PENGARUH ANCAMAN SIBER DAN STRATEGI MITIGASI RISIKO TERHADAP KEPERCAYAAN NASABAH BANK SYARIAH INDONESIA

SKRIPSI

Diajukan Untuk Memenuhi Syarat -Syarat
Guna Memperoleh Gelar Sarjana (S.1)
Pada Program Studi Perbankan Syariah

DISUSUN OLEH:

DELA SARI

NIM: 21631016

PROGRAM STUDI PERBANKAN SYARIAH

FAKULTAS SYARIAH DAN EKONOMI ISLAM

INSTITUT AGAMA ISLAM NEGERI (IAIN) CURUP

2025

Hal: Pengajuan Skripsi

Kepada

Yth. Dekan Fakultas Syariah dan Ekonomi Islam

Di Tempat

Assalammualaikum Wr. Wb

Setelah mengadakan pemeriksaan dan perbaikan seperlunya, maka kami berpendapat bahwa skripsi saudari Dela Sari mahasiswi IAIN yang berjudul ***"Pengaruh Ancaman Siber dan Strategi Mitigasi Risiko Terhadap Kepercayaan Nasabah Bank Syariah Indonesia"*** sudah dapat diajukan dalam siding Munaqasyah Di Institut Agama Islam Negeri (IAIN) Curup.

Demikian permohonan ini kami ajukan dan atas perhatiannya kami ucapkan terimakasih.

Wassalammualaikum Wr. Wb

Curup, 7 Juli 2025

Pembimbing I	Pembimbing II
Noprizal, M.Ag	Dr. Hendrianto, M.A
NIP.19771105 200901 1 007	NIP.19870621 202321 1 022

PERNYATAAN BEBAS PLAGIASI

Yang bertanda tangan dibawah ini:

Nama	: Dela Sari
Nomor Induk Mahasiswa	: 21631016
Fakultas	: Syari'ah dan Ekonomi Islam
Program Studi	: Perbankan Syari'ah
Judul Skripsi	: Pengaruh Ancaman Siber dan Strategi Mitigasi Risiko Terhadap Kepercayaan Nasabah Bank Syari'ah Indonesia

Dengan ini menyatakan bahwa skripsi ini bukan merupakan karya yang pernah diajukan oleh orang lain untuk memperoleh gelar kesarjanaan disuatu perguruan tinggi dan sepanjang pengetahuan penulis juga tidak terdapat karya atau pendapat yang pernah ditulis atau diterbitkan oleh orang lain, kecuali secara tertulis diajukan untuk dirujuk dalam naskah ini dan disebutkan dalam referensi. Apabila kemudian hari terbukti bahwa pernyataan ini tidak benar, saya bersedia menerima hukuman atau sanksi sesuai peraturan yang berlaku. Demikian pernyataan ini saya buat dengan sebenarnya, semoga dapat dipergunakan seperlunya.

Curup, Juli 2025

Dela Sari

21631016

KEMENTERIAN AGAMA REPUBLIK INDONESIA
INSTITUT AGAMA ISLAM NEGERI (IAIN) CURUP
FAKULTAS SYARIAH DAN EKONOMI ISLAM
Jalan : Dr. AK Gani No. 01 PO 108 Tlp (0732) 21010 -21759 Fax 21010 Curup 39119
Website facebook. Fakultas Syariah dan Ekonomi Islam IAIN Curup Email: Fakultassyariah&ekonomi islam@gmail.com

PENGESAHAN SKRIPSI MAHASISWA

Nomor: 510 /In.34/FS/PP.00.9/02/2025

Nama	:	**Dela Sari**
NIM	:	**21631016**
Fakultas	:	**Syariah dan Ekonomi Islam**
Prodi	:	**Perbankan Syariah**
Judul	:	**Pengaruh Ancaman Siber Dan Strategi Mitigasi Risiko Terhadap Kepercayaan Nasabah Bank Syariah Indonesia**

Telah di munaqasahkan dalam sidang terbuka Institut Agama Islam Negeri (IAIN) Curup, pada :

Hari/ Tanggal	:	**Rabu, 20 Agustus 2025**
Pukul	:	**13.30 – 15.00 WIB**
Tempat	:	**Ruang 3 Gedung Fakultas Syariah dan Ekonomi Islam IAIN Curup**

Dan telah diterima untuk melengkapi sebagai syarat-syarat guna memperoleh gelar Sarjana Ekonomi (S.E) dalam Bidang Ilmu Perbankan Syariah.

TIM PENGUJI

Ketua,	Sekretaris,
Dr. H.M.Abu Dzar, Lc, M.H.I	**Sidiq Aulia, S.H.I., M.H.I**
NIP. 198110162009121001	**NIP. 198804122020121004**

Penguji I	Penguji II
Topan Alparedi, S.E., M.M	**Sineba Arli Silvia, S.E.I., M.E**
NIP. 198812202020121004	**NIP. 199105192023212037**

Mengesahkan
Dekan, Fakultas Syariah dan Ekonomi Islam

Dr. Ngadri, M.Ag
NIP. 196902061995031001

KATA PENGANTAR

بِسْمِ اللَّهِ الرَّحْمَٰنِ الرَّحِيمِ

Alhamdulillah hirobbil aalamiin. Puji dan syukur kehadirat Allah SWT yang telah melimpahkan rahmat dan karunia-Nya sehingga peneliti dapat menyelesaikan skripsi ini dengan baik. Sholawat dan salam semoga senantiasa tercurah kepada nabi Muhammad SAW, karena berkat beliau kita masih bisa merasakan zaman yang penuh dengan ilmu pengetahuan.

Adapun skripsi ini berjudul **"Pengaruh Ancaman Siber dan Strategi Mitigasi Risiko Terhadap Kepercayaan Nasabah Bank Syariah Indonesia"** yang disusun dalam rangka memenuhi salah satu syarat dalam menyelesaikan studi tingkat Sarjana (S.1) pada Program Studi Perbankan Syariah Fakultas Syariah dan Ekonomi Islam, Institut Agama Islam Negeri Curup (IAIN) Curup.

Peneliti menyadari sepenuhnya bahwa tanpa ada dorongan dan bantuan berbagai pihak, maka tidak mungkin terselesainya skripsi ini sehingga skripsi ini bukan semata-mata hasil usaha sendiri. Untuk itu dalam kesempatan ini peneliti ingin menyampaikan ucapan terima kasih yang sebesar-besarnya kepada semua pihak yang memberikan saran dalam menyelesaikan skripsi ini terutama kepada :

1. Prof. Dr. Idi Warsah, M.Pd.I, selaku Rektor Institut Agama Islam Negeri (IAIN) Curup.
2. Dr. Ngadri, M. Ag, selaku Dekan Fakultas Syariah dan Ekonomi Islam.
3. Ranas Wijaya, M.E, selaku Ketua Program Studi Perbankan Syariah.

4. Khairul Umam Khudori, M.E.I, selaku pembimbing akademik yang selalu bersedia memberikan nasehat khususnya dalam proses akademik peneliti.
5. Noprizal, M.Ag, dan Dr. Hendrianto, M.A, selaku Dosen Pembimbing I dan II, yang telah membimbing serta mengarahkan peneliti, terima kasih atas dukungan, doa, waktu dan motivasi sehingga peneliti dapat menyelesaikan skripsi ini.
6. Kepala Perpustakaan IAIN Curup beserta seluruh karyawan, yang telah mengarahkan dan memberi kemudahan kepada peneliti dalam memperoleh referensi dan data-data dalam penyusunan skripsi ini.
7. Seluruh Dosen Fakultas Syariah dan Ekonomi Islam dan Karyawan IAIN Curup yang telah memberikan petunjuk dan bimbingan kepada peneliti selama berada dibangku kuliah.
8. Terima kasih kepada Wakil Rektor III Bapak Nelson, M.Pd.I, selaku Pembina Forum Mahasiswa Bidikmisi, seluruh mahasiswa KIP-K Angkatan 2022-2023 yang terlibat dalam penelitian ini, dimana telah banyak membantu dan meluangkan waktu untuk memberikan informasi, data yang peneliti butuhkan dalam menyelesaikan skripsi ini.
9. Teman-teman seperjuangan Prodi Perbankan Syariah angkatan 2021 yang tak bisa disebutkan satu per satu, terima kasih atas dukungan dan doa-doa baiknya.
10. Semua pihak yang telah membantu dalam menyelesaikan skripsi ini yang tidak dapat peneliti sebutkan satu persatu.

Peneliti juga sangat mengharapkan saran dan kritik yang bersifat membangun terutama dari para pembaca dan dosen pembimbing. Mungkin dalam penyusunan skripsi ini masih terdapat kesalahan dan kekurangan. Atas saran dan kritik dari pembaca dan dosen pembimbing, peneliti mengucapkan terima kasih dan semoga skripsi ini dapat bermanfaat serta menambah ilmu pengetahuan peneliti dan pembaca. Aamiin Ya Robbal'Aalamiin.

Curup, 2 Juli 2025
Peneliti

Dela Sari
NIM.21631016

MOTTO

اَللَّهُمَّ يَسِّرْ وَ لَا تُعَسِّرْ

"Ya Allah, Mudahkanlah, bantulah, dan janganlah Engkau persulit."

"Apa yang kamu anggap sebagai keterlambatan, bisa jadi cara Tuhan untuk menyelamatkanmu dari sesuatu yang belum siap kamu hadapi"

"Skripsi yang baik adalah skripsi yang selesai"

(Dela Sari)

PERSEMBAHAN

Puji dan syukur peneliti panjatkan kepada Allah SWT, yang telah memberikan kesehatan, rahmat serta hidayah-Nya, sehingga peneliti masih diberi kesempatan untuk bisa menyelesaikan skripsi ini. Meskipun masih jauh dari kata sempurna, peneliti merasa bangga bisa sampai pada titik ini. Skripsi ini saya persembahkan kepada :

1. Cinta pertama dan panutanku, Ayahanda Saimin (Alm). Beliau memang sudah tidak bisa lagi dipeluk raganya, namun perjuangan, nasehat, doa, serta dukungan yang telah beliau berikan kepada peneliti selama ini sangat berarti. Terima kasih telah mengajarkan banyak pelajaran hidup kepada peneliti sehingga peneliti mampu bertahan sampai dititik ini.
2. Pintu surgaku, Ibunda Kasmiatun. Terima kasih atas segala bentuk bantuan, nasihat, semangat dan doa yang diberikan selama ini. Terima kasih karena selalu sabar menunggu peneliti berproses, memberikan segala bentuk cinta dan dukungan serta semangat yang tiada henti sehingga peneliti dapat menyelesaikan semuanya dengan baik.
3. Saudaraku tercinta dan tersayang, Dewi Lestari, S.S, Terima kasih karena sudah berperan besar dalam proses peneliti menempuh pendidikan selama ini. Terima kasih atas semua bentuk bantuan, nasehat, semangat dan doa yang diberikan selama ini. Apapun itu, semoga bisa membuatmu bangga.
4. Kepada seseorang yang bernama Aji Pangestu. Terima kasih atas semua bentuk bantuan, doa dan semangat yang telah diberikan kepada peneliti selama menempuh pendidikan selama ini. Terima kasih telah bersedia menemani,

menghibur, dan memberikan *support* terbaiknya kepada peneliti hingga sampai pada titik ini, *you are precious*.

5. Kepada seseorang yang ada didalam proses penyelesaian tugas akhir ini, Deri Sukarianti, Esa Julita, S.E, Fitri Ananda, S.E, Icu Ayu, S.Pd, Najwa Rani, Metha Putri, S.Pd, Asmaul Fatanah, S.Pd, Sindi Apriyani, S.Pd, Delima, Rara, Tria, Wenda, Rahma, Lastriana Sutarni, S.H, Harum, Silvia, Jamiatul Karamah, S.Pd, Deska Purnama, S.Pd, terima kasih telah memberikan *support* kepada peneliti dalam menyelesaikan tugas akhir ini. Terima kasih telah menjadi rumah di tanah rantauan ini. *See you on stop, guys!!*
6. Terima kasih juga peneliti sampaikan kepada keluarga besar Ma'had Al Jamiah IAIN Curup, atas bimbingan serta arahannya selama peneliti tinggal di asrama.
7. Terakhir, terima kasih untuk diri sendiri, Dela Sari, sosok gadis kecil yang berjuang tanpa henti dibalik layar. Perjuangannya jarang ada yang mengapresiasi, setiap langkahnya berat namun semangat dan tekadnya besar setiap harinya. Terima kasih karena telah mampu berusaha keras dan berjuang sejauh ini. Terima kasih telah bertahan dan menyelesaikan semuanya dengan baik dan tepat waktu. Mampu mengendalikan diri dari berbagai tekanan diluar keadaan dan tidak pernah memutuskan untuk menyerah sesulit apapun proses penyusunan skripsi ini, ini merupakan pencapaian yang patut dibanggakan untuk diri sendiri. Semua perjuangan 4 tahun dalam menempuh Pendidikan ini dibayar lunas dengan selesainya skripsi ini. *You did it* del!

ABSTRAK

Dela Sari NIM. 21631016 **"Pengaruh Ancaman Siber dan Strategi Mitigasi Risiko Terhadap Kepercayaan Nasabah Bank Syariah Indonesia"** Skripsi, Program Studi Perbankan Syariah.

Ancaman siber menjadi salah satu tantangan serius di era digital yang berdampak langsung pada tingkat kepercayaan nasabah, khususnya di sektor perbankan syariah. Penelitian ini bertujuan untuk mengetahui pengaruh ancaman siber (X1) dan strategi mitigasi risiko (X2) terhadap kepercayaan nasabah (Y) Bank Syariah Indonesia (BSI). Metode penelitian yang digunakan adalah metode kuantitatif asosiatif dengan teknik purposive sampling. Populasi penelitian adalah mahasiswa penerima Kartu Indonesia Pintar Kuliah (KIP-K) di IAIN Curup yang menjadi nasabah aktif BSI, dengan jumlah sampel sebanyak 187 responden. Data dikumpulkan melalui kuesioner dan dianalisis menggunakan alat bantu SPSS versi 26.

Hasil penelitian menunjukkan bahwa secara parsial ancaman siber (X1) dengan nilai t hitung sebesar 1,310 < t tabel 1,973 dan signifikansi 0,192 > 0,05 tidak berpengaruh signifikan terhadap kepercayaan nasabah. Strategi mitigasi risiko (X2) juga memiliki nilai t hitung -0,905 < t tabel 1,973 dengan signifikansi 0,367 > 0,05, sehingga tidak berpengaruh signifikan terhadap kepercayaan nasabah. Secara simultan, nilai f hitung sebesar 1,409 < f tabel 3,05 dengan signifikansi 0,247 > 0,05 menunjukkan bahwa ancaman siber dan strategi mitigasi risiko tidak berpengaruh signifikan secara bersama-sama terhadap kepercayaan nasabah. Koefisien determinasi (R^2) sebesar 0,004 mengindikasikan bahwa variabel independen hanya memengaruhi kepercayaan nasabah sebesar 0,4%, sedangkan sisanya dipengaruhi oleh faktor lain yang tidak diteliti.

Kata kunci*:* *Ancaman Siber, Strategi Mitigasi Risiko, Kepercayaan Nasabah, Bank Syariah Indonesia.*

DAFTAR ISI

DAFTAR GAMBAR

DAFTAR GRAFIK

DAFTAR TABEL

BAB I

PENDAHULUAN

A. Latar Belakang

Perkembangan teknologi informasi dan digitalisasi layanan telah memberikan berbagai kemudahan serta efisiensi dalam sektor perbankan. Namun di balik kemajuan ini, terdapat tantangan besar yang harus dihadapi, salah satunya adalah ancaman siber. Di era digital saat ini, bank tidak hanya dituntut untuk menyediakan layanan yang cepat dan praktis, tetapi juga harus memastikan keamanan informasi serta transaksi para nasabahnya. Ancaman siber telah menjadi isu global yang terus meningkat baik dalam kompleksitas, frekuensi, maupun dampaknya. Menurut laporan dari *Cybersecurity Ventures*, kerugian global akibat serangan siber diperkirakan mencapai $6 triliun pada tahun 2021, dan angka ini diprediksi akan terus meningkat setiap tahunnya seiring dengan evolusi metode serangan yang semakin canggih dan terorganisir.[1]

Seiring dengan meningkatnya ancaman siber di sektor perbankan, Bank Syariah Indonesia (BSI) mengalami tekanan yang signifikan dalam menjaga kepercayaan nasabah. Berdasarkan laporan resmi Badan Siber dan Sandi Negara (BSSN), insiden serangan siber nasional mengalami peningkatan yang konsisten setiap tahunnya, seperti ditunjukkan pada tabel berikut:

[1] Rian Dwi Hapsari, "Ancaman Cybercrime di Indonesia: Sebuah Tinjauan Pustaka Sistematis," *Jurnal Konstituen* 5, no. 1 (2023): 1–17

Tabel 1.1

Statistik Digitalisasi, Insiden Siber, dan Kepercayaan Nasabah BSI (2021–2024)

Tahun	Nasabah Digital (juta)	Pengguna BSI Mobile (juta)	Total Transaksi Digital (triliun)	Jumlah Insiden Siber	Rata-rata Kepuasan/ Kepercayaan Nasabah (%)
2021	11,3	7,5	122,5	12	83%
2022	14,7	9,8	187,3	23	80%
2023	17,1	11,2	265,0	36	74%
2024	19,3	13,6	328,7 (proyeksi)	18 (hingga April 2024	77% (pulih pasca *ransomware*)

Sumber: Otoritas Jasa Keuangan, diakses 25 Mei 2025

Perkembangan teknologi digital dalam sektor perbankan syariah mengalami pertumbuhan signifikan dalam beberapa tahun terakhir. Bank Syariah Indonesia (BSI), sebagai entitas terbesar di industri ini, menjadi garda terdepan dalam transformasi layanan digital syariah. Hal ini tercermin dari peningkatan jumlah nasabah digital dan pengguna aplikasi BSI *Mobile* secara konsisten dari tahun 2021 hingga 2024. Total transaksi digital BSI pun melonjak dari Rp122,5 triliun pada tahun 2021 menjadi lebih dari Rp328 triliun pada awal 2024. Peningkatan ini menunjukkan bahwa digitalisasi telah menjadi tulang punggung pelayanan BSI dalam menjangkau nasabah di seluruh indonesia.[2]

[2] Otoritas Jasa Keuangan (OJK), Data Statistik Perbankan Syariah dan Laporan Industri Triwulan I 2024, diakses 25 Mei 2025, https://www.ojk.go.id.

Namun, pertumbuhan ini juga dibayangi oleh meningkatnya kerentanan terhadap serangan siber. Pada tahun 2023, BSI menghadapi salah satu insiden siber terbesar dalam sejarah perbankan syariah indonesia, yaitu serangan *ransomware* yang berdampak pada kelumpuhan layanan digital selama beberapa hari. Jumlah insiden siber yang tercatat meningkat tajam dari 12 kasus pada 2021 menjadi 36 kasus pada 2023. Dampak dari serangan ini tidak hanya bersifat teknis tetapi juga memengaruhi psikologis dan persepsi keamanan nasabah, yang tercermin dari penurunan rata-rata kepuasan dan kepercayaan nasabah dari 83% (2021) menjadi 74% (2023).[3]

Upaya pemulihan dilakukan secara intensif sepanjang tahun 2024, termasuk peningkatan sistem keamanan, pelatihan keamanan siber internal, dan edukasi nasabah mengenai literasi digital. Hasilnya, kepercayaan nasabah mulai menunjukkan tren positif, dengan nilai kepuasan yang meningkat menjadi 77% pada kuartal pertama 2024. Jumlah insiden yang terdeteksi pun berkurang signifikan menjadi 18 kasus hingga April 2024.

Berdasarkan catatan Badan Siber dan Sandi Negara (BSSN), dalam enam bulan pertama tahun 2023 saja, terdapat lebih dari 176 juta insiden siber, meningkat tajam dari tahun-tahun sebelumnya. Ancaman ini meliputi serangan *phishing, malware, ransomware*, serta serangan yang menargetkan sistem digital lembaga keuangan. Lembaga perbankan seperti Bank Syariah Indonesia (BSI), sebagai entitas yang menyimpan dan mengelola dana masyarakat serta data-data

[3] Bank Syariah Indonesia. *Laporan Tahunan Bank Syariah Indonesia 2021–2023*. (Jakarta: BSI Press, 2024) 34-36

pribadi, menjadi salah satu target utama dari para pelaku kejahatan siber. Ancaman siber yang berhasil menembus sistem keamanan perbankan dapat menimbulkan kerugian yang sangat besar, baik secara finansial maupun dalam bentuk kepercayaan masyarakat terhadap lembaga tersebut.[4]

Kepercayaan nasabah pada Bank Syariah Indonesia (BSI) menjadi aset fundamental yang perlu dipelihara secara berkelanjutan agar mendukung kinerja dan pertumbuhan bank. Kepercayaan nasabah dipengaruhi oleh dua hal utama, yaitu persepsi terhadap ancaman siber dan strategi mitigasi risiko yang diterapkan oleh pihak bank. Ancaman siber yang tidak ditangani dengan baik dapat mengurangi rasa aman nasabah dalam bertransaksi, sedangkan strategi mitigasi risiko yang kuat dapat meningkatkan keyakinan mereka bahwa data dan dana yang dimiliki terlindungi dengan optimal.[5]

Fenomena ancaman siber semakin meresahkan masyarakat, khususnya di sektor keuangan syariah yang mengandalkan kepercayaan sebagai pondasi layanan. Salah satu kasus besar terjadi pada Mei 2023, ketika Bank Syariah Indonesia (BSI) mengalami serangan siber yang menyebabkan gangguan layanan digital selama beberapa hari. Insiden ini menjadi perhatian nasional dan berdampak langsung terhadap persepsi nasabah mengenai keamanan data pribadi mereka. Gangguan tersebut juga dialami oleh sebagian mahasiswa

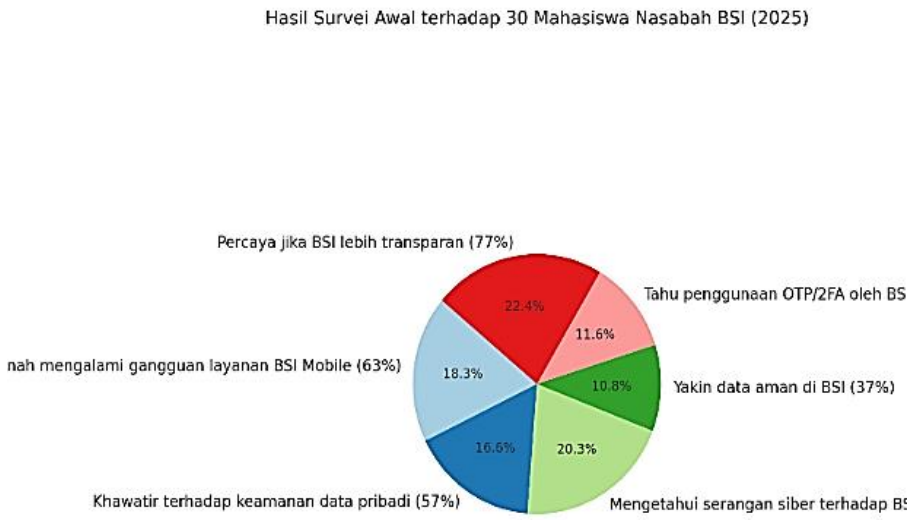
[4] Yusep Ginanjar, "Strategi Indonesia Membentuk Cyber Security dalam Menghadapi Ancaman Cyber Crime melalui Badan Siber dan Sandi Negara," *Dinamika Global: Jurnal Ilmu Hubungan Internasional* 7, no. 2 (2022): 291–312

[5] Tabina Dea Anindyaa, dkk "Edukasi Bahaya Social Engineering Menggunakan Media Belajar Quizizz untuk Meningkatkan Kesadaran Keamanan Informasi Nasabah Perbankan," JITTER: *Jurnal Ilmiah Teknologi dan Komputer* 4, no. 3 (2024): 2056–2069

penerima KIP-K di IAIN Curup yang merupakan nasabah aktif BSI, terutama pengguna layanan digital BSI Mobile.

Gambar 1.1

Rekapitulasi Hasil Survei Awal



Sumber: Data yang diolah, 2025

Sebagai bagian dari studi pendahuluan, penulis melakukan survei awal terhadap 30 mahasiswa IAIN Curup penerima KIP-K yang merupakan nasabah aktif Bank Syariah Indonesia (BSI). Hasil survei menunjukkan bahwa sekitar 63% responden mengaku pernah mengalami gangguan layanan saat menggunakan aplikasi BSI *Mobile*, seperti transaksi gagal, sistem yang lambat, atau saldo yang tidak sesuai. Selain itu, 57% responden menyatakan kekhawatiran terhadap keamanan data pribadi mereka, terutama setelah insiden serangan siber yang dialami BSI pada Mei 2023 diketahui publik.

Menariknya, meskipun sebagian besar responden mengetahui bahwa BSI pernah menjadi korban serangan digital (sekitar 70%), hanya sekitar 37% yang merasa yakin bahwa data mereka benar-benar aman saat menggunakan layanan BSI. Bahkan, kurang dari setengahnya mengetahui adanya strategi keamanan seperti autentikasi dua faktor (OTP/2FA) yang diterapkan oleh pihak bank. Namun demikian, mayoritas responden (77%) menyatakan bahwa mereka akan lebih percaya jika BSI bersikap lebih terbuka dan transparan terkait kebijakan keamanan digitalnya.

Selanjutnya, BSI telah mengklaim bahwa mereka telah menerapkan berbagai strategi mitigasi risiko siber, seperti pembaruan sistem keamanan, penerapan autentikasi ganda (*two-factor authentication*), serta pelatihan internal untuk meningkatkan kesadaran keamanan digital. Namun, efektivitas dari strategi tersebut masih dirasakan belum optimal oleh sebagian nasabah. Hal ini terlihat dari temuan bahwa hanya 41% responden merasa yakin bahwa data mereka aman bersama BSI, meskipun mereka tetap menggunakan layanan bank tersebut karena keterbatasan pilihan.

Berdasarkan landasan teoritis, penelitian ini berlandaskan pada Cybersecurity Risk Theory yang menekankan bahwa ancaman siber dapat menurunkan rasa aman nasabah sehingga berdampak pada menurunnya tingkat kepercayaan. Selain itu, *Enterprise Risk Management* (ERM) menjelaskan pentingnya strategi mitigasi risiko untuk mengurangi dampak serangan siber melalui langkah preventif, detektif, dan korektif. Dalam konteks perilaku nasabah, *Trust Theory* menegaskan bahwa kepercayaan terbentuk dari persepsi

terhadap keamanan, reliabilitas, serta transparansi lembaga keuangan. Teori perilaku lain seperti *Technology Acceptance Model* (TAM) dan *Theory of Planned Behavior* (TPB) juga mendukung bahwa kepercayaan nasabah terhadap layanan digital sangat dipengaruhi oleh persepsi keamanan dan efektivitas strategi mitigasi risiko. Secara empiris, Zamzami Akromi Lubis dan Fauzi Arif Lubis menemukan bahwa persepsi keamanan digital berpengaruh signifikan terhadap kepercayaan nasabah BSI.[6] Sementara penelitian Faridatul Khusnul Khotima membuktikan bahwa strategi mitigasi risiko siber mampu memperkuat kepercayaan terhadap layanan digital. [7]Selanjutnya, studi Lutfi Maulana dan Nadia Fitriana menunjukkan bahwa insiden siber BSI berdampak langsung pada turunnya kepercayaan nasabah, namun dapat dipulihkan melalui langkah mitigasi risiko yang tepat.[8] Bahkan, Restika dan Era Sonita menegaskan bahwa keamanan siber juga berkorelasi dengan stabilitas keuangan bank syariah, sehingga menjadi aspek fundamental dalam menjaga kepercayaan publik.[9] Berdasarkan temuan-temuan tersebut, dapat ditegaskan adanya celah penelitian, yaitu belum banyak kajian yang secara khusus menguji pengaruh ancaman siber dan strategi mitigasi risiko terhadap kepercayaan nasabah di sektor perbankan

[6] Zamzami Akromi Lubis dan Fauzi Arif Lubis, "Pengaruh Persepsi Keamanan dan Kepercayaan terhadap Loyalitas Nasabah: Studi Kasus Serangan Siber di Bank Syariah Indonesia,", *Jurnal Ekonomi Syariah* 5, no. 1 (2024): 50–53.

[7] Faridatul Khusnul Khotima, "Analisis Mitigasi Risiko Ancaman Siber Terhadap Sistem Layanan Digital Pada Masa Pandemi Covid-19 (Studi Pada Bank Perkreditan Rakyat Anugrah Dharma Yuwana Jember)" (Skripsi, Universitas Jember, 2022). 44-48

[8] Lutfi Maulana dan Nadia Fitriana, "Analisis Dampak Insiden BSI Error dan Dugaan Hacking Bank Syariah Indonesia (BSI) terhadap Kepercayaan dan Loyalitas Nasabah Bank Syariah Indonesia di Kabupaten Subang*", Jurnal Manajemen dan Bisnis* 15, no. 1 (2023): 20–25.

[9] Restika dan Era Sonita, "Tantangan Keamanan Siber dalam Manajemen Likuiditas Bank Syariah: Menjaga Stabilitas Keuangan di Era Digital", *Jurnal Ekonomi Islam* 14, no. 2 (2023): 49–52.

syariah, khususnya pada segmen mahasiswa di daerah seperti Curup yang memiliki tingkat literasi digital beragam. Oleh karena itu, penelitian ini penting untuk dilakukan guna mengisi kesenjangan teoritis dan praktis tersebut.

Situasi ini menegaskan pentingnya penelitian mengenai pengaruh ancaman siber dan strategi mitigasi risiko terhadap kepercayaan nasabah, khususnya dalam konteks perbankan syariah dan lingkungan akademik di daerah seperti Curup. Penelitian ini tidak hanya relevan secara akademik, tetapi juga memberikan kontribusi praktis bagi pengembangan kebijakan keamanan informasi yang adaptif dan berbasis kepercayaan publik.[10]

Oleh karena itu, penelitian ini dilakukan untuk mengidentifikasi dan menganalisis pengaruh ancaman siber serta strategi mitigasi risiko terhadap kepercayaan nasabah BSI, khususnya di kalangan mahasiswa IAIN Curup sebagai salah satu segmen pengguna layanan perbankan syariah yang aktif. Hasil dari penelitian ini diharapkan dapat memberikan kontribusi teoritis dan praktis dalam mengembangkan kepercayaan nasabah terhada system digital di sektor perbankan syariah. Maka dari itu, penulis memilih topik tersebut untuk dibahas, sehingga muncul judul " ***Pengaruh Ancaman Siber dan Strategi Mitigasi Risiko Terhadap Kepercayaan Nasabah Bank Syariah Indonesia***".

