

**PENGUNGKAPAN KEAMANAN SIBER PADA PERUSAHAAN
SUBSEKTOR PERBANKAN YANG TERDAFTAR DI BURSA EFEK
INDONESIA PERIODE 2025**

SKRIPSI

**Untuk Memenuhi Sebagian Syarat - Syarat
Guna Mencapai Gelar Sarjana Akuntansi**



Diajukan Oleh:

DHANIA KURNIA PUTRI

NPM. 220110051

FAKULTAS EKONOMI DAN BISNIS

UNIVERSITAS TRIDINANTI

2026

UNIVERSITAS TRIDINANTI
FAKULTAS EKONOMI DAN BISNIS

HALAMAN PERSETUJUAN SKRIPSI

Nama : Dhania Kurnia Putri
Nomor Pokok : 22.01.12.00.51
Jurusan/ Prog. Studi : Akuntansi
Jenjang Pendidikan : Strata 1
Mata Kuliah Pokok : Akuntansi Manajemen
Judul Skripsi : Pengungkapan Keamanan Siber Pada Perusahaan Subsektor
Perbankan yang Terdaftar di Bursa Efek Indonesia Periode
2025

Pembimbing Skripsi :

Tanggal 28-07-2026 Pembimbing I : 
Dr. Rosalina Pebrica Mayasari, SE., Ak., M.Si
NIDN : 0026028301

Tanggal 28-07-2026 Pembimbing II : 
Dr. Lia Sari, SE., M.Si
NIDN : 0016058201

Mengetahui,

Dekan,

Ketua Program Studi,



Dr. H. Msv. Mikial., SE., M.Si., Ak., CA., CSRS
NIDN : 0205026401

Dr. Riza Syahputera, S.E., M.Ak., Ak CA CPA
NIDN : 0224108301

UNIVERSITAS TRIDINANTI
FAKULTAS EKONOMI DAN BISNIS

HALAMAN PENGESAHAN SKRIPSI

Nama : Dhania Kurnia Putri
Nomor Pokok : 22.01.12.00.51
Jurusan/ Prog. Studi : Akuntansi
Jenjang Pendidikan : Strata 1
Mata Kuliah Pokok : Akuntansi Manajemen
Judul Skripsi : Pengungkapan Keamanan Siber Pada Perusahaan Subsektor
Perbankan yang Terdaftar di Bursa Efek Indonesia Periode
2025

Penguji Skripsi

Tanggal 28-07-2026 Ketua Penguji : Dr. Rosalina Pebrica Mayasari, SE., Ak., M.Si
NIDN : 0026028301

Tanggal 28-07-2026 Penguji I : Dr. Lia Sari, SE., M.Si
NIDN : 0016058201

Tanggal 28-07-2026 Penguji II : H/Sugiharto, SE., M.Si, AK, CA
NIDN : 0205096701

Dekan,

Mengesahkan,

Ketua Program Studi,



Dr. H. Msy. Mikial., SE., M.Si., Ak., CA., CSRS
NIDN : 0205026401

Tanggal : 28 - 07 - 2026

Dr. Riza Syahputera, S.E., M.Ak., Ak CA CPA
NIDN : 0224108301

Tanggal : 28 - 07 - 2026

MOTTO DAN PERSEMBAHAN

Motto:

“Aku tidak berlomba dengan siapa pun, aku hanya berusaha menjadi lebih baik dari diriku yang kemarin.”

"Tak perlu bersinar paling terang, cukup tetap bercahaya di tengah gelap."

"Kesabaran adalah seni menunggu tanpa kehilangan harapan."

"Hidup bukan tentang siapa yang tercepat, tetapi siapa yang tetap berjalan ketika yang lain menyerah."

Percayalah, setiap halaman yang selesai ditulis hari ini adalah langkah menuju gelar yang selama ini diperjuangkan."

(Dhania Kurnia Putri)

"It does not matter how slowly you go as long as you do not stop."

(Confusius)

Kupersembahkan Kepada:

- Ayah dan Almh Ibu Tercinta
- Sudara-Saudaraku Tersayang
- Keluarga Besarku
- Sahabat-Sahabatku
- Para Pendidik Yang Saya Hormati
- Teman Seperjuangan Akuntansi 2022
- Almamater Tercinta

PERNYATAAN BEBAS PLAGIAT

Saya yang bertanda tangan di bawah ini:

Nama : Dhania Kurnia Putri

Nomor Pokok : 22.