

**ANALISIS MANAJEMEN RESIKO PENGGUNAAN MOBILE
BANKING PADA BANK DEVELOPMENT BANK OF SINGAPORE
(DBS) INDONESIA**

Dhea Yurike Silaban¹, Rani Selfia Sipayung², Ruhama Girsang³, Depina Tumangger⁴, Irma Siagian⁵

Universitas Negeri Medan

Email: dheasilaban1@gmail.com¹, raniselviasipayung@gmail.com², ruhamagirsang14@gmail.com³, depinatumangger9@gmail.com⁴, irmasiagian@unimed.ac.id⁵

Abstrak – Masa ini perkembangan teknologi informasi dan komunikasi, telah menjadikan suatu Industri perbankan bersaing ketat dalam menciptakan inovasi produk serta layanan berbasis digital atau elektronik dalam layanan transaksinya. Mobile banking merupakan bagian dari contoh Perkembangan teknologi yang begitu menarik karena dapat melakukan transaksi secara langsung kapan saja, dimana saja serta dapat diakses selama 24 jam dengan menggunakan internet melalui smartphone. Penelitian ini menggunakan pendekatan kualitatif dengan metode studi kasus untuk menganalisis manajemen risiko penggunaan mobile banking di bank DBS. Hasilnya mengungkapkan bahwa DBS telah menerapkan beberapa langkah keamanan, seperti otentikasi multi-faktor, enkripsi data, dan sistem deteksi penipuan canggih, untuk meningkatkan keamanan platform mobile bankingnya, digibank. Namun, penelitian ini juga mengidentifikasi tantangan yang signifikan, termasuk kebutuhan untuk peningkatan pendidikan pelanggan mengenai literasi digital dan risiko ancaman dunia maya, yang dapat merusak kepercayaan pelanggan. Sebagai kesimpulan, sementara DBS telah membuat langkah-langkah dalam pengamanan layanan perbankan digitalnya, efektivitas langkah-langkah ini harus terus dievaluasi dan dinilai. Studi ini merekomendasikan strategi komprehensif yang mencakup investasi berkelanjutan dalam teknologi, peningkatan pendidikan pelanggan, dan komunikasi transparan untuk menumbuhkan kepercayaan dan memastikan keamanan transaksi pelanggan di lanskap digital.

Kata Kunci : Manajemen Risiko Digital, Mobile Banking, Keamanan Siber, Pendidikan Pelanggan, Deteksi Penipuan, DBS, Mitigasi Risiko, Jasa Keuangan.

PENDAHULUAN

Masa ini perkembangan teknologi informasi dan komunikasi, telah menjadikan suatu Industri perbankan bersaing ketat dalam menciptakan inovasi produk serta layanan berbasis digital atau elektronik dalam layanan transaksinya. Kemampuan manajemen dalam mengadopsi teknologi baru sangat menentukan tingkat keberhasilan dalam pengembangan inovasi layanan (Trisnawati & Fahmi, 2017).

Salah satu Layanan berbasis teknologi yang disediakan oleh bank adalah mobile banking (M-Banking) yang mampu memberikan layanan kemudahan melaksanakan transaksi Perbankan seperti pembayaran, pembiayaan, transfer, dan lain sebagainya. Fasilitas teknologi Mobile banking diharapkan mampu memberi kemudahan untuk nasabah dalam melakukan Transaksi (Sri Wahyuni & Darlinda, 2021). Mobile banking merupakan bagian dari contoh Perkembangan teknologi yang begitu menarik karena dapat melakukan transaksi secara langsung kapan saja, dimana saja serta dapat diakses selama 24 jam dengan menggunakan internet atau mobile data melalui smartphone (Fandi, 2019).

Banyak masyarakat yang meragukan keamanan pada layanan mobile banking (Jayantari & Seminari, 2018). Apabila dilihat dari aktivitas financial yang dilakukan, layanan mobile Banking lebih banyak digunakan untuk mencari informasi. Bahkan, jumlah aktivitas pencarian Informasinya bisa sampai tiga kali lipat dibanding dengan kegiatan transaksi (Jayantari & Seminari, 2018). Hal itu dikarenakan banyaknya tindak kejahatan melalui media teknologi Informasi yang dimanfaatkan oleh orang-orang yang tidak bertanggung jawab. Mobile banking menimbulkan kekhawatiran yang tinggi pada nasabah perihal terjadinya penipuan, pencurian data, dan tindak kejahatan lainnya, sehingga, inilah salah satu alasan yang menjadikan pertumbuhan mobile banking cukup lambat (Nurdin dkk. 2020:89). Penelitian ini dalam rangka menganalisis aspek manajemen risiko layanan mobile banking bank The Development Bank Of Singapore Limited (DBS), serta mengetahui bagaimana cara-cara bank DBS dalam menyelesaikan berbagai kendala dan permasalahan yang ada.

