memperhatikan kerentanan dan ancaman siber dari aspek manusia dengan memantau perkembangan siber terkini yang bersumber dari internal dan eksternal, antara lain ketidakcukupan kapasitas dan kapabilitas SDM.	Ya/Parsial/Tidak
11	Identifikasi risiko siber dilakukan dengan memperhatikan kerentanan dan ancaman siber dari aspek proses dengan memantau perkembangan siber terkini yang bersumber dari internal dan eksternal, antara lain ketidakcukupan kebijakan, standar, dan prosedur KKS.	Ya/Parsial/Tidak
12	Identifikasi risiko siber dilakukan dengan memperhatikan kerentanan dan ancaman siber dari aspek teknologi dengan memantau perkembangan siber terkini yang bersumber dari internal dan eksternal, antara lain *vulnerability* teknologi baru.	Ya/Parsial/Tidak
13	Identifikasi risiko siber dilakukan dengan memperhatikan objek yang akan dilindungi meliputi data yang dikelola oleh penyelenggara.	Ya/Parsial/Tidak
14	Identifikasi risiko siber dilakukan dengan memperhatikan objek yang akan dilindungi meliputi sistem aplikasi dan konfigurasinya yang dikelola oleh penyelenggara.	Ya/Parsial/Tidak
15	Identifikasi risiko siber dilakukan dengan memperhatikan objek yang akan dilindungi meliputi infrastruktur teknologi informasi dan konfigurasinya yang dikelola oleh penyelenggara.	Ya/Parsial/Tidak
16	Memiliki konfigurasi keterhubungan antar objek yang dilindungi yang tersimpan dalam *configuration management system*.	Ya/Parsial/Tidak
17	Hasil identifikasi kerentanan siber dan ancaman siber didokumentasikan pada inventaris risiko siber (*cyber risk register*) pada level fungsi manajemen KKS.	Ya/Parsial/Tidak

NO	INDIKATOR	NILAI
18	Hasil identifikasi kerentanan siber dan ancaman siber didokumentasikan pada inventaris risiko siber (*cyber risk register*) pada level *enterprise risk management.*	Ya/Parsial/Tidak
	FAKTOR: PENGINIAN PROFIL RISIKO SIBER	
19	Profil risiko siber dievaluasi dan dikinikan paling sedikit 1 kali dalam 1 tahun.	Ya/Parsial/Tidak
DIMENSI: PROTEKSI		
	FAKTOR: PEMBANGUNAN SISTEM PERTAHANAN	
20	Keamanan pihak internal dan pihak ketiga dipastikan dengan melakukan verifikasi latar belakang pihak internal dan/atau pihak ketiga yang akan dipekerjakan.	Ya/Parsial/Tidak
21	Verifikasi latar belakang dilakukan dengan memperhatikan ketentuan organisasi terkini, klasifikasi informasi yang diakses, dan risiko yang dihadapi.	Ya/Parsial/Tidak
22	Mewajibkan personel pihak internal dan/atau pihak ketiga telah menandatangani perjanjian atau surat pernyataan untuk menjaga kerahasiaan data dan/atau informasi dari pihak yang tidak berwenang.	Ya/Parsial/Tidak
23	Persyaratan perjanjian kerahasiaan dan *Non-Disclosure Agreement* (NDA) ditinjau secara berkala dan ketika terjadi perubahan yang mempengaruhi persyaratan ini.	Ya/Parsial/Tidak
24	Terdapat mekanisme sanksi terhadap pelanggaran kebijakan KKS.	Ya/Parsial/Tidak
25	Menerapkan manajemen akses antara lain standar penggunaan *password* yang meliputi kompleksitas *password*, limit upaya percobaan penggunaan *password*, dan penggantian *default password*.	Ya/Parsial/Tidak
26	Semua *password* dan akun *default* telah diubah sebelum implementasi sistem aplikasi dan infrastruktur teknologi informasi.	Ya/Parsial/Tidak
27	*User access matrix* dan daftar akses pengguna dievaluasi secara berkala (contoh: ketika ada pergantian peran atau personel yang keluar dari organisasi).	Ya/Parsial/Tidak
28	Menerapkan kontrol keamanan fisik berlapis antara lain personel *security*, CCTV, dan sistem alarm.	Ya/Parsial/Tidak
29	Memiliki prosedur pengawalan tamu, vendor, dan pihak ketiga lainnya di area kritikal antara lain ruang operator dan *data center*.	Ya/Parsial/Tidak
30	*User access review* dilakukan secara berkala untuk setiap sistem aplikasi dan infrastruktur teknologi informasi.	Ya/Parsial/Tidak

NO	INDIKATOR	NILAI
31	Melakukan perencanaan dan *due diligence* untuk mengurangi risiko sebelum melakukan kerja sama dengan pihak ketiga.	Ya/Parsial/Tidak
32	Terdapat persyaratan keamanan siber untuk setiap kontrak/perjanjian antara Penyelenggara dengan pihak ketiga, termasuk menjaga kerahasiaan informasi.	Ya/Parsial/Tidak
33	Akses ke sistem menggunakan *single factor authentication* antara lain *Personal Identification Number* (PIN) atau *password*.	Ya/Parsial/Tidak
	FAKTOR: PENGAMANAN DATA DAN/ATAU INFORMASI	
34	Pengamanan dan pelindungan data dan/atau informasi dilakukan sesuai dengan ketentuan mengenai pelindungan data pribadi.	Ya/Parsial/Tidak
	DIMENSI: DETEKSI	
	FAKTOR: PEMANTAUAN	
35	Sistem dilengkapi oleh sistem *alarm*, kamera pemantau (CCTV) dan petugas keamanan pada area dan/atau objek kritikal atau vital.	Ya/Parsial/Tidak
36	Seluruh *log* / rekaman akses logis dan fisik disimpan dan di*backup* dengan memperhatikan masa retensi.	Ya/Parsial/Tidak
37	Log/rekaman akses logis dan fisik dilakukan review secara berkala.	Ya/Parsial/Tidak
38	Perubahan terhadap akses logis dan fisik dilakukan dengan prinsip *segregation of duties* dan dikelola melalui prosedur manajemen perubahan.	Ya/Parsial/Tidak
39	Pemindaian kerentanan siber dilakukan pada setiap sistem aplikasi, infrastruktur teknologi informasi, dan data secara bergiliran dan terjadwal mengacu pada profil risiko siber.	Ya/Parsial/Tidak
40	Pemindaian kerentanan siber dilakukan dan dianalisis sebelum dilakukan *deployment* atau *re-deployment* terhadap terhadap sistem aplikasi dan/atau infrastruktur teknologi informasi baru atau eksisting.	Ya/Parsial/Tidak
	FAKTOR: PEMELIHARAAN DAN PENGUJIAN SISTEM DETEKSI	
41	Sistem pemantauan terpelihara dengan versi perangkat lunak terkini dan telah teruji sesuai standar yang berlaku di penyelenggara.	Ya/Parsial/Tidak
AREA: PENANGANAN		
	DIMENSI: RESPONS	
	FAKTOR: PENYUSUNAN RENCANA PENANGANAN DAN PEMULIHAN INSIDEN SIBER	
42	Rencana penanganan insiden siber memuat penetapan status insiden siber berdasarkan kriteria penetapan insiden siber.	Ya/Parsial/Tidak

NO	INDIKATOR	NILAI
43	Daftar personel internal dan pihak ketiga beserta kontak yang dapat dihubungi dilakukan verifikasi dan diperbarui berkala.	Ya/Parsial/Tidak

LAMPIRAN 4
Format Laporan Hasil Identifikasi Infrastruktur Informasi Vital (IIV)

A. Informasi Pelapor

1. Nama Penyelenggara : .....
2. Alamat Kantor Pusat Penyelenggara : .....
3. Nomor Telepon : .....
4. Nama Narahubung : .....
5. Nomor Telepon Narahubung : .....
6. Tanggal Penyampaian Laporan : .../..../.....(dd/mm/yyyy)
7. Periode Pelaporan : ..... (yyyy)

B. Hasil Asemen Mandiri Infrastruktur Informasi Vital (IIV)

NO	DAFTAR INFRASTRUKTUR INFORMASI VITAL (IIV)	
1	**Nama Sistem Aplikasi**	Nama sistem aplikasi yang merupakan hasil identifikasi termasuk kategori IIV.
	Layanan Sistem Aplikasi	Daftar layanan yang didukung oleh Sistem Aplikasi.
	Kategori Sistem Aplikasi	Diisi dengan Kategori Sistem Elektronik: Strategis, Tinggi, atau Rendah, sesuai dengan Peraturan Badan Siber Dan Sandi Negara Nomor 7 Tahun 2023 tentang Identifikasi Infrastruktur Informasi Vital. Strategis / Tinggi
	Tingkat Vitalitas Sistem Aplikasi	Diisi dengan hasil pengukuran tingkat vitalisasi Sistem Elektorinik berdasarkan dampak, sesuai dengan skala dampak yang diatur dalam Lampiran dari Peraturan Badan Siber Dan Sandi Negara Nomor 7 Tahun 2023 tentang Identifikasi Infrastruktur Informasi Vital. Serius / Signifikan / Terbatas / Minor.
	Infrastruktur Pendukung	Daftar Infrastruktur pendukung Sistem Aplikasi.
	Ukuran	Tingkat eksposur Penyelenggara yang diukur berdasarkan frekuensi, volume transaksi, dan jumlah pengguna Sistem Informasi. • Frekuensi: *realtime* atau *batch* (dilengkapi periode dan jumlah *batch* per hari). • Volume: rata-rata nominal transaksi dalam periode tertentu (hari, minggu, bulan, tahun) dalam rupiah. • Jumlah pengguna yang dibedakan antara pengguna internal, pelanggan, atau penyelenggaraan lain.
	Keterhubungan	Keterhubungan antar-Sistem Informasi yang dipergunakan dalam pelaksanaan kegiatan usaha Penyelenggara di Sistem Keuangan dan perekonomian nasional.
	Ketergantian	Ketersediaan Sistem Informasi alternatif yang dapat dipergunakan untuk bertransaksi.

NO	DAFTAR INFRASTRUKTUR INFORMASI VITAL (IIV)	
	Kompleksitas	Variasi dan ketergantungan komponen Sistem Informasi.

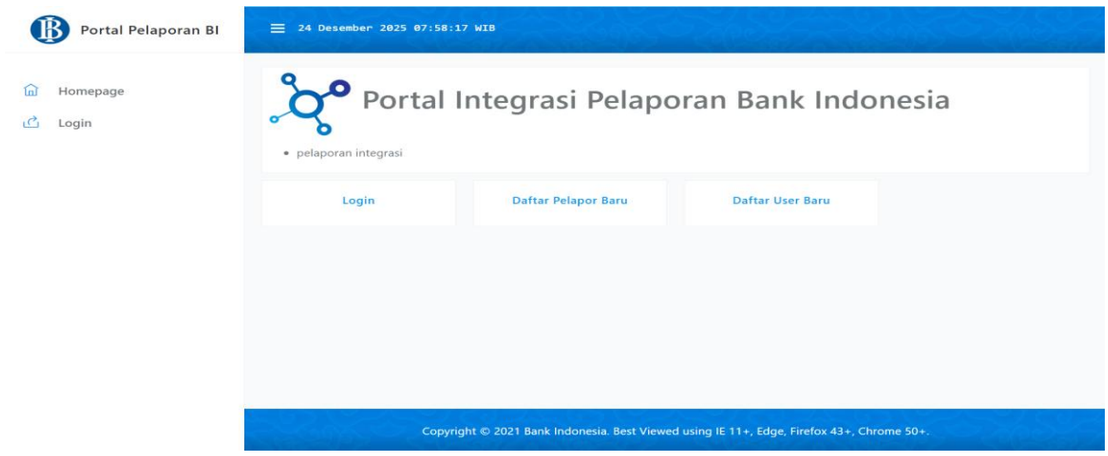
Contoh Pengisian:

NO	DAFTAR INFRASTRUKTUR INFORMASI VITAL (IIV)	
1	**Nama Sistem Aplikasi**	Core Banking System (CBS).
	Layanan Sistem Aplikasi	• ATM (Anjungan Tunai Mandiri). • Dana elektronik. • Transfer. • Internet banking.
	Kategori Sistem Aplikasi	Strategis.
	Tingkat Vitalitas Sistem Aplikasi	Serius.
	Infrastruktur Pendukung	• Mainframe. • Storage. • Sistem Back Up. • Jaringan (internet/ekstranet/intranet). • Data Center alternatif di Bandung. • *Disaster Recovery Center* (DRC) di Surabaya. • Lokasi kerja alternatif (*Business Resumption Site*) di beberapa lokasi yaitu Bandung dan Surabaya.
	Ukuran	• Frekuensi : *realtime*. • Volume Transaksi: 100 Miliar Rupiah per Hari. • Jumlah pengguna: 100 internal dan 2 Juta pelanggan.
	Keterhubungan	**Eksternal:** • Terkoneksi dengan Bank Indonesia: BI-FAST, BI-SKN RTGS. • Terkoneksi dengan penyelenggara lain: E-Wallet PT. ABC. **Internal:** • Terkoneksi dengan CRM. • Terkoneksi dengan ERP.
	Ketergantian	• Terdapat Sistem Backup di Data Center alternatif dengan konfigurasi aktif-aktif dengan lokasi di Bandung. • Terdapat Sistem Backup di DRC dengan lokasi di Surabaya. • Terdapat aplikasi pengganti yaitu Alternate Banking Systems (ABS).
	Kompleksitas	• Cloud/On premise, Micro Service, AWS, Windows X, VMWare/Hyper V/BladeRack. • Windows X, Microsoft EDR. • Account Enquiry, Jawa Oracle/SQL. • REST/SOAP. FTP/SFTP, TLS/HTTPS. • Firewall, Fortinet IDS, SNORT. • Messaging, Apache KAFKA, Websphere.

LAMPIRAN 5
Panduan Penggunaan Sistem Pelaporan KKS Bank Indonesia

1. Daftar Pelapor Baru

Untuk mendaftarkan pelapor baru pada sistem pelaporan KKS, *user* dapat mengakses *website* https://pelaporan.bi.go.id/, lalu klik tombol "Daftar Pelapor Baru" dan isi data detail pelapor yang akan didaftarkan.

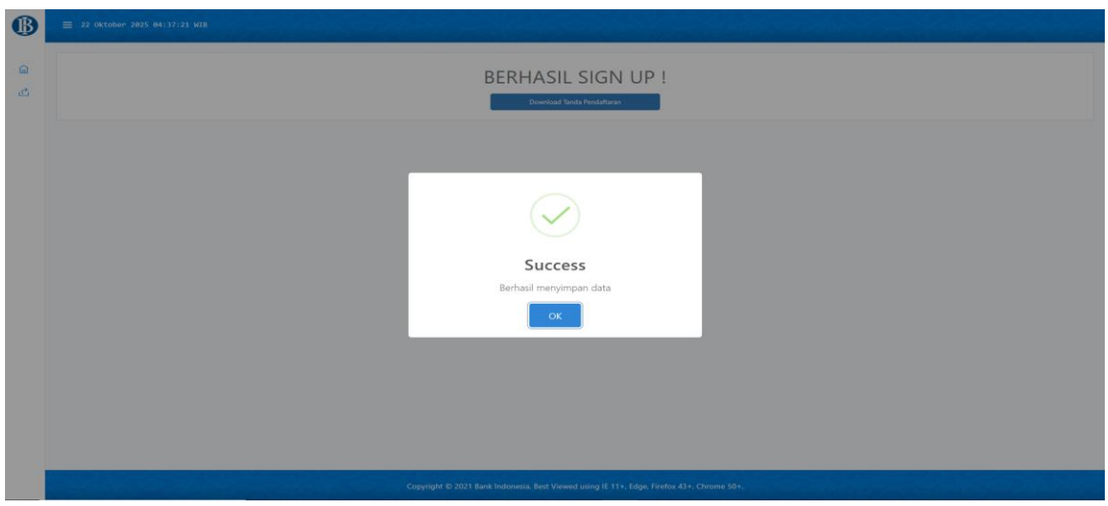


Gambar 1. Homepage Pelaporan.bi.go.id.

