STRATEGI PENERAPAN MANAJEMEN RISIKO UNTUK MENCEGAH KEJAHATAN SIBER DI *MOBILE BANKING* PADA BANK PEMBANGUNAN DAERAH YOGYAKARTA KANTOR CABANG SYARIAH

Disusun oleh

YUNAN DWI PRASETYO

20213067

PROGRAM STUDI ANALISIS KEUANGAN

PROGRAM SARJANA TERAPAN

FAKULTAS BISNIS DAN EKONOMIKA

UNIVERSITAS ISLAM INDONESIA

JULI, 2024

PERNYATAAN KEASLIAN SKRIPSI

Saya menyatakan dengan sesungguhnya bahwa Skripsi dengan judul "Strategi Penerapan Manajemen Risiko Untuk Mencegah Kejahatan Siber Di *Mobile banking* Pada Bank Pembangunan Daerah Yogyakarta Kantor Cabang Syariah" yang disusun untuk melengkapi sebagian persyaratan menjadi Sarjana Terapan pada Program Studi Analisis Keuangan, Program Sarjana Terapan, Fakultas Bisnis dan Ekonomika, Universitas Islam Indonesia, sejauh yang saya ketahui bukan merupakan tiruan atau duplikasi dari Skripsi yang sudah dipublikasikan dan atau pernah dipakai untuk mendapatkan gelar Sarjana Terapan di lingkungan Universitas Islam Indonesia maupun di perguruan tinggi atau instansi manapun, kecuali bagian yang sumber informasinya dicantumkan sebagaimana mestinya.

Yogyakarta, 17 Juli 2024

Yunan Dwi Prasetyo

20213067

ii

HALAMAN PERSETUJUAN

Skripsi dengan judul "Strategi Penerapan Manajemen Risiko Untuk Mencegah Kejahatan Siber Di *Mobile banking* Pada Bank Pembangunan Daerah Yogyakarta Kantor Cabang Syariah" disusun untuk melengkapi sebagain persyaratan menjadi Sarjana Terapan pada Program Studi Analisis Keuangan, Program Sarjana Terapan, Fakultas Bisnis dan Ekonomika, Universitas Islam Indonesia, dan disetujui untuk diajukan dalam sidang ujian Skripsi.

Yogyakarta,

Pembimbing

Dr. Phil. Ninik Sri Rahayu, SE., MM.

NIK: 052130103

Mengetahui,

Ketua Program Studi

Dr. Phil. Ninik Sri Rahayu, SE., MM.

NIK: 052130103

HALAMAN PENGESAHAN

Skripsi dengan judul "Strategi Penerapan Manajemen Risiko Untuk Mencegah Kejahatan Siber Di *Mobile banking* Pada Bank Pembangunan Daerah Yogyakarta Kantor Cabang Syariah", telah dipertahankan dalam ujian wawancara dan diterima sebagai syarat menjadi Sarjana Terapan, Program Studi Analisis Keuangan, Program Sarjana Terapan, Fakultas Bisnis dan Ekonomika, Universitas Islam Indonesia, pada tanggal 29 Juli 2024

Tim penguji

Penguji I,

Dr. Phil. Ninik Sri Rahayu, SE., MM.
NIK: 052130103

Penguji II,

Dra. Indah Susantun, M.Si
NIK: 883110104

Mengetahui,
Ketua Program Studi

Dr. Phil. Ninik Sri Rahayu, SE., MM.
NIK: 052130103

iv

KATA PENGANTAR

Puji syukur kehadirat Allah Subhanahu wa Ta'ala, atas segala limpahan Rahmat-Nya beserta Karunia-Nya. Shalawat serta salam yang senantiasa tercurahkan kepada baginda Nabi Muhammad Shalallahu'Alaihi Wassalam, sehingga penulis dapat menyelesaikan laporan skripsi ini yang berjudul terkait **"Strategi Penerapan Manajemen Risiko Untuk Mencegah Kejahatan Siber Di *Mobile banking* Pada Bank Pembangunan Daerah Yogyakarta Kantor Cabang Syariah"**

Penelitian ini bertujuan untuk sebagai salah satu persyaratan menjadi Sarjana Terapan pada Program Studi Analisis Keuangan, Fakultas Bisnis dan Ekonomika, Universitas Islam Indonesia. Diharapkan hasil studi ini akan memberikan kontribusi terhadap akademik, mahasiswa, insatansi, dan juga penelitian selanjutnya. Atas tersusunnya laporan skripsi ini, penulis mengucapkan terimakasih khususnya kepada:

1. Ibu (Sudarti) saya yang selalu mendampingi saya dan memberikan dukungan baik materi, moril, nasihat, doa serta kasih sayang yang tak terhingga sehingga saya dapat menyelesaikan skripsi ini dengan baik.
2. Bapak (Puguh Wahyudi) saya yang selalu mendampingi saya dan memberikan dukungan baik materi, moril, nasihat, doa serta kasih sayang yang tak terhingga sehingga saya dapat menyelesaikan skripsi ini dengan baik.
3. Kakak saya, Maritha Eka Puji Panestri yang telah memberikan dukungan dan semangat untuk dapat menyelesaikan skripsi ini.
4. Ibu Dr. Phil. Ninik Sri Rahayu, SE., MM. selaku kaprodi dan serta dosen pembimbing riset terapan telah memberikan bimbingan dan arahan sehingga saya dapat dengan mudah dalam melaksanakan proses riset dan penyusunan laporan skripsi ini.
5. Bapak/Ibu dosen yang sudah membimbing saya dalam membekali pembelajaran selama ini.

6. Sahabat saya Destya Eka Nurviana yang senantiasa membantu saya, berdiskusi, dan memberikan masukan serta semangat sehingga dapat menyelesaikan skripsi ini dengan baik.
7. Sahabat, teman-teman seangkatan, dan semua pihak yang tidak dapat saya sebutkan satu persatu.
8. Diri saya sendiri Yunan Dwi Prasetyo terimakasih sudah mau berjuang sejauh ini. Terimakasih sudah memilih untuk tetap berusaha dan semangat untuk merayakan setiap hal kecil yang dilakukan.

Penulis berharap semoga laporan skripsi ini dapat bermanfaat bagi pembaca serta dapat menjadi bahan referensi untuk mahasiswa lain yang akan melaksanakan penelitian selanjutnya. Semoga ALLAH SWT berkenan membalas segala kebaikan pihak yang sudah terlibat dalam penulisan laporan skripsi ini. Dengan ini penulis sampaikan terimakasih atas perhatian pembaca.

Yogyakarta, 17 Juli 2024

Yunan Dwi Prasetyo

20213067

ABSTRAK

Kehadiran *mobile banking* pada bank BPD DIY Syariah sudah banyak dimanfaatkan oleh masyarakat. Hal ini dapat dilihat dari banyak masyarakat yang bergantung pada *mobile banking* dalam bertransaksi sehari-hari. Tingginya penggunaan *mobile banking* mengakibatkan juga maraknya kejahatan siber yang akan terjadi. Tujuan dari penelitian ini yaitu untuk mengetahui praktik strategi manajemen risiko, seberapa efektif strategi manajemen risiko, dan apa tantangan utama dalam menerapkan strategi manajemen risiko untuk mencegah kejahatan siber di *mobile banking* pada Bank Pembangunan Daerah Yogyakarta Kantor Cabang Syariah. Metode penelitian yang digunakan pada penelitian ini yaitu menggunakan *Mixed methods* dengan cara penyebaran kuesioner dan juga Wawancara Key Informant Interview (KII). Hasil penelitian ini menunjukan ada beberapa faktor seperti bagaimana praktik manajemen risiko, seberapa efektif strategi manajemen risiko, dan apa tantangan utama dalam menerapkan strategi manajemen risiko. Rekomendasi praktik dan inovatif yang dapat dilakukan oleh bank untuk keamanan *mobile banking.*

Kata kunci: Perbankan seluler, Manajemen risiko, Kejahatan siber

ABSTRACT

The presence of *mobile banking* at BPD DIY Syariah banks has been widely used by the public. This can be seen from many people who depend on *mobile banking* in their daily transactions. The high use of *mobile banking* has resulted in the rampant cybercrime that will also occur. The purpose of this study is to find out the practice of risk management strategies, how effective are risk management strategies, and what are the main challenges in implementing risk management strategies to prevent cybercrime in *mobile banking* at Bank Pembangunan Daerah Yogyakarta Sharia Branch Office. The research method used in this study is using mixed methods by distributing questionnaires and also Key Informant Interview (KII). The results of this study show that there are several factors such as how risk management practices are, how effective the risk management strategy is, and what are the main challenges in implementing risk management strategies. Recommendations for practices and innovations that banks can do for *mobile banking* security.

Keywords: Mobile banking, Risk management, Cybercrime

DAFTAR ISI

DAFTAR TABEL

BAB I
PENDAHULUAN

1.1 Latar Belakang Masalah

Teknologi Informasi dan Komunikasi membuat industri perbankan sangat kompetitif dengan inovasi dalam produk dan layanan perbankan elektronik. Kemampuan manajemen untuk mengelola teknologi baru secara signifikan memastikan tingkat keberhasilan dalam pengembangan inovasi layanan (Ngamal & Perajaka, 2022). Sektor perbankan menyediakan inovator untuk layanan perbankan berbasis teknologi, yang dapat memberikan kemudahan, kecepatan dan keamanan dalam hal melakukan transaksi pembayaran dan transaksi lainnya, sehingga perusahaan yang melakukan layanan perbankan berusaha memberikan nilai lebih kepada nasabah mereka melalui layanan yang sesuai dengan kebutuhan sehari-hari nasabah, salah satu layanan bank adalah *Mobile Banking* (Prakosa, 2019).

Mobile banking adalah layanan perbankan untuk melakukan berbagai transaksi perbankan melalui berbagai fungsi di ponsel pintar (*smartphone*). *Mobile banking* dapat melakukan transaksi yang berbeda tanpa harus datang langsung ke bank (Putra & Sari, 2020). Otoritas Jasa Keuangan (OJK) mencatat bahwa dari tahun 2016 hingga 2021, terjadi peningkatan data sebesar 300% terkait penggunaan *Mobile banking* dan *e-banking*, peningkatan transaksi tersebut disebabkan oleh perubahan transportasi umum dalam penggunaan teknologi digital untuk kegiatan perbankan, dalam hal ini bank mengembangkan layanan dan produk digital, selama pandemi Covid-19. Berdasarkan pernyataan tersebut, kehadiran *Mobile banking* semakin meningkat dari tahun ke tahun (Sari et al., 2022). Di sisi lain, *Mobile banking* memiliki kelebihan dan manfaat, ada sejumlah risiko atau ancaman yang perlu dipertimbangkan, dan kejahatan dunia maya salah satunya yang sangat berbahaya bagi nasabahnya. Karena fasilitas *Mobile banking* kini sengaja disalahgunakan oleh banyak pihak, kejahatan siber, penipuan, dan pembobolan rekening (Pratama & Pratika, 2020).

