Tugas 5

Team 1

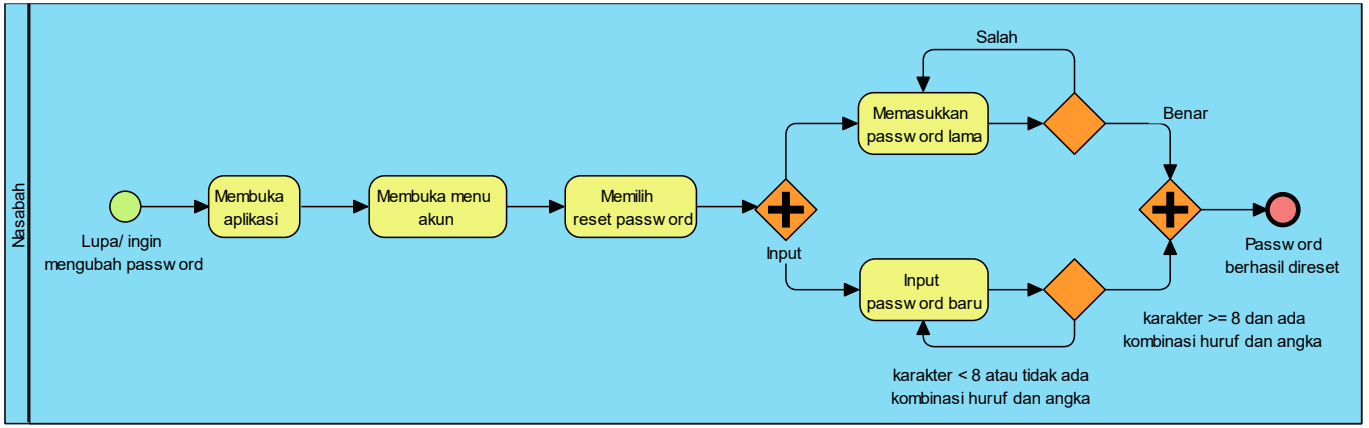
Nama Anggota Kelompok :

