

TUGAS AKHIR
SISTEM MANAJEMEN KEAMANAN INFORMASI
KELAS B



Kelompok : I
Ketua Kelompok : Sari Andarwati
Anggota : Muhammad Shamad
Maysarah
Mumami

Kendali Dokumen:

Nama Penulis	Versi	Tanggal	Tanda Tangan
Tim Layanan Mobile	1.0	1 Februari 2022	
Tim Audit	1.1	20 Maret 2022	

DAFTAR ISI

- A. Pedoman Sistem Manajemen Keamanan Informasi (khusus kepentingan pelatihan)
 - I. Informasi tentang Organisasi (Nama, Alamat, Visi/Misi/Tujuan organisasi)
 - II. Pengesahan Dokumen (Pimpinan Organisasi)
 - III. Informasi Dokumen (Judul dokumen, versi, tanggal terbit)
 - IV. Issue Internal dan Eksternal
 - V. Kebutuhan Pemangku Kepentingan (stakeholder)
 - VI. Ruang Lingkup penerapan SMKI
 - VII. Persyaratan hukum dan peraturan perundang undangan terkait SMKI
 - VIII. Organisasi / Struktur Organisasi SMKI
 - IX. Kebijakan dan Komitmen SMKI
 - X. Sasaran Sistem Manajemen Keamanan Informasi
 - XI. Kebutuhan Sumber Daya dan Kompetensinya
 - XII. Komunikasi Informasi
- B. Risk Register
- C. *The Statement of Applicability (SoA)*
- D. Prosedur (3 Prosedur)
- E. Instruksi Kerja (disesuaikan setiap prosedur)
- F. Form / Logbook (disesuaikan setiap prosedur / Instruksi Kerja)
- G. Pengamatan Ketidaksesuaian dan Tindakan Perbaikan Video 1 sd 4

Informasi tentang Organisasi

Nama Organisasi: Bank XYZ

Alamat : Jl. Pangeran No. 20, Jakarta Barat, Indonesia

Visi

Menjadi Lembaga keuangan yang terunggul dalam layanan dan kinerja secara berkelanjutan

Misi :

1. Memberikan layanan prima dan solusi digital kepada seluruh nasabah selaku mitra bisnis pilihan utama
2. Memperkuat layanan internasional untuk mendukung kebutuhan Mitra Bisnis Global
3. Meningkatkan nilai investasi yang unggul bagi investor
4. Menciptakan kondidi terbaik bagi karyawan sebagai tempat kebanggaan untuk berkarya dan berprestasi
5. Meningkatkan kepedulian dan tanggungjawab kepada lingkungan dan masyarakat
6. Menjadi acuan Pelaksanaan Kepatuhan dan tata Kelola perusahaan yang baik bagi industri.

Tujuan : Memperbaiki ekonomi rakyat dan berpartisipasi dalam pembangunan ekonomi nasional.

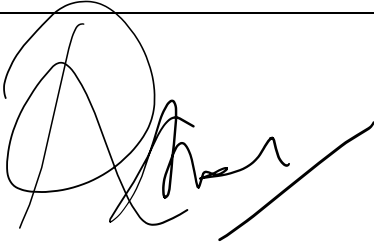


LEMBAR PENGESAHAN

JENIS KEGIATAN : Layananan E-mobile Banking

KEGIATAN STANDAR KEAMANAN INFORMASI

E-MOBILE BANKING

BANK XYZ

Nomor Dokumen	: 01/TIK.02.K.SMKI/14/2022	
Versi	: 1	
Tanggal Ditetapkan	: 1 Maret 2022	
Tanggal Ditinjau Kembali	: 1 Maret 2023	
Diperiksa oleh:		
Tim Layanan Mobile	Kepala Layanan TIK dan Informasi	Direktur Utama PT Bank XYZ
		
Ratna	Adi	Musa Alfonso
Catatan : 1. Jika versi terbaru telah diterbitkan, maka versi sebelumnya ditetapkan tidak berlaku. 2. Versi terbaru terdapat dalam bentuk elektronik.		

INFORMASI DOKUMEN
BANK XYZ

Versi	Tanggal	Penulis	Deskripsi
1	1 Februari 2022	Tim Layanan Mobile	Dokumen awal
2	20 Maret 2022	Tim Audit	Perubahan klausul audit internal

PENERAPAN SISTEM MANAJEMEN KEAMANAN INFORMASI

I. Issue Internal dan Eksternal

Ruang lingkup penerapan SMKI pada Layanan Mobile Banking Bank XYZ dipengaruhi oleh isu internal dan eksternal sebagaimana pada table dibawah.

Tabel 1. Isu Internal Eksternal

No	Issue	Internal	Eksternal
1	Pencurian Saldo nasabah	Lemahnya internal control	
		Masalah SDM	
2	Penipuan yang mengatas namakan pihak bank		1. Phising : Tindakan memperoleh informasi pribadi seperti user id, nomor rekening bank/no kartu kredit secara tidak sah 2. tidak peduli dengan keamanan data pribadi
3	Peraturan perundangan yang berlaku		Ketaatan terhadap peraturan perundangan yang berlaku terkait layanan mobile banking
4	Layanan Prima	Memberikan layanan prima yang menggunakan teknologi IT	

II. Kebutuhan Pemangku Kepentingan

Pihak yang berkepentingan dalam pengelolaan Layanan Mobile Banking dalam rangka mendukung Layanan Pelanggan berbasis elektronik diantaranya adalah:

Tabel 2. Stakeholder terkait

No	Pemangku Kepentingan	Harapan	Kebutuhan
1	Nasabah	Aplikasi aman namun mudah digunakan	Transaksi keuangan
2	Bank/ Organisasi Financial lain	Transaksi antar bank lancar dan aman	Transaksi keuangan lintas bank
3	Developer aplikasi	Aplikasi dapat berjalan dengan baik tanpa error	Membuat aplikasi dengan mudah
4	Tim infrastruktur TI	Infrastruktur dapat memfasilitasi semua permintaan trafik aplikasi	Menyediakan infrastruktur untuk mendukung kinerja aplikasi
5	Infrastruktur TI external (AWS)	Infrastruktur outsourcing dapat memfasilitasi semua permintaan trafik aplikasi yang diminta	Menyediakan infrastruktur tambahan untuk mendukung kinerja aplikasi

III. Ruang Lingkup penerapan SMKI

Dalam menentukan ruang lingkup penerapan SMKI di Bank XYZ, telah dipertimbangkan terkait isu-isu internal dan eksternal sebagaimana tersebut dalam bab 2.1 sesuai dengan klausul 4.1 dan memahami kebutuhan pihak-pihak berkepentingan sebagaimana tersebut dalam bab 2.1 sesuai dengan klausul 4.2, bahwa dalam rangka lebih mendukung layanan kepada nasabah berbasis elektronik dimasa yang akan datang, maka akan diterapkan Sistem Manajemen keamanan informasi dilingkup BRIN secara bertahap mulai dari lingkup **Layanan Mobile Banking**, selanjutnya ke lingkup Layanan ATM,

lingkup internet banking, lingkup simpanan dalam bentuk deposito, lingkup simpanan dalam bentuk tabungan dan layanan pinjaman.

IV. Persyaratan hukum dan peraturan perundang undangan terkait SMKI

Dalam penerapan SMKI pada Bank XYZ juga mempertimbangkan beberapa regulasi peraturan perundang – udangan yang terkait.

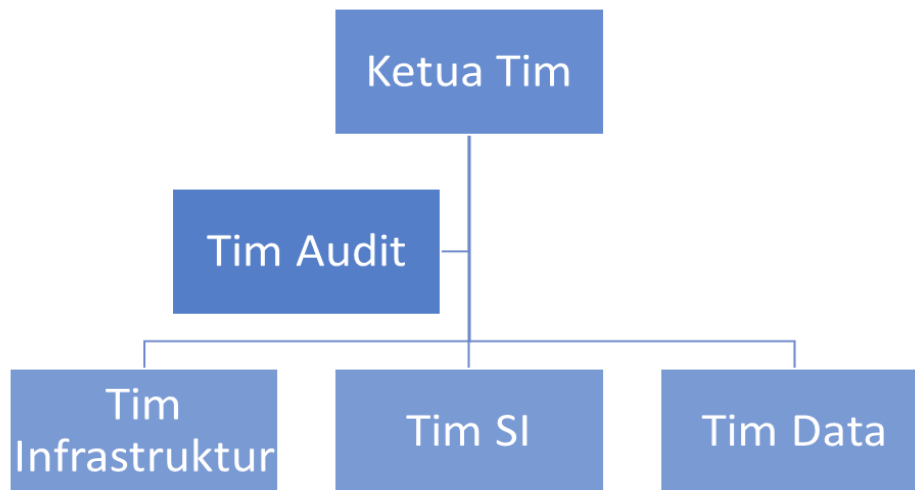
Tabel 3. Peraturan Perundangan – Undangan

No	Peraturan Perundangan	Tentang
1.	Undang - Undang Nomor 10 Tahun 1998	Undang - Undang tentang perbankan
2.	Undang-Undang Nomor 8 tahun 1999	Tentang Perlindungan Konsumen, merupakan segala upaya yang dilakukan untuk melindungi konsumen sekaligus dapat meletakkan konsumen dalam kedudukan yang seimbang dengan pelaku usaha. Termasuk tentang penyelesaian sengketa baik melalui pengadilan maupun diluar pengadilan
3.	Undang-Undang Nomor 3 tahun 2011	Tentang Transfer Dana yang melindungi nasabah terhadap transfer dana dari dan ke rekening nasabah melalui mobil banking
4.	Undang-Undang Nomor 19 tahun 2016	Tentang Informasi dan Transaksi Elektronik, terkait dengan para pihak yang melakukan kegiatan transaksi elektronik atau transaksi yang menggunakan mobile banking

5.	Peraturan Bank Indonesia Nomor 7/6/PBI/2005	Tentang Transparansi Informasi Produk Bank dan Penggunaan Data Pribadi Nasabah, mengatur bahwa bank wajib menerapkan transparansi informasi tentang produk bank dan penggunaan data pribadi nasabah.
6.	Peraturan Bank Indonesia Nomor 14/27/PBI/2012	<p>Tentang Penerapan Program Anti Pencucian Uang dan Pencegahan Pendanaan Terorisme Bagi Bank Umum, meliputi:</p> <ol style="list-style-type: none"> 1. Pengaturan mengenai transfer dana. 2. Pengaturan mengenai area berisiko tinggi. 3. Pengaturan Customer Due Dilligence (CDD) sederhana khususnya dalam rangka mendukung dengan strategi nasional dan global keuangan inklusif (financial inclusion). 4. Pengaturan mengenai Cross Border Correspondent Banking.
7.	Peraturan Otoritas Jasa Keuangan Nomor 1/POJK.07/2013	Tentang Perlindungan Konsumen Sektor Jasa Keuangan. Perlindungan Konsumen menerapkan prinsip transparansi, perlakuan yang adil, keandalan, kerahasiaan dan keamanan data/informasi. Bank wajib menyampaikan informasi tentang produk atau layanan yang akurat, jujur, dan tidak menyesatkan kepada nasabah.

8.	Peraturan Bank Indonesia Nomor 18/9/PBI/2016	Pengaturan dan Pengawasan Sistem Pembayaran dan Pengelolaan Uang Rupiah. Bank Indonesia selaku bank sentral melakukan pengaturan dan pengawasan sistem pembayaran dan pengelolaan uang rupiah.
9.	Peraturan Otoritas Jasa Keuangan Nomor 38/POJK.03/2016	Penerapan Manajemen Risiko Dalam Penggunaan Teknologi Informasi oleh Bank Umum. Dimana bank yang menyelenggarakan kegiatan electronic banking wajib memenuhi peraturan terkait dan memberikan edukasi kepada nasabah mengenai produk electronic banking dan pengamanannya.
10.	Peraturan Otoritas Jasa Keuangan Nomor 12/POJK.03/2018	Penyelenggaraan Layanan Perbankan Digital oleh Bank Umum, bank wajib menerapkan manajemen risiko, prinsip kehati-hatian
11.	Peraturan Otoritas Jasa Keuangan Nomor 18/POJK.07/2018	Layanan Pengaduan Konsumen di Sektor Jasa Keuangan, bank wajib menjamin terselenggarakannya mekanisme penyelesaian pengaduan nasabah secara efektif dalam jangka waktu yang memadai.

V. Organisasi / Struktur Organisasi SMKI



Gambar 1. Struktur Tim SMKI

Tabel 4. Peran dan Tanggung Jawab

No	Peran	Tanggung Jawab
1.	Ketua Tim	1. Memberikan arahan dan masukan terkait penerapan SMKI 2. Menyediakan sumber daya bagi penerapan SMKI dalam layanan mobile banking 3. Memantau pengukuran efektifitas kontrol implementasi SMKI 4. Memberikan laporan mengenai pelaksanaan SMKI
2.	Tim Audit	1. Melakukan audit internal TIK terhadap layanan mobile banking secara berkala 2. Mengajukan saran atas tindakan perbaikan yang harus dilakukan. 3. Membuat laporan internal audit
3.	Tim Infrastruktur	1. Mengembangkan infrastruktur yang mendukung layanan mobile banking

		2. Melakukan pemeliharaan infrastruktur 3. Memastikan seluruh perangkat TIK dikelola dan dimanfaatkan secara efektif dan efisien
4.	Tim SI	1. Mengembangkan aplikasi mobile banking 2. Melakukan maintenance aplikasi
5.	Tim Data	1. Mengelola data transaksi dan pelanggan 2. Memastikan perbaikan dan peredaran dokumen SMKI dilakukan oleh pihak yang berwenang sesuai standar dan regulasi yang berlaku

VI. Kebijakan dan Komitmen SMKI

Manajemen Bank XYZ berkomitmen untuk:

1. memastikan kebijakan keamanan informasi dan sasaran keamanan informasi ditetapkan dan selaras dengan Visi Misi Bank XYZ “**Menjadi The Most Valuable Banking Group di Asia Tenggara and Champion of Financial Inclusion**”;
2. memastikan persyaratan SMKI terintegrasi ke dalam proses bisnis yang berlaku;
3. memastikan tersedianya sumber daya yang dibutuhkan untuk SMKI;
4. mengomunikasikan pentingnya manajemen keamanan informasi yang efektif dan kesesuaian dengan persyaratan SMKI;
5. memastikan bahwa SMKI mencapai manfaat yang diharapkan;
6. memberikan arahan dan dukungan pada personel untuk berkontribusi dalam efektivitas SMKI;
7. mempromosikan perbaikan berkelanjutan; dan
8. mendukung peran serta staff yang relevan untuk menunjukkan kepemimpinannya ketika diterapkan pada wilayah tanggung jawabnya.

VII. Sasaran Sistem Manajemen Keamanan Informasi

Tabel 5. Sasaran SMKI Mobile Banking

No	Sasaran	KPI	Aktifitas pencapaian Kinerja	Indikator Pencapaian	Kebutuhan Sumber Daya	PIC	Jangka Waktu	Evaluasi
1	Kebijakan penerapan keamanan pada layanan mobile banking	Kebijakan penerapan SMKI	Penyusunan kebijakan dan dokumentasi	Sertifikasi ISO 27001	Seluruh organisasi	Ketua Tim	1 Tahun	Sertifikasi
			Pelaksanaan kegiatan operasional sesuai dengan prosedur					
2	Pelanggan memahami prosedur keamanan penggunaan mobile banking	Kesalahan transaksi pelanggan	Menyusun media campaign untuk prosedur terkait	Kesalahan transaksi < 0,05%	Pelanggan, Tim SI, Tim Layanan Pelanggan	Ketua Tim	1 Tahun	Laporan per triwulan
			Membuat double authentication pada transaksi pelanggan					
			Membuat beberapa proses pengamanan (otomatis logout, permintaan perubahan password berjangka)					
3	Manajemen keamanan sistem yang handal	Percobaan pelanggaran hak akses	Pengujian sistem	Keberhasilan pelanggaran hak akses < 0,05%	Tim SI, Tim Infrastruktur, Tim Data	Ketua Tim	1 Tahun	Laporan per triwulan
			Menyusun prosedur layanan keamanan					

4	Kinerja sistem yang handal	Kinerja mobile banking	Audit TIK	Kinerja sistem > 99,95 %	Seluruh organisasi	Tim Audit	1 Tahun	Laporan hasil audit
---	----------------------------	------------------------	-----------	--------------------------	--------------------	-----------	---------	---------------------

VIII. Komunikasi Informasi

Komunikasi dibagi menjadi 2, komunikasi internal dan komunikasi eksternal. Komunikasi internal organisasi merupakan proses penyampaian informasi antara pegawai untuk memastikan setiap informasi yang berhubungan dengan pelaksanaan sistem manajemen layanan sampai kepada pihak yang tepat. Komunikasi eksternal organisasi merupakan komunikasi antara Bank XYZ dengan pihak di luar Bank XYZ.

Tabel 6. Komunikasi Kebijakan SMKI

No	Materi Komunikasi	Periode Komunikasi	Target Penerima	Bentuk Komunikasi	PIC
1	Kebijakan SMKI umum	Setiap Tahun	Seluruh Stakeholder	Pemberitahuan di dalam web	Ketua Tim
2	Keamanan data nasabah	Setiap Tahun	Seluruh pegawai perbankan	Sosialisasi	Ketua Tim
3	Awareness tentang clean desk policy	Setiap Tahun	Seluruh pegawai perbankan	Sosialisasi	Ketua Tim
4	Keamanan Password	Setiap Tahun	Pelanggan	1. Sosialisasi 2. Flyer/pengumuman di web	Ketua Tim
5	Awareness terhadap prosedur email	Setiap Tahun	Seluruh pegawai perbankan	1. Sosialisasi 2. Pamflet/blast email ke pelanggan	Ketua Tim

IX. Kebutuhan Sumber Daya dan Kompetensinya

Managemen Bank XYZ memiliki komitmen untuk menyediakan dan mengelola sumber daya manusia yang dibutuhkan untuk penetapan, penerapan, pemeliharaan dan perbaikan berkelanjutan terhadap SMKI,

dalam rangka menjaga efektifitas keamanan informasi terkait dengan perencanaan mitigasi risiko dan pelaksanaan kontrol keamanan informasi. Untuk mendapatkan SDM yang handal, telah ditentukan persyaratan minimal yang harus dipenuhi oleh personel yang menangani SMKI. Tata cara dan persyaratan rekrutmen tersebut dapat dilihat pada prosedur pengelolaan SDM. Untuk meningkatkan kompetensi personel, manajemen memiliki komitmen yang tinggi dengan mengalokasikan dana dan waktu bagi pelaksanaan Pendidikan / pelatihan teknis bagi pegawai termasuk untuk pegawai yang menangani SMKI, memastikan tercapainya kompetensi yang dibutuhkan dan melaksanakan tugas-tugas yang diperlukan. Tim SMKI merekam seluruh data terkait kompetensi pegawai.