Kejahatan siber atau kejahatan dunia maya adalah jenis kejahatan atau tindakan kriminal yang menggunakan teknologi komputer berbasis dunia internet yang saat ini sangat canggih dan sangat cepat. Di media online, kini sangat sering terjadi kasus kejahatan, mulai dari penipuan hingga penipuan jual beli (Ningrum & Robekha, 2023). Menurut Sulisrudatin (2018), Kejahatan siber di Indonesia 99% *social engineering*. *Social engineering* atau rekayasa sosial adalah kejahatan yang mempengaruhi pikiran orang dengan perasaan sedih dan senang. Metode ini adalah salah satu cara paling umum di mana penjahat dunia maya dapat menipu dan menipu calon korban. Pelaku akan mengaku sebagai *customer service* atau pegawai bank maupun lembaga keuangan lainnya. Skripsi ini akan berfokus pada permasalahan mengenai **Strategi Penerapan Manajemen Risiko Untuk Mencegah Kejahatan Siber Di *Mobile banking* Pada Bank Pembangunan Daerah Yogyakarta Kantor Cabang Syariah.**

1.2 Rumusan Masalah

Berdasarkan latar belakang di atas, adapun rumusan masalah pada penelitian ini antara lain

1. Apa praktik manajemen risiko saat ini yang digunakan dalam *mobile banking* untuk mencegah kejahatan siber?
2. Seberapa efektif strategi manajemen risiko ini dalam mencegah kejahatan siber di *mobile banking*?
3. Apa tantangan utama dalam menerapkan strategi manajemen risiko untuk keamanan *mobile banking*?
4. Praktik terbaik dan pendekatan inovatif apa yang dapat direkomendasikan untuk meningkatkan manajemen risiko untuk mencegah kejahatan siber di *mobile banking*?

1.3 Tujuan Penelitian

Penelitian ini bertujuan untuk:

1. Untuk melakukan apa praktik manajemen risiko saat ini yang digunakan dalam *mobile banking* untuk mencegah kejahatan siber

2. Untuk mengevaluasi seberapa efektif strategi manajemen risiko ini dalam mencegah kejahatan siber di *mobile banking*
3. Untuk mengidentifikasi apa tantangan utama dalam menerapkan strategi manajemen risiko untuk keamanan *mobile banking*
4. Untuk melakukan praktik terbaik dan pendekatan inovatif apa yang dapat direkomendasikan untuk meningkatkan manajemen risiko untuk mencegah kejahatan siber di *mobile banking*

1.4 Manfaat

1.4.1 Manfaat Teoritis

Penelitian ini penting dilakukan terkait pengguna *mobile banking* yang rawan terjadinya kejahatan siber dan dapat meminimalisir terjadinya tindak kejahatan siber pada layanan *mobile banking*. Meskipun sudah banyak kajian mengenai kejahatan siber, namun pada penelitian ini lebih berfokus pada penerapan manajemen risiko untuk mencegah tindak kejahatan siber pada layanan *mobile banking* di Bank BPD DIY Syariah yang diharapkan hasil penelitian ini dapat memberikan ilmu dan wawasan kepada mahasiswa UII sebagai masukan untuk pengembangan ilmu perbankan khususnya tentang pencegahan kejahatan siber pada layanan *mobile banking*. Serta dapat mengelola dan meminimalisir terjadinya risiko lainnya kedepanya.

1.4.2 Manfaat Praktis

Penelitian ini diharapkan bermanfaat bagi BPD DIY Syariah untuk menjadi bahan pertimbangan dalam pencegahan tindak kejahatan siber pada layanan *mobile banking* guna meningkatkan citra baik perbankan syariah dan meminimalisir risiko yang akan terjadi pada bank dan nasabah.

BAB II
KAJIAN PUSTAKA

2.1 Landasan Teori

2.1.1 *Mobile banking*

Mobile banking merupakan layanan yang disediakan oleh bank atau lembaga keuangan lainnya yang memungkinkan bagi nasabah untuk melakukan transaksi keuangan jarak jauh menggunakan *handphone* seperti *smartphone* atau tablet. *Mobile banking* memiliki layanan utama yang hampir mirip dengan yang ditawarkan langsung oleh bank, seperti melihat saldo rekening, transfer, penarikan tanpa kartu, pembayaran tagihan, dan pembayaran lainnya (Purwanto & Loisa, 2020).

Perkembangan *Mobile banking* dari waktu ke waktu menjadi semakin cepat, dan sudah banyak di Indonesia yang menawarkan *Mobile banking*. Bank menawarkan layanan *Mobile banking* untuk memenuhi persyaratan dan kebutuhan masyarakat agar tidak ketinggalan zaman menggunakan teknologi modern seperti sekarang ini. *Mobile banking* memiliki dampak positif bagi masyarakat umum, karena memiliki banyak fitur dan keunggulan dalam penggunaannya. Nasabah yang menggunakan *Mobile banking* dapat dengan mudah mengakses banyak fitur perbankan seperti transfer uang, cek saldo, pembayaran tagihan, pembelian pulsa dan token listrik, dan lain-lain. Selain itu, layanan ini bekerja nonstop selama 24 jam dan dapat diakses di mana saja, kapan saja (Mutiasari, 2020).

Transaksi dengan *Mobile banking* memiliki banyak keuntungan bagi nasabah yang menggunakan fasilitasnya, namun di sisi lain, layanan *Mobile banking* ini memiliki beberapa kelemahan. Seperti kesalahan dalam operasi (*human error*), penipuan (*fraud*), kejahatan siber, dan kesalahan lain yang terjadi dalam penggunaan layanan *Mobile banking*. Oleh karena itu, ketika menggunakan *Mobile banking*, bank dan nasabah diharapkan untuk tetap menyadari risiko yang terkait dengan penggunaan fasilitas *Mobile banking* (Sari et al., 2021).

2.1.2 Pengertian Kejahatan siber

Kejahatan dunia maya Atau Kejahatan siber adalah kejahatan di dunia maya yang menyerang keamanan jaringan komputer dan informasi telekomunikasi. Kejahatan siber yang muncul sebagai akibat dari perkembangan teknologi informasi. Perhatian khusus harus diberikan pada kejahatan dunia maya yang relevan dalam implementasinya sehubungan dengan kerahasiaan, integritas dan keberadaan data dan sistem komputer, karena kejahatan tersebut memiliki karakter yang berbeda dari kejahatan tradisional (Chintia et al., 2018).

2.1.3 Jenis-jenis Kejahatan siber

Bentuk-bentuk kejahatan siber di Indonesia dapat dikaitkan dengan ketentuan hukum pidana Indonesia, baik ketentuan KUHP maupun ketentuan pidana dalam peraturan perundang-undangan di luar KUHP yaitu UU No. 11 Tahun 2008 Jo UU No. 19 Tahun 2016 tentang Informasi dan Transaksi Elektronik. Meskipun demikian, ada perbedaan konsepsi antara hukum pidana Indonesia dengan karakteristik kejahatan siber. Beberapa tekninologi KUHP sulit digunakan sebagai dasar hukum untuk mengadili kejahatan siber, misalnya pengertian di depan umum yang disamakan dengan pengertian di dalam internet, pengertian memasuki pekarangan tertutup sebagaimana diatur dalam KUHP untuk mengadili kasus memasuki ruang (*spacey*) milik pihak lain di internet (*illegal access*) (Suwiknyo, 2021).

Tindak kejahatan siber di sektor jasa keuangan dan perbankan secara umum terbagi atas dua (2) jenis yakni:

1. *Sosial engineering*, adalah manipulasi psikologis seseorang dengan tujuan untuk mendapatkan informasi tertentu dengan cara menipu secara halus, baik disadari atau tidak melalui telepon atau berbicara langsung.
2. *Skimming*, adalah tindakan pencurian informasi dengan cara menyalin informasi yang terdapat pada strip magnetik kartu debit atau kredit secara illegal. Metode skimming merupakan metode yang digunakan untuk mencuri informasi nasabali pada saat bertransaksi menggunakan ATM. “Dalam menjalankan tindak kejahatan ini terdapat tiga (3) alat utama yang digunakan yaitu: skimmer, hidden camera dan keypad. Alat skimmer berfungsi untuk

merekam aktivitas Farodilah Muqoddam, Mengenal Modus Kejahatan Keuangan, Definisi Skimming, Phishing dan Vishing, 2019. diakses darim.bisnis.com pada tanggal 2 Oktober 2020. nasabah dalam menggunakan mesin ATM, alat ini mampu merekam strip elektromagnetik yang ada pada kartu korban pada saat kartu dimasukkan ke mesin ATM. Hidden camera dan keypad digunakan untuk merekam aktivitas korban pada saat melakukan penginputan PIN pada mesin ATM.

Adapun teknik dasar memperoleh informasi dengan modus *social engineering* bermacam-macam, ada tiga (3) yang paling lumrah yakni:

1. *Phishing*, teknik phising digunakan para pelaku dengan mengelabui atau memanipulasi para pemilik rekening bank sehingga mereka memberikan data dan informasi yang bisa digunakan untuk mengakses akun perbankan milik nasabah. Pengelabuan yang dilakukan untuk mendapatkan informasi rahasia seperti password dengan menyamar sebagai orang atau bisnis terpercaya dalam sebuah komunikasi elektronik. Saluran yang digunakan sebagai email, layanan pesan instan (SMS), atau penyebaran link palsu di internet untuk mengarahkan korban ke website yang telah dirancang untuk menipu.
2. *Vishing*, yakni upaya penipu biasanya menelepon korban dan berpura-pura menjadi karyawan bank, lembaga penegak hukum, atau perusahaan lain yang tepercaya. Mereka kemudian akan meminta korban untuk memberikan informasi pribadi, seperti nomor kartu kredit atau nomor jaminan sosial, dengan dalih untuk menyelesaikan masalah atau memverifikasi informasi..
3. *Impersonation*, yakni upaya penipu biasanya berpura-pura menjadi orang yang dikenal korban, seperti teman, keluarga, atau kolega. Mereka kemudian akan menghubungi korban melalui email, pesan teks, atau media sosial dan meminta bantuan keuangan, informasi pribadi, atau akses ke akun online korban..

2.1.4 Dampak Kejahatan Siber

Dampak dari kejahatan siber dalam perbankan adalah: 1) hilangnya pendapatan, 2) kerusakan reputasi, 3) kehilangan pelanggan, dan 4) sanksi peraturan. Fokus dari sebagian besar penelitian yang telah direview mengenai kejahatan siber adalah pada perspektif keuangan sektor perbankan dan persepsi nasabah terhadap layanan

perbankan, yaitu implikasi kejahatan siber terhadap persepsi nasabah dan jasa keuangan (Lana, 2021). Gelombang kejahatan siber yang meningkat yang berdampak negatif pada pertumbuhan ekonomi lembaga keuangan, secara tidak langsung melalui kurangnya kepercayaan pada infrastruktur digital dan internet atau secara langsung melalui penipuan dan pemerasan. Untuk mengurangi kejahatan dunia maya, seseorang harus mempertimbangkan pengembangan pendekatan multi-disiplin untuk gangguan yang efektif terhadap infrastruktur penjahat dunia maya melalui berbagi intelijen tanpa kompromi dan kerja sama yang erat antara penegak hukum dan badan investigasi kejahatan untuk pengumpulan intelijen yang cepat.

2.1.5 Manajemen Risiko

Manajemen risiko adalah upaya untuk mengidentifikasi, menganalisis dan mengendalikan risiko dalam semua kegiatan operasional dengan tujuan untuk mendapatkan efisiensi dan efisiensi yang lebih tinggi (Qintharah, 2019). Menurut Desda dan Yurasti (2019) manajemen risiko adalah seperangkat metodologi dan prosedur yang digunakan untuk mengidentifikasi, mengukur, memantau dan memantau risiko yang timbul dari setiap kegiatan. Selain itu, manajemen risiko bertindak sebagai sarana untuk memeriksa apakah keputusan risiko sejalan dengan strategi dan aturan bisnis.

Secara umum, risiko yang dihadapi perbankan syariah merupakan risiko yang relatif sama sama dengan yang dihadapi bank konvensional. Namun selain itu, bank syariah juga menghadapi risiko yang memiliki keunikan tersendiri, karena harus mengikuti prinsip-prinsip syariah. Risiko kredit, risiko pasar, risiko operasional dan risiko likuiditas harus dihadapi bank syariah. Risiko unik ini muncul karena isi neraca bank syariah berbeda dengan bank konvensional. Dalam hal ini pola bagi hasil yang dilakukan bank syari'ah menambah kemungkinan munculnya risiko-risikolain. Seperti *withdrawal risk, fiduciary risk, dan displaced commercial risk* merupakan contoh risiko unik yang harus dihadapi bank syariah (Syafii & Siregar, 2020).