B. Identifikasi Masalah

Berdasarkan latar belakang yang telah dipaparkan, dapat diidentifikasi bahwa Bank Syariah Indonesia (BSI) menghadapi sejumlah permasalahan serius

[10] Sindy Ariyaningsi, dkk, "Korelasi Kejahatan Siber Dengan Percepatan Digitalisasi Di Indonesia", *Justisia: Jurnal Ilmu Hukum* 1 no. 1 (2023) 1-11

terkait ancaman siber dan pengaruhnya terhadap kepercayaan nasabah. Meningkatnya jumlah serangan siber yang menyasar sistem layanan keuangan digital BSI menunjukkan bahwa bank ini menjadi salah satu target utama serangan digital. Di sisi lain, tingkat literasi keamanan digital di kalangan nasabah masih tergolong rendah, sehingga banyak dari mereka menjadi sasaran empuk serangan seperti *phishing* dan rekayasa sosial (*social engineering*).

Namun demikian, strategi mitigasi risiko yang diterapkan oleh BSI belum sepenuhnya mampu merespons dinamika ancaman yang terus berkembang secara efektif. Hal ini turut berkontribusi pada fluktuasi tingkat kepercayaan nasabah terhadap sistem keamanan bank, terlebih setelah adanya beberapa insiden siber yang sempat mencoreng reputasi BSI. Ketidaksesuaian antara strategi mitigasi yang dijalankan dengan ekspektasi nasabah terhadap perlindungan data pribadi juga memperburuk situasi. Oleh karena itu, penting untuk menggali lebih dalam mengenai hubungan antara intensitas ancaman siber, efektivitas strategi mitigasi risiko, dan tingkat kepercayaan nasabah BSI secara menyeluruh.

C. Batasan Masalah

Objek penelitian dibatasi pada mahasiswa KIP-K IAIN Curup yang merupakan nasabah aktif BSI, sehingga temuan yang dihasilkan tidak dimaksudkan untuk digeneralisasikan pada nasabah BSI secara nasional. Penelitian ini tidak membahas secara teknis sistem keamanan digital secara mendalam, melainkan menitikberatkan pada persepsi nasabah terhadap ancaman

siber serta efektivitas strategi mitigasi risiko yang diterapkan oleh bank dalam membangun kepercayaan.

Berdasarkan batasan tersebut, penelitian diharapkan dapat memberikan gambaran yang lebih jelas, spesifik, dan terukur mengenai hubungan antara intensitas ancaman siber, strategi mitigasi risiko, dan kepercayaan nasabah dalam konteks perbankan syariah digital.

D. Rumusan Masalah

1. Apakah ancaman siber berpengaruh terhadap kepercayaan nasabah pada Bank Syariah Indonesia (BSI)?
2. Apakah strategi mitigasi risiko berpengaruh terhadap kepercayaan nasabah pada Bank Syariah Indonesia (BSI)?
3. Apakah ancaman siber dan strategi mitigasi risiko berpengaruh terhadap kepercayaan nasabah pada Bank Syariah Indonesia (BSI)?

E. Tujuan Penelitian

1. Untuk mengetahui pengaruh ancaman siber terhadap kepercayaan nasabah pada Bank Syariah Indonesia (BSI).
2. Untuk mengetahui pengaruh strategi mitigasi risiko terhadap kepercayaan nasabah pada Bank Syariah Indonesia (BSI).
3. Untuk mengetahui pengaruh simultan antara ancaman siber dan strategi mitigasi risiko terhadap kepercayaan nasabah pada Bank Syariah Indonesia (BSI).

F. Manfaat Penelitian

Penelitian ini diharapkan dapat memberikan beberapa manfaat, baik secara teoritis maupun praktis, yaitu:

1. Manfaat Secara Teoritis

Penelitian ini diharapkan dapat memberikan kontribusi terhadap pengembangan kajian ilmu manajemen risiko dan perbankan syariah, khususnya dalam memahami hubungan antara ancaman siber, strategi mitigasi risiko, dan kepercayaan nasabah. Hasil penelitian ini juga dapat menjadi referensi tambahan bagi peneliti selanjutnya yang ingin meneliti isu keamanan digital dan perilaku nasabah di sektor keuangan syariah.

2. Manfaat Secara Praktis

a. Bagi Bank Syariah Indonesia (BSI)

Penelitian ini dapat menjadi masukan bagi manajemen BSI dalam mengevaluasi efektivitas strategi mitigasi risiko siber yang telah diterapkan. Temuan dari penelitian ini dapat digunakan untuk meningkatkan sistem keamanan digital serta memperkuat kepercayaan nasabah, khususnya di kalangan mahasiswa yang merupakan pengguna aktif layanan digital banking.

b. Bagi Mahasiswa dan Nasabah BSI

Penelitian ini dapat meningkatkan kesadaran mahasiswa sebagai nasabah terhadap pentingnya keamanan informasi pribadi dalam transaksi perbankan. Selain itu, hasil penelitian ini juga dapat membantu nasabah

dalam menilai sejauh mana perlindungan yang diberikan oleh pihak bank terhadap data mereka.

c. Bagi Pemerintah dan Regulator Keuangan

Penelitian ini memberikan gambaran tentang urgensi perlindungan data nasabah dalam layanan keuangan digital, sehingga dapat menjadi bahan pertimbangan dalam penyusunan kebijakan dan regulasi yang lebih adaptif terhadap tantangan keamanan siber di era digital.

G. Tinjauan Kajian Terdahulu

Berdasarkan penelitian yang telah dilakukan seperti skripsi dan jurnal sebelumnya dengan tema yang hampir sama dengan penelitian yang akan dilakukan oleh penulis, diantaranya:

1. **Zamzami Akromi Lubis dan Fauzi Arif Lubis, Jurnal "Pengaruh Persepsi Keamanan dan Kepercayaan Terhadap Loyalitas Nasabah: Studi Kasus Serangan Siber di Bank Syariah Indonesia", Sumatera Utara, 2024.**

Latar belakang dari penelitian tersebut yaitu, industri perbankan islam di indonesia telah mengalami pertumbuhan yang signifikan dalam beberapa tahun terakhir, menjadi alternatif yang menarik bagi mereka yang ingin melakukan transaksi keuangan sesuai prinsip islam. Kepercayaan nasabah terhadap lembaga keuangan syariah penting karena mencerminkan keyakinan mereka terhadap kejujuran, transparansi, dan kepatuhan bank terhadap prinsip-prinsip islam. Namun, dengan meningkatnya penggunaan teknologi informasi di sektor perbankan, ancaman seperti serangan dunia maya telah

menjadi masalah serius yang dapat mempengaruhi persepsi nasabah terhadap keamanan dan privasi, serta kepercayaan mereka.

Tujuan dari penelitian yaitu, untuk menganalisis hubungan antara persepsi nasabah terhadap keamanan, kepercayaan dan loyalitas pada bank syariah indonesia dan memberikan informasi yang berguna bagi lembaga keuangan untuk meningkatkan kepercayaan dan loyalitas nasabah, kami bermaksud untuk membuat rekomendasi bagi lembaga keuangan syariah untuk meningkatkan keamanan dan membangun kepercayaan nasabah sehingga dapat meningkatkan loyalitas nasabah. bahwa mereka dapat meningkatkan loyalitas dan mendukung pengembangan lembaga keuangan islam. [11]

2. **Faridatul Khusnul Khotima, Skripsi "Analisis Mitigasi Risiko Ancaman Siber Terhadap Sistem Layanan Digital Pada Masa Pandemi Covid_19 (Studi Pada Bank Perkreditan Rakyat Anugrah Dharma Yuwana Jember), Jember, 2022.**

Penelitian ini dilatarbelakangi oleh meningkatnya penggunaan layanan digital di sektor perbankan, terutama di masa pandemi COVID-19. Dengan keterbatasan fisik dan kebutuhan beradaptasi dengan situasi baru, banyak bank, termasuk Bank Perkreditan Rakyat BPR ADY Jember, telah memilih layanan digital. Namun, evolusi ini juga membawa risiko baru, termasuk ancaman dunia maya, yang dapat membahayakan keamanan data

[11] Lubis dan Lubis, "Pengaruh Persepsi Keamanan dan Kepercayaan terhadap Loyalitas Nasabah," 51.

dan kepercayaan pelanggan. Oleh karena itu, penting untuk menganalisis dan memahami risiko ini dan bagaimana bank dapat memitigasinya untuk melindungi sistem layanan digital mereka.

Tujuannya yaitu, untuk mengidentifikasi dan menganalisis risiko ancaman siber yang dihadapi BPR ADY Jember dalam operasional layanan digital selama pandemi COVID-19. Mengembangkan strategi mitigasi yang efektif untuk mengurangi dampak risiko ini guna meningkatkan keamanan dan kepercayaan nasabah terhadap layanan digital yang disediakan oleh bank.[12]

3. **Lutfi Maulana dan Nadia Fitriana, Jurnal "Analisis dampak Insiden BSI Eror dan Dugaan *Hacking* Bank Syariah Indonesia (BSI) terhadap kepercayaan dan loyalitas nasabah Bank Syariah Indonesia di Kabupaten Subang, 2023.**

Kabupaten Subang, salah satu daerah ekonomi yang berkembang pesat, memiliki klien BSI yang beragam. Oleh karena itu, penting untuk memahami bagaimana insiden ini memengaruhi persepsi pelanggan di tingkat lokal. Studi ini bertujuan untuk mengisi kesenjangan pengetahuan mengenai dampak insiden tersebut. Rusaknya kepercayaan dan loyalitas nasabah serta memberikan informasi yang berguna bagi BSI dan lembaga keuangan islam lainnya untuk mengelola risiko dan membangun kembali citra positif mereka. Kejadian ini juga berdampak pada loyalitas pelanggan dengan dampak

[12] Khotima, "Analisis Mitigasi Risiko Ancaman Siber terhadap Sistem Layanan Digital," 46.

sebesar 356. Hilangnya kepercayaan dapat menyebabkan hilangnya loyalitas, yang dapat berdampak jangka panjang pada hubungan pelanggan-pelanggan. barang dan BSI. Hal ini menunjukkan bahwa insiden keamanan tidak hanya memengaruhi kepercayaan tetapi juga memainkan peran penting dalam menjaga loyalitas pelanggan.[13]

4. **Restika dan Era Sonita, Jurnal "Tantangan Keamanan Siber Dalam Manajemen Likuiditas Bank Syariah: Menjaga Stabilitas Keuangan Di Era Digital", Bukit Tinggi, 2023.**

Temuan studi ini memberikan wawasan tentang bagaimana bank islam dapat mengatasi dan menanggapi tantangan keamanan siber serta strategi yang dapat diterapkan untuk menjaga stabilitas. Pengambilan keputusan keuangan di era digital. Implikasi praktis dan rekomendasi untuk lembaga keuangan serupa juga dibahas. , berkontribusi pada pemahaman praktis dan kebijakan terkait manajemen likuiditas dan keamanan siber. Studi ini memberikan pemahaman yang lebih mendalam tentang hubungan antara keamanan siber dan stabilitas keuangan, menyediakan kerangka kerja yang diperlukan bagi bank syariah dan lembaga keuangan lainnya untuk mengatasi tantangan yang kompleks ini. Analisis ini menggarisbawahi kompleksitas tantangan keamanan siber yang dihadapi oleh bank syariah. Melibatkan berbagai aspek seperti teknologi, regulasi, dan kepatuhan syariah, penanganan tantangan ini memerlukan pendekatan holistik yang mencakup

[13] Maulana dan Fitriana, "Analisis Dampak Insiden BSI Error," 22.

pendidikan keamanan, kebijakan yang kuat, dan investasi dalam teknologi canggih untuk melindungi stabilitas keuangan dan kepercayaan nasabah.[14]

[14] Restika dan Era Sonita, "*Tantangan Keamanan Siber Dalam Manajemen Likuiditas Bank Syariah: Menjaga Stabilitas Keuangan di Era Digital*," Jurnal Ekonomi Islam (Bukittinggi, 2023). 30-35

BAB II

TINJAUAN PUSTAKA

A. Teori Terkait Dengan Variabel Penelitian

1. Ancaman Siber

Ancaman siber merupakan fenomena global yang semakin kompleks, di mana entitas digital, baik individu maupun organisasi, menjadi target berbagai bentuk serangan digital yang bersifat merusak, manipulatif, dan invasif. Ancaman siber dapat berasal dari dalam (*internal threat*) maupun luar organisasi (*external threat*), termasuk di antaranya *malware, ransomware, phishing,* serangan *distributed denial-of-service* (DDoS), hingga rekayasa sosial (*social engineering*) yang bertujuan mencuri data sensitif atau merusak reputasi institusi.[15]

Ancaman Siber dapat diartikan sebagai setiap jenis serangan yang dapat terjadi yang bertujuan untuk menggunakan kelemahan sistem informasi, seperti:

a. *Malware* adalah suatu pemrograman (kode, skrip, konten aktif, serta perangkat lunak lain) yang telah dirancang untuk mengganggu atau menyangkal operasi, mengumpulkan berbagai informasi yang mengarah pada musnahnya privasi atau eksploitasi, memperoleh akses tidak sah pada sumber daya sistem, serta perilaku kasar lainnya.

[15] Alhassan et al., "Cybersecurity Threats in the Banking Sector: A Review", *International Journal of Computer Applications* 975, no. 17 (2020): 1–7.

b. *Phishing* adalah penipuan online yang berusaha untuk mendapatkan informasi pribadi seperti kata sandi dan nomor kartu kredit.
c. *Ransomware* adalah serangan yang mengenkripsi data dan mengharuskan korban membayar tebusan untuk mendapatkan akses kembali.
d. dan serangan *denial-of-service* adalah serangan terhadap server atau jaringan dengan membanjiri lalu lintas, mengakibatkan akses kesitus web menjadi sangat lambat atau macet bahkan membuatnya tidak tersedia untuk pengguna yang sah.[16]

Sektor perbankan merupakan salah satu bidang yang paling rentan terhadap serangan siber, yang dapat berdampak besar pada kepercayaan masyarakat terhadap sistem keuangan dan stabilitas ekonomi. Studi dari Kshetri menunjukkan bahwa sektor keuangan menjadi target utama serangan karena tingginya nilai aset dan informasi yang dikelola.[17] Oleh karena itu, memahami karakteristik, bentuk, dan tujuan dari ancaman siber menjadi bagian penting dalam menyusun kebijakan keamanan informasi yang proaktif dan adaptif.

Ancaman siber tidak hanya berdampak secara teknis, tetapi juga menyentuh aspek psikologis dan kepercayaan nasabah. Ketika data nasabah mengalami kebocoran atau penyalahgunaan, hal ini dapat menyebabkan

[16] Budiyanto*, Pengantar Cybercrime Dalam Sistem Hukum Pidana di Indonesia* (Sada Kurnia Pustaka: Jakarta Press 2021), 22

[17] N. Kshetri, "Cybersecurity in the Financial Sector: A Global Perspective", *Journal of Financial Crime* 24, no. 4 (2022): 564–577

kepanikan, penarikan dana besar-besaran (*bank run*), serta kerusakan reputasi jangka panjang bagi institusi perbankan.

2. Strategi Mitigasi Risiko

Strategi mitigasi risiko merupakan proses menyeluruh yang dilakukan oleh organisasi untuk mengantisipasi berbagai potensi gangguan yang dapat menghambat pencapaian tujuan strategisnya. Dalam konteks ancaman siber, strategi mitigasi tidak hanya terbatas pada penerapan teknologi keamanan, tetapi juga mencakup aspek kebijakan, prosedur, pelatihan, dan budaya organisasi.[18]

Hillson menyatakan bahwa mitigasi risiko bukan hanya bentuk pertahanan, tetapi juga bagian dari upaya penciptaan nilai yang memungkinkan organisasi untuk lebih tanggap terhadap dinamika eksternal.[19]

Strategi mitigasi risiko mencakup berbagai tindakan seperti :

a. Penghindaran (*Avoid risk*) adalah pendekatan yang efektif dalam mengatasi risiko karena dapat menghilangkan risiko tersebut sepenuhnya. Beberapa langkah yang dapat diambil untuk mengurangi risiko ini antara lain mengurangi jumlah jalur kritis, memodifikasi pekerjaan untuk mengurangi ketergantungan aktivitas, menjadwalkan aktivitas dengan ketidakpastian tertinggi sejak awal, menghindari

[18] Hidayat, Muhammad Syahrul, "Risiko dan Mitigasi Digital" (Skripsi, UIN Sayyid Ali Rahmatullah, 2023), 75–77.

[19] David Hillson, "Perluasan Proses Manajemen Risiko dalam Rangka Pengelolaan Peluang", *International Journal of Project Management.* 20, no. 3 (2023): 235–240

anggota staff yang mengerjakan aktivitas kritis secara berurutan atau bersamaan, dan mengurangi aktivitas yang panjang menjadi lebih rinci.

b. Pengurangan risiko (*Mitigate risk*) adalah sesuatu strategi yang sangat penting untuk manajemen risiko, karena penghindaran dan pengalihan risiko tidak akan pernah dapat menangani setiap risiko proyek yang signifikan. Salah satu strategi pengurangan risiko yang penting dalam pengelolaan risiko proyek adalah meningkatkan komunikasi tim. Dengan menyadarkan tim tentang konsekuensi risiko yang mungkin terjadi mereka akan bekerja dengan cara yang meminimalkan risiko tersebut. Komunikasi yang efektif dapat secara signifikan mengurangi kemungkinan terjadinya risiko.
c. Pengalihan risiko (*Transfer risk*) adalah salah satu strategi dalam pengelolaan risiko. Dalam hal ini, pengalihan risiko mengacu pada transfer tanggungjawab finansial terhadap pihak lain. Contoh paling umum dari pengalihan risiko adalah melalui asuransi, dimana pembeli asuransi membayar premi untuk melindungi diri mereka dari risiko keuangan yang mungkin timbul.
d. Penerimaan risiko (*Keep risk*) adalah pendekatan yang digunakan dalam manajemen risiko untuk mengakui bahwa risiko tertentu tidak dapat dihindari atau dieliminasi. [20]

[20] Indah Mawarni, dkk, *Manajemen Risiko*, (Sumatera Barat: CV. Gita Lentera, 2024) 44

Strategi manajemen risiko dalam organisasi perbankan berkembang lebih lanjut menjadi *Enterprise Risk Management* (ERM), yang mengintegrasikan risiko teknologi informasi dengan risiko keuangan, hukum, operasional, dan reputasi. Pendekatan ini bertujuan untuk membentuk sistem pertahanan berlapis yang tidak hanya reaktif terhadap serangan, tetapi juga mampu memprediksi dan mencegah serangan secara dini melalui sistem pemantauan cerdas.

3. Kepercayaan Nasabah

Kepercayaan merupakan fondasi utama dalam hubungan antara lembaga keuangan dan nasabah. Tanpa kepercayaan, tidak akan tercipta loyalitas, keberlangsungan transaksi, maupun kestabilan institusi. Kepercayaan nasabah dalam konteks perbankan digital mencakup keyakinan bahwa sistem yang digunakan aman, bahwa data pribadi mereka dilindungi, dan bahwa layanan yang diberikan konsisten, responsif, dan sesuai dengan nilai-nilai hukum maupun moral.[21]

Teori yang dikemukakan oleh Mayer, Davis, dan Schoorman menjelaskan bahwa kepercayaan terbentuk dari tiga dimensi: kemampuan (*competence*), integritas (*integrity*), dan niat baik (*benevolence*).[22] Dalam layanan digital, dimensi ini diwujudkan melalui teknologi yang handal, komunikasi yang transparan, serta perlindungan terhadap hak-hak digital konsumen.

---

[21]Gupta, dkk "Impact of Cyber Security on Customer Trust in Banking Sector", *International Journal of Bank Marketing* 37, no. 5 (2021): 1123–1138

[22] Mayer, dkk, "An Integrative Model of Organizational Trust*", Academy of Management Review* 20, no. 3 (2020): 709–734

Berdasarkan teori trust, Moorman et al. mendefinisikan kepercayaan sebagai kesediaan untuk menyerahkan sesuatu kepada mitra yang dianggap dapat dipercaya. Penelitian Morgan dan Hunt sejalan dengan Moorman et al, mereka menemukan bahwa kepercayaan dan komitmen sangat mempengaruhi perilaku perusahaan dengan mitranya, sehingga dapat diperkirakan bahwa kepercayaan akan mempunyai hubungan yang positif dengan proses dependen berdasarkan contoh pengalaman yang relevan tetapi terbatas. Secara ringkas, kepercayaan adalah suatu harapan yang diharapkan. Sedangkan menurut Robbins, *trust* adalah suatu sejarah proses dependen didasarkan pada contoh pengalaman -pengalaman yang relevan namun terbatas.[23] Dapat diambil garis besar bahwa *trust* adalah suatu harapan yang positif dan relevan terhadap orang lain yang dapat menjadi *familiaritas* (kedekatan) serta ada unsur resiko.

Kepercayaan dalam dunia perbankan syariah, termasuk BSI, didukung oleh nilai-nilai spiritual yang menekankan prinsip amanah dan maslahah. Konsep amanah dalam islam, sebagaimana dijelaskan dalam QS An-Nisa ayat 58, menuntut lembaga untuk menjaga kepercayaan yang diberikan oleh nasabah sebagai tanggung jawab moral dan religius.[24] Oleh karena itu, kepercayaan dalam konteks ini tidak hanya diukur dari kepuasan nasabah secara rasional, tetapi juga dari persepsi nilai-nilai etik dan kesesuaian syariah yang dijalankan oleh bank.

[23] Danang Kusuma Bakti, "Studi Indigenous Trust to Leader pada Karyawan Jawa", (Skripsi: Universitas Negeri Semarang, 2022), 69

[24] Al-Qur'an, QS. An-Nisa [4]: 58 (Kementerian Agama Republik Indonesia, Mushaf Al-Qur'an Standar Indonesia, Jakarta: Lajnah Pentashihan Mushaf Al-Qur'an, 2019)

Pemilihan variabel dalam penelitian ini didasarkan pada relevansi fenomena yang terjadi di sektor perbankan syariah, khususnya Bank Syariah Indonesia (BSI), dengan tantangan keamanan digital yang semakin meningkat. Variabel Ancaman Siber (X1) dipilih karena serangan digital seperti *malware*, *phishing*, *ransomware*, dan DDoS terbukti mampu mengganggu sistem perbankan dan menurunkan tingkat kepercayaan nasabah. Variabel Strategi Mitigasi Risiko (X2) dipilih karena bank membutuhkan langkah antisipatif dan proaktif dalam menjaga stabilitas operasional serta perlindungan data nasabah. Sementara itu, variabel Kepercayaan Nasabah (Y) dipilih sebagai variabel dependen karena kepercayaan merupakan fondasi utama keberlangsungan bank syariah, yang menentukan loyalitas dan keberlanjutan hubungan antara nasabah dengan bank.

Oleh karena itu, hubungan antara ancaman siber, strategi mitigasi risiko, dan kepercayaan nasabah menjadi relevan untuk diteliti dalam rangka memberikan kontribusi pada penguatan sistem keamanan dan pelayanan BSI.

4. Bank Syariah Indonesia (BSI)

Bank Syariah Indonesia (BSI) merupakan institusi keuangan syariah terbesar di Indonesia, hasil penggabungan tiga bank syariah milik BUMN, yaitu BRI Syariah, BNI Syariah, dan Mandiri Syariah. Bank Syariah Indonesia, yang resmi berdiri pada 1 Februari 2021, merupakan hasil penggabungan beberapa bank syariah di Indonesia. Sejarah perbankan

syariah di Indonesia dimulai pada tahun 1992 dengan pendirian Bank Muamalat, yang menjadi bank syariah pertama di negara ini.[25] Sebagai bank yang mengusung prinsip-prinsip syariah, BSI memiliki tantangan ganda yaitu menjaga kepatuhan terhadap prinsip-prinsip islam dan sekaligus mengembangkan sistem perbankan digital yang modern, aman, dan terpercaya.

Seiring dengan berkembangnya era digitalisasi, BSI telah meluncurkan berbagai inovasi teknologi seperti *mobile banking*, integrasi sistem keuangan digital, serta layanan *cashless*. Namun, peningkatan layanan digital ini juga berbanding lurus dengan meningkatnya potensi risiko siber. Oleh karena itu, BSI aktif dalam mengembangkan strategi keamanan informasi yang komprehensif, termasuk membentuk *cybersecurity task force*, memperkuat sistem enkripsi, serta meningkatkan edukasi keamanan digital kepada nasabah.[26]

Penelitian yang dilakukan oleh Arif Lubis mengungkapkan bahwa kepercayaan nasabah terhadap BSI dapat terganggu akibat insiden serangan siber, namun penerapan mitigasi yang efektif dapat memulihkan kepercayaan tersebut. Hal ini menunjukkan pentingnya sinergi antara keamanan teknologi dan pendekatan etis syariah dalam membangun kembali kepercayaan publik.[27]

---

[25] Otoritas Jasa Keuangan (OJK), "*Sejarah Perbankan Syariah*," OJK, 50

[26] Agyekum & Alhassan, "Cybersecurity in Islamic Banking: A Review of the Literature", *Journal of Islamic Banking and Finance* 8, no. 1 (2020): 1–12.

[27] Lubis dan Lubis, "Pengaruh Persepsi Keamanan dan Kepercayaan terhadap Loyalitas Nasabah," 70

Penelitian ini didukung oleh beberapa teori yang menjadi dasar konseptual. Pertama, Teori Risiko (*Risk Management Theory*) yang menyatakan bahwa setiap organisasi menghadapi berbagai risiko yang harus diidentifikasi, dievaluasi, dan dimitigasi agar tidak mengganggu pencapaian tujuan strategis. Teori ini menjadi landasan dalam memahami variabel strategi mitigasi risiko. Kedua, Teori Kepercayaan (*Trust Theory*) yang dikemukakan oleh Mayer, Davis, dan Schoorman, yang menekankan bahwa kepercayaan dibangun melalui persepsi kemampuan, integritas, dan niat baik suatu pihak.[28] Teori ini relevan dalam mengukur kepercayaan nasabah terhadap BSI. Ketiga, Teori Sistem Informasi dan Keamanan Siber, yang menekankan pentingnya menjaga kerahasiaan, integritas, dan ketersediaan data dari berbagai ancaman digital. Teori ini mendasari pemilihan variabel ancaman siber sebagai faktor yang memengaruhi kepercayaan nasabah. Keempat, Teori Amanah dalam Islam, yang menjelaskan bahwa menjaga amanah merupakan kewajiban moral dan religius, sehingga perbankan syariah dituntut untuk menjaga titipan nasabah secara aman, transparan, dan sesuai syariat. Dengan memadukan teori manajemen risiko, teori kepercayaan, teori keamanan siber, dan teori amanah Islam, penelitian ini memiliki kerangka konseptual yang komprehensif dalam menjelaskan hubungan antar variabel penelitian.

[28] Roger dkk, "An Integrative Model of Organizational Trust," *Academy of Management Review* 20, no. 3 (1995): 709–734.

Setiap variabel dalam penelitian ini diturunkan ke dalam beberapa indikator yang merujuk pada teori dan hasil penelitian terdahulu. Variabel ancaman siber (X1) diukur melalui indikator seperti *malware*, *phishing*, *ransomware*, DDoS, dan *social engineering*. Variabel strategi mitigasi risiko (X2) diukur melalui indikator penghindaran risiko, pengurangan risiko, pengalihan risiko, penerimaan risiko, dan manajemen risiko terintegrasi. Sedangkan variabel kepercayaan nasabah (Y) diukur melalui indikator kompetensi, integritas, *benevolence*, kepuasan, dan amanah (*syariah compliance*). Rincian indikator tiap variabel dapat dilihat pada Tabel 2.1 berikut.

Tabel 2.1

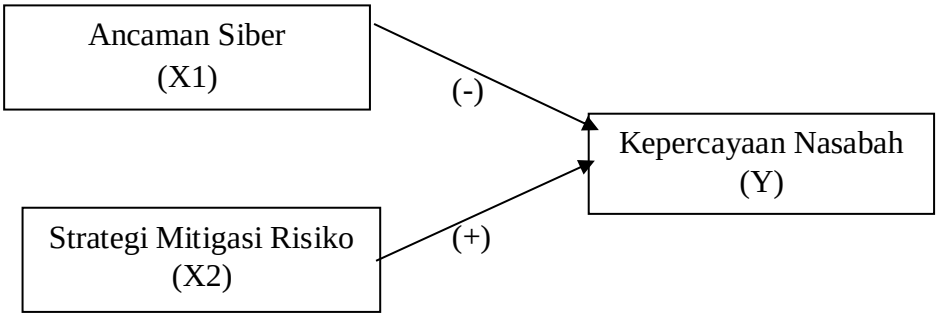
Indikator Penelitian

Variabel	**Definisi Teoritis**	**Indikator**	**Sumber**
Variabel Independen (X1)	Ancaman terhadap sistem digital berupa serangan yang merusak, manipulatif, dan mencuri data nasabah.	1. *Malware* (*virus, trojan*, dll.) 2. *Phishing* (penipuan data pribadi) 3. *Ransomware* (penguncian data untuk tebusan) 4. DDoS (serangan akses layanan) 5. *social engineering* (rekayasa sosial).	Alhassan (2020), Budiyanto (2025), Kshetri (2017)
Variabel Independen (X2)	Upaya organisasi untuk mengantisipasi dan mengurangi dampak risiko siber.	1. Penghindaran risiko (*avoidance*) 2. Pengurangan risiko (*mitigation*) 3. Pengalihan risiko (*transfer*)	Hillson (2002), Hidayat (2023), Indah Mawarni (2024)

		4. Penerimaan risiko (*acceptance*) 5. penerapan ERM dan penguatan sistem keamanan.	
Variabel Devenden (Y)	Keyakinan nasabah bahwa bank amanah, kompeten, dan melindungi data serta transaksi digital.	1. Kompetensi (keandalan sistem & teknologi) 2. Integritas (kejujuran & transparansi layanan) 3. *Benevolence* (niat baik bank terhadap nasabah) 4. Kepuasan & keyakinan nasabah dalam bertransaksi digital 5. kesesuaian syariah (amanah & nilai maslahah).	Mayer et al. (1995), Gupta (2019), QS An-Nisa:58

B. Kerangka Pemikiran

Kepercayaan nasabah merupakan aset penting bagi Bank Syariah Indonesia (BSI). Namun, kepercayaan tersebut dapat terganggu akibat adanya ancaman siber, seperti pencurian data, peretasan sistem, maupun gangguan layanan digital. Ancaman-ancaman ini dapat menurunkan rasa aman nasabah dalam bertransaksi.



Kerangka pemikiran penelitian ini menjelaskan bahwa kepercayaan nasabah (Y) dipengaruhi oleh dua variabel independen, yaitu ancaman siber (X1) dan strategi mitigasi risiko (X2).

Ancaman siber (X1) merupakan faktor eksternal yang dapat mengurangi rasa aman nasabah. Serangan atau ancaman terhadap sistem perbankan, seperti pencurian data, peretasan, maupun penyalahgunaan informasi, dapat menurunkan tingkat kepercayaan nasabah.

Sebaliknya, strategi mitigasi risiko (X2) merupakan langkah yang ditempuh oleh bank untuk mengantisipasi dan mengurangi dampak ancaman siber. Strategi ini meliputi penerapan teknologi keamanan, kebijakan perlindungan data, hingga prosedur penanganan insiden. Strategi mitigasi risiko yang efektif akan mampu meningkatkan kepercayaan nasabah, karena mereka merasa terlindungi dari potensi ancaman.