Tabel 7. Kompetensi

No	Peran	Kompetensi
1	Ketua Tim	<ol style="list-style-type: none"> 1. Pendidikan minimal S1 2. Mempunyai keahlian di bidang manajerial 3. Mempunyai pengalaman sebagai Project Manager menangani project yang berhubungan dengan project-project di bidang Finance dan Banking minimal 5 tahun 4. Memiliki Sertifikat PMP 5. Memiliki awareness ISO 27001
2	Tim Audit	<ol style="list-style-type: none"> 1. Pendidikan minimal S1 2. Memiliki sertifikasi CISA 3. Memiliki pengalaman sebagai IT Auditor minimal 5 tahun 4. Memiliki kemampuan analisa, investigasi dan komunikasi yang baik 5. Mempunyai pengalaman dalm bidang audit perbankan minimal 5 Tahun 6. Memiliki awareness ISO 27001
3	Tim SI	<ol style="list-style-type: none"> 1. Pendidikan minimal S1 bidang SI/IT 2. Mengusai bahasa pemrograman Java/Kotlin 3. Pengalaman minimal 2 Tahun untuk developing enterprise-scale mobile solutions 4. Mampu membaca spesifikasi pekerjaan dan mengimplementasikannya dalam kode program

4	Tim Infrastruktur	<ol style="list-style-type: none"> 1. Pendidikan minimal S1 bidang SI/IT 2. Menguasai perangkat security jaringan (firewall, IPS, WAF, dll) 3. Pengalaman minimal 2 Tahun di jaringan komputer LAN/Wireless LAN, sistem operasi Windows dan Linux, Perangkat Router (Mikrotik/Juniper), Perangkat Switching, Perangkat DSLAM/OLT
5	Tim Data	<ol style="list-style-type: none"> 1. Pendidikan minimal S1 bidang SI/IT 2. Mempunyai sertifikasi terkait pengelolaan data transaksi dan pelanggan 3. Mampu mengelola data ETL (Extraction, Transform, and Load) untuk Data Warehouse 4. Menguasai DBA (Oracle, SQLServer, SQLReplication, ETL, DB Tuning, DB Optimized, Troubleshoot)




PANDUAN SISTEM MANAJEMEN KEAMANAN INFORMASI BANK XYZ



**Maysarah
Mumami
Sari Andarwati
Muh Shamad**

**BANK XYZ
2022**

LEMBAR PENGESAHANAN PANDUAN SISTEM KEAMANAN INFORMASI
BANK XYZ

Nomor Dokumen	: 01/TIK.02.K.SMKI/14/2022	
Versi	: 1	
Tanggal Ditetapkan	: 1 Maret 2022	
Tanggal Ditinjau Kembali	: 1 Maret 2023	
Diperiksa oleh:		
Tim Layanan Mobile	Kepala Layanan TIK dan Informasi	Direktur Utama PT Bank XYZ
		
Ratna	Adi	Musa Alfonso
Catatan : 1. Jika versi terbaru telah diterbitkan, maka versi sebelumnya ditetapkan tidak berlaku. 2. Versi terbaru terdapat dalam bentuk elektronik.		

RIWAYAT DOKUMEN

Versi	Tanggal	Penulis	Deskripsi
1	1 Februari 2022	Tim Layanan Mobile	Dokumen awal
2	20 Maret 2022	Tim Audit	Perubahan klausul audit internal

PERNYATAAN KERAHASIAAN

Informasi dalam dokumen ini adalah milik Layanan Mobile Banking Bank XYZ. Tim Layanan membuat dokumen ini dengan pemahaman bahwa dokumen ini akan dijaga kerahasiaannya dan tidak akan diungkapkan, digandakan, atau digunakan, baik keseluruhan maupun sebagian, untuk tujuan apapun tanpa persetujuan tertulis sebelumnya.

Daftar Isi

LEMBAR PENGESAHANAN PANDUAN SISTEM KEAMANAN INFORMASI	ii
BANK XYZ	ii
RIWAYAT DOKUMEN.....	3
PERNYATAAN KERAHASIAAN	4
1. Pendahuluan	3
2. Konteks Organisasi	3
2.1 Organisasi dan Konteks	3
2.2 Kebutuhan dan Harapan	8
2.3 Ruang Lingkup Penerapan SMKI.....	8
2.4 Sistem Manajemen Keamanan Informasi	8
3. Kepemimpinan	8
3.1 Komitmen Manajemen	8
3.2 Kebijakan.....	9
3.3 Organisasi SMKI (Peran, Tanggung Jawab, dan Wewenang)	9
4. Sasaran Keamanan Informasi	10
5. Dukungan	12
5.1 Sumber Daya	12
5.2 Kompetensi dan Kepedulian	12
5.3 Komunikasi	13
5.4 Pengendalian Dokumen dan Rekaman	14
6. Operasi.....	14
6.1 Perencanaan dan Pengendalian Operasional.....	14
6.2 Penilaian Risiko Keamanan Informasi	14
6.3 Penanganan Risiko Keamanan Informasi	15
7. Evaluasi Kinerja	15
7.1 Pemantauan, Pengukuran, Analisis, dan Evaluasi	15
7.2 Audit Internal	15
7.3 Kaji Ulang Manajemen	16
8. Perbaikan	16

8.1 Ketidaksesuaian dan Tindakan Korektif	16
8.2 Perbaikan Berkelanjutan	16

PANDUAN SISTEM MANAJEMEN KEAMANAN INFORMASI

BANK XYZ

1. Pendahuluan

Informasi dalam bentuk elektronik dan non elektronik merupakan elemen kritis di lingkungan Bank XYZ dalam rangka menjalankan proses bisnis yang memanfaatkan Teknologi Informasi dan Komunikasi (TIK) untuk memberikan layanan kepada nasabah. Oleh karena itu, untuk menjamin keamanan informasinya, Bank XYZ menerapkan Sistem Manajemen Keamanan Informasi (SMKI) yang terdiri dari 3 aspek yang menjadi fokus dalam penerapannya, yaitu :

1. Kerahasiaan (confidentiality) berupa informasi yang tidak diketahui atau tidak diungkapkan oleh pihak yang tidak berwenang,
2. Keabsahan (integrity) berupa akurasi dan kelengkapan informasi, serta
3. Ketersediaan (availability) berupa informasi yang selalu tersedia untuk diakses pada saat dibutuhkan.

Dokumen manual SMKI ini merupakan dokumen yang bertujuan untuk memberikan panduan dalam membangun, mengimplementasikan, melaksanakan, memelihara, dan meningkatkan SMKI di lingkungan Bank XYZ berdasarkan standar ISO/IEC 27000-1:2022 tentang Information Security Management System (ISMS) – Requirements.

2. Konteks Organisasi

2.1 Organisasi dan Konteks

Ruang lingkup penerapan SMKI pada Layanan Mobile Banking Bank XYZ dipengaruhi oleh isu internal dan eksternal sebagaimana pada table dibawah.

No	Issue	Internal	Eksternal
1	Pencurian Saldo nasabah	Lemahnya internal control	
		Masalah SDM	
2	Penipuan yang mengatas namakan pihak bank		1. Phising : Tindakan memperoleh informasi pribadi seperti user id, nomor rekening bank/no kartu kredit secara tidak sah 2. tidak peduli dengan keamanan data pribadi
3	Peraturan perundangan yang berlaku		Ketaatan terhadap peraturan perundangan yang berlaku terkait layanan mobile banking
4	Layanan Prima	Memberikan layanan prima yang menggunakan teknologi IT	

Pihak yang berkepentingan dalam pengelolaan Layanan Mobile Banking dalam rangka mendukung Layanan Pelanggan berbasis elektronik diantaranya adalah:

No	Pemangku Kepentingan	Harapan	Kebutuhan
1	Nasabah	Aplikasi aman namun mudah digunakan	Transaksi keuangan

2	Bank/ Organisasi Financial lain	Transaksi antar bank lancar dan aman	Transaksi keuangan lintas bank
3	Developer aplikasi	Aplikasi dapat berjalan dengan baik tanpa error	Membuat aplikasi dengan mudah
4	Tim infrastruktur TI	Infrastruktur dapat memfasilitasi semua permintaan trafik aplikasi	Menyediakan infrastruktur untuk mendukung kinerja aplikasi
5	Infrastruktur TI external (AWS)	Infrastruktur outsourcing dapat memfasilitasi semua permintaan trafik aplikasi yang diminta	Menyediakan infrastruktur tambahan untuk mendukung kinerja aplikasi

Dalam penerapan SMKI pada Bank XYZ juga mempertimbangkan beberapa regulasi peraturan perundang – undangan yang terkait,

No	Peraturan Perundangan	Tentang
1.	Undang - Undang Nomor 10 Tahun 1998	Undang - Undang tentang perbankan
2.	Undang-Undang Nomor 8 tahun 1999	Tentang Perlindungan Konsumen, merupakan segala upaya yang dilakukan untuk melindungi konsumen sekaligus dapat meletakkan konsumen dalam kedudukan yang seimbang dengan pelaku usaha. Termasuk tentang penyelesaian sengketa baik melalui pengadilan maupun diluar pengadilan
3.	Undang-Undang Nomor 3 tahun 2011	Tentang Transfer Dana yang melindungi nasabah terhadap transfer dana dari dan ke rekening nasabah melalui mobil banking
4.	Undang-Undang Nomor 19 tahun 2016	Tentang Informasi dan Transaksi Elektronik, terkait dengan para pihak yang melakukan kegiatan transaksi elektronik atau transaksi yang menggunakan mobile banking
5.	Peraturan Bank Indonesia Nomor 7/6/PBI/2005	Tentang Transparansi Informasi Produk Bank dan Penggunaan Data Pribadi Nasabah, mengatur bahwa bank wajib menerapkan transparansi informasi tentang produk bank dan penggunaan data pribadi nasabah.
6.	Peraturan Bank Indonesia Nomor 14/27/PBI/2012	Tentang Penerapan Program Anti Pencucian Uang dan Pencegahan Pendanaan Terorisme Bagi Bank Umum, meliputi: 1. Pengaturan mengenai transfer dana. 2. Pengaturan mengenai area berisiko tinggi. 3. Pengaturan Customer Due Dilligence (CDD) sederhana khususnya dalam rangka mendukung

		<p>dengan strategi nasional dan global keuangan inklusif (financial inclusion).</p> <p>4. Pengaturan mengenai Cross Border Correspondent Banking.</p>
7.	Peraturan Otoritas Jasa Keuangan Nomor 1/POJK.07/2013	<p>Tentang Perlindungan Konsumen Sektor Jasa Keuangan. Perlindungan Konsumen menerapkan prinsip transparansi, perlakuan yang adil, keandalan, kerahasiaan dan keamanan data/informasi. Bank wajib menyampaikan informasi tentang produk atau layanan yang akurat, jujur, dan tidak menyesatkan kepada nasabah.</p>
8.	Peraturan Bank Indonesia Nomor 18/9/PBI/2016	<p>Pengaturan dan Pengawasan Sistem Pembayaran dan Pengelolaan Uang Rupiah. Bank Indonesia selaku bank sentral melakukan pengaturan dan pengawasan sistem pembayaran dan pengelolaan uang rupiah.</p>
9.	Peraturan Otoritas Jasa Keuangan Nomor 38/POJK.03/2016	<p>Penerapan Manajemen Risiko Dalam Penggunaan Teknologi Informasi oleh Bank Umum. Dimana bank yang menyelenggarakan kegiatan electronic banking wajib memenuhi peraturan terkait dan memberikan edukasi kepada nasabah mengenai produk electronic banking dan pengamanannya.</p>
10.	Peraturan Otoritas Jasa Keuangan Nomor 12/POJK.03/2018	<p>Penyelenggaraan Layanan Perbankan Digital oleh Bank Umum, bank wajib menerapkan manajemen risiko, prinsip kehati-hatian</p>
11.	Peraturan Otoritas Jasa Keuangan Nomor 18/POJK.07/2018	<p>Layanan Pengaduan Konsumen di Sektor Jasa Keuangan, bank wajib menjamin terselenggarakannya mekanisme penyelesaian pengaduan nasabah secara efektif dalam jangka waktu yang memadai.</p>

2.2 Kebutuhan dan Harapan

2.3 Ruang Lingkup Penerapan SMKI

Dalam menentukan ruang lingkup penerapan SMKI di Bank XYZ, telah dipertimbangkan terkait isu-isu internal dan eksternal sebagaimana tersebut dalam bab 2.1 sesuai dengan klausul 4.1 dan memahami kebutuhan pihak-pihak berkepentingan sebagaimana tersebut dalam bab 2.1 sesuai dengan klausul 4.2, bahwa dalam rangka lebih mendukung layanan kepada nasabah berbasis elektronik dimasa yang akan datang, maka akan diterapkan Sistem Manajemen keamanan informasi dilingkup Bank XYZ secara bertahap mulai dari lingkup **Layanan Mobile Banking**, selanjutnya ke lingkup Layanan ATM, lingkup internet banking, lingkup simpanan dalam bentuk deposito, lingkup simpanan dalam bentuk tabungan dan layanan pinjaman.

2.4 Sistem Manajemen Keamanan Informasi

Tim Mobile Banking berkomitmen menetapkan, menerapkan, memelihara dan memperbaiki secara berkelanjutan SMKI, sesuai dengan yang dipersyaratkan SNI ISO-IEC 27001. Penerapan SMKI dilakukan integrasi bersama dengan Sistem Manajemen lain yang diterapkan serta regulasi peraturan perundang undangan yang berlaku. Penerapan SMKI dilaksanakan berdasarkan proses P-D-C-A (Plan-Do-Check-Act) terhadap seluruh proses bisnis.

3. Kepemimpinan

3.1 Komitmen Manajemen

Manajemen Bank XYZ berkomitmen untuk:

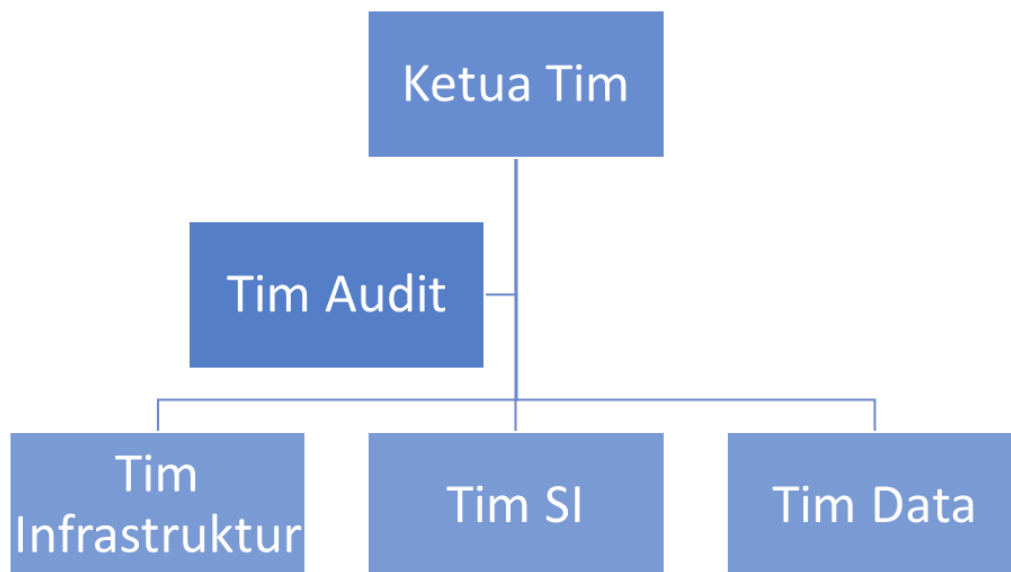
1. memastikan kebijakan keamanan informasi dan sasaran keamanan informasi ditetapkan dan selaras dengan Visi Misi Bank XYZ “**Menjadi The Most Valuable Banking Group dan Champion of Financial Inclusion**”;
2. memastikan persyaratan SMKI terintegrasi ke dalam proses bisnis yang berlaku;
3. memastikan tersedianya sumber daya yang dibutuhkan untuk SMKI;
4. mengomunikasikan pentingnya manajemen keamanan informasi yang efektif dan kesesuaian dengan persyaratan SMKI;
5. memastikan bahwa SMKI mencapai manfaat yang diharapkan;
6. memberikan arahan dan dukungan pada personel untuk berkontribusi dalam efektivitas SMKI;
7. mempromosikan perbaikan berkelanjutan; dan
8. mendukung peran serta staff yang relevan untuk menunjukkan kepemimpinannya ketika diterapkan pada wilayah tanggung jawabnya.

3.2 Kebijakan

Menetapkan kebijakan Manajemen Keamanan Informasi sebagai berikut:

1. Seluruh aset dan informasi di layanan mobile banking harus dilindungi dari segala bentuk ancaman dari aspek kerahasiaan (Confidentiality), keabsahan (Integrity) dan ketersediaan (Availability).
2. Manajemen, pegawai dan seluruh pihak yang terlibat, harus mengetahui dan mematuhi kebijakan manajemen keamanan informasi ini.
3. Manajemen dan Tim Mobile Banking harus memastikan terpenuhinya Sasaran Manajemen Keamanan Informasi.
4. Kebijakan dan prosedur SMKI harus disosialisasikan.
5. Manajemen menyediakan dan menjamin sumber daya yang diperlukan untuk penerapan SMKI.
6. Seluruh kegiatan SMKI harus dilakukan pemantauam, pengukuran dan evaluasi secara berkala untuk perbaikan berkelanjutan dalam kegiatan audit baik internal maupun eksternal dan kaji ulang manajemen.
7. Setiap pelanggaran yang dilakukan atas Kebijakan Manajemen Keamanan Informasi akan dikenai sanksi dan/atau penindakan disiplin sesuai dengan peraturan yang berlaku.