2.2 Penelitian Terdahulu

Dalam penyusunan laporan skripsi ini perlu pertimbangan terkait data-data yang relevan terhadap penelitian sebelumnya dengan mencari bahan rujukan. Kajian pustaka bertujuan untuk mengkaji teori-teori yang digunakan pada penelitian sebelumnya serta pengumpulan data informasi yang relevan terhadap penelitian yang akan dilakukan agar tidak terjadi pengulangan.

Judul	Tujuan	Metode	Temuan Penting
Upaya *Risk Management* Dalam Mengatasi Penipuan Modus *Social Engineering* Melalui *Smartphone*	Mengeksplorasi upaya risk management yang dapat diimplementasikan untuk mengatasi penipuan melalui smartphone yang menggunakan teknik social engineering	Metode kualitatif deskriptif dengan menggunakan studi pustaka.	Penelitian ini menemukan bahwa penipuan melalui smartphone yang menggunakan teknik social engineering merupakan ancaman serius dalam lingkungan digital saat ini. Melalui analisis literatur, penelitian ini menunjukkan bahwa upaya risk management yang efektif melibatkan kombinasi strategi teknis dan non-teknis. Selain itu, peneliti juga menyoroti pentingnya kerjasama antara pengguna smartphone dan penyedia layanan untuk mengatasi ancaman penipuan ini. Dengan demikian, penelitian ini memberikan wawasan yang berharga dalam menghadapi tantangan penipuan digital yang semakin kompleks di era teknologi informasi
Perlindungan Hukum Nasabah Terhadap Kejahatan Pencurian Data Pribadi (Phising) Di Lingkungan Perbankan	Menganalisis efektivitas Perlindungan Hukum Nasabah Terhadap Kejahatan Phising Di Lingkungan Perbankan Wilayah Bank Rakyat Indonesia Kantor Cabang Watansoppeng.	Metode hukum empiris	Penelitian menemukan celah perlindungan hukum nasabah BRI Cabang Watansoppeng dari phising. Pelaku phising menipu nasabah untuk mendapatkan data pribadi dan mengakses internet banking mereka. Diperlukan kerjasama bank, penegak hukum, dan masyarakat untuk memerangi phising melalui edukasi dan pelaporan. Korban harus melapor ke polisi untuk membantu pencegahan dan penindakan. Kerjasama dan edukasi antar pihak, serta pelaporan oleh korban, adalah kunci memperkuat perlindungan nasabah dari phising di BRI Cabang Watansoppeng.

Perancangan Keamanan Pengguna Cardless dari Ancaman Cyber Crime Menggunakan Kriptografi Curva Elliptic	Mengevaluasi tingkat keamanan dan kepuasan dari para pengguna brimo terhadap tarik tunai tanpa kartu atau cardless menggunakan metode pieces Framework	Metode Curve25519	Penelitian ini menekankan perlunya peningkatan keamanan transaksi Cardless di aplikasi *mobile banking*. Direkomendasikan penggunaan kriptografi Curva Elliptic untuk mengenkripsi PIN pengguna, sehingga mempersulit akses bagi penjahat cyber. Hal ini diharapkan dapat mengurangi risiko pencurian identitas, pengeluaran tidak terkendali, dan kompromi sistem. Meningkatkan kesadaran akan keamanan Cardless dan sosialisasi yang lebih luas tentang layanan ini dapat membantu mengurangi korban cybercrime dan membangun kepercayaan masyarakat.
Analisis Manajemen Risiko Layanan *Mobile banking* Pada Bank Syariah	Menganalisi jenis risiko dalam layanan *mobile banking* dan menganalisis berbagai upaya bank syariah dalam menyelesaikannya	Kualitatif deskriptif	Temuan dalam penelitian ini bahwa risiko operasional dalam layanan *mobile banking* pada bank syariah dapat timbul akibat kegagalan sistem, human error, serta pengendalian dan prosedur yang kurang efektif. Bank syariah perlu waspada terhadap upaya penipuan melalui telepon, SMS, dan email yang meminta informasi pribadi atau transfer dana tanpa alasan yang jelas. Selain itu, nasabah disarankan untuk menghindari mengunduh software palsu yang dapat meminta data pribadi seperti kode aktivasi dan PIN, yang kemudian dapat disalahgunakan oleh pihak yang tidak bertanggung jawab. Oleh karena itu, bank syariah perlu terus mengembangkan strategi untuk mengatasi risiko-risiko tersebut agar layanan *mobile banking* tetap aman dan terpercaya bagi nasabah
Analisis Pharming Dalam Cyber Crime di Layanan*Mobile banking*	Penelitian ini bertujuan untuk menganalisis metode pharming dalam konteks kejahatan siber yang menargetkan layanan perbankan mobile	Kualitatif Desktiptif	Temuan dari penelitian ini memberikan wawasan tentang risiko yang terkait dengan pharming dalam sektor perbankan mobile dan menekankan pentingnya langkah-langkah keamanan yang kuat untuk mengurangi ancaman tersebut. Analisis ini berkontribusi dalam meningkatkan pemahaman tentang pharming dalam konteks kejahatan siber dan menekankan

	perlunya upaya yang berkelanjutan untuk melindungi pengguna perbankan mobile dari serangan yang canggih ini.

Pada beberapa penelitian sebelumnya telah diketahui secara keseluruhan membahas tentang berbagai risiko terkait keamanan di era digital, dengan fokus pada penipuan *smartphone, phising,* transaksi *Cardless, mobile banking syariah, dan pharming.* Namun tidak membahas dan mengkaji terkait upaya apa saja yang harus dilakukan Bank untuk mencegah tindak kejahatan siber pada aplikasi *mobile banking*. Perbedaan penelitian ini dengan beberapa penelitian sebelumnya terletak pada upaya yang dilakukan Bank BPD DIY Kantor Cabang Syariah dalam memanajemen risiko agar terhindar dari kejahatan siber pada *mobile banking* dan metode penelitian yang digunakan pada penelitian ini menggunakan *mixed method*. Diharapkan dengan adanya trobosan inovasi ini dapat membantu meningkatkan keamanan dalam layanan *mobile banking.*

BAB III
METODE PENELITIAN

3.1 Tempat dan Waktu Penelitian

Proses kegiatan penelitian dilaksanakan di Bank Pembangunan Daerah Yogyakarta Kantor Cabang Syariah Seluruh Yogyakarta. Penelitian ini dilaksanakan selama enam bulan terhitung sejak tanggal 18 September 2023 – 18 Maret 2024. Tempat pelaksanaan penelitian riset berlokasikan di Daerah Istimewa Yogyakarta, serta website resmi https://www.bpddiy.co.id.

3.2 Desain Penelitian

Penelitian yang digunakan pada penelitian ini adalah pendekatan *mixed method*. Pendekatan *mixed method* merupakan penelitian yang menggabungkan penggunaan pendekatan penelitian kualitatif dan kuantitatif dalam penelitian ilmiah. Contoh praksis adalah penggunaan teknik wawancara terbuka sekaligus teknik angket atau kuisioner untuk pengumpulan data penelitian (Waruwu, 2023). Penelitian kualitatif merupakan riset yang bersifat deskriptif dan cenderung menggunakan analisis dengan pendekatan induktif. Pendekatan kualitatif menitik beratkan kepada makna, penalaran, situasi dan definisi dalam konteks tertentu dengan melihat hubungan dengan kehidupan sehari-hari (Sidiq et al., 2019). Penelitian kuantitatif meliputi pemeriksaan dan deskripsi objek penelitian dengan menggunakan angka-angka dan penarikan kesimpulan berdasarkan fenomena-fenomena yang terjadi selama proses penelitian. Untuk mengetahui ada tidaknya hubungan antara faktor independen dengan variabel dependen dalam penelitian ini digunakan metode kuantitatif (Yam & Taufik, 2021).

Data primer adalah data yang diambil langsung dari pihak pertama atau sumber pertama sebagai sumber informasi. Objek penelitian yang akan diteliti pada penelitian ini adalah masyarakat pengguna *mobile banking* di Daerah Istimewa Yogyakarta khususnya Sleman. Data didapatkan dengan menyebarkan kuesioner secara *online*. Kuesioner *online* dibuat menggunakan *Google Form* dan didistribusikan ke responden dengan melakukan berbagai macam media seperti ke grup-grup dan chat pribadi di aplikasi *whatsapp* maupun dibagikan via *email*.

Teknik pendistribusian kuesioner secara online memungkinkan untuk mendapatkan sampel data dari seluruh Daerah Istimewa Yogyakarta.

3.3 Pendekatan Kuantitatif

1. Populasi dan Sampel

Dalam suatu penelitian, populasi adalah totalitas subjek. Populasi adalah suatu kelompok yang dipelajari dari suatu objek atau topik tertentu yang mempunyai jumlah dan kualitasnya menimbulkan pada data yang terdapat informasi dalam suatu penelitian sehingga dapat diambil kesimpulan. Nasabah yang aktif menggunakan layanan *mobile banking* di Daerah Istimewa Yogyakarta khususnya di Sleman merupakan demografi yang digunakan dalam penelitian ini.

Pengertian sampel adalah sebagian dari kuantitas dan karakteristik populasi yang diambil untuk mewakili populasi yang ada sebagai sampel. Responden yang terpilih sebagai sampel adalah mereka yang memenuhi kriteria peneliti. Peraturan mengenai kriteria pemuatan sampel adalah sebagai berikut:

a. Responden adalah pelanggan BPD DIY Syariah dengan rentang usia 20 sampai 35 tahun yang berasal dari Daerah Istimewa Yogyakarta, pemilihan rentang usia umumnya lebih akrab dengan teknlogi dan lebih cepat beradaptasi dengan perubahan teknologi.
b. Responden menggunakan layanan *mobile banking* minimal satu bulan dan melakukan transaksi menggunakan *mobile banking* minimal dua kali.

Penelitian ini merupakan penelitian survei, dengan menggunakan kuesioner sebagai alat pengumpulan data utama dan pengambilan sampel secara langsung. Untuk menentukan jumlah sampel penelitian apabila populasi tidak diketahui maka penelitian ini relevan untuk dapat menggunkan formula *Corhran* sebagai berikut:

$$n = \frac{z^2 pq}{e^2}$$

n = Sample size

z = Standar error associated with the chosen level of confidence (typically 1.96)

p = Variability / standard deviation

q = 1-p

e = Acceptable sampel error

Dengan menggunakan formula *cochran* maka dibutuhkan jumlah sampel minimal yaitu 96 responden.

2. Teknik Pengumpulan Data

Pengumpulan data menggunakan instrument kuisioner. Kuesioner merupakan cara pengumpulan data dengan menyediakan daftar pertanyaan atau pernyataan dalam bentuk kuesioner untuk diisi oleh responden sesuai dengan kebutuhan dari masing-masing variabel penelitian. Pemberian kuesioner atau angket biasanya pada responden dalam jumlah yang banyak dan diberikan kepada sumber penelitian dengan tingkat pemahaman yang memadai (Gebang et al., 2022). Pengambilan sampel (*Purposive Sampling*). *Purposive sampling* merupakan teknik pengambilan sampel sumber data dengan pertimbangan tertentu. Strategi pengambilan sampel non-acak atau *proporsive sampling*, yang melibatkan pemilihan sampel berdasarkan karakteristik *non-probability* yang dimana tidak semua anggota populasi memiliki peluang yang sama untuk dipilih. Pemilihan sampel berdasarkan karakteristik ini sangat berguna ketika peneliti ingin mendalami kasus-kasus tertentu atau kelompok populasi yang memiliki karakteristik unik, sehingga dapat memberikan wawasan yang lebih mendalam terkait permasalahan yang diteliti (Kusumastuti & Khoiron, 2019).