Isi detail data pelapor baru, klik tombol Simpan.

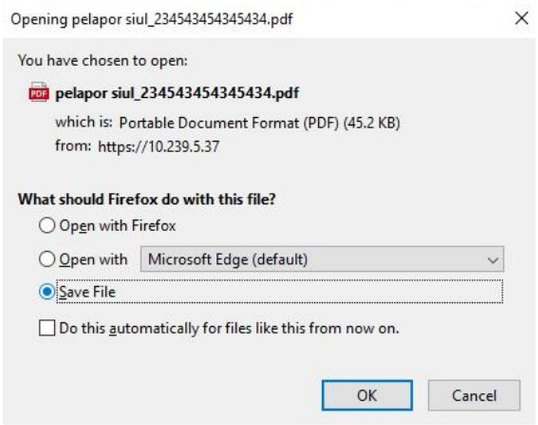
Gambar 2. Halaman Daftar Pelapor Baru.

Setelah klik simpan maka akan muncul notifikasi berhasil *sign up*, silahkan klik tombol *download* tanda pendaftaran.



Gambar 3. Pop up Berhasil Daftar Pelapor Baru.

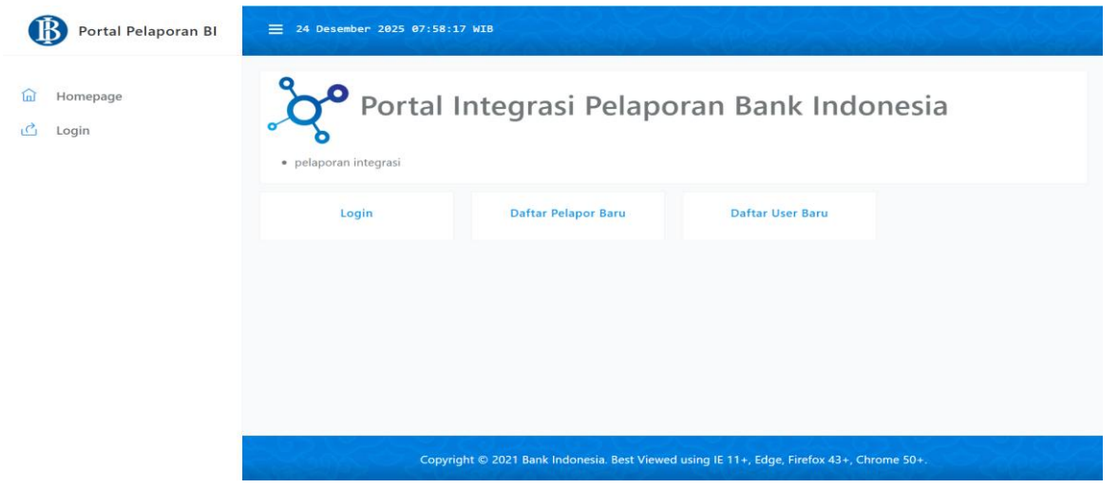
Maka bukti pendaftaran akan ter-*download* sesuai dengan pelapor yang sudah didaftarkan.



Gambar 4. Bukti Pendaftaran Pelapor Baru.

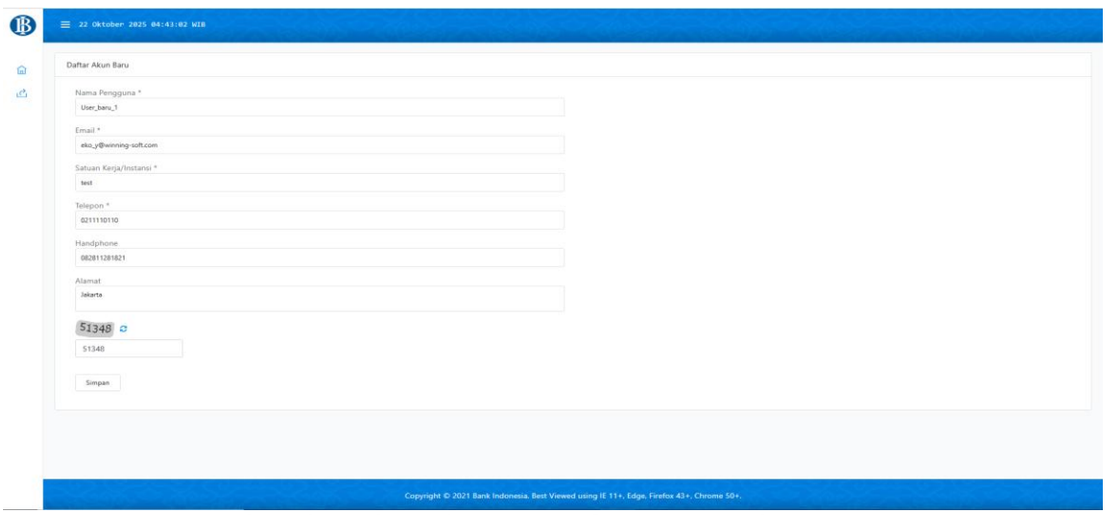
2. Daftar User Pelapor Baru

Untuk melakukan daftar *user* pelapor baru pada Sistem Pelaporan KKS, *user* dapat mengakses *website* https://pelaporan.bi.go.id/, lalu klik tombol "Daftar *User* Baru" dan isi data *user* lalu klik simpan.



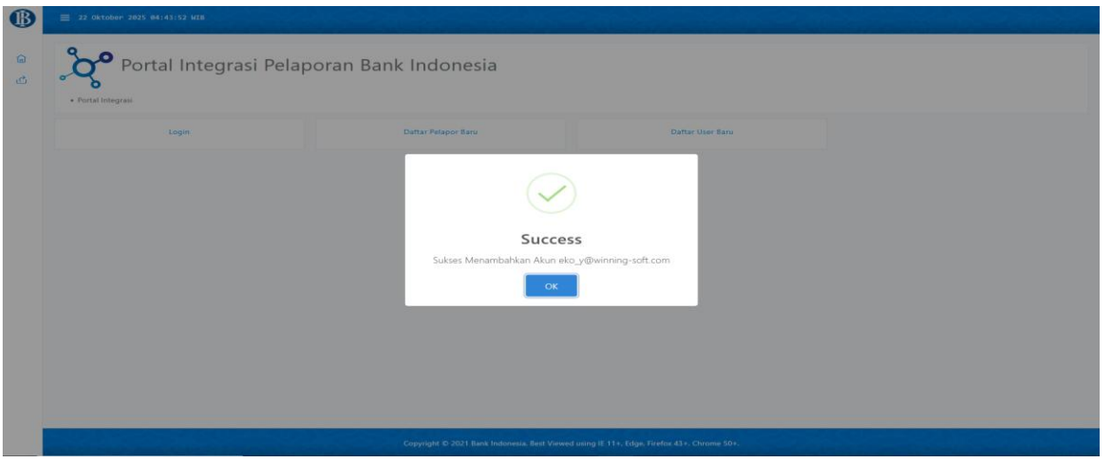
Gambar 5. Homepage Pelaporan.bi.go.id.

Isi detail data user baru, klik tombol simpan.



Gambar 6. Halaman Daftar User Pelapor Baru.

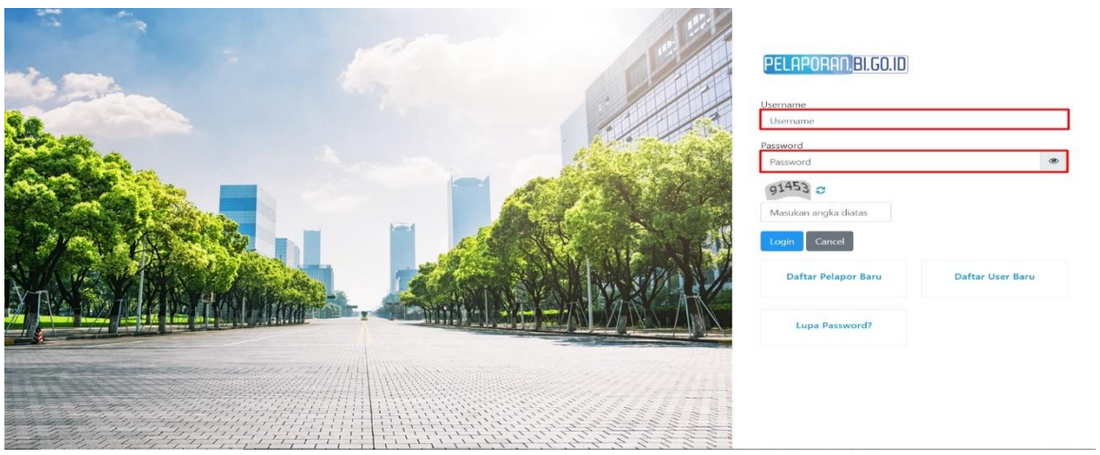
Jika muncul notifikasi sukses, maka *user* baru sudah berhasil didaftarkan. Silahkan menghubungi admin untuk melakukan konfigurasi selanjutnya seperti aktivasi *user*, akses sistem pelaporan dan lain-lain.



Gambar7. Pop up Berhasil Daftar User Pelapor Baru.

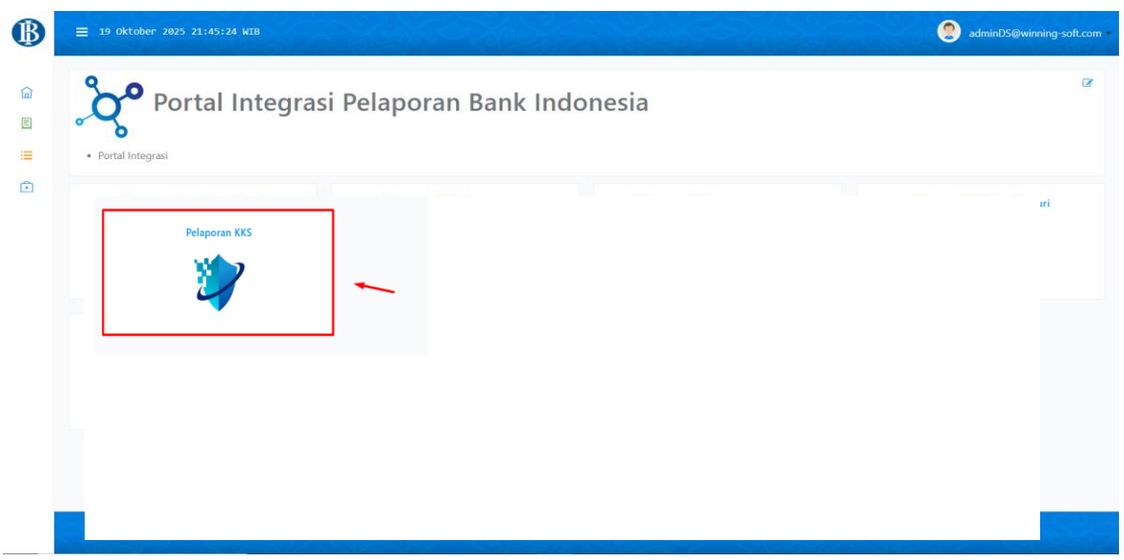
3. *Login*

Untuk melakukan *login* pada sistem pelaporan KKS, *user* dapat mengakses *website* https://pelaporan.bi.go.id/Account/Login lalu isi data *username* dan *password* yang sudah terdaftar.



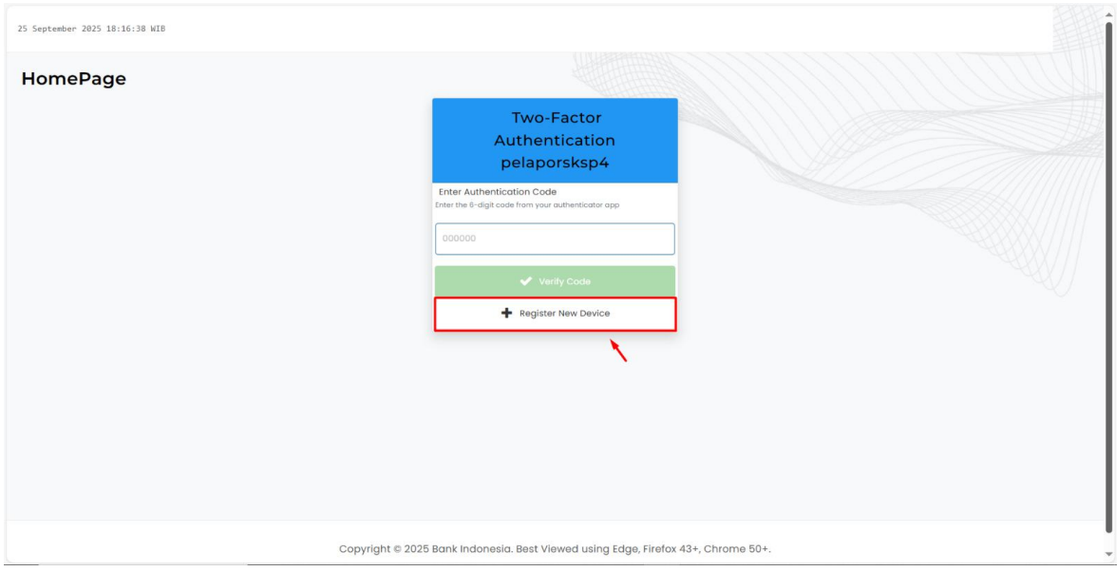
Gambar 8. Halaman Login Pelaporan.bi.go.id.

Input Captcha lalu klik tombol *Login* maka akan tampil halaman *homepage* sebagai berikut dan klik modul Pelaporan KKS.



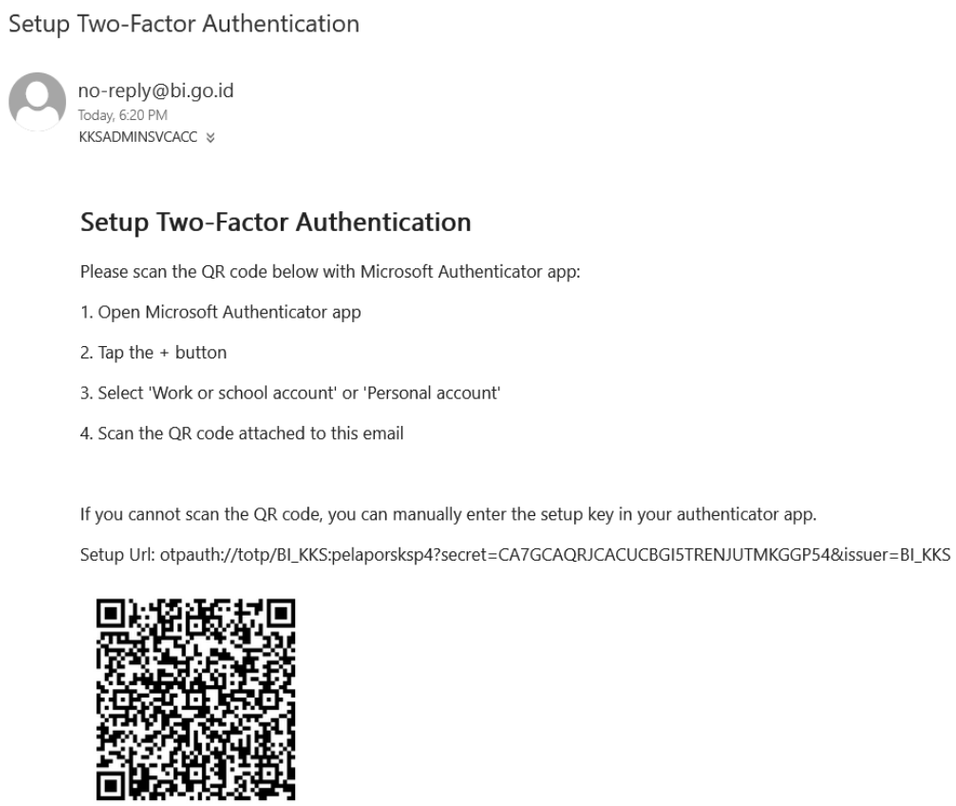
Gambar 9. Homepage Portal Integrasi Pelaporan Bank Indonesia.