C. Hipotesis

Hipotesis adalah kesimpulan sementara yang mungkin belum terbukti kebenarannya dan merupakan kegiatan penelitian teoritis yang peneliti sebelum melakukan penelitian.

1. Pengaruh Ancaman Siber Terhadap Kepercayaan Nasabah

Kepercayaan nasabah merupakan salah satu faktor fundamental dalam membangun loyalitas pada lembaga perbankan. Menurut Mayer, Davis, dan Schoorman, kepercayaan terbentuk melalui keyakinan terhadap

integritas, kompetensi, dan niat baik suatu organisasi. Dalam konteks perbankan syariah, kepercayaan juga diperkuat oleh nilai-nilai spiritual yang menekankan amanah serta kepatuhan terhadap prinsip syariah, sehingga mendorong terciptanya loyalitas nasabah.[29]

Penelitian terdahulu yang dilakukan oleh Akromi Lubis, Zamzami, dan Fauzi Arif Lubis, menunjukkan bahwa kepercayaan berpengaruh signifikan terhadap loyalitas nasabah pada Bank Syariah Indonesia. Hasil penelitian tersebut memperkuat pandangan bahwa semakin tinggi tingkat kepercayaan nasabah, maka semakin besar pula kemungkinan nasabah untuk tetap loyal terhadap layanan perbankan syariah. Temuan ini sejalan dengan penelitian-penelitian sebelumnya yang menegaskan pentingnya membangun kepercayaan dalam meningkatkan loyalitas pelanggan pada sektor perbankan.[30]

Dengan merujuk pada penelitian tersebut, maka hipotesis dalam penelitian ini adalah:

H1 =Ancaman siber berpengaruh signifikan terhadap kepercayaan nasabah Bank Syariah Indonesia (BSI).

[29] Mayer, Davis, dan Schoorman, "An Integrative Model of Organizational Trust," 56
[30] Lubis dan Lubis, “Pengaruh Persepsi Keamanan dan Kepercayaan terhadap Loyalitas Nasabah,” 88

2. Pengaruh Strategi Mitigasi Risiko Terhadap Kepercayaan Nasabah

Mitigasi risiko merupakan bagian penting dari manajemen risiko yang bertujuan untuk meminimalisasi dampak negatif dari potensi ancaman yang dapat mengganggu keberlangsungan suatu usaha. Menurut Hillson, mitigasi risiko adalah strategi yang dirancang untuk mengurangi kemungkinan terjadinya risiko maupun dampak yang ditimbulkannya. Dengan penerapan mitigasi risiko yang tepat, organisasi atau pelaku usaha dapat meningkatkan kemampuan bertahan sekaligus menjaga stabilitas operasional.[31]

Penelitian yang dilakukan oleh Wilda Yulia Rusyida, menunjukkan bahwa mitigasi risiko berpengaruh signifikan terhadap strategi bertahan pengusaha batik di Pasar Grosir Batik Setono. Temuan ini mengindikasikan bahwa semakin baik kemampuan pelaku usaha dalam melakukan mitigasi risiko, maka semakin besar peluang usaha tersebut untuk bertahan menghadapi dinamika lingkungan bisnis. Hasil ini sejalan dengan penelitian-penelitian sebelumnya yang menegaskan bahwa mitigasi risiko merupakan faktor krusial dalam mendukung keberlanjutan usaha, baik pada sektor UMKM maupun sektor keuangan seperti perbankan.[32]

---

[31] David Hillson, *Effective Opportunity Management for Projects: Exploiting Positive Risk* (New York: CRC Press, 2002), 65

[32] Wilda Yulia Rusyida, "Pengaruh Kemampuan Manajerial, Literasi Keuangan, dan Mitigasi Risiko Terhadap Keberlangsungan Usaha UMKM," *Jurnal Ilmu Manajemen, Ekonomi dan Kewirausahaan* 1, no. 1 (Januari 2023), 80

Dengan merujuk pada penelitian tersebut, maka hipotesis dalam penelitian ini adalah:

H2 = Strategi mitigasi risiko berpengaruh signifikan terhadap kepercayaan nasabah Bank Syariah Indonesia (BSI).

3. Pengaruh Ancaman Siber dan Strategi Mitigasi Risiko Terhadap Kepercayaan Nasabah

Keamanan siber dan manajemen risiko merupakan faktor penting dalam membangun kepercayaan pengguna layanan keuangan digital. Menurut teori manajemen risiko, setiap organisasi harus mampu mengidentifikasi, mengevaluasi, dan mengendalikan risiko agar tidak mengganggu tujuan strategisnya.[33].

Penelitian yang dilakukan oleh Setiawan dan Oktavia, menunjukkan bahwa keamanan siber dan strategi manajemen risiko berpengaruh signifikan secara simultan terhadap kepercayaan pengguna *e-banking*. Temuan ini sejalan dengan penelitian-penelitian sebelumnya yang menegaskan bahwa penerapan sistem keamanan informasi yang kuat dan strategi manajemen risiko yang terintegrasi merupakan faktor utama dalam membangun dan mempertahankan kepercayaan pengguna layanan keuangan digital.[34]

[33] Hillson, Effective Opportunity Management for Projects, 63

[34] Setiawan dan Oktavia, "Pengaruh Keamanan Siber dan Strategi Manajemen Risiko terhadap Kepercayaan Pengguna E-Banking," *Jurnal Manajemen dan Teknologi Informasi* 12, no. 1 (2023): 45–59.

Dengan merujuk pada penelitian tersebut, maka hipotesis dalam penelitian ini adalah:

H3 = Ancaman siber dan strategi mitigasi risiko secara simultan berpengaruh signifikan terhadap kepercayaan nasabah Bank Syariah Indonesia (BSI).

BAB III

METODE PENELITIAN

A. Jenis Penelitian

Jenis penelitian yang digunakan adalah kuantitatif. Penelitian kuantitatif adalah investigasi sistematis mengenai sebuah fenomena dengan mengumpulkan sebuah data yang dapat diukur menggunakan teknik statistik, matematika atau komputasi.[35]

Penelitian ini merupakan penelitian kuantitatif dengan pendekatan asosiatif. Penelitian kuantitatif digunakan karena bertujuan untuk mengukur pengaruh antara variabel-variabel melalui pengumpulan data numerik yang kemudian dianalisis secara statistik. Pendekatan asosiatif digunakan karena penelitian ini ingin mengetahui hubungan atau pengaruh antara dua variabel independen, yaitu ancaman siber (X1) dan strategi mitigasi risiko (X2), terhadap variabel dependen yaitu kepercayaan nasabah (Y) pada Bank Syariah Indonesia (BSI).

B. Subjek Penelitian

1. Populasi

Populasi adalah wilayah generalisasi yang terdiri atas objek/subjek yang mempunyai kualitas dan karakteristik tertentu yang ditetapkan oleh penelitian untuk dipelajari kemudian ditarik kesimpulan.

[35] Muhammad Ramdhan, *Metode Penelitian*, (Jakarta: Cipta Media Nusantara, 2021), 6

Populasi dalam penelitian ini adalah mahasiswa penerima KIP-K IAIN Curup angkatan 2022-2023 yang merupakan nasabah BSI dengan jumlah keseluruhan mahasiswa 350 orang dan jumlah populasi yang akan dijadikan responden kuisioner berjumlah 350 orang.

2. Sampel

Sampel adalah bagian dari jumlah dan karakteristik yang dimiliki oleh populasi tersebut. Sampel dalam penelitian ini ditentukan menggunakan rumus *Slovin* karena jumlah populasi diketahui, yaitu sebanyak 350 mahasiswa penerima KIP-K IAIN Curup yang menjadi nasabah aktif Bank Syariah Indonesia (BSI). Dengan tingkat kesalahan (*e*) sebesar 5% atau 0,05. Berdasarkan perhitungan dengan rumus slovin pada tingkat kesalahan (*margin of error*) sebesar 5%, diperoleh jumlah sampel ideal sebanyak 187 responden.[36]

Teknik pengambilan sampel yang digunakan adalah *purposive sampling*, yaitu metode pengambilan sampel secara sengaja dengan mempertimbangkan kriteria tertentu.[37] Adapun kriteria inklusi dalam penelitian ini yaitu: (1) mahasiswa aktif penerima KIP-K IAIN Curup, (2) merupakan nasabah aktif BSI, dan (3) bersedia menjadi responden. Sedangkan kriteria eksklusi yaitu mahasiswa yang sedang cuti kuliah atau tidak menggunakan layanan digital BSI secara aktif.

[36] Umar, Husein, *Metode Penelitian untuk Skripsi dan Tesis Bisnis* (Jakarta: Raja Grafindo Persada, 2003), 108

[37] Arikunto, Suharsimi, *Prosedur Penelitian: Suatu Pendekatan Praktik* (Jakarta: Rineka Cipta, 2013), 183

C. Jenis Data

Data kuantitatif adalah data yang dapat diukur dan dinyatakan dalam angka. Jenis data ini biasanya digunakan untuk analisis statistik dan memungkinkan peneliti untuk menguji hipotesis.[38] Dalam konteks penelitian ini, data kuantitatif dapat mencakup:

1. Survei kuesioner: kuesioner yang dirancang untuk mengumpulkan informasi dari nasabah BSI.
2. Skala *likert*: penggunaan skala *likert* (misalnya, 1-5 atau 1-7) untuk mengukur sikap dan persepsi responden terhadap berbagai pernyataan terkait ancaman siber dan kepercayaan.
3. Data demografis: informasi tentang karakteristik responden, seperti usia, jenis kelamin, pendidikan, dan lama menjadi nasabah BSI.

D. Instrumen Penelitian/Teknik Pengumpulan Data

1. Instrument Penelitian

Instrumen penelitian dapat diartikan sebagai alat untuk mengumpulkan, mengolah, menganalisa dan menyajikan data-data secara sistematis serta objektif dengan tujuan memecahkan suatu persoalan atau menguji suatu hipotesis.[39]

Instrumen penelitian adalah suatu alat yang digunakan untuk memperoleh, mengolah, dan menginterpretasikan informasi yang diperoleh

[38] Sugiyono*, Metode Penelitian Kuantitatif, Kualitatif*, dan R&D, 65

[39] Hamni Fadlilah Nasution, '*Instrumen Penelitian Dan Urgensinya Dalam Penelitian Kuantitatif*', 2022, 42

dari para responden yang dilakukan dengan menggunakan pola ukur yang sama. Instrumen yang digunakan pada penelitian ini berupa kuesioner.[40]

Pengukuran variabel dalam penelitian ini dilakukan dengan menggunakan skala Likert. Dimana dalam skala likert menyatakan bahwa setiap item pertanyaan didesain sebagai observasi trail yang dikehendaki. Setiap item pertanyaan digunakan untuk mengukur *true score*. Jika dihitung nilai rata-rata (penjumlahan) dari setiap item pertanyaan maka kesalahan pengukuran diasumsikan mendekati nol sehingga hasil estimasi menjadi *true score*. Kesalahan pengukuran berhubungan terbalik dengan *reliability*. Semakin besar nilai kesalahan pengukuran maka semakin buruk nilai *reliability*.[41]

2. Teknik Pengumpulan Data

Teknik pengumpulan data merupakan langkah yang paling strategis dalam penelitian, karena tujuan utama dari penelitian adalah mendapatkan data, tanpa mengetahui teknik pengumpulan data, maka peneliti tidak akan mendapatkan data yang memenuhi standar yang di tetapkan. Pengumpulan data dapat dilihat dari berbagai setting, berbagai sumber dan berbagai cara.[42]

Pada penelitian ini pengumpulan data dapat dilihat dari berbagai cara, yaitu :

---

[40] Nani Agustina, "Mengukur Kualitas Layanan Sistem Informasi Akademik pada SMP Uswatun Hasanah Jakarta," *Jurnal Paradigma* 19, no. 1 (April 2017): 61–68

[41] Imam Ghozali*, Desain Penelitian Kuantitaif dan Kualitatif untuk Akademisi, Bisnis, dan Ilmu Sosial lainnya* (Semarang : Yoga Pratama, 2013), 115

[42] Sugiyono, *Metode Penelitian Kuantitatif, Kualitatif, dan R&D*, (Bandung : ALFABETA, 2022), 224

a. Kuesioner (Angket)

Kuesioner merupakan teknik pengumpulan data yang dilakukan dengan cara memberi seperangkat pertanyaan atau pernyataan tertulis kepada responden untuk dijawabnya. Kuesioner merupakan teknik pengumpulan data yang efisien bila peneliti tahu dengan pasti variabel yang akan diukur dan tahu apa yang bisa diharapkan dari responden.[43]

Kuesioner dalam penelitian ini menggunakan desain skala *Likert* yang terdiri dari beberapa item Sangat Setuju (SS), Setuju (ST), Netral (N), Tidak Setuju (TS), Sangat Tidak Setuju (STS) dan beberapa pernyataan tentang Pengaruh Ancaman Siber dan Strategi Mitigasi Risiko Terhadap Kepercayaan Nasabah Bank Syariah Indonesia.

Tabel 3.1 Skala *Likert*

Pernyataan	**Keterangan**	**Skor**
Sangat Setuju	SS	5
Setuju	S	4
Netral	N	3
Tidak Setuju	TS	2
Sangat Tidak Setuju	STS	1

[43] Sugiyono, *Metode Penelitian Kuantitatif*, (Bandung : ALFABETA, 2022), 219

b. Studi Pustaka

Teknik ini digunakan untuk mengumpulkan data sekunder yang mendukung dan melengkapi data primer. Data diperoleh dari berbagai sumber seperti buku, jurnal ilmiah, laporan hasil penelitian, artikel, dan dokumen lainnya yang relevan dengan topik penelitian, terutama yang berkaitan dengan ancaman siber, strategi mitigasi risiko, dan kepercayaan nasabah di sektor perbankan.

c. Definisi Operasional

Definisi operasional variabel menjelaskan bagaimana masing-masing variabel dalam penelitian ini diukur menggunakan indikator yang jelas dan terukur. Definisi ini berfungsi untuk menghindari perbedaan penafsiran terhadap variabel penelitian.

1) Ancaman Siber

Segala bentuk potensi bahaya atau serangan digital yang dapat mengganggu keamanan, kerahasiaan, dan integritas data serta layanan perbankan digital BSI.[44]

2) Strategi Mitigasi Risiko

Upaya yang dilakukan oleh BSI dalam mengurangi kemungkinan dan dampak risiko serangan siber agar tidak merugikan nasabah.[45]

[44] Budiyanto, Pengantar Cybercrime, 67.
[45] Hillson, Effective Opportunity Management, 92.

3) Kepercayaan Nasabah

Tingkat keyakinan nasabah terhadap BSI dalam memberikan layanan perbankan yang aman, dapat diandalkan, dan melindungi data pribadi.[46]

E. Teknik Pengolahan Data

Penelitian ini menggunakan metode analisis statistik dengan model regresi linear berganda yaitu berfungsi untuk menguji pengaruh antara variabel independen terhadap variabel dependen dengan menggunakan program komputer (*software*) SPSS.

1. Uji Kualitas Data

a. Uji Validitas

Uji validitas adalah tingkatan dimana kuisioner yang digunakan untuk menghitung valid atau tidaknya data yang diproleh. Dalam hal ini suatu instrument penelitian yaitu angket dapat dikatakan valid apa bila dapat mengukur apa yang perlu diukur.[47] Suatu kuesioner dapat dikatakan valid apabila rhitung > rtabel dengan taraf signifikannya yaitu 0,05 dan instrumen penelitian dikatakan tidak valid apabila rhitung ≤ rtabel. Dianggap valid jika ada hubungan antar variabel tersebut.

[46] Mayer, Davis, and Schoorman, "An Integrative Model of Organizational Trust," 725.

[47] Nilda Miftahul Janna dan H. Herianto, "*Konsep Uji Validitas Dan Reliabilitas Dengan Menggunakan SPSS*," preprint (Open Science Framework, 22 Januari 2021), https://doi.org/10.31219/osf.io/v9j52.

b. Uji Reliabilitas

Uji reliabilitas merupakan suatu instrumen yang dapat digunakan untuk menghitung apakah alat ukur tetap yang digunakan akan tetap konsisten apabila pengukuran tersebut diulang.[48]Terdapat banyak metode dalam pengukuran *reliabilitas* tetapi metode yang banyak digunakan dalam penelitian adalah metode *Cronbach Alpha*. Perhitungan dengan menggunakan rumus *Cronbach Alpha* ini dapat diterima, apabila perhitungan rhitung > rtabel 5% dan dapat dikatakan *reliabel*.

Pada penelitian ini, uji *reliabilitas* dilakukan dengan menggunakan koefisien *Cronbach's Alpha* melalui bantuan *software* SPSS. Suatu instrumen dikatakan reliabel apabila nilai *Cronbach's Alpha* > 0,70. Jika nilai *Cronbach's Alpha* berada pada rentang 0,60 – 0,70, instrumen masih dapat diterima pada penelitian eksploratori. Jika nilai *Cronbach's Alpha* < 0,60, maka instrumen dianggap kurang reliabel dan perlu diperbaiki.

Dengan demikian, uji reliabilitas dalam penelitian ini menggunakan SPSS (*Statistical Package for the Social Sciences*) sebagai alat bantu analisis.

[48] Nilda Miftahul Janna dan Herianto Herianto, "Konsep Uji Validitas dan Reliabilitas dengan Menggunakan SPSS," 2021, OSF Preprints, diakses pada 23 juni 2025 https://osf.io/preprints/v9j52/.

c. Kategori TCR (Tingkat Capaian Responden)

Dalam penelitian kuantitatif dengan kuesioner skala *Likert*, analisis deskriptif sering menggunakan Tingkat Capaian Responden (TCR) untuk mengkategorikan hasil rata-rata jawaban responden. Rumusnya:

$$TCR = \frac{\text{Skor Perolehan}}{\text{Skor Maksimal}} \times 100\%$$

Keterangan:

1) Skor perolehan= Jumlah skor yang diperoleh responden (total jawaban kuisioner)
2) Skor maksimal= Jumlah skor tertinggi yang mungkin dicapai (jumlah item x skor tertinggi per item x jumlah responden).

Kemudian untuk kategori nilai pencapaian responden adalah sebagai berikut:[49]

Presentase TCR	Kategori
80% - 100%	Sangat Baik
61% - 80%	Baik
41% - 60%	Cukup
21% - 40%	Kurang
0% - 20%	Sangat Kurang

[49] Suharsimi Arikunto, *Prosedur Penelitian: Suatu Pendekatan Praktik* (Jakarta: Rineka Cipta, 2013), 245.

2. Uji Asumsi Klasik

Sebelum dilakukan analisis regresi, dilakukan uji asumsi klasik untuk memastikan bahwa data memenuhi syarat regresi linier berganda. Uji ini meliputi:

a. Analisis Deskriptif

Uji statistik deskriptif digunakan untuk memberikan gambaran umum mengenai data penelitian sebelum dilakukan pengujian hipotesis. Analisis ini mencakup penyajian data dalam bentuk distribusi frekuensi, nilai minimum, maksimum, rata-rata (mean), dan standar deviasi.[50] Uji deskriptif membantu peneliti memahami karakteristik responden serta kecenderungan jawaban terhadap setiap variabel penelitian.

b. Uji Normalitas

Menggunakan metode kolmogorov-smirnov untuk mengetahui apakah data berdistribusi normal. Kriteria pengujian:[51]

1) Jika nilai signifikansi (Asymp. Sig.) > 0,05 → data berdistribusi normal.
2) Jika nilai signifikansi ≤ 0,05 → data tidak berdistribusi normal.

[50] Arikunto, Prosedur Penelitian: Suatu Pendekatan Praktik,

[51] Imam Ghozali, *Aplikasi Analisis Multivariate dengan Program SPSS* (Semarang: Badan Penerbit Universitas Diponegoro, 2018), 129.

c. **Uji Multikolinearitas**

Dilakukan untuk mengetahui apakah terdapat korelasi tinggi antar variabel independen. Indikator tidak terdapat multikolinearitas adalah nilai *tolerance* ≥ 0,10 dan VIF ≤ 10. Kriteria pengujian:[52]

1) Tolerance ≥ 0,10 dan VIF ≤ 10 → tidak terjadi multikolinearitas.
2) Tolerance < 0,10 dan VIF > 10 → terdapat multikolinearitas.

d. Uji Heteroskedastisitas

Uji ini bertujuan mengetahui apakah ada ketidaksamaan varians residual antar observasi. Kriteria pengujian (*Glejser Test*):[53]

1) Jika signifikansi > 0,05 → tidak terdapat heteroskedastisitas.
2) Jika signifikansi ≤ 0,05 → terdapat heteroskedastisitas.

3. Uji Hipotesis

Uji hipotesis merupakan teknik analisis data yang digunakan untuk menguji dugaan atau asumsi sementara (hipotesis) yang telah dirumuskan dalam penelitian.[54] Dalam penelitian ini, hipotesis yang diuji berkaitan dengan pengaruh variabel independen, yaitu Ancaman Siber (X1) dan Strategi Mitigasi Risiko (X2), terhadap variabel dependen yaitu Kepercayaan Nasabah (Y). Pengujian dilakukan secara parsial dan simultan.

[52] Ghozali, Aplikasi Analisis Multivariate dengan Program SPSS, 132.
[53] Ghozali, Aplikasi Analisis Multivariate dengan Program SPSS, 135
[54] Arikunto, Prosedur Penelitian: Suatu Pendekatan Praktik,

a. Regresi Linier Berganda

Regresi linier berganda digunakan untuk mengetahui pengaruh lebih dari satu variabel independen terhadap satu variabel dependen.[55] Model ini dipilih karena penelitian ini melibatkan dua variabel bebas, yaitu Ancaman Siber (X1) dan Strategi Mitigasi Risiko (X2), serta satu variabel terikat yaitu Kepercayaan Nasabah (Y).[56] Persamaan umum regresi linier berganda adalah sebagai berikut:

$$Y=a+b1X1+b2X2+e$$

Keterangan:

Y = Variabel dependen (Kepercayaan Nasabah)

a = Konstanta (nilai Y ketika X1 dan X2 = 0)

b1 = Koefisien regresi variabel X1 (Ancaman Siber)

b2 = Koefisien regresi variabel X2 (Strategi Mitigasi Risiko)

X1 = Variabel independen (Ancaman Siber)

X2 = Variabel independen (Strategi Mitigasi Risiko)

e = *Error* (faktor kesalahan)

Interpretasi koefisien:

1) Nilai b1 menunjukkan seberapa besar perubahan Y dipengaruhi oleh X1, dengan asumsi X2 konstan.

[55] Ibid., 252.

[56] Putri Prasmono, dkk "Analisis Regresi Berganda Pada Faktor-Faktor Yang Mempengaruhi Kinerja Fisik Preservasi Jalan Dan Jembatan Di Provinsi Sumatera Selatan: Analisis Regresi Berganda", *Emerging Statistics And Data Science Journal* 1, No. 1 (2023) hlm 47–56.

2) Nilai b2 menunjukkan seberapa besar perubahan Y dipengaruhi oleh X2, dengan asumsi X1 konstan.
3) Jika koefisien bernilai positif, maka terdapat hubungan searah (kenaikan X meningkatkan Y).
4) Jika koefisien bernilai negatif, maka terdapat hubungan berlawanan (kenaikan X menurunkan Y).

Analisis regresi linier berganda pada penelitian ini dilakukan dengan bantuan software SPSS, sehingga akan diperoleh nilai konstanta, koefisien regresi, serta signifikansi statistik yang digunakan dalam uji t, uji F, dan uji koefisien determinasi (R^2).

b. Uji t

Uji t digunakan untuk mengetahui pengaruh masing-masing variabel independen secara individual terhadap variabel dependen. Apabila nilai signifikansi (p-value) < 0,05, maka variabel tersebut secara parsial berpengaruh signifikan terhadap kepercayaan nasabah.[57] Dalam uji t, keputusan diambil berdasarkan perbandingan antara nilai probabilitas dan taraf signifikansi α yang ditentukan. Jika probabilitas lebih tinggi dari α (0,05 atau 5%) atau nilai t-statistik lebih rendah dari nilai kritis yang terdapat dalam tabel t, maka H0 diterima. Sebaliknya, jika probabilitas lebih rendah dari α (0,05 atau 5%) atau nilai t-statistik lebih tinggi dari nilai kritis yang terdapat dalam tabel t,

[57] Ghozali, Aplikasi Analisis Multivariate dengan Program SPSS, 77

maka H0 ditolak. Analisis tersebut harus dilakukan untuk setiap variabel secara individual. Dengan demikian:

1) H_0 diterima apabila ancaman siber dan strategi mitigasi risiko tidak berpengaruh signifikan terhadap kepercayaan nasabah BSI.
2) H_0 ditolak apabila ancaman siber dan strategi mitigasi risiko berpengaruh signifikan terhadap kepercayaan nasabah BSI.

c. Uji f

Uji F digunakan untuk menguji pengaruh variabel tingkat tent secara simultan terhadap variabel dependen.[58] Jika nilai signifikansi < 0,05, maka dapat disimpulkan bahwa secara tingkat-sama ancaman siber dan strategi mitigasi risiko berpengaruh signifikan terhadap kepercayaan nasabah.

d. Uji Koefisien Determinasi

Koefisien determinasi (R^2) digunakan untuk mengetahui seberapa besar variasi variabel dependen (Y) dapat dijelaskan oleh variabel independen (X1 dan X2). Interpretasi nilai R^2:[59]

1) Nilai R^2 berkisar antara 0 hingga 1.
2) Semakin mendekati 1, maka semakin baik kemampuan model dalam menjelaskan variasi variabel dependen.

[58] Ibid., 78
[59] Arikunto, Prosedur Penelitian: Suatu Pendekatan Praktik, 89

3) Semakin mendekati 0, maka variabel independen hanya mampu menjelaskan sebagian kecil variasi variabel dependen, sehingga terdapat faktor lain di luar model yang berpengaruh.

Selain R^2, sering digunakan juga nilai *Adjusted* R^2 yang telah disesuaikan dengan jumlah variabel dalam model. Nilai ini lebih akurat karena memperhitungkan jumlah variabel independen yang digunakan dalam analisis. Dalam penelitian ini, nilai R^2 akan digunakan untuk melihat seberapa besar pengaruh Ancaman Siber dan Strategi Mitigasi Risiko terhadap Kepercayaan Nasabah secara kuantitatif.

BAB IV

TEMUAN PENELITIAN DAN PEMBAHASAN

A. GAMBARAN OBJEKTIF WILAYAH

1. Gambaran Umum Mahasiswa Penerima KIP-K di IAIN Curup Sebagai Pengguna BSI

Forum Mahasiswa Bidikmisi IAIN Curup, yang saat ini dikenal sebagai Forum Mahasiswa KIP-K (FORMADIKSI), berdiri pada tahun 2015 sebagai respon atas pentingnya wadah koordinasi, komunikasi, serta pengembangan potensi mahasiswa penerima beasiswa Bidikmisi. Forum ini lahir dari inisiatif bersama mahasiswa angkatan pertama Bidikmisi IAIN Curup yang menyadari perlunya organisasi internal untuk mendukung prestasi akademik, penguatan karakter, serta kegiatan pengabdian kepada masyarakat.[60]

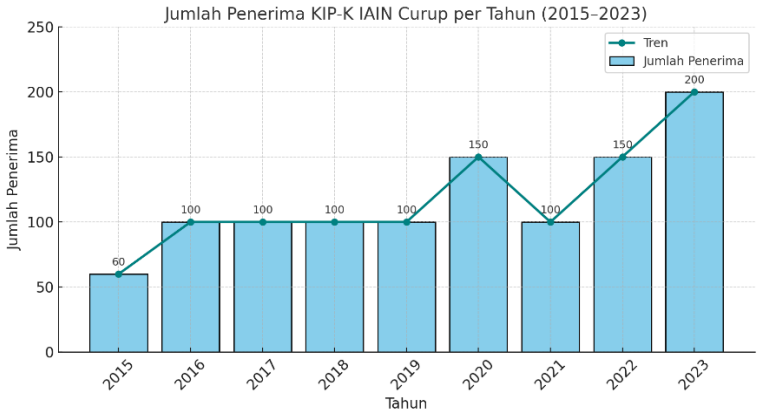
Seiring perubahan kebijakan nasional pada tahun 2020 yang mengganti program Bidikmisi menjadi KIP-Kuliah (KIP-K), forum ini pun menyesuaikan diri dengan nama dan fungsi baru, tetapi tetap mempertahankan visi awal: mencetak mahasiswa yang tidak hanya unggul secara akademik, tetapi juga aktif, berprestasi, dan memiliki kepedulian sosial yang tinggi. Sejak berdiri, FORMADIKSI IAIN Curup rutin menyelenggarakan berbagai kegiatan, di antaranya: pembinaan internal,

[60] Forum Mahasiswa Bidikmisi FORMADIKSI KIP-K IAIN Curup," IAIN Curup, diakses 3 September 2025, https://iaincurup.ac.id/tag/forum-mahasiswa-bidikmisi-formadiksi-kip-k/

pelatihan kepemimpinan, penguatan karakter, diskusi ilmiah, bakti sosial, hingga program pengabdian masyarakat.

Grafik 4.1

Jumlah penerima bidikmisi per tahun



Berikut adalah tabel data jumlah penerima beasiswa KIP-Kuliah IAIN Curup dari tahun 2013-2023.

Tabel 4.1
Jumlah penerima Bidikmisi per tahun

Tahun	Jumlah Penerima
2015	60
2016-2019	100
2020	150
2021	100
2022	150
2023	200

Sejak tahun 2015, IAIN Curup mulai menerima mahasiswa penerima beasiswa Bidikmisi, yang kemudian beralih menjadi KIP-Kuliah seiring kebijakan nasional. Pada periode awal 2015, jumlah penerima masih relatif sedikit dengan fluktuasi yang cukup signifikan. Namun, mulai tahun 2016 hingga 2019 jumlah penerima stabil di angka sekitar 100 mahasiswa setiap tahun. Peningkatan signifikan terjadi pada tahun 2020, di mana jumlah penerima mencapai 150 mahasiswa. Meski pada tahun 2021 sempat turun kembali menjadi 100 mahasiswa, jumlah penerima KIP-K kembali naik menjadi 150 pada 2022, dan pada 2023 mencapai jumlah tertinggi yaitu 200 mahasiswa. Kenaikan jumlah penerima KIP-K tersebut menunjukkan komitmen IAIN Curup dalam mendukung pemerataan akses pendidikan tinggi serta membantu mahasiswa berprestasi dari keluarga kurang mampu agar dapat melanjutkan studi dengan lebih baik.

