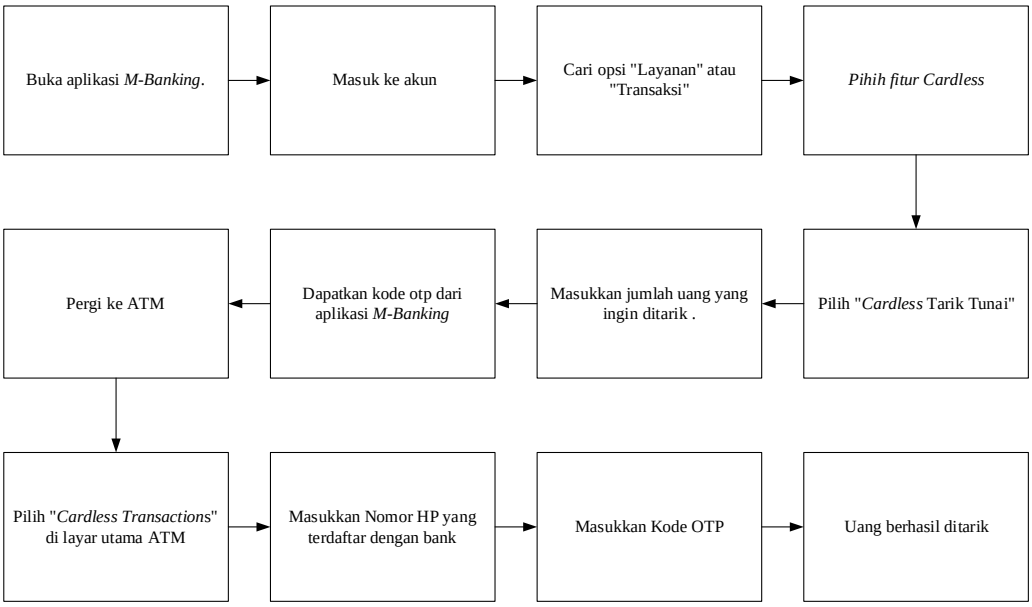
BAB IV
PEMBAHASAN

IV.1 Mekanisme Transaksi *Cardless Banking*

Terdapat 2 (dua) mekanisme dalam fitur *cardless banking* yaitu tarik tunai dan setor tunai. Alur mekanisme penarikan tunai pada fitur *cardless* dapat digambarkan pada gambar berikut ini:



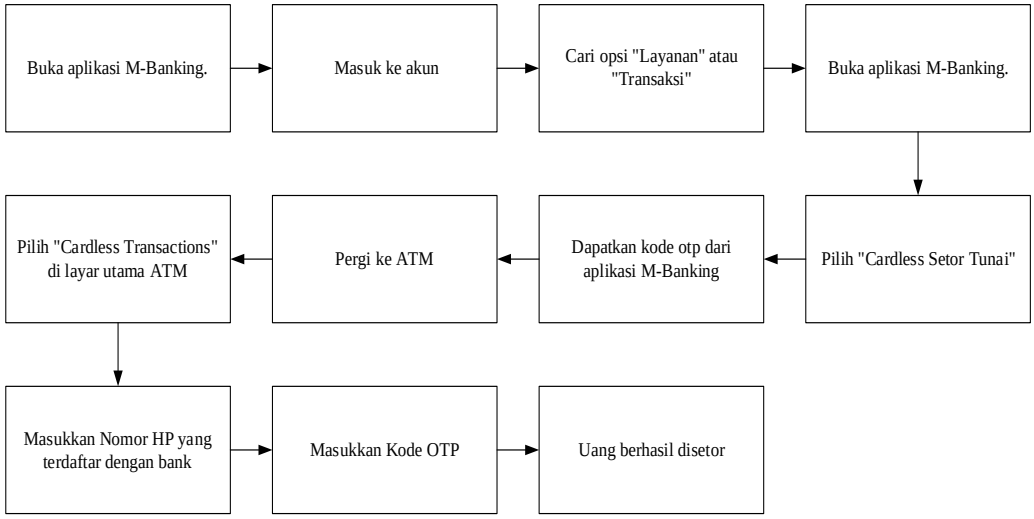
Sumber : Data diolah (2023)