METODOLOGI PENELITIAN

Penelitian ini menggunakan pendekatan kualitatif dengan metode studi kasus untuk menganalisis manajemen resiko penggunaan mobile mbaking di bank DBS. Pendekatan kualitatif dipilih karena memungkinkan para peneliti untuk memahami secara mendalam pengalaman dan perspektif pengguna serta pihak-pihak terkait dalam penggunaan mobile mbaking ini.

Adapun teknik utama pengumpulan data pada penelitian ini yaitu melalui wawancara mendalam . Wawancara dilakukan pada salah satu karyawan bank DBS dan juga nasabah pengguna aktif mobile mbaking bank DBS. Pertanyaan-pertanyaan yang ditanyakan mencakup:

1. Pengalaman pengguna dalam menggunakan mobile mbaking
2. Persepsi pengguna terhadap resiko keamanan mobile mbaking
3. Upaya yang telah dilakukan bank DBS dalam mengelola resiko keamanan mobile mbaking
4. Efektivitas kebijakan dan prosedur manajemen risiko yang diterapkan
5. Keluhan yang dialami banyak nasabah selama menggunakan mobile mbaking

Dengan metode penelitian ini diharapkan para peneliti dapat memberikan pemahaman yang mendalam tentang manajemen resiko penggunaan mobile mbaking di bank DBS dan memberikan rekomendasi yang bermanfaat untuk meningkatkan keamanan dan kenyamanan pengguna.

HASIL DAN PEMBAHASAN

PT Bank DBS Indonesia (DBS Indonesia atau Bank) didirikan pada tanggal 30 Juni 1989 dengan nama PT. Bank Mitsubishi Buana, yang merupakan usaha bersama antara Mitsubishi Bank Ltd dan PT Bank Buana Indonesia. Di tahun 1997, DBS Bank Ltd mengakuisisi saham Mitsubishi Bank Ltd di PT Bank Mitsubishi Buana dan mengubah nama Bank menjadi PT Bank DBS Buana. Kemudian, pada bulan Oktober 2000 nama Bank berubah kembali menjadi PT Bank DBS Indonesia.

DBS Indonesia merupakan anak perusahaan DBS Bank Ltd. (DBS Bank) yang berpusat dan terdaftar di Singapura sebagai sebuah grup pemberi jasa keuangan terkemuka di Asia sejak didirikan tahun 1968. DBS Indonesia telah mencapai pertumbuhan yang pesat dengan hanya 3 kantor cabang di tahun 2004 hingga berkembang pada tahun 2018 menjadi 44 kantor cabang di 13 kota utama di Indonesia (Jakarta, Surabaya, Medan, Bandung, Semarang, Yogyakarta, Pekanbaru, Palembang, Makassar, Pontianak, Samarinda, Bogor, dan Tangerang). DBS Indonesia menyediakan layanan perbankan menyeluruh untuk korporasi, usaha kecil dan menengah (SME), dan aktivitas perbankan konsumen.

DBSI adalah PT Bank DBS Indonesia, suatu institusi perbankan yang berizin dan diawasi oleh Otoritas Jasa Keuangan (OJK) serta merupakan peserta penjaminan Lembaga Penjamin Simpanan (LPS). Nasabah bank ini diwajibkan untuk berlayanan dengan aplikasi mobile banking yang di berikan nama digibank. Aplikasi digibank by DBS adalah aplikasi digital dari DBSI yang memberikan kemudahan bagi Pemegang Kartu Kredit digibank untuk melakukan aktivitas perbankan termasuk layanan kartu kredit yaitu program perubahan tagihan menjadi cicilan. Aplikasi digibank ini sama seperti aplikasi Mobile banking lainnya yang sangat membantu nasabah dalam melakukan transaksi tanpa harus pergi ke bank namun dapat dari handphone saja. Banyak jenis transaksi yang dapat dilakukan mulai dari yang non finansial seperti informasi saldo dan mutasi rekening (dapat memudahkan nasabah untuk dapat mengecek rekening koran untuk memastikan setiap transaksi yang dilakukan benar adanya dan dapat terhindar dari transaksi pencurian dana tabungan) hingga ke transaksi finansial seperti transfer, pembayaran tagihan serta pembelian pulsa.