Setelah klik modul Pelaporan KKS maka akan muncul halaman MFA, klik tombol *Register New Device* untuk mendapatkan kode autentikasi baru.



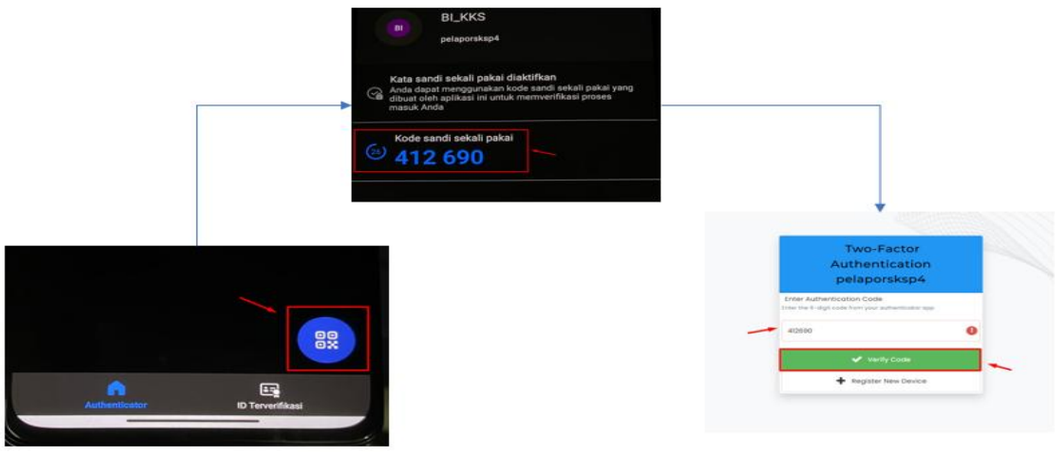
Gambar 10. Halaman Multi-Factor Authentication (MFA).

Setelah mendapatkan keterangan sukses, QR *code* akan dikirim ke *email* yang sebelumnya sudah didaftarkan saat pendaftaran *user*.



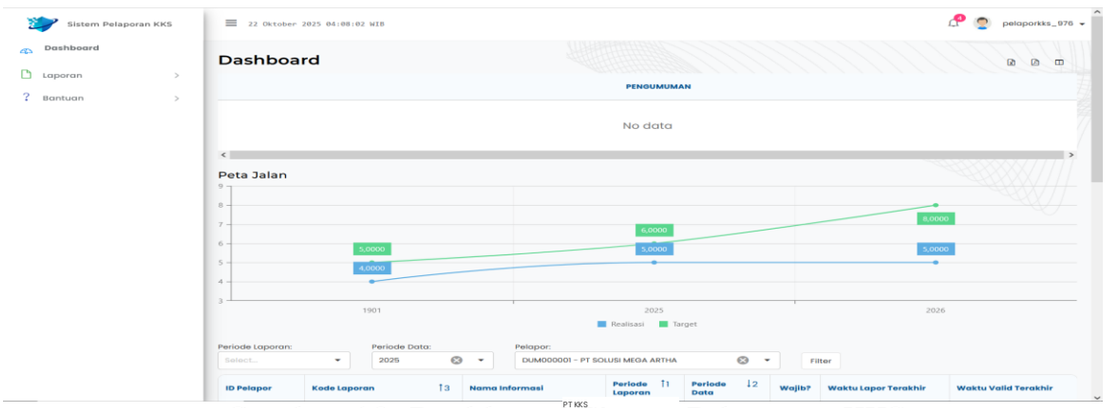
Gambar 11. Notifikasi Email QR Code.

Buka aplikasi *Microsoft Authenticator*. Klik *icon scan* QR pada pojok kanan bawah lalu lakukan *scan* QR yang ada pada *email*, maka otomatis data *authentication* untuk *user* sudah ditambahkan.



Gambar 12. Scan QR Code.

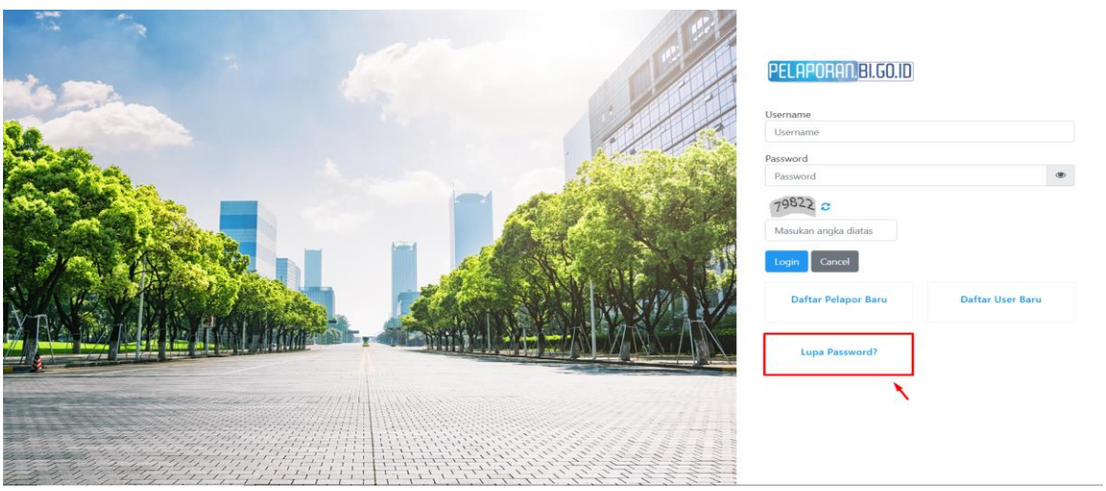
Input kode yang ada pada *Microsoft Authenticator* pada halaman MFA sistem pelaporan KKS lalu klik *Verify Code*, maka akan masuk ke sistem pelaporan KKS dan menampilkan halaman *Dashboard*.



Gambar 13. Dashboard Sistem Pelaporan KKS.

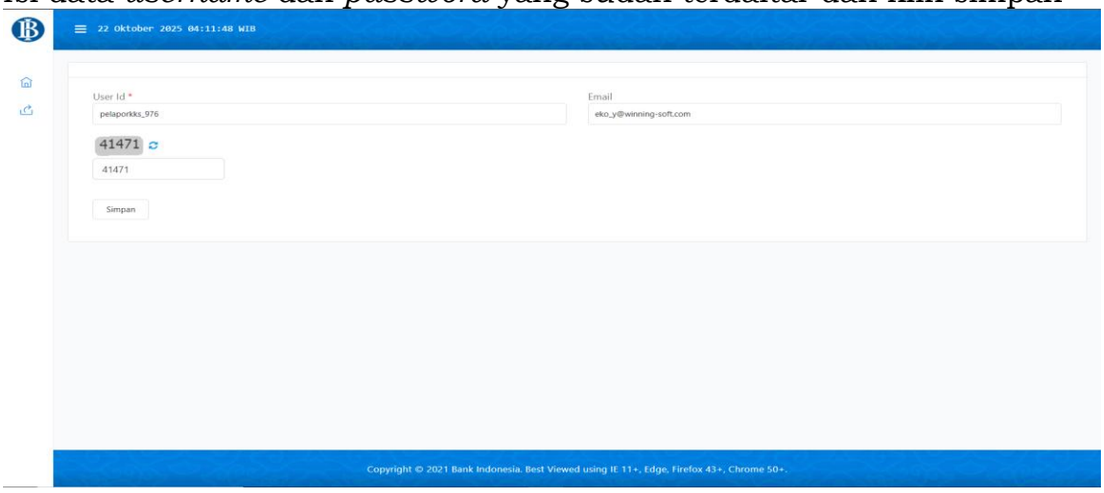
4. Reset Password

Untuk melakukan *Reset Password* pada sistem pelaporan KKS, *user* dapat mengakses *website* https://pelaporan.bi.go.id/Account/Login, lalu klik tombol Lupa *Password*.



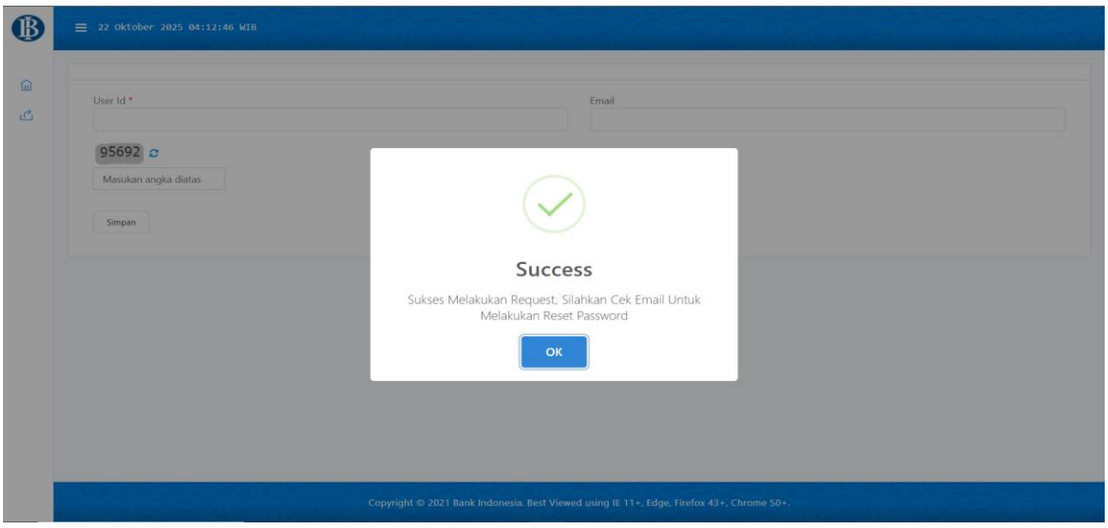
Gambar 14. Halaman Login Pelaporan.bi.go.id.

Isi data *username* dan *password* yang sudah terdaftar dan klik simpan



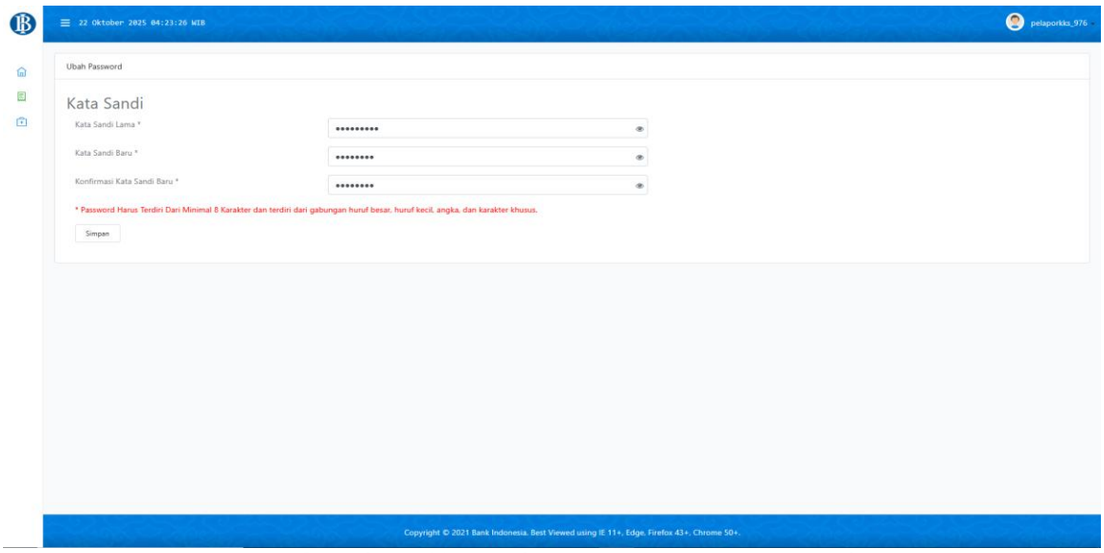
Gambar 15. Halaman Reset Password.

Jika muncul notifikasi sukses, maka *user* dapat melakukan cek *email* untuk melanjutkan tahapan reset *password*.



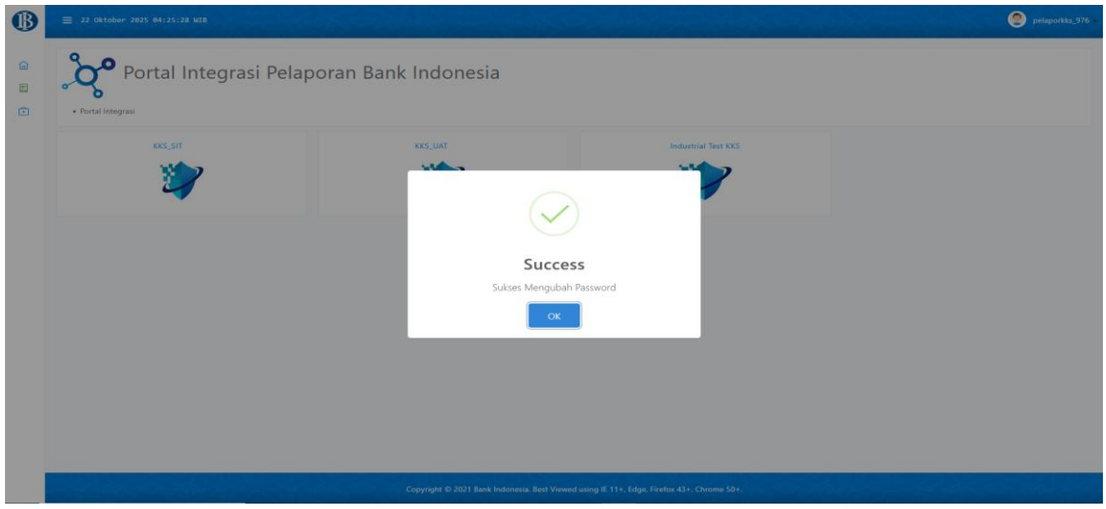
Gambar 16. Pop up Request Reset Password.

Setelah klik *link* pada *email*, maka *user* akan diarahkan ke halaman reset *password* untuk *input password* lama dan *password* baru sebagai berikut.



Gambar 17. Halaman Reset Password.