Penelitian ini menggunakan skala likert, lebih tepatnya skala harga, yang mengukur tingkat persetujuan responden terhadap suatu pertanyaan yang mana mereka harus memilih satu dari sekian banyak kemungkinan jawaban. Setiap indikator variabel akan dievaluasi dengan menggunakan skala Likert sebagai acuannya, dan setiap indikator akan dijadikan alat bantu berupa pertanyaan sebagai berikut:

Tabel 3.1 Skala Likert

Jawaban	Nilai
Sangat Tidak Setuju	1
Tidak Setuju	2
Netral	3
Setuju	4
Sangat Setuju	5

Sumber: Data diolah penulis (2024)

3. Variabel Penelitian

Riset ini memiliki tiga variabel independen:

a. **Praktik untuk mencegah kejahatan siber.** Variabel ini diukur dari 1) Manakah dari langkah-langkah keamanan berikut yang Anda gunakan untuk *mobile banking*, 2) Apakah Anda penilaian risiko kejahatan siber secara berkala, 3) Apakah Anda menerapkan kontrol keamanan untuk mengurangi risiko kejahatan siber, 4) Apakah Anda memiliki rencana untuk merespons insiden kejahatan siber, 5) Menurut anda penting pendidikan pengguna dalam mencegah kejahatan dunia maya di *mobile banking*, 6) Apakah Anda menerima segala bentuk pendidikan atau pelatihan tentang keamanan *mobile banking* dari bank Anda, 7) Apakah pendidikan atau pelatihan dalam meningkatkan kesadaran dan praktik sangat efektif bagi Anda.

b. Strategi yang efektif dalam mencegah kejahatan siber. Variabel ini diukur dari 1) Seberapa yakin Anda menilai efektivitas keseluruhan strategi manajemen risiko bank Anda dalam mencegah kejahatan dunia maya, 2) Seberapa puas Anda dengan langkah-langkah keamanan saat ini yang disediakan oleh aplikasi *mobile banking* Anda.

c. Tantangan utama terhadap keamanan *mobile banking.* Variabel ini diukur dari 1) Dukungan yang tidak memadai dari bank dalam memastikan transaksi *mobile banking* yang aman, 2) Kurangnya kesadaran/edukasi tentang ancaman siber dalam transaksi *mobile banking,* 3) Kompleksitas langkah-langkah keamanan dalam transaksi *mobile banking,* 4) Kendala teknik yang dihadapai saat melalukukan transaksi *mobile banking*.

4. Analisis Deskriptif

Data yang terkumpul akan dianalisis secara statistik melalui pendekatan destriptif untuk menunjukan rata-rata dan distribusi frekuensi variabel (indikator) yang diteliti.

3.4 Pendekatan Kualitatif

Penelitian kualitatif merupakan penelitian yang bersifat deskriptif dan cenderung menggunakan analisis dengan pendekatan induktif. Misalnya dengan melakukan observasi, untuk melihat persepsi dan perilaku subyek sehingga dapat ditemukan

tindakan-tindakan secara langsung (Sidiq et al, 2019). Pada penelitian ini menggunakan teknik pengumpulan data sebagai berikut:

1. Observasi

Observasi adalah metode yang melibatkan interaksi peneliti dalam kehidupan sehari-hari suatu kelompok atau orang, sehingga peneliti dapat mempelajari aspek yang tampak maupun tersembunyi dari rutinitas kehidupan dan kebudayaan suatu kelompok tersebut (Nugrahani & Hum, 2014).

2. Key Informant Interview (KII)

Wawancara adalah teknik pengumpulan informasi secara langsung kepada narasumber agar data yang diperoleh sesuai dengan fenomena yang terjadi pada saat melakukan observasi. KII merupakan narasumber yang memiliki pengetahuan terkait isu yang terjadi dan mengamati secara langsung pada obyek penelitian tujuan KII adalah untuk mengetahui lebih lanjut terkait informasi secara akurat terhadap obyek penelitian (Pujaastawa, 2016).

Tabel 3.2 Daftar Responden KII

Kategori Narasumber	Jumlah	Topik Pembahasan
- Pimpinan Cabang - Pemasaran Bisnis - Account Officer (AO) - Customer Service (CS)	2 2 1 1	• Apa praktik manajemen risiko saat ini yang digunakan dalam *mobile banking* untuk mencegah kejahatan siber • Seberapa efektif strategi manajemen risiko ini dalam mencegah kejahatan siber di *mobile banking* • Apa tantangan utama dalam menerapkan strategi manajemen risiko untuk keamanan *mobile banking* • Praktik terbaik dan pendekatan inovatif apa yang dapat direkomendasikan untuk meningkatkan manajemen risiko untuk mencegah kejahatan siber di *mobile banking*
Total	6	

Sumber: Data diolah penulis (2024)

3.5 Teknik Analisis Data

1. Data Kuantitatif

   Analisis statistik deskriptif adalah statistik yang digunakan untuk menganalisis data dengan cara mendeskripsikan atau menggambarkan data yang telah

terkumpul. Analisis ini hanya berupa akumulasi data dasar dalam bentuk deskripsi semata dalam arti tidak mencari atau menerangkan saling hubungan, menguji hipotesis, membuat ramalan, atau melakukan penarikan kesimpulan (Darwin et al., 2021).

Analisis data multivariat dilakukan dengen menggunakan aplikasi software Statistical Package for the Social Science (SPSS) versi 24 untuk mengetahui praktik manajemen risiko, seberapa efektif strategi menejemen risiko, tantangan utama dalam menerapkap strategi manajemen risiko, praktik terbaik dan pendekatan inovatif yang digunakan dalam *mobile banking* untuk mencegah kejahatan siber yaitu uji Korelasi Spearman dengan tingkat keyakinan 0,1 (Sarwono & Handayani, 2021). Statistik inferensial untuk mengadakan penarikan kesimpulan dan membuat keputusan berdasarkan analisis yang telah dilakukan. Biasanya analisis unu mengambil samper tertentu dari sebauh populasi yang jumlahnya banyak, dan dari hasil analisis terhadap sampel tersebut digeneralisasikan terhadap populasi (Waruwu, 2023).

2. Data Kualitatif

   Analisis data dalam penelitian kualtatif, dilakukan pada saat pengumpulan data berlangsung, dan setelah selesai pengumpulan dalam periode tertentu. Pada saat wawancara, peneliti sudah melakukan analisis terhadap jawaban yang diwawancarai. Menurut Miles and Huberman dalam Sugiono (2016), mengemukakan bahwa aktivitas dalam analisis data kualitatif dilakukan secara interaktif dan berlangsung secara terus menerus sampai tuntas, sehingga datanya sudah jenuh. Aktivitas dalam analisis data yaitu *data reduction*, *data display*, dan *conclusion drawing/verification*.

   Analisis data sangat memegang peranan penting dalam penelitian. Data yang diperoleh dari penelitian kualitatif dengan cara observasi, wawancara mendalam, dan dokumentasi atau gabungan ketigannya (*triangulasi)* (Abdussamad & Sik, 2021). Pengorganisasian dan pengelolaan data tersebut bertujuan menemukan tema dan hipotesis kerja yang akhirnya diangkat menjadi teori substantif oleh karena itu, analisis data merupakan bagian yang amat penting karena dengan analisislah suatu data dapat diberi arti dan makna yang

berguna untuk masalah penelitian. Dalam proses analisis data dimulai dengan menelaah seluruh data yang tersedia dari berbagai sumber, yaitu dari wawancara, pengamatan yang sudah dituliskan dalam catatan lapangan, dokumen pribadi, dokumen resmi, gambar, foto, dan sebagainya (Siregar, 2021).

BAB IV
HASIL DAN PEMBAHASAN

4.1 Deskripsi Umum BPD DIY Syariah

Bank Pembangunan Daerah Yogyakarta atau Bank BPD DIY merupakan Bank Pembangunan Daerah yang sudah berdiri sejak tanggal 15 Desember 1961. Pada tahun 2013 berdasarkan akta notaris No.11 oleh R.M Soerjanto Partaningrat, Bank BPD DIY melakukan perubahan hukum dari perusahaan daerah menjadi perseroan terbatas. Pada tahun 2007 tanggal 19 Februari Bank BPD DIY membuka unit usaha syariah dengan satu kantor layanan yaitu Kantor Cabang Syariah Cik Ditiro. Kantor cabang tersebut berada di Jalan Cik Ditiro No.34, Yogyakarta. Berdirinya unit usaha syariah didasari karena perkembangan perbankan syariah di Indonesia. Masyarakat Indonesia mayoritas beragama Islam hal ini membuat perbankan syariah berkembang cukup pesat.

Bank Syariah Indonesia menempati posisi ke-9 tingkat global, pada tahun 2019 perkembangan asset perbankan syariah sebesar 9,93% dengan total asset nya Rp.538,32 triliun (Thohari & Hakim, 2021). Bank BPD DIY Syariah merupakan Unit Usaha Syariah yang memiliki berbagai produk dan jasa perbankan yang beroperasi sesuai prinsip-prinsip syariah, yaitu seperti Tabungan Sutera Mudharabah, Tabungan Simpeda Wadiah, Tabungan Haji dan berbagai produk pembiayaan berupa Pembiayaan Pemilikan Rumah, KUR, Pembiayaan Pemilikan Emas, dan Pembiayaan Pemilikan Kendaraan.

4.2 Visi dan Misi BPD DIY

a. Visi

Menjadi Bank Terpercaya, Istimewa dan Pilihan Masyarakat.

b. Misi

1. Menyediakan solusi kebutuhan keuangan masyarakat dengan memberikan pengalaman perbankan yang berkesan.
2. Menjalankan prinsip kehati-hatian dan menerapkan bisnis yang beretika untuk meningkatkan nilai perusahaan.

3. Mencapai SDM yang unggul, berintegras dan profesional.
4. Mengembangkan keunggulan kompetitif dengan layanan prima dan produk yang inovatif berbasis budaya untuk menjadi regional Champion yang berkelanjutan.
5. Menjalankan fungsi agen pembangunan yang fokus mengembangkan sektor UMKM, mendorong pertumbuhan perekonomian daerah dan menjaga lingkungan.

4.3 Pembahasan

4.3.1 Karakteristik Demografi Responden

Karakteristik demografis responden menjelaskan data detail terkait responden yang mengisi kuesioner. Responden yang mengisi kuesioner akan diolah menjadi data seperti tabel dibawah ini:

Tabel 4.1 Karakteristik Demografi Responden

Variabel	Kategori	Frekuensi	Persentase
Usia	- 18-24	41	42,7%
	- 25-34	32	33,3%
	- 35-44	23	24%
Jenis Kelamin	- Laki-laki	45	46,9%
	- Perempuan	51	53,1%
Pekerjaan	- Pelajar/Mahasiswa	28	29,2%
	- Bekerja (Sektor Perbankan)	35	36,5%
	- Bekerja (Sektor Non-Perbankan)	20	20,8%
	- Wiraswasta	11	11,5%
	- Lain-lain	2	2,1%
Tingkat Pendidikan	- SMA	19	19,8%
	- Diploma	24	25%
	- Sarjana	50	52,1%
	- Pascasarjana (S2-S3)	3	3,1%

Sumber: Data diolah penulis (2024)

Dari tabel 4.1 diatas menunjukan bahwa karakteristik responden terbagi dalam beberapa variabel yaitu:

1. Usia

   Tabel 4.1 diatas menunjukan bahwa sebagian besar responden adalah pengguna *mobile banking* yang berusia 18-24 tahun sebanyak 41 orang

(42,7%), berusia 25-34 tahun sebanyak 32 orang (33,3%), dan yang berusia 35-44 tahun sebanyak 23 orang (24%).