3.3 Organisasi SMKI (Peran, Tanggung Jawab, dan Wewenang)



No	Peran	Tanggung Jawab
1.	Ketua Tim	<ol style="list-style-type: none"> 1. Memberikan arahan dan masukan terkait penerapan SMKI 2. Menyediakan sumber daya bagi penerapan SMKI dalam layanan mobile banking 3. Memantau pengukuran efektifitas kontrol implementasi SMKI 4. Memberikan laporan mengenai pelaksanaan SMKI
2.	Tim Audit	<ol style="list-style-type: none"> 1. Melakukan audit internal TIK terhadap layanan mobile banking secara berkala 2. Mengajukan saran atas tindakan perbaikan yang harus dilakukan. 3. Membuat laporan internal audit
3.	Tim Infrastruktur	<ol style="list-style-type: none"> 1. Mengembangkan infrastruktur yang mendukung layanan mobile banking 2. Melakukan pemeliharaan infrastruktur 3. Memastikan seluruh perangkat TIK dikelola dan dimanfaatkan secara efektif dan efisien
4.	Tim SI	<ol style="list-style-type: none"> 1. Mengembangkan aplikasi mobile banking 2. Melakukan maintenance aplikasi
5.	Tim Data	<ol style="list-style-type: none"> 1. Mengelola data transaksi dan pelanggan 2. Memastikan perbaikan dan peredaran dokumen SMKI dilakukan oleh pihak yang berwenang sesuai standar dan regulasi yang berlaku

4. Sasaran Keamanan Informasi

Sasaran dalam implementasi SMKI dalam rangka mencapai tingkat keamanan yang memadai dapat dilihat dalam dokumen Quality Objective SMKI sebagai berikut:

N o	Sasaran	KPI	Aktifitas pencapaian Kinerja	Indikator Pencapaian	Kebutuhan Sumber Daya	PIC	Jangka Waktu	Evaluasi
1	Kebijakan penerapan keamanan pada layanan mobile banking	Kebijakan penerapan SMKI	Penyusunan kebijakan dan dokumentasi Pelaksanaan kegiatan operasional sesuai dengan prosedur	Sertifikasi ISO 27001	Seluruh organisasi	Ketua Tim	1 Tahun	Sertifikasi
2	Pelanggan memahami prosedur keamanan penggunaan mobile banking	Kesalahan transaksi pelanggan	Menyusun media campaign untuk prosedur terkait Membuat double authentication pada transaksi pelanggan Membuat beberapa proses pengamanan (otomatis logout, permintaan perubahan password berjangka)	Kesalahan transaksi < 5%	Pelanggan, Tim SI, Tim Layanan Pelanggan	Ketua Tim	1 Tahun	Laporan per triwulan
3	Manajemen keamanan sistem yang handal	Percobaan pelanggaran hak akses	Pengujian sistem Menyusun prosedur layanan keamanan	Keberhasilan pelanggaran hak akses < 0,5%	Tim SI, Tim Infrastruktur, Tim Data	Ketua Tim	1 Tahun	Laporan per triwulan
4	Kinerja sistem yang handal	Kinerja mobile banking	Audit TIK	Kinerja sistem > 99 %	Seluruh organisasi	Tim Audit	1 Tahun	Laporan hasil audit

5. Dukungan

5.1 Sumber Daya

Manajemen harus mengalokasikan anggaran, peralatan dan perlengkapan kerja, serta personil sumber daya manusia yang kompeten bagi penerapan, pemeliharaan dan perbaikan berkelanjutan terhadap SMKI layanan mobile banking.

5.2 Kompetensi dan Kepedulian

Manajemen Bank XYZ memiliki komitmen untuk menyediakan dan mengelola sumber daya manusia yang dibutuhkan untuk penetapan, penerapan, pemeliharaan dan perbaikan berkelanjutan terhadap SMKI, dalam rangka menjaga efektifitas keamanan informasi terkait dengan perencanaan mitigasi risiko dan pelaksanaan kontrol keamanan informasi.

Untuk mendapatkan SDM yang handal, telah ditentukan persyaratan minimal yang harus dipenuhi oleh personel yang menangani SMKI. Tata cara dan persyaratan rekrutmen tersebut dapat dilihat pada prosedur pengelolaan SDM. Untuk meningkatkan kompetensi personel, manajemen memiliki komitmen yang tinggi dengan mengalokasikan dana dan waktu bagi pelaksanaan Pendidikan / pelatihan teknis/ sertifikasi bagi pegawai yang menangani SMK. Tim SMKI harus merekam seluruh data terkait kompetensi pegawai

No	Peran	Kompetensi
1	Ketua Tim	<ol style="list-style-type: none">1. Pendidikan minimal S12. Mempunyai keahlian di bidang manajerial3. Mempunyai pengalaman sebagai Project Manager menangani project yang berhubungan dengan project-project di bidang Finance dan Banking minimal 5 tahun4. Memiliki Sertifikat PMP
2	Tim Audit	<ol style="list-style-type: none">1. Pendidikan minimal S12. Memiliki sertifikasi CISA3. Memiliki pengalaman sebagai IT Auditor minimal 5 tahun4. Memiliki kemampuan analisa, investigasi dan komunikasi yang baik5. Mempunyai pengalaman dalm bidang audit perbankan minimal 5 Tahun

3	Tim SI	<ol style="list-style-type: none"> 1. Pendidikan minimal S1 bidang SI/IT 2. Mengusai bahasa pemrograman Java/Kotlin 3. Pengalaman minimal 2 Tahun untuk developing enterprise-scale mobile solutions 4. Mampu membaca spesifikasi pekerjaan dan mengimplementasikannya dalam kode program
4	Tim Infrastruktur	<ol style="list-style-type: none"> 1. Pendidikan minimal S1 bidang SI/IT 2. Mengusai perangkat security jaringan (firewall, IPS, WAF, dll) 3. Pengalaman minimal 2 Tahun di jaringan komputer LAN/Wireless LAN, sistem operasi Windows dan Linux, Perangkat Router (Mikrotik/Juniper), Perangkat Switching, Perangkat DSLAM/OLT
5	Tim Data	<ol style="list-style-type: none"> 1. Pendidikan minimal S1 bidang S1/TI 2. Mempunyai sertifikasi terkait pengelolaan data transaksi dan pelanggan 3. Mampu mengelola data ETL (Extraction, Transform, and Load) untuk Data Warehouse 4. Mengusai DBA (Oracle, SQLServer, SQLReplication, ETL, DB Tuning, DB Optimized, Troubleshoot)

5.3 Komunikasi

Komunikasi dibagi menjadi 2, komunikasi internal dan komunikasi eksternal. Komunikasi internal organisasi merupakan proses penyampaian informasi antara pegawai untuk memastikan setiap informasi yang berhubungan dengan pelaksanaan sistem manajemen layanan sampai kepada pihak yang tepat. Komunikasi eksternal organisasi merupakan komunikasi antara Bank XYZ dengan pihak di luar Bank XYZ.

No	Materi Komunikasi	Periode	Target Penerima	Bentuk Komunikasi	PIC
Komunikasi					
1	Kebijakan SMKI umum	Setiap Tahun	Seluruh Stakeholder	Pemberitahuan di dalam web	Ketua Tim
2	Keamanan data nasabah	Setiap Tahun	Seluruh pegawai perbankan	Sosialisasi	Ketua Tim
3	Awareness tentang clean desk policy	Setiap Tahun	Seluruh pegawai perbankan	Sosialisasi	Ketua Tim
4	Keamanan Password	Setiap Tahun	Pelanggan	<ol style="list-style-type: none"> 1. Sosialisasi 2. Flyer/pengumuman di web 	Ketua Tim

5	Awareness terhadap prosedur email	Setiap Tahun	Seluruh pegawai perbankan	1. Sosialisasi 2. Pamflet/blast email ke pelanggan	Ketua Tim
---	-----------------------------------	--------------	---------------------------	---	-----------

5.4 Pengendalian Dokumen dan Rekaman

Pada implementasi SMKl membutuhkan perangkat dokumen yang berisi aturan – aturan untuk memastikan bahwa proses SMKl dilaksanakan secara konsisten. Dokumen pada SMKl dibagi menjadi :

1. Dokumen Level 1 berupa Panduan Mutu
2. Dokumen Level 2 berupa Prosedur
3. Dokumen Level 3 berupa Instruksi kerja
4. Dokumen Level 4 berupa Formulir

Dokumen yang digunakan dalam implementasi SMKl harus dilindungi dan dikendalikan. Proses pengendalian meliputi indentifikasi, penyimpanan dokumen, distribusi dokumen, dan penghapusan dokumen.

6. Operasi

6.1 Perencanaan dan Pengendalian Operasional

Perencanaan dan pengendalian operasional meliputi :

No.	Aspek	Periode	Metode
1.	Manajemen Risiko	Evaluasi setiap 1x dalam satu tahun	Risk register
2.	Manajemen Maintenance	Setiap bulan	Prosedur, IK, Formulir maintenance
3.	Manajemen insiden	Setiap bulan	Prosedur, IK, Formulir penanganan insiden

6.2 Penilaian Risiko Keamanan Informasi

Tim Mobile Banking melakukan penilaian risiko keamanan informasi secara rutin sesuai dengan waktu yang telah direncanakan atau ketika terjadi perubahan signifikan pada perencanaan. dengan mempertimbangkan kriteria yang ditetapkan.

Manajemen Risiko Keamanan Informasi diterapkan dengan hasil berupa :

1. Daftar Risiko
2. Rencana Pengendalian

6.3 Penanganan Risiko Keamanan Informasi

Prosedur untuk menangani risiko sesuai dengan risiko/kejadian yang terjadi harus ditetapkan untuk menjadi acuan. Setiap penanganan risiko keamanan informasi harus direkam dan rekamannya dipelihara untuk mejadi bahan evaluasi.

7. Evaluasi Kinerja

7.1 Pemantauan, Pengukuran, Analisis, dan Evaluasi

Ketua tim Bersama dengan tim audit melakukan Pemantauan, Pengukuran, Analisis, dan Evaluasi kinerja dan efektifitas penerapan SMKI secara berkala dengan beberapa ketentuan :

1. Menetapkan metode pelaksanaan Pemantauan, Pengukuran, Analisis, dan Evaluasi
2. Menetapkan periode pelaksanaan Pemantauan, Pengukuran, Analisis, dan Evaluasi
3. Hasil Pemantauan, Pengukuran, Analisis, dan Evaluasi dilaporkan kepada manajemen Bank XYZ
4. Kegiatan Pemantauan, Pengukuran, Analisis, dan Evaluasi harus direkam.

7.2 Audit Internal

Audit internal SMKI harus diadakan minimal 1 (satu) kali dalam setahun dengan mencakup keseluruhan ruang lingkup SMKI yang ditetapkan dalam dokumen ini dan dilaksanakan oleh Tim Internal Audit SMKI.

Tujuan pelaksanaan Audit Internal SMKI adalah

1. sesuai dengan:
 - a. persyaratan yang ditetapkan dalam penerapan SMKI
 - b. persyaratan Standar SNI ISO-IEC 27001
 - c. SMKI diimplementasikan dan dipelihara secara efektif.
2. mengeliminasi ketidaksesuaian dengan mengutamakan solusi pada penyebab utamanya.

Program audit dilakukan dengan mempertimbangkan pentingnya proses yang bersangkutan dan hasil audit sebelumnya.

7.3 Kaji Ulang Manajemen

Manajemen Bank XYZ wajib melakukan kaji ulang manajemen terhadap pelaksanaan SMKl dalam interval 1 tahun sekali untuk memastikan kesesuaian, kecukupan dan efektivitas. Hasil kaji ulang manajemen ini digunakan untuk mengevaluasi kondisi pelaksanaan keamanan informasi yang telah dilakukan dan menentukan peningkatan terhadap implementasi SMKl.

8. Perbaikan

8.1 Ketidaksesuaian dan Tindakan Korektif

Jika terjadi ketidaksesuaian harus diambil tindakan untuk mengendalikan dan mengoreksinya; dan menangani konsekuensinya. Selain itu juga harus dilakukan Tindakan untuk mengevaluasi kebutuhan tindakan untuk menghilangkan penyebab ketidaksesuaian, agar hal itu tidak terulang.

Tindakan korektif harus sesuai dengan efek dari ketidaksesuaian yang ditemui. Tim mobile banking merekam semua tindakan yang dilakukan untuk mengendalikan ketidaksesuaian dan tindakan berikutnya yang diambil, dan hasil dari setiap tindakan korektif.

8.2 Perbaikan Berkelanjutan

Manajemen harus memiliki komitmen untuk terus memperbaiki kesesuaian, kecukupan dan efektivitas SMKl, secara berkelanjutan meningkatkan efektivitas SMKl melalui pengguna kebijakan SMKl, objektif pengamanan informasi, hasil audit, analisis terhadap insiden, tindakan perbaikan dan pencegahan, serta kaji ulang manajemen.

Manajemen SMKl harus menentukan tindakan untuk menghilangkan penyebab dari insiden atau potensi insiden. Mekanisme dalam pelaksanaan tindakan perbaikan dan pencegahan terhadap ketidaksesuaian yang terjadi mengacu pada prosedur tindakan perbaikan dan pencegahan.

DAFTAR RISIKO
BANK XYZ

NO	ASET/PROSES/LAYANAN	DESKRIPSI RISIKO - DAMPAK (RISK DESCRIPTION - IMPACT)			RISIKO TANPA PENGENDALIAN (INHERENT RISK)			Risk owner	PENGENDALIAN YANG ADA (EXISTING CONTROL)	RISIKO SAAT INI (CURRENT RISK)			KEPUTUSAN	RENCANA PENANGGULANGAN (RISK TREATMENT PLAN)			Pemenuhan Annex	RISIKO SISA (RESIDUAL RISK)			KEPUTUSAN	RENCANA PENANGGULANGAN (RISK TREATMENT PLAN)			RISIKO SISA (RESIDUAL RISK)		
					Kemungkinan (Likelihood Scale)	Nilai Dampak (Impact Scale)	Nilai Risiko (Risk Score)			Kemungkinan (Likelihood)	Nilai Dampak (Impact Score)	Nilai Risiko (Risk Score)		Uraian	Kemungkinan (Likelihood)	Nilai Dampak (Impact Score)		Nilai Risiko (Risk Score)	Uraian	Kemungkinan (Likelihood)		Nilai Dampak (Impact Score)	Nilai Risiko (Risk Score)				
		Kerawanan (Vulnerability)	Ancaman CIA (Threat)	Uraian Dampak (Impact Description)																							
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	
1	Proses : Transaksi Pelanggan	Pelanggan gagal melakukan transaksi karena kurang efisiennya algoritma dalam pemrograman atau gangguan jaringan internet	L, A	1. Kepuasan pelanggan menurun 2. Reputasi bank mengalami penurunan	Sering Terjadi	Signifikan	Tinggi (19)	Bagian IT	Belum Ada	Sering Terjadi	Signifikan	Tinggi (19)	Mitigasi	1. Monitoring sistem layanan 2. Evaluasi kinerja		Jarang Terjadi	Signifikan	Sedang (13)	Mitigasi	Perbaikan/Update aplikasi berkala	Hampir Tidak Terjadi	Signifikan	Rendah (8)				
		Layanan pelanggan delay/mengalami keterlambatan	L, A	1. Kepuasan pelanggan menurun 2. Reputasi bank mengalami penurunan	Sering Terjadi	Tidak Signifikan	Rendah (6)	Bagian IT	Belum Ada	Sering Terjadi	Tidak Signifikan	Rendah (6)	Penerimaan														
2	Aset :Server	Internet server mengalami gangguan	A	Layanan terhenti sehingga pelanggan tidak bisa mengakses layanan mobile banking	Sering Terjadi	Signifikan	Tinggi (19)	Bagian IT	Belum Ada	Sering Terjadi	Signifikan	Tinggi (19)	Transfer	Backup		Jarang Terjadi	Signifikan	Sedang (13)	Mitigasi	Mirroring server	Hampir Tidak Terjadi	Signifikan	Rendah (8)				
		Gangguan/Kerusakan pada perangkat keras server	A	Layanan terhenti sehingga pelanggan tidak bisa mengakses layanan mobile banking	Jarang Terjadi	Signifikan	Sedang (13)	Bagian IT	Belum Ada	Jarang Terjadi	Signifikan	Sedang (13)	Transfer	1. Penggantian perangkat 2. Maintenance		Hampir Tidak Terjadi	Signifikan	Rendah (8)									
		Perangkat server dan storage tidak berfungsi	C, I, A	Terganggunya/terhentinya layanan/aplikasi yang beroperasi	Jarang Terjadi	Signifikan	Sedang (13)	Bagian IT	Belum Ada	Jarang Terjadi	Signifikan	Sedang (13)	Mitigasi	1. Maintenance pada perangkat server dan storage 2. Manajemen kapasitas server dan storage agar tidak melebihi ambang batas 3. Maintenance sistem operasi 5. Update Firmware perangkat storage		Hampir Tidak Terjadi	Signifikan	Rendah (8)									
3	Proses : Transaksi Pelanggan	Akun pelanggan mengalami Phising	C, I, A	1. Pelanggan mengalami kerugian finansial 2. Reputasi bank mengalami penurunan	Sering Terjadi	Signifikan	Tinggi (19)	Helpdesk, Bagian IT	Sosialisasi dan Awareness kepada pelanggan	Kadang - Kadang Terjadi	Signifikan	Tinggi (17)	Mitigasi	Incident Respon Plan (IRP) dan Incident Handling		Jarang Terjadi	Signifikan	Sedang (13)	Mitigasi	Double Authentication	Hampir Tidak Terjadi	Signifikan	Rendah (8)				
4	Pengelolaan antivirus	Antivirus dalam Server tidak update	C, I, A	Kehilangan data Penting di PC, yang terenkript seperti serangan Ransomware	Sering Terjadi	Signifikan	Tinggi (19)	Organisasi / Biro xxx	Belum Ada	Sering Terjadi	Signifikan	Tinggi (19)	Mitigasi	Prosedur Penanganan Antivirus	A.12.2.1 Kendali terhadap malware	Hampir Tidak Terjadi	Signifikan	Rendah (8)									