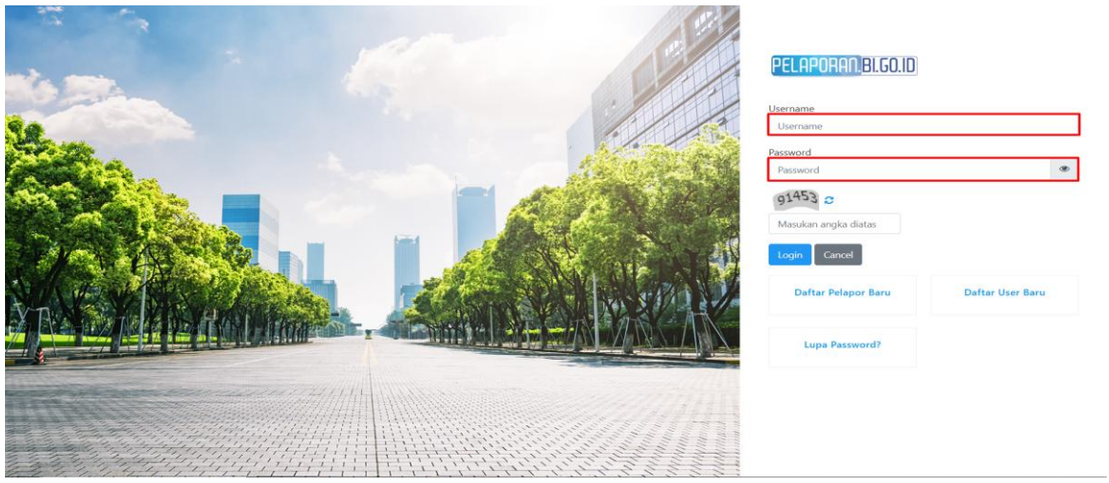
Klik Simpan, maka *password* sudah berhasil diubah.



Gambar 18. Berhasil Reset Password.

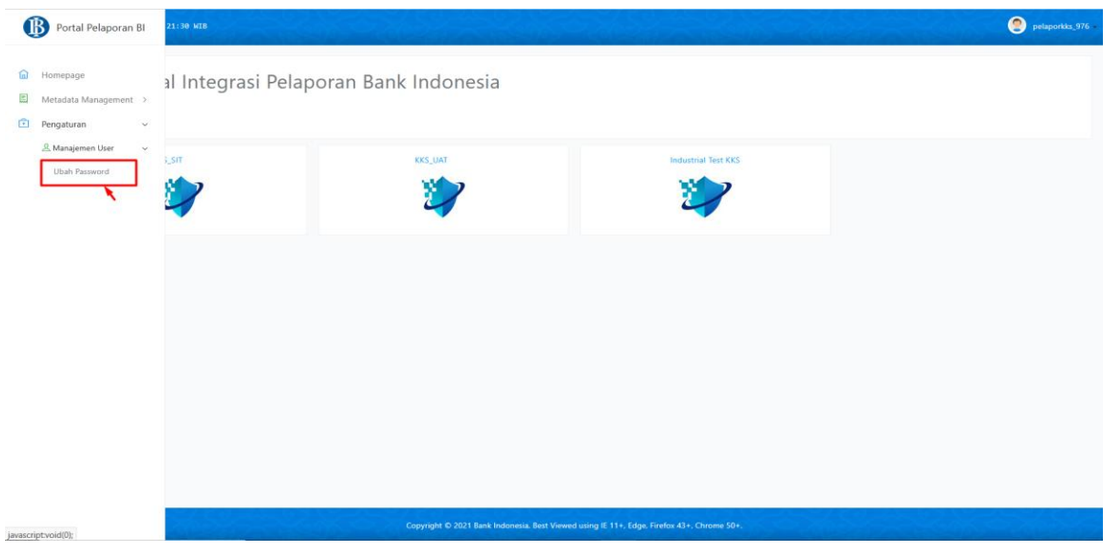
5. Ubah Password

User login pada sistem pelaporan KKS melalui *website* https://pelaporan.bi.go.id/Account/Login lalu isi data *username* dan *password* yang sudah terdaftar.



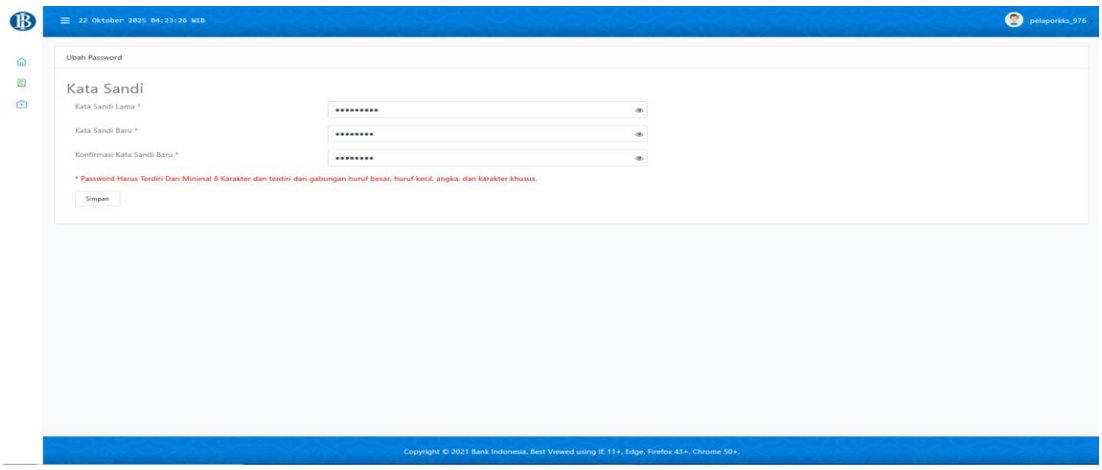
Gambar 19. Halaman Login Pelaporan.bi.go.id.

Input Captcha lalu klik tombol *Login*, maka akan tampil halaman *homepage* dan klik Ubah *Password.*



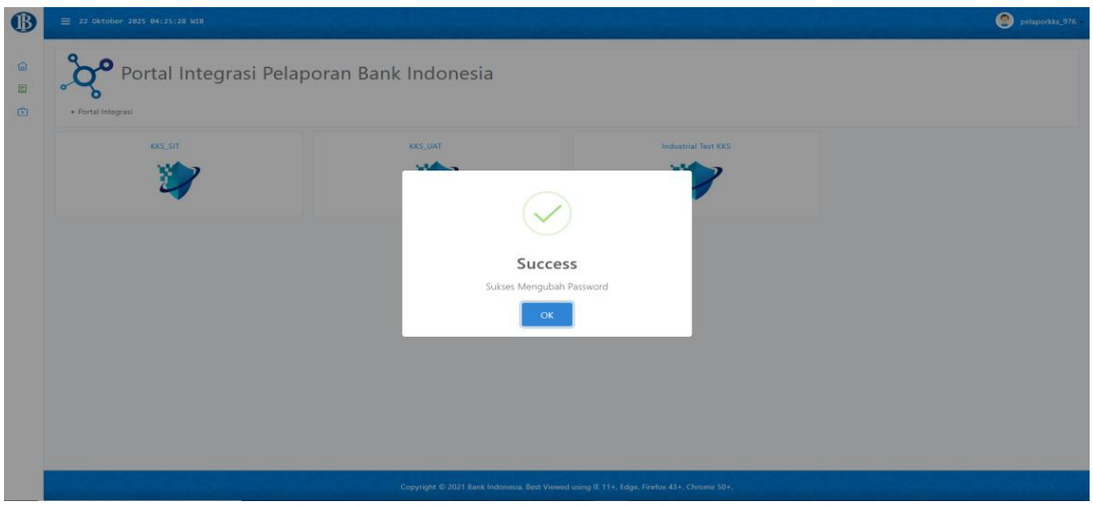
Gambar 20. Homepage Portal Integrasi Pelaporan Bank Indonesia.

Setelah klik Ubah *Password*, maka *user* akan diarahkan ke halaman ubah *password* untuk *input password* lama dan *password* baru.



Gambar 21. Halaman Ubah Password.

Klik Simpan, maka *password* sudah berhasil diubah.



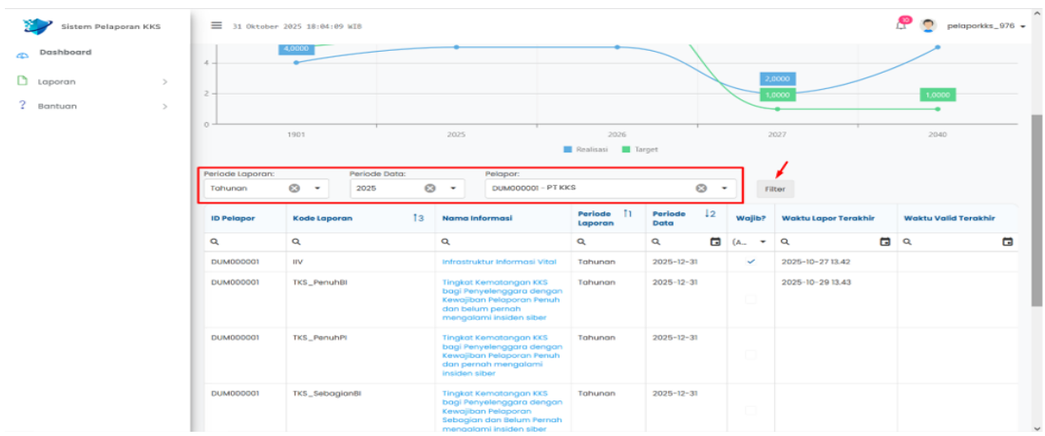
Gambar 22. Berhasil Ubah Password.

6. Laporan KKS

Menu ini digunakan untuk melakukan pelaporan seperti tambah data laporan, *edit*, *delete*, dan *submit* laporan.

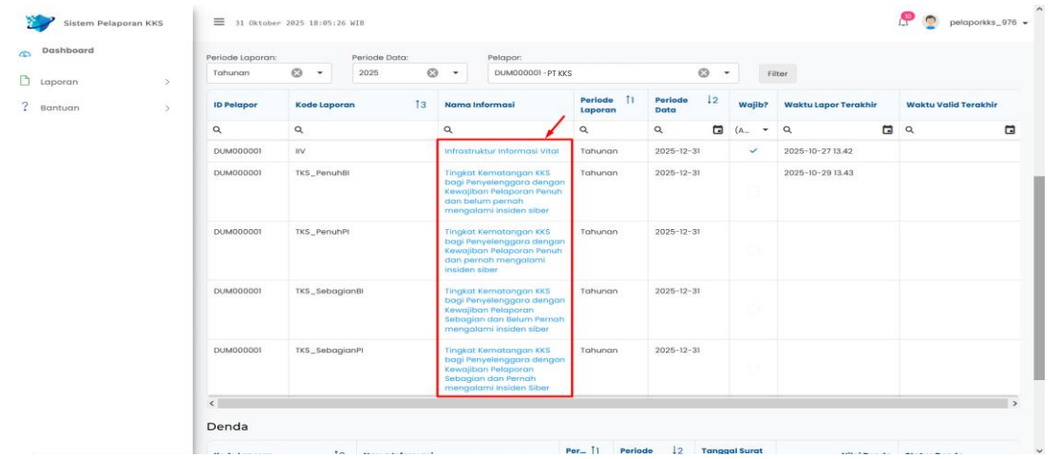
a. Akses Laporan KKS

Untuk mengakses halaman Laporan KKS, *login* sebagai pelapor lalu pada *dashboard* pilih Periode Laporan dan Periode Data, lalu klik *Filter*.



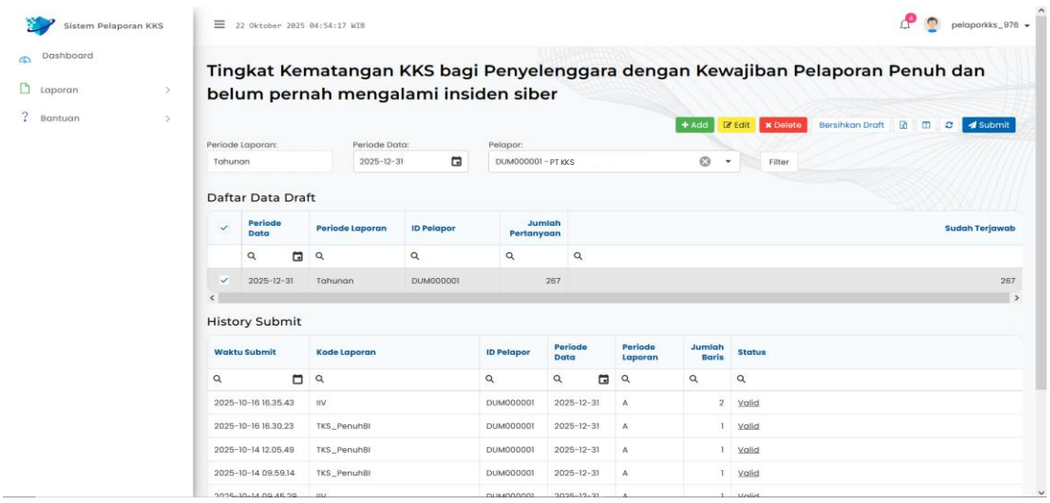
Gambar 23. Dashboard Pelaporan.

Lalu klik Nama Informasi Laporan yang akan dilaporkan.



Gambar 24. Pilih Laporan KKS.

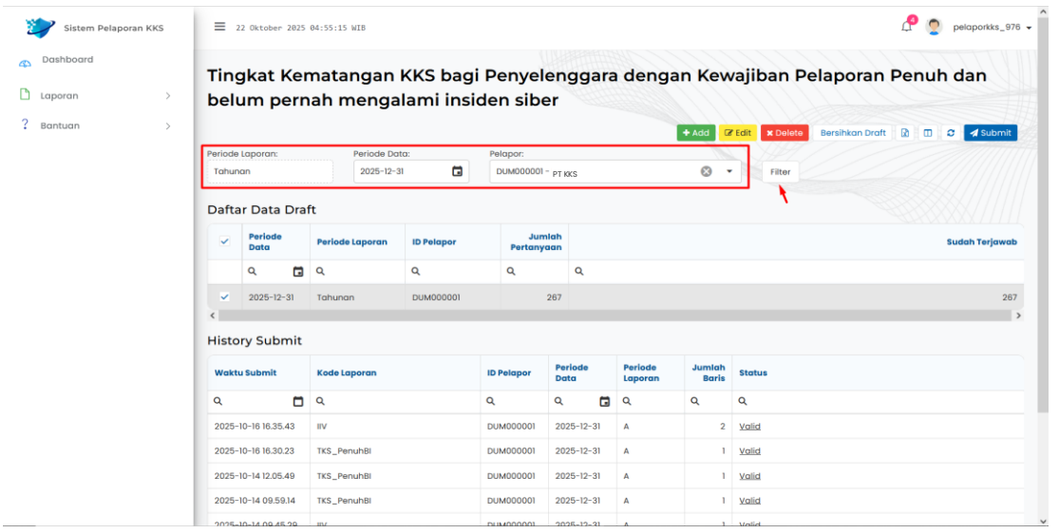
Maka akan tampil halaman laporan sesuai dengan laporan yang dipilih.



Gambar 25. Tampilan Laporan KKS yang dipilih.