Formadiksi KIP-Kuliah IAIN Curup adalah singkatan dari forum mahasiswa Bidikmisi Kartu Indonesia Pintar Kuliah. Pada tahun 2020, Program Bidikmisi IAIN Curup yang menyediakan bantuan biaya pendidikan untuk mahasiswa miskin berprestasi resmi digantikan oleh Kartu Indonesia Pintar (KIP) Kuliah. Beasiswa KIP Kuliah ini adalah perluasan dari beasiswa Bidikmisi. Tak sampai disitu saja, beasiswa KIP Kuliah ini tak hanya menghapuskan beasiswa Bidikmisi melainkan juga beasiswa pemerintah lainnya seperti Bantuan Biaya Pendidikan Peningkatan Prestasi Akademik (BPP-PPA) dan Beasiswa Afirmasi Pendidikan (Adik). Hal ini

karena KIP Kuliah ini dianggap perluasan dari ketiga beasiswa yang disebutkan.

Program Bidikmisi pertama kali diimplementasikan di IAIN Curup untuk mendukung mahasiswa berprestasi dari keluarga kurang mampu, sebagai tindak lanjut amanat Undang-Undang Nomor 12 Tahun 2012 tentang Pendidikan Tinggi. Sejak tahun 2020, program ini dialihkan menjadi Kartu Indonesia Pintar Kuliah (KIP-K) sesuai ketentuan Peraturan Menteri Pendidikan dan Kebudayaan Republik Indonesia Nomor 10 Tahun 2020.

Sebagai perguruan tinggi yang berada di bawah naungan Kementerian Agama, IAIN Curup juga mengacu pada Peraturan Menteri Agama Republik Indonesia Nomor 56 Tahun 2014 untuk pelaksanaan Bidikmisi, dan Peraturan Sekretaris Jenderal Kementerian Agama Nomor 26 Tahun 2020 sebagai dasar teknis pelaksanaan program KIP Kuliah.

Penelitian ini dilaksanakan pada mahasiswa penerima Kartu Indonesia Pintar Kuliah (KIP-K) di Institut Agama Islam Negeri (IAIN) Curup, yang merupakan salah satu perguruan tinggi keagamaan islam negeri yang berada di bawah naungan Kementerian Agama Republik Indonesia. IAIN Curup berlokasi di Kabupaten Rejang Lebong, Provinsi Bengkulu, dan memiliki peran strategis dalam pengembangan pendidikan tinggi keislaman di wilayah barat indonesia. Kampus ini tidak hanya menjadi pusat kajian keilmuan keislaman, tetapi juga memiliki komitmen dalam mendukung pemerataan akses pendidikan bagi mahasiswa dari berbagai

latar belakang sosial ekonomi, khususnya mereka yang berasal dari keluarga kurang mampu.

Salah satu program unggulan pemerintah dalam mendukung mahasiswa dari keluarga prasejahtera adalah melalui Kartu Indonesia Pintar Kuliah (KIP-K). Program ini bertujuan untuk memberikan bantuan pembiayaan pendidikan secara penuh kepada mahasiswa yang memenuhi kriteria tertentu, agar mereka dapat menyelesaikan studi di perguruan tinggi tanpa terbebani oleh biaya pendidikan. Di IAIN Curup, jumlah mahasiswa penerima KIP-K dari angkatan 2022 hingga 2023 tercatat sebanyak 350 orang. Mahasiswa-mahasiswa ini tersebar di berbagai fakultas dan program studi yang ada di lingkungan kampus, dan mereka secara aktif menggunakan layanan perbankan untuk menerima dana bantuan pendidikan secara rutin setiap semester.

Sebagai bagian dari proses penyaluran dana KIP-K, IAIN Curup menjalin kerja sama dengan Bank Syariah Indonesia (BSI) sebagai mitra lembaga keuangan resmi yang menyalurkan bantuan tersebut. Dengan demikian, seluruh mahasiswa penerima KIP-K di kampus ini diwajibkan untuk memiliki rekening BSI yang aktif dan digunakan secara berkala untuk pencairan dana. Di samping itu, mahasiswa juga memanfaatkan berbagai layanan digital BSI seperti BSI *Mobile*, ATM, dan internet banking, yang semakin penting dalam era perbankan digital saat ini. Hal ini menunjukkan bahwa kelompok mahasiswa penerima KIP-K di IAIN Curup bukan hanya

sebagai nasabah pasif, tetapi juga aktif dalam mengakses dan memanfaatkan layanan perbankan digital untuk kebutuhan sehari-hari mereka.

Kondisi ini menjadikan mahasiswa penerima KIP-K di IAIN Curup sebagai kelompok responden yang sangat relevan dalam penelitian ini. Mereka tidak hanya berperan sebagai penerima dana bantuan pendidikan, tetapi juga sebagai pengguna aktif layanan digital BSI. Dengan pengalaman langsung terhadap penggunaan layanan keuangan digital, kelompok ini memiliki persepsi yang otentik terhadap isu ancaman siber, efektivitas strategi mitigasi risiko, serta tingkat kepercayaan mereka terhadap sistem perbankan syariah digital, khususnya BSI.

2. Pengujian dan Hasil Analisis Data Responden

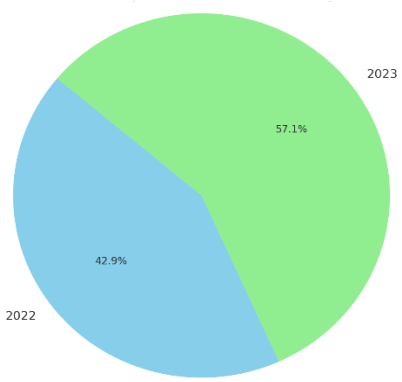
a. Karakteristik Responden

Responden dalam penelitian ini adalah mahasiswa penerima Kartu Indonesia Pintar Kuliah (KIP-K) di IAIN Curup yang merupakan nasabah aktif Bank Syariah Indonesia (BSI). Jumlah responden yang terlibat sebanyak 187 orang, yang dipilih menggunakan teknik purposive sampling berdasarkan kriteria inklusi: mahasiswa aktif, penerima KIP-K, serta pengguna aktif layanan digital BSI seperti BSI *Mobile*.

1) Deskripsi Angkatan

Berdasarkan distribusi angkatan, sebanyak 150 responden (42,9%) berasal dari angkatan 2022 dan 200 responden (57,1%) berasal dari angkatan 2023. Grafik berikut menggambarkan distribusi responden berdasarkan tahun angkatan:

Gambar 4.1 Distribusi Responden



Distribusi yang cenderung seimbang ini menunjukkan bahwa kedua angkatan memiliki representasi yang cukup kuat dalam penelitian, sehingga data yang dikumpulkan diharapkan mampu memberikan gambaran yang akurat mengenai persepsi nasabah terhadap ancaman siber, strategi mitigasi risiko, dan tingkat kepercayaan terhadap layanan digital BSI.

2) Jenis Kelamin

Tabel 4.2

Jenis Kelamin

Jenis Kelamin	Frekuensi	Persentase
Laki -laki	55	29,41%
Perempuan	132	70,59%
Jumlah	187	100%

Jumlah responden dalam penelitian ini sebanyak 187 orang, yang terdiri dari 55 responden laki-laki (29,41%) dan 132 responden perempuan (70,59%). Dengan demikian, dapat disimpulkan bahwa responden dalam penelitian ini mayoritas berjenis kelamin perempuan.

b. Statistik Deskriptif

Untuk mengukur hasil pencapaian dalam mengisi suatu kuesioner, dalam penelitian ini menggunakan skala *likert*. Skala *likert* sendiri adalah suatu teknik yang mana memungkinkan seorang responden untuk mengepresikan kemampuan mereka. Adapun langkah dalam mambuat skala *likert* adalah dengan mengumpulkan pernyataan pernyataan dan membuat skor total untuk setiap responden dengan memjumlah skor untuk semua jawaban.[61]

[61] Aulia Rahma, "Penerapan Sistem Manajemen Mutu Iso 9001: 2008 Terhadap Realisasi Produk Beton Ready Mix Di Pt. Scg Jayamix," (Tesis, 2019), 88

Rumus skala likert N= T x Pn

T = Total Jumlah Pemilih

Pn = Pilihan angka skor liket

N = Jumlah responden

Untuk menghitung tingkat pencapain responden dianalisis dengan langkah berikut ini:

1. Melakukan tabulasi terhadap angket yang diisi oleh responden
2. Melakukan perhitungan setiap skor
3. Menghitung skor total
4. Menganalisis dengan analisis persentase

Adapun rumus pencapaian responden sebagai berikut:

Tingkat pencapaian:

$$TCR = \frac{Skor\ Rata - Rata}{Skor\ Ideal\ Maksimun} x\ 100\%$$

Skor rata – rata/ skor ideal maksimum x 100%

Kemudian untuk kategori nilai pencapaian responden adalah sebagai berikut:

Tabel 4.3

Kategori Pencapaian Responden[62]

Rentang	Keterangan
80% - 100%	Sangat Baik
61% - 80%	Baik
41% - 60%	Cukup
21% - 40%	Kurang
0% - 20%	Sangat Kurang

Berdasarkan penjelasan di atas adapun hasil uji tingkat pencapaian responden yang telah di olah dan dianalisis dalam penelitian ini adalah sebagai berikut.

Tabel 4.4

Hasil Tingkat Pencapaian Responden Variabel X1

Variabel X1	SS	S	N	TS	STS	N	Skor	Mean	TCR	Kategori
X1.1	36	53	72	17	9	187	201	3,48	69,6	Baik
X1.2	13	60	85	18	11	187	185	3,25	64,4	Baik
X1.3	40	62	64	18	3	187	215	3,63	72,6	Baik

[62] Arikunto, Prosedur Penelitian: Suatu Pendekatan Praktik, 134

Lanjutan tabel 4.4

X1.4	23	99	60	4	1	187	227	3,74	75,8	Baik
X1.5	27	52	93	14	1	187	211	3,48	72,8	Baik
X1.6	23	52	92	17	3	187	205	3,40	71,4	Baik
X1.7	25	65	51	27	19	187	189	3,27	64,6	Baik
X1.8	33	84	68	1	1	187	230	3,79	77,2	Baik
X1.9	29	80	76	2	0	187	229	3,73	76,6	Baik

Sumber : Data Primer SPSS 26 yang diolah, 11 Juni 2025

Dari tabel 4.4 diatas dapat dilihat bahwa total pencapaian responden (TCR) sebanyak 9 item variabel memenuhi kategori baik.

Tabel 4.5

Hasil Tingkat Pencapaian Responden X2

Variabel X2	SS	S	N	TS	STS	N	Skor	Mean	TCR	Kategori
X2.1	30	76	77	4	0	187	693	3,71	74,12	Baik
X2.2	36	93	57	1	0	187	725	3,88	77,54	Baik
X2.3	45	66	71	4	1	187	711	3,80	76,04	Baik
X2.4	33	71	82	1	0	187	697	3,73	74,55	Baik
X2.5	35	66	84	1	1	187	694	3,71	74,22	Baik
X2.6	34	81	67	5	0	187	705	3,77	75,40	Baik
X2.7	36	83	66	1	1	187	713	3,81	76,26	Baik
X2.8	48	88	51	0	0	187	745	3,98	79,68	Baik
X2.9	37	94	54	2	0	187	727	3,89	77,75	Baik

Sumber : Data Primer SPSS 26 yang diolah, 11 Juni 2025

Dari tabel 4.5 diatas dapat dilihat bahwa total pencapaian responden (TCR) sebanyak 9 item variabel memenuhi kategori baik.

Tabel 4.6

Hasil Tingkat Pencapaian Responden Y

Variabel Y	SS	S	N	TS	STS	N	Skor	Mean	TCR	Kategori
Y1.1	53	81	50	3	0	187	745	3,98	79,68	Baik
Y1.2	50	81	54	2	0	187	740	3,96	79,14	Baik
Y1.3	49	94	42	2	0	187	751	4,02	80,32	Baik
Y1.4	55	85	47	0	0	187	756	4,04	80,86	Baik
Y1.5	49	96	41	1	0	187	754	4,03	80,64	Baik
Y1.6	45	97	42	2	1	187	744	3,98	79,57	Baik
Y1.7	59	86	40	1	1	187	762	4,07	81,50	Sangat baik
Y1.8	44	99	42	2	0	187	746	3,99	79,79	Baik
Y1.9	84	83	17	3	0	187	809	4,33	86,52	Sangat baik

Sumber : Data Primer SPSS 26 yang diolah, 11 Juni 2025

Dari tabel 4.6 diatas dapat dilihat bahwa total pencapaian responden (TCR) sebanyak 2 item memenuhi kategori sangat baik dan 7 item variabel memenuhi kategori baik.

c. Analisis Instrumen Penelitian

1) Uji Validitas

Uji validitas adalah analisis pengelolaan data untuk mengukur valid tidaknya suatu angket dalam penelitian. Dapat

dikatakan valid ketika pertanyaan mampu mengungkapkan apa yang diukur pada kuesioner tersebut. Kriteria dalam penelitian uji validitas dengan taraf signifikan= 0,05 jika r-hitung > r-tabel, maka angket sebagai alat pengukur dikatakan valid. Jika nilai r-hitung < r-tabel, maka angket sebagai alat pengukur dikatakan tidak valid.[63] Karena sampel yang digunakan pada uji ini berjumlah 50 sampel, maka untuk nilai r- tabel adalah 0,279, dan r- hitung harus lebih besar dari 0,279 dengan taraf signifikan 0,05.[64] Berikut merupakan tabel hasil pengujian validitas:

Tabel 4.7

Hasil Uji Validitas Variabel Ancaman Siber

Item	r hitung	r tabel	Keterangan
X1.1	0,817	0,279	Valid
X1.2	0,598	0,279	Valid
X1.3	0,589	0,279	Valid
X1.4	0,421	0,279	Valid
X1.5	0,619	0,279	Valid
X1.6	0,678	0,279	Valid
X1.7	0,432	0,279	Valid
X1.9	0,466	0,279	Valid

Sumber: Data yang diolah SPSS 26, 13 Juni 2025

[63] Syafrida Hafni Sahir, Metode Penelitian, ed. Try Koryati, 1st ed (Jawa Timur: KBM Indonesia, 2020), 32.

[64] Arikunto, Prosedur Penelitian: Suatu Pendekatan Praktik, 124

Dari tabel 4.7 menunjukkan bahwa ancaman siber memiliki kriteria valid untuk semua kriteria pernyataan berdasarkan kriteria r – hitung lebih besar dari r- tabel (0,279).

Tabel 4.8

Hasil Uji Validitas Variabel Strategi Mitigasi Risiko

Item	r hitung	r tabel	Keterangan
X2.1	0,368	0,279	Valid
X2.2	0,505	0,279	Valid
X2.3	0,344	0,279	Valid
X2.4	0,444	0,279	Valid
X2.5	0,487	0,279	Valid
X2.6	0,370	0,279	Valid

Sumber: Data yang diolah SPSS 26, 13 Juni 2025

Dari tabel 4.8 menunjukkan bahwa ancaman siber memiliki kriteria valid untuk semua kriteria pernyataan berdasarkan kriteria r – hitung lebih besar dari r- tabel (0,279).

Tabel 4.9

Hasil Uji Validitas Kepercayaan Nasabah

Item	r hitung	r tabel	Keterangan
Y.1	0,432	0,279	Valid
Y.2	0,498	0,279	Valid
Y.3	0,520	0,279	Valid
Y.4	0,358	0,279	Valid
Y.5	0,321	0,279	Valid
Y.6	0,455	0,279	Valid

Lanjutan tabel 4.9

Y.7	0,418	0,279	Valid
Y.8	0,422	0,279	Valid
Y.9	0,418	0,279	Valid

Sumber: Data yang diolah SPSS 26, 13 Juni 2025

Dari tabel 4.9 menunjukkan bahwa ancaman siber memiliki kriteria valid untuk semua kriteria pernyataan berdasarkan kriteria r – hitung lebih besar dari r- tabel (0,279).

2) Uji Reliabilitas

Uji reliabilitas mengukur variabel yang digunakan melalui pertanyaan atau pernyataan yang digunakan. Jika menggunakan program SPSS, metode yang digunakan dalam pengujian reliabilitas ini adalah menggunakan metode *Cronbach Alpah*. Kriteria pengujiannya yaitu: jika nilai *Cronbach Alpah* > 0,60, maka instrument dikatakan reliabel. Jika nilai *Cronbach Alpah* < 0,60, maka instrumen dikatakan tidak reliabel.[65]Adapun hasil uji reliabilitas yang diperoleh dalam penelitian ini yaitu:

[65] Syafrida Hafni Sahir, *Metode Penelitian*, ed. Try Koryati, 1st ed (Jawa Timur: KBM Indonesia, 2022), 33.

Tabel 4.10

Hasil Uji Reliabilitas

Variabel	*Cronbach Alpah*	Keterangan
Ancaman siber (X1)	0,730 > 0,60	*Reliabel*
Mitigasi Risiko (X2)	0,626 > 0,60	*Reliabel*
Kepercayaan Nasabah (Y)	0,762 > 0,60	*Reliabel*

Dari keterangan tabel 4.10 dapat diketahui bahwa hasil uji reliabilitas memperlihatkan semua item pernyataan nilai *Cronbach Alpah* > 0,60. Sehingga dapat disimpulkan bahwa reliabel atau dapat dipercaya untuk digunakan ke tahap selanjutnya.

d. Uji Asumsi Klasik

1) Uji Normalitas

Uji normalitas menggunakan histogram dan normal P-Plot adalah untuk melihat apakah model regresi tersebut terdistribusi secara normal atau tidak. Jika grafik membentuk lonceng atau gunung maka distribusi normal. Begitu juga dengan grafik P-Plot, jika titik-titiknya menyebar sekitar garis dan mengikuti garis diagonal maka residual pada model regresi tersebut terdistribusi secara normal.[66] serta menggunakan metode uji Kolmogorov-

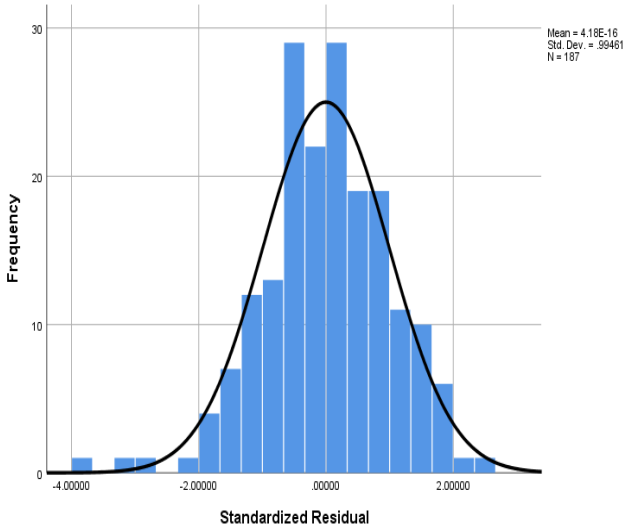
[66] Syafrida H afni Sahir, *Metode Penelitian, ed. Try Koryati, 1st ed* (Jawa Timur: KBM Indonesia, 2022) 69.

Smirnov dilihat dari *monten carlo* sig nya. Jika nilai signifikasinya lebih dari 0,05 maka data residual terdistribusi normal.[67]

Berikut uji normalitas yang didapat dalam penelitian ini dapat dilihat pada gambar dibawah ini:

Gambar 4.2

Uji Normalitas Metode Grafik Histogram



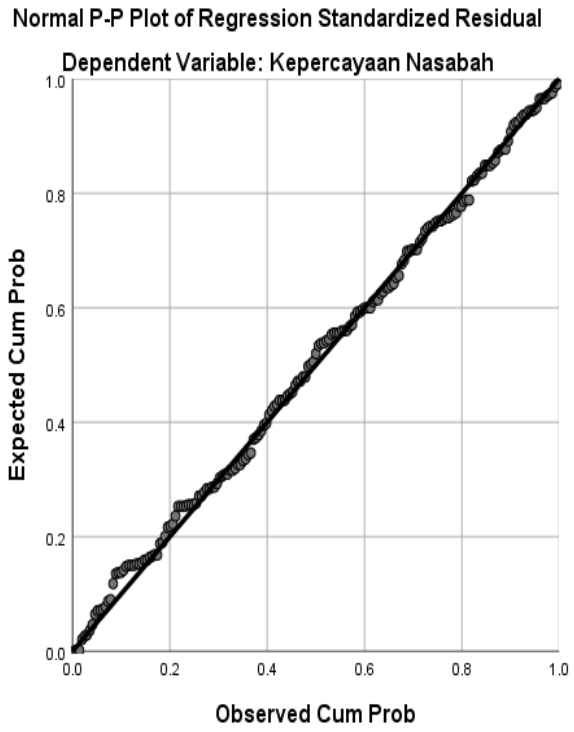
Sumber: Data yang diolah SPSS 26, 20 Juni 2025

Berdasarkan Gambar 4.2, terlihat bahwa distribusi residual mengikuti pola kurva normal (berbentuk lonceng simetris). Nilai mean dari residual adalah 0, dan standar deviasi mendekati 1, yaitu 0,99461. Dengan jumlah responden sebanyak 187 orang, dapat disimpulkan bahwa residual data berdistribusi normal. Oleh karena itu, asumsi normalitas terpenuhi.

[67] Suhadi dan Siti mudrika Zein, Path "*Analysis Faktor Dominan Penentu Rasa Percaya Diri Teori dan Riset"* (Malang: CV. Literasi Nusantara Abaddi,2022) 64.

Gambar 4.3

Uji Normalitas Metode Normal P- Plot



Sumber: Data yang diolah SPSS 26, 20 Juni 2025

Pada Gambar 4.3, terlihat bahwa titik-titik data menyebar mendekati dan mengikuti garis diagonal. Hal ini menunjukkan bahwa distribusi residual mendekati distribusi normal. Oleh karena itu, dapat disimpulkan bahwa asumsi normalitas dalam analisis regresi telah terpenuhi

Tabel 4.11

Hasil Uji Normalitas

Tests of Normality

	Kolmogorov-Smirnov[a]			Shapiro-Wilk		
	Statistic	df	Sig.	Statistic	df	Sig.
Standardized Residual	.049	187	.200*	.986	187	.058

*. This is a lower bound of the true significance.

a. Lilliefors Significance Correction

Sumber: Data yang diolah SPSS 26, 20 Juni 2025

Berdasarkan kriteria pengambilan keputusan, jika nilai signifikansi lebih besar dari 0,05 (α = 5%), maka residual dinyatakan berdistribusi normal. Karena nilai Sig. = 0,200 > 0,05, maka dapat disimpulkan bahwa data residual berdistribusi normal. Dengan demikian, asumsi normalitas dalam model regresi linear terpenuhi

2) Uji Multikolinearitas

Uji Multikolinearitas ini dilakukan dengan tujuan untuk mengetahui apakah pada suatu model regresi ditemukan adanya korelasi antar variabel independen.[68] Jika terjadi korelasi maka dinamakan terdapat masalah multikolinearitas, model regresi yang baik seharusnya tidak terjadi korelasi yang tinggi diantara variabel bebas. Metode pengujian yang bisa digunakan yaitu dengan melihat nilai Inflacation factor (VIF) dan Toletance pada model regresi. Jika nilai

[68] Sugiyono dan Agus Susanto, *Cara mudah belajar SPSS & LISREL Teori dan Aplikasi untuk Analisis Data Penelitian* (Bandung: Alfabeta, 2015): 331

VIF < 10 dan Toletance > 0,10 maka model regresi bebas dari multikolinearitas. Adapun hasil uji multikolinearitas pada penelitian ini yaitu sebagai berikut:

Tabel 4.12

Hasil Uji Multikolinearitas

Coefficients[a]

Model		Collinearity Statistics	
		Tolerance	VIF
1	V10	.989	1.011
	V19	.989	1.011

a. Dependent Variable: kepercayaan_nasabah

Sumber: Data yang diolah SPSS 26, 20 Juni 2025

Berdasarkan hasil uji multikolinearitas menunjukkan nilai *telorance* untuk variabel ancaman siber (X1) sebesar 0,989, variabel mitigasi risiko (X2) sebesar 0,989 nilai tolerance yang diperoleh tersebut lebih besar dari 0,10 serta nilai VIF untuk variabel ancaman siber (X1) sebesar 1.011, variabel mitigasi risiko (X2) sebesar 1.011 dimana nilai VIF pada variabel tersebut lebih kecil dari 10. Berdasarkan nilai tersebut dapat disimpulkan bahwa tidak terjadi gejala multikolinearitas.

3) Heteroskedastisitas

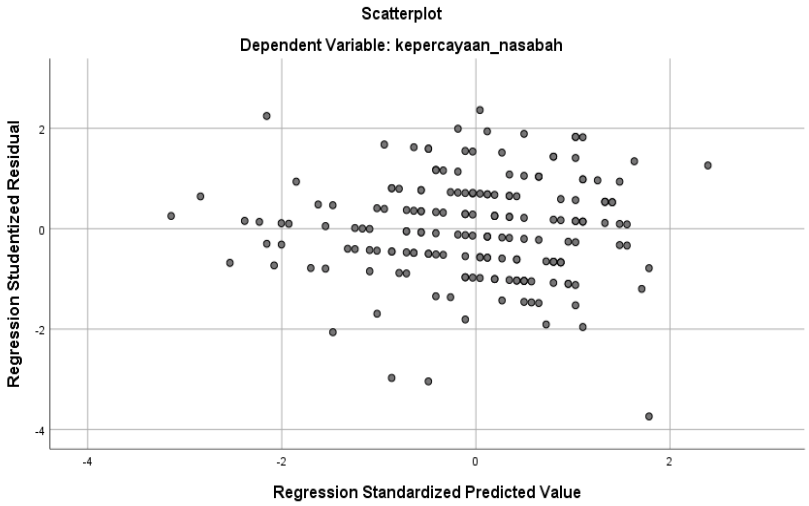
Uji heteroskedastisitas digunakan untuk mengetahui variabel penganggu dalam persamaan regresi mempunyai varians yang sama atau tidak. Jika mempunyai varians yang sama, bearti tidak terjadi heteroskedastisitas, sedangkan jika mempunyai varians yang tidak sama maka terdapat heteroskedastisitas.

Cara memprediksi ada tidaknya heteroskedastisitas pada suatu model dapat dilihat dari pola gambar scatterplot. Pada model regresi berganda tidak terdapat heteroskedastisitas, jika titik-titik menyebar diatas dan dibawah atau sekitar angka 0 maka model regresi tidak terjadi heteroskedastisitas. Kedua uji heteroskedastisitas pada penelitian ini menggunakan Uji Glejser, dimana akan terjadi heteroskedastisitas jika nilai sig < 0,05, dan sebaliknya jika nilai sig > 0,05 maka terjadi heteroskedastisitas.[69]

[69] Sugiyono dan Agus Susanto, *Cara mudah belajar SPSS & LISREL Teori dan Aplikasi untuk Analisis Data Penelitian* (Bandung: Alfabeta, 2015), 376

Gambar 4.4

Uji Heterokedastisitas



Sumber: Data yang diolah SPSS, 26 Juni 2025

Berdasarkan gambar 4.4 hasil scatterplot, titik-titik data menyebar secara acak dan tidak membentuk pola tertentu, baik pola mengerucut maupun melebar. Hal ini menunjukkan bahwa model regresi dalam penelitian ini tidak mengalami masalah heterokedastisitas, sehingga dapat dikatakan bahwa varian residual bersifat konstan (homoskedastisitas).

Tabel 4.13

Hasil Uji Heteroskedastisitas Metode Glejser

Variabel	Sig	Keterangan
(X1)	0,217 > 0.05	Tidak terjadi heterokedastisitas
(X2)	0,139 > 0,05	Tidak terjadi heterokedastisitas

Sumber: Data yang diolah SPSS 26, 20 Juni 2025

Dari keterangan tabel 4.13 dapat diketahui bahwa hasil uji heteroskedastisitas memperlihatkan bahwa semua variabel memiliki nilai sig > 0,05. Sehingga dapat disimpulkan bahwa tidak terjadi gejala heteroskedastisitas.

e. Uji Hipotesis

1) Regresi Linier Berganda

Regresi liniear berganda merupakan analisis yang memiliki variabel bebas lebih dari satu. Teknik regresi linear berganda digunakan untuk mengetahui ada atau tidaknya pengaruh signifikan dua atau lebih variabel bebas (X) yaitu variabel ancaman siber, mitigasi risiko terhadap variabel terikat (Y) yaitu kepercayaan nasabah.[70] Hasil analisis regresi linear berganda variabel bebas dan terikat pada penelitian ini adalah sebagai berikut:

[70] Kurnia Sandi, dkk, *Tutorial PHP Machine Learning Menggunakan Regresi Linear Berganda Pada Aplikasi Bank Sampah Istimewa Versi 2.0 Berbasis Web* (Bandung: Kreatif Industri Nusantara, 2020), 49.

Tabel 4.14

Hasil Analisis Regresi Liner Berganda

Coefficients[a]

Model		Unstandardized Coefficients		Standardized Coefficients		
		B	Std. Error	Beta	t	Sig.
1	(Constant)	28.169	2.501		11.264	.000
	Ancaman siber (X1)	.067	.051	.096	1.310	.192
	Mitigasi Risiko (X2)	-.089	.099	-.067	-.905	.367

a. Dependent Variable: Kepercayaan Nasabah

Sumber: Data yang diolah SPSS 26, 21 Juni 2025

Pada tabel 4.14 merupakan hasil pengolahan analisis regresi linier berganda yang juga menghasilkan persamaan regresi sebagai berikut:

$$\mathbf{Y = 28{,}169 + 0{,}067\ X_1 + 0{,}089\ X_2 + e}$$

Interprestasi dari persamaan tersebut adalah sebagai berikut:

a. Nilai konstanta (a) sebesar 28,169. Nilai konstanta bernilai positif artinya nilai Ancaman Siber dan Strategi Mitigasi Risiko dianggap konstan atau sama dengan (nol), maka Kepercayaan Nasabah akan meningkat berada pada nilai 28,169.
b. Koefisien regresi X_1 (Ancaman Siber) sebesar 0,067. Nilai koefisien X_1 bernilai positif artinya pengaruh ancaman siber terhadap kepercayaan nasabah bersifat positif dan cukup kuat. artinya setiap peningkatan satu satuan pada variabel Ancaman Siber akan

menurunkan Kepercayaan Nasabah sebesar 0,067, dengan asumsi variabel Mitigasi Risiko tetap.

c. Koefisien regresi X_2 (Strategi Mitigasi Risiko) sebesar -0,089. Nilai koefisien X_2 bernilai negatif artinya artinya setiap peningkatan satu satuan pada variabel Mitigasi Risiko justru diprediksi menurunkan Kepercayaan Nasabah sebesar 0,089, dengan asumsi variabel Ancaman Siber tetap.

d. *e* mewakili pengaruh factor -faktor lain yang tidak diteliti dalam model ini.