ISO/IEC 27001:2013 Statement of Applicability			Deskripsi Kontrol	(YA / TIDAK)	Justifikasi
Area	Section	Control			
A.5 Kebijakan keamanan informasi					
	A.5.1 Arahan manajemen untuk keamanan informasi	A.5.1.1 Kebijakan untuk keamanan informasi	Kendali Seperangkat kebijakan untuk keamanan informasi harus ditetapkan, disetujui oleh manajemen, diterbitkan dan dikomunikasikan kepada karyawan dan pihak luar yang terkait.	YA	Kebijakan telah dibuat yang tertuang pada Panduan Mutu.
		A.5.1.2 Reviu kebijakan keamanan informasi	Kendali Kebijakan untuk keamanan informasi harus direviu pada interval waktu terencana atau jika terjadi perubahan signifikan untuk memastikan kesesuaian, kecukupan dan keefektifan yang berkelanjutan	YA	Review telah dilakukan secara periodik 1 kali per tahun atau sewaktu-waktu jika dibutuhkan.
A.6 Organisasi keamanan informasi					
	A.6.1 Organisasi internal	A.6.1.1 Peran dan tanggung jawab keamanan informasi	Kendali Semua tanggung jawab keamanan informasi harus didefinisikan dan dialokasikan.	YA	Semua tanggung jawab keamanan informasi ditetapkan dan dialokasikan sesuai dengan Kebijakan dan Standar Sistem Manajemen Keamanan Informasi yang ditetapkan pada Panduan Mutu tentang Pengendalian Organisasi Keamanan Informasi dan SK No.34/BANKXYZ/I/2022 tentang Organisasi Keamanan Informasi
		A.6.1.2 Pemisahan tugas	Kendali Tugas dan area tanggung jawab yang bertentangan harus dipisahkan (dijabat oleh personel yang berbeda) untuk mengurangi kemungkinan dari modifikasi yang tidak sah atau tidak sengaja atau penyalahgunaan aset organisasi.	YA	Semua tanggung jawab keamanan informasi ditetapkan dan dialokasikan sesuai dengan Kebijakan dan Standar Sistem Manajemen Keamanan Informasi yang ditetapkan pada Panduan Mutu tentang Pengendalian Organisasi Keamanan Informasi dan SK No.34/BANKXYZ/I/2022 tentang Organisasi Keamanan Informasi
		A.6.1.3 Hubungan dengan pihak berwenang	Kendali Hubungan baik dengan pihak berwenang terkait harus dipelihara.	YA	- Sesuai dengan Kebijakan Sistem Manajemen Keamanan Informasi Top Manajemen menjaga hubungan dengan BI/Kemenkeu/OJK dengan melakukan komunikasi secara rutin/periodik paling tidak 1x dalam setahun atau saat dibutuhkan - Sesuai SK No.34/BANKXYZ/I/2022 tentang Organisasi Keamanan Informasi, masing - masing PIC mempunyai kontak dengan stakeholder
		A.6.1.4 Hubungan dengan kelompok minat khusus	Kendali Hubungan baik dengan komunitas, forum, dan asosiasi profesional spesialis keamanan harus dipelihara.	YA	Semua tanggung jawab keamanan informasi ditetapkan dan dialokasikan sesuai dengan Kebijakan dan Standar Sistem Manajemen Keamanan Informasi yang ditetapkan pada Panduan Mutu tentang Pengendalian Organisasi Keamanan Informasi
		A.6.1.5 Keamanan informasi dalam manajemen proyek	Kendali Keamanan informasi harus diterapkan ke dalam manajemen proyek, tanpa memperhatikan tipe proyeknya.	YA	- Pernyataan Menjaga Kerahasiaan (Non Disclosure Agreement) bagi personil yang melakukan akses informasi penting/rahasia - Risk Register - SOP No. 032/BANKXYZ/01/2022 - Pengelolaan Insiden
	A.6.2 Perangkat bergerak (mobile device) dan teleworking	A.6.2.1 Kebijakan perangkat bergerak	Kendali Kebijakan dan tindakan keamanan yang mendukung harus diadopsi untuk mengelola risiko yang terjadi akibat dari penggunaan perangkat bergerak.	YA	- Pengelolaan risiko mengacu kepada Kebijakan Pengelolaan Keamanan Informasi Bab manajemen risiko - Risk Register SMK
		A.6.2.2 Teleworking	Kendali Kebijakan dan tindakan keamanan yang mendukung harus diimplementasikan untuk melindungi informasi yang diakses, diproses atau disimpan di dalam situs teleworking.	YA	- Pelaksanaan teleworking mengacu kepada Kebijakan Pengelolaan Keamanan Informasi Bab Pengendalian Akses Terhadap Aset Informasi. - Pedoman teleworking berisi ketentuan mengenai ruang lingkup kegiatan teleworking, tata cara permohonan akses untuk kegiatan teleworking, dan aspek keamanan informasi yang harus diperhatikan oleh pelaksana kegiatan teleworking.

ISO/IEC 27001:2013 Statement of Applicability			Deskripsi Kontrol	(YA / TIDAK)	Justifikasi
Area	Section	Control			
A.7 Keamanan sumber daya manusia					
	A.7.1 Sebelum dipekerjakan	A.7.1.1 Penyaringan	Kendali Verifikasi latar belakang dari semua calon pegawai harus dilaksanakan berdasarkan hukum, regulasi dan etika terkait dan harus proporsional terhadap persyaratan bisnis, klasifikasi informasi yang akan diakses, dan risiko yang dipersepsikan.	Ya	Kebijakan telah dibuat berdasarkan panduan mutu terkait penyaringan pegawai
		A.7.1.2 Syarat dan ketentuan kepegawaian	Kendali Perjanjian tertulis dengan pegawai dan kontraktor harus menyatakan tanggung jawab keamanan informasi mereka dan organisasi.	Ya	Kebijakan dilaksanakan cara periode setiap awal tahun
	A.7.2 Selama bekerja	A.7.2.1 Management responsibilities	Kendali Manajemen harus mewajibkan semua pegawai dan kontraktor menerapkan keamanan informasi berdasarkan kebijakan dan prosedur organisasi yang sudah ditetapkan.	Ya	Setiap pegawai dan kontraktor menerapkan keamanan informasi berdasarkan pedoman yang telah ditetapkan
		A.7.2.2 Information security awareness, education and training	Kendali Semua pegawai organisasi dan kontraktor (jika relevan) harus menerima kepedulian, pendidikan, dan pelatihan yang memadai dan pemberitahuan secara berkala mengenai kebijakan dan prosedur organisasi, sesuai dengan fungsi kerja mereka.	Ya	Semua pegawai dan kontraktor wajib mengikuti semua kegiatan diklat yang telah ditetapkan sesuai ketentuan
		A.7.2.3 Disciplinary process	Kendali Harus ada proses pendisiplinan yang resmi dan terkomunikasikan terhadap penindakan pegawai yang melakukan pelanggaran keamanan informasi.	Ya	Semua aturan pendisiplinan terhadap penindakan pegawai harus dilakukan secara jelas dan terdokumentasi
	A.7.3 Penghentian dan perubahan kepegawaian	A.7.3.1 Termination or change of employment responsibilities	Kendali Setelah penghentian atau perubahan kepegawaian, tugas dan tanggung jawab keamanan informasi yang masih berlaku harus ditetapkan, dikomunikasikan kepada pegawai atau kontraktor, dan ditegakkan.	Ya	Semua informasi terkait setelah penghentian atau perubahan kepegawaian harus dibuat sesuai SK yang telah ditetapkan sebelumnya
A.8 Manajemen Aset					
	A.8.1 Tanggung jawab terhadap aset	A.8.1.1 Inventaris Aset	Kendali Aset yang berhubungan dengan informasi dan fasilitas pengolahan informasi harus diidentifikasi dan inventaris dari aset-aset ini harus dicatat dan dipelihara.	Ya	Dibuat suatu kebijakan terkait pemeliharaan aset
		A.8.1.2 Kepemilikan Aset	Kendali Aset yang dipelihara dalam inventaris harus dimiliki (ada personel yang bertanggung jawab).	Ya	Ditetapkan SK personal aset dan inventaris
		A.8.1.3 Penggunaan yang dapat diterima (acceptable use) atas aset	Kendali Aturan untuk penggunaan yang dapat diterima atas informasi dan aset yang berhubungan dengan informasi dan fasilitas pengolahan informasi harus diidentifikasi, didokumentasi dan diimplementasikan.	Ya	Ditetapkan aturan terkait informasi dan fasilitas pengolahan informasi aset dan inventaris
		A.8.1.4 Pengembalian aset	Kendali Semua pegawai dan pengguna pihak eksternal harus mengembalikan semua aset organisasi yang dikuasainya ketika terjadi penghentian kepegawaian, kontrak atau perjanjian mereka.	Ya	Ditetapkan suatu aturan terkait pengembalian aset ketika terjadi penghentian kepegawaian, kontrak atau perjanjian kerja
	A.8.2 Klasifikasi Informasi	A.8.2.1 Klasifikasi Informasi	Kendali Informasi harus diklasifikasikan sesuai persyaratan hukum, nilai, kekritisn dan kerentanan terhadap penyingkapan atau modifikasi yang tidak sah.	Ya	Dilakukan diklat bagi setiap personel terkait aturan dan lainnya terhadap penyingkapan atau modifikasi yang tidak sah
		A.8.2.2 Pelabelan informasi	Kendali Seperangkat prosedur yang tepat untuk pelabelan informasi harus dikembangkan dan diimplementasikan sesuai dengan skema klasifikasi informasi yang diadopsi oleh organisasi.	Ya	Ditetapkan suatu kebijakan terkait prosedur SOP pelabelan informasi

ISO/IEC 27001:2013 Statement of Applicability			Deskripsi Kontrol	(YA / TIDAK)	Justifikasi
Area	Section	Control			
		A.8.2.3 Penanganan Aset	Kendali Prosedur penanganan aset harus dikembangkan dan diimplementasikan sesuai dengan skema klasifikasi informasi yang diadopsi organisasi.	Ya	Ditetapkan SOP penanganan aset sesuai skema klasifikasi informasi yang diadopsi organisasi
	A.8.3 Media Handling	A.8.3.1 Management of removable media	Kendali Prosedur harus diimplementasikan untuk manajemen media yang dapat dipindahkan sesuai dengan skema klasifikasi yang diadopsi organisasi	Ya	Setiap personil bertanggung jawab terhadap prosedur untuk manajemen yang dapat dipindahkan sesuai dengan skema klasifikasi yang diadopsi organisasi
		A.8.3.2 Disposal of media	Kendali Media harus dihancurkan dengan aman saat tidak lagi dibutuhkan, dengan menggunakan prosedur baku.	Ya	Ditetapkan SOP terkait penghancuran media yang tidak dibutuhkan lagi
		A.8.3.3 Physical media transfer	Kendali Media yang mengandung informasi harus dilindungi terhadap akses, penyalahgunaan, atau perubahan yang tidak sah selama dipindahkan.	Ya	Kebijakan telah dibuat Panduan mutu terkait Physical media transfer
A.9 Kendali Akses					
	A.9.1 Persyaratan bisnis untuk kendali akses	A.9.1.1 Kebijakan kendali akses	Kendali Kebijakan kendali akses harus ditetapkan, didokumentasikan, dan direviu berdasarkan dan persyaratan bisnis dan keamanan informasi.	Ya	Kebijakan telah dibuat Panduan Mutu terkait Kendali akses
		A.9.1.2 Akses ke jaringan dan layanan jaringan	Kendali Pengguna hanya akan disediakan akses ke jaringan dan layanan jaringan yang telah secara khusus diberi wewenang untuk digunakan.	Ya	Ditetapkan SK kepada pengguna akses jaringan dan layanan jaringan
	A.9.2 Manajemen akses pengguna	A.9.2.1 Registrasi dan pembatalan registrasi pengguna	Kendali Proses registrasi dan pembatalan registrasi pengguna yang resmi harus diimplementasikan untuk mengaktifkan penetapan hak akses.	Ya	Melakukan sosialisasi untuk mengaktifkan penetapan hak akses terkait proses registrasi dan pembatalan registrasi pengguna yang resmi
		A.9.2.2 Penyediaan akses pengguna	Kendali Proses penyediaan akses pengguna yang resmi harus diimplementasikan untuk menetapkan atau mencabut hak akses untuk semua tipe pengguna ke semua sistem dan layanan.	Ya	Melakukan sosialisasi penyediaan akses pengguna
		A.9.2.3 Manajemen hak akses istimewa	Kendali Pengalokasian dan penggunaan hak akses istimewa harus dibatasi dan dikendalikan.	Ya	Ditetapkan SOP manajemen hak akses istimewa
		A.9.2.4 Manajemen informasi otentikasi rahasia dari pengguna	Kendali Alokasi dari informasi otentikasi rahasia harus dikendalikan melalui proses manajemen yang resmi.	Ya	Ditetapkan SOP terkait Manajemen Informasi otentikasi rahasia dari pengguna
		A.9.2.5 Reviu hak akses pengguna	Kendali Pemilik aset harus mereviu hak akses pengguna secara periodik.	Ya	Dilakukan reviu secara periodik terkait hak akses pengguna
		A.9.2.6 Penghapusan atau penyesuaian hak akses	Kendali Hak akses semua pegawai dan pengguna pihak eksternal pada informasi dan fasilitas pengolahan informasi harus dihapus sewaktu terjadi penghentian kepegawaian, kontrak atau perjanjian mereka, atau disesuaikan atas perubahan yang terjadi.	Ya	Ditetapkan SOP penghapusan atau penyesuaian hak akses
	A.9.3 Tanggung Jawab Pengguna	A.9.3.1 Penggunaan informasi otentikasi rahasia	Kendali Pengguna harus disyaratkan mengikuti praktik organisasi dalam penggunaan informasi otentikasi rahasia.	Ya	Ditetapkan SOP penggunaan informasi otentikasi rahasia
	A.9.4 System and application access control	A.9.4.1 Information access restriction	Kendali Akses ke informasi dan fungsi sistem aplikasi harus dibatasi sesuai dengan kebijakan kendali akses.	Ya	Dibuat kebijakan terkait Information access restriction
		A.9.4.2 Secure log-on procedures	Kendali Ketika disyaratkan oleh kebijakan pengendalian akses, akses ke sistem dan aplikasi harus dikendalikan oleh prosedur log-on yang aman.	Ya	Dibuatkan SOP terkait Secure log-on procedures

ISO/IEC 27001:2013 Statement of Applicability			Deskripsi Kontrol	(YA / TIDAK)	Justifikasi
Area	Section	Control			
		A.9.4.3 Password management system	Kendali Sistem manajemen kata kunci harus interaktif dan menjamin kualitas kata kunci.	Ya	Mensosialisasikan kepada setiap personil tentang Password management system
		A.9.4.4 Penggunaan program utilitas istimewa	Kendali Penggunaan program utilitas yang mungkin mampu membatalkan kendali sistem dan aplikasi harus dibatasi dan dikendalikan secara ketat.	Ya	Ditetapkan SK terkait penggunaan program utilitas istimewa
		A.9.4.5 Kendali akses ke kode sumber program	Kendali Akses ke kode sumber program harus dibatasi.	Ya	Ditetapkan SK personil yang memegang kendali akses ke kode sumber program
A.10 Kriptografi					
	A.10.1 Kendali Kriptografi	A.10.1.1 Kebijakan terhadap penggunaan kendali kriptografi	Kendali Kebijakan terhadap penggunaan kendali kriptografi untuk perlindungan informasi harus dikembangkan dan diimplementasikan.	Ya	Kebijakan telah dibuat panduan mutu dan mensosilasikan kembali terkait penggunaan kendali kriptografi
		A.10.1.2 Manajemen kunci	Kendali Kebijakan terhadap penggunaan, perlindungan dan masa hidup kunci kriptografi harus dikembangkan dan diimplementasikan dalam keseluruhan siklus hidupnya.	Ya	Dibuat pasuatu kebijakan tentang panduan mutu manajemen kunci dan mensosilasikan kembali terkait penggunaan kendali kriptografi
A.11 Keamanan fisik dan lingkungan					
	A.11.1 Daerah aman				
		A.11.1.1 Batas fisik (perimeter) keamanan	Kendali Batas fisik keamanan harus ditetapkan dan digunakan untuk melindungi area yang mengandung informasi dan fasilitas pengolahan informasi yang sensitif atau kritis.	Ya	Kendali Batas fisik harus ditetapkan dengan cara Letakkan komputer server pada lokasi yang aman, dengan kunci yang hanya bisa diakses oleh otoritas yang berwenang saja. Sebisa mungkin letakkan komputer server pada tempat yang sulit untuk di lihat orang. Pastikan CCTV juga ikut mengawasi seluruh perangkat fisik jaringan komputer selama 24 penuh.
		A.11.1.2 Kendali masuk fisik	Kendali Daerah aman harus dilindungi oleh kendali masuk yang sesuai untuk menjamin hanya personel berwenang saja yang diizinkan untuk mengakses.	Ya	Kendali masuk harus dikendalikan oleh personel yang berwenang saja, agar tidak terjadi campur tangan oleh pihak lain dan agar mudah di kendalikan
		A.11.1.3 Mengamankan kantor, ruangan dan fasilitas	Kendali Keamanan fisik untuk kantor, ruangan dan fasilitas harus dirancang dan diterapkan.	Ya	Keamanan fisik sering mengacu pada tindakan yang diambil untuk melindungi sistem, gedung, dan infrastruktur pendukung yang terkait terhadap ancaman yang berhubungan dengan lingkungan fisik,
		A.11.1.4 Melindungi terhadap ancaman eksternal dan lingkungan	Kendali Perlindungan fisik terhadap bencana alam, serangan jahat atau kecelakaan harus dirancang dan diterapkan.	Ya	Melindungi Serangan dari pihak pihak yang tidak bertanggung jawab dan agar informasi bisa tampil secara teratur
		A.11.1.5 Bekerja dalam daerah aman	Kendali Prosedur untuk bekerja dalam daerah aman harus dirancang dan diterapkan.	Ya	Ruangan server dan lain yang berhubungan dengan pengembangan aplikasi menerapkan prosedur agar aman.
		A.11.1.6 Daerah pengiriman dan bongkar muat	Kendali Titik akses seperti area bongkar muat dan titik lain yang dapat dimasuki orang yang tidak berwenang harus dikendalikan dan, jika mungkin, dipisahkan dari fasilitas pengolahan informasi untuk mencegah akses oleh pihak yang tidak berwenang	Ya	Untuk Mengatasi kebocoran Kemanaan Informasi oleh pihak yang tidak berwenang
	A.11.2 Peralatan	A.11.2.1 Penempatan dan perlindungan peralatan	Kendali Peralatan harus ditempatkan dan dilindungi untuk mengurangi risiko dari ancaman dan bahaya lingkungan, dan peluang untuk akses oleh pihak yang tidak berwenang.	Ya	Infrastruktur seperti server dan sebagainya ditempatkan pada ruangan khusus yang aman dari ancaman dan bahaya lingkungan.
		A.11.2.2 Utilitas pendukung	Kendali Peralatan harus dilindungi dari kegagalan catu daya dan gangguan lain yang disebabkan kegagalan utilitas pendukung.	Ya	Telah disediakan mekanisme cadangan untuk mengantisipasi adanya kegagalan utilitas pendukung yang sedan beroperasi.
		A.11.2.3 Keamanan kabel	Kendali Kabel daya dan telekomunikasi yang membawa data atau layanan informasi pendukung harus dilindungi dari pencegatan, interferensi atau kerusakan.	Ya	Kabel jaringan dan perangkat pendukung telah ditempatkan pada tempat yang aman dan terlindungi dari bahaya lingkungan