2. Jenis Kelamin

   Data yang dihasilkan dari tabel 4.1 diatas menunjukan bahwa responden adalah pengguna *mobile banking* yang didominasi oleh jenis kelamin perempuan sebanyak 51 orang (53,1%), dan sisanya dengan jenis kelamin laki-laki sebanyak 45 orang (46,9%).

3. Pekerjaan

   Tabel 4.1 diatas menunjukan bahwa sebagian besar responden bekerja di sektor perbankan yakni sebanyak 35 orang (36,5%), sedangkan untuk pelajar/mahasiswa sebanyak 28 orang (29,2%), selanjutnya yang bekerja di di sektor non-perbankan 20 orang (20,8%), lalu untuk wiraswasta sebanyak 11 orang (11,5%), dan lain-lain sebanyak 2 orang (2,1%).

4. Tingkat Pendidikan

   Tabel 4.1 diatas menunjukan bahwa sebagian besar responden memiliki tingkat pendidikan sarjana yakni sebesar 50 orang (52,1%), selanjutnya tingkat pendidikan diploma dengan jumlah sebanyak 24 orang (25%), lalu dengan tingkat pendidikan SMA Sebanyak 19 orang (19,8%), dan yang terkahir dengan tingkat pendidikan pascasarjan (S2-S3) sebanyak 3 orang (3,1%).

4.3.2 Praktik Manajemen Risiko Saat Ini Yang Digunakan Dalam *Mobile Banking* Untuk Mencegah Kejahatan Siber

Tabel 4.2 menyajikan data distribusi frekuensi jawaban responden terkait praktik manajemen risiko saat ini untuk mencegah kejahatan siber. Kuesioner praktik manajemen risiko memiliki 7 pernyataan yang berhubungan tentang praktik-praktik apa aja yang dilakukan saat ini guna mencegah kejahatan siber.

Tabel 4.2 Praktik Manajemen Risiko

Peryantaan	Kategori	Frekuensi	Persentase
Manakah dari langkah-langkah keamanan berikut yang Anda gunakan untuk *mobile banking*	- Kata sandi yang kuat	67	26,2%
	- Otentikasi dua faktor	59	23%
	- Otentikasi biometrik	68	26,6%

	- Memperbarui aplikasi *mobile banking*	40	15,6%
	- Menghindari Wi-Fi publik	22	8,6%
Apakah Anda penilaian risiko kejahatan siber secara berkala	- Ya	76	79,2%
	- Tidak	20	20,8%
Apakah Anda menerapkan kontrol keamanan untuk mengurangi risiko kejahatan siber	- Ya	90	93,8%
	- Tidak	6	6,2%
Apakah Anda memiliki rencana untuk merespons insiden kejahatan siber	- Ya	84	87,5%
	- Tidak	12	12,5%
Menurut anda penting pendidikan pengguna dalam mencegah kejahatan dunia maya di *mobile banking*	- Ya	93	96,9%
	- Tidak	3	3,1%
Apakah Anda menerima segala bentuk pendidikan atau pelatihan tentang keamanan *mobile banking* dari bank Anda	- Ya	79	82,3%
	- Tidak	17	17,7%
Apakah pendidikan atau pelatihan dalam meningkatkan kesadaran dan praktik sangat efektif bagi Anda	- Ya	90	93,8%
	- Tidak	6	6,2%

Sumber: Data diolah penulis (2024)

Berdasarkan data dari tabel 4.2 dapat disimpulkan bahwa praktik manajemen risiko saat ini yang digunakan dalam *mobile banking* untuk mencegah kejahatan siber yaitu:

1. Manakah dari langkah-langkah keamanan berikut yang Anda gunakan untuk *mobile banking*

   Tabel 4.2 diatas menunjukkan persentase terbanyak responden dalam menggunakan langah-langkah keamanan *mobile banking* ialah menggunakan keamanan otentifikasi biometrik yang berjumlah 68 responden (26,6%). Dikarenakan untuk pernyataan ini responden dibebaskan memilih lebih dari 1 pilihan, maka memungkinkan tiap responden memilih jawaban yang sama.
2. Apakah Anda penilaian risiko kejahatan siber secara berkala

   Tabel 4.2 diatas menunjukan bahwa sebagian besar responden memilih frekuensi dari pernyataan apakah anda penilaian risiko kejahatan siber secara berkala berjumlah sebanyak 76 responden (79,2%), dan responden yang memilih frekuensi tidak sebanyak 20 responden (20,8%).
3. Apakah anda menerapkan kontrol keamanan untuk mengurangi risiko kejahatan siber

Tabel 4.2 diatas menunjukan bahwa sebagian besar responden memilih frekuensi dari pernyataan apakah anda menerapkan kontrol keamanan untuk mengurangi risiko kejahatan siber berjumlah sebanyak 90 responden (93,8%), dan responden yang memilih frekuensi tidak sebanyak 6 responden (6,2%).

4. Apakah anda memiliki rencana untuk merespon insiden kejahatan siber

   Tabel 4.2 diatas menunjukan bahwa sebagian besar responden memilih frekuensi dari pernyataan apakah anda memiliki rencana untuk merespon insiden kejahatan siber berjumlah sebanyak 84 responden (87,5%), dan responden yang memilih frekuensi tidak sebanyak 12 responden (12,5%).

5. Menurut anda penting pendidikan pengguna dalam mencegah kejahatan siber di *mobile banking*

   Tabel 4.2 diatas menunjukan bahwa sebagian besar responden memilih frekuensi dari pernyataan menurut anda penting pendidikan pengguna dalam mencegah kejahatan siber di *mobile banking* berjumlah sebanyak 93 responden (96,9%), dan responden yang memilih frekuensi tidak sebanyak 3 responden (3,1%).

6. Apakah anda menerima segala bentuk pendidikan atau pelatihan tentang keamanan *mobile banking* dari bank anda

   Tabel 4.2 diatas menunjukan bahwa sebagian besar responden memilih frekuensi dari pernyataan apakah anda menerima segala bentuk pendidikan atau pelatihan tentang keamanan *mobile banking* dari bank anda berjumlah sebanyak 79 responden (82,3%), dan responden yang memilih frekuensi tidak sebanyak 17 responden (17,7%).

7. Apakah pendidikan atau pelatihan dalam meningkatkan kesadaran dan praktik sangat efektif bagi anda

   Tabel 4.2 diatas menunjukan bahwa sebagian besar responden memilih frekuensi dari pernyataan apakah pendidikan atau pelatihan dalam meningkatkan kesadaran dan praktik sangat efektif bagi anda berjumlah sebanyak 90 responden (93,8%), dan responden yang memilih frekuensi tidak sebanyak 6 responden (6,2%).

Data lain yang diperoleh ialah melalui wawancara langsung bersama pimpinan kantor cabang pembantu UII, (Wijanarko) menjelaskan bawah:

> "Praktik manajemen risiko yang utama dilakukan dari sisi pengamanan pada waktu instalasi melakukan proses verifikasi berupa token yang hanya dikirimkan kepada nomor yang teregistrasi melalui ATM. Selanjutnya adanya password, password hanya digunakan atau diketahui oleh pemilik, dan pasti sudah terinskripsi." (Wawancara personal, 2024)

Dapat disimpulkan bahwa praktik manajemen risiko yang digunakan oleh Bank BPD DIY Syariah belum menggunakan keamanan seperti sidik jadi dan *face id*. Bahwasannya Bank BPD DIY harus menambahkan fitur keamanan biometrik untuk meningkatkan keamanan yang sudah ada dan agar masyarakat tetep percaya akan data pribadinya terjaga dengan aman. Berdasarkan hasil wawancara dari pimpinan kantor cabang pembantu Maguwoharjo (Sanjaya), menjelakan bahwa:

> "Sebagai langkah pengamanan untuk dapat menikmati layanan *mobile banking* Bank BPD DIY diperlukan tatap muka dengan petugas untuk memastikan bahwa pemohon adalah nasabah dan secara sadar mengaktifkan layanan *mobile banking*. Selanjutnya jika nasabah melakukan penggantian perangkat maka sistem akan langsung masuk ke dalam *safe mode*, untuk dapat mengaktifkannya kembali nasabah harus mengunjungi petugas *customer service* di kantor terdekat." (Wawancara personal, 2024)

Dari data diatas dapat disimpulkan bahwa praktik manajemen risiko yang dilakukan sudah cukup baik, namun untuk penanganannya masih terbilang rumit, dikarenakan nasabah harus berkunjung langsung ke kantor BPD DIY terdekat jika *mobile banking* yang digunakan mengalami kendala.

4.3.3 Seberapa Efektif Strategi Manajemen Risiko Ini Dalam Mencegah Kejahatan Siber Di *Mobile Banking*

Tabel 4.3 menyajikan data distribusi frekuensi jawaban responden terkait efektifitas strategi manajemen risiko ini dalam mencegah kejahatan siber. Kuesioner efektifitas strategi manajemen risiko memiliki 2 pernyataan yang berhubungan tentang seberapa efektif strategi manajemen risiko ini dalam mencegah kejahatan siber di *mobile banking*.

Tabel 4.3 Efektifitas Stategi Manajemen Risiko

Pernyataan	STS		TS		N		S		SS	
	f	%	f	%	f	%	f	%	f	%
Seberapa yakin Anda menilai efektivitas keseluruhan strategi manajemen risiko bank dalam mencegah kejahatan siber	0	0	3	3,1	23	24	45	46,9	25	26
Seberapa puas Anda dengan langkah-langkah keamanan saat ini yang disediakan oleh aplikasi *mobile banking* Anda	2	2,1	4	4,2	19	19,8	41	42,7	30	31,1

Sumber: Data diolah penulis (2024)

Tabel 4.3 menunjukan bahwa frekuensi jawaban setuju paling banyak terdapat pada pernyataan seberapa yakin anda menilai efektifitas keseluruhan strategi manajemen risiko bank dalam mencegah kejahatan siber dengan jumlah sebanyak 45 responden (46,9%), dan untuk frekuensi jawaban sangat setuju sebanyak 25 responden (26%). Sedangkan frekuensi setuju untuk pernyataan seberapa puas anda dengan langkah-langkah keamanan saat ini yang disediakan oleh aplikasi *mobile banking* sebanyak 41 responden (42,7%), dan untuk frekuensi jawaban sangat setuju sebanyak 30 responden (31,1%).

Data lain yang diperoleh ialah melalui wawancara langsung bersama pimpinan kantor cabang pembantu UII (Wijanarko) dan juga pimpinan kantor cabang pembantu Maguwoharjo (Sanjaya) menjelaskan bawah:

> "Keamanan produk dari pengembangan divisi IT termasuk handal, sejak peluncuran *mobile banking* di tahun 2016 langkah ini dinilai cukup efektif untuk menangkal adanya upaya pembobolan sistem, jadi kecil kemungkinan untuk diambil celah oleh pihak yang tidak bertanggung jawab." (Wawancara personal, 2024)

Dapat disimpulkan bahwa efektifitas strategi manajemen risiko yang digunakan oleh Bank BPD DIY sudah cukup efektif untuk mencegah kehajatan siber saat ini, dan juga faktor utama tetap kembali ke pengguna, selama pengguna *mobile banking* tidak memberitahukan no handphone, password dan PIN transaksi kepada orang lain maka keamanan saldo rekening dapat terjaga. Berdasarkan hasil wawancara dari pemasaran bisnis Bank BPD DIY Kantor Cabang Syariah (Rikowicaksono) menjelaskan bahwa:

> "Manajemen risiko kita gunakan sudah cukup efektif untuk menurunkan tingkat kejahatan siber, dengan kita mengingatkan kembali ke pihak nasabah, dan kita menjaga sistem dimana data harus dijaga dengan aman."(Wawancara personal, 2024)

Dapat disimpulkan bahwa efektifitas strategi manajemen risiko yang digunakan oleh Bank BPD DIY sudah cukup efektif mengingat keamanan data nasabah dan keamanan sistem dikelola secara menyeluruh dengan sangat baik.