2) Uji Signifikansi Parsial (Uji – T)

Uji-T digunakan untuk memahami apakah variabel bebas bepengaruh secara parsial (individu) terhadap variabel terikat, dengan memperlihatkan tingkat signifikan yaitu 0,05 jika nilai signifikan < 0,05 dapat diambil kesimpulan bahwa variabel bebas secara parsial berpengaruh signifikan terhadap variabel terikat.[71]

Jika t-hitung > t-tabel maka Ha diterima dan H0 ditolak atau variabel bebas memiliki pengaruh signifikan terhadap variabel terikat, begitupun sebaliknya. Besar t-tabel dicari berdasarkan rumus df = n-k, dimana n = banyaknya responden sedangkan k =

[71] Syafrida Hfni Sahir, *metode Penelitian, ed. Try Koryati, 1st ed* (Jawa Timur: KBM Indonesia, 2022), 53

banyaknya variabel bebas atau terikat, jadi df = 187 – 3 = 184, jadi t- tabel yaitu 1,973. Dapat dilihat pada tabel berikut:

Tabel 4.15

Hasil Uji T

Coefficients[a]

Model		Unstandardized Coefficients		Standardized Coefficients		
		B	Std. Error	Beta	t	Sig.
1	(Constant)	28.169	2.501		11.264	.000
	Ancaman siber (X1)	.067	.051	.096	1.310	.192
	Mitigasi Risiko (X2)	-.089	.099	-.067	-.905	.367

a. Dependent Variable: Kepercayaan Nasabah

Sumber: Data yang diolah SPSS 26, 21 Juni 2025

Pada uji t hasil pengujian variabel ancaman siber (X_1) terhadap kepercayaan nasabah (Y) diperoleh, nilai t hitung = 1,310 < t tabel = 1,973 dan nilai signifikansi (0,192) > 0,05, sehingga H_{01} diterima dan H_{a1} ditolak. Kesimpulannya ancaman siber tidak berpengaruh signifikan terhadap kepercayaan nasabah.

Hasil pengujian variabel mitigasi risiko (X2) terhadap kepercayaan nasabah (Y) diperoleh, Untuk variabel strategi mitigasi risiko (X_2), nilai t hitung = -0,905 < t tabel = 1,973 dan nilai signifikansi (0,367) > 0,05, maka H_{02} diterima dan H_{a2} ditolak. Kesimpulannya,

strategi mitigasi risiko juga tidak berpengaruh signifikan terhadap kepercayaan nasabah.

3) Uji Signifikansi Simultan (Uji F)

Uji-F dipakai untuk melihat apakah semua variabel bebas berpengaruh secara simultan atau bersama-sama terhadap variabel terikat. Pengujian ini dilakukan dengan membandingkan nilai f hitung dengan f-tabel jika f-hitung > f-tabel maka Ha diterima dan H0 ditolak, jika f-hitung < f-tabel maka Ha ditolak dan H0 diterima.[72] 5 F-tabel dapat dihitung dengan cara dfI = k-1 dan df2 = n - k, dimana k adalah jumlah variabel dependen dan independen. Maka, df1 = 3 – 1 = 2 dan df2 = 187 – 3 = 184, jadi f tabel adalah 3,05.

Tabel 4.16

Hasil Uji F

ANOVA[a]

Model		Sum of Squares	df	Mean Square	F	Sig.
1	Regression	16.201	2	8.101	1.409	.247[b]
	Residual	1057.574	184	5.748		
	Total	1073.775	186			

a. Dependent Variable: Kepercayaan Nasabah (Y)

b. Predictors: (Constant), Ancaman siber (X1), Mitigasi Risiko(X2)

Sumber: Data yang diolah SPSS 26, 22 Juni 2025

[72]Ibid., 544

Pada uji simultan, hasil pengujian variabel ancaman siber (X1), strategi mitigasi risiko (X2) terhadap kepercayaan nasabah (Y) diperoleh, nilai f hitung sebesar 1.409 dimana 1.409 lebih kecil dari 0,247 dengan nilai signifikansi lebih besar dari 0,05 (247 > 0,05). Hal ini menunjukkan bahwa H_O diterima dan H_1 ditolak. Kesimpulannya, variabel ancaman siber dan strategi mitigasi risiko secara simultan tidak berpengaruh signifikan terhadap kepercayaan nasabah.

4) Koefisien Determinasi (R2)

Koefisien determinasi digunakan untuk mengetahui kontribusi yang diberikan oleh sebuah variabel bebas terhadap variabel terikat dapat ditunjukan dalam SPSS 25, koefisien determinasi terletak pada Model Summary dan tertulis R Square. Analisis koefisien determinasi (R2) digunakan untuk mengetahui seberapa besar presentase (%) pengaruh keseluruhan variabel bebas terhadap variabel terikat.[73] Hasil uji dapat dilihat pada tabel di bawah ini:

[73] Syafrida Hafni Sahir, Metode Penelitian, ed. Try Koryati, 1st ed,(JawaTimur: KBM Indonesia,2022) hlm 54

Tabel 4.17

Hasil Uji Koefisien Determinasi

Model Summary[b]

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate
1	.123[a]	.015	.004	2.397

a. Predictors: (Constant), Ancaman Siber, Strategi Mitigasi Risiko

b. Dependent Variable: Kepercayaan Nasabah

Sumber: Data yang diolah SPSS 26, 22 Juni 2025

Tabel 4.17 diatas menunjukkan koefisien korelasi (R) sebesar 0,123 ini berarti tidak ada hubungan antara variabel terikat (kepercayaan nasabah) dengan variabel bebas (ancaman siber dan strategi mitigasi risiko) sebesar 0,123. Ini berarti koefisien determinasi (Adjusted R Square) sebesar 0,004 ini berarti kontribusi variabel independen (ancaman siber dan strategi mitigasi risiko) tidak mempengaruhi variabel dependen (kepercayaan nasabah) sebesar 1,5%. Sedangkan sisanya sebesar 95% dipengaruhi oleh variabel lain.

Tabel 4.18

Hasil Hipotesis

Hipotesis		**Kesimpulan**
Hipotesis 1	Tidak terdapat pengaruh ancaman siber terhadap kepercayaan nasabah.	Ditolak
Hipotesis 2	Tidak terdapat pengaruh strategi mitigasi risiko terhadap kepercayaan nasabah.	Ditolak
Hipotesis 3	Tidak terdapat pengaruh ancaman siber dan strategi mitigasi risiko terhadap kepercayaaan nasabah.	Ditolak

Sumber: Data yang diolah SPSS 26, 22 Juni 2025

B. Pembahasan

Penelitian ini bertujuan untuk mengetahui pengaruh ancaman siber dan strategi mitigasi risiko terhadap kepercayaan nasabah bank syariah indonesia. Pembahasan masing – masing hipotesis adalah sebagai berikut:

a. Pengaruh ancaman siber terhadap kepercayaan nasabah bank syariah indonesia mahasiswa kip-k IAIN Curup.

Menurut Kshetri, sektor keuangan merupakan target utama dari serangan siber karena besarnya aset yang dikelola serta data pribadi yang sensitif. Ancaman siber meliputi *malware, ransomware, phishing*, dan serangan *denial-of-service* (DoS), yang dapat merusak sistem dan menurunkan kepercayaan pengguna terhadap lembaga keuangan. Teori ini menekankan bahwa meningkatnya kompleksitas dan frekuensi serangan digital menuntut lembaga perbankan untuk meningkatkan postur keamanan mereka secara proaktif.[74]

Hasil uji t menunjukkan bahwa ancaman siber tidak berpengaruh signifikan terhadap kepercayaan nasabah, dengan nilai t hitung 1,310 < t tabel 1,973 dan signifikansi sebesar 0,192 > 0,05. Meskipun mayoritas responden menyadari adanya serangan *ransomware* yang pernah terjadi pada BSI, namun persepsi mereka terhadap ancaman siber tidak secara langsung menurunkan tingkat kepercayaan terhadap bank. Hal ini

[74] Kshetri, The Global Cybercrime Industry, 2022, 97.

menunjukkan bahwa nasabah, khususnya mahasiswa, lebih fokus pada fungsionalitas layanan daripada risiko keamanan di baliknya.

Hasil penelitian ini menunjukkan bahwa persepsi nasabah terhadap ancaman siber memiliki kecenderungan mempengaruhi tingkat kepercayaan mereka. Ketika risiko serangan digital meningkat, nasabah cenderung merasa was-was dan keragu-raguan muncul. Hal ini sejalan dengan firman Allah SWT dalam QS. Al-Hujurat ayat 6:

يَٰٓأَيُّهَا ٱلَّذِينَ ءَامَنُوٓا۟ إِن جَآءَكُمْ فَاسِقٌۢ بِنَبَإٍ فَتَبَيَّنُوٓا۟ أَن تُصِيبُوا۟ قَوْمًۢا
بِجَهَٰلَةٍ فَتُصْبِحُوا۟ عَلَىٰ مَا فَعَلْتُمْ نَٰدِمِينَ

Artinya: "Wahai orang-orang yang beriman, jika datang kepada kalian orang fasik membawa suatu berita, maka periksalah dengan teliti".[75] Ayat ini menekankan pentingnya berhati-hati dan memverifikasi informasi agar tidak terjebak kepanikan yang justru dapat melemahkan rasa percaya.

Temuan ini bertolak belakang dengan teori kepercayaan dari Mayer, Davis, dan Schoorman, yang menyatakan bahwa persepsi terhadap integritas dan kompetensi sistem memengaruhi kepercayaan pengguna terhadap suatu lembaga. Jika persepsi terhadap keamanan terganggu, kepercayaan pun menurun. Namun dalam konteks penelitian ini, kepercayaan relatif stabil meskipun terdapat ancaman siber, yang

[75] Kementerian Agama Republik Indonesia, Al-Qur'an dan Terjemahannya (Jakarta: Lajnah Pentashihan Mushaf Al-Qur'an, 2019), Q.S. Al-Hujurāt [49]: 6.

bisa disebabkan oleh rendahnya literasi digital atau ketergantungan responden terhadap BSI sebagai satu-satunya kanal pencairan dana KIP-K.[76]

Berdasarkan hasil uji t, variabel ancaman siber (X1) tidak berpengaruh signifikan terhadap kepercayaan nasabah (Y) dengan nilai signifikansi 0,192 (> 0,05). Artinya, meskipun mahasiswa penerima KIP-K IAIN Curup mengetahui adanya ancaman siber seperti malware, phishing, maupun serangan ransomware pada BSI, hal tersebut tidak serta-merta mengurangi tingkat kepercayaan mereka terhadap BSI. Kondisi ini menunjukkan bahwa variabel X1 tidak berpengaruh langsung terhadap Y, yang kemungkinan besar dipengaruhi oleh faktor ketergantungan responden terhadap BSI sebagai satu-satunya bank penyalur dana KIP-K. Hasil ini berbeda dengan teori Mayer, Davis, dan Schoorman yang menyatakan bahwa persepsi keamanan memengaruhi kepercayaan pengguna, namun sejalan dengan konteks empiris responden yang lebih mementingkan aksesibilitas layanan daripada risiko ancaman siber.

b. Pengaruh strategi mitigasi risiko terhadap kepercayaan nasabah bank syariah indonesia mahasiswa kip-k IAIN Curup

Menurut David Hillson, strategi mitigasi risiko bukan sekadar perlindungan, melainkan bagian dari penciptaan nilai dan keunggulan

[76] Mayer, dkk "*An Integrative Model of Organizational Trust*," Academy of Management Review 20, no. 3 (2020): 709–734.

organisasi. Strategi ini dapat berupa penghindaran risiko (risk avoidance), pengurangan risiko (risk mitigation), pengalihan risiko (risk transfer), dan penerimaan risiko (risk acceptance). Dalam konteks perbankan digital, strategi mitigasi mencakup penerapan teknologi keamanan seperti enkripsi data, autentikasi ganda (2FA), serta kebijakan keamanan dan pelatihan pegawai.[77]

Hasil uji t menunjukkan bahwa strategi mitigasi risiko tidak berpengaruh signifikan terhadap kepercayaan nasabah, dengan hasil nilai t hitung -0,905 dan signifikansi 0,367 > 0,05. Artinya, penerapan sistem keamanan seperti autentikasi dua faktor, pembaruan sistem, maupun pelatihan internal tidak secara langsung memengaruhi persepsi kepercayaan responden. Salah satu kemungkinan penyebabnya adalah ketidaktahuan sebagian besar nasabah terhadap keberadaan strategi tersebut.

Penelitian ini menemukan bahwa penerapan strategi mitigasi risiko yang baik dapat meningkatkan rasa aman, sehingga memperkuat kepercayaan nasabah. Hal ini sejalan dengan firman Allah SWT dalam QS. Al-Baqarah ayat 195:

النَّهْلُكَةِ إِلَى بِأَيْدِيكُمْ تُلْقُوا وَلَا

[77] Hillson, Effective Opportunity Management for Projects, 2023, 76

Artinya: Dan janganlah kamu menjatuhkan dirimu sendiri ke dalam kebinasaan".[78]

Ayat ini memberi pelajaran agar kita aktif berupaya menghindari risiko kebinasaan, termasuk dengan tindakan mitigasi.

Berbeda dengan hasil penelitian Wilda Yulia Rusyida yang menunjukkan bahwa mitigasi risiko berpengaruh signifikan terhadap strategi bertahan pelaku usaha, temuan dalam penelitian ini menunjukkan bahwa konteks nasabah muda dan mahasiswa membutuhkan pendekatan komunikasi dan edukasi yang lebih intensif agar strategi mitigasi dirasakan secara nyata dan tidak hanya bersifat teknis.[79]

Hasil uji t menunjukkan bahwa strategi mitigasi risiko (X2) juga tidak berpengaruh signifikan terhadap kepercayaan nasabah (Y), dengan nilai signifikansi 0,367 (> 0,05). Hal ini berarti penerapan mitigasi risiko seperti autentikasi ganda, pembaruan sistem, maupun kebijakan keamanan internal bank tidak secara langsung meningkatkan kepercayaan mahasiswa penerima KIP-K sebagai nasabah BSI. Faktor yang memengaruhi kondisi ini adalah minimnya pemahaman responden terhadap mekanisme keamanan yang diterapkan oleh bank, sehingga strategi mitigasi risiko tidak dipersepsikan sebagai sesuatu yang

[78] Kementerian Agama Republik Indonesia, Al-Qur'an dan Terjemahannya (Jakarta: Lajnah Pentashihan Mushaf Al-Qur'an, 2019), Q.S. Al-Baqarah [2]: 195.

[79] Rusyida, "Pengaruh Kemampuan Manajerial, Literasi Keuangan, dan Mitigasi Risiko," 7, 90

memengaruhi keputusan kepercayaan mereka. Dengan demikian, variabel X2 tidak berpengaruh signifikan terhadap Y, berbeda dengan temuan Wilda Yulia Rusyida yang menyatakan mitigasi risiko berpengaruh positif pada keberlangsungan usaha. Pengaruh ancaman siber dan strategi mitigasi risiko terhadap kepercayaan nasabah bank syariah indonesia mahasiswa kip-k IAIN Curup

Moorman et al. mendefinisikan kepercayaan sebagai kemauan seseorang untuk bergantung pada pihak lain berdasarkan harapan bahwa pihak tersebut akan bertindak secara menguntungkan dan tidak mengeksploitasi situasi. Kepercayaan dalam konteks ini melibatkan resiko, karena nasabah menyerahkan data dan dana kepada bank tanpa bisa mengawasi langsung sistem yang berjalan.[80]

Hasil uji F memperlihatkan bahwa kedua variabel bebas tidak berpengaruh signifikan secara simultan terhadap kepercayaan nasabah (f hitung = 1,409 < f tabel = 3,05; sig. = 0,247 > 0,05). Koefisien determinasi (R^2) yang sangat rendah, yaitu 1,5%, menandakan bahwa hampir seluruh variasi dalam kepercayaan nasabah ditentukan oleh variabel lain yang tidak diteliti dalam studi ini.

Secara bersama-sama, adanya ancaman siber yang disertai strategi mitigasi risiko mempengaruhi tingkat kepercayaan nasabah.

[80] Christine Moorman, Gerald Zaltman, dan Rohit Deshpandé, "*Relationships Between Providers and Users of Market Research: The Dynamics of Trust Within and Between Organizations*," Journal of Marketing Research 29, no. 3 (1992): 314–328.

Keseimbangan antara kesadaran risiko dan langkah nyata mitigasi menjadi kunci membangun rasa aman.

Allah SWT berfirman dalam QS. Al-Anfal ayat 60:

بَاطِ الْخَيْلِ تُرْهِبُوْنَ بِهٖ عَدُوَّ ِۙوَاَعِدُّوْا لَهُمْ مَّا اسْتَطَعْتُمْ مِّنْ قُوَّةٍ وَّمِنْ ر

اللّٰهِ وَعَدُوَّكُمْ

Artinya: "Dan siapkanlah untuk menghadapi mereka kekuatan apa saja yang kamu sanggupi dan dari kuda-kuda yang ditambat untuk berperang (yang dengan persiapan itu) kamu menggentarkan musuh Allah dan musuhmu".[81]

Ayat ini mengajarkan pentingnya kesiapsiagaan dan strategi sebagai bentuk usaha menjaga keamanan.

Berbeda dengan hasil penelitian Setiawan dan Oktavia, yang menjelaskan bahwa kombinasi antara keamanan siber dan strategi manajemen risiko mampu menjelaskan hingga 61,3% variabel kepercayaan pengguna e-banking secara signifikan. Perbedaan hasil ini menunjukkan bahwa konteks lokal, tingkat literasi, serta peran nasabah sebagai pengguna aktif atau pasif sangat berpengaruh dalam membentuk kepercayaan.[82]

Berdasarkan uji F, variabel X1 dan X2 secara simultan tidak berpengaruh signifikan terhadap kepercayaan nasabah (Y), dengan nilai

[81] Kementerian Agama Republik Indonesia, Al-Qur'an dan Terjemahannya (Jakarta: Lajnah Pentashihan Mushaf Al-Qur'an, 2019), Q.S. Al-Anfāl [8]: 60.

[82] Setiawan dan Oktavia, "Pengaruh Keamanan Siber dan Strategi Manajemen Risiko",45

signifikansi 0,247 (> 0,05) dan R^2 hanya 1,5%. Artinya, variabel ancaman siber dan strategi mitigasi risiko hanya memberikan kontribusi kecil dalam membentuk kepercayaan nasabah, sementara faktor lain di luar model penelitian lebih dominan, seperti transparansi layanan, kualitas aplikasi BSI *Mobile*, dan kepuasan terhadap layanan bank. Hasil ini menunjukkan bahwa hipotesis 3 ditolak, berbeda dengan penelitian Setiawan & Oktavia yang membuktikan adanya pengaruh simultan keamanan siber dan mitigasi risiko terhadap kepercayaan pengguna *e-banking* sebesar 61,3%. Oleh karena itu, penelitian selanjutnya disarankan menambahkan variabel lain yang lebih relevan dalam menjelaskan kepercayaan nasabah perbankan digital.

BAB V

PENUTUP

A. Kesimpulan

Berdasarkan hasil penelitian mengenai Pengaruh Ancaman Siber dan Strategi Mitigasi Risiko terhadap Kepercayaan Nasabah Bank Syariah Indonesia (BSI) pada mahasiswa penerima KIP-K IAIN Curup, maka dapat disimpulkan hal-hal sebagai berikut:

1. Ancaman Siber tidak berpengaruh signifikan terhadap kepercayaan nasabah. Berdasarkan hasil uji t, diperoleh nilai signifikansi sebesar 0,192 (> 0,05) dan nilai t hitung sebesar 1,310 (< t tabel 1,973), sehingga Ha ditolak dan Ho diterima. Artinya, persepsi mahasiswa terhadap ancaman siber yang pernah terjadi pada BSI tidak secara langsung memengaruhi kepercayaan mereka sebagai nasabah. Hal ini menunjukkan bahwa kepercayaan nasabah relatif stabil meskipun terdapat insiden siber, kemungkinan karena keterbatasan pilihan layanan bank atau literasi digital yang masih rendah.
2. Strategi Mitigasi Risiko juga tidak berpengaruh signifikan terhadap kepercayaan nasabah. Hasil uji t menunjukkan nilai signifikansi sebesar 0,367 (> 0,05) dan nilai t hitung sebesar -0,905 (< t tabel 1,973), maka Ha ditolak dan Ho diterima. Hal ini menunjukkan bahwa meskipun BSI telah menerapkan berbagai upaya mitigasi risiko, seperti otentikasi ganda dan pembaruan sistem, persepsi nasabah terhadap efektivitas strategi tersebut belum cukup kuat untuk meningkatkan kepercayaan secara signifikan.

3. Ancaman Siber dan Strategi Mitigasi Risiko secara simultan tidak berpengaruh signifikan terhadap kepercayaan nasabah. Hasil uji F menunjukkan nilai F hitung sebesar 1,409 < F tabel sebesar 3,05 dan nilai signifikansi sebesar 0,247 (> 0,05), maka Ho diterima. Artinya, kedua variabel bebas secara bersama-sama tidak memiliki pengaruh signifikan terhadap tingkat kepercayaan nasabah terhadap BSI.

B. Saran

Berdasarkan hasil penelitian yang telah dilakukan mengenai pengaruh ancaman siber dan strategi mitigasi risiko terhadap kepercayaan nasabah bank syariah indonesia, maka peneliti mengajukan saran sebagai berikut:

1. Bagi Bank Syariah Indonesia (BSI):

   Perlu dilakukan pendekatan yang lebih transparan dan komunikatif dalam memberikan informasi kepada nasabah mengenai sistem keamanan digital yang diterapkan. Selain itu, bank perlu mengintensifkan edukasi kepada nasabah, terutama generasi muda, mengenai pentingnya keamanan informasi digital.

2. Bagi Mahasiswa dan Nasabah BSI:

   Diharapkan meningkatkan literasi digital serta kewaspadaan terhadap potensi ancaman siber. Nasabah juga sebaiknya aktif mengikuti informasi kebijakan keamanan dari pihak bank agar dapat mengambil tindakan preventif dalam menjaga keamanan data pribadi.

3. Bagi Peneliti Selanjutnya:

Penelitian ini hanya terbatas pada mahasiswa penerima KIP-K di IAIN Curup sebagai responden. Penelitian selanjutnya disarankan untuk memperluas cakupan populasi dan menambahkan variabel lain seperti transparansi layanan, kemudahan akses aplikasi, atau kepuasan pelanggan untuk mendapatkan gambaran yang lebih komprehensif tentang faktor-faktor yang memengaruhi kepercayaan nasabah terhadap perbankan digital syariah.

DAFTAR PUSTAKA

Buku:

Al-Qur'an, QS. An-Nisa [4]: 58 (Kementerian Agama Republik Indonesia, Mushaf Al-Qur'an Standar Indonesia, Jakarta: Lajnah Pentashihan Mushaf Al-Qur'an, 2019)

Arikunto Suharsimi, Prosedur Penelitian: Suatu Pendekatan Praktik (Jakarta: Rineka Cipta, 2013), 245.

Budiyanto, Pengantar Cybercrime Dalam Sistem Hukum Pidana di Indonesia (Jakarta Press: Sada Kurnia Pustaka, 2022).

Ghozali Imam, Desain Penelitian Kuantitatif dan Kualitatif untuk Akademisi, Bisnis, dan Ilmu Sosial lainnya (Semarang: Yoga Pratama, 2013).

Hillson David, Effective Opportunity Management for Projects: Exploiting Positive Risk (New York: CRC Press, 2023).

Indah Mawarni, et.al. Manajemen Risiko (Sumatera Barat: CV. Gita Lentera, 2024).

Kementerian Agama Republik Indonesia. Al-Qur'an dan Terjemahannya. Jakarta: Lajnah Pentashihan Mushaf Al-Qur'an, 2019.

M. Kshetri, The Global Cybercrime Industry: Economic, Institutional and Strategic Perspectives (Berlin: Springer, 2022).

Muhammad Ramdhan, Metode Penelitian (Jakarta: Cipta Media Nusantara, 2021).

Sandi Kurnia, et.al, Tutorial PHP Machine Learning Menggunakan Regresi Linear Berganda Pada Aplikasi Bank Sampah Istimewa Versi 2.0 Berbasis Web (Bandung: Kreatif Industri Nusantara, 2020).

Sugiyono, Metode Penelitian Kuantitatif (Bandung: Alfabeta, 2022).

Sugiyono, metode penelitian kuantitatif, kualitatif, dan R&D (Bandung: Alfabeta, 2022).

Sugiyono dan Agus Susanto, Cara Mudah Belajar SPSS & LISREL Teori dan Aplikasi untuk Analisis Data Penelitian (Bandung: Alfabeta, 2015).

Sugiyono. Metode Penelitian Kuantitatif, Kualitatif, dan R&D. Bandung: Alfabeta, 2019.

Suhadi dan Siti Mudrika Zein, Path Analysis Faktor Dominan Penentu Rasa Percaya Diri Teori dan Riset (Malang: CV. Literasi Nusantara Abaddi, 2022).

Syafrida Hafni Sahir, Metode Penelitian, ed. Try Koryati, 1st ed (Jawa Timur: KBM Indonesia, 2020–2022).

Jurnal:

Agustina Nani, "Mengukur Kualitas Layanan Sistem Informasi Akademik pada SMP Uswatun Hasanah Jakarta," Paradigma 19, no. 1 (April 2017): 61–68

Alhassan, Abdul, and Robert Aryeetey Aryekum. "Cybersecurity in Islamic Banking: A Review of the Literature." Journal of Islamic Banking and Finance, 2020: 1–12.

Alhassan, Abdul, et al. "Cybersecurity Threats in the Banking Sector: A Review." International Journal of Computer Applications, 2020: 975–7.

Anindyaa, Tabina Dea. "Edukasi Bahaya Social Engineering Menggunakan Media Belajar Quizizz untuk Meningkatkan Kesadaran Keamanan Informasi Nasabah Perbankan." Jurnal 4, no. 3 (2023).

Rian, Dwi Hapsari. "Ancaman Cybercrime di Indonesia: Sebuah Tinjauan Pustaka Sistematik." Jurnal 5, no. 1 (2023).

Ginanjar. "Strategi Indonesia Membentuk Cyber Security dalam Menghadapi Ancaman Cyber Crime Melalui Badan Siber dan Sandi Negara." Jurnal 7, no. 2 (2022).

Gupta, B., et al. “Impact of Cyber Security on Customer Trust in Banking Sector.” International Journal of Bank Marketing 37, no. 5 (2021): 1123–1138.

Hillson, David. “Extending the Risk Management Process to Manage Opportunities.” International Journal of Project Management (2023): 235–240. Lubis Akromi, et.al, 2024. “Pengaruh Persepsi Keamanan dan Kepercayaan Terhadap Loyalitas Nasabah: Studi Kasus Serangan Siber di Bank Syariah Indonesia.”

Lubis, Z., & Lubis, A. F. (2024). Pengaruh persepsi keamanan dan kepercayaan terhadap loyalitas nasabah: Studi kasus serangan siber di Bank Syariah Indonesia. Jurnal Ekonomi dan Keuangan Islam, 5(7).

Mayer, R. C., Davis, J. H., & Schoorman, F. D. (1995). An integrative model of organizational trust. Academy of Management Review, 20(3), 709–734.

Moorman, C., Zaltman, G., & Deshpandé, R. (1992). Relationships between providers and users of market research: The dynamics of trust within and between organizations. Journal of Marketing Research, 29(3), 314–328.

Kshetri, N. (2022). Cybersecurity in the financial sector: A global perspective. Journal of Financial Crime, 24(4), 564–577.

Prasmono, P., et al. (2021). Analisis regresi berganda pada faktor-faktor yang mempengaruhi kinerja fisik preservasi jalan dan jembatan di Provinsi Sumatera Selatan. Emerging Statistics and Data Science Journal, 1.

Setiawan, A., & Oktavia, N. (2023). Pengaruh keamanan siber dan strategi manajemen risiko terhadap kepercayaan pengguna e-banking. Jurnal Manajemen dan Teknologi Informasi, 12(1), 45–59.

Arivianingsi, S., et al. (2023). Korelasi kejahatan siber dengan percepatan digitalisasi di Indonesia. Vol. 1(1).

Wilda, Y. R. (2023). Pengaruh kemampuan manajerial, literasi keuangan, dan mitigasi risiko terhadap keberlangsungan usaha UMKM. Jurnal Ilmu Manajemen, Ekonomi, dan Kewirausahaan, 1(1).

Skripsi:

Kusuma Bakti Danang, 2025. "Studi Indigenous Trust to Leader pada Karyawan Jawa" (Skripsi: Universitas Negeri Semarang, 2013).

Website:

Al-Qur'an, QS. An-Nisa: 58.

Bank Syariah Indonesia. Laporan Tahunan Bank Syariah Indonesia 2021–2023. Jakarta: BSI Press, 2024.

Miftahul Janna Nilda dan Herianto. "Konsep Uji Validitas dan Reliabilitas dengan Menggunakan SPSS." Preprint (Open Science Framework), 2021. https://doi.org/10.31219/osf.io/v9j52

Otoritas Jasa Keuangan (OJK). "Sejarah Perbankan Syariah." OJK.