Gambar 2. Diagram Alur penggunaan penarikan tunai pada fitur *cardless*

Proses dimulai dengan nasabah membuka aplikasi *mobile banking* yang terdapat pada perangkat ponsel dan masuk ke akun rekening. Selanjutnya, di dalam menu utama aplikasai *mobile banking* nasabah memilih opsi layanan atau transaksi. Di dalam menu layanan atau transaksi, pengguna dapat memilih fitur *cardless* lalu memilih *cardless* Tarik Tunai. Pada tahap ini, nasabah dapat memasukkan jumlah uang yang ingin ditarik. Setelah itu, aplikasi *mobile banking* akan membuat kode OTP yang akan digunakan dalam fitur penarikan *cardless* dan nasabah harus mencatat kode tersebut untuk dimasukkan ke dalam ATM. Langkah selanjutnya, nasabah pergi ke lokasi ATM yang tersedia dan memilih menu *cardless transaction* pada layar ATM. Lalu, Nasabah harus memasukkan nomor HP yang telah terdaftar

pada bank dan *mobile banking*. Jika nomor yang dimasukkan oleh nasabah benar, maka ATM akan meminta nasabah untuk memasukkan nomor OTP yang sebelumnya telah dibuat oleh *mobile banking*. Proses tarik tunai berhasil jika kode OTP yang dimasukkan oleh nasabah benar.

Sedangkan alur mekanisme penyetoran tunai pada fitur *cardless* dapat digambarkan pada gambar berikut ini:



Sumber : Data diolah (2023)

Gambar 3. Alur penggunaan penyetoran tunai pada fitur *cardless*

Proses dimulai dengan nasabah membuka aplikasi *mobile banking* yang terdapat pada perangkat ponsel dan masuk ke akun rekening. Selanjutnya, di dalam menu utama aplikasai *mobile banking* nasabah memilih opsi layanan atau transaksi. Di dalam menu layanan atau transaksi, pengguna dapat memilih fitur *cardless* lalu memilih *cardless* Setor Tunai. Setelah itu, aplikasi *mobile banking* akan membuat kode OTP yang akan digunakan dalam fitur penarikan *cardless* dan nasabah harus mencatat kode tersebut untuk dimasukkan ke dalam ATM. Langkah selanjutnya, nasabah pergi ke lokasi ATM yang tersedia dan memilih menu *cardless transaction* pada layar ATM. Lalu, Nasabah harus memasukkan nomor HP yang telah terdaftar pada bank dan *mobile banking*. Jika nomor yang dimasukkan oleh nasabah benar, maka ATM akan meminta nasabah untuk memasukkan nomor OTP yang sebelumnya telah dibuat oleh *mobile banking*. Langkah terakhir, nasabah diminta untuk memasukkan uang yang akan disetorkan kepada ATM.

Untuk menetapkan tujuan dan konteks dalam penulisan ini, pendekatan yang digunakan adalah dengan melakukan diskusi tentang risiko dan manajemen risiko dengan *expert* di setiap bagian.

IV.2 Identifikasi Risiko

Proses identifikasi risiko dalam penggunaan fitur *cardless* melibatkan observasi dan wawancara dengan ahli serta melakukan analisis terperinci terhadap risiko-risiko yang terkait. Dalam proses ini dilakukan pengamatan dan wawancara dengan pihak terkait, seperti pengguna, dan ahli, untuk memahami secara mendalam risiko-risiko yang mungkin timbul dalam penggunaan fitur *cardless*.

Setelah pengumpulan informasi yang komprehensif, risiko diidentifikasi daftar indikator risiko dengan uraian lengkap dan dampak yang mungkin terjadi terhadap setiap risiko. Dalam proses tersebut, tujuh jenis kejadian risiko berhasil teridentifikasi, yang terdiri dari tiga risiko terkait Kesalahan Sistem, dua risiko terkait Penipuan, satu risiko terkait keamanan aplikasi, dan satu risiko terkait ketidakhati-hatian pengguna.

Setiap jenis risiko memiliki uraian yang jelas, mencakup penyebab potensial dan kemungkinan dampak yang dapat terjadi. Uraian dan dampak risiko ini kemudian dikompilasi dalam sebuah tabel, yang memberikan gambaran yang komprehensif tentang risiko-risiko yang mungkin timbul dalam penggunaan fitur *cardless*. Tabel tersebut menjadi acuan risiko untuk mengambil tindakan pencegahan yang tepat dalam mengurangi risiko dan memastikan penggunaan yang aman dari fitur *cardless*.