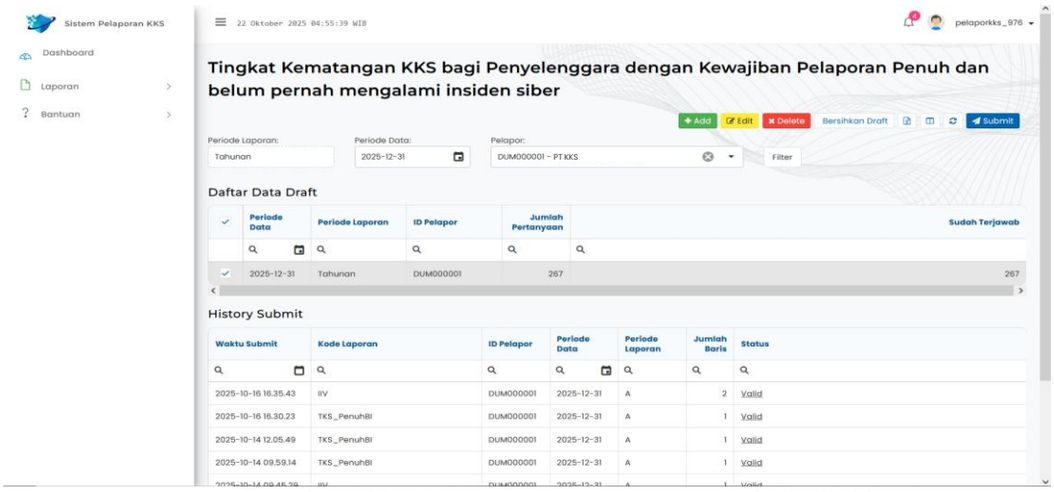
b. *Filter* Laporan KKS

Untuk melakukan *filter* pada data Laporan KKS, pilih Periode Laporan, Periode Data dan Pelapor, lalu klik tombol *Filter*.



Gambar 26. Filter Laporan KKS.

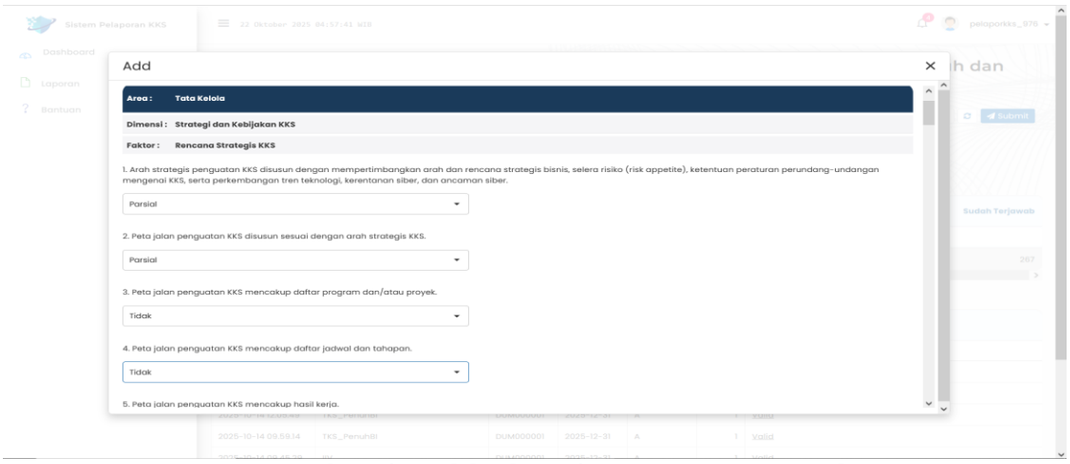
Maka akan tampil data sesuai hasil *filter* sebagai berikut.



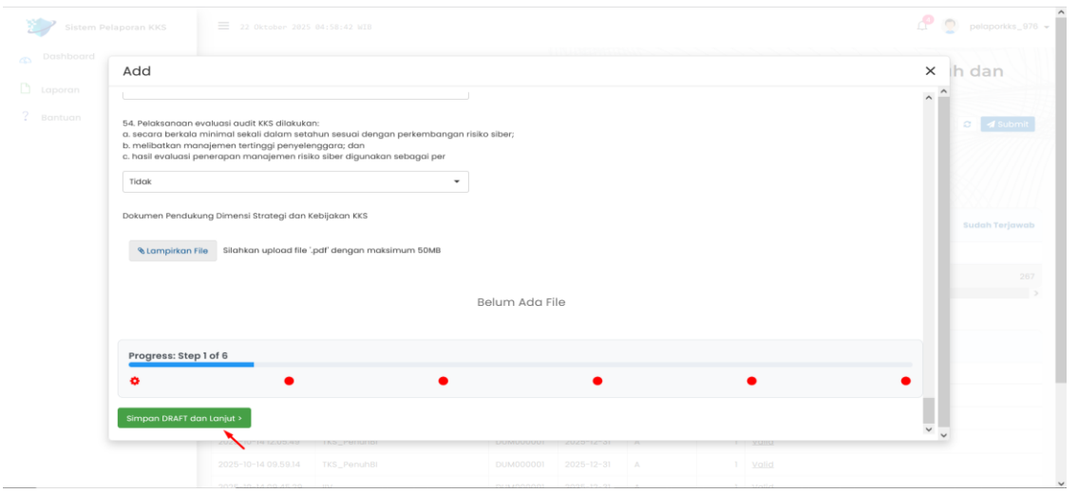
Gambar 27. Tampilan Data yang telah di-filter.

c. Tambah Laporan KKS

Untuk menambahkan laporan KKS, klik *icon* Add pada Laporan KKS lalu isi semua *quesioner* lalu klik tombol Simpan *Draft* dan Lanjut.



Gambar 28. Quesioner Laporan KKS.



Gambar 29. Progress Bar Laporan KKS.

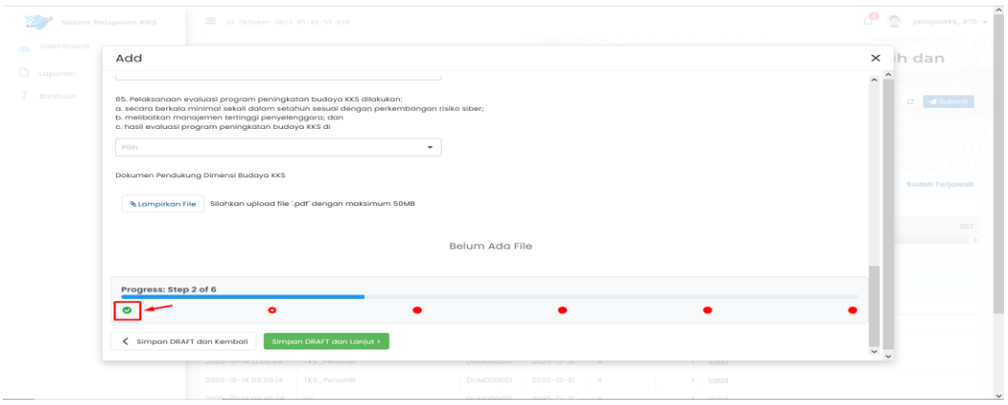
Setelah klik simpan *draft* dan lanjut, pastikan *progress* bar menunjukkan warna hijau sebagai informasi jika data sudah sesuai.

Sebagai informasi tambahan:

1) Untuk Laporan Tingkat Kematangan KKS dengan jawaban yang berisi "Ya" meng-*upload* dokumen pendukung menjadi *mandatory*,

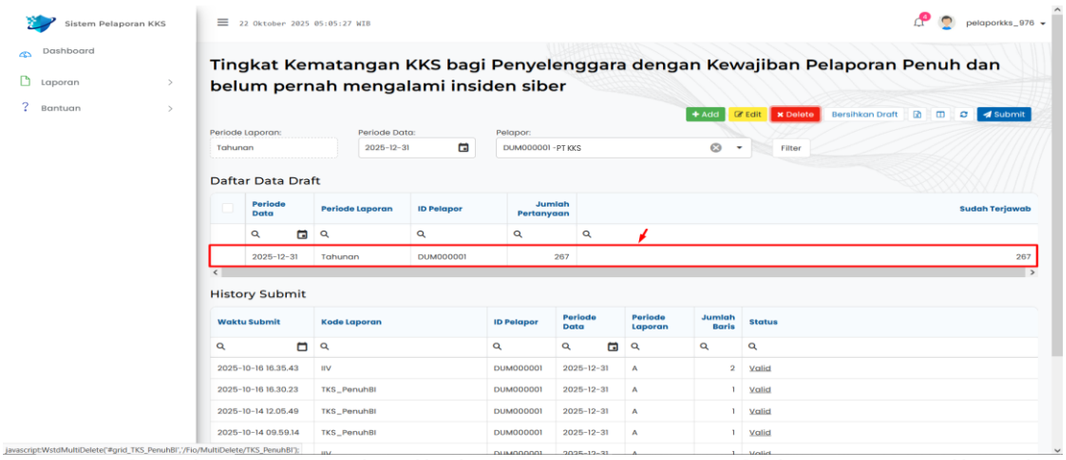
sedangkan jika jawaban "*Partial*" maka dokumen pendukung menjadi *optional* namun dapat di-*upload* sebagai bahan pertimbangan bagi Pengawas. Jika jawaban "Tidak" maka dokumen pendukung tidak perlu di-*upload*.

2) Untuk Laporan selain Laporan Tingkat Kematangan KKS, *upload* dokumen pendukung adalah *optional*



Gambar 30. *Progress Bar* Laporan KKS dengan *icon* hijau.

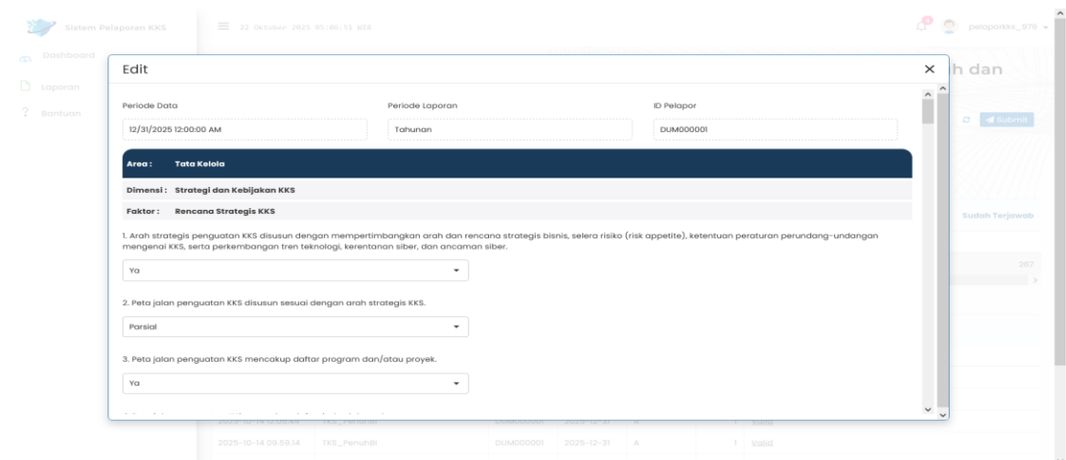
Lanjutkan semua *step* sehingga semua *quesioner* berhasil diisi dan disimpan sebagai *draft*, maka hasil *draft* tersebut akan tertampil pada halaman *grid* laporan sebagai berikut.



Gambar 31. Berhasil simpan Laporan KKS dan tertampil pada *Grid*.

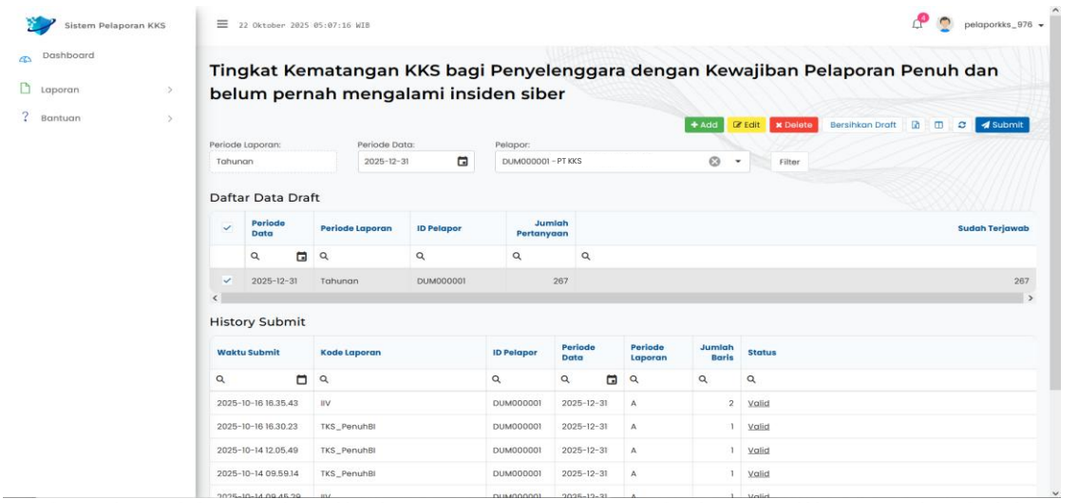
d. *Edit* Laporan KKS

Untuk mengedit laporan KKS, klik salah satu Laporan KKS lalu klik *icon* Edit, sesuaikan *quesioner* yang akan diubah lalu klik tombol *save*.



Gambar 32. *Quesioner* Laporan KKS.

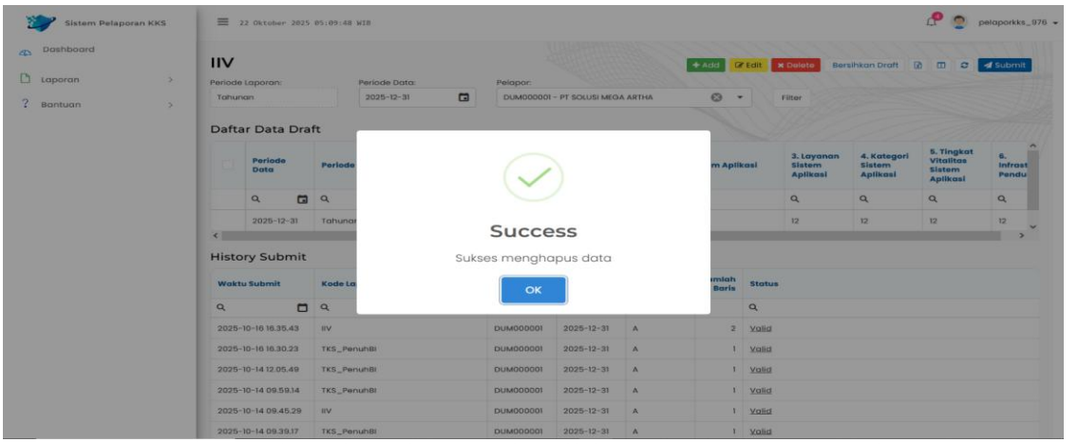
Setelah klik *save*, maka data akan tersimpan dan ter*update* pada halaman *grid* sebagai berikut.



Gambar 33. Berhasil simpan Laporan KKS dan terlihat pada *Grid*.

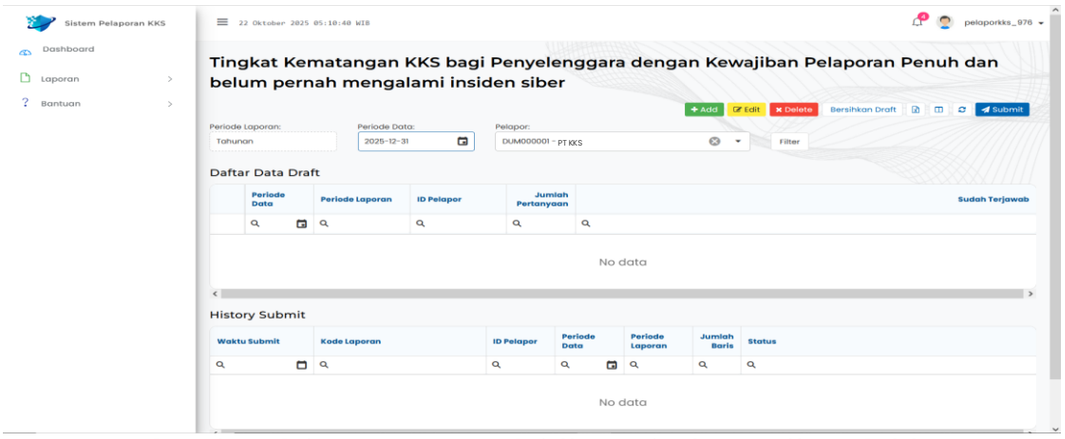
e. Hapus Laporan KKS

Untuk menghapus laporan KKS yang sebelumnya sudah di-*input*, klik salah satu Laporan KKS lalu klik *icon* Delete.