Otoritas Jasa Keuangan (OJK). Data Statistik Perbankan Syariah dan Laporan Industri Triwulan I 2024. Diakses 25 Mei 2025. https://www.ojk.go.id

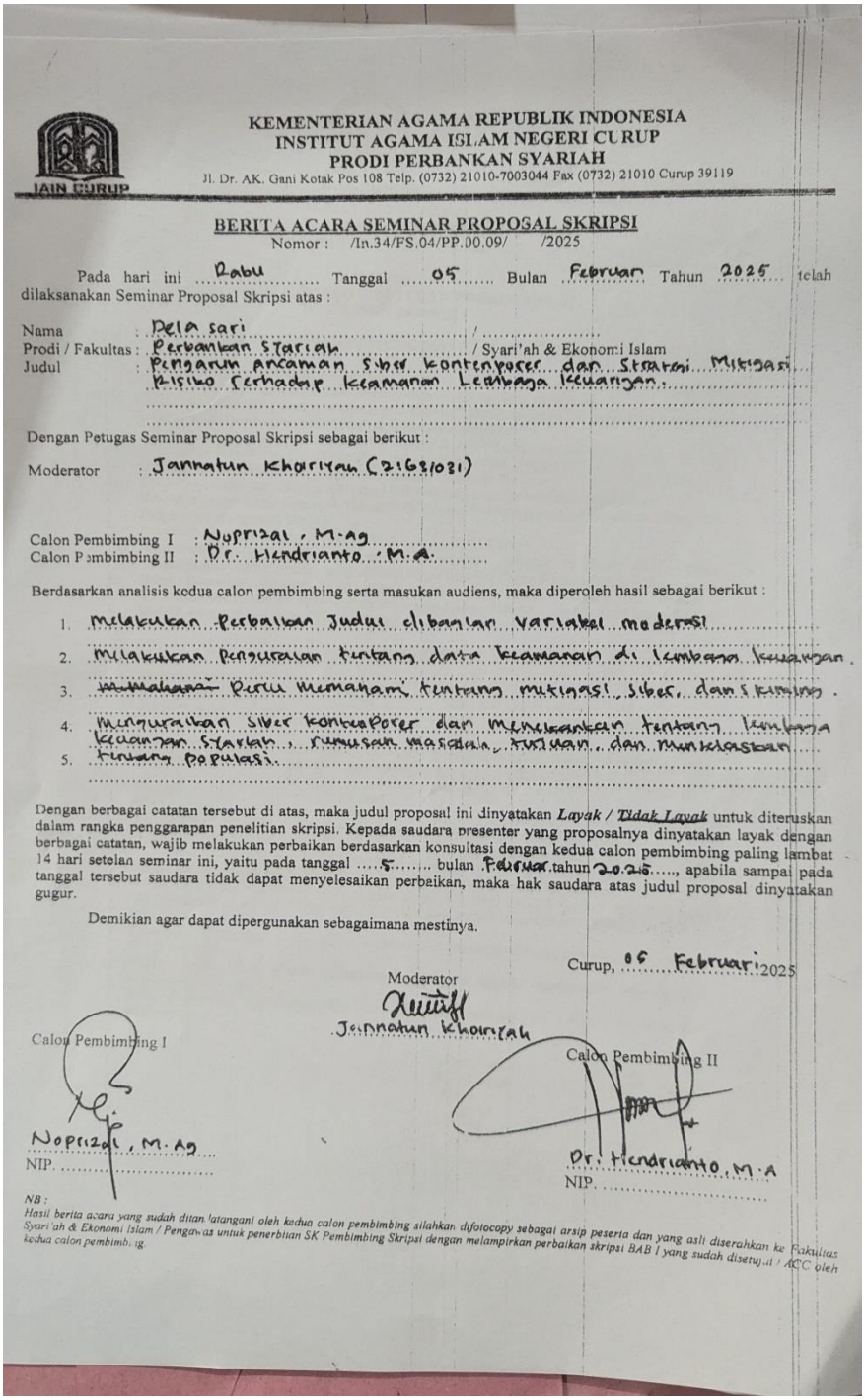
Prasmoro Putri, et al., dan Aulia Rahma. "Penerapan Sistem Manajemen Mutu ISO 9001:2008 Terhadap Realisasi Produk Beton Ready Mix di PT SCG Jayamix." ESDS, vol. 1, no. 1 (2008). https://doi.org/10.20885/esds.vol1.iss1.art6

Suharsimi Arikanto, Prosedur Penelitian: Suatu Pendekatan Praktik (Jakarta: Rineka Cipta, 2013), 183

Umar, Husein, Metode Penelitian untuk Skripsi dan Tesis Bisnis (Jakarta: Raja Grafindo Persada, 2003), 108

L
A
M
P
I
R
A
N

Lampiran 1. Berita Acara Seminar Proposal Skripsi



KEMENTERIAN AGAMA REPUBLIK INDONESIA
INSTITUT AGAMA ISLAM NEGERI CURUP
PRODI PERBANKAN SYARIAH
Jl. Dr. AK. Gani Kotak Pos 108 Telp. (0732) 21010-7003044 Fax (0732) 21010 Curup 39119

BERITA ACARA SEMINAR PROPOSAL SKRIPSI
Nomor : /In.34/FS.04/PP.00.09/ /2025

Pada hari ini Rabu Tanggal 05 Bulan Februari Tahun 2025 telah dilaksanakan Seminar Proposal Skripsi atas :

Nama : Dela sari
Prodi / Fakultas : Perbankan Syariah / Syari'ah & Ekonomi Islam
Judul : Pengaruh ancaman siber kontemporer dan Strategi Mitigasi Risiko terhadap keamanan Lembaga keuangan.

Dengan Petugas Seminar Proposal Skripsi sebagai berikut :

Moderator : Jannatun khairiyah (21631031)

Calon Pembimbing I : Nuprizal, M.Ag
Calon Pembimbing II : Dr. Hendrianto, M.A.

Berdasarkan analisis kedua calon pembimbing serta masukan audiens, maka diperoleh hasil sebagai berikut :

1. Melakukan Perbaikan Judul dibagian variabel moderasi
2. Melakukan Pengutaian tentang data keamanan di lembaga keuangan
3. Mahasiswa perlu memahami tentang mitigasi, siber, dan strategi.
4. Menguraikan siber kontemporer dan menjelaskan tentang lembaga keuangan syariah, rumusan masalah, tujuan, dan manfaatnya
5. tentang populasi.

Dengan berbagai catatan tersebut di atas, maka judul proposal ini dinyatakan ***Layak / Tidak Layak*** untuk diteruskan dalam rangka penggarapan penelitian skripsi. Kepada saudara presenter yang proposalnya dinyatakan layak dengan berbagai catatan, wajib melakukan perbaikan berdasarkan konsultasi dengan kedua calon pembimbing paling lambat 14 hari setelan seminar ini, yaitu pada tanggal ....5..... bulan Februari tahun 2025....., apabila sampai pada tanggal tersebut saudara tidak dapat menyelesaikan perbaikan, maka hak saudara atas judul proposal dinyatakan gugur.

Demikian agar dapat dipergunakan sebagaimana mestinya.

Curup, 05 Februari 2025

Moderator

Jannatun khairiyah

Calon Pembimbing I

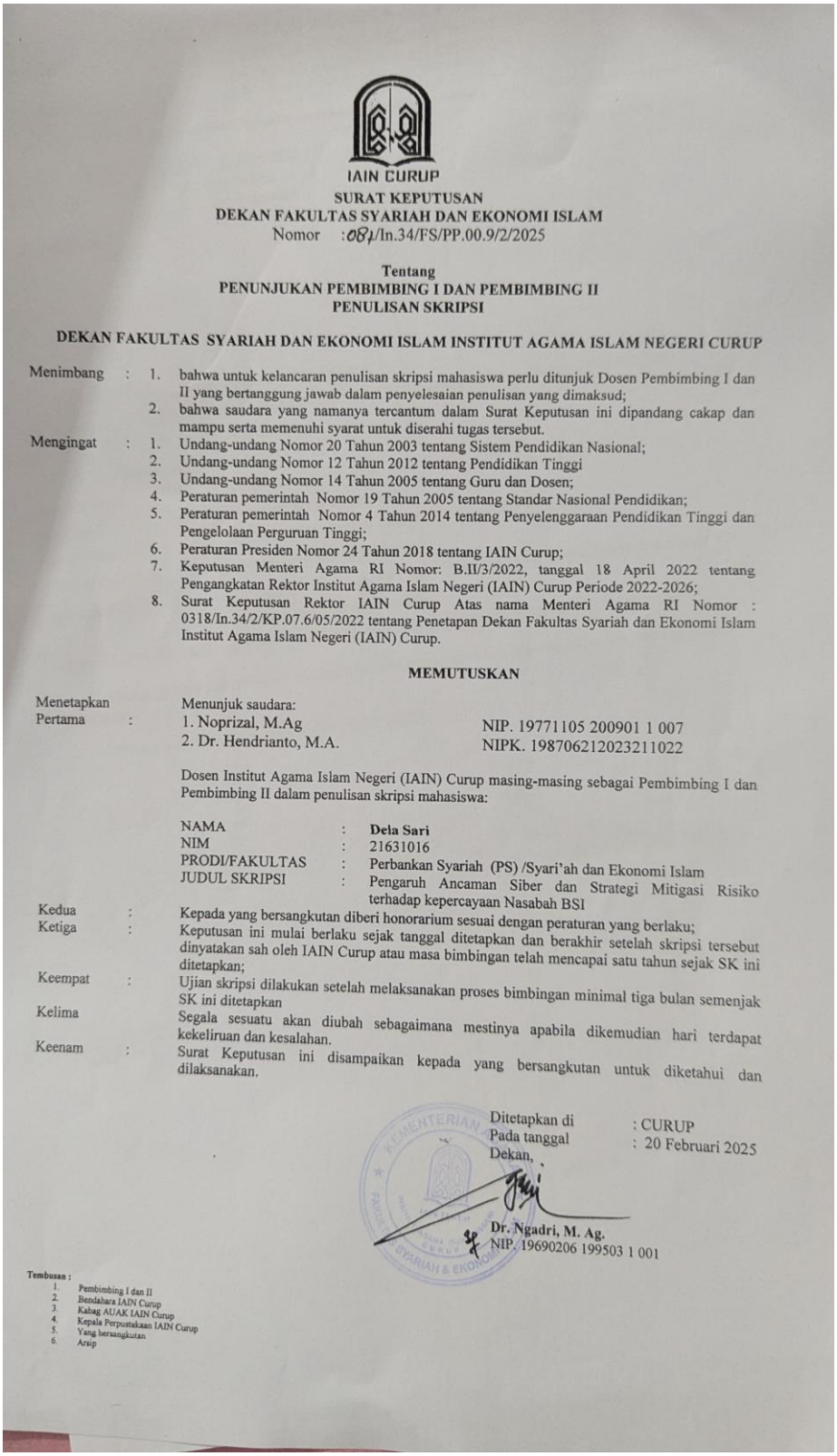
Nuprizal, M.Ag
NIP. .....

Calon Pembimbing II

Dr. Hendrianto, M.A
NIP. .....

NB :
Hasil berita acara yang sudah ditandatangani oleh kedua calon pembimbing silahkan difotocopy sebagai arsip peserta dan yang asli diserahkan ke Fakultas Syari'ah & Ekonomi Islam / Pengawas untuk penerbitan SK Pembimbing Skripsi dengan melampirkan perbaikan skripsi BAB I yang sudah disetujui / ACC oleh kedua calon pembimbing.

Lampiran 2. SK Pembimbing



IAIN CURUP

SURAT KEPUTUSAN
DEKAN FAKULTAS SYARIAH DAN EKONOMI ISLAM
Nomor :081/In.34/FS/PP.00.9/2/2025

Tentang
PENUNJUKAN PEMBIMBING I DAN PEMBIMBING II
PENULISAN SKRIPSI

DEKAN FAKULTAS SYARIAH DAN EKONOMI ISLAM INSTITUT AGAMA ISLAM NEGERI CURUP

Menimbang :
1. bahwa untuk kelancaran penulisan skripsi mahasiswa perlu ditunjuk Dosen Pembimbing I dan II yang bertanggung jawab dalam penyelesaian penulisan yang dimaksud;
2. bahwa saudara yang namanya tercantum dalam Surat Keputusan ini dipandang cakap dan mampu serta memenuhi syarat untuk diserahi tugas tersebut.

Mengingat :
1. Undang-undang Nomor 20 Tahun 2003 tentang Sistem Pendidikan Nasional;
2. Undang-undang Nomor 12 Tahun 2012 tentang Pendidikan Tinggi
3. Undang-undang Nomor 14 Tahun 2005 tentang Guru dan Dosen;
4. Peraturan pemerintah Nomor 19 Tahun 2005 tentang Standar Nasional Pendidikan;
5. Peraturan pemerintah Nomor 4 Tahun 2014 tentang Penyelenggaraan Pendidikan Tinggi dan Pengelolaan Perguruan Tinggi;
6. Peraturan Presiden Nomor 24 Tahun 2018 tentang IAIN Curup;
7. Keputusan Menteri Agama RI Nomor: B.II/3/2022, tanggal 18 April 2022 tentang Pengangkatan Rektor Institut Agama Islam Negeri (IAIN) Curup Periode 2022-2026;
8. Surat Keputusan Rektor IAIN Curup Atas nama Menteri Agama RI Nomor : 0318/In.34/2/KP.07.6/05/2022 tentang Penetapan Dekan Fakultas Syariah dan Ekonomi Islam Institut Agama Islam Negeri (IAIN) Curup.

MEMUTUSKAN

Menetapkan
Pertama : Menunjuk saudara:
1. Noprizal, M.Ag — NIP. 19771105 200901 1 007
2. Dr. Hendrianto, M.A. — NIPK. 198706212023211022

Dosen Institut Agama Islam Negeri (IAIN) Curup masing-masing sebagai Pembimbing I dan Pembimbing II dalam penulisan skripsi mahasiswa:

NAMA	:	**Dela Sari**
NIM	:	21631016
PRODI/FAKULTAS	:	Perbankan Syariah (PS) /Syari'ah dan Ekonomi Islam
JUDUL SKRIPSI	:	Pengaruh Ancaman Siber dan Strategi Mitigasi Risiko terhadap kepercayaan Nasabah BSI

Kedua : Kepada yang bersangkutan diberi honorarium sesuai dengan peraturan yang berlaku;
Ketiga : Keputusan ini mulai berlaku sejak tanggal ditetapkan dan berakhir setelah skripsi tersebut dinyatakan sah oleh IAIN Curup atau masa bimbingan telah mencapai satu tahun sejak SK ini ditetapkan;
Keempat : Ujian skripsi dilakukan setelah melaksanakan proses bimbingan minimal tiga bulan semenjak SK ini ditetapkan
Kelima : Segala sesuatu akan diubah sebagaimana mestinya apabila dikemudian hari terdapat kekeliruan dan kesalahan.
Keenam : Surat Keputusan ini disampaikan kepada yang bersangkutan untuk diketahui dan dilaksanakan.

Ditetapkan di : CURUP
Pada tanggal : 20 Februari 2025
Dekan,

Dr. Ngadri, M. Ag.
NIP. 19690206 199503 1 001

Tembusan :
1. Pembimbing I dan II
2. Bendahara IAIN Curup
3. Kabag AUAK IAIN Curup
4. Kepala Perpustakaan IAIN Curup
5. Yang bersangkutan
6. Arsip

Lampiran 3. Angket Penelitian

KUESINONER PENELITIAN
PENGARUH ANCAMAN SIBER DAN STRATEGI MITIGASI RISIKO TERHADAP KEPERCAYAAN NASABAH BANK SYARIAH INDONESIA

Dalam rangka penyusunan skripsi. Saya Dela Sari NIM. 21631016 bermaksud melakukan penelitian ilmiah untuk penyusunan skripsi dengan judul "Pengaruh Ancaman Siber dan Strategi Mitigasi Risiko Terhadap Kepercayaan Nasabah Bank Syariah Indonesia". sehubung dengan hal tersebut, saya sangat mengharapkan kesediaan saudara/i untuk meluangkan waktunya sejenak untuk mengisi beberapa pertanyaan pada kuisioner ini.

Atas perhatian dan kerja samanya, saya ucapkan terima kasih.

Nama :
NIM :
Angkatan :

Petunjuk pengisian:

Silakan berikan penilaian Anda terhadap setiap pernyataan berikut sesuai dengan kondisi yang Anda rasakan saat ini, dengan skala sebagai berikut:

1 = Sangat Tidak Setuju
2 = Tidak Setuju
3 = Netral
4 = Setuju
5 = Sangat Setuju

DAFTAR PERTANYAAN:

No.	Pernyataan	Alternatif Jawaban				
	Ancaman siber (X1)	**STS**	**TS**	**N**	**S**	**SS**
1.	**Kekhawatiran nasabah atas serangan siber**					
1.	Saya khawatir data pribadi saya dapat diretas atau dicuri saat menggunakan layanan digital BSI.					
2.	Saya khawatir transaksi online saya di BSI bisa menjadi sasaran kejahatan digital seperti phishing atau penipuan.					
3.	Saya merasa khawatir jika BSI menjadi target serangan siber seperti bank lainnya.					
2.	**Persepsi terhadap keamanan dan perlindungan BSI**					
1.	Saya semakin ragu menggunakan layanan digital BSI setelah mendengar isu keamanan siber.					
2.	Menurut saya, perlindungan BSI terhadap serangan siber dalam transaksi nasabah masih perlu ditingkatkan.					
3.	Isu keamanan siber memengaruhi rasa percaya saya saat menggunakan layanan digital BSI.					
3.	**Pengetahuan atau informasi terkait serangan siber**					
1.	Saya pernah mendengar kasus kebocoran data pada layanan bank digital termasuk BSI.					

2.	Saya sering mendapatkan informasi dari media atau sumber lain tentang serangan siber yang menyerang bank.					
3.	Saya mengetahui bahwa BSI pernah menjadi target serangan siber.					
	Strategi Mitigasi Risiko (X2)					
1.	**Edukasi dan komunikasi dari BSI**					
1.	Saya pernah menerima sosialisasi atau edukasi dari BSI mengenai cara melindungi akun dari serangan siber.					
2.	BSI secara rutin mengirimkan informasi keamanan digital melalui media resmi (seperti SMS, email, atau aplikasi).					
3.	Saya pernah menerima pemberitahuan resmi dari BSI ketika terjadi insiden keamanan digital.					
2.	**Fitur keamanan dan bantuan**					
1.	Saya mengetahui bahwa BSI menyediakan autentikasi dua faktor (2FA) pada BSI Mobile untuk melindungi akun nasabah.					
2.	BSI menyediakan layanan bantuan yang cepat jika nasabah mengalami kebocoran data atau akses ilegal.					
3.	Saya merasa nyaman menggunakan layanan BSI Mobile karena adanya perlindungan terhadap virus dan malware.					
3.	**Sistem keamanan dan transparansi**					
1.	Saya yakin BSI memiliki tim keamanan TI yang aktif dan siaga untuk menangani ancaman siber.					
2.	Saya merasa BSI bersikap terbuka dan transparan ketika menghadapi pelanggaran keamanan digital.					
3.	Saya memahami langkah-langkah yang dilakukan BSI dalam menangani insiden keamanan siber.					
	Kepercayaan Nasabah (Y)					
1.	**Rasa aman menggunakan layanan**					
1.	Saya merasa aman menggunakan teknologi digital BSI untuk mengakses dan melakukan transaksi keuangan.					
2.	Saya merasa aman saat menggunakan aplikasi atau layanan digital BSI.					
3.	Saya puas dengan tingkat keamanan dalam layanan digital BSI.					
2.	**Persepsi terhadap kemampuan BSI menangani ancaman**					
1.	Saya yakin BSI mampu mengantisipasi dan menangani ancaman siber.					
2.	Saya percaya BSI memiliki komitmen yang tinggi dalam menjaga keamanan data nasabah.					
3.	Saya yakin BSI terus meningkatkan teknologinya agar mampu menghadapi ancaman keamanan digital terbaru.					

3.	**Loyalitas dan rekomendasi**					
1.	Saya yakin BSI akan terus meningkatkan sistem keamanannya.					
2.	Saya akan terus menggunakan layanan digital BSI karena merasa aman dan nyaman.					
3.	Saya merekomendasikan BSI kepada orang lain karena kepercayaannya terhadap keamanan.					

Lampiran 4. Data Responden

No.	Nama	NIM	Angkatan
1.	Dewi Lestari	22531018	2022
2	Rivan afriansyah	22531027	2022
3	Indriana farah azizah	23541010	2023
4	Lisna Ariani	23551035	2023
5	Lili Zakia	22531079	2022
6	Aji Pangestu	23541029	2023
7	Ade Akbar AS	22591001	2022
8	Adli andesta	22561002	2022
9	Berliana Azizah	22531027	2022
10	Rangga pranata	22631054	2022
11	Ali Akbar	22651001	2022
12	Amirul Alen Gymnastiar	22631007	2022
13	Azizah Dwi pahrezq	22621004	2022
14	Amrina rosada	22541001	2022
15	Budiman shaleh	22531028	2022
16	Tria ananta	22541031	2022
17	Andi Wijaya	22621001	2022
18	Bunga monica	22531029	2022
19	Daniel febriyan	22521005	2022
20	Dedek kurniasih	22561014	2022
21	Anish Fitriani	22591018	2022
22	Bunga valentina	22631014	2022
23	Delfi Rara anjeska	22551009	2022
24	Chika Febriana	22601001	2022
25	Annisa Yunara	22631009	2022
26	Delta vistoria	22511005	2022
27	Deni supriadi	22541007	2022
28	Ahmat Purnomo	22671001	2022
29	Rizki putri	22631062	2022
30	Ariansa	22621002	2022
31	Muhammad Adi Saputra	22621023	2022
32	Lusiyani	22591118	2022
33	Nabila	22541016	2022

34	M. Edio Alfian Prayoga	22641022	2022
35	Nadia permata Sari	22531099	2022
36	Marimbi Putri	22531088	2022
37	Nadia Ramadani	22691012	2022
38	Mayang Sari	22591126	2022
39	Nesha ramawani	22591140	2022
40	Puji Rahayu	22661016	2022
41	Novia Rapika Nanda	22591146	2022
42	Putri Dhea Ananda	22591150	2022
43	Putri dilpasari	22591151	2022
44	Novri Yunita	22571008	2022
45	Nurul Arysha	22541019	2022
46	Putri Setiawati	22691014	2022
47	Sulaiman Ajo Wijoyo	22531141	2022
48	Vioni Cahya mutiara	22551056	2022
49	Syari Fatul Latifah	22531144	2022
50	Wahyu Nova andria	22561045	2022
51	Tamara Jesica Dwi	22561043	2022
52	Weli yanzi	22631077	2022
53	Tasya Adelina	22631072	2022
54	Aisyah amini	23591004	2023
55	Alin Alda rinda	23591008	2023
56	Lala Nabila Utami	23671033	2023
57	Cepi mariska	23531020	2023
58	Gilang Arianto	22681015	2022
59	Japar	22641019	2022
60	Nada azara	23591106	2023
61	Selpi yanti	23671057	2023
62	Riski karunia illahi	23671056	2023
63	Vivi hafizza	23511026	2023
64	Syari padila	23531145	2023
65	Syauqi Ilham lubis	23601014	2023
66	Tia Kartika	23531148	2023
67	Walyol azim	23531158	2023
68	Reta balkis	22661020	2022
69	Sinta hairani	22661022	2022
70	Zeni leony putri b	22671053	2022
71	Abid nayyiro firel	23571001	2023
72	Ayu lolita sari	23671010	2023
73	Dio sirindang	23531032	2023
74	Hansdewi kusrindi antika	23591069	2023
75	Eki dwijaya	23591051	2023
76	Annisa layinnatul arifah	23621008	2023

77	Apita Wulansari	23631009	2023
78	Pitrianah	22541021	2022
79	Reni Diana Larasati	22551042	2022
80	Amrullah	23521004	2023
81	Anggun nerdiyani	23591016	2023
82	Anis Fitria khalis	23681011	2023
83	DIYE ALPAYAT	22691005	2022
84	Zhava zhavira ramadhania	23591206	2023
85	Yuliza Aidil Fitri	23621042	2023
86	Wela aulia	23551016	2023
87	Vina sari	23631069	2023
88	Tiara utari	23561064	2023
89	Tedi ivandri	23641018	2023
90	Suro warsito	23671061	2023
91	Sri alnisa	23631026	2023
92	Jastra ningrat atmaja	23521015	2023
93	Sanu vera	23541031	2023
94	Okti zuleni sari	23531106	2023
95	Reza ravika	22671039	2022
96	Dewi Aqilah	22531036	2022
97	Duwi agustari	22671014	2022
98	Fahmi alfarissi	22551017	2022
99	Ernis Oktavia	22591064	2022
100	Firdaus	22541011	2022
101	Yola monicha	22531162	2022
102	Yupi Dwi rani	22641038	2022
103	Anggun anggrea	23591014	2023
104	Andini Agnes Safitri	23561003	2023
105	Carissa	23551014	2023
106	Cristin letavia	23561009	2023
107	Dea afrianti	23561011	2023
108	Deka yunara	23657002	2023
109	Hikmatul mahpiro	23561022	2023
110	Helena Salsabilah	23591010	2023
111	Honik sahiron	23531054	2023
112	Ika Septi oktaviana	23641013	2023
113	Kiki lestari	23591083	2023
114	Leni Rahmawati	23521017	2023
115	Marsya intan ayu	23681038	2023
116	Masya sindiati	23591092	2023
117	Mahages sholiwa	23631037	2023
118	Milsa alvina	23511020	2023
119	Nabila iswandari	23531093	2023

120	Nadiatul fiqri	23541021	2023
121	Rezen prima Saputra	23521024	2023
122	Eggen gustina	22591057	2022
123	Remil yuliana	22531116	2022
124	Gustiantara	22551019	2022
125	Kurnia Amanda Putri	22591109	2022
126	Laita Aprilia	22531077	2022
127	Yaumatuz zulaiha	22591211	2022
128	Windri asmeily	22521035	2022
129	Fra fela hernindah	22521014	2022
130	Genta putri roliansi	22691024	2022
131	Exti Hendri Effendi	22671017	2022
132	Yudha Adi Setiawan	22601008	2022
133	Dhani noveleo alfarez	22531039	2022
134	Erdo Febri jeksen	22681015	2022
135	Halima tus'adia	22531064	2022
136	Gusmani sagian	22561022	2022
137	Tri Cindy prescelia	23591176	2023
138	Via Desi Puspita Sari	23631068	2023
139	Vina sari	23631069	2023
140	Vira Bella nur novriyantika	23531157	2023
141	Wahyu kristianto	23621040	2023
142	zelika ramadina	23531168	2023
143	sela fitria haryani	22631065	2022
144	lira mariska	22591115	2022
145	chika febriana	22601001	2022
146	dia anggil lia	22601001	2022
147	Fauziah tur rahmi	22511008	2022
148	Mira Mayang Sari	22691011	2022
149	Raju Ardiansyah	22661018	2022
150	Raja Arda mahendra	22521027	2022
151	delvi sari margareta	22571003	2022
152	dwi agustari	22671014	2022
153	ainin fadhila	23671003	2023
154	alisya riski anatasya	23671005	2023
155	ananda melisa briliant	23561002	2023
156	Thaharah nur aini	23591171	2023
157	Syerli Agnes dwiviola	23561062	2023
158	Surchi Kurnia sari	23561061	2023
159	Sangkutmi	23691015	2023
160	Rene finka A Lulu	23641023	2023
161	Rahmi eflia Agustina	23591133	2023
162	Reke ayu Ningrum	23531116	2023

163	Pandi Saputra	23531107	2023
164	Nurpaizah	23591120	2023
165	Padeli Ari tunang	23681047	2023
166	Nur sasi Septian rani	23621031	2023
167	Nova	23551046	2023
168	Naufal Ardiansyah	23551045	2023
169	Mukhlis Apriansyah	23671041	2023
170	Jesi nuraini	22551021	2022
171	Rani martina	22531113	2022
172	Dwicha putri Okta fhadilla	22511007	2022
173	Tamara Jesica Dwi L	22561043	2022
174	Riska neri julianti	22591174	2022
175	Septa Sindi laura	22701013	2022
176	Nabila Putri maeza	22541016	2022
177	Lira mariska	22591115	2022
178	Gita yulia	22691007	2022
179	Ferdis pernandes	22531056	2022
180	Ariansa	22621002	2022
181	Ahmad Dwi Apriansyah	22631002	2022
182	Alifah Egi anindyah	23551003	2023
183	Andreza Saputra	23531009	2023
184	Anggun nerdiyani	23591016	2023
185	Annisa	23541003	2023
186	Arranty vadialova	23631010	2023
187	Cici arzeti	23531021	2023

Lampiran 5. Jawaban Responden

Variabel X1. Ancaman Siber

X1.1	X1.2	X1.3	X1.4	X1.5	X1.6	X1.7	X1.8	X1.9
3	1	2	4	3	1	2	5	5
1	1	2	4	3	1	1	5	5
3	2	4	4	4	3	2	4	4
3	3	2	5	2	2	2	4	4
2	2	3	5	2	3	3	5	4
3	3	4	3	4	3	4	4	3
4	3	2	5	3	4	2	1	3
4	2	5	2	3	4	4	5	3
4	1	3	5	5	3	2	4	3
5	4	2	2	2	3	4	4	2
4	2	5	4	4	4	3	5	3
2	3	4	5	2	1	3	3	4
3	3	3	4	3	3	3	3	3
5	4	2	3	1	3	3	3	4

3	4	3	4	5	3	5	4	3
3	4	5	4	5	3	4	5	4
4	2	3	5	4	4	3	4	4
3	3	3	3	4	3	4	3	4
2	3	4	5	2	1	3	3	4
3	3	3	4	3	3	3	3	3
5	4	2	3	1	3	3	3	4
3	4	3	4	5	3	5	4	3
3	4	5	4	5	3	4	5	4
4	2	3	5	4	4	3	4	4
3	3	3	3	4	3	4	3	4
3	4	5	3	4	5	5	4	3
3	4	3	5	4	3	4	4	5
4	4	3	4	3	4	3	4	5
4	5	3	4	3	2	5	4	4
4	3	3	3	3	3	5	4	4
2	3	4	4	4	4	3	4	3
3	4	5	3	4	5	3	5	4
4	5	4	3	5	4	3	5	4
3	3	3	4	2	4	4	5	5
3	2	3	3	4	5	4	3	2
2	1	3	3	2	3	5	3	3
3	4	3	4	5	3	4	5	3
2	3	3	5	3	3	2	4	3
3	4	5	4	4	4	3	3	4
1	3	2	4	3	3	2	4	5
3	4	5	3	4	5	4	3	5
1	2	2	3	3	2	3	3	5
4	5	3	4	5	3	4	5	3
2	3	2	4	2	3	2	3	4
3	4	5	3	3	4	5	3	5
4	5	3	3	2	4	5	3	4
2	2	3	4	3	2	3	4	3
3	4	5	4	3	2	3	3	4
4	5	3	4	5	3	4	5	4
1	2	3	3	2	3	2	4	4
2	3	2	3	3	3	3	4	5
4	3	2	5	5	4	5	4	3
2	3	2	2	3	2	3	3	4
3	4	5	3	2	4	3	5	4
2	2	1	1	3	2	3	4	4

4	3	5	4	3	2	4	3	5
1	2	3	3	3	2	3	4	4
4	3	5	4	3	5	3	5	3
1	1	2	3	2	3	2	4	3
3	4	5	4	3	2	4	3	4
4	3	4	5	3	4	5	3	3
3	4	4	3	2	4	5	3	4
4	3	5	4	3	5	3	4	4
3	5	4	4	5	3	5	4	3
3	4	5	3	4	5	3	4	5
3	4	5	3	4	5	4	3	5
3	4	3	4	5	3	3	4	3
3	2	4	4	4	3	3	4	5
4	3	5	3	4	4	3	4	5
3	4	5	4	3	2	3	3	4
3	4	3	4	5	4	3	4	5
3	3	4	4	5	3	4	5	4
3	3	3	4	5	4	3	4	5
3	4	3	3	4	5	4	4	3
3	4	4	3	5	4	4	3	4
3	4	5	4	3	3	4	4	3
3	3	4	3	4	5	4	3	4
3	4	5	4	3	4	3	5	4
4	3	4	4	3	4	3	4	4
3	4	3	4	4	3	4	3	4
3	4	4	3	4	5	4	3	3
3	4	4	5	3	3	4	3	3
3	4	4	5	2	3	3	4	4
4	3	2	3	3	4	2	3	4
3	4	3	4	5	2	2	3	4
3	1	1	3	3	4	5	4	3
3	1	2	3	4	5	3	4	3
1	1	1	3	4	3	5	4	3
2	1	2	3	2	2	3	4	3
1	2	3	4	3	2	3	4	5
3	3	2	2	4	3	4	5	5
4	3	5	4	3	5	4	3	3
5	4	3	4	3	2	5	4	3
5	2	5	4	4	2	3	3	4
5	5	4	5	4	3	4	5	3
3	3	4	4	5	3	4	5	3