ISO/IEC 27001:2013 Statement of Applicability			Deskripsi Kontrol	(YA / TIDAK)	Justifikasi
Area	Section	Control			
		A.11.2.4 Pemeliharaan peralatan	Kendali Peralatan harus dipelihara secara tepat untuk menjamin ketersediaan yang berkelanjutan dan integritas	Ya	Jadwal pemeliharaan peralatan telah disusun dan dijadikan acuan untuk melakukan pemeliharaan secara sistematis.
		A.11.2.5 Pemindahan aset	Kendali Peralatan, informasi atau perangkat lunak tidak boleh dibawa keluar lokasi tanpa izin yang berwenang	Ya	Telah ada prosedur yang mengatur pemindahan Peralatan, informasi atau perangkat lunak.
		A.11.2.6 Keamanan dari peralatan dan aset di luar lokasi (off-premises)	Kendali Keamanan harus diterapkan untuk aset di luar kantor dengan memperhitungkan risiko yang berbeda akibat bekerja di luar lokasi organisasi.	Ya	Setiap aset wajib memiliki hasil kajian penggunaan di luar kantor agar menjamin aset aman baik di dalam maupun di luar kantor.
		A.11.2.7 Pembuangan atau penggunaan kembali peralatan secara aman	Kendali Semua peralatan yang mengandung media penyimpanan harus diverifikasi untuk menjamin bahwa data rahasia dan perangkat lunak berlisensi apapun sudah dihapus atau ditimpa secara aman sebelumnya untuk dibuang atau dipergunakan kembali.	Ya	Telah dibuat prosedur untuk mengatur penghapusan atau penggunaan kembali peralatan yang mengandung media penyimpanan.
		A.11.2.8 Peralatan pengguna yang tidak diawasi	Kendali Pengguna harus menjamin bahwa peralatan yang tidak diawasi memiliki perlindungan yang layak.	Ya	Peminjam aset wajib menandatangani perjanjian untuk menjaga serta memastikan aset selalu aman dan tidak rusak.
		A.11.2.9 Kebijakan mengosongkan meja dan mengosongkan layar	Kendali Kebijakan mengosongkan meja dari kertas dan media penyimpanan yang dapat dipindah dan kebijakan mengosongkan layar dari fasilitas pengolahan informasi harus diadopsi.	Ya	Telah dibuat prosedur pemanfaatan layar maupun meja agar selalu mengosongkan saat akan ditinggalkan atau selesai digunakan.
A.12 Keamanan operasi					
	A.12.1 Prosedur dan tanggung jawab operasional	A.12.1.1 Prosedur operasional yang didokumentasikan	Kendali Prosedur operasional harus didokumentasikan dan tersedia untuk semua pengguna yang membutuhkannya.	Ya	Prosedur operasional agar memenuhi tahap tahap yang sudah ditentukan
		A.12.1.2 Manajemen perubahan	Kendali Perubahan terhadap organisasi, proses bisnis, fasilitas pengolahan informasi dan sistem yang mempengaruhi keamanan informasi harus dikendalikan.	Ya	Managemen perubahan terhadap organisasi, proses bisnis, pengolahan informasi dan sistem harus mempunyai keamanan yang memadai
		A.12.1.3 Manajemen Kapasitas	Kendali Penggunaan sumber daya harus diawasi, diatur dan dibuat proyeksi atas kebutuhan kapasitas di masa datang untuk memastikan performa sistem yang dibutuhkan.	Ya	Selalu dilakukan evaluasi triwulan terhadap kapasitas sumber daya seperti penyimpanan server, cloud, dan lain-lain.
		A.12.1.4 Pemisahan lingkungan pengembangan, pengujian dan operasional	Kendali Lingkungan pengembangan, pengujian, dan operasional harus dipisahkan untuk mengurangi risiko akses atau perubahan tidak sah pada lingkungan operasional	Ya	Lingkungan pengembangan, pengujian, dan operasional telah dipisahkan serta terdapat prosedur agar akses terhadap lingkungan tersebut memperhatikan hak akses dan sensitifitas data aplikasi yang digunakan.
	A.12.2 Perlindungan dari malware	A.12.2.1 Kendali terhadap malware	Kendali Kendali deteksi, pencegahan dan pemulihan untuk melindungi terhadap malware harus diimplementasikan, digabungkan dengan kepedulian pengguna yang sesuai.	Ya	Antivirus dengan kredibilitas baik diinstall di setiap komputer serta diupdate secara rutin.
	A.12.3 Cadangan (Backup)	A.12.3.1 Cadangan Informasi	Kendali Salinan cadangan informasi, perangkat lunak dan image sistem harus diambil dan diuji secara berkala sesuai dengan kebijakan cadangan yang disetujui.	Ya	Database aplikasi dibackup sesuai jadwal yang elah disusun serta dilakukan ujicoba restore secara berkala setiap triwulan.
	A.12.4 Pencatatan (logging) dan pemantauan	A.12.4.1 Pencatatan kejadian (event logging)	Kendali Catatan kejadian yang merekam aktivitas pengguna, pengecualian (exception), kegagalan dan kejadian keamanan informasi harus diciptakan, disimpan dan direviu secara berkala.	Ya	Fasilitas logging di setiap sistem maupun aplikasi diaktifkan dan diatur agar dapat dilakukan forensik.
		A.12.4.2 Perlindungan terhadap informasi log	Kendali Fasilitas untuk mencatat log dan informasi log harus dilindungi terhadap pemalsuan dan akses yang tidak berwenang.	Ya	Log dilakukan proteksi pengaksesan dan hanya dapat diakses oleh admin

ISO/IEC 27001:2013 Statement of Applicability			Deskripsi Kontrol	(YA / TIDAK)	Justifikasi
Area	Section	Control			
		A.12.4.3 Log administrator dan operator	Kendali Aktivitas administrator sistem dan operator sistem harus dicatat dan catatan tersebut dilindungi dan direviu secara berkala.	Ya	Aktivitas administrator direview setiap triwulan atau jika ada kebutuhan lain.
		A.12.4.4 Sinkronisasi waktu	Kendali Waktu dari semua sistem pengolahan informasi yang terkait dalam organisasi atau wilayah keamanan harus disinkronisasikan ke sumber waktu acuan tunggal.	Ya	Waktu perangkat wajib tersinkronisasi dengan ntp.bsn.go.id
	A.12.5 Kendali perangkat lunak operasional	A.12.5.1 Instalasi perangkat lunak pada sistem operasional	Kendali Prosedur harus diimplementasikan untuk mengendalikan instalasi perangkat lunak pada sistem operasional.	Ya	Prosedur telah diatur agar instalasi perangkat lunak hanya bisa dilakukan oleh administrator.
	A.12.6 Manajemen kerentanan teknis	A.12.6.1 Manajemen kerentanan teknis	Kendali Informasi mengenai kerentanan teknis sistem informasi yang digunakan harus diperoleh tepat waktu, keterpaparan (exposure) organisasi terhadap kerentanan tersebut dievaluasi dan tindakan yang tepat diambil untuk mengatasi risiko terkait.	Ya	Informasi kerentanan teknis sistem informasi dapat dilaporkan oleh siapa saja ke bagian Insiden Keamanan untuk segera ditindaklanjuti.
		A.12.6.2 Pembatasan terhadap instalasi perangkat lunak	Kendali Aturan yang mengatur instalasi perangkat lunak oleh pengguna harus ditetapkan dan diimplementasikan.	Ya	Setiap PC/ Laptop wajib menggunakan Windows Pro agar perangkat lunak yang diinstall atas persetujuan administrator.
	A.12.7 Pertimbangan audit sistem informasi	A.12.7.1 Information systems audit controls	Kendali Persyaratan dan aktivitas audit yang melibatkan verifikasi sistem operasional harus direncanakan secara hati-hati dan disepakati untuk memperkecil gangguan ke proses bisnis.	Ya	Audit dilakukan di luar jam operasional.
A.13 Keamanan Komunikasi					
	A.13.1 Manajemen keamanan jaringan	A.13.1.1 Kendali jaringan	Kendali Jaringan harus dikelola dan dikendalikan untuk melindungi informasi dalam sistem dan aplikasi.	Ya	Agar tidak terjadi kebocoran informasi oleh pihak pihak yang tidak bertanggung jawab
		A.13.1.2 Keamanan layanan jaringan	Kendali Mekanisme keamanan, tingkat layanan dan persyaratan manajemen dari semua layanan jaringan harus diidentifikasi dan dimasukkan dalam perjanjian layanan jaringan yang dapat dikerjakan sendiri atau dialihdayakan.	Ya	Telah dibuat SLA untuk setiap layanan layanan jaringan.
		A.13.1.3 Pemisahan dalam jaringan	Kendali Kelompok layanan informasi, pengguna dan sistem informasi harus dipisahkan pada jaringan.	Ya	Kelompok jaringan dan pemisahan membantu mencegah musuh untuk membobol lewat jaringan dan akan membuat musuh kesulitan mencari dan mendapatkan akses informasi yang paling sensitif
	A.13.2 Perpindahan informasi	A.13.2.1 Prosedur dan kebijakan perpindahan informasi	Kendali Kebijakan, prosedur dan kendali perpindahan yang resmi harus ada untuk melindungi perpindahan informasi melalui penggunaan semua jenis fasilitas komunikasi.	Ya	Telah dilakukan sosialisasi ke setiap pegawai agar mematuhi prosedur yang telah dibuat terkait pemindahan informasi.
		A.13.2.2 Perjanjian perpindahan informasi	Kendali Perjanjian harus mengatur perpindahan informasi bisnis yang aman antara organisasi dan pihak eksternal.	Ya	Pihak eksternal wajib menandatangani Non Disclosure Agreement (NDA)
		A.13.2.3 Pesan elektronik	Kendali Informasi yang terdapat dalam pesan elektronik harus dilindungi dengan tepat.	Ya	Pesan elektronik terkait operasional harus dilakukan melalui aplikasi yang aman atau menerapkan end-to-end encryption.
		A.13.2.4 Perjanjian kerahasiaan atau menjaga rahasia (nondisclosure agreement)	Kendali Persyaratan untuk perjanjian kerahasiaan atau menjaga rahasia mencerminkan kebutuhan organisasi untuk perlindungan informasi harus diidentifikasi, direviu secara teratur dan didokumentasikan.	Ya	NDA direview secara rutin setiap tahun atau jika ada perubahan yang dapat memengaruhi.
A.14 Akuisisi, pengembangan dan perawatan sistem					
	A.14.1 Persyaratan keamanan sistem informasi	A.14.1.1 Analisis dan spesifikasi persyaratan keamanan informasi	Kendali Persyaratan yang terkait keamanan informasi harus termasuk dalam persyaratan untuk sistem informasi baru atau pengembangan sistem informasi yang ada.	Ya	- Kebijakan dan Standar Sistem Manajemen Keamanan Informasi tertuang dalam pedoman mutu bab Pengendalian Keamanan Informasi, Pengembangan dan pemeliharaan sistem informasi

ISO/IEC 27001:2013 Statement of Applicability			Deskripsi Kontrol	(YA / TIDAK)	Justifikasi
Area	Section	Control			
		A.14.1.2 Pengamanan layanan aplikasi pada jaringan publik	Kendali Informasi yang terdapat dalam layanan aplikasi yang melewati jaringan publik harus dilindungi dari aktivitas yang bersifat menipu, perselisihan kontrak, dan pembukaan rahasia dan modifikasi secara tidak sah.	Ya	- Kebijakan dan Standar Sistem Manajemen Keamanan Informasi tertuang dalam pedoman mutu bab Pengendalian Keamanan informasi, Pengembangan dan pemeliharaan sistem informasi
		A.14.1.3 Perlindungan transaksi layanan aplikasi	Kendali Informasi yang terdapat di dalam transaksi layanan aplikasi harus dilindungi untuk mencegah transmisi yang tidak lengkap, pemilihan jalur yang salah (mis-routing), perubahan pesan yang tidak sah, pembukaan rahasia yang tidak sah, duplikasi atau balasan pesan yang tidak sah.	Ya	Setiap transaksi harus memastikan bahwa: 1) informasi otentikasi rahasia pengguna dari semua pihak valid dan diverifikasi; 2) transaksi tetap rahasia; 3) privasi yang terkait dengan semua pihak yang terlibat; 4) jalur komunikasi antara semua pihak dienkripsi;
	A.14.2 Keamanan dalam proses pengembangan dan dukungan	A.14.2.1 Kebijakan pengembangan yang aman	Kendali Aturan untuk pengembangan perangkat lunak dan sistem harus ditetapkan dan diterapkan untuk pengembangan dalam organisasi.	Ya	Kebijakan pengembangan tertuang dalam SOP No.11/BANXYZ/01/2022 - Keamanan pengembangan dan proses pendukungnya
		A.14.2.2 Prosedur kendali perubahan sistem	Kendali Perubahan terhadap sistem dalam daur hidup pengembangan harus dikendalikan dengan penggunaan prosedur kendali perubahan yang baku.	Ya	- Penambahan atau pengurangan fitur dalam aplikasi ataupun perubahan aplikasi secara besar - besaran harus sesuai dengan SOP No.11/BANXYZ/01/2022 - Keamanan pengembangan dan proses pendukungnya - Perubahan dilakukan oleh pihak yang berwenang - Memperoleh persetujuan dari ketua tim sebelum dilakukan - Implementasi perubahan on time, on schedule, on budget dan tidak mengganggu proses bisnis
		A.14.2.3 Reviu teknis aplikasi setelah perubahan platform operasitform changes	Kendali Ketika platform operasi diubah, aplikasi kritis bisnis harus direviu dan diuji untuk memastikan tidak adanya dampak yang merugikan pada operasi atau keamanan organisasi.	Ya	Tinjauan teknis harus dilakukan sesuai dengan SOP yang mencakup proses ; a) peninjauan kontrol aplikasi dan prosedur integritas untuk memastikan bahwa operasional tidak mengalami gangguan; b) perubahan platform operasi disediakan tepat waktu untuk memungkinkan uji dan reviu dilakukan sebelum implementasi; c) perubahan yang dilakukan sesuai dengan Business Continuity Management
		A.14.2.4 Pembatasan dalam perubahan paket perangkat lunak	Kendali Modifikasi pada paket perangkat lunak harus dicegah, dibatasi untuk perubahan yang diperlukan, dan semua perubahan harus dikendalikan dengan ketat.	Ya	- Tidak diperkenankan melakukan modifikasi terhadap sistem. - Mitigasi risiko sesuai dengan risk register
		A.14.2.5 Prinsip rekayasa sistem yang aman	Kendali Prinsip untuk rekayasa sistem yang aman harus ditetapkan, didokumentasikan, dipertahankan dan diterapkan ke setiap upaya implementasi sistem informasi.	Ya	Lingkungan pengembangan sesuai persyaratan yang tertuang di dalam SOP No.11/BANXYZ/01/2022 - Keamanan pengembangan dan proses pendukungnya
		A.14.2.6 Lingkungan pengembangan yang aman	Kendali Organisasi harus membangun dan melindungi secara memadai lingkungan pengembangan yang aman untuk upaya pengembangan dan integrasi sistem yang mencakup seluruh daur hidup pengembangan sistem.	Ya	Lingkungan pengembangan sesuai persyaratan yang tertuang di dalam SOP No.11/BANXYZ/01/2022 - Keamanan pengembangan dan proses pendukungnya
		A.14.2.7 Pengembangan oleh alihdaya	Kendali Organisasi harus mengawasi dan memantau aktivitas pengembangan sistem yang dialihdayakan.	Ya	Pengembangan sistem dapat di alihdayakan asal memenuhi persyaratan yang tertuang di dalam SOP No.11/BANXYZ/01/2022 - Keamanan pengembangan dan proses pendukungnya
		A.14.2.8 Pengujian keamanan sistem	Kendali Pengujian fungsi keamanan harus dilakukan selama pengembangan.	Ya	- Kebijakan dan Standar Sistem Manajemen Keamanan Informasi tertuan dalam pedoman mutu Pengendalian Keamanan informasi dalam Akuisisi, Pengembangan dan pemeliharaan sistem informasi. - Prosedur pelaksanaan pengujian tertuang dalam SOP No.31/BANKXYZ/01/2022 tentang Pengujian sistem - Pihak alihdaya menandatangani kebijakan kerahasiaan data