Mobile banking memiliki kelebihan dan manfaat, ada sejumlah risiko atau ancaman yang perlu dipertimbangkan, dan kejahatan dunia maya yang sangat berbahaya bagi nasabahnya. Karena fasilitas Mobile banking kini sengaja disalahgunakan oleh banyak pihak, kejahatan siber, penipuan, dan pembobolan rekening (Pratama & Pratika, 2020). Salah satu karyawan DBS cabang Medan, Lusi Mawanti Munthe menyebutkan tantangan yang sering di hadapi pihak bank adalah ketika nasabah mengalami penipuan dari pihak yang tidak bertanggung jawab dan mengatasnamakan bank. Kemudian, nasabah akan komplain dan menjelek-jelekkan nama bank. Sehingga dapat menimbulkan kekhawatiran pihak bank akan kepercayaan nasabah lain yang berkurang kepada bank.

Dalam era digital yang terus berkembang, aplikasi mobile banking menjadi tulang punggung layanan perbankan modern. Bank DBS Indonesia, seperti lembaga keuangan lainnya, menghadapi serangkaian tantangan khusus terkait pengembangan dan pengelolaan aplikasi mobile banking mereka.

1. Keamanan siber menjadi tantangan krusial lainnya. Dengan semakin banyaknya transaksi yang dilakukan melalui aplikasi mobile banking, risiko serangan siber dan kejahatan keuangan juga meningkat. DBS Indonesia harus berinvestasi dalam teknologi keamanan terbaru dan menerapkan langkah-langkah keamanan yang ketat untuk melindungi data dan dana nasabah. Ini termasuk enkripsi data, otentikasi multi-faktor, dan sistem deteksi penipuan yang canggih.
2. Persaingan dengan fintech dan bank digital juga menjadi tantangan signifikan. Perusahaan-perusahaan ini sering kali lebih lincah dan mampu mengembangkan aplikasi

dengan fitur-fitur inovatif yang menarik bagi nasabah DBS Indonesia perlu terus memantau tren pasar dan mengembangkan fitur-fitur baru yang relevan untuk tetap kompetitif.

3. Edukasi nasabah tentang penggunaan aplikasi mobile banking yang aman dan efektif juga menjadi tantangan. Tidak semua nasabah memiliki tingkat literasi digital yang sama, dan beberapa mungkin memerlukan bantuan untuk memahami cara menggunakan aplikasi dengan aman. DBS Indonesia perlu menyediakan sumber daya pendidikan yang memadai dan dukungan pelanggan yang responsif untuk membantu nasabah mengatasi tantangan ini.

Di kutip dari [dbs.com](https://www.dbs.com) memiliki dan sudah menyusun manajemen risiko untuk meminimalisir tantangan tantangan yang di hadapi bang. Mengejar prioritas strategis dan peluang bisnis pada dasarnya mengandung risiko. Penting bagi DBS Group dan sesama karyawan untuk memahami risiko yang melekat dalam aktivitas bisnis, dan mampu mengidentifikasi, menilai, memitigasi, memantau, melaporkan, dan mengukur risiko tersebut dengan tepat.

DBS memiliki Di Risk Management Group (RMG), yang bertugas untuk mengembangkan dan memelihara kerangka kerja manajemen risiko dan pengendalian internal. memberikan tinjauan dan tantangan independen terhadap bisnis, sebagai bagian dari upaya untuk memastikan bahwa keseimbangan yang tepat dipertimbangkan dalam keputusan risiko/imbalance hasil. Selain itu, RMG juga bertanggung jawab atas pemantauan dan pelaporan masalah risiko utama di Bank. Untuk mengelola risiko secara efektif dan memberikan kinerja keuangan yang kuat, berinvestasi secara signifikan pada orang-orang dan infrastruktur.