4	4	3	3	4	5	4	3	3
4	2	3	3	3	4	5	4	3
2	2	3	3	3	3	4	4	3
5	5	5	5	3	3	3	5	4
3	3	3	3	3	4	5	3	4
4	3	5	4	3	4	3	3	4
5	5	4	5	4	5	4	5	3
3	4	5	4	3	4	2	3	4
2	5	4	3	4	4	2	3	4
5	5	5	4	3	3	1	4	4
5	2	5	4	3	4	5	4	3
3	3	3	4	4	4	3	5	3
5	5	4	4	3	3	4	2	3
4	3	3	4	4	3	1	3	3
3	1	4	3	3	3	1	3	4
4	3	3	3	4	3	3	4	4
3	3	4	4	5	5	4	3	5
5	3	5	5	5	3	1	5	4
2	3	4	3	3	4	1	4	4
3	4	5	4	4	5	3	3	4
4	4	4	4	3	3	1	3	4
5	5	4	4	4	3	2	4	3
3	4	4	5	3	3	1	4	3
3	3	3	4	4	4	2	5	4
4	3	3	4	3	3	1	4	4
2	3	4	4	3	3	4	3	5
2	3	3	3	4	3	1	3	4
3	3	4	3	4	3	4	4	4
2	3	2	4	3	5	4	4	3
4	3	5	4	3	2	1	4	3
3	3	5	4	3	3	2	4	3
4	3	3	4	5	4	3	4	3
4	3	3	5	4	3	3	4	4
4	3	4	4	3	4	5	3	4
5	3	4	3	4	5	4	3	5
3	3	4	5	3	3	1	3	4
3	3	4	4	4	5	5	3	4
4	3	4	3	5	4	3	5	4
5	3	3	4	3	3	2	3	4
4	4	3	3	3	4	5	4	5
5	4	3	3	4	3	5	3	4

3	4	4	3	5	3	4	3	4
5	4	3	3	3	3	1	4	4
3	4	3	3	4	4	3	4	4
4	3	4	3	4	4	3	5	4
3	4	3	4	5	4	3	4	3
4	3	4	5	4	3	4	5	4
4	3	3	3	4	3	1	4	4
3	4	3	3	4	3	4	5	4
3	4	3	4	3	3	2	4	3
3	4	3	4	5	4	3	4	5
4	3	5	4	3	3	1	3	4
1	2	4	3	3	4	4	4	3
5	3	4	3	4	5	4	3	5
4	3	4	5	4	3	4	3	3
3	3	3	4	3	3	4	3	3
3	4	3	4	4	3	1	3	3
5	4	3	4	5	4	4	3	3
3	4	5	4	3	5	4	3	5
4	4	4	3	3	3	2	4	3
4	3	3	4	3	3	2	4	3
3	3	4	4	3	4	4	5	4
4	3	3	4	4	3	2	3	4
3	4	3	4	3	4	1	3	4
5	3	4	3	3	3	2	3	4
4	3	3	4	5	3	3	3	3
3	4	4	3	3	3	4	4	5
4	4	3	4	3	3	1	4	3
3	4	4	3	4	5	4	3	4
5	3	4	3	3	4	4	5	5
4	3	5	4	3	3	2	3	3
3	4	3	4	3	4	3	4	4
4	3	5	4	4	3	5	4	3
5	3	5	4	5	3	4	3	4
4	4	5	5	3	4	4	3	5
5	4	5	4	3	3	4	3	3
5	4	3	4	3	4	5	3	4
5	4	4	3	4	4	5	3	3
4	3	3	4	3	3	4	5	3
5	3	4	4	3	4	4	4	3
5	4	5	4	3	3	2	4	3
4	3	5	4	3	3	1	3	4

4	3	4	5	3	3	2	4	3
5	3	4	4	3	3	5	4	3
3	3	4	4	3	3	4	4	3
5	3	4	4	3	3	4	4	3
5	3	4	4	3	3	4	4	3
5	3	4	3	3	3	4	5	4
5	3	4	4	3	3	4	4	3
5	3	4	4	3	4	4	3	4
5	3	4	4	3	3	4	4	3
5	3	4	4	3	3	4	4	3
4	3	3	4	3	3	4	4	3
5	3	4	4	3	3	4	4	3
5	3	4	4	3	3	4	4	4
4	4	4	4	3	3	3	4	3
4	3	4	4	3	3	2	4	3

Variabel X2. Strategi Mitigasi Risiko

X2.1	X2.2	X2.3	X2.4	X2.5	X2.6	X2.7	X2.8	X2.9
4	4	4	5	5	4	5	4	4
5	4	5	4	4	4	4	4	4
4	4	4	3	4	3	3	4	3
4	4	3	3	3	3	3	3	3
4	4	4	4	4	3	3	4	3
3	4	4	4	4	4	3	3	3
4	4	4	5	3	3	4	5	5
2	4	2	3	4	2	2	4	3
2	5	3	3	1	3	3	3	4
3	3	5	4	4	5	3	4	4
4	4	5	3	4	5	3	5	4
5	3	5	4	2	3	4	4	5
4	3	3	3	3	5	5	5	4
5	4	5	3	5	2	1	4	5
3	3	4	4	3	4	3	3	4
2	4	5	3	4	5	5	3	4
3	4	3	4	4	4	4	5	3
4	4	4	4	4	3	3	4	4
4	4	3	5	3	3	4	5	3
2	4	4	5	3	3	4	3	5
3	4	5	4	4	3	5	4	4
5	3	5	4	4	5	4	4	3
4	5	5	3	4	4	5	4	4

4	3	3	3	3	3	3	3	4
4	4	4	3	4	4	3	5	5
3	4	5	4	3	5	4	5	4
3	5	2	3	3	4	5	4	3
3	4	4	4	4	4	4	5	5
3	4	5	3	4	4	4	5	4
4	3	4	4	5	5	4	4	5
4	4	5	3	4	5	3	4	5
4	4	5	3	5	4	4	5	5
5	5	4	3	5	3	5	3	4
5	4	3	4	5	4	3	4	4
3	4	4	5	3	5	3	4	4
3	4	5	4	3	4	4	5	4
4	4	5	3	3	2	3	3	4
3	4	4	5	3	4	3	5	4
4	5	4	3	4	5	3	5	4
5	4	5	3	4	3	5	5	3
4	3	4	5	3	4	4	4	5
4	5	3	5	4	3	5	4	3
3	5	3	4	5	3	4	3	2
4	3	4	4	5	4	4	5	4
4	4	3	4	4	4	5	5	5
4	5	3	5	3	4	4	5	4
4	4	4	5	3	4	4	4	3
3	5	3	4	4	4	5	3	5
4	3	4	3	4	4	4	5	4
3	4	5	5	3	4	3	4	4
3	3	4	5	4	4	5	4	3
4	4	5	3	4	5	3	4	3
4	5	5	4	3	4	3	5	5
5	4	3	5	4	3	4	4	5
3	4	5	3	5	4	3	4	5
5	3	4	4	4	5	3	5	3
3	3	3	2	5	3	4	3	4
4	5	3	4	5	3	4	4	5
3	5	3	4	4	3	4	3	4
3	4	3	3	3	3	3	5	5
5	3	4	4	3	3	5	4	5
3	4	3	4	5	4	3	3	4
4	3	2	4	4	4	5	3	5
4	5	3	4	4	3	4	4	4

3	4	5	4	5	3	4	5	4
3	4	3	4	5	3	4	5	4
3	4	5	4	3	4	3	5	4
3	4	3	4	3	4	5	4	5
3	4	5	4	3	4	5	4	3
4	5	4	3	4	5	4	3	4
3	4	5	4	3	4	5	4	3
3	4	4	4	5	4	3	4	4
5	3	4	4	3	4	5	3	4
5	3	4	3	4	3	4	4	4
4	4	4	4	3	4	4	4	3
4	3	2	4	3	4	5	4	3
5	3	4	5	3	4	4	3	4
3	5	5	4	3	4	5	3	4
3	3	1	3	4	2	4	3	4
4	4	5	4	3	4	5	4	4
4	3	4	5	4	3	5	4	3
4	4	3	5	3	4	5	4	3
3	4	3	3	4	2	5	3	4
4	5	3	4	3	5	4	3	5
4	3	4	3	5	4	4	3	3
4	5	3	4	5	3	5	3	4
5	4	4	3	5	3	4	5	3
4	5	4	3	5	4	3	4	5
4	2	4	3	5	4	3	5	4
4	4	5	4	5	4	3	4	5
4	4	3	4	4	5	3	4	2
4	5	4	3	4	5	3	4	4
3	4	3	3	4	5	4	4	3
3	4	4	5	4	4	5	4	3
5	4	3	5	3	4	3	4	5
3	5	5	4	5	3	4	5	3
4	3	3	3	3	3	4	4	4
3	3	3	3	3	4	5	5	4
3	5	3	3	4	5	4	3	5
3	5	4	3	3	4	4	5	3
5	4	3	3	4	5	3	3	5
5	5	4	5	5	5	4	3	4
4	5	5	4	5	3	4	4	3
5	4	5	3	4	5	3	4	4
4	4	3	4	4	5	3	4	2

4	5	4	3	4	5	3	4	4
3	4	3	3	4	5	4	4	3
3	4	4	5	4	4	5	4	3
5	4	3	5	3	4	3	4	5
3	5	5	4	5	3	4	5	3
4	3	3	3	3	3	4	4	4
3	3	3	3	3	4	5	5	4
3	5	3	3	4	5	4	3	5
3	5	4	3	3	4	4	5	3
5	4	3	3	4	5	3	3	5
5	5	4	5	5	5	4	3	4
4	5	5	4	5	3	4	4	3
5	4	5	3	4	5	3	4	4
4	5	3	3	4	4	3	4	5
3	4	5	4	4	5	3	5	3
3	5	4	3	5	4	3	5	4
5	4	5	3	4	4	4	3	3
5	4	3	3	4	5	3	4	4
5	4	5	4	3	5	4	5	3
3	4	5	4	3	5	4	3	4
3	5	4	3	4	5	4	3	4
5	4	5	4	3	4	5	3	4
4	3	5	4	3	4	5	4	3
4	3	4	5	4	4	5	4	3
3	4	3	5	4	3	3	5	4
4	3	5	4	3	4	4	3	5
4	3	3	3	3	3	4	4	4
3	3	3	4	3	3	4	5	4
3	3	4	5	4	3	4	5	4
3	4	4	3	3	3	4	5	5
4	3	3	3	3	4	3	4	3
4	3	3	3	3	3	4	3	4
3	3	4	3	3	3	4	4	4
4	3	3	3	4	3	4	4	4
3	3	4	3	3	3	4	5	4
4	3	3	4	4	3	4	4	3
3	4	3	3	3	3	4	4	4
4	3	3	3	3	4	4	3	3
3	3	3	3	4	4	3	4	3
4	4	3	3	3	3	4	4	3
4	3	3	3	3	3	4	4	3

3	3	3	3	3	4	4	4	4
3	3	3	3	3	4	4	4	3
3	3	3	4	3	3	3	4	4
3	3	3	3	4	4	4	4	4
4	3	3	3	3	4	4	4	3
3	4	4	3	3	3	3	3	4
4	4	3	3	3	4	3	4	4
3	4	3	5	4	3	3	5	4
4	3	5	4	3	4	4	3	5
4	3	3	3	3	3	4	4	4
3	3	3	4	3	3	4	5	4
3	3	4	5	4	3	4	5	4
3	4	4	3	3	3	4	5	5
4	3	3	3	3	4	3	4	3
4	3	3	3	3	3	4	3	4
3	3	4	3	3	3	4	4	4
4	3	3	3	4	3	4	4	4
3	3	4	3	3	3	4	5	4
4	3	3	4	4	3	4	4	3
3	4	3	3	3	3	4	4	4
4	3	3	3	3	4	4	3	3
3	3	3	3	4	4	3	4	3
4	4	3	3	3	3	4	4	3
4	3	3	3	3	3	4	4	3
3	3	3	3	3	4	4	4	4
3	3	3	3	3	4	4	4	3
3	3	3	4	3	3	3	4	4
3	3	3	3	4	4	4	4	4
4	3	3	3	3	4	4	4	3
3	4	4	3	3	3	3	3	4
4	4	3	3	3	4	3	4	4
4	3	4	5	4	4	5	4	3
3	4	5	3	4	5	3	4	3
5	3	4	4	3	5	5	4	3
4	5	3	4	5	5	4	3	3
4	5	4	3	4	4	3	4	5
3	4	5	4	3	5	3	4	3
3	4	3	3	3	3	3	5	4
4	4	4	3	3	3	4	4	5
3	4	4	5	3	4	4	3	5
4	3	4	5	4	3	4	5	4

3	4	3	3	4	5	4	5	4

Variabel Y Kepercayaan Nasabah

Y1	Y2	Y3	Y4	Y5	Y6	Y7	Y8	Y9
5	5	4	4	5	4	5	5	4
4	4	4	4	4	4	4	4	5
4	4	4	4	4	4	4	4	4
3	3	3	3	3	3	3	3	3
4	4	4	4	4	4	4	4	3
3	3	3	3	4	4	4	4	3
5	2	2	3	3	1	3	4	5
4	4	4	5	4	3	4	5	3
5	4	4	5	4	5	2	2	4
4	5	2	3	5	4	5	4	5
4	4	3	5	5	5	4	4	2
3	5	4	5	4	4	3	5	4
4	4	4	4	4	4	3	4	4
4	4	5	3	3	3	5	3	4
5	5	5	5	4	5	5	4	4
3	5	5	4	4	2	1	2	3
3	4	4	3	4	3	4	3	4
3	4	4	4	4	4	4	4	4
3	4	5	4	3	2	5	5	4
4	5	4	4	4	4	5	3	2
4	3	3	4	3	4	4	3	4
3	4	4	4	3	4	5	5	4
4	3	5	4	4	4	4	5	2
4	4	4	4	4	4	4	4	4
5	3	4	4	4	4	4	4	3
4	5	5	4	3	3	4	5	4
4	5	4	3	3	4	5	4	4
4	4	5	5	3	5	5	4	4
4	5	4	3	5	4	5	4	5
5	4	4	5	4	5	4	3	3
4	3	3	4	5	4	3	4	5
4	4	4	4	5	4	5	4	4
5	3	4	5	3	5	3	4	4
3	4	5	4	4	5	3	4	5
5	3	4	5	3	4	5	5	5
3	4	4	4	4	5	3	5	4
5	3	3	4	5	3	5	4	3

3	3	4	4	4	3	5	4	4
3	5	5	3	4	4	4	4	5
3	4	5	4	3	3	4	5	5
4	3	4	4	5	4	4	3	4
5	5	5	4	4	4	5	4	5
5	3	4	4	5	5	4	4	5
5	3	4	5	4	4	3	4	5
4	4	4	4	3	4	4	4	4
4	3	5	5	4	5	5	4	4
4	4	4	4	4	4	4	4	5
4	4	3	4	5	5	4	4	4
3	3	4	4	5	4	3	4	4
5	4	4	3	4	4	5	4	4
4	4	3	4	5	5	4	5	5
4	4	5	3	4	3	3	4	4
4	5	3	4	4	5	3	4	3
4	3	4	4	5	3	5	4	3
4	4	3	5	4	3	3	5	4
5	4	3	4	5	3	4	4	5
5	4	3	4	4	5	3	4	4
4	5	3	5	5	4	4	3	5
3	3	5	4	5	4	3	4	5
4	3	4	5	3	4	5	3	4
3	4	5	4	5	4	5	4	4
5	3	4	5	4	3	4	5	4
4	3	4	4	3	4	4	5	3
3	3	4	4	3	4	4	5	4
4	3	4	5	3	4	4	5	4
4	4	5	4	4	5	4	3	4
5	3	4	4	3	3	5	3	5
4	3	3	4	3	4	5	3	4
4	5	4	3	4	4	3	4	5
3	4	4	3	3	4	4	3	5
3	4	4	3	4	5	3	4	4
5	4	4	3	3	4	3	4	4
4	3	4	5	4	3	4	4	3
3	4	5	3	4	3	4	3	4
3	4	4	3	3	4	4	4	4
3	4	5	3	3	4	4	4	5
5	4	3	4	5	4	3	3	4
5	4	3	5	5	3	4	4	5

5	3	3	4	5	4	3	4	5
3	2	4	3	1	3	3	4	5
5	4	4	3	4	4	5	3	4
2	3	3	3	4	4	5	4	5
2	3	4	5	3	4	4	5	5
4	3	5	4	5	4	4	5	4
5	4	3	5	3	4	5	3	5
5	4	5	3	5	5	4	3	4
4	5	4	3	5	4	3	5	5
4	3	4	5	4	3	4	5	5
4	5	3	4	5	4	3	4	5
5	4	5	3	4	5	5	5	5
3	4	5	4	5	3	4	5	4
5	3	5	4	4	5	4	3	5
3	4	5	3	4	5	3	4	5
5	4	5	4	4	3	3	3	4
5	4	5	3	4	5	3	4	5
4	5	4	3	4	4	5	5	4
5	5	4	4	5	4	5	4	4
4	3	4	3	4	5	4	5	5
3	4	4	5	5	3	3	4	5
5	4	5	3	4	5	4	5	4
5	4	3	5	4	3	5	5	5
5	4	3	5	4	5	5	5	4
3	3	5	5	4	4	4	5	5
5	3	4	4	3	4	5	3	4
3	5	4	5	3	4	4	4	5
3	4	3	4	3	4	5	4	3
2	3	4	5	4	3	4	3	5
5	4	4	4	5	4	5	4	3
3	5	4	4	4	5	4	5	4
3	5	5	5	4	3	5	5	5
4	5	4	3	4	4	3	4	4
5	4	3	4	5	4	3	4	5
5	3	4	3	4	5	4	5	4
5	3	4	5	3	4	5	3	4
4	4	3	4	4	4	3	4	5
4	5	4	3	4	5	4	3	4
4	5	3	4	4	3	3	5	5
3	3	4	3	4	5	4	3	4
3	3	5	3	4	4	4	5	4

4	3	4	5	4	3	4	4	5
4	5	4	3	4	4	5	4	4
5	5	5	4	4	5	4	5	5
3	3	4	3	4	4	3	4	5
4	3	4	4	5	3	4	4	4
3	5	5	4	4	3	4	4	4
5	3	4	5	4	4	5	3	5
3	3	4	3	4	5	4	3	5
4	4	3	3	5	4	3	4	5
3	3	4	5	4	3	5	3	4
5	5	4	3	3	3	3	3	4
4	5	4	5	4	3	4	4	5
5	3	4	3	5	4	4	4	4
4	5	3	4	5	3	4	4	5
3	5	4	4	5	3	4	5	5
4	3	3	4	4	3	5	3	4
4	5	4	5	4	4	5	3	4
3	4	3	4	5	4	4	3	5
4	3	4	5	4	4	4	3	5
4	5	3	4	3	3	4	4	3
5	4	3	4	3	3	4	3	4
3	3	4	5	3	4	3	4	4
3	4	4	3	4	4	4	4	5
5	4	3	4	3	3	4	4	5
5	3	4	4	3	4	4	3	3
5	4	5	4	4	3	3	4	4
3	4	5	4	4	4	4	3	4
4	4	3	5	3	4	5	4	5
3	5	4	3	4	4	5	4	4
4	5	3	4	3	4	4	4	4
4	4	4	3	3	4	3	4	4
4	3	4	5	5	4	4	4	5
3	5	5	3	4	5	4	3	5
4	4	4	5	5	5	3	4	5
5	4	5	5	5	5	4	4	5
4	4	5	4	5	5	4	4	5
5	5	3	3	4	4	5	3	4
4	3	3	3	4	5	3	4	5
3	4	3	4	3	4	3	3	4
3	5	5	4	3	3	4	3	3
4	5	4	3	4	5	4	3	4

5	5	4	5	5	4	5	4	5
3	4	5	5	5	5	5	4	5
3	4	5	4	3	4	4	5	4
4	5	4	5	4	4	4	5	5
4	4	3	4	4	5	4	5	5
5	5	5	5	5	4	5	4	5
5	5	5	5	4	5	5	4	5
3	4	3	4	5	3	4	3	4
4	5	4	4	5	4	5	4	5
4	3	4	5	5	5	5	4	4
4	5	5	5	5	4	4	4	5
4	5	5	5	4	4	4	4	4
5	5	5	5	5	5	5	4	5
5	5	5	4	4	4	5	4	5
4	4	4	4	4	4	4	5	4
5	5	5	5	4	4	5	4	5
4	4	3	5	4	4	5	5	4
4	4	5	5	4	5	5	4	5
4	4	4	5	5	4	5	5	5
3	4	4	4	4	4	4	5	5
4	5	4	5	4	5	5	5	5
4	4	3	4	4	4	5	4	5
4	4	4	4	4	4	5	5	5
4	3	4	4	4	3	4	4	5
4	4	4	4	4	4	4	4	5
4	4	4	4	5	5	4	4	4
4	4	5	5	4	5	5	4	5

Lampiran 6. Hasil Olah Data SPSS
Uji Validitas X1: Ancaman Siber

Correlations

		X1.1	X1.2	X1.3	X1.4	X1.5	X1.6	X1.7	X1.8	total_skor
X1.1	Pearson Correlation	1	.436**	.408**	.220	.456**	.441**	.371**	.412**	.8
	Sig. (2-tailed)		.002	.003	.125	.001	.001	.008	.003	
	N	50	50	50	50	50	50	50	50	
X1.2	Pearson Correlation	.436**	1	.161	.112	.348*	.264	.228	.193	.5
	Sig. (2-tailed)	.002		.265	.439	.013	.064	.111	.180	
	N	50	50	50	50	50	50	50	50	
X1.3	Pearson Correlation	.408**	.161	1	.117	.181	.463**	.168	.113	.5
	Sig. (2-tailed)	.003	.265		.417	.209	.001	.242	.435	
	N	50	50	50	50	50	50	50	50	
X1.4	Pearson Correlation	.220	.112	.117	1	.191	.266	-.059	.216	.4
	Sig. (2-tailed)	.125	.439	.417		.183	.062	.683	.133	
	N	50	50	50	50	50	50	50	50	
X1.5	Pearson Correlation	.456**	.348*	.181	.191	1	.269	.075	.344*	.6
	Sig. (2-tailed)	.001	.013	.209	.183		.059	.605	.014	
	N	50	50	50	50	50	50	50	50	
X1.6	Pearson Correlation	.441**	.264	.463**	.266	.269	1	.281*	.142	.6
	Sig. (2-tailed)	.001	.064	.001	.062	.059		.048	.325	
	N	50	50	50	50	50	50	50	50	
X1.7	Pearson Correlation	.371**	.228	.168	-.059	.075	.281*	1	-.120	.4
	Sig. (2-tailed)	.008	.111	.242	.683	.605	.048		.408	
	N	50	50	50	50	50	50	50	50	
X1.8	Pearson Correlation	.412**	.193	.113	.216	.344*	.142	-.120	1	.4
	Sig. (2-tailed)	.003	.180	.435	.133	.014	.325	.408		
	N	50	50	50	50	50	50	50	50	
total_skor_X1	Pearson Correlation	.817**	.598**	.589**	.421**	.619**	.678**	.432**	.466**	
	Sig. (2-tailed)	.000	.000	.000	.002	.000	.000	.002	.001	
	N	50	50	50	50	50	50	50	50	

**. Correlation is significant at the 0.01 level (2-tailed).

*. Correlation is significant at the 0.05 level (2-tailed).

Hasil Uji Validitas X2: Ancaman Siber

Correlations

		X2.1	X2.2	X2.3	X2.4	X2.5	X2.6	X2.7	X2.8	X2.9	total_s
X2.1	Pearson Correlation	1	-.145	.097	-.261	.168	-.210	.048	.038	.141	
	Sig. (2-tailed)		.316	.502	.067	.243	.143	.743	.793	.328	
	N	50	50	50	50	50	50	50	50	50	
X2.2	Pearson Correlation	-.145	1	.053	.070	.280*	-.229	.129	-.076	-.072	
	Sig. (2-tailed)	.316		.717	.630	.049	.110	.371	.600	.621	
	N	50	50	50	50	50	50	50	50	50	
X2.3	Pearson Correlation	.097	.053	1	-.095	.049	-.032	.039	.220	.077	
	Sig. (2-tailed)	.502	.717		.512	.736	.824	.787	.124	.595	
	N	50	50	50	50	50	50	50	50	50	
X2.4	Pearson Correlation	-.261	.070	-.095	1	-.237	-.138	.038	.004	-.091	
	Sig. (2-tailed)	.067	.630	.512		.097	.338	.794	.978	.529	
	N	50	50	50	50	50	50	50	50	50	
X2.5	Pearson Correlation	.168	.280*	.049	-.237	1	-.344*	.139	-.080	.047	
	Sig. (2-tailed)	.243	.049	.736	.097		.015	.337	.582	.746	
	N	50	50	50	50	50	50	50	50	50	
X2.6	Pearson Correlation	-.210	-.229	-.032	-.138	-.344*	1	-.121	-.035	-.031	
	Sig. (2-tailed)	.143	.110	.824	.338	.015		.403	.809	.831	
	N	50	50	50	50	50	50	50	50	50	
X2.7	Pearson Correlation	.048	.129	.039	.038	.139	-.121	1	.108	-.159	
	Sig. (2-tailed)	.743	.371	.787	.794	.337	.403		.456	.271	
	N	50	50	50	50	50	50	50	50	50	
X2.8	Pearson Correlation	.038	-.076	.220	.004	-.080	-.035	.108	1	.099	
	Sig. (2-tailed)	.793	.600	.124	.978	.582	.809	.456		.494	
	N	50	50	50	50	50	50	50	50	50	
X2.9	Pearson Correlation	.141	-.072	.077	-.091	.047	-.031	-.159	.099	1	
	Sig. (2-tailed)	.328	.621	.595	.529	.746	.831	.271	.494		
	N	50	50	50	50	50	50	50	50	50	
total_skor_X2	Pearson Correlation	.273	.368**	.505**	.126	.344*	-.103	.444**	.487**	.370**	
	Sig. (2-tailed)	.055	.009	.000	.383	.014	.475	.001	.000	.008	
	N	50	50	50	50	50	50	50	50	50	

*. Correlation is significant at the 0.05 level (2-tailed).

**. Correlation is significant at the 0.01 level (2-tailed).

Hasil Uji Validitas Y: Kepercayaan Nasabah

Correlations

		Y1	Y2	Y3	Y4	Y5	Y6	Y7	Y8	Y9	total_
Y1	Pearson Correlation	1	-.035	-.058	.266	.084	.230	.141	-.112	.081	
	Sig. (2-tailed)		.811	.690	.062	.563	.108	.330	.441	.577	
	N	50	50	50	50	50	50	50	50	50	
Y2	Pearson Correlation	-.035	1	.412**	-.208	.087	.008	.220	.207	.134	
	Sig. (2-tailed)	.811		.003	.147	.546	.956	.124	.150	.352	
	N	50	50	50	50	50	50	50	50	50	
Y3	Pearson Correlation	-.058	.412**	1	.044	-.206	.034	.264	.260	.270	
	Sig. (2-tailed)	.690	.003		.763	.151	.817	.064	.068	.058	
	N	50	50	50	50	50	50	50	50	50	
Y4	Pearson Correlation	.266	-.208	.044	1	-.048	.450**	-.162	.271	-.098	
	Sig. (2-tailed)	.062	.147	.763		.738	.001	.261	.057	.500	
	N	50	50	50	50	50	50	50	50	50	
Y5	Pearson Correlation	.084	.087	-.206	-.048	1	.191	.108	-.063	.039	
	Sig. (2-tailed)	.563	.546	.151	.738		.184	.454	.666	.790	
	N	50	50	50	50	50	50	50	50	50	
Y6	Pearson Correlation	.230	.008	.034	.450**	.191	1	-.179	-.014	.137	
	Sig. (2-tailed)	.108	.956	.817	.001	.184		.212	.923	.344	
	N	50	50	50	50	50	50	50	50	50	
Y7	Pearson Correlation	.141	.220	.264	-.162	.108	-.179	1	.073	-.054	
	Sig. (2-tailed)	.330	.124	.064	.261	.454	.212		.614	.707	
	N	50	50	50	50	50	50	50	50	50	
Y8	Pearson Correlation	-.112	.207	.260	.271	-.063	-.014	.073	1	.145	
	Sig. (2-tailed)	.441	.150	.068	.057	.666	.923	.614		.314	
	N	50	50	50	50	50	50	50	50	50	
Y9	Pearson Correlation	.081	.134	.270	-.098	.039	.137	-.054	.145	1	
	Sig. (2-tailed)	.577	.352	.058	.500	.790	.344	.707	.314		
	N	50	50	50	50	50	50	50	50	50	
total_skor_Y	Pearson Correlation	.432**	.498**	.520**	.358*	.321*	.455**	.418**	.422**	.418**	
	Sig. (2-tailed)	.002	.000	.000	.011	.023	.001	.003	.002	.003	
	N	50	50	50	50	50	50	50	50	50	

**. Correlation is significant at the 0.01 level (2-tailed).

*. Correlation is significant at the 0.05 level (2-tailed).

