




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:

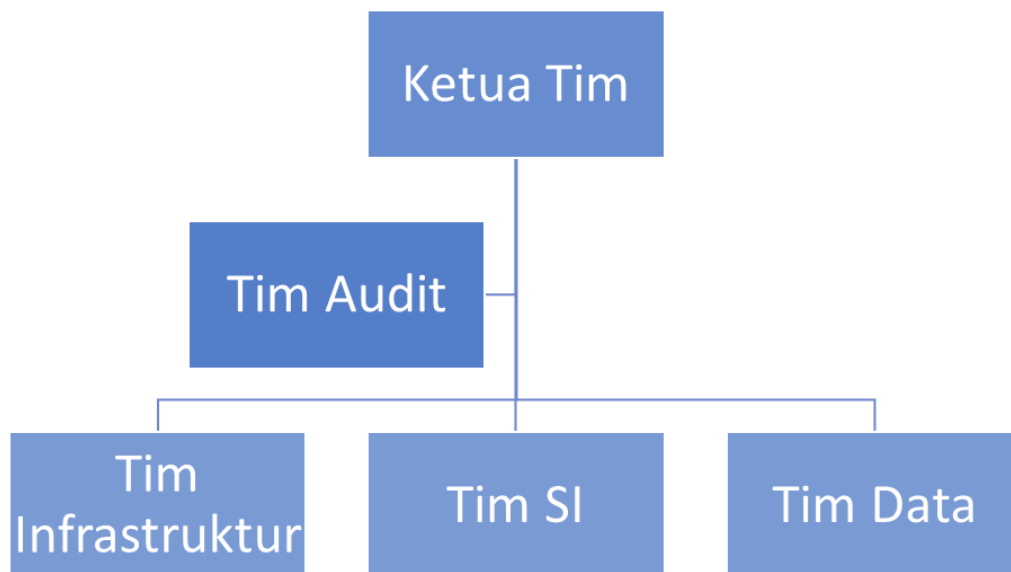
1. memastikan kebijakan keamanan informasi dan sasaran keamanan informasi ditetapkan dan selaras dengan Visi Misi Bank XYZ “**Menjadi The Most Valuable Banking Group dan Champion of Financial Inclusion**”;
2. memastikan persyaratan SMKI terintegrasi ke dalam proses bisnis yang berlaku;
3. memastikan 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 SMKI membutuhkan perangkat dokumen yang berisi aturan – aturan untuk memastikan bahwa proses SMKI dilaksanakan secara konsisten. Dokumen pada SMKI 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 SMKI 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.