Tabel 3. Dampak Risiko

No	Risiko	Uraian Risiko	Dampak
1	Kesalahan sistem	a. Gangguan dan kesalahan sistem pada transaksi *cardless*.	Hilangnya data transaksi, menyebabkan kerugian finansial atau kesulitan dalam mendapatkan informasi yang diperlukan.
		b. Uang di Mesin ATM tidak keluar ketika dilakukan penarikan	Kemungkinan kehilangan uang jika penarikan dicatat sebagai berhasil namun uang tidak keluar dari mesin.
		c. Uang yang disetorkan tertelan oleh mesin dan tidak terbaca	Kehilangan uang yang disetorkan, yang sulit untuk dipulihkan jika mesin tidak dapat membaca jumlah yang disetorkan dengan benar.
2	Penipuan	a. Penipuan melalui pesan teks atau email palsu yang meminta kode OTP.	Identitas dan informasi keuangan dapat diakses oleh penipu.
		b. Kode OTP/kode tarik dicuri oleh pihak lain.	Penyalahgunaan data pribadi dan keuangan pengguna.
3	Keamanan Aplikasi	a. Serangan siber seperti *malware* atau *hacking*	Potensi kerentanan terhadap serangan siber yang dapat mengakibatkan kebocoran data dan pencurian informasi pribadi dan keuangan.
4	Ketidak hati hatian pengguna	a. Kehilangan Perangkat atau dicuri sehingga aplikasi *cardless banking* dapat dibobol	Penyalahgunaan data dan keuangan pengguna oleh pihak yang menemukan atau mencuri perangkat tersebut.

Sumber : Data diolah (2023)

Dalam tabel tersebut dijelaskan bahwa tiap tiap risiko yang terjadi dalam penggunaan *cardless banking* mempunyai dampak yang berbeda-beda, berikut uraian penjelasan terhadap identifikasi dari risiko tersebnut:

1. Kesalahan pada sistem

   Risiko ini sering kali terjadi karena adanya Gangguan sistem pada transaksi *cardless*. Banyaknya transaksi yang di layani oleh sistem perbankan dan aplikasi *mobile banking* seringkali menyebabkan gangguan yang dapat berdampak dengan kegagalan masuk pada aplikasi *mobile banking* dan tidak keluar nya kode OTP. Gangguan sistem ini juga biasanya terjadi pada sistem karena matinya jaringan ATM, baik perawatan atau masalah teknis.

   Selanjutnya risiko yang dapat terjadi ialah uang di Mesin ATM tidak keluar ketika dilakukan penarikan. Seringkali, ketika menarik uang tunai dari ATM, nasabah mengalami masalah seperti saldo berkurang namun uang tidak keluar. Hal ini kadang terjadi di beberapa ATM. Ada beberapa kemungkinan yang dapat menyebabkan uang tidak keluar namun saldo berkurang, salah satunya adalah karena kesalahan sistem yang menjadi tanggung jawab pihak bank.

   Kemudian risiko serupa dapat terjadi seperti uang yang disetorkan tertelan oleh mesin dan tidak terbaca. Jika uang nasabah dalam kondisi lecek atau kusut akan membuat tidak terbaca oleh mesin ATM. Mesin ATM yang rusak atau mengalami kesalahan dapat menjadi penyebab uang nasabah tertelan oleh mesin ATM.

2. Penipuan

   Penipuan melalui pesan teks atau email palsu yang menargetkan layanan *cardless* merupakan salah satu risiko. Metode penipuan ini disebut dengan *Phising* yang secara definisi merupakan jenis serangan yang dilakukan dengan cara mengirim email atau pesan palsu dengan tujuan mencuri informasi pribadi atau keuangan, biasanya memanfaatkan identitas dari suatu instansi, perusahaan atau pihak yang mungkin dikenal oleh seseorang. Pelaku penipuan *phising* akan memalsukan alamat email dan tautan yang menyerupai instansi, perusahaan, merk terkenal. Terkadang pelaku *phising* berusaha menipu dengan cara

mengirimkan dokumen palsu, mengirim nomor resi, bukti transfer atau dokumen penting lainnya.