Gambar 34. Berhasil hapus Laporan KKS.

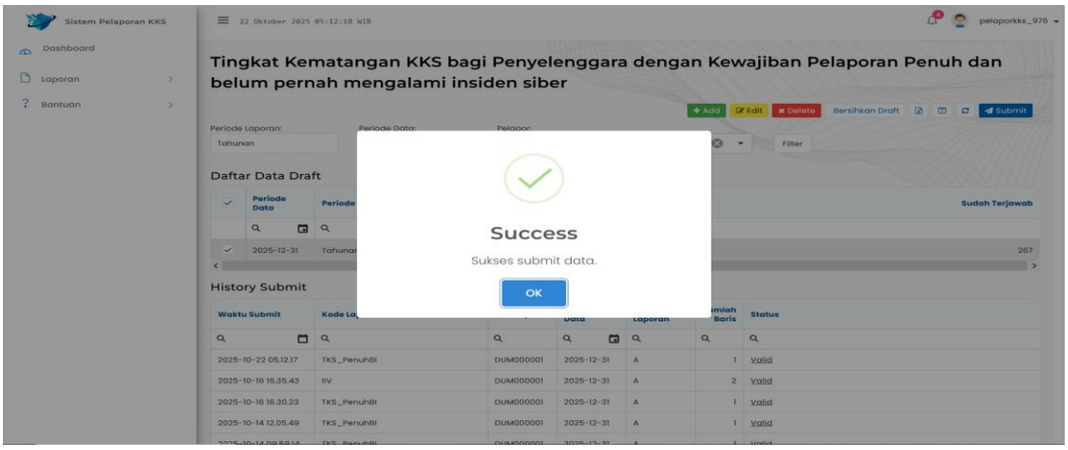
Setelah muncul notif sukses menghapus data, maka data akan terhapus dan hilang dari *grid*.



Gambar 35. Laporan KKS hilang dari tampilan *Grid*.

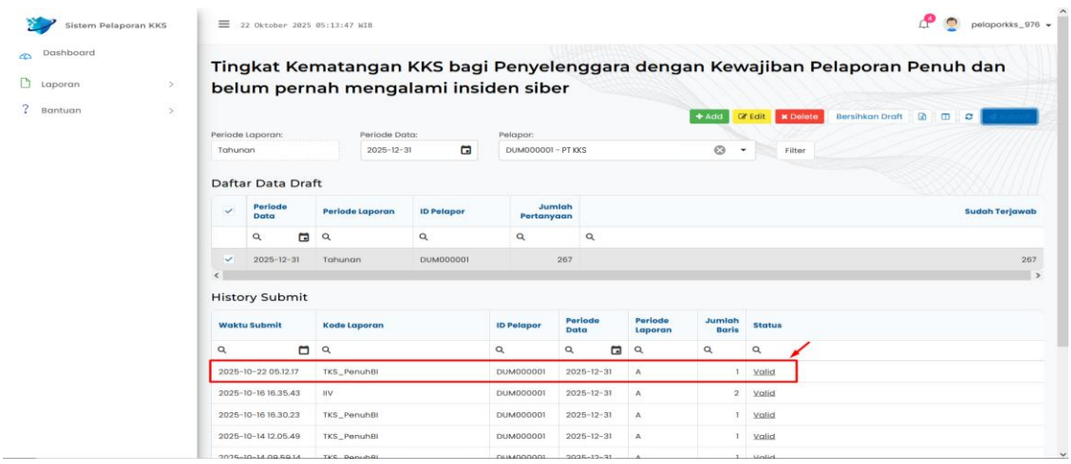
f. Submit Laporan KKS

Untuk *submit* laporan KKS yang sebelumnya sudah di-*input*, klik salah satu Laporan KKS lalu klik *icon* Submit.



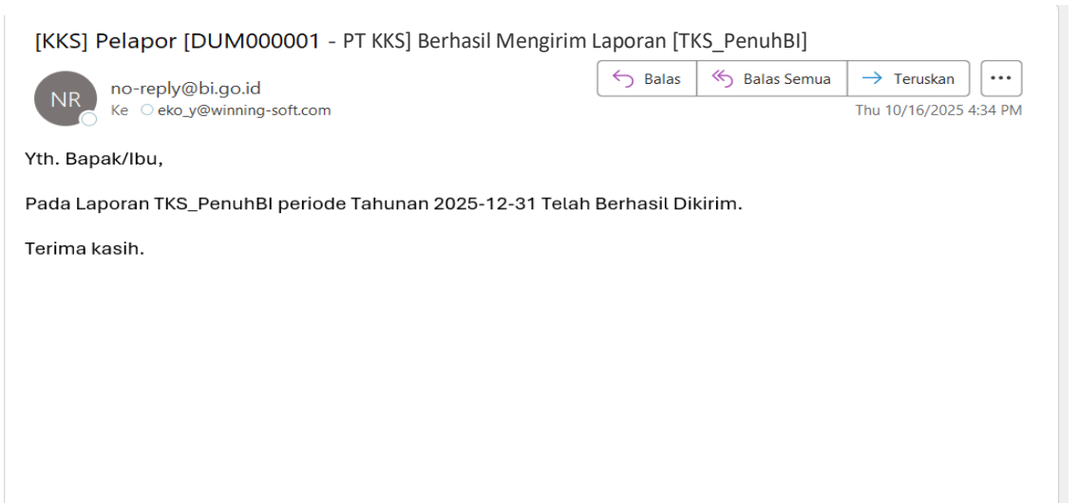
Gambar 36. Berhasil *Submit* Laporan KKS.

Setelah muncul notif sukses *submit* data, maka data yang berhasil disubmit tersebut akan muncul pada *history submit* sebagai berikut.

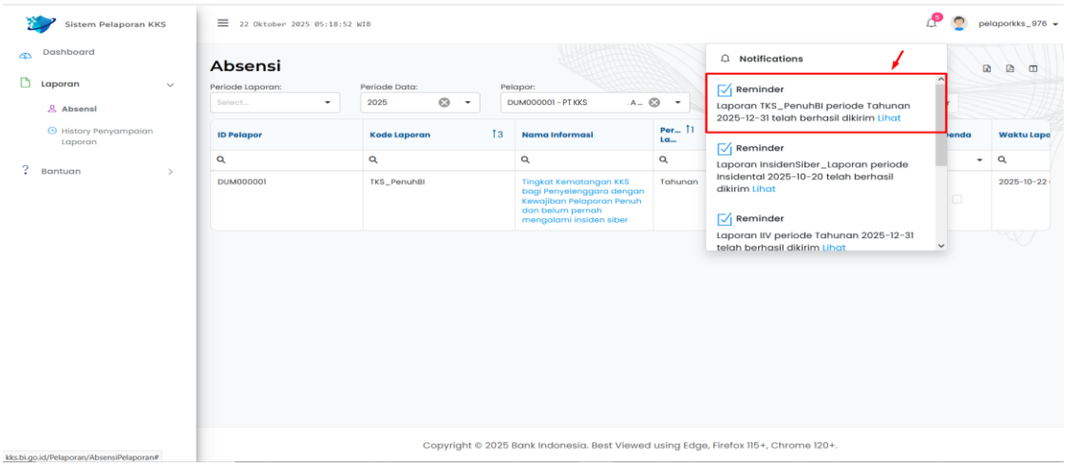


Gambar 37. Laporan KKS yang berhasil disubmit muncul pada History Submit.

Dan *user* akan menerima notifikasi *email* berhasil *submit* dan notifikasi pada *icon* lonceng dipojok kanan atas sebagai berikut.



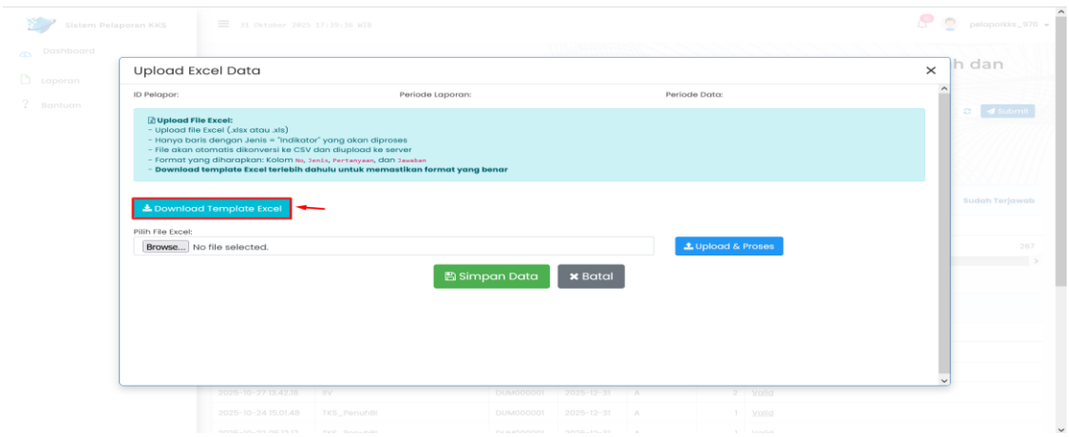
Gambar 38. Notifikasi Email berhasil submit Laporan KKS.



Gambar 39. Notifikasi Sistem berhasil submit Laporan KKS.

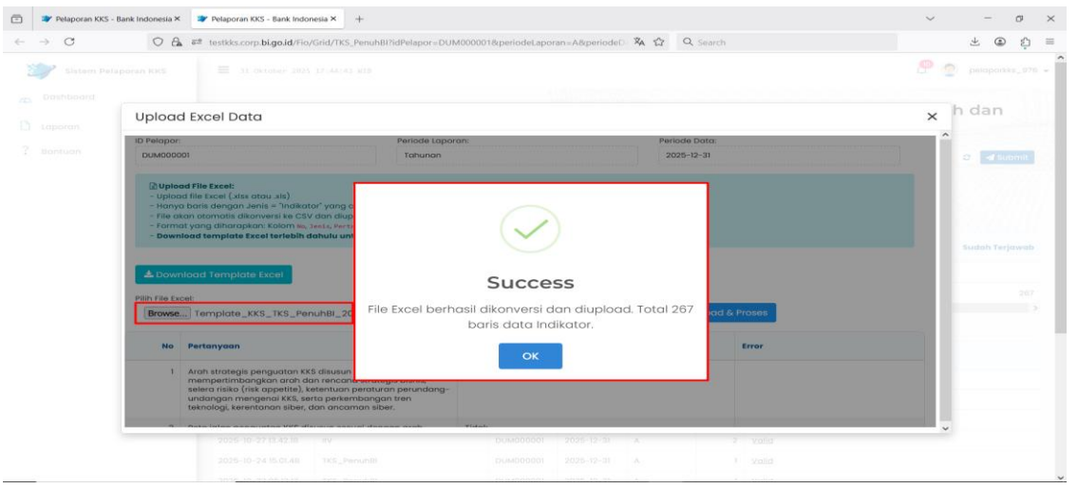
g. *Upload* Laporan KKS

Untuk *upload* data Laporan Tingkat Kematangan KKS, klik *icon* Upload pada menu Laporan KKS lalu klik *download template*.



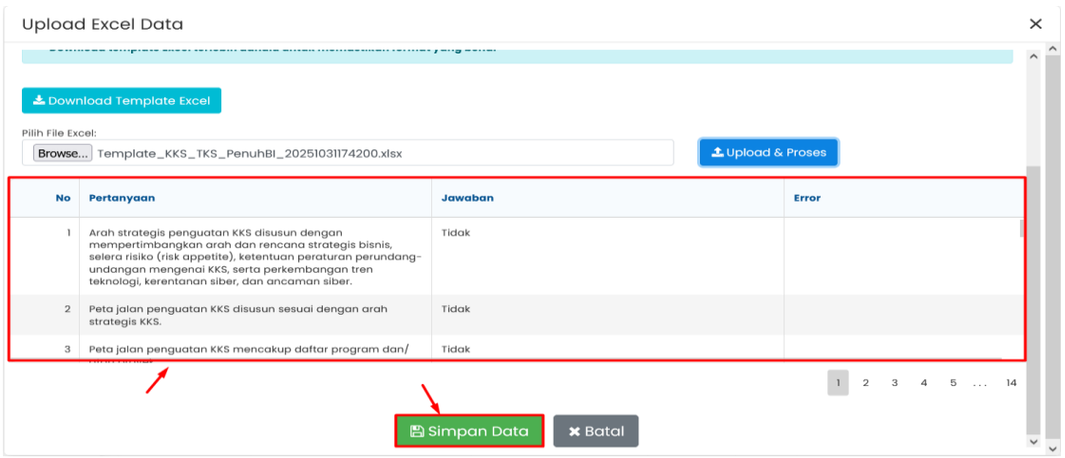
Gambar 40. Halaman Upload Excel Data Laporan KKS.

Isi jawaban pada *template* yang sudah di-*download* lalu klik *browse* dan pilih *template* yang sudah terisi semua jawaban lalu klik *Upload* & Proses.



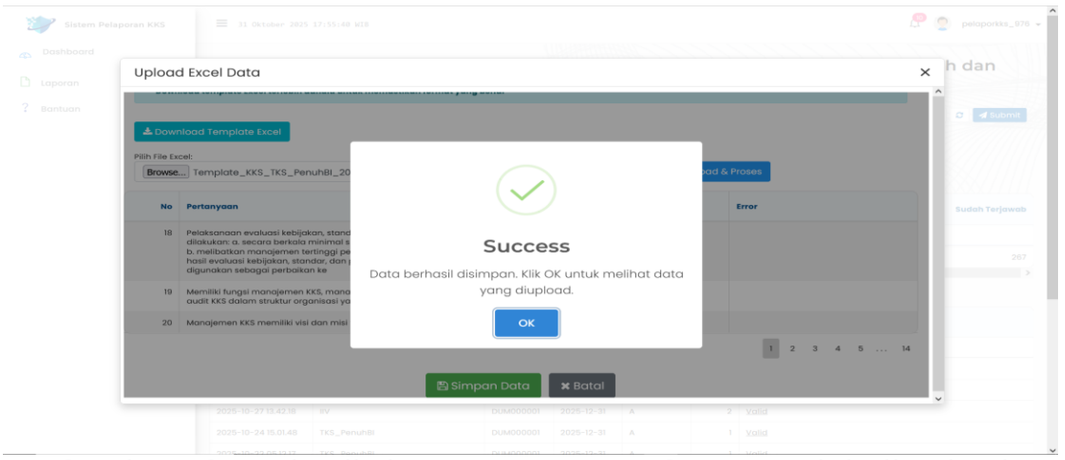
Gambar 41. Laporan KKS Berhasil di Upload.

Jika sudah muncul notifikasi sukses maka file excel berhasil dikonversi dan data akan tertampil pada *grid*.