4.3.4 Tantangan Utama Dalam Menerapkan Strategi Manajemen Risiko Untuk Keamanan *Mobile Banking*

Tabel 4.3 menyajikan data distribusi frekuensi jawaban responden terkait tantangan utama dalam menerapkan strategi manajemen risiko. Kuesioner tantangan utama memiliki 4 pernyataan yang berhubungan tentang tantangan utama dalam menerapkan strategi manajemen risiko untuk keamanan *mobile banking*.

Tabel 4.4 Tantangan Utama Dalam Menerapkan Strategi Manajemen Risiko

Pernyataan	STS		TS		N		S		SS	
	f	%	f	%	f	%	f	%	f	%
Dukungan yang tidak memadai dari bank dalam memastikan transaksi *mobile banking* yang aman	2	2,1	10	10,4	24	25	40	41,7	20	20,8
Kurangnya kesadaran/edukasi tentang ancaman siber dalam transaksi *mobile banking*	0	0	4	4,2	17	17,7	46	47,9	29	30,2
Kompleksitas langkah-langkah keamanan dalam transaksi *mobile banking*	0	0	3	3,1	20	20,8	46	47,9	27	28,2
Kendala teknik yang dihadapai saat melalukukan transaksi *mobile banking*	0	0	4	4,2	21	21,9	43	44,8	28	29,1

Sumber: Data diolah penulis (2024)

Tabel 4.4 menunjukan bahwa frekuensi jawaban setuju paling banyak terdapat 2 pernyataan yaitu kurangnya kesadaran/edukasi tentang ancaman siber dalam transaksi *mobile banking* dan kompleksitas langkah-langkah keamanan dalam transaksi *mobile banking* yang sama-sama berjumlah sebanyak 46 responden (47,9%). Disamping itu, frekuensi setuju untuk pernyataan kendala teknik yang dihadapai saat melakukan transaksi *mobile banking* sebanyak 43 responden (44,8%). Selanjutnya frekuensi setuju untuk pernyataan dukungan yang tidak

memadai dari bank dalam memastikan transaksi *mobile banking* yang aman sebanyak 40 responden (41,7%)

Data lain yang diperoleh ialah melalui wawancara langsung bersama pimpinan kantor cabang pembantu UII, (Wijanarko) menjelaskan bawah:

> "Menerapkan dan mempertahankan strategi manajemen risiko, kita tetap mengedukasi ke nasabah bahwasannya penggunaan *mobile banking* ini cukup rentan terhadap kejahatan siber, selanjutnya untuk kendala internal hampir tidak ada, kalau untuk faktor ekternal terkadang beberapa nasabah memiliki kesulitan dalam menghafal, baik itu password, dan PIN, itu menjadi kendala teknis yang menghambat." (Wawancara personal, 2024)

Penjelasan yang dilakukan oleh Wijanarko bahwasannya strategi manajemen risiko di Bank BPD DIY sudah diterapkan dan dipertahankan dengan baik, untuk nasabah sendiri sudah dilakukannya edukasi terhadap kejahatan siber. Berdasarkan hasil wawancara dari pimpinan kantor cabang pembantu Maguwoharjo (Sanjaya) terdapat kendala lain yang ditemukan, sebagai berikut:

> "Kendala teknis yang ditemui terjadi ketika ada pemadaman listrik yang cukup lama, hal ini pernah terjadi dan diatasi dengan menyewa genset dengan kapasitas besar. Kendala lain yang ditemui adanya kegagalan di sistem pendinginnya, jika hal ini terjadi unit data *center* akan langsung melakukan perbaikan agar mencapai suhu yang optimal kembali." (Wawancara personal, 2024)

Dari hasil diatas dapat disimpulkan bahwa tantangan yang paling umum adalah terjadinya pemadaman listrik dan juga masalah *overheat* dibagian pendingin data *center*, dikarenakan data *center* bekerja selama 24 jam penuh.

4.3.5 Praktik Terbaik Dan Pendekatan Inovatif Apa Yang Dapat Direkomendasikan Untuk Meningkatkan Manajemen Risiko Untuk Mencegah Kejahatan Siber Di *Mobile banking*

Bank perlu melakukan praktik dan inovatif dalam meningkatkan keamanan *mobile banking*. Rekomendasi praktik dan inovatif yang dapat dilakukan oleh bank, sebagai berikut:

1. Menambahkan fitur keamanan biometrik

Fitur keamanan biometrik adalah sistem yang menggunakan karakteristik fisik atau perilaku seseorang untuk mengidentifikasi mereka. Contoh fitur keamanan biometrik termasuk sidik jari, pengenalan wajah, pemindaian iris mata, dan pengenalan suara. Fitur keamanan biometrik dapat membantu meningkatkan keamanan data dan akun online karena lebih sulit untuk dipalsukan daripada kata sandi atau PIN.

2. Melakukan seminar atau pelatihan tentang bahaya kejahatan siber

   Seminar atau pelatihan tentang bahaya kejahatan siber dapat membantu meningkatkan kesadaran masyarakat tentang risiko yang terkait dengan penggunaan internet. Seminar dan pelatihan ini dapat membahas topik seperti:

   a. Jenis-jenis kejahatan siber yang umum
   b. Cara melindungi diri dari kejahatan siber
   c. Apa yang harus dilakukan jika Anda menjadi korban kejahatan siber

3. Memberikan literasi digital

   Literasi digital adalah kemampuan untuk menggunakan internet dan teknologi secara bertanggung jawab dan aman. Literasi digital dapat membantu masyarakat untuk:

   a. Memahami informasi yang mereka temukan di internet
   b. Menghindari penipuan online
   c. Menjaga privasi mereka di internet
   d. Menggunakan internet untuk tujuan yang positif

4. Pendidikan tentang teknologi informasi

   Pendidikan tentang teknologi informasi dapat membantu masyarakat untuk:

   a. Memahami cara kerja teknologi
   b. Menggunakan teknologi secara efektif
   c. Menyadari risiko dan manfaat teknolog

5. Memberikan informasi rinci tentang fitur keamanan dan cara menggunakannya

   Informasi rinci tentang fitur keamanan dan cara menggunakannya dapat membantu masyarakat untuk:

   a. Mengaktifkan fitur keamanan yang tersedia untuk mereka
   b. Menggunakan fitur keamanan dengan benar

c. Menjaga keamanan data dan akun online mereka

6. Melaksanakan kampanye edukasi pengguna secara reguler tentang ancaman keamanan siber

   Kampanye edukasi pengguna secara reguler tentang ancaman keamanan siber dapat membantu meningkatkan kesadaran masyarakat tentang risiko yang terkait dengan penggunaan internet. Kampanye edukasi ini dapat menggunakan berbagai media, seperti, media sosial, situs web, televisi, radio.

Dari hasil data pembahasan terdapat beberapa rekomendasi dari masyarakat untuk Bank BPD DIY, tentu bank harus mengambil langkah yang tepat dalam mencegah kejahatan siber yang akan terjadi kedepannya, Bank BPD DIY juga dapat melakukan praktik dan pendekatan invotif diatas untuk dapat memaksimalkan keamanan yang sudah ada, tapi disamping itu faktor utama keamanan *mobile banking* terletak pada sisi pengguna. Selama pengguna tidak pernah memberitahukan no handphone, password dan PIN transaksi kepada orang lain sehingga diharapkan pengguna merasa tenang akan keamanan data pribadi dan juga saldo rekening dalam kegiatan sehari-hari.

BAB V
PENUTUP

5.1 Kesimpulan

Berdasarkan hasil analisis dan pembahasan pada penelitian "Strategi Penerapan Manajemen Risiko Untuk Mencegah Kejahatan Siber Di *Mobile banking* Pada Bank Pembangunan Daerah Yogyakarta Kantor Cabang Syariah" dapat disimpulkan bahwa:

1. Kebanyakan pengguna *mobile banking* dan juga pihak Bank BPD DIY Kantor Cabang Syariah sudah melaksanakan praktik manajemen risiko dengan cukup baik terkait keamanan *mobile banking* agar terhindar dari kejahatan siber saat ini.
2. Dari data pembahasan efektifitas strategi manajemen risiko kebanyakan pengguna sudah mengaku puas dengan keamanan saat ini dan juga yang digunakan oleh Bank BPD DIY sudah cukup efektif untuk mencegah kejahatan siber.
3. Dari data pembahasan tantangan utama dalam menerapkan strategi manajemen kebanyakan dibagian kurangnya kesadaran atau edukasi tentang kejahatan siber dan kompleksitas langkah-langkah keamanan dalam transaksi *mobile banking* dan tantangan yang sering dihadapi oleh Bank BPD DIY ialah terjadinya pemadaman listrik dan juga masalah *overheat* dibagian pendingin data *center*.
4. Dari data pembahasan praktik terbaik dan pendekatan inovatif yang dapat digunakan oleh Bank BPD DIY untuk memperkuat keamanan *mobile banking* yaitu menambahkan fitur keamanan biometrik, melakukan seminar atau pelatihan tentang bahaya kejahatan siber, memberikan literasi digital, pendidikan tentang teknologi informasi, memberikan informasi rinci tentang fitur keamanan dan cara menggunakannya, melaksanakan kampanye edukasi pengguna secara reguler tentang ancaman keamanan siber.

5.2 Implikasi

5.2.1 Implikasi Teoritis

Terkait dengan teori, temuan dalam penelitian ini akan memperkaya kajian yang pertama penguatan keamanan *mobile banking*, seperti penerapan strategi manajemen risiko yang komprehensif dalam membangun infrastruktur *mobile banking* yang lebih aman dan tangguh terhadap kejahatan siber. Kedua dengan meningkatkan kepercayaan nasabah, nasabah akan merasa lebih aman dan nyaman dalam bertransaksi keuangan melalui *mobile banking.* Ketiga keunggulan kompetitif dalam keamanan *mobile banking*, hal ini dapat menarik lebih banyak nasabah, terutama mereka yang sangat peduli dengan keamanan siber dan memperkuat posisi Bank BPD DIY Syariah sebagai bank syariah yang terpercaya.

5.2.2 Implikasi Praktik

Hasil penelitian ini digunakan sebagai masukan bagi Bank BPD DIY agar selalu melakukan pembaruan aplikasi *mobile banking* dan juga diharapkan menambahkan keamanan biometrik, melakukan seminar atau pelatihan tentang bahaya kejahatan siber, memberikan literasi digital, pendidikan tentang teknologi informasi, memberikan informasi rinci tentang fitur keamanan dan cara menggunakannya, melaksanakan kampanye edukasi pengguna secara reguler tentang ancaman keamanan siber.

5.3 Keterbatasan Penelitian

Penelitian ini memiliki keterbatasan yang perlu dipertimbangkan, yaitu tidak dapat melakukan wawancara langsung dengan divisi IT Bank BPD DIY, sehingga data yang diperoleh bisa rentan terhadap bias responden.

5.4 Rekomendasi

Berdasarkan penelitian yang telah dilaksanakan mengenai Strategi Penerapan Manajemen Risiko Untuk Mencegah Kejahatan Siber Di *Mobile banking* Pada Bank Pembangunan Daerah Yogyakarta Kantor Cabang Syariah, maka rekomendasi untuk penelitian selanjutnya yaitu melakukan wawancara langsung ke divisi IT Bank BPD DIY. Sehingga data yang dikumpulkan lebih banyak dan permasalahan yang dialami oleh nasabah dan juga internal bank akan lebih beragam. Pada penelitian selanjutnya dapat meneliti permasalahan yang timbul

pada penelitian ini terkait Strategi Penerapan Manajemen Risiko Untuk Mencegah Kejahatan Siber Di *Mobile banking* Pada Bank Pembangunan Daerah Yogyakarta Kantor Cabang Syariah.