Hasil Uji Reliabilitas X1: Ancaman Siber

Reliability Statistics

Cronbach's Alpha	N of Items
.730	6

Item-Total Statistics

	Scale Mean if Item Deleted	Scale Variance if Item Deleted	Corrected Item-Total Correlation	Cronbach's Alpha if Item Deleted
X1.1	18.46	8.907	.680	.621
X1.2	18.20	10.571	.415	.707
X1.3	18.06	10.302	.394	.716
X1.5	18.10	10.255	.473	.690
X1.6	17.90	10.418	.489	.686
X1.8	17.58	11.677	.351	.722

Hasil Uji Reliabilitas X2: Strategi Mitigasi Risiko

Reliability Statistics

Cronbach's Alpha	N of Items
.626	5

Item-Total Statistics

	Scale Mean if Item Deleted	Scale Variance if Item Deleted	Corrected Item-Total Correlation	Cronbach's Alpha if Item Deleted
X2 1	13.66	12.964	.122	.699
X2 2	13.30	11.316	.424	.553
X2 5	13.56	8.619	.697	.383
X2 8	12.96	14.121	.061	.703
X2 9	13.56	8.619	.697	.383

Hasil Uji Reliabilitas Y: Kepercayaan Nasabah

Reliability Statistics

Cronbach's Alpha	N of Items
.762	7

Item-Total Statistics

	Scale Mean if Item Deleted	Scale Variance if Item Deleted	Corrected Item-Total Correlation	Cronbach's Alpha if Item Deleted
Y3	49.04	19.386	.364	.755
Y4	48.86	19.511	.452	.748
Y5	48.92	20.606	.260	.769
Y6	48.84	18.464	.615	.726
Y7	49.04	16.815	.698	.699
Y8	24.38	7.016	.892	.706
Y9	49.04	16.815	.698	.699

Hasil Uji Normalitas

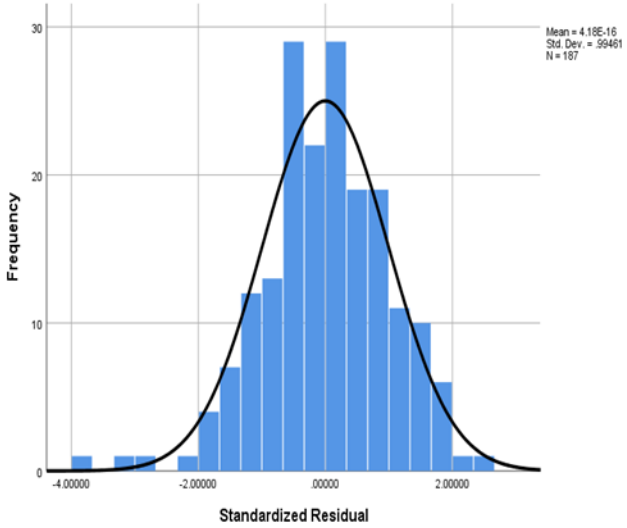
Tests of Normality

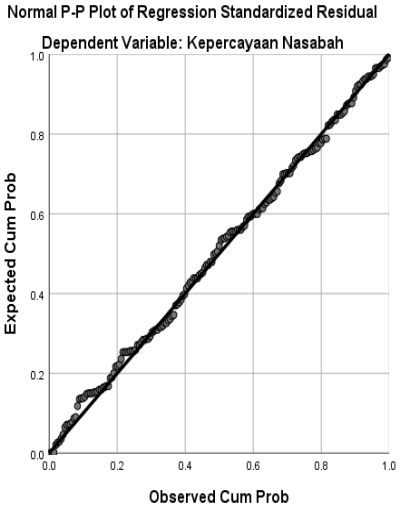
	Kolmogorov-Smirnov[a]			Shapiro-Wilk		
	Statistic	df	Sig.	Statistic	df	Sig.
Standardized Residual	.049	187	.200*	.986	187	.058

*. This is a lower bound of the true significance.

a. Lilliefors Significance Correction

Hasil Uji Normalitas Metode Grafik Histogram Uji Normalitas Metode Normal P-Plot





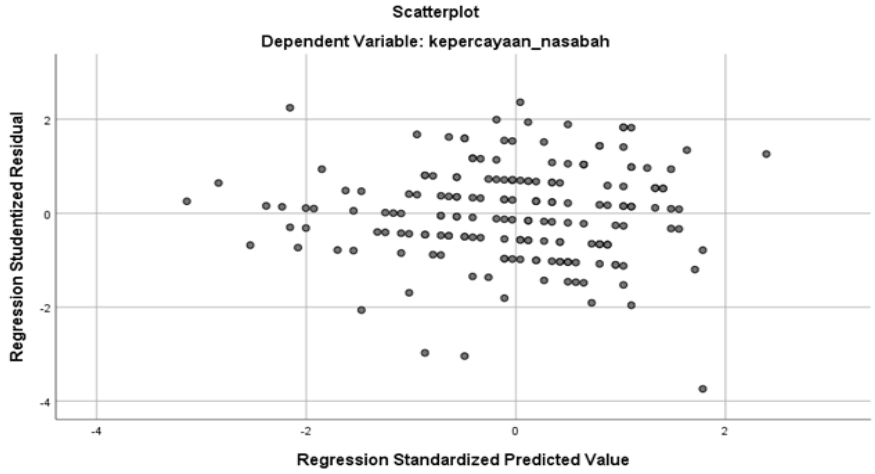
Hasil Uji Multikolinearitas

Coefficients[a]

Model		Collinearity Statistics	
		Tolerance	VIF
1	V10	.989	1.011
	V19	.989	1.011

a. Dependent Variable: kepercayaan_nasabah

Hasil Uji Heterokedastisitas



Hasil Uji Heterokedastisitas Metode Glejser

variabel	Sig	Keterangan
(X1)	0,217 > 0.05	Tidak terjadi heterokedastisitas
(X2)	0,139 > 0,05	Tidak terjadi heterokedastisitas

Uji T

Coefficients[a]

Model		Unstandardized Coefficients		Standardized Coefficients		
		B	Std. Error	Beta	t	Sig.
1	(Constant)	28.169	2.501		11.264	.000
	Ancaman siber (X1)	.067	.051	.096	1.310	.192
	Mitigasi Risiko (X2)	-.089	.099	-.067	-.905	.367

a. Dependent Variable: Kepercayaan Nasabah

Uji F

ANOVA[a]

Model		Sum of Squares	df	Mean Square	F	Sig.
1	Regression	16.201	2	8.101	1.409	.247[b]
	Residual	1057.574	184	5.748		
	Total	1073.775	186			

a. Dependent Variable: Kepercayaan Nasabah (Y)

b. Predictors: (Constant), Ancaman siber (X1), Mitigasi Risiko(X2)

Hasil Uji Koefisien Determinasi

Model Summary[b]

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate
1	.123[a]	.015	.004	2.397

a. Predictors: (Constant), Ancaman Siber, Strategi Mitigasi Risiko

b. Dependent Variable: Kepercayaan Nasabah

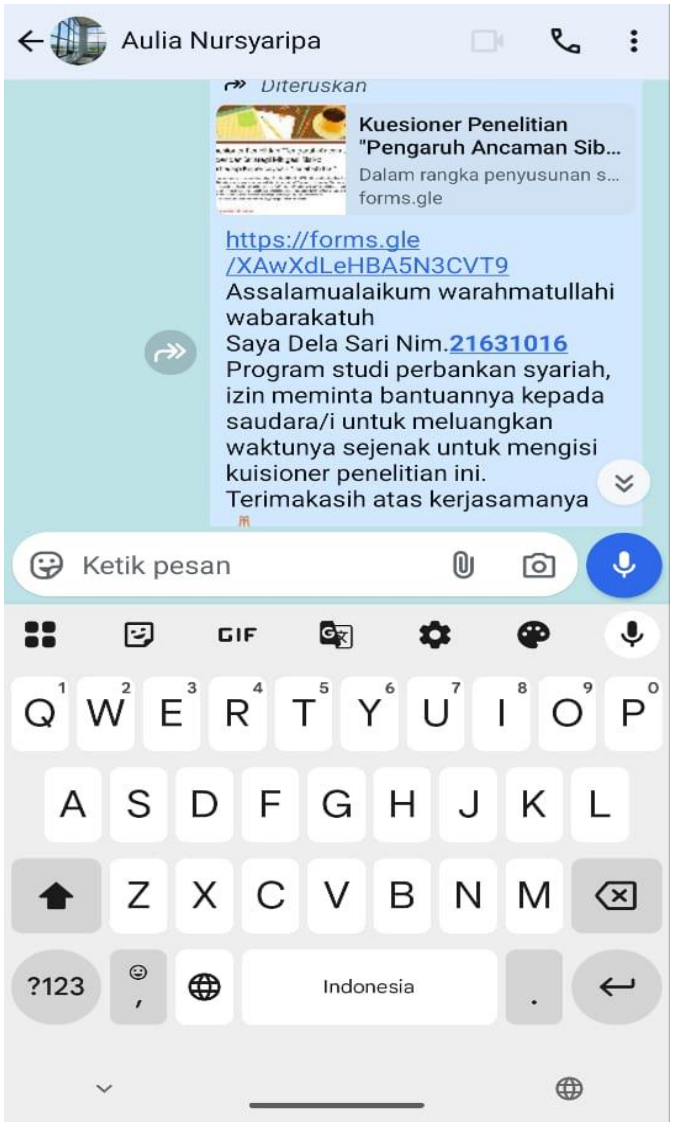
T Tabel

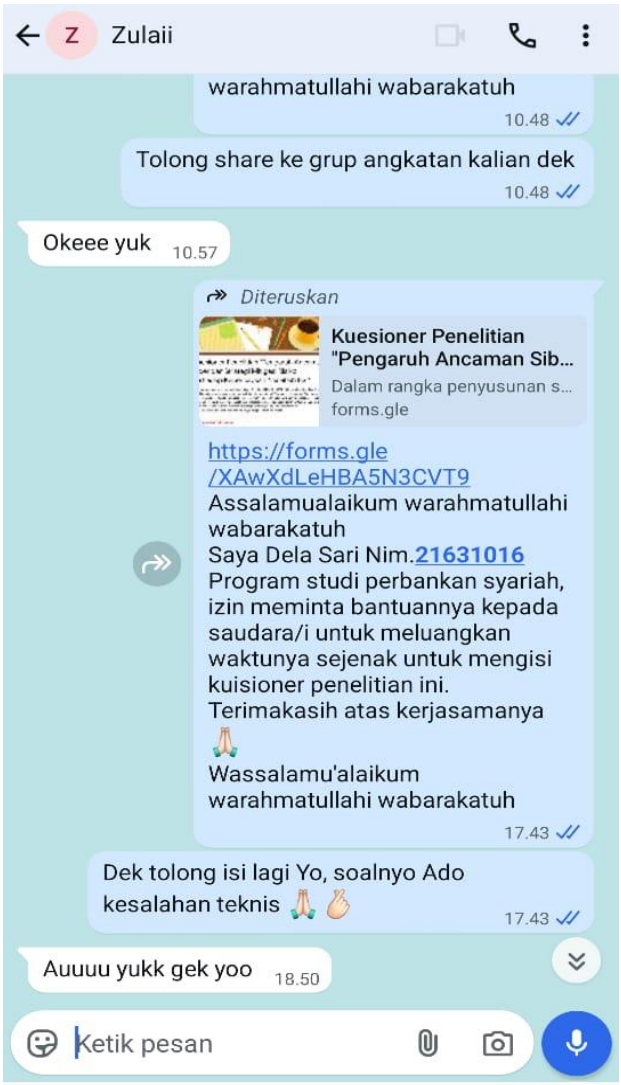
DF atau DK	Tabel Distribusi Student t						Tabel Uji Korelasi Pearson Product Moment					
	uji satu sisi (one tailed)						uji satu sisi (one tailed)					
	0,25	0,1	0,05	0,025	0,01	0,005	0,25	0,1	0,05	0,025	0,01	0,005
	Uji dua sisi (two tailed)						Uji dua sisi (two tailed)					
	0,5	0,2	0,1	0,05	0,02	0,01	0,5	0,2	0,1	0,05	0,02	0,01
156	0,676	1,287	1,655	1,975	2,350	2,608	0,054	0,102	0,131	0,156	0,185	0,204
157	0,676	1,287	1,655	1,975	2,350	2,608	0,054	0,102	0,131	0,156	0,184	0,204
158	0,676	1,287	1,655	1,975	2,350	2,607	0,054	0,102	0,131	0,155	0,184	0,203
159	0,676	1,287	1,654	1,975	2,350	2,607	0,054	0,102	0,130	0,155	0,183	0,202
160	0,676	1,287	1,654	1,975	2,350	2,607	0,053	0,101	0,130	0,154	0,183	0,202
161	0,676	1,287	1,654	1,975	2,350	2,607	0,053	0,101	0,129	0,154	0,182	0,201
162	0,676	1,287	1,654	1,975	2,350	2,607	0,053	0,101	0,129	0,153	0,182	0,201
163	0,676	1,287	1,654	1,975	2,349	2,606	0,053	0,100	0,128	0,153	0,181	0,200
164	0,676	1,287	1,654	1,975	2,349	2,606	0,053	0,100	0,128	0,152	0,180	0,199
165	0,676	1,287	1,654	1,974	2,349	2,606	0,053	0,100	0,128	0,152	0,180	0,199
166	0,676	1,287	1,654	1,974	2,349	2,606	0,052	0,099	0,127	0,151	0,179	0,198
167	0,676	1,287	1,654	1,974	2,349	2,606	0,052	0,099	0,127	0,151	0,179	0,198
168	0,676	1,287	1,654	1,974	2,349	2,605	0,052	0,099	0,127	0,151	0,178	0,197
169	0,676	1,287	1,654	1,974	2,349	2,605	0,052	0,098	0,126	0,150	0,178	0,196
170	0,676	1,287	1,654	1,974	2,348	2,605	0,052	0,098	0,126	0,150	0,177	0,196
171	0,676	1,287	1,654	1,974	2,348	2,605	0,052	0,098	0,125	0,149	0,177	0,195
172	0,676	1,286	1,654	1,974	2,348	2,605	0,051	0,098	0,125	0,149	0,176	0,195
173	0,676	1,286	1,654	1,974	2,348	2,605	0,051	0,097	0,125	0,148	0,176	0,194
174	0,676	1,286	1,654	1,974	2,348	2,604	0,051	0,097	0,124	0,148	0,175	0,194
175	0,676	1,286	1,654	1,974	2,348	2,604	0,051	0,097	0,124	0,148	0,175	0,193
176	0,676	1,286	1,654	1,974	2,348	2,604	0,051	0,097	0,124	0,147	0,174	0,193
177	0,676	1,286	1,654	1,973	2,348	2,604	0,051	0,096	0,123	0,147	0,174	0,192
178	0,676	1,286	1,653	1,973	2,347	2,604	0,051	0,096	0,123	0,146	0,173	0,192
179	0,676	1,286	1,653	1,973	2,347	2,604	0,050	0,096	0,123	0,146	0,173	0,191
180	0,676	1,286	1,653	1,973	2,347	2,603	0,050	0,095	0,122	0,146	0,172	0,190
181	0,676	1,286	1,653	1,973	2,347	2,603	0,050	0,095	0,122	0,145	0,172	0,190
182	0,676	1,286	1,653	1,973	2,347	2,603	0,050	0,095	0,122	0,145	0,171	0,189
183	0,676	1,286	1,653	1,973	2,347	2,603	0,050	0,095	0,121	0,144	0,171	0,189
184	0,676	1,286	1,653	1,973	2,347	2,603	0,050	0,094	0,121	0,144	0,170	0,188
185	0,676	1,286	1,653	1,973	2,347	2,603	0,050	0,094	0,121	0,144	0,170	0,188
186	0,676	1,286	1,653	1,973	2,347	2,603	0,049	0,094	0,120	0,143	0,170	0,187
187	0,676	1,286	1,653	1,973	2,346	2,602	0,049	0,094	0,120	0,143	0,169	0,187
188	0,676	1,286	1,653	1,973	2,346	2,602	0,049	0,093	0,120	0,142	0,169	0,186
189	0,676	1,286	1,653	1,973	2,346	2,602	0,049	0,093	0,119	0,142	0,168	0,186
190	0,676	1,286	1,653	1,973	2,346	2,602	0,049	0,093	0,119	0,142	0,168	0,185
191	0,676	1,286	1,653	1,972	2,346	2,602	0,049	0,093	0,119	0,141	0,167	0,185
192	0,676	1,286	1,653	1,972	2,346	2,602	0,049	0,092	0,118	0,141	0,167	0,185
193	0,676	1,286	1,653	1,972	2,346	2,602	0,049	0,092	0,118	0,141	0,166	0,184
194	0,676	1,286	1,653	1,972	2,346	2,601	0,048	0,092	0,118	0,140	0,166	0,184
195	0,676	1,286	1,653	1,972	2,346	2,601	0,048	0,092	0,118	0,140	0,166	0,183
196	0,676	1,286	1,653	1,972	2,346	2,601	0,048	0,091	0,117	0,139	0,165	0,183
197	0,676	1,286	1,653	1,972	2,345	2,601	0,048	0,091	0,117	0,139	0,165	0,182
198	0,676	1,286	1,653	1,972	2,345	2,601	0,048	0,091	0,117	0,139	0,164	0,182
199	0,676	1,286	1,653	1,972	2,345	2,601	0,048	0,091	0,116	0,138	0,164	0,181
200	0,676	1,286	1,653	1,972	2,345	2,601	0,048	0,091	0,116	0,138	0,164	0,181
201	0,676	1,286	1,652	1,972	2,345	2,601	0,048	0,090	0,116	0,138	0,163	0,180
202	0,676	1,286	1,652	1,972	2,345	2,600	0,047	0,090	0,115	0,137	0,163	0,180
203	0,676	1,286	1,652	1,972	2,345	2,600	0,047	0,090	0,115	0,137	0,162	0,180
204	0,676	1,286	1,652	1,972	2,345	2,600	0,047	0,090	0,115	0,137	0,162	0,179
205	0,676	1,286	1,652	1,972	2,345	2,600	0,047	0,089	0,115	0,136	0,162	0,179
206	0,676	1,286	1,652	1,972	2,345	2,600	0,047	0,089	0,114	0,136	0,161	0,178
207	0,676	1,286	1,652	1,971	2,344	2,600	0,047	0,089	0,114	0,136	0,161	0,178

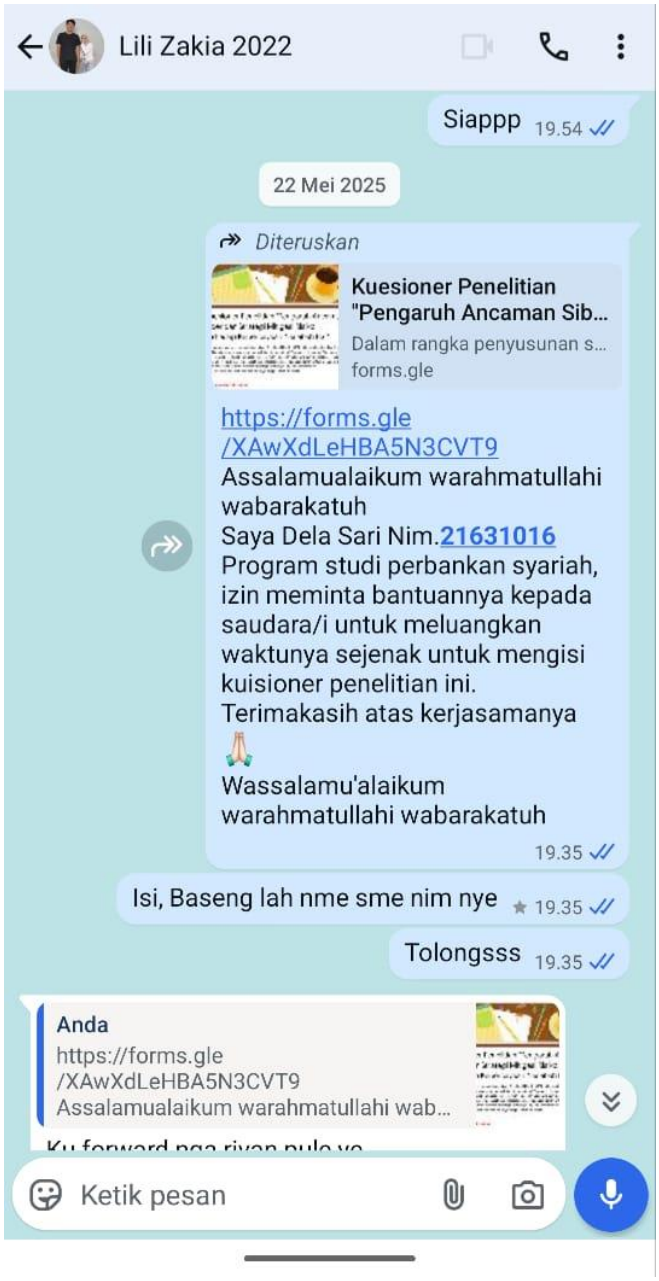
F Tabel

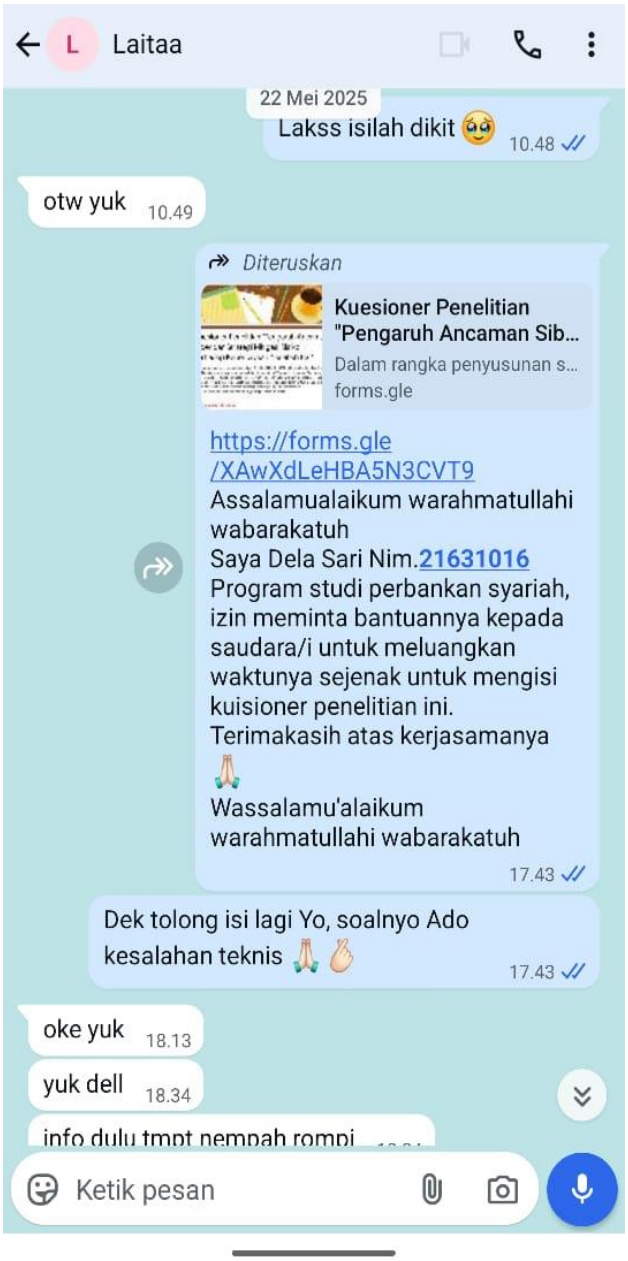
167	3.90	3.05	2.66	2.43	2.27
168	3.90	3.05	2.66	2.43	2.27
169	3.90	3.05	2.66	2.43	2.27
170	3.90	3.05	2.66	2.42	2.27
171	3.90	3.05	2.66	2.42	2.27
172	3.90	3.05	2.66	2.42	2.27
173	3.90	3.05	2.66	2.42	2.27
174	3.90	3.05	2.66	2.42	2.27
175	3.90	3.05	2.66	2.42	2.27
176	3.89	3.05	2.66	2.42	2.27
177	3.89	3.05	2.66	2.42	2.27
178	3.89	3.05	2.66	2.42	2.26
179	3.89	3.05	2.66	2.42	2.26
180	3.89	3.05	2.65	2.42	2.26
181	3.89	3.05	2.65	2.42	2.26
182	3.89	3.05	2.65	2.42	2.26
183	3.89	3.05	2.65	2.42	2.26
184	3.89	3.05	2.65	2.42	2.26
185	3.89	3.04	2.65	2.42	2.26
186	3.89	3.04	2.65	2.42	2.26
187	3.89	3.04	2.65	2.42	2.26
188	3.89	3.04	2.65	2.42	2.26
189	3.89	3.04	2.65	2.42	2.26
190	3.89	3.04	2.65	2.42	2.26
191	3.89	3.04	2.65	2.42	2.26
192	3.89	3.04	2.65	2.42	2.26
193	3.89	3.04	2.65	2.42	2.26
194	3.89	3.04	2.65	2.42	2.26
195	3.89	3.04	2.65	2.42	2.26
196	3.89	3.04	2.65	2.42	2.26
197	3.89	3.04	2.65	2.42	2.26
198	3.89	3.04	2.65	2.42	2.26
199	3.89	3.04	2.65	2.42	2.26
200	3.89	3.04	2.65	2.42	2.26
201	3.89	3.04	2.65	2.42	2.26
202	3.89	3.04	2.65	2.42	2.26
203	3.89	3.04	2.65	2.42	2.26
204	3.89	3.04	2.65	2.42	2.26
205	3.89	3.04	2.65	2.42	2.26
206	3.89	3.04	2.65	2.42	2.26
207	3.89	3.04	2.65	2.42	2.26
208	3.89	3.04	2.65	2.42	2.26
209	3.89	3.04	2.65	2.41	2.26

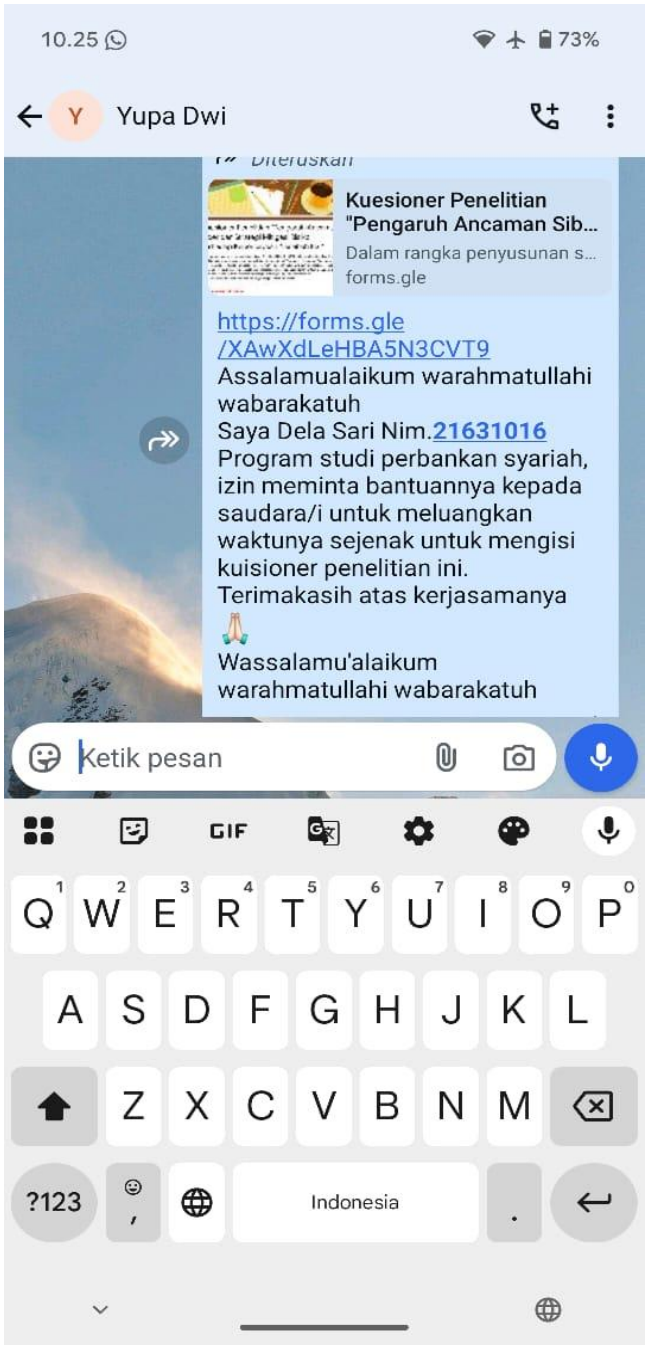
DOKUMENTASI


Aulia Nursyaripa
Diteruskan
Kuesioner Penelitian "Pengaruh Ancaman Sib...
Dalam rangka penyusunan s...
forms.gle
https://forms.gle/XAwXdLeHBA5N3CVT9
Assalamualaikum warahmatullahi wabarakatuh
Saya Dela Sari Nim.21631016
Program studi perbankan syariah, izin meminta bantuannya kepada saudara/i untuk meluangkan waktunya sejenak untuk mengisi kuisioner penelitian ini.
Terimakasih atas kerjasamanya
Ketik pesan
GIF
Q W E R T Y U I O P
A S D F G H J K L
Z X C V B N M
?123
Indonesia


Z
Zulaii
warahmatullahi wabarakatuh
10.48
Tolong share ke grup angkatan kalian dek
10.48
Okeee yuk 10.57
Diteruskan
Kuesioner Penelitian "Pengaruh Ancaman Sib...
Dalam rangka penyusunan s...
forms.gle
https://forms.gle/XAwXdLeHBA5N3CVT9
Assalamualaikum warahmatullahi wabarakatuh
Saya Dela Sari Nim.21631016
Program studi perbankan syariah, izin meminta bantuannya kepada saudara/i untuk meluangkan waktunya sejenak untuk mengisi kuisioner penelitian ini.
Terimakasih atas kerjasamanya
🙏
Wassalamu'alaikum warahmatullahi wabarakatuh
17.43
Dek tolong isi lagi Yo, soalnyo Ado kesalahan teknis 🙏🤞
17.43
Auuuu yukk gek yoo 18.50
Ketik pesan


Lili Zakia 2022
Siappp 19.54
22 Mei 2025
Diteruskan
Kuesioner Penelitian "Pengaruh Ancaman Sib...
Dalam rangka penyusunan s...
forms.gle
https://forms.gle /XAwXdLeHBA5N3CVT9
Assalamualaikum warahmatullahi wabarakatuh
Saya Dela Sari Nim.21631016
Program studi perbankan syariah, izin meminta bantuannya kepada saudara/i untuk meluangkan waktunya sejenak untuk mengisi kuisioner penelitian ini.
Terimakasih atas kerjasamanya
🙏
Wassalamu'alaikum warahmatullahi wabarakatuh
19.35
Isi, Baseng lah nme sme nim nye 19.35
Tolongsss 19.35
Anda
https://forms.gle /XAwXdLeHBA5N3CVT9
Assalamualaikum warahmatullahi wab...
Ketik pesan


Laitaa
22 Mei 2025
Lakss isilah dikit
10.48
otw yuk
10.49
Diteruskan
Kuesioner Penelitian "Pengaruh Ancaman Sib...
Dalam rangka penyusunan s...
forms.gle
https://forms.gle/XAwXdLeHBA5N3CVT9
Assalamualaikum warahmatullahi wabarakatuh
Saya Dela Sari Nim.21631016
Program studi perbankan syariah, izin meminta bantuannya kepada saudara/i untuk meluangkan waktunya sejenak untuk mengisi kuisioner penelitian ini.
Terimakasih atas kerjasamanya
Wassalamu'alaikum warahmatullahi wabarakatuh
17.43
Dek tolong isi lagi Yo, soalnyo Ado kesalahan teknis
17.43
oke yuk
18.13
yuk dell
18.34
info dulu tmpt nempah rompi
Ketik pesan


10.25
73%
Yupa Dwi
Diteruskan
Kuesioner Penelitian "Pengaruh Ancaman Sib...
Dalam rangka penyusunan s...
forms.gle
https://forms.gle/XAwXdLeHBA5N3CVT9
Assalamualaikum warahmatullahi wabarakatuh
Saya Dela Sari Nim.21631016
Program studi perbankan syariah, izin meminta bantuannya kepada saudara/i untuk meluangkan waktunya sejenak untuk mengisi kuisioner penelitian ini.
Terimakasih atas kerjasamanya
Wassalamu'alaikum warahmatullahi wabarakatuh
Ketik pesan
GIF
Indonesia
?123


10.27
73%
A
Alda Formakip
Kuesioner Penelitian "Pengaruh Ancaman Siber dan Strategi Mitigasi Risiko terhadap Kepercayaan Nasab...
Dalam rangka penyusunan skripsi. Saya Dela Sari NIM. 21631016 bermaksud melakukan penelitian ilmiah untuk penyusunan skripsi dengan judul "Pengaruh Ancaman Siber dan Strategi Mitigasi Risiko Terhadap Kepercayaan Nasabah Bank Syariah Indone...
forms.gle
https://forms.gle/XAwXdLeHBA5N3CVT9
Assalamualaikum warahmatullahi wabarakatuh
Saya Dela Sari Nim.21631016
Program studi perbankan syariah, izin meminta bantuannya kepada saudara/i untuk meluangkan waktunya sejenak untuk mengisi kuisioner penelitian ini.
Ketik pesan
GIF
Indonesia
?123