ISO/IEC 27001:2013 Statement of Applicability			Deskripsi Kontrol	(YA / TIDAK)	Justifikasi
Area	Section	Control			
		A.14.2.9 Pengujian penerimaan sistem	Kendali Program pengujian penerimaan dan kriteria terkait harus ditetapkan untuk sistem informasi baru, peningkatan dan versi baru.	Ya	- Kebijakan dan Standar Sistem Manajemen Keamanan Informasi tertuang dalam pedoman mutu Pengendalian Keamanan informasi dalam Akuisisi, Pengembangan dan pemeliharaan sistem informasi. - Prosedur pelaksanaan pengujian tertuang dalam SOP No.31/BANKXYZ/01/2022 tentang Pengujian sistem
	A.14.3 Data Uji	A.14.3.1 Proteksi data uji	Kendali Data uji harus dipilih dengan hati-hati, dilindungi, dan dikendalikan.	Ya	Dibuatkan prosedur tentang perlindungan terhadap data uji, metode simpan dan atau proteksi yang diperlukan untuk mengakses data tersebut pada SOP No.45/BANKXYZ/01/2022 tentang Data Uji
A.15 Hubungan pemasok					
	A.15.1 Keamanan informasi dalam hubungan pemasok	A.15.1.1 Kebijakan keamanan informasi untuk hubungan pemasok	Kendali Persyaratan keamanan informasi untuk mitigasi risiko yang berkaitan dengan akses pemasok untuk aset organisasi harus disetujui dengan pemasok dan didokumentasikan.	YA	Sesuai dengan Kebijakan Sistem Manajemen Keamanan Informasi pada klausul 7.4 dilakukan Pengendalian Hubungan dengan Pihak Ketiga Atau Penyedia.
		A.15.1.2 Memasukkan klausul keamanan dalam perjanjian pemasok	Kendali Semua persyaratan keamanan informasi yang relevan harus ditetapkan dan disetujui dengan setiap pemasok yang dapat mengakses, memroses, menyimpan, berkomunikasi, atau menyediakan komponen infrastruktur TI untuk informasi organisasi.	YA	Sesuai dengan Kebijakan Sistem Manajemen Keamanan Informasi pada klausul 7.4 dilakukan Pengendalian Hubungan dengan Pihak Ketiga Atau Penyedia.
		A.15.1.3 Rantai pasok teknologi informasi dan komunikasi	Kendali Perjanjian dengan pemasok harus termasuk persyaratan untuk mengatasi risiko keamanan informasi terkait rantai pasok layanan dan produk teknologi informasi dan komunikasi.	YA	- Kebijakan dan Standar Sistem Manajemen Keamanan Informasi tentang Pengendalian Hubungan dengan Pihak Ketiga Atau Penyedia.dan sesuai dengan SOP No. 22/BANKXYZ/01/2022 - Pengelolaan Pemasok
	A.15.2 Manajemen penyampaian layanan pemasok	A.15.2.1 Pemantauan dan revidi layanan pemasok	Kendali Organisasi harus secara teratur memantau, merevisi dan mengaudit penyampaian layanan pemasok..	YA	- Kebijakan dan Standar Sistem Manajemen Keamanan Informasi tentang Pengendalian Hubungan dengan Pihak Ketiga Atau Penyedia.dan sesuai dengan SOP No. 22/BANKXYZ/01/2022 - Pengelolaan Pemasok
		A.15.2.2 Mengelola perubahan layanan pemasok	Kendali Perubahan ketentuan layanan oleh pemasok, termasuk mempertahankan dan meningkatkan kebijakan, prosedur dan kendali keamanan informasi yang ada harus dikelola dengan memperhitungkan tingkat kekritisan informasi, sistem dan proses bisnis yang terlibat, dan asesmen ulang terhadap risiko.	YA	- Kebijakan dan Standar Sistem Manajemen Keamanan Informasi tentang Pengendalian Hubungan dengan Pihak Ketiga Atau Penyedia.dan sesuai dengan SOP No. 22/BANKXYZ/01/2022 - Pengelolaan Pemasok
A.16 Manajemen insiden keamanan informasi					
	A.16.1 Manajemen insiden keamanan informasi dan perbaikan	A.16.1.1 Tanggung jawab dan prosedur	Kendali Tanggung jawab dan prosedur manajemen harus ditetapkan untuk memastikan tanggapan yang cepat, efektif dan tepat untuk insiden keamanan informasi.	YA	Kebijakan tentang tanggung jawab dan prosedur terkait insiden ditetapkan didalam SOP No. 32/BANKXYZ/01/2022 - Pengelolaan Insiden
		A.16.1.2 Pelaporan kejadian keamanan informasi	Kendali Kejadian keamanan informasi harus dilaporkan melalui saluran manajemen yang sesuai secepat mungkin.	YA	Pelaporan terkait kejadian keamanan informasi dapat dilakukan sesuai dengan SOP No. 32/BANKXYZ/01/2022 - Pengelolaan Insiden
		A.16.1.3 Pelaporan kelemahan keamanan informasi	Kendali Karyawan dan kontraktor yang menggunakan sistem informasi dan layanan organisasi harus mencatat dan melaporkan kelemahan keamanan informasi yang diamati dan dicurigai dalam sistem atau layanan.	YA	Pencatatan dan Pelaporan kelemahan keamanan informasi pada mobile banking dapat dilakukan sesuai dengan OP No. 32/BANKXYZ/01/2022 - Pengelolaan Insiden
		A.16.1.4 Asesmen dan keputusan pada kejadian keamanan informasi	Kendali Kejadian keamanan informasi harus dinilai dan harus diputuskan jika akan diklasifikasikan sebagai insiden keamanan informasi.	YA	Kebijakan tentang klasifikasi ditetapkan didalam SOP No. 32/BANKXYZ/01/2022 - Pengelolaan Insiden dan Instruksi kerja No.132/BANKXYZ/01/2022 - Klasifikasi insiden keamanan informasi
		A.16.1.5 Tanggapan terhadap insiden keamanan informasi	Kendali Insiden keamanan informasi harus ditanggapi sesuai dengan prosedur yang telah didokumentasikan..	YA	Kebijakan tentang tanggapan atas terjadinya insiden ditetapkan didalam SOP No. 032/BANKXYZ/01/2022 - Pengelolaan Insiden

ISO/IEC 27001:2013 Statement of Applicability			Deskripsi Kontrol	(YA / TIDAK)	Justifikasi
Area	Section	Control			
		A.16.1.6 Pembelajaran dari insiden keamanan informasi	Kendali Pengetahuan yang diperoleh dari menganalisis dan mengatasi insiden keamanan informasi harus digunakan untuk mengurangi kemungkinan insiden atau dampak insiden di masa depan.	YA	- Kebijakan tentang tanggapan atas terjadinya insiden ditetapkan didalam SOP No. 32/BANKXYZ/01/2022 - Pengelolaan Insiden - Risk register manajemen keamanan informasi
		A.16.1.7 Pengumpulan bukti	Kendali Organisasi harus mendefinisikan dan menetapkan prosedur untuk identifikasi, pengumpulan, akuisisi dan preservasi informasi, yang dapat berguna sebagai bukti.	YA	Sesuai dengan Kebijakan dan Standar Sistem Manajemen Keamanan Informasi tentang Pengendalian Pengelolaan Gangguan Keamanan Informasi
A.17 Aspek keamanan informasi dari manajemen					
	A.17.1 Keberlangsungan keamanan informasi	A.17.1.1 Perencanaan keberlangsungan keamanan informasi	Kendali Organisasi harus menentukan persyaratannya untuk keamanan informasi dan keberlangsungan manajemen keamanan informasi dalam situasi yang merugikan, contoh selama krisis atau bencana.	YA	- Kebijakan dan Standar Sistem Manajemen Keamanan Informasi dalam panduan mutu tentang Pengendalian Aspek Keamanan Informasi dalam Pengelolaan Keberlangsungan Kegiatan. - SOP No. 37/BANKXYZ/01/2022 - Pengelolaan Rencana Keberlangsungan
		A.17.1.2 Mengimplementasikan keberlangsungan keamanan informasi	Kendali Organisasi harus menetapkan, mendokumentasikan, menerapkan dan menjaga proses, prosedur, dan kendali untuk memastikan tingkat yang dibutuhkan dalam keberlangsungan keamanan informasi selama situasi yang merugikan.	YA	- Kebijakan dan Standar Sistem Manajemen Keamanan Informasi dalam panduan mutu tentang Pengendalian Aspek Keamanan Informasi dalam Pengelolaan Keberlangsungan Kegiatan. - SOP No. 37/BANKXYZ/01/2022 - Pengelolaan Rencana Keberlangsungan
		A.17.1.3 Memeriksa, mereview dan mengevaluasi keberlangsungan keamanan informasi	Kendali Organisasi harus memeriksa kendali keberlangsungan keamanan informasi yang ditetapkan dan diimplementasikan secara berkala untuk memastikan bahwa kendali tersebut valid dan efektif selama situasi yang merugikan.	YA	- Kebijakan dan Standar Sistem Manajemen Keamanan Informasi dalam panduan mutu tentang Pengendalian Aspek Keamanan Informasi dalam Pengelolaan Keberlangsungan Kegiatan. - SOP No. 37/BANKXYZ/01/2022 - Pengelolaan Rencana Keberlangsungan
	A.17.2 Redudansi	A.17.2.1 Ketersediaan fasilitas pengolahan informasi	Kendali Fasilitas pengolahan informasi harus diimplementasikan dengan redundansi yang cukup untuk memenuhi persyaratan ketersediaan.	YA	Kebijakan dan Standar Sistem Manajemen Keamanan Informasi di dalam panduan mutu tentang Pengendalian Aspek Keamanan Informasi dalam Pengelolaan Keberlangsungan Kegiatan.
A.18 Kesesuaian					
	A.18.1 Kesesuaian dengan persyaratan hukum dan kontraktual	A.18.1.1 Identifikasi persyaratan perundang-undangan dan kontraktual yang berlaku	Kendali Semua persyaratan undang-undang, peraturan, kontraktual yang relevan, dan pendekatan organisasi untuk memenuhi persyaratan ini, harus diidentifikasi secara eksplisit, didokumentasikan dan dijaga tetap mutakhir untuk setiap sistem informasi dan organisasi.	YA	Kebijakan dan Standar Sistem Manajemen Keamanan Informasi di dalam panduan mutu tentang Pengendalian Kepatuhan
		A.18.1.2 Hak kekayaan intelektual	Kendali Prosedur yang sesuai harus diimplementasikan untuk memastikan kesesuaian dengan persyaratan hukum dan perundang-undangan serta kontraktual yang terkait dengan hak atas kekayaan intelektual dan penggunaan produk perangkat lunak proprietary.	YA	Kebijakan dan Standar Sistem Manajemen Keamanan Informasi di dalam panduan mutu tentang Pengendalian Kepatuhan
		A.18.1.3 Perlindungan rekaman	Kendali Rekaman harus dilindungi dari kehilangan, kerusakan, pemalsuan, akses tidak sah dan rilis tidak sah, sesuai dengan persyaratan peraturan perundangan, kontraktual dan bisnis..	YA	Kebijakan dan Standar Sistem Manajemen Keamanan Informasi di dalam panduan mutu tentang Pengendalian Kepatuhan
		A.18.1.4 Privasi dan perlindungan atas informasi pribadi yang dapat diidentifikasi	Kendali Privasi dan perlindungan informasi pribadi yang dapat diidentifikasi harus dipastikan sebagaimana disyaratkan dalam peraturan perundangan yang relevan.	YA	Kebijakan dan Standar Sistem Manajemen Keamanan Informasi di dalam panduan mutu tentang Pengendalian Kepatuhan
		A.18.1.5 Peraturan kendali kriptografi	Kendali kendali kriptografi harus sesuai dengan semua peraturan perundangan dan perjanjian yang relevan.	YA	Kebijakan dan Standar Sistem Manajemen Keamanan Informasi di dalam panduan mutu tentang Pengendalian Kepatuhan

ISO/IEC 27001:2013 Statement of Applicability			Deskripsi Kontrol	(YA / TIDAK)	Justifikasi
Area	Section	Control			
	A.18.2 Reviu keamanan informasi	A.18.2.1 Reviu independen terhadap keamanan informasi	Kendali Pendekatan organisasi untuk mengelola keamanan informasi dan implementasinya (contoh: sasaran kendali, kendali, kebijakan, proses dan prosedur untuk keamanan informasi) harus direviu berkala secara independen atau ketika terjadi perubahan signifikan.	YA	- Kebijakan dan Standar Sistem Manajemen Keamanan Informasi di dalam panduan mutu tentang Pengendalian Kepatuhan - Rencana Sistem Manajemen Keamanan Informasi
		A.18.2.2 Kesesuaian dengan kebijakan dan standar keamanan	Kendali Manajer harus secara teratur mereviu kesesuaian prosedur dan pemrosesan informasi dalam area tanggung jawab mereka dengan kebijakan keamanan, standar dan persyaratan keamanan lainnya yang sesuai.	YA	Kesesuaian terdapat pada SOP No. 14/BANKXYZ/01/2022 - Evaluasi Kepatuhan terhadap Kebijakan dan Standar Keamanan Informasi
		A.18.2.3 Reviu kesesuaian teknis	Kendali Sistem informasi harus direviu secara reguler agar tetap sesuai dengan kebijakan dan standar keamanan informasi organisasi.	YA	- Kebijakan dan Standar Sistem Manajemen Keamanan Informasi di dalam panduan mutu tentang Pengendalian Kepatuhan - Rencana Sistem Manajemen Keamanan Informasi


Hasil Temuan Audit

Team 1

Nama Anggota Kelompok :

1. Maysarah
2. Mumami
3. Sari Andarwati
4. Muh Shamad

No	Temuan	Anex	Akar Penyebab	Tindakan Perbaikan/Pencegahan	Batas Waktu Penyelesaian	Verifikasi
Video I	Laptop dibiarkan menyala dan tidak dikunci saat istirahat di ruang rapat. Hal ini tidak sesuai dengan Pengelolaan Informasi dari Otentikasi Rahasia Milik Pengguna	A.9.2.4 Manajemen informasi otentikasi rahasia dari pengguna	Kelalaian personil	- Perbaikan prosedur penggunaan sarana informasi (Auto lock screen setelah 5 menit tanpa aktivitas)	1 minggu, 25 April 2022	Close
	Papan tulis tidak dihapus, terdapat informasi yang bersifat rahasia (IP, User name, Password)	A.11.2.7 Pembuangan atau penggunaan kembali peralatan secara aman A.9.4.3 Password management system	Kelalaian personil	Sosialisasi untuk meningkatkan awareness personil terkait kerahasiaan informasi	1 minggu, 25 April 2022	Close
	Meja tidak dirapikan, terdapat dokumen yang bersifat rahasia	A.11.2.7 Pembuangan atau penggunaan kembali peralatan secara aman	Kelalaian personil	- Sosialisasi untuk meningkatkan awareness personil terkait kerahasiaan informasi - menyusun prosedur berisi Kebijakan desk clean, untuk memastikan tidak terdapat barang tidak dibutuhkan di atas meja	1 minggu, 25 April 2022	Close
Video II	Ditemukan kertas berisi password ditemukan ditempel di layar monitor.	A.9.2.4 Manajemen informasi otentikasi rahasia dari pengguna A.9.4.3 Password management system	Kelalaian personil	- Sosialisasi untuk meningkatkan awareness personil terkait kerahasiaan informasi - menyusun prosedur berisi Kebijakan desk clean, untuk memastikan tidak terdapat barang tidak dibutuhkan di atas meja	1 minggu, 25 April 2022	Close
	Laptop dibiarkan menyala dan tidak dikunci saat istirahat di ruang rapat. Hal ini tidak sesuai dengan Pengelolaan Informasi dari Otentikasi Rahasia Milik Pengguna	A.9.2.4 Manajemen informasi otentikasi rahasia dari pengguna	Kelalaian personil	- Perbaikan prosedur (Auto lock screen setelah 5 menit tanpa aktivitas)	1 minggu, 25 April 2022	Close
	Papan tulis tidak dihapus, terdapat informasi yang bersifat rahasia yang bisa dibaca oleh pihak yang tidak berwenang	A.11.2.7 Pembuangan atau penggunaan kembali peralatan secara aman	Kelalaian personil	Sosialisasi untuk meningkatkan awareness personil terkait kerahasiaan informasi	1 minggu, 25 April 2022	Close
Video III	Personel yang tidak berwenang saja diizinkan untuk mengakses ruang server, tidak ditemukan pengamanan ruang server. Ruang server dalam kondisi terbuka dan tidak terkunci	A.11.1.2 Kendali masuk fisik	- kelalaian personil - Prosedur hak akses ruangan tidak dijalankan	- Sosialisasi untuk meningkatkan awareness personil terkait kerahasiaan informasi - Penambahan sarana keamanan hak akses ruangan - Evaluasi prosedur hak akses ruangan	1 bulan, 18 Mei 2022	Close
Video IV	Tidak dilakukan pemeriksaan hak akses masuk ruang kerja terhadap tamu	A.11.1.3 Mengamankan kantor, ruangan dan fasilitas	- kelalaian personil - Prosedur hak akses ruangan tidak dijalankan	- Sosialisasi untuk meningkatkan awareness personil terkait kerahasiaan informasi - Evaluasi prosedur hak akses ruangan	1 bulan, 18 Mei 2022	Close

	RESET PASSWORD MOBILE BANKING	No. Dok. : P.SMKI.1 Revisi : 0 Tgl. Terbit : 20 April 2022 Halaman : 1 dari 2
---	--------------------------------------	--

TUJUAN:

Untuk memastikan nasabah dapat melakukan reset password melalui aplikasi mobile banking sesuai dengan ketentuan.

RUANG LINGKUP:

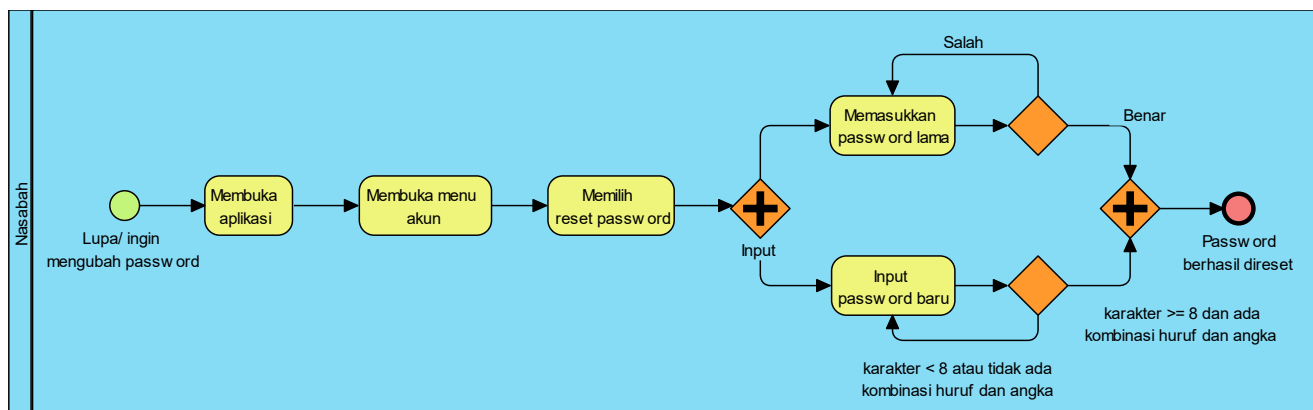
Prosedur ini digunakan untuk reset password aplikasi mobile banking.

INDIKATOR KINERJA:


80% nasabah berhasil melakukan reset password secara mandiri melalui aplikasi mobile banking.