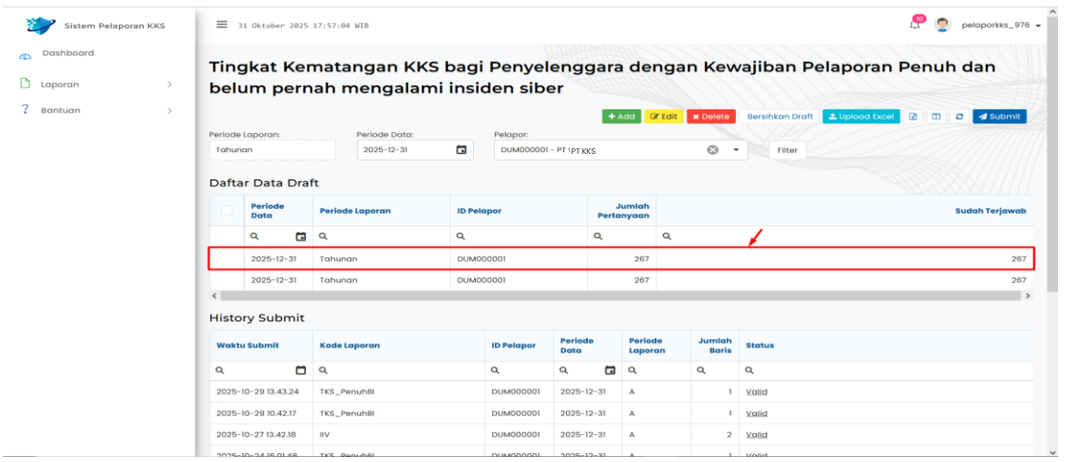


Gambar 42. Laporan KKS tertampil pada grid upload.

Klik tombol simpan data, maka laporan berhasil ter-*upload* dan tampil di *list* laporan sebagai berikut.



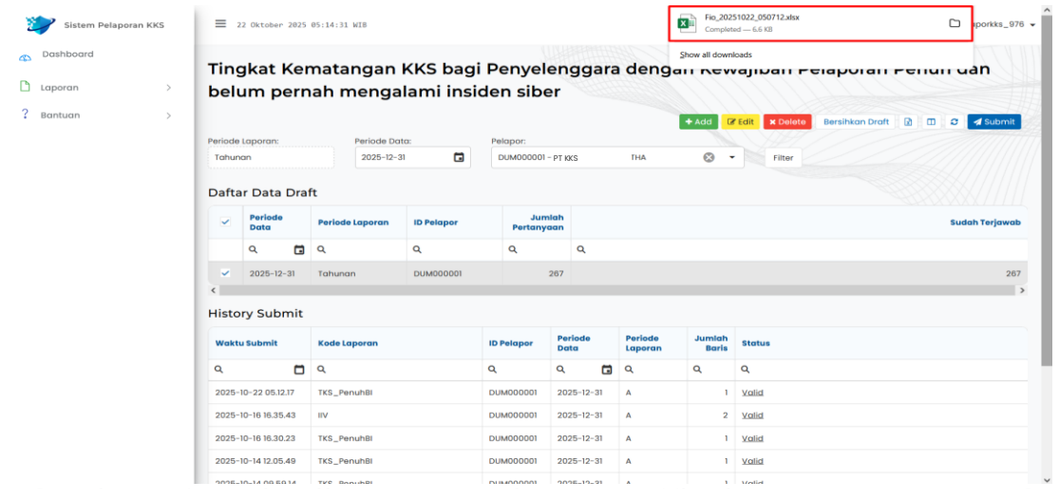
Gambar 43. Berhasil simpan Laporan KKS yang sudah di upload.



Gambar 44. Laporan Tingkat Kematangan KKS tertampil pada Grid.

h. *Export Excel Laporan KKS*

Untuk melakukan *export* excel pada Laporan KKS, bisa klik *icon*  maka akan terunduh hasil *export* dalam format excel sebagai berikut.



Gambar 45. Berhasil Export Excel Laporan Tingkat Kematangan KKS.

7. Laporan - Absensi

Menu ini digunakan untuk menampilkan data absensi pelapor yang melaporkan laporan KKS berupa status absensi, denda dan lainnya.

a. *Filter* Absensi

Untuk melakukan *filter* pada data absensi, Isi Periode Laporan, Periode Data, Penyelenggara dan Nama Informasi lalu klik tombol *Filter*.

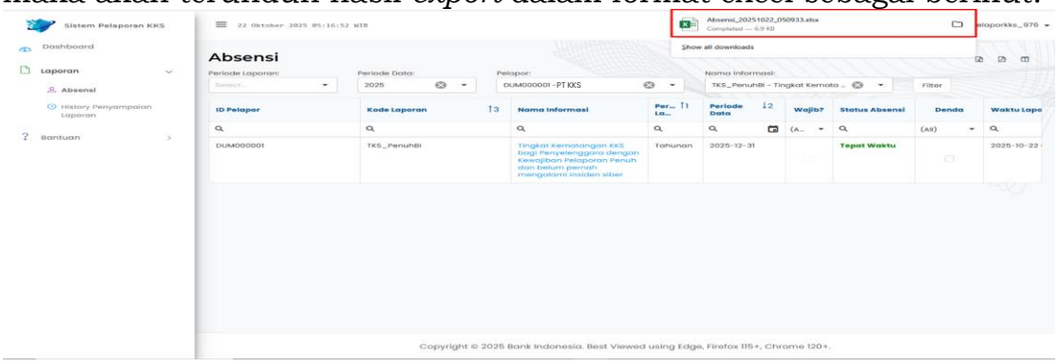
Gambar 46. Halaman Absensi.

Maka akan tampil data sesuai hasil *filter* sebagai berikut.

Gambar 47. Hasil Filter Absensi.

b. *Export Excel Absensi*

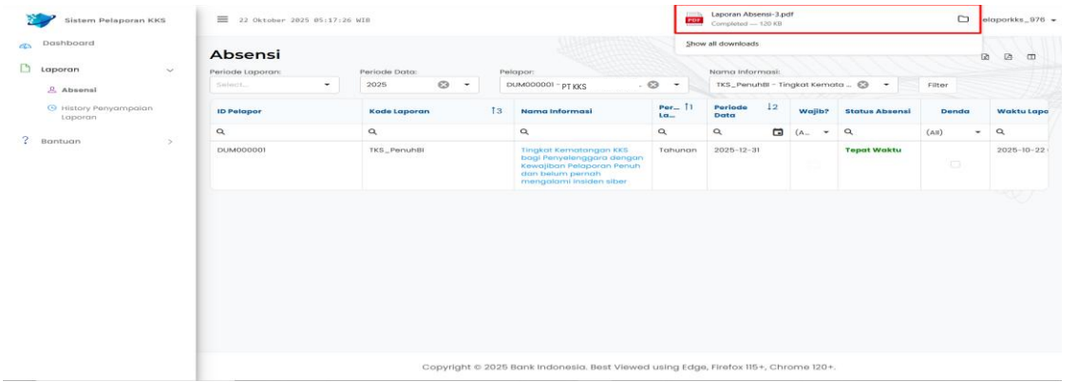
Untuk melakukan *export* excel pada absensi *user*, bisa klik *icon* maka akan terunduh hasil *export* dalam format excel sebagai berikut.



Gambar 48. Berhasil Export Excel data Absensi.

c. *Export* PDF Absensi

Untuk melakukan *export* PDF pada absensi *user*, bisa klik *icon* maka akan terunduh hasil *export* dalam format PDF sebagai berikut.



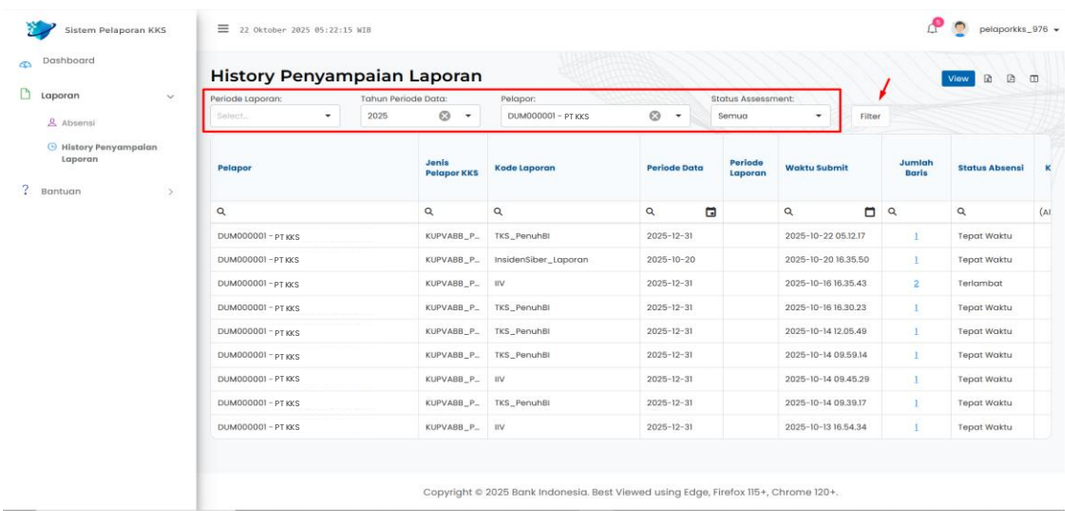
Gambar 49. Berhasil Export PDF Data Absensi.

8. Laporan - *History* Penyampaian Laporan

Menu ini digunakan untuk menampilkan data *history* laporan yang sudah berhasil di-*submit* oleh Penyelenggara.

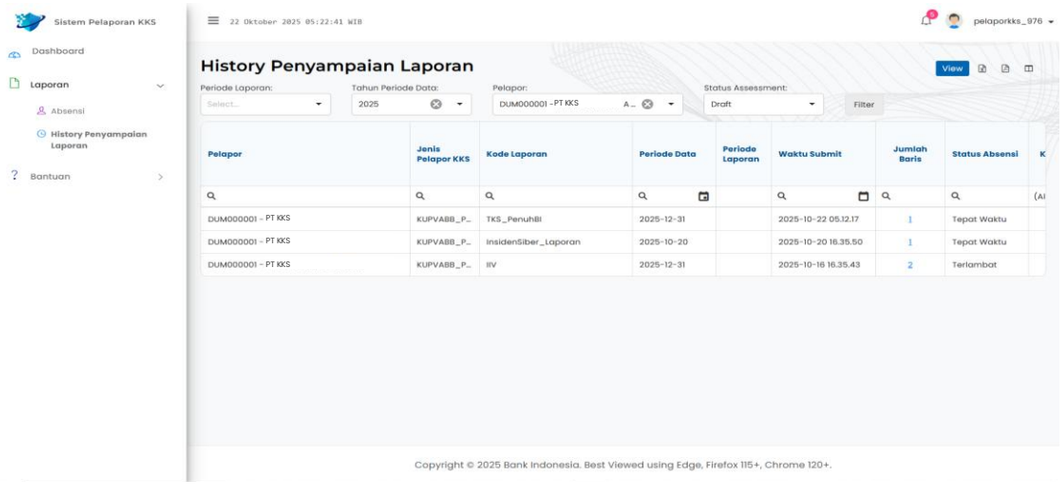
a. *Filter History* Penyampaian Laporan

Untuk melakukan *filter* pada data *History* Penyampaian Laporan, Isi Periode Laporan, Periode Data, Penyelenggara dan Status *Assessment* lalu klik tombol *Filter*.



Gambar 50. Halaman History Penyampaian Laporan.

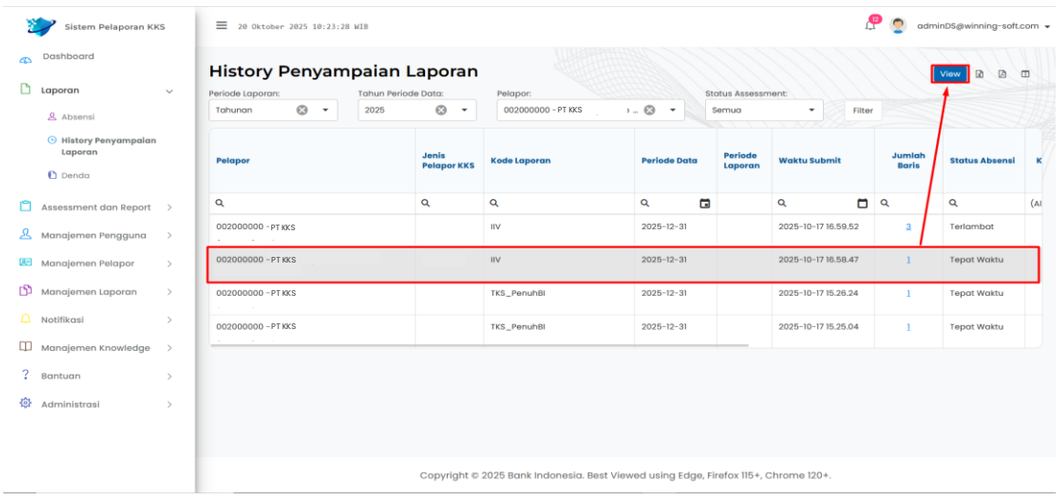
Maka akan tampil data sesuai hasil *filter* sebagai berikut.



Gambar 51. Hasil Filter History Penyampaian Laporan.

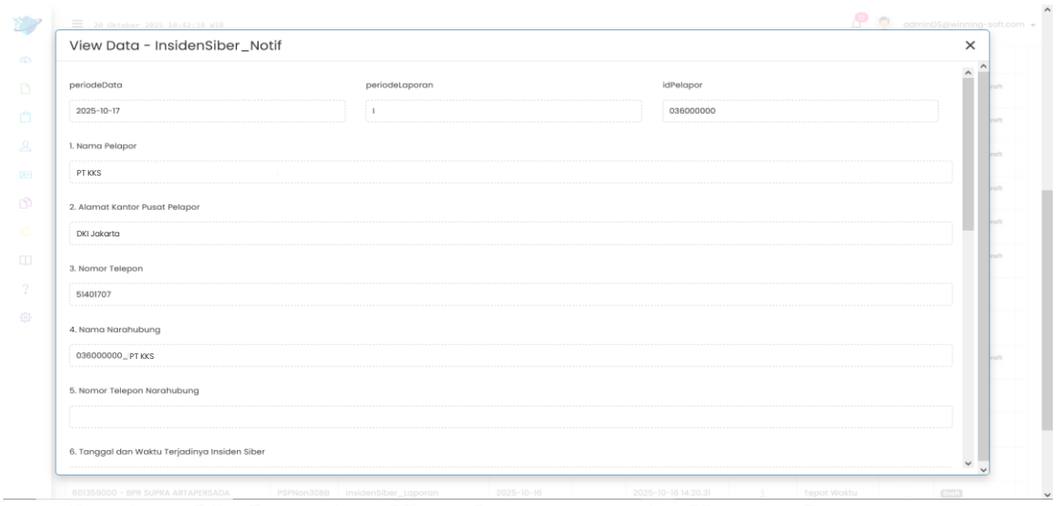
b. *View Detail Laporan*

Untuk melakukan *view* detail laporan, pilih laporan lalu klik tombol *View*.



Gambar 52. View History Penyampaian Laporan.