Kemudian risiko pada fitur *cardless banking* yang kerap terjadi ialah Kode OTP/kode tarik dicuri oleh pihak lain. Pada tahun 2020, dilansir dari Kompas.com. Direktorat Tindak Pidana Siber Bareskrim Polri berhasil menangkap 10 pelaku yang melakukan pembobolan sebanyak 3.070 rekening dengan cara menipu korban untuk mendapatkan kode OTP. Kerugian yang dialami oleh para nasabah mencapai Rp.21 miliar. Kejadian ini menunjukan bahwa masih banyak masyarakat yang kurang memahami pentingnya menjaga kerahasiaan kode OTP dan tidak boleh membagikan kepada orang lain, terutama kepada pihak yang mengaku-ngaku sebagai perwakilan bank atau pihak lainnya. Oleh karena itu, sangat penting bagi para nasabah untuk memahami apa itu OTP dan mengapa harus menjaganya agar terhindar dari kasus pembobolan rekening.

3. Keamanan Aplikasi

   Pada dasarnya sebuah sistem kemanan yang dirancang pada sebuah aplikasi tidak selalu sempurna. Terlebih lagi aplikasi pada bidang perbankan menjadi sasaran empuk bagi para *hacker* untuk meretas sistem keamanan tersebut dan mencari keuntungan dari perilaku tersebut. Salah satu contoh risiko tersebut ialah serangan siber berupa *malware* atau program jahat yang dapat menginfeksi perangkat dan sistem dengan tujuan merusak atau mencuri data - data pengguna seperti informasi login atau informasi lainnya. Serangan ini dapat membuat oknum – oknum yang tidak bertanggung jawab tersebut mengakses aplikasi *mobile banking* untuk melakukan penarikan dengan metode *cardless withdrawal.*

4. Ketidakhati-hatian pengguna

   Kehilangan perangkat seluler atau *handphone* dapat menjadi kerugian finansial dan waktu yang harus dikeluarkan untuk mencari atau membeli *handphone* baru, karena aplikasi perbankan, aplikasi *e-wallet*, data pribadi yang tersimpan di dalamnya juga berpotensi untuk disalahgunakan oleh pihak yang tidak bertanggung jawab. Ketika seseorang kehilangan *handphone*, risiko terhadap keamanan keuangan mereka dapat meningkat. Misalnya, jika seseorang telah

mengaktifkan layanan *mobile banking* di perangkatnya, maka potensi penyalahgunaan informasi dan akses ke akun perbankan mereka dapat terjadi. Transaksi *cardless* yang dilakukan melalui *mobile banking* dapat mengekspos pengguna terhadap risiko kehilangan saldo di rekening bank mereka.

Berdasarkan hasil identifikasi risiko maka didapatkan skala kemungkinan – kemungkinan dari risiko pada penggunaan *cardless banking* dapat dilihat pada tabel berikut:

Tabel 4. Kerangka Pengukuran Probabilitas

Probabilitas		**Kriteria**
Rating	%	
1	0-10	Sangat tidak mungkin/hampir mustahil
2	10-30	Kecil kemungkinan, tapi tidak mustahil
3	30-50	Kemungkinan terjadi
4	50-90	Sering terjadi
5	>90	Hampir pasti terjadi

Sumber : Data diolah (2023)

Berdasarkan hasil identifikasi risiko maka didapatkan skala dampak dari risiko pada penggunaan *cardless banking* dapat dilihat pada tabel berikut:

Tabel.5 Kerangka Pengukuran Dampak

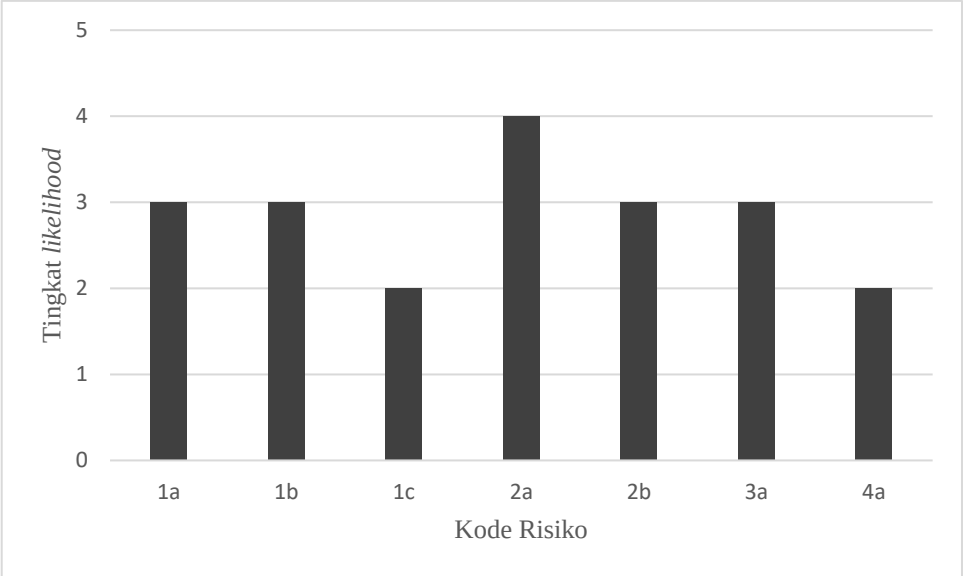
Dampak		**Keterangan**
Skala	**Rating**	
1	Sangat Rendah	Dapat ditangani pada kegiatan rutin.
2	Kecil	Mengancam efisiensi dan efektivitas beberapa aspek program dan sedikit mempengaruhi stakeholder.
3	Menengah / Medium	Kerugian keuangan cukup besar dan mempengaruhi stakeholder
4	Besar	Kerugian cukup besar dari segi keuangan maupun kelangsungan perusahaan
5	Sangat Tinggi / Katastropik	Kerugian sangat besar dari segi keuangan maupun kelangsungan perusahaan