Tim RMG menjelaskan bahwa mereka berusaha untuk terus berinovasi, meningkatkan, dan menanamkan kemampuan manajemen risiko. Sebagai bagian dari tim, Anda akan belajar tentang bagaimana RMG telah meningkatkan proses manajemen risiko melalui analisis data dan algoritma. Peran utama dalam RMG mencakup berbagai fungsi: Risiko Kredit, Risiko Pasar dan Likuiditas, Risiko Operasional, Analisis Portofolio Grup, Validasi Model, serta Arsitektur Perusahaan dan Digital Risiko.

1. **Risiko Kredit:**

Risiko kredit adalah potensi kerugian yang timbul akibat kegagalan pihak lain (debitur) dalam memenuhi kewajiban pembayaran sesuai dengan perjanjian. Dalam konteks perbankan, ini sering kali terkait dengan pemberian pinjaman. Manajemen risiko kredit melibatkan penilaian kelayakan kredit calon debitur, penetapan batas kredit, dan pemantauan portofolio kredit secara berkala.

2. **Risiko Pasar dan Likuiditas:**

Risiko pasar berkaitan dengan potensi kerugian akibat perubahan kondisi pasar, seperti suku bunga, nilai tukar, dan harga komoditas. Sementara itu, risiko likuiditas adalah risiko ketidakmampuan suatu entitas untuk memenuhi kewajiban keuangannya yang jatuh tempo. Manajemen risiko pasar dan likuiditas melibatkan analisis sensitivitas portofolio terhadap perubahan pasar dan pengelolaan arus kas yang efektif.

3. **Risiko Operasional:**

Risiko operasional mencakup potensi kerugian akibat kegagalan proses internal, kesalahan manusia, sistem yang tidak memadai, atau kejadian eksternal. Ini bisa berupa kesalahan dalam transaksi, kegagalan sistem teknologi informasi, atau penipuan. Manajemen risiko operasional melibatkan identifikasi risiko, pengembangan prosedur pengendalian internal, dan penerapan sistem manajemen risiko.

4. **Analisis Portofolio Grup:**

Analisis portofolio grup melibatkan evaluasi risiko dan kinerja seluruh portofolio

investasi atau aset suatu kelompok perusahaan. Tujuannya adalah untuk memahami eksposur risiko secara keseluruhan, mengidentifikasi konsentrasi risiko, dan mengoptimalkan alokasi aset untuk mencapai tujuan keuangan grup.

5. **Validasi Model:**

Validasi model adalah proses evaluasi dan pengujian model-model kuantitatif yang digunakan dalam manajemen risiko. Ini penting untuk memastikan bahwa model-model tersebut akurat, andal, dan sesuai dengan tujuan penggunaannya. Validasi model melibatkan pengujian asumsi, parameter, dan hasil model terhadap data historis dan skenario stres.

6. **Arsitektur Perusahaan dan Digital Risiko:**

Arsitektur perusahaan dan risiko digital berkaitan dengan kerangka kerja dan sistem yang digunakan untuk mengelola risiko dalam era digital. Ini mencakup identifikasi dan mitigasi risiko yang terkait dengan teknologi informasi, keamanan siber, dan transformasi digital. Manajemen risiko digital melibatkan penerapan teknologi untuk memantau dan mengendalikan risiko, serta pengembangan kebijakan dan prosedur untuk melindungi data dan sistem.

Selain itu, beberapa tips yang diberikan kepada nasabah perihal pencegahan dan mitigasi risiko yang mungkin bisa timbul adalah:

a. **Menjaga Informasi Rahasia Akun Bank**

Selain oleh nasabah, upaya yang dilakukan Bank untuk menjaga rahasia akun bank juga adalah dengan Bank tidak akan memberikan informasi apapun apabila ada orang yang menanyakan identitas nasabah atau aktivitasnya di bank kecuali pihak- pihak yang telah diberi kuasa atau wewenang untuk meminta informasi tersebut sebagaimana yang telah ditentukan dalam UU. No. 10 Tahun 1999 mengenai perbankan, yang didalamnya dijelaskan bahwa Kepolisian, Kejaksaan serta Pengadilan. Menghimbau bahwasannya nasabah harus lebih meningkatkan kewaspadaan juga ketelitian dalam menjaga keamanan informasi akun Bank seperti kode aktivasi, nomor PIN, nomor rekening serta nomor telepon, bahkan kepada staff Bank yang bersangkutan pun jangan memberikan informasi kepada siapapun termasuk pihak Bank

b. **Hindari Mengunduh Software Palsu**

Saat ini sudah banyak software dengan nama dan logo yang sama dengan perbankan asli di Playstore dan App Store. Sehingga orang tidak dapat membedakan aplikasi tersebut asli atau palsu. Oleh karena itu, Bank menghimbau nasabah untuk tidak mengunduh software palsu, 9 karena apabila terjadi pengunduhan nasabah pun akan dituntun mengisi data pribadi seperti kode aktivasi dan PIN. Kemudian data tersebut akan diolah dan disalahgunakan oleh pemilik software yang melakukan penipuan tersebut.