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

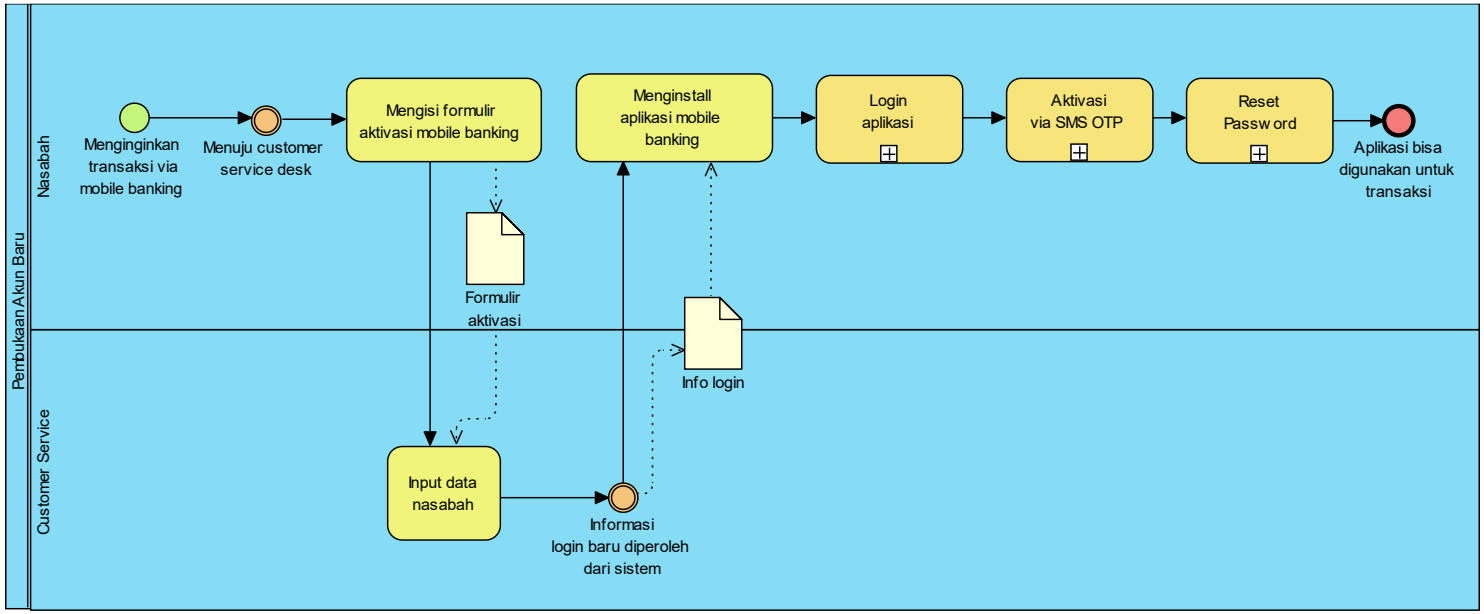
Nama Organisasi : Bank XYZ

Ruang Lingkup : Layanan Mobile Banking

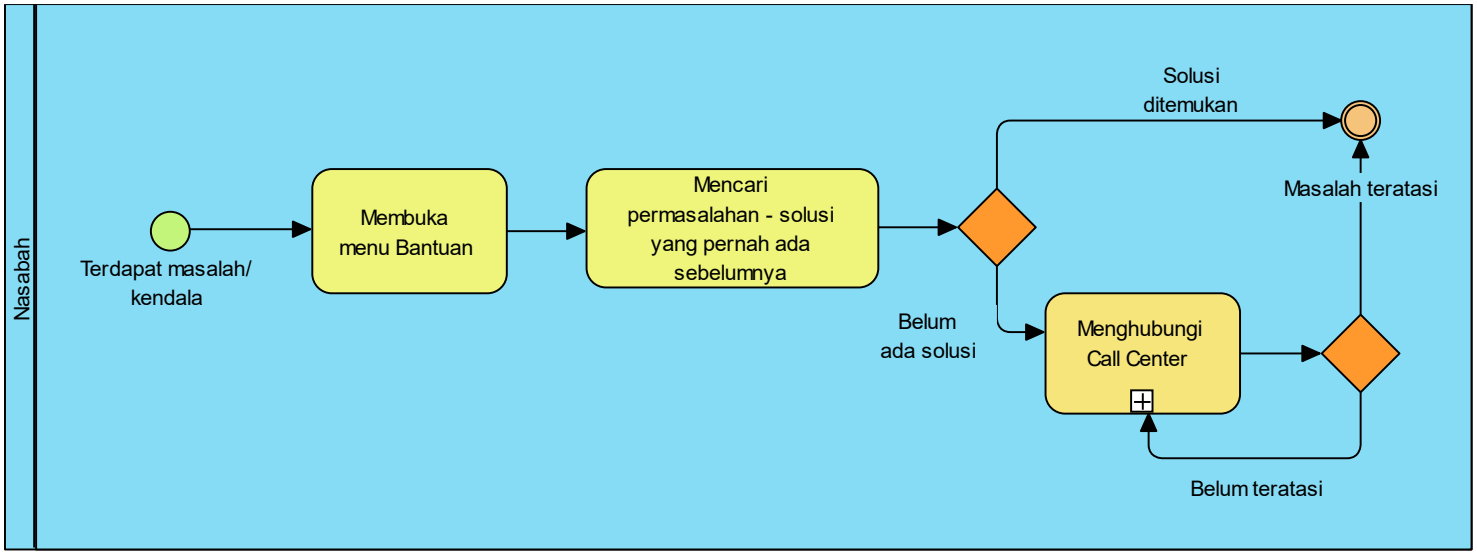
1. Flowchart Proses Bisnis



Gambar 1. Rubah Password Nasabah



Gambar 2 Pembuatan akun baru



Gambar 3. Layanan pengaduan nasabah

Versi 1.0
Tanggal 04/18/2022
Ruang Lingkup SMKI Mobile Banking - Bank XYZ

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 Managemen 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 SMKI
		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 dankontraktor menerapkan keamanan informasi berdasarkakan 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 ditetapkansesuai 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 harud 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 setlah 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 informasidan 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, kekritisan dan kerentanan terhadap penyingkapan atau modifikasi yang tidak sah.	Ya	Dilakukan diklat bagi setiap personal 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 bertangjawab 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 Physiacal 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	Melakukakn 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 rahasaia 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	Ditetpakan 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 acsess 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 Pasword 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 mensosilsakan 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 mensosilsakan 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 beratanggung 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 kebijkaan 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), pengubahan 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 pengubahan 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 kerahasian 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/BANXYZ/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 reviu layanan pemasok	Kendali Organisasi harus secara teratur memantau, mereviu 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, mereviu 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 diidentifikasikan	Kendali Privasi dan perlindungan informasi pribadi yang dapat diidentifikasikan 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