Sumber : Data diolah (2023)

IV.3 Pengukuran Risiko

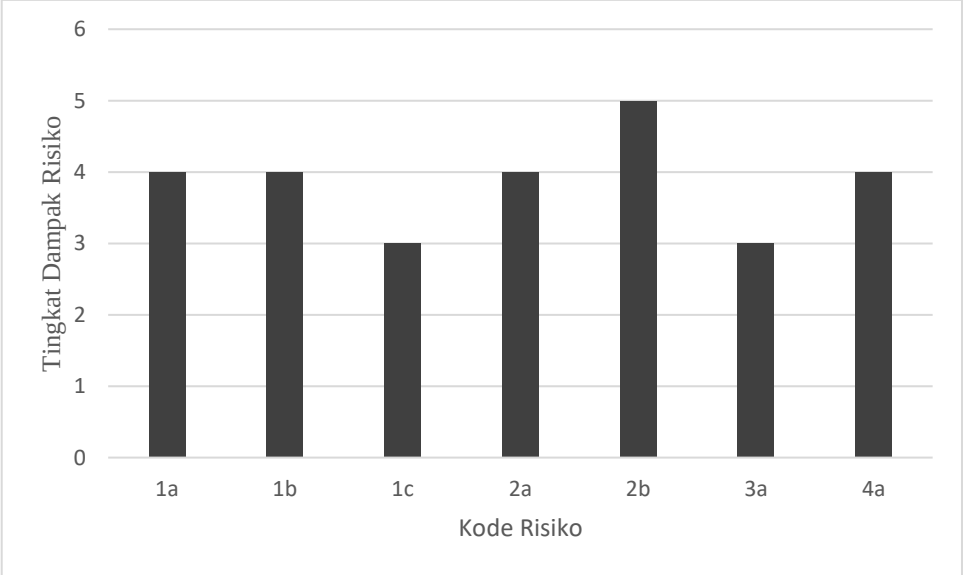
Setelah melakukan identifikasi terhadap risiko apa saja yang terdapat dalam penggunaan *cardless*, dilakukan pengukuran dan peniliaian oleh *expert* menggunakan metode *expert judging* yang dilakukan dengan wawancara untuk mengetahui tingkat skala probabilitas, skala dampaknya sehingga mendapatkan status risiko.

Selanjutnya hasil dari pengukuran dan penilaian ini akan memberikan status risiko untuk setiap potensi masalah yang teridentifikasi. Risiko dapat diberi label sebagai risiko tinggi, sedang, atau rendah, tergantung pada tingkat probabilitas dan dampak yang ditentukan oleh para ahli. Status risiko ini akan menjadi dasar untuk pengembangan strategi mitigasi yang tepat guna mengurangi risiko yang muncul dalam penggunaan *cardless*. Selain itu, informasi ini dapat sigunakan untuk merancang langkah-langkah keamanan yang lebih baik berdasarkan status risikonya.