c. **Waspadai E-mail, SMS dan Telepon Mencurigakan**

Waspadai upaya penipuan dari oknum yang mengatasnamakan petugas bank melalui telepon, sms atau e-mail yang meminta informasi pribadi atau mengharuskan untuk mentransfer sejumlah uang tanpa alasan yang realistis. Cek dulu identitas pengirim. Biasanya akan ada beberapa pihak yang menyamar sebagai instansi bank lalu meminta nasabah mengunjungi link atau website tertentu untuk memperbaharui informasi rekening nasabah. Bila terjadi hal seperti ini, sebaiknya lakukan konfirmasi terlebih dahulu pada bank yang bersangkutan. Nasabah dihimbau untuk secepatnya menutup telepon serta melakukan pengecekan informasi yang diterima jika menelepon mengabarkan bahwa nasabah sebagai pemenang iklan tertentu (Nurdin dkk, 2020). Biasanya, sandiwara yang dilakukan oleh penelpon yang berniat menipu nasabah yaitu, menelepon mengabarkan keluarga nasabah mendapatkan musibah, maka pada saat itu nasabah dihimbau jangan dahulu panik dan mengikuti perintah menelepon. Tanyakanlah perihal identitas serta lakukan pengecekan.

d. **Hubungi Customer Service**

Bank Ketika semua cara telah dilakukan, akan tetapi masih ada kejanggalan pada akun rekening bank, maka nasabah harus menelpon atau mendatangi customer service bank yang bersangkutan.

e. Konfirmasi Penerima Uang dan Rutin Mengecek Rekening

Setelah melakukan transfer sebaiknya nasabah segera menghubungi si penerima uang dan mengkonfirmasi apakah uang telah diterima di rekening penerima. Selanjutnya secara berkala rutin mengecek rekening sehingga bila ada transaksi yang aneh dapat dilaporkan ke pihak bank secepatnya.

KESIMPULAN

Perkembangan teknologi digital dalam industri perbankan telah mengubah cara transaksi keuangan dilakukan, salah satunya melalui mobile banking. Bank DBS Indonesia telah mengadopsi teknologi ini melalui aplikasi digibank, yang memberikan kemudahan bagi nasabah dalam melakukan transaksi kapan saja dan di mana saja. Namun, meskipun mobile banking menawarkan berbagai manfaat, terdapat sejumlah tantangan dan risiko yang dihadapi oleh perbankan serta nasabah. Salah satu tantangan terbesar dalam penggunaan mobile banking adalah keamanan siber. Banyak nasabah masih merasa khawatir dengan risiko penipuan, pencurian data, serta penyalahgunaan informasi pribadi. Kejahatan siber yang semakin canggih, seperti phishing, malware, dan pencurian identitas, menjadi ancaman yang dapat menyebabkan hilangnya kepercayaan nasabah terhadap layanan mobile banking. Hal ini mengakibatkan nasabah lebih sering menggunakan mobile banking untuk mengecek informasi saldo dibandingkan melakukan transaksi finansial. Bank DBS Indonesia telah menerapkan berbagai kebijakan dalam manajemen risiko, termasuk melalui Risk Management Group (RMG) yang berfokus pada pengelolaan risiko kredit, pasar, likuiditas, dan operasional.