TAHAP PROSEDUR:

1. Alur Proses



- Proses ini dipicu oleh nasabah yang ingin mengganti password.
- Nasabah membuka aplikasi (termasuk login) lalu membuka menu akun. Setelah itu memilih pilihan reset password.

	RESET PASSWORD MOBILE BANKING	No. Dok. : P.SMKI.1 Revisi : 0 Tgl. Terbit : 20 April 2022 Halaman : 2 dari 2
---	--------------------------------------	--

c. Nasabah harus mengisi formulir F.SMKI.1.0.1 Reset password dengan memasukkan password lama dengan benar dan password baru minimal 8 karakter dan terdiri atas kombinasi huruf dan angka.

d. Jika poin c di atas dilakukan dengan benar, password nasabah berhasil direset dengan password yang baru.

2. Login Mobile Banking

Untuk dapat menggunakan menu Akun pada aplikasi Mobile Banking, pengguna harus login terlebih dahulu menggunakan username, password, serta PIN mobile banking.

DOKUMEN TERKAIT

F.SMKI.1.0.1: Formulir Reset Password Mobile Banking

Disetujui oleh:	Diperiksa oleh:	Disiapkan oleh:
-----------------	-----------------	-----------------

	PEMBUKAAN AKUN BARU MOBILE BANKING	No. Dok. : P.SMKI.2 Revisi : 0 Tgl. Terbit : 21 April 2022 Halaman : 1 dari 3
---	---	--

TUJUAN:

Untuk memastikan keamanan dan kelancaran dalam proses pembukaan akun mobile banking baru.

RUANG LINGKUP:

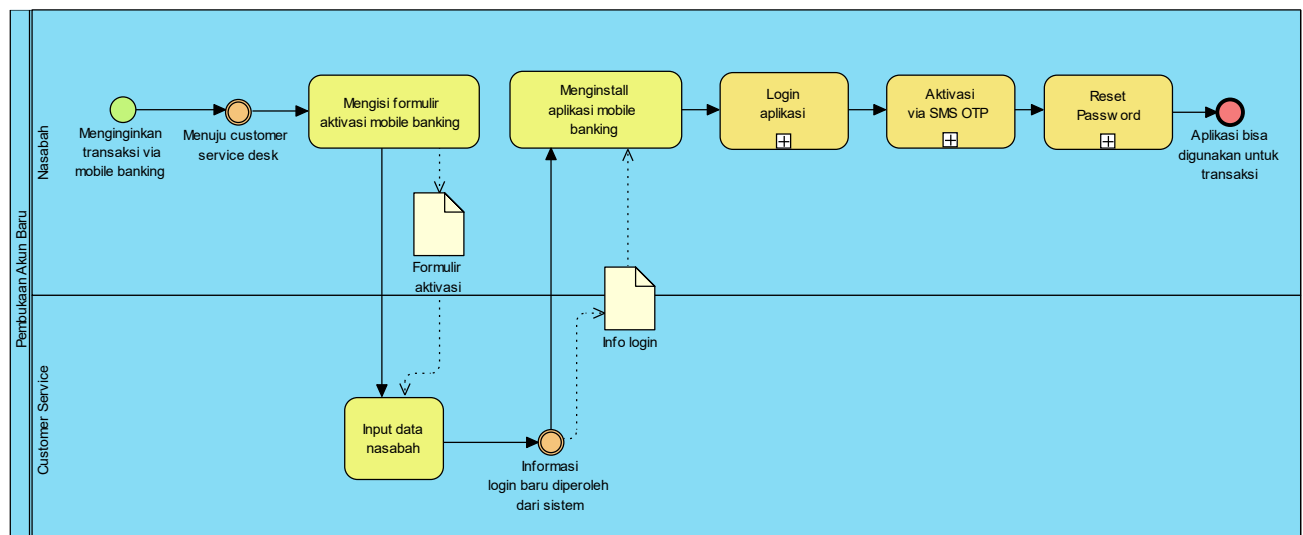
Prosedur ini digunakan untuk pembukaan akun mobile banking yang dilakukan langsung di kantor Bank XYZ.

INDIKATOR KINERJA:

Laporan bulanan pembukaan akun mobile banking.

TAHAP PROSEDUR:

1. Alur Proses



- Proses ini dipicu oleh nasabah yang ingin melakukan transaksi via mobile banking atau internet.
- Nasabah harus melakukan permohonan ke kantor Bank XYZ.

	PEMBUKAAN AKUN BARU MOBILE BANKING	No. Dok. : P.SMKI.2 Revisi : 0 Tgl. Terbit : 21 April 2022 Halaman : 2 dari 3
---	---	--

- c. Nasabah mengisi formulir F.SMKI.2.0.1 aktivasi mobile banking kemudian memberikan formulir tersebut ke petugas customer service untuk diinput ke dalam sistem.
- d. Setelah itu sistem akan mengeluarkan username, password, dan PIN default untuk login sementara nasabah ke dalam mobile banking.
- e. Pada saat login pertama kali, nasabah akan diminta memasukkan kode OTP yang dikirimkan ke nomor ponsel nasabah untuk verifikasi.
- f. Setelah kode OTP benar, nasabah akan diminta mengubah PIN dan mereset password.

2. Syarat Nasabah

Untuk dapat menggunakan aplikasi Mobile Banking, nasabah harus memiliki smartphone yang mendukung aplikasi Mobile Banking. Berikut syarat minimal smartphone yang didukung:

- a. Sistem operasi Android versi 5.0 ke atas atau iOS versi 10 ke atas
- b. RAM minimal 1GB
- c. Penyimpanan minimal 5GB

3. Ketentuan keamanan informasi login

Nasabah harus menjaga informasi login baik username, password, maupun PIN. Informasi login tidak boleh diberikan ke orang lain termasuk karyawan Bank XYZ.

	<p align="center">PEMBUKAAN AKUN BARU MOBILE BANKING</p>	<p>No. Dok. : P.SMKI.2 Revisi : 0 Tgl. Terbit : 20 April 2022 Halaman : 3 dari 3</p>
---	---	---

DOKUMEN TERKAIT

F.SMKI.2.0.1: Formulir Aktivasi Mobile Banking

IK.SMKI.2.1: Tatacara Input Data Nasabah untuk Mobile Banking

P.SMKI.1: Reset Password Mobile Banking

<p>Disetujui oleh:</p>	<p>Diperiksa oleh:</p>	<p>Disiapkan oleh:</p>
------------------------	------------------------	------------------------

	<p style="text-align: center;">PENGUJIAN KEAMANAN APLIKASI MOBILE BANKING</p>	<p>No. Dok. : P.SMKI.3 Revisi : 0 Tgl. Terbit : 21 April 2022 Halaman : 1 dari 2</p>
---	--	---

TUJUAN:

Untuk memastikan aplikasi mobile banking yang dikembangkan tidak terdapat celah keamanan.

RUANG LINGKUP:

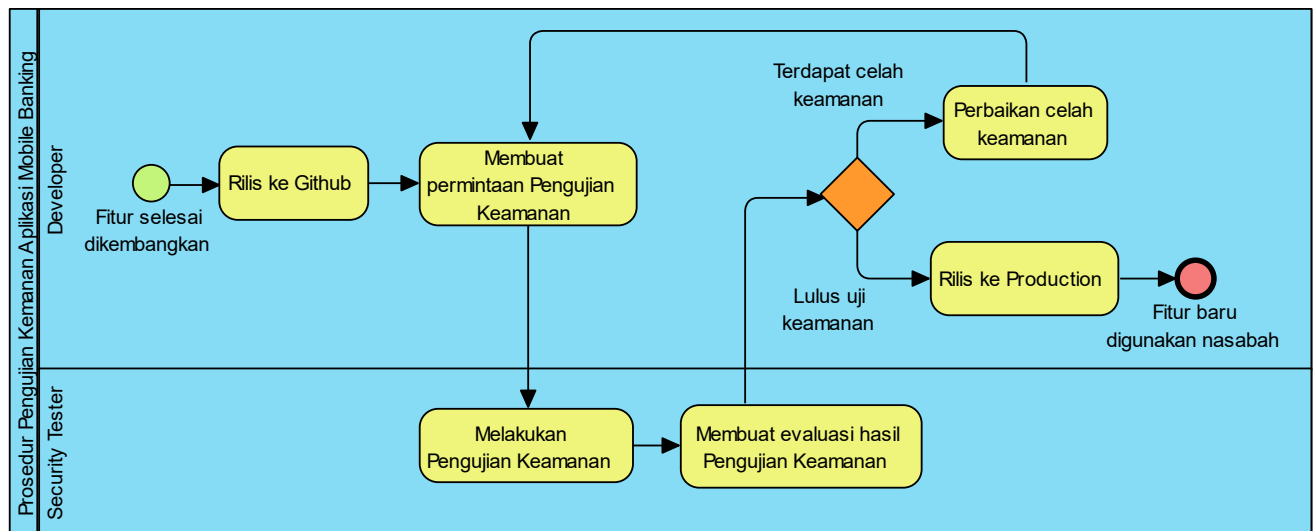
Prosedur ini digunakan untuk pengujian aplikasi mobile banking Bank XYZ.

INDIKATOR KINERJA:

Laporan evaluasi hasil pengujian keamanan.

TAHAP PROSEDUR:

1. Alur Proses



- Proses ini dimulai Ketika fitur atau fungsi aplikasi selesai dikembangkan sehingga perlu dilakukan pengujian keamanan.
- Developer harus merilis perubahan kode ke repository Github yang telah ditentukan.

	PENGUJIAN KEAMANAN APLIKASI MOBILE BANKING	No. Dok. : P.SMKI.3 Revisi : 0 Tgl. Terbit : 21 April 2022 Halaman : 2 dari 2
---	---	--

- c. Developer membuat permintaan pengujian keamanan melalui formulir F.SMKI.3.0.1.
- d. Security tester melakukan pengujian berdasarkan instruksi kerja pada IK.SMKI.3.1 dan membuat evaluasi hasil pengujian.
- e. Jika masih terdapat celah keamanan, developer harus segera menutup atau memperbaiki celah keamanan tersebut.
- f. Jika sudah lulus uji keamanan, fitur dapat dirilis untuk produksi.

2. Syarat Security Tester

Security tester bukan merupakan developer aplikasi atau independen. Data yang digunakan untuk pengujian keamanan wajib dijaga keamanan informasinya jika merupakan data real. Data sangat rahasia tidak boleh digunakan saat uji coba keamanan aplikasi.

DOKUMEN TERKAIT

F.SMKI.3.0.1: Formulir Permintaan Pengujian Keamanan

IK.SMKI.3.1: Tatacara Pengujian Keamanan Aplikasi

Disetujui oleh:	Diperiksa oleh:	Disiapkan oleh:
-----------------	-----------------	-----------------

	<p align="center">INPUT DATA NASABAH UNTUK AKTIVASI MOBILE BANKING</p>	<p>No. Dok. : IK.SMKI.2.1 Revisi : 0 Tgl. Terbit : 21 April 2022 Halaman : 1 dari 1</p>
---	---	--

TUJUAN:

Untuk mendukung proses aktivasi akun baru mobile banking nasabah.

INSTRUKSI KERJA:

Instruksi kerja ini dilakukan oleh petugas Customer Service yang melayani nasabah yang ingin aktivasi mobile banking. Berikut tatacara input data nasabah ke dalam sistem.

1. Periksa formulir F.SMKI.2.0.1 sudah terisi dengan benar dengan ketentuan sebagai berikut:
 - Isian nama, NIK, alamat, jenis kelamin, dan pekerjaan konsisten dengan KTP
 - Jika ada data yang tidak sesuai KTP agar dilakukan konfirmasi ke nasabah
 - Alamat email sesuai dengan format email.
2. Jika isian formulir sudah benar, pada aplikasi internal Bank, buka menu Pendaftaran lalu pilih Aktivasi Mobile Banking.
3. Isikan form sesuai dengan formulir F.SMKI.2.0.1 yang telah diisi nasabah.
4. Sampaikan ke nasabah untuk menginstall aplikasi Mobile Banking melalui Play Store atau App Store
5. Informasikan username, password, dan PIN default sesuai yang tertera pada aplikasi.
6. Pandu nasabah sesuai prosedur P.SMKI.2 hingga berhasil melakukan reset PIN dan password.

Disetujui oleh:	Diperiksa oleh:	Disiapkan oleh:
-----------------	-----------------	-----------------

	TATACARA PENGUJIAN KEAMANAN APLIKASI	No. Dok. : IK.SMKI.3.1 Revisi : 0 Tgl. Terbit : 21 April 2022 Halaman : 1 dari 1
---	---	---

TUJUAN:

Untuk mendukung proses pengujian aplikasi mobile banking.

INSTRUKSI KERJA:

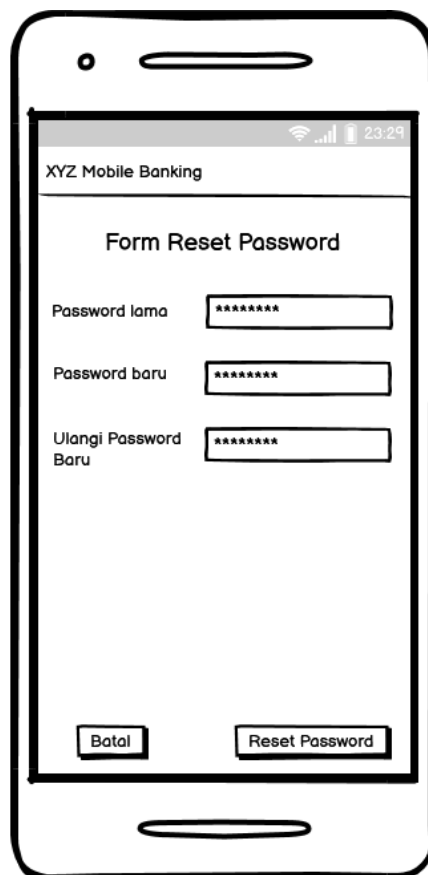
Instruksi kerja ini dilakukan oleh security tester. Berikut tatacara pengujian aplikasinya.

1. Melakukan deploy/instalasi source code aplikasi dari repository/ github.
2. Melakukan pengujian keamanan pada area berikut:
 - Vulnerability Scanning
 - Security Scanning
 - Penetration Testing
 - Security Auditing
 - Ethical Hacking
 - Otentikasi dan Otorisasi
3. Setelah melakukan pengujian di atas, dibuat evaluasi hasil pengujian dan rekomendasi untuk perbaikan.
4. Hasil evaluasi diserahkan ke developer untuk segera dilakukan perbaikan.
5. Evaluasi dapat diberikan secara iterasi untuk mempercepat proses pengembangan aplikasi.

Disetujui oleh:	Diperiksa oleh:	Disiapkan oleh:
-----------------	-----------------	-----------------

	<p align="center">FORMULIR RESET PASSWORD MOBILE BANKING</p>	<p>No. Dok. : F.SMKI.1.0.1 Revisi : 0 Tgl. Terbit : 20 April 2022 Halaman : 1 dari 1</p>
---	---	---

Formulir Reset Password Mobile Banking*



* Formulir ini ditampilkan dalam aplikasi mobile banking

Disetujui oleh:	Diperiksa oleh:	Disiapkan oleh:
-----------------	-----------------	-----------------

	<p align="center">PERMINTAAN PENGUJIAN KEAMANAN APLIKASI</p>	<p>No. Dok. : F.SMKI.3.0.1 Revisi : 0 Tgl. Terbit : 21 April 2022 Halaman : 1 dari 1</p>
---	---	---

Formulir Permintaan Pengujian Keamanan Aplikasi

Data Developer

Nama developer/ Nama Tim : _____

Fitur yang dikembangkan : _____

Nama/versi rilis : _____

Link Repository : _____

Catatan : _____

Developer/ Tim Leader

Disetujui oleh:	Diperiksa oleh:	Disiapkan oleh:
-----------------	-----------------	-----------------



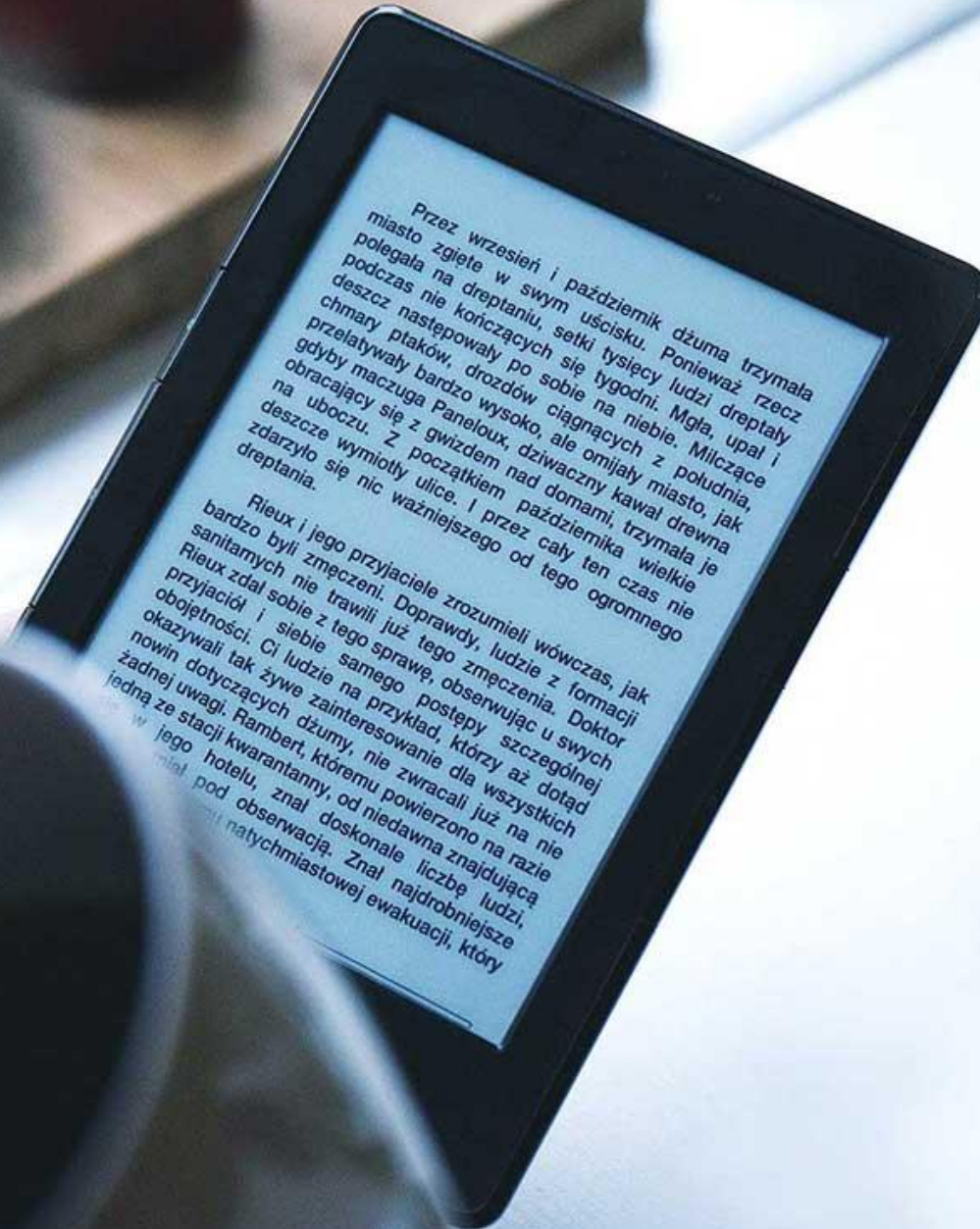
Layanan Mobile Banking

BANK XYZ

Maysarah
Mumami
Sari Andarwati
Muh Shamad

**ALWAYS ON
YOUR SIDE**





Organizational Information

Internal & External Issues

Stakeholder

Scope

Laws & Regulations

Organizational Structure

Policies and Commitment

SMKI Target

Resources and Competencies

Communication

01
02
03
04
05
06
07
08
09
10

Organizational Information

VISI

Menjadi Lembaga keuangan yang terunggul dalam layanan dan kinerja secara berkelanjutan



MISI

1. Memberikan layanan prima dan solusi digital kepada seluruh nasabah selaku mitra bisnis pilihan utama
2. Memperkuat layanan internasional untuk mendukung kebutuhan Mitra Bisnis Global
3. Meningkatkan nilai investasi yang unggul bagi investor
4. Menciptakan kondidi terbaik bagi karyawan sebagai tempat kebanggaan untuk berkarya dan berprestasi
5. Meningkatkan kepedulian dan tanggungjawab kepada lingkungan dan masyarakat
6. Menjadi acuan Pelaksanaan Kepatuhan dan tata Kelola perusahaan yang baik bagi industri.