Sumber : Data diolah (2023)

Gambar 4. Grafik Tingkat *Likelihood*



Sumber : Data diolah (2023)

Gambar 5. Grafik Tingkat Dampak Risiko

Tabel 6. Pengukuran Risiko

No	Risiko	Uraian Risiko	Skala Probabilitas	Skala Dampak	Status Risiko
1	Kesalahan sistem	a. Gangguan dan kesalahan sistem pada transaksi *cardless*.	3	4	12
		b. Uang di Mesin ATM tidak keluar ketika dilakukan penarikan	3	4	12
		c. Uang yang disetorkan tertelan oleh mesin dan tidak terbaca	2	3	6
2	Penipuan	a. Penipuan melalui pesan teks atau email palsu yang meminta kode OTP.	4	4	16
		b. Kode OTP/kode tarik dicuri oleh pihak lain.	3	5	15
3	Keamanan Aplikasi	a. Serangan siber seperti *malware* atau *hacking*	3	3	9
4	Ketidak hati hatian pengguna	a. Kehilangan Perangkat atau dicuri sehingga aplikasi *cardless banking* dapat dibobol	2	4	8

Sumber : Data diolah (2023)

Pada langkah ini, matriks risiko digunakan untuk mengidentifikasi risiko-risiko yang paling prioritas untuk ditangani. Setiap nilai risiko, termasuk tingkat kemungkinan terjadinya (*occurrence*) dan tingkat keparahan (*severity*), dimasukkan ke dalam matriks risiko untuk membantu penyusun memahami tingkat kejadian risiko yang berbeda, seperti risk level *extreme*, *high*, *moderate*, *low*, dan *very low*.

IV.4 Pemetaan Risiko

Pemetaan risiko ini juga memberikan kemudahan bagi peneliti untuk memprioritaskan respons atau penanganan risiko yang paling penting. Tabel berikut menunjukkan hasil matriks risiko dari kejadian risiko yang terkait dengan penggunaan fitur cardles. Berikut merupakan tabel matriks analisis risiko:

Tabel 7. Peta/Profil Risiko

Matriks Analisis Risiko 5x5			**Dampak**				
			1	**2**	**3**	**4**	**5**
Diskripsi	**Probabi-litas**	***Like-lihood***	**Sangat Rendah**	**Kecil**	**Medium**	**Besar**	**Katas-tropic**
Hampir Pasti	**90%**	**5**					
Kemungki-nan Besar	**70%**	**4**				2a	
Mungkin	**50%**	**3**			3a	1a,1b	2b
Kemungki-nan Kecil	**30%**	**2**			1c	4a	
Sangat Jarang	**10%**	**1**					

Sumber : Data diolah (2023)

Setelah melakukan pemetaan risiko penggunaan *cardless*, Berdasarkan tabel tersebut, terdapat berbagai tingkat risiko dalam transaksi *cardless banking*. Penipuan melalui pesan teks atau email palsu yang meminta kode OTP memiliki level risiko tertinggi dengan skor 16, diikuti oleh pencurian kode OTP/kode tarik

oleh pihak lain dengan level risiko 15. Gangguan dan kesalahan sistem pada transaksi *cardless* serta uang yang tidak keluar dari mesin ATM saat penarikan memiliki level risiko sebanding dengan skor 12. Risiko serangan siber seperti *malware* atau *hacking* memiliki level risiko 9, sementara kehilangan perangkat atau pencurian yang dapat menyebabkan aplikasi *cardless banking* dibobol memiliki level risiko 8. Risiko terendah adalah uang yang tertelan oleh mesin dan tidak terbaca, dengan level risiko 6. Untuk mengatasi risiko-risiko ini, diperlukan langkah-langkah mitigasi yang sesuai agar keamanan dalam transaksi *cardless banking* tetap terjaga.

Selanjutnya, perhitungan pada matriks analisis risiko yang telah dikalukan sebelumnya, risiko tersebut dapat diurutkan dengan prioritas risiko berdasarkan status risikonya. Mitigasi akan diprioritaskan terhadap risiko dengan nilai paling tinggi.