DAFTAR PUSTAKA

Abdussamad, H. Z., & Sik, M. S. (2021). *Metode penelitian kualitatif*. CV. Syakir Media Press.

Chintia, E., Nadiah, R., Ramadhani, H. N., Haedar, Z. F., Febriansyah, A., & Kom, N. A. R. S. (2018). Kasus Kejahatan Siber Yang Paling Banyak Terjadi Di Indonesia Dan Penanganannya. *JIEET (Journal of Information Engineering and Educational Technology)*, *2*(2), 65–69.

Darwin, M., Mamondol, M. R., Sormin, S. A., Nurhayati, Y., Tambunan, H., Sylvia, D., Adnyana, I. M. D. M., Prasetiyo, B., Vianitati, P., & Gebang, A. A. (2021). *Metode Penelitian Pendekatan Kuantitatif*.

Data diolah penulis. (2024).

Desda, M. M., & Yurasti, Y. (2019). Analisis Penerapan Manajemen Risiko Kredit Dalam Meminimalisir Kredit Bermasalah Pada PT. BPR Swadaya Anak Nagari Bandarejo Simpang Empat Periode 2013-2018. *Mbia*, *18*(1), 94–106.

Gebang, A. A., Prasetiyo, B., Sylvia, D., Tambunan, H., Adnyana, I. M. D. M., Mamondol, M. R., Darwin, M., Vianitati, P., Sormin, S. A., & Nurhayati, Y. (2022). *Metode penelitian pendekatan kuantitatif*.

Kusumastuti, A., & Khoiron, A. M. (2019). *Metode penelitian kualitatif*. Lembaga Pendidikan Sukarno Pressindo (LPSP).

Lana, A. (2021). Dampak kejahatan siber terhadap teknologi informasi dan pengendalian internal. *Journal of Economics, Social and Education*, *1*(3), 1–13.

Mutiasari, A. I. (2020). Perkembangan Industri Perbankan Di Era Digital. *Jurnal Ekonomi Bisnis Dan Kewirausahaan*, *9*(2), 32–41.

Ngamal, Y., & Perajaka, M. A. (2022). Penerapan Model Manajemen Risiko Teknologi Digital Di Lembaga Perbankan Berkaca Pada Cetak Biru Transformasi Digital Perbankan Indonesia. *Jurnal Manajemen Risiko*, *2*(2), 59–74.

Ningrum, D. P. S., & Robekha, J. (2023). Analisa Yuridis Dalam Kasus Kejahatan Siber Terhadap Internet Banking di Indonesia. *PESHUM: Jurnal Pendidikan, Sosial Dan Humaniora*, *2*(4), 765–776.

Nugrahani, F., & Hum, M. (2014). Metode penelitian kualitatif. *Solo: Cakra Books*, *1*(1), 3–4.

Prakosa, A. (2019). Analisis pengaruh persepsi teknologi dan persepsi risiko terhadap kepercayaan pengguna m-banking. *Jurnal Manajemen*, *9*(2), 270–282.

Pratama, I. P. A. E., & Pratika, M. T. S. (2020). Manajemen risiko teknologi informasi terkait manipulasi dan peretasan sistem pada Bank XYZ tahun 2020 menggunakan ISO 31000: 2018. *Jurnal Telematika*, *15*(2), 63–70.

Pujaastawa, I. B. G. (2016). Teknik wawancara dan observasi untuk pengumpulan bahan informasi. *Universitas Udayana*, *4*.

Purwanto, E., & Loisa, J. (2020). The intention and use behaviour of the *mobile banking* system in Indonesia: UTAUT Model. *Technology Reports of Kansai University*, *62*(06), 2757–2767.

Putra, M. I. A., & Sari, R. C. (2020). Pengaruh Persepsi Kegunaan, Persepsi Kemudahan Penggunaan, Kepercayaan, Dan Persepsi Risiko Terhadap Minat Menggunakan *Mobile banking* Dengan Gender Sebagai Variabel Moderasi. *Jurnal Profita: Kajian Ilmu Akuntansi*, *8*(8).

Qintharah, Y. N. (2019). Perancangan Penerapan Manajemen Risiko. *JRAK: Jurnal Riset Akuntansi Dan Komputerisasi Akuntansi*, *10*(1), 67–86.

Sari, A., Afrida, Y., & Mardiah, N. (2022). The Influence Of *Mobile banking* Service Quality On Customer Satisfaction Of Indonesian Sharia Bank (Case Study: Asn Uin Imam Bonjol Padang). *Al-Masraf: Jurnal Lembaga Keuangan Dan Perbankan*, *7*(1), 55–68.

Sari, D. M., Fasa, M. I., & Suharto, S. (2021). Manfaat Dan Risiko Penggunaan Layanan Perbankan Melalui Aplikasi *Mobile banking*. *Al-Infaq: Jurnal Ekonomi Islam*, *12*(2), 170–182.

Sarwono, A. E., & Handayani, A. (2021). *Metode kuantitatif*. Unisri Press. https://books.google.com/books?hl=id&lr=&id=Tr2bEAAAQBAJ&oi=fnd&pg=PR1&dq=METODE+KUANTITATIF+Penulis+:+Dr.+Aris+Eddy+Sarwono,+MSi.,Ak+Dr.+Asih+Handayani+M.Si.,+M.Pd.&ots=sKrX5EzUp4&sig=UVSf7icrYtLwVt5iJ9xuhjMzzik

Sidiq, U., Choiri, M., & Mujahidin, A. (2019). Metode penelitian kualitatif di bidang pendidikan. *Journal of Chemical Information and Modeling*, *53*(9), 1–228.

Siregar, M. (2021). Analisis Kepuasan Pelanggan Ompu Gende Coffee Medan. *Jurnal Diversita*, *7*(1), 114–120.

Sugiono, S. (2016). *Metode penelitian kuantitatif, kualitatif, dan r & d* (Vol. 288).

Sulisrudatin, N. (2018). Analisa Kasus Cybercrime Bidang Perbankan Berupa Modus Pencurian Data Kartu Kredit. *Jurnal Ilmiah Hukum Dirgantara*, *9*(1).

Suwiknyo, F. B. (2021). Tindak Kejahatan Siber Di Sektor Jasa Keuangan Dan Perbankan. *LEX PRIVATUM*, *9*(4).

Syafii, I., & Siregar, S. (2020). *Manajemen Risiko Perbankan Syariah*. *1*(1), 662–665.

Waruwu, M. (2023). Pendekatan penelitian pendidikan: Metode penelitian kualitatif, metode penelitian kuantitatif dan metode penelitian kombinasi (Mixed Method). *Jurnal Pendidikan Tambusai*, *7*(1), 2896–2910.

Wawancara personal. (2024, July).

Yam, J. H., & Taufik, R. (2021). Hipotesis Penelitian Kuantitatif. *Perspektif: Jurnal Ilmu Administrasi*, *3*(2), 96–102.

Lampiran 1. Surat Permohonan Izin Pengambilan Data

UNIVERSITAS ISLAM INDONESIA

FAKULTAS
BISNIS DAN EKONOMIKA

Gedung Prof. Dr. Ace Partadiredja
Universitas Islam Indonesia
Condong Catur Depok Yogyakarta 55283
T. (0274) 881546, 885376
F. (0274) 882589
E. fbe@uii.ac.id
W. fbe.uii.ac.id

Nomor : 044.057/Ket/20/Akd/VI/2024
Lamp : -
Perihal : **Permohonan izin pengambilan data**

Kepada Yth.
Kepala/Pimpinan/HRD
Bank Pembangunan Daerah Kantor Cabang Syariah Yogyakarta
Jalan Magelang 55285 Sendangadi Yogyakarta

Assalamu'alaikum Wr Wb

Diberitahukan dengan hormat, bahwa setiap mahasiswa sebelum mengakhiri studi di Program Sarjana Terapan Fakultas Bisnis dan Ekonomika UII Yogyakarta, diwajibkan membuat Penelitian Terapan sebagai syarat kelulusan. Sehubungan dengan itu, mahasiswa/i kami :

Nama	: Yunan Dwi Prasetyo
No Mhs	: 20213067
Jurusan	: Analisis Keuangan
Judul	: Strategi Penerapan Manajemen Risiko untuk Mencegah Kejahatan Siber di Mobile Banking pada Bank Pembangunan Daerah Yogyakarta Kantor Cabang Syariah
Tanggal Pengambilan Data	: 04 Juli 2024
No Hp	: 082234553391

Bermaksud untuk melakukan pengambilan data di **Bank Pembangunan Daerah Kantor Cabang Syariah Yogyakarta.** Oleh karena itu kami mohon bantuan Bapak/Ibu untuk dapat memberikan data tersebut kepada mahasiswa kami.

Atas bantuan dan kerjasama Bapak/Ibu pimpinan, diucapkan terima kasih.

Wassalamu'alaikum Wr Wb

Yogyakarta, 25 Juni 2024
Ketua Prodi D4 Analisis Keuangan

Dr. Phil. Ninik Sri Rahayu, S.E., M.M.

Lampiran 2. Kuesioner Penelitian

KUESIONER PENELITIAN

Strategi Penerapan Manajemen Risiko Untuk Mencegah Kejahatan Siber Di *Mobile Banking* Pada Bank Pembangunan Daerah Yogyakarta Kantor Cabang Syariah

Tujuan: Penggunaan *Mobile banking* Kesadaran dan Persepsi Ancaman Siber Praktik Manajemen Risiko Evaluasi Strategi Manajemen Risiko Standar Peraturan dan Industri Kesadaran dan Pendidikan Pengguna.

Sebelum mengisi lembar kuisioner, mohon terlebih dahulu membaca instruksi pengisian pada masing-masing bagian

Bagian 1: Informasi Demografis

Isilah identitas anda dibawah ini:

1. Nama : (boleh menggunakan inisial)
2. Nomor tlp : (opsional)
3. Umur :
    a. Di bawah 18 tahun
    b. 18-24
    c. 25-34
    d. 35-44
    e. 45-54
    f. 55 ke atas
4. Jenis kelamin:
    a. Laki-laki
    b. Perempuan
5. Kerja:
    a. Pelajar
    b. Bekerja (Sektor Perbankan)
    c. Bekerja (Sektor Non-Perbankan)
    d. Wiraswasta
    e. Pengangguran

f. Lain-lain

6. Tingkat Pendidikan:
    a. SD-SMP
    b. SMA
    c. Diploma
    d. Sarjana
    e. Pascasarjana (S2-S3)

Bagian 2: Penggunaan *Mobile banking*

1. Seberapa sering Anda menggunakan layanan *mobile banking*?
    a. Harian
    b. Mingguan
    c. Bulanan
    d. Jarang
    e. Tidak pernah
2. Manakah dari layanan *mobile banking* berikut yang Anda gunakan? (Pilih semua yang berlaku)
    a. Memeriksa saldo
    b. Mentransfer uang
    c. Membayar tagihan
    d. Mengajukan pinjaman
    e. Setoran seluler
    f. Lainnya (sebutkan)

Bagian 3: Kesadaran dan Persepsi tentang Ancaman Cyber

1. Seberapa sadar Anda tentang ancaman cyber yang terkait dengan *mobile banking*?
    a. Sangat sadar
    b. Agak sadar
    c. Netral
    d. Agak tidak sadar
    e. Sangat tidak sadar

2. Pernahkah Anda mengalami ancaman atau serangan cyber saat menggunakan *mobile banking*?
    a. Ya
    b. Tidak
    c. Jika ya, jelaskan sifat ancaman atau serangan dunia maya:

Bagian 4: Praktik Manajemen Risiko

Pertanyaan	**Jawaban**
Manakah dari langkah-langkah keamanan berikut yang Anda gunakan untuk mobile banking?	a. Kata sandi yang kuat b. Otentikasi dua faktor (2FA) c. Otentikasi biometrik (sidik jari, pengenalan wajah) d. Memperbarui aplikasi mobile banking secara berkala e. Menghindari Wi-Fi publik untuk *mobile banking* f. Lainnya (sebutkan)
Apakah Anda penilaian risiko kejahatan siber secara berkala?	a. Iya b. Tidak
Apakah Anda menerapkan kontrol keamanan untuk mengurangi risiko kejahatan siber?	a. Iya b. Tidak
Apakah Anda memiliki rencana untuk merespons insiden kejahatan siber?	a. Iya b. Tidak
Menurut anda penting pendidikan pengguna dalam mencegah kejahatan dunia maya di *mobile banking*?	a. Iya b. Tidak
Apakah Anda menerima segala bentuk pendidikan atau pelatihan tentang keamanan *mobile banking* dari bank Anda?	a. Iya b. Tidak

Apakah pendidikan atau pelatihan dalam meningkatkan kesadaran dan praktik sangat efektif bagi Anda?	**a. Iya** **b. Tidak**

Bagian 5: Evaluasi Strategi Manajemen Risiko

Keterangan	**STS**	**TS**	**N**	**S**	**SS**
Seberapa yakin Anda menilai efektivitas keseluruhan strategi manajemen risiko bank Anda dalam mencegah kejahatan dunia maya					
Seberapa puas Anda dengan langkah-langkah keamanan saat ini yang disediakan oleh aplikasi *mobile banking* Anda					

Bagian 6: Tantangan Utama

Keterangan	**STS**	**TS**	**N**	**S**	**SS**
Dukungan yang tidak memadai dari bank dalam memastikan transaksi *mobile banking* yang aman					
Kurangnya kesadaran/edukasi tentang ancaman siber dalam transaksi *mobile banking*					
Kompleksitas langkah-langkah keamanan dalam transaksi *mobile banking*					
Kendala teknik yang dihadapai saat melalukukan transaksi *mobile banking*					

Bagian 7: Pertanyaan Terbuka

1. Silakan bagikan pengalaman pribadi apa pun yang Anda miliki dengan ancaman cyber di *mobile banking* dan bagaimana penyelesaiannya:

2. Menurut Anda, apa langkah paling penting yang harus diambil bank untuk meningkatkan keamanan *mobile banking*?
3. Apa langkah-langkah tambahan atau fitur yang akan Anda rekomendasikan untuk meningkatkan keamanan *mobile banking*?
4. Apakah Anda memiliki komentar atau saran lain mengenai keamanan *mobile banking* dan manajemen risiko?
5. Perbaikan apa pada standar peraturan yang akan Anda sarankan untuk meningkatkan keamanan *mobile banking*?
6. Sumber daya atau dukungan pendidikan tambahan apa yang menurut Anda bermanfaat dalam mengamankan aktivitas *mobile banking* Anda?

Lampiran 3. Wawancara informan kunci

Pedoman Wawancara

Praktik Manajemen Risiko Saat Ini

1. Gambaran Umum Praktik:
    a. Apa praktik manajemen risiko utama yang saat ini digunakan oleh bank Anda untuk mencegah kejahatan dunia maya di *mobile banking*?
2. Langkah-langkah khusus:
    a. Dapatkah Anda menguraikan langkah-langkah keamanan khusus seperti otentikasi multi-faktor, otentikasi biometrik, dan pembaruan perangkat lunak reguler?
    b. Bagaimana langkah-langkah ini bekerja dalam praktik?
3. Efektivitas:
    a. Menurut Anda, seberapa efektif praktik manajemen risiko ini dalam mencegah kejahatan dunia maya?
    b. Dapatkah Anda memberikan contoh situasi di mana praktik-praktik ini berhasil mengurangi ancaman dunia maya?

Tantangan dalam Menerapkan Strategi Manajemen Risiko

4. Tantangan Utama:
    a. Apa tantangan utama yang Anda hadapi dalam menerapkan dan mempertahankan strategi manajemen risiko yang efektif untuk keamanan *mobile banking*?
    b. Apakah ada faktor internal atau eksternal tertentu yang menghambat upaya ini?
5. Masalah teknis:
    a. Masalah teknis apa yang Anda temui dengan langkah-langkah keamanan saat ini?
    b. Bagaimana masalah ini berdampak pada keamanan layanan *mobile banking* secara keseluruhan?
6. Kesadaran Pengguna:
    a. Bagaimana perilaku dan kesadaran pengguna mempengaruhi efektivitas strategi manajemen risiko bank Anda?

b. Langkah-langkah apa yang telah diambil untuk mendidik pengguna tentang keamanan *mobile banking*?

Standar Peraturan dan Industri

7. Dampak Regulasi:
   a. Bagaimana kerangka peraturan dan standar industri mempengaruhi strategi manajemen risiko bank Anda?
   b. Apakah ada persyaratan peraturan yang menurut Anda sangat sulit untuk dipatuhi?
8. Perbaikan:
   a. Perbaikan apa pada standar peraturan yang akan Anda sarankan untuk meningkatkan keamanan *mobile banking*?

Praktik Terbaik dan Rekomendasi

9. Strategi Sukses:
   a. Dapatkah Anda berbagi praktik terbaik atau pendekatan inovatif yang telah sangat berhasil dalam mencegah kejahatan cyber di *mobile banking*?
10. Rekomendasi:
    a. Apa langkah-langkah tambahan atau strategi yang akan Anda rekomendasikan untuk lebih meningkatkan keamanan dan manajemen risiko layanan *mobile banking*?
11. Tren Masa Depan:
    a. Apa tren atau teknologi masa depan yang Anda yakini akan berdampak signifikan pada keamanan *mobile banking*?

Pertanyaan Terbuka

12. Pengalaman Pribadi:
    a. Dapatkah Anda berbagi pengalaman pribadi dengan ancaman cyber di *mobile banking* dan bagaimana mereka diselesaikan?
13. Langkah Kritis:
    a. Menurut Anda, apa langkah paling penting yang harus diambil bank untuk meningkatkan keamanan *mobile banking*?
14. Komentar Tambahan:

Apakah Anda memiliki komentar atau saran lain mengenai keamanan *mobile banking* dan manajemen risiko?

Lampiran 4. Distribusi Frekuensi Variabel Penelitian

1. Informasi Demografis

USIA					
		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	18-24	41	42.7	42.7	42.7
	25-34	32	33.3	33.3	76.0
	35-44	23	24.0	24.0	100.0
	Total	96	100.0	100.0	

JENIS KELAMIN					
		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Laki-laki	45	46.9	46.9	46.9
	Perempuan	51	53.1	53.1	100.0
	Total	96	100.0	100.0	

PEKERJAAN					
		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Pelajar/Mahasiswa	28	29.2	29.2	29.2
	Bekerja (Sektor Perbankan)	35	36.5	36.5	65.6
	Bekerja (Sektor Non-Perbankan)	20	20.8	20.8	86.5
	Wiraswasta	11	11.5	11.5	97.9
	Lain-lain	2	2.1	2.1	100.0
	Total	96	100.0	100.0	

PENDIDIKAN					
		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	SMA	19	19.8	19.8	19.8
	Diploma	24	25.0	25.0	44.8
	Sarjana	50	52.1	52.1	96.9
	Pascasarjana (S2-S3)	3	3.1	3.1	100.0

	Total	96	100.0	100.0	

2. Praktik Manajemen Risiko

LANGKAH LANGKAH KEAMANAN *MOBILE BANKING*					
		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Kata sandi yang kuat	67	26.2	26.2	26.2
	Otentifikasi dua faktor (2FA)	59	23.0	23.0	49.2
	Otentikasi biometrik (sidik jari, pengenalan wajah)	68	26.6	26.6	75.8
	Memperbarui aplikasi *mobile banking* secara berkala	40	15.6	15.6	91.4
	Menghindari Wi-Fi publik untuk *mobile banking*	22	8.6	8.6	100.0
	Total	256	100.0	100.0	

Apakah Anda penilaian risiko kejahatan siber secara berkala?					
		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Ya	76	79.2	79.2	79.2
	Tidak	20	20.8	20.8	100.0
	Total	96	100.0	100.0	

Apakah Anda menerapkan kontrol keamanan untuk mengurangi risiko kejahatan siber?					
		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Ya	90	93.8	93.8	93.8
	Tidak	6	6.3	6.3	100.0
	Total	96	100.0	100.0	

Apakah Anda menerapkan kontrol keamanan untuk mengurangi risiko kejahatan siber?					
		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Ya	84	87.5	87.5	87.5
	Tidak	12	12.5	12.5	100.0
	Total	96	100.0	100.0	

Menurut anda penting pendidikan pengguna dalam mencegah kejahatan dunia maya di *mobile banking*?					
		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Ya	93	96.9	96.9	96.9
	Tidak	3	3.1	3.1	100.0
	Total	96	100.0	100.0	

Apakah Anda menerima segala bentuk pendidikan atau pelatihan tentang keamanan *mobile banking* dari bank Anda?					
		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Ya	79	82.3	82.3	82.3
	Tidak	17	17.7	17.7	100.0
	Total	96	100.0	100.0	

Apakah pendidikan atau pelatihan dalam meningkatkan kesadaran dan praktik sangat efektif bagi Anda?					
		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Ya	90	93.8	93.8	93.8
	Tidak	6	6.3	6.3	100.0
	Total	96	100.0	100.0	

3. Evaluasi Strategi Manajemen Risiko

Seberapa yakin Anda menilai efektivitas keseluruhan strategi manajemen risiko bank Anda dalam mencegah kejahatan dunia maya					
		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Tidak Setuju	3	3.1	3.1	3.1
	Netral	23	24.0	24.0	27.1
	Setuju	45	46.9	46.9	74.0
	Sangat Setuju	25	26.0	26.0	100.0
	Total	96	100.0	100.0	

Seberapa puas Anda dengan langkah-langkah keamanan saat ini yang disediakan oleh aplikasi *mobile banking* Anda					
		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Sangat Tidak Setuju	2	2.1	2.1	2.1
	Tidak Setuju	4	4.2	4.2	6.3
	Netral	19	19.8	19.8	26.0
	Setuju	41	42.7	42.7	68.8
	Sangat Setuju	30	31.3	31.3	100.0
	Total	96	100.0	100.0	

4. Tantangan Utama

Dukungan yang tidak memadai dari bank dalam memastikan transaksi *mobile banking* yang aman					
		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Sangat Tidak Setuju	2	2.1	2.1	2.1
	Tidak Setuju	10	10.4	10.4	12.5
	Netral	24	25.0	25.0	37.5
	Setuju	40	41.7	41.7	79.2
	Sangat Setuju	20	20.8	20.8	100.0
	Total	96	100.0	100.0	

Kurangnya kesadaran/edukasi tentang ancaman siber dalam transaksi *mobile banking*					
		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Tidak Setuju	4	4.2	4.2	4.2
	Netral	17	17.7	17.7	21.9
	Setuju	46	47.9	47.9	69.8
	Sangat Setuju	29	30.2	30.2	100.0
	Total	96	100.0	100.0	

Kompleksitas langkah-langkah keamanan dalam transaksi *mobile banking*					
		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Tidak Setuju	3	3.1	3.1	3.1
	Netral	20	20.8	20.8	24.0
	Setuju	46	47.9	47.9	71.9
	Sangat Setuju	27	28.1	28.1	100.0
	Total	96	100.0	100.0	

Kendala teknik yang dihadapai saat melalukukan transaksi *mobile banking*					
		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Tidak Setuju	4	4.2	4.2	4.2
	Netral	21	21.9	21.9	26.0
	Setuju	43	44.8	44.8	70.8
	Sangat Setuju	28	29.2	29.2	100.0
	Total	96	100.0	100.0	