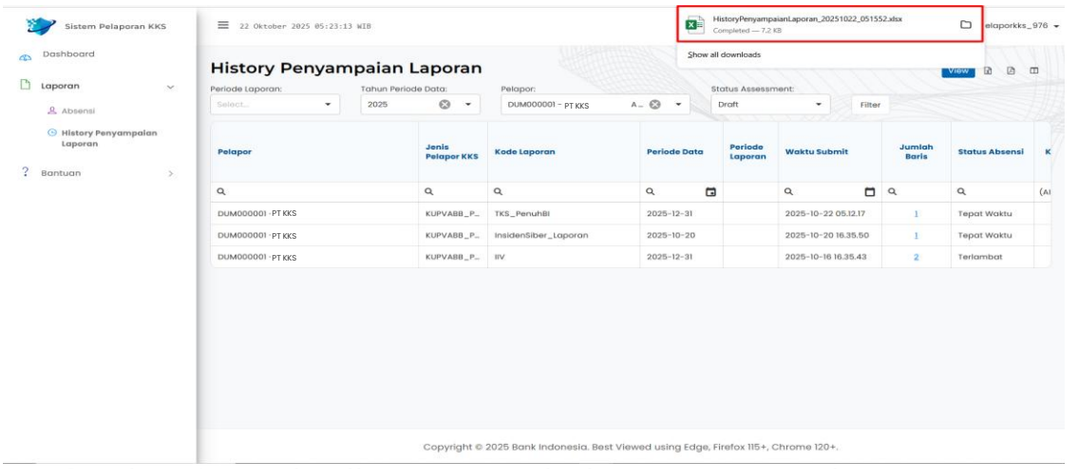
Setelah klik tombol *View* maka akan muncul *pop up* tampilan detail laporan sebagai berikut.



Gambar 53. Tampilan View Laporan pada History Penyampaian Laporan.

c. *Export Excel History Penyampaian Laporan*

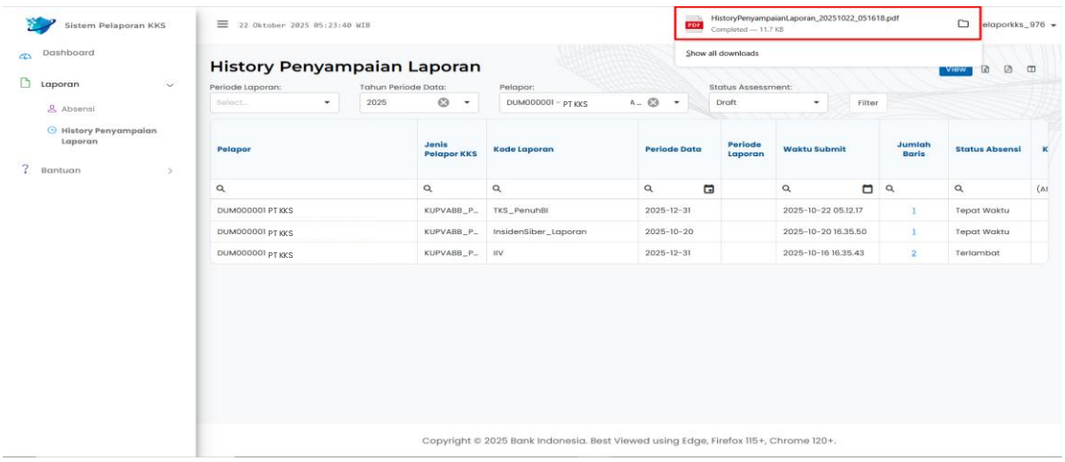
Untuk melakukan *export* excel pada *History* Penyampaian Laporan, bisa klik *icon* maka akan terunduh hasil *export* dalam format excel sebagai berikut.



Gambar 54. Berhasil Export Excel History Penyampaian Laporan.

d. *Export PDF History Penyampaian Laporan*

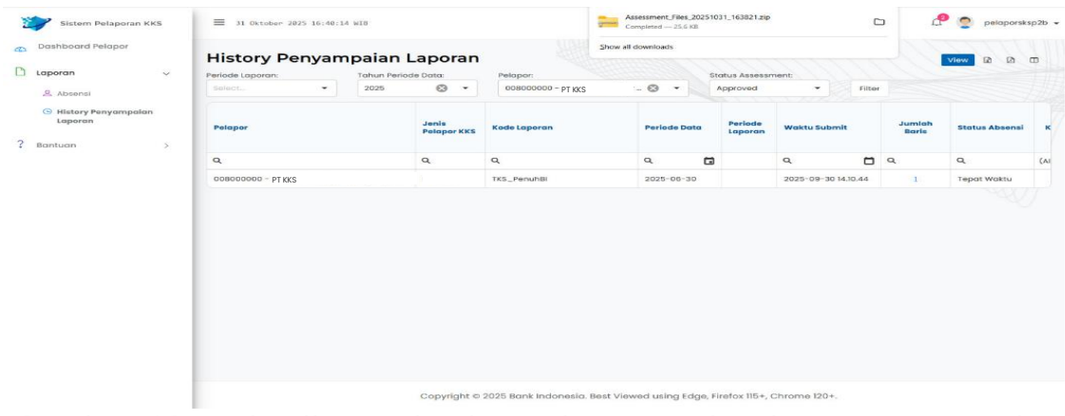
Untuk melakukan *export* PDF pada *History* Penyampaian Laporan, bisa klik *icon* maka akan terunduh hasil *export* dalam format PDF.



Gambar 55. Berhasil Export PDF History Penyampaian Laporan.

e. *Download Attachment dari Pengawas*

Untuk melakukan *download attachment* pada *History* Penyampaian Laporan, bisa klik status *assesment* yang sudah *Approved* maka akan terunduh dalam format PDF sebagai berikut.



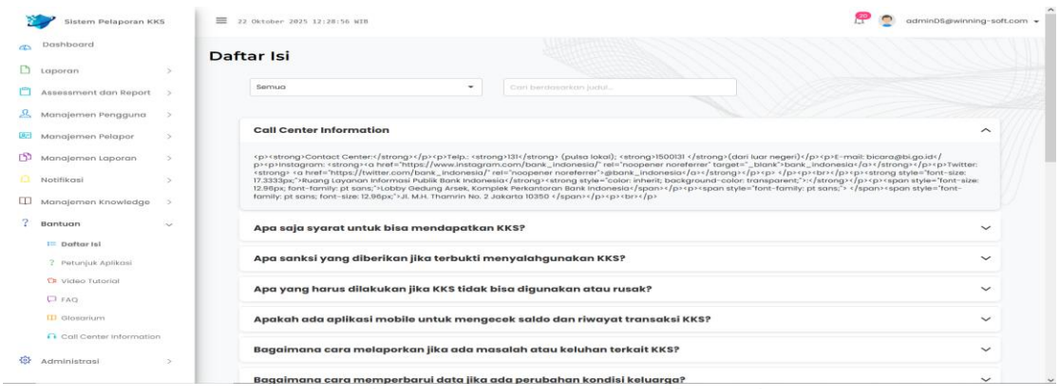
Gambar 56. Berhasil Download Attachment pada History Penyampaian Laporan.

9. Bantuan

Menu ini digunakan untuk menampilkan informasi yang dapat membantu *user* terkait Sistem pelaporan KKS seperti Daftar Isi, Petunjuk Aplikasi, Video Tutorial, FAQ, *Glosarium*, dan *Call Center Information*.

a. Menampilkan Daftar Isi

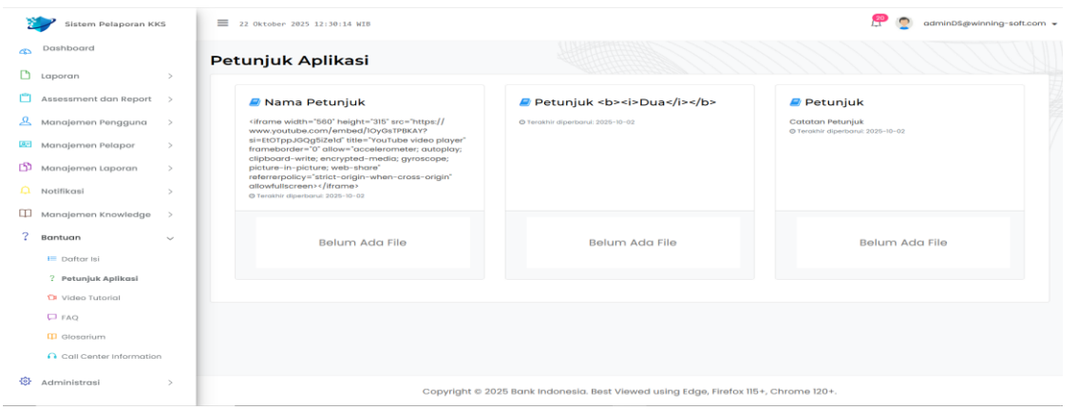
Untuk menampilkan daftar isi, pilih Bantuan lalu klik menu Daftar Isi.



Gambar 57. Halaman Daftar Isi.

b. Menampilkan Petunjuk Aplikasi

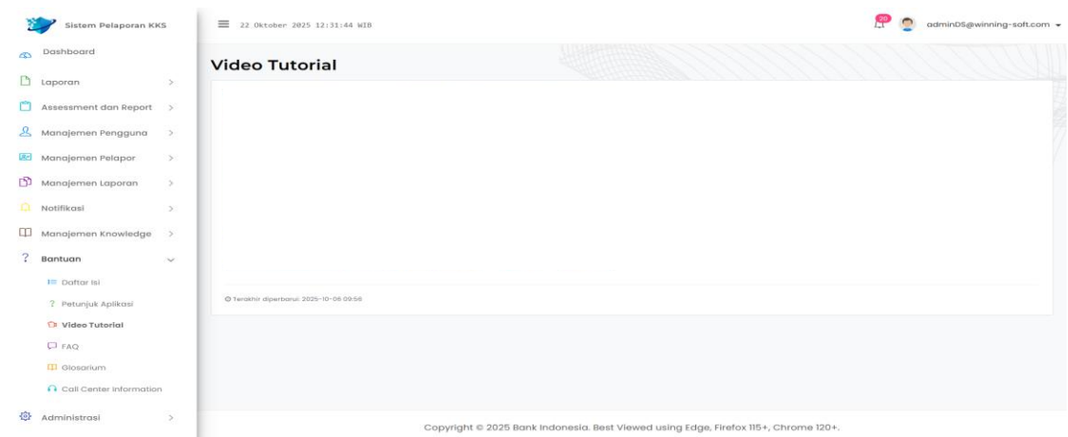
Untuk menampilkan petunjuk aplikasi, pilih Bantuan lalu klik menu Petunjuk Aplikasi.



Gambar 58. Halaman Petunjuk Aplikasi.

c. Menampilkan Video Tutorial

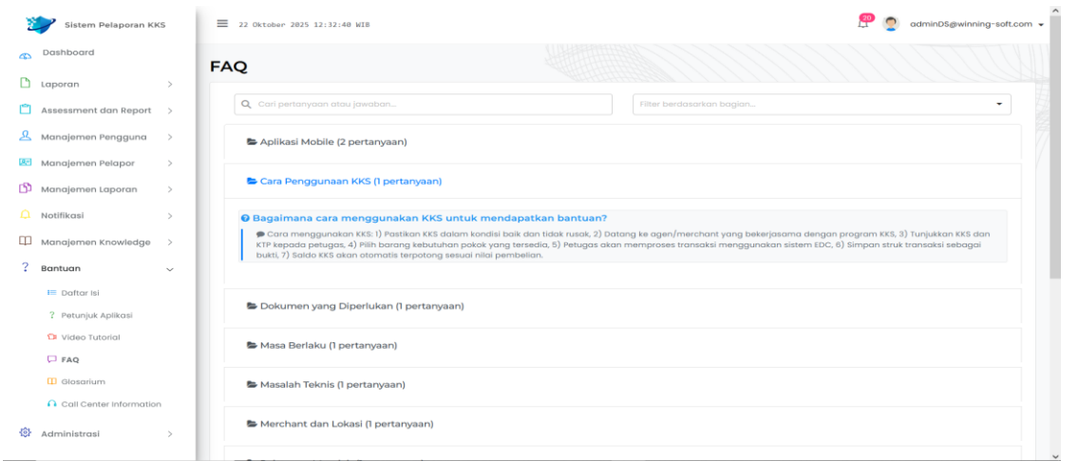
Untuk menampilkan video tutorial, pilih Bantuan lalu klik menu Video Tutorial.



Gambar 59. Halaman Video Tutorial.

d. Menampilkan FAQ

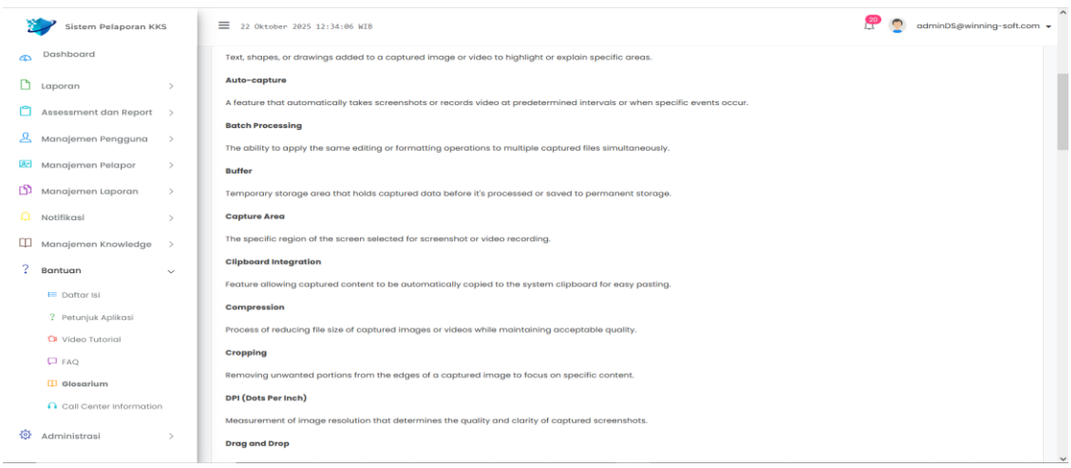
Untuk menampilkan FAQ, pilih Bantuan lalu klik menu FAQ.



Gambar 60. Halaman FAQ.

e. Menampilkan Glosarium

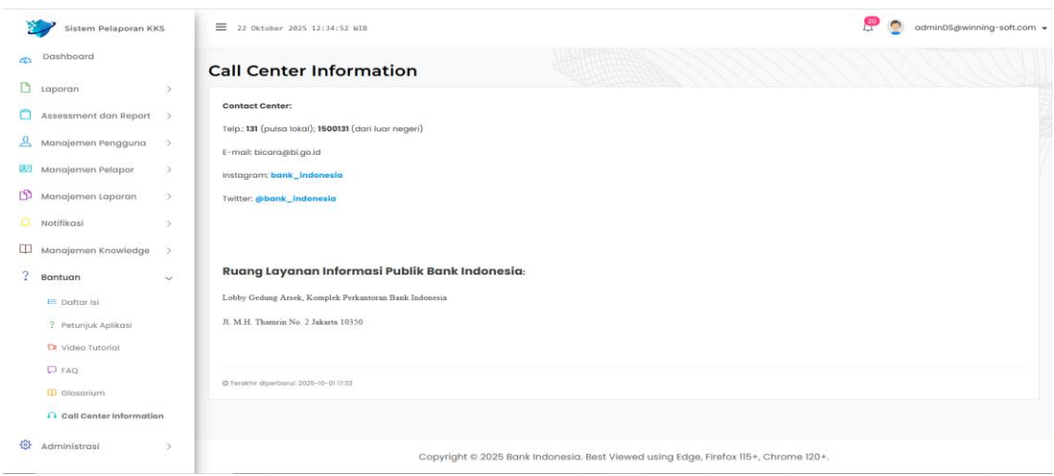
Untuk menampilkan *glosarium*, pilih Bantuan lalu klik menu *Glosarium*.



Gambar 61. Halaman Glosarium.

f. Menampilkan Call Center Information

Untuk menampilkan *call center information*, pilih Bantuan lalu klik menu *Call Center Information*.



Gambar 62. Halaman Call Center Information.