Tabel 8. Urutan prioritas risiko *cardless banking*

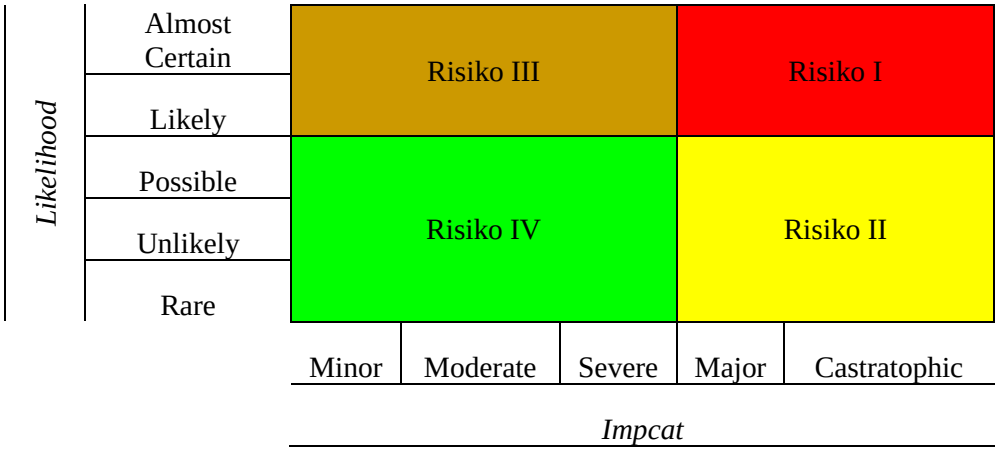
No	Kode	Uraian Risiko	Level Risiko
1	2a	Penipuan melalui pesan teks atau email palsu yang meminta kode OTP	16
2	2b	Kode OTP/kode tarik dicuri oleh pihak lain.	15
3	1a	Gangguan dan kesalahan sistem pada transaksi *cardless*.	12
4	2b	Uang di Mesin ATM tidak keluar ketika dilakukan penarikan.	12
5	3a	Serangan siber seperti *malware* atau *hacking*	9
6	4a	Kehilangan Perangkat atau dicuri sehingga aplikasi *cardless banking* dapat dibobol	8
7	1c	Uang yang disetorkan tertelan oleh mesin dan tidak terbaca	6

Sumber : Data diolah (2023)

Penipuan melalui pesan teks atau email palsu yang meminta kode OTP menjadi prioritas paling tinggi. Selanjutnya pencurian kode OTP oleh pihak lain mempunyai tingkat prioritas ke-dua. Gangguan dan kesalahan sistem serta uang di Mesin ATM tidak keluar mempunyai level risiko yang sama.

IV.5 Mitigasi Risiko

Tabel 9. Peta Risiko



Sumber : Data diolah (2023)

Upaya pengurangan risiko dilakukan terhadap risiko-risiko dengan nilai yang signifikan berdasarkan pengukuran serta pemetaan yang sudah dilakukan pada tahap sebelumnya. Tindakan mitigasi dilaksanakan untuk mengurangi kemungkinan terjadinya risiko serta dampak yang mungkin ditimbulkan oleh risiko tersebut.

Setiap tingkat risiko memiliki pendekatan yang berbeda. Pada tingkat risiko kuadran I, yang dapat mengancam pencapaian tujuan perusahaan, risiko ditangani dengan menghindarinya, yaitu dengan tidak melakukan atau menghentikan kegiatan yang meningkatkan risiko. Pada tingkat risiko kuadran II, yang berbahaya tetapi jarang terjadi, risiko ditangani dengan membaginya kepada pihak lain. Pada tingkat risiko kuadran III, yang terjadi secara rutin, risiko ditangani dengan menguranginya, misalnya melalui perbaikan prosedur, kebijakan baru, penggantian atau pembelian peralatan. Pada tingkat risiko kuadran IV, yang tidak berbahaya, risiko ditangani dengan menerima risiko dalam batas toleransi dan mengelolanya agar tidak berkembang menjadi tingkat yang tinggi.

Adapun cara pengendalian ataupun mitigasi terhadap risiko – risiko tersebut dapat ditangani dengan berbagai cara sebagai berikut:

1. Gangguan dan kesalahan sistem pada transaksi *cardless*

   Mitigasi :

   Nasabah dapat melaporkan kepada pihak bank dengan mencatat kapan terjadinya gangguan sistem dan layanan, transaksi apa yang dilakukan serta bukti-bukti terkait Ketika terjadinya kesalahan sistem saat menggunakan fitur *cardless.*

   Pihak bank juga harus rutin melakukan pemeliharaan sistem pada layanan aplikasi *mobile banking* agar tidak terjadinya risiko tersebut dan merugikan banyak nasabah.
2. Uang di Mesin ATM tidak keluar ketika dilakukan penarikan

   Mitigasi :

   Nasabah dapat menuunggu selama 5 hingga 10 menit. Ada kemungkinan uang akan keluar secara tiba-tiba dari mesin ATM, atau mungkin uang tidak akan keluar dan akan dikembalikan dengan sendirinya melalui proses pengembalian dana.