Kepercayaan nasabah terhadap mobile banking dapat menurun jika mereka mengalami kasus penipuan yang mengatasnamakan bank. Beberapa modus penipuan yang sering terjadi melibatkan panggilan telepon, email, atau SMS palsu yang meminta informasi pribadi nasabah. Kurangnya pemahaman nasabah terhadap ancaman ini dapat meningkatkan risiko kehilangan dana akibat serangan siber. Di sisi lain, DBS Indonesia telah menerapkan sejumlah langkah strategis untuk meningkatkan keamanan mobile banking, seperti penerapan otentikasi multi-faktor, enkripsi data, dan sistem deteksi penipuan yang lebih ketat. Bank juga menyediakan layanan pelanggan yang dapat membantu nasabah dalam menangani permasalahan terkait keamanan. Namun, efektivitas kebijakan ini masih perlu ditingkatkan agar dapat memberikan perlindungan maksimal bagi nasabah. Secara keseluruhan, meskipun mobile banking membawa berbagai kemudahan bagi nasabah, tingkat adopsinya masih menghadapi hambatan karena kekhawatiran terhadap keamanan dan kepercayaan terhadap sistem yang ada. Oleh karena itu, perlu adanya strategi yang lebih komprehensif untuk meningkatkan keamanan, edukasi, dan transparansi dalam layanan mobile banking.

Rekomendasi

1. Peningkatan Keamanan Digital: DBS Indonesia perlu terus berinvestasi dalam teknologi terbaru untuk meningkatkan keamanan mobile banking, seperti enkripsi data, otentikasi multi-faktor, dan sistem deteksi penipuan yang lebih canggih.
2. Edukasi Nasabah: Bank perlu meningkatkan literasi digital bagi nasabah dengan menyediakan edukasi yang jelas mengenai cara menggunakan aplikasi dengan aman serta cara mengidentifikasi potensi penipuan.
3. Peningkatan Kepercayaan Nasabah: Untuk mengatasi penurunan kepercayaan, perlu ada transparansi dan kebijakan yang lebih ketat dalam menangani keluhan nasabah terkait penipuan, dengan memberikan respons cepat terhadap masalah yang dihadapi nasabah.
4. Mitigasi Risiko Kejahatan Siber: Nasabah juga dihimbau untuk menjaga kerahasiaan

data pribadi mereka dan menghindari aplikasi palsu yang dapat merugikan mereka. Pihak bank harus terus mengingatkan nasabah tentang pentingnya kewaspadaan terhadap tindak penipuan yang sering terjadi melalui berbagai saluran komunikasi.

DAFTAR PUSTAKA

- A.K. Singh dan S. K. Singh, 2015. “Keamanan dan Privasi dalam Penggunaan Mobile Banking” oleh Journal of Information Security and Applications, Vol. 20,
- Ciawi Indah, Yusrizal. 2019. FINANCIAL RATIO ANALYSIS TO ASSESS THE FINANCIAL PERFORMANCE OF PT. BANK DBS INDONESIA PERIODE 2010– 2017. Bilancia: Jurnal Ilmiah Akuntansi. Vol. 3 No. 3, hal. 302-312
- Davis, F.D. (1989). Perceived usefulness, perceived ease of use, and user acceptance of information technology. MIS quarterly, 319-340.
- Oktaviani Sukma, Nuhbatul Basyariah. 2022. Analisis Manajemen Risiko Layanan Mobile Banking Pada Bank Syariah. Jurnal Manajemen dan Penelitian Akuntansi (JUMPA). Vol. 15, No. 1, 29-34.
- Parasuraman, A. Zeithaml, V. A., & Berry, L. L. (1988). SERVQUAL: A multiple-item scale for measuring customer perceptions of service quality. Journal of Retailing, 64(1), 12-40.
- PRASETYO YUNAN DWI. 2024. STRATEGI PENERAPAN MANAJEMEN RISIKO UNTUK MENCEGAH KEJAHATAN SIBER DI MOBILE BANKING PADA BANK PEMBANGUNAN DAERAH YOGYAKARTA KANTOR CABANG SYARIAH
- R. A. Sutanto dan E. Y. Setiawan, 2011, “Analisis Risiko Penggunaan Mobile Banking pada Bank di Asia” Journal of Banking and Finance, Vol. 35, No. 10
- S. W. Lee dan H. S. Kim, 2015. Manajemen Risiko dalam Penggunaan Mobile Banking” oleh S. W. Lee dan H. S. Kim, Journal of Risk Management, Vol. 12, No. 2
- Siregar Hotnaida, Juharati Dinia, Retno Septiani. 2021. ANALISIS MANAJEMEN RISIKO TERHADAP PENGGUNAAN E-BANKING (MOBILE BANKING DAN INTERNET BANKING) PADA BANK BNI SYARIAH. Jurnal Manajemen Bisnis. Vol. 10 I No.2, hal 187-192.