MISI



Jl. Pangeran No. 20, Jakarta Barat, Indonesia

02
Bank XYZ 01

Internal & Eksternal Issues



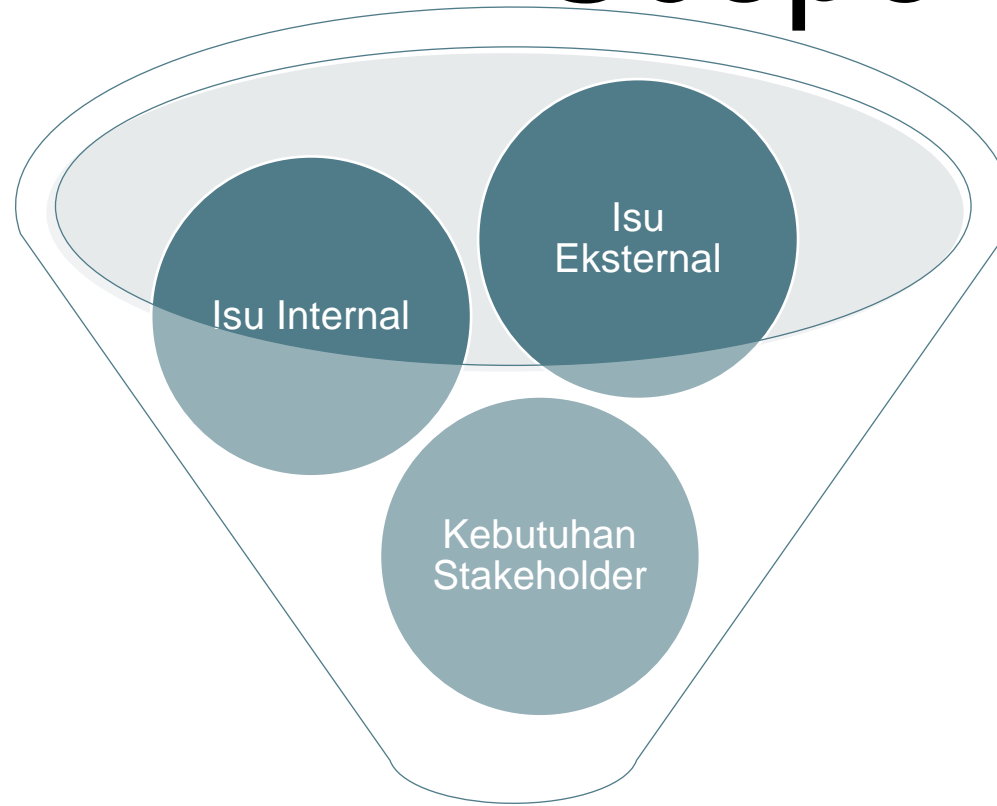
No	Issue	Internal	Eksternal
1	Pencurian Saldo nasabah	Lemahnya internal control Masalah SDM	
2	Penipuan yang mengatas namakan pihak bank		1. Phising : Tindakan memperoleh informasi pribadi seperti user id, nomor rekening bank/no kartu kredit secara tidak sah 2. tidak peduli dengan keamanan data pribadi
3	Peraturan perundangan yang berlaku		Ketaatan terhadap peraturan perundangan yang berlaku terkait layanan mobile banking
4	Layanan Prima	Memberikan layanan prima yang menggunakan teknologi IT	

Stakeholder

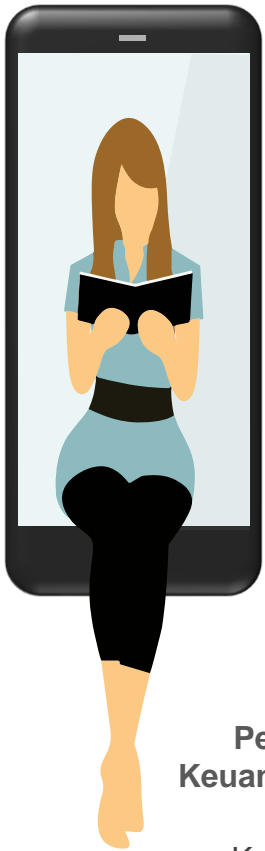
No	Pemangku Kepentingan	Harapan	Kebutuhan
1	Nasabah	Aplikasi aman namun mudah digunakan	Transaksi keuangan
2	Bank/ Organisasi Financial lain	Transaksi antar bank lancar dan aman	Transaksi keuangan lintas bank
3	Developer aplikasi	Aplikasi dapat berjalan dengan baik tanpa error	Membuat aplikasi dengan mudah
4	Tim infrastruktur TI	Infrastruktur dapat memfasilitasi semua permintaan trafik aplikasi	Menyediakan infrastruktur untuk mendukung kinerja aplikasi
5	Infrastruktur TI external (AWS)	Infrastruktur outsourcing dapat memfasilitasi semua permintaan trafik aplikasi yang diminta	Menyediakan infrastruktur tambahan untuk mendukung kinerja aplikasi



Scope SMKI



Layanan Mobile Banking



Law & Regulation



UU No.10 Tahun 1998
UU Perbankan



UU No.8 Tahun 1999
Perlindungan Konsumen



UU No.3 Tahun 2011
Transfer Dana melalui mobile banking



Peraturan Otoritas Jasa Keuangan No 18/POJK.07/2018
Layanan Pengaduan Konsumen di Sektor Jasa Keuangan



UU No.19 Tahun 2016
Informasi dan Transaksi Elektronik



Peraturan Bank Indonesia No. 7/6/PBI/2005
Transparansi Informasi Produk Bank dan Penggunaan Data Pribadi Nasabah



Peraturan Bank Indonesia Nomor 14/27/PBI/2012
Penerapan Program Anti Pencucian Uang dan Pencegahan Pendanaan Terorisme Bagi Bank Umum



Peraturan Otoritas Jasa Keuangan No 12/POJK.03/2018
Penyelenggaraan Layanan Perbankan Digital oleh Bank Umum



Otoritas Jasa Keuangan No 1/POJK.07/2013
Perlindungan Konsumen Sektor Jasa Keuangan

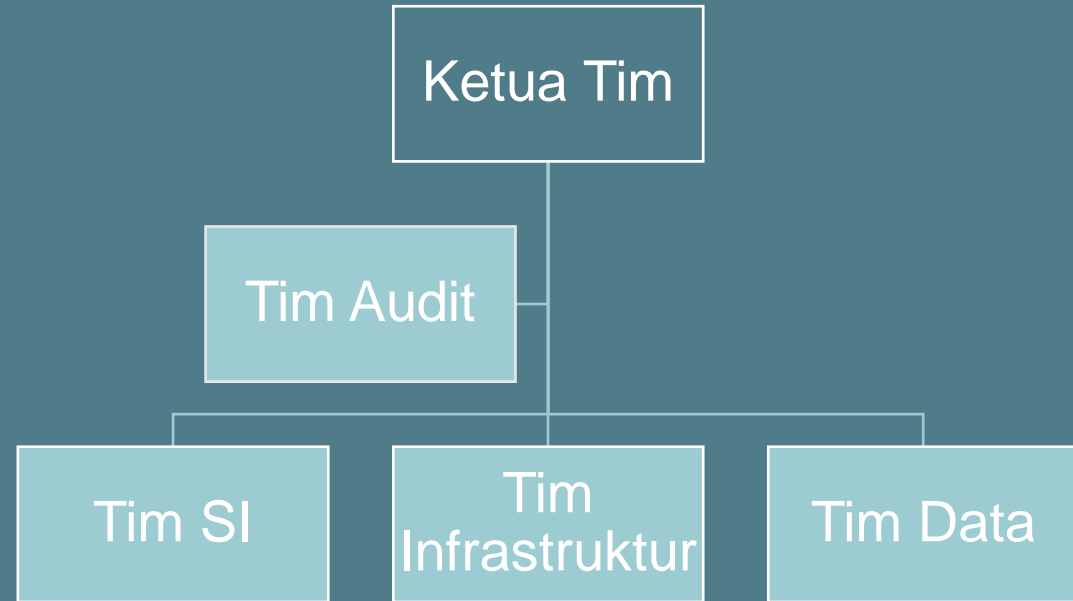


Peraturan Bank Indonesia Nomor 18/9/PBI/2016
Pengaturan dan Pengawasan Sistem Pembayaran dan Pengelolaan Uang Rupiah



Peraturan Otoritas Jasa Keuangan No 38/POJK.03/2016
Penerapan Manajemen Risiko Dalam Penggunaan Teknologi Informasi oleh Bank Umum

Organizational Structure



Nb	Peran	Tanggung Jawab
1.	Ketua Tim	1. Memberikan arahan dan masukan terkait penerapan SMK 2. Menyediakan sumber daya bagi penerapan SMK dalam layanan mobile banking 3. Memantau pengukuran efektifitas kontrol implementasi SMK 4. Memberikan laporan mengenai pelaksanaan SMK
2.	Tim Audit	1. Melakukan audit internal TIK terhadap layanan mobile banking secara berkala 2. Mengajukan saran atas tindakan perbaikan yang harus dilakukan. 3. Membuat laporan internal audit
3.	Tim Infrastruktur	1. Mengembangkan infrastruktur yang mendukung layanan mobile banking 2. Melakukan pemeliharaan infrastruktur 3. Memastikan seluruh perangkat TIK dikelola dan dimanfaatkan secara efektif dan efisien
4.	Tim SI	1. Mengembangkan aplikasi mobile banking 2. Melakukan maintenance aplikasi
5.	Tim Data	1. Mengelola data transaksi dan pelanggan 2. Memastikan perbaikan dan peredaran dokumen SMK dilakukan oleh pihak yang berwenang sesuai standar dan regulasi yang berlaku



Policies and Commitment

1. memastikan kebijakan keamanan informasi dan sasaran keamanan informasi ditetapkan dan selaras dengan Visi Misi Bank XYZ “**Menjadi The Most Valuable Banking Group dan Champion of Financial Inclusion**”;
2. memastikan persyaratan SMK terintegrasi ke dalam proses bisnis yang berlaku;
3. memastikan tersedianya sumber daya yang dibutuhkan untuk SMK;
4. mengomunikasikan pentingnya manajemen keamanan informasi yang efektif dan kesesuaian dengan persyaratan SMK;
5. memastikan bahwa SMK mencapai manfaat yang diharapkan;
6. memberikan arahan dan dukungan pada personel untuk berkontribusi dalam efektivitas SMK;
7. mempromosikan perbaikan berkelanjutan; dan
8. mendukung peran serta staff yang relevan untuk menunjukkan kepemimpinannya ketika diterapkan pada wilayah tanggung jawabnya



Policies and Commitment (Cont..)

1. Seluruh aset dan informasi di layanan mobile banking harus dilindungi dari segala bentuk ancaman dari aspek kerahasiaan (Confidentiality), keabsahan (Integrity) dan ketersediaan (Availability).
2. Manajemen, pegawai dan seluruh pihak yang terlibat, harus mengetahui dan mematuhi kebijakan manajemen keamanan informasi ini.
3. Manajemen dan Tim Mobile Banking harus memastikan terpenuhinya Sasaran Manajemen Keamanan Informasi.
4. Kebijakan dan prosedur SMK harus disosialisasikan.
5. Manajemen menyediakan dan menjamin sumber daya yang diperlukan untuk penerapan SMK.
6. Seluruh kegiatan SMK harus dilakukan pemantauan, pengukuran dan evaluasi secara berkala untuk perbaikan berkelanjutan dalam kegiatan audit baik internal maupun eksternal dan kaji ulang manajemen.
7. Setiap pelanggaran yang dilakukan atas Kebijakan Manajemen Keamanan Informasi akan dikenai sanksi dan/atau penindakan disiplin sesuai dengan peraturan yang berlaku.

SMKI Target

No	Sasaran	KPI	Aktifitas pencapaian Kinerja	Indikator Pencapaian	Kebutuhan Sumber Daya	PIC	Jangka Waktu	Evaluasi
1	Kebijakan penerapan keamanan pada layanan mobile banking	Kebijakan penerapan SMKI	Penyusunan kebijakan dan dokumentasi	Sertifikasi ISO 27001	Seluruh organisasi	Ketua Tim	1 Tahun	Sertifikasi
			Pelaksanaan kegiatan operasional sesuai dengan prosedur					
2	Pelanggan memahami prosedur keamanan penggunaan mobile banking	Kesalahan transaksi pelanggan	Menyusun media campaign untuk prosedur terkait	Kesalahan transaksi < 5%	Pelanggan, Tim SI, Tim Layanan Pelanggan	Ketua Tim	1 Tahun	Laporan per triwulan
			Membuat double authentication pada transaksi pelanggan					
			Membuat beberapa proses pengamanan (otomatis logout, permintaan perubahan password berjangka)					
3	Manajemen keamanan sistem yang handal	Percobaan pelanggaran hak akses	Pengujian sistem	Keberhasilan pelanggaran hak akses < 0,5%	Tim SI, Tim Infrastruktur, Tim Data	Ketua Tim	1 Tahun	Laporan per triwulan
			Menyusun prosedur layanan keamanan					
4	Kinerja sistem yang handal	Kinerja mobile banking	Audit TIK	Kinerja sistem > 99 %	Seluruh organisasi	Tim Audit	1 Tahun	Laporan hasil audit

Resources and Competencies

No	Peran	Kompetensi
1	Ketua Tim	<ol style="list-style-type: none">1. Pendidikan minimal S12. Mempunyai keahlian di bidang manajerial3. Mempunyai pengalaman sebagai Project Manager menangani project yang berhubungan dengan project-project di bidang Finance dan Banking minimal 5 tahun4. Memiliki Sertifikat PMP
2	Tim Audit	<ol style="list-style-type: none">1. Pendidikan minimal S12. Memiliki sertifikasi CISA3. Memiliki pengalaman sebagai IT Auditor minimal 5 tahun4. Memiliki kemampuan analisa, investigasi dan komunikasi yang baik5. Mempunyai pengalaman dalm bidang audit perbankan minimal 5 Tahun
3	Tim SI	<ol style="list-style-type: none">1. Pendidikan minimal S1 bidang SI/IT2. Mengusai bahasa pemrograman Java/Kotlin3. Pengalaman minimal 2 Tahun untuk developing enterprise-scale mobile solutions4. Mampu membaca spesifikasi pekerjaan dan mengimplementasikannya dalam kode program
4	Tim Infrastruktur	<ol style="list-style-type: none">1. Pendidikan minimal S1 bidang SI/IT2. Menguasai perangkat security jaringan (firewall, IPS, WAF, dll)3. Pengalaman minimal 2 Tahun di jaringan komputer LAN/Wireless LAN, sistem operasi Windows dan Linux, Perangkat Router (Mikrotik/Juniper), Perangkat Switching, Perangkat DSLAM/OLT
5	Tim Data	<ol style="list-style-type: none">1. Pendidikan minimal S1 bidang S1/TI2. Mempunyai sertifikasi terkait pengelolaan data transaksi dan pelanggan3. Mampu mengelola data ETL (Extraction, Transform, and Load) untuk Data Warehouse4. Menguasai DBA (Oracle, SQLServer, SQLReplication, ETL, DB Tuning, DB Optimized, Troubleshoot)



Communication

Nb	Materi Komunikasi	Periode Komunikasi	Target Penerima	Bentuk Komunikasi	PIC
1	Kebijakan SMK umum	Setiap Tahun	Seluruh Stakeholder	Pemberitahuan di dalam web	Ketua Tim
2	Keamanan data nasabah	Setiap Tahun	Seluruh pegawai perbankan	Sosialisasi	Ketua Tim
3	Awareness tentang clean desk policy	Setiap Tahun	Seluruh pegawai perbankan	Sosialisasi	Ketua Tim
4	Keamanan Password	Setiap Tahun	Pelanggan	1. Sosialisasi 2. Flyer/pengumuman di web	Ketua Tim
5	Awareness terhadap prosedur email	Setiap Tahun	Seluruh pegawai perbankan	1. Sosialisasi 2. Pamflet/blast email ke pelanggan	Ketua Tim



Prosedur



IK



Formulir



Risk Register



SoA



THANK YOU