   Apabila langkah pertama tidak berhasil, Nasabah dapat segera melaporkannya kepada pihak bank, baik dengan datang langsung ke bank atau menggunakan layanan call-center yang disediakan oleh bank tersebut.

   Tunggu proses dari bank. Setelah melaporkan masalah bahwa uang tidak keluar namun saldo berkurang, laporan tersebut akan diproses dalam beberapa waktu, tergantung pada sumber masalah yang menyebabkannya. Setelah proses laporan selesai, bank akan mengembalikan uang baik dalam bentuk saldo rekening maupun uang tunai. Penyebab masalah ini dapat beragam, seperti gangguan pada sistem bank atau kerusakan mesin ATM. Prosedur pelaporan yang digunakan dalam situasi ini sama, tidak tergantung pada bank yang digunakan.
3. Uang yang disetorkan tertelan oleh mesin dan tidak terbaca

   Mitigasi :

   Memberikan panduan yang jelas kepada pengguna mengenai cara yang benar untuk menyimpan uang dan menghindari masalah dalam proses penyetoran. Menerapkan prosedur yang ketat untuk menangani situasi Ketika uang terjebak

di dalam mesin, termasuk pelaporan, penelusuran dan pengembalian dana dengan cepat kepada pengguna.

4. Penipuan melalui pesan teks atau email palsu yang meminta kode OTP.

   Mitigasi :

   Memberikan pemahaman yang jelas kepada pengguna mengenai komunikasi resmi dan valid dari bank atau Lembaga keuangan menunjukan metode yang tepat untuk berinteraksi dan membagikan informasi sensitif.

   Kode OTP merupakan seperti kunci rumah yang sangat penting. Bahkan, pihak yang mengaku sebagai institusi seharusnya tidak akan meminta kode OTP. Kode OTP/kode tarik dicuri oleh pihak lain. Pengguna juga harus diberikan pemahanan untuk tidak memberikan yang diterima saat menggunakan aplikasi kepada siapa pun. Berbagi kode OTP adalah sebuah kesalahan yang serius.

5. Kode OTP ditarik / dicuri oleh pihak lain.

   Mitigasi :

   Pengguna dapat menerapkan teknologi otentikasi yang kuat, seperti verifikasi sidik jari atau pengemalan wajah, sebagai Langkah tambahan untuk melindungi akun pengguna dari upaya pencurian kode OTP. Serta dapat melakukan pergantian *password* secara berkala pada aplikasi atau perbankan yang digunakan. Pengguna dapat membuat PIN yang unik untuk setiap aplikasi yang digunakan, misalnya dengan mengombinasikan angka dan huruf agar sulit ditebak oleh orang lain.

6. Serangan siber seperti *malware* atau *hacking*

   Mitigasi :

   Nasabah harus melindungi data pribadinya, Di dunia maya, penting bagi nasabah untuk menjaga kerahasiaan data pribadi dengan tidak membagikannya kepada orang asing, termasuk dalam hal *one-time password* (OTP). Selain itu, nasabah harus menghindari menampilkan nomor telepon pribadi secara sembarangan jika tidak diperlukan, misalnya dengan menyertakan nomor HP pribadi dalam CV online yang kemudian unggah di media sosial.

   Selanjutnya, meningkatkan keamanan data Salah satu cara untuk menghindari *phising* adalah dengan meningkatkan keamanan data yang miliki di dunia maya. Misalnya, aktifkan autentikasi dua faktor (2FA) untuk akun yang nasabah

daftarkan di internet. Selain itu, juga dapat menggunakan surel khusus untuk membuat akun media sosial dan akun yang berisi informasi keuangan yang digunakan untuk transaksi daring.

7. Kehilangan Perangkat atau dicuri sehingga aplikasi *cardless banking* dapat dibobol

   Mitigasi :

   Perangkat dilindungi dengan pengamanan yang kuat, seperti kunci layar, pola, PIN, atau sidik jari. Jika hilang atau dicuri, orang lain akan kesulitan untuk mengaksesnya. Nasabah juga dapat menerapkan fitur penguncian perangkat jarak jauh, sehingga perangkat yang hilang atau dicuri dapat dinonaktifkan dan dihapus data di dalamnya. Selain itu, nasabah harus segera hubungi penyedia layanan perbankan dan melaporkan untuk mematikan akses ke fitur *cardless banking* agar mencegah orang lain untuk melakukan transaksi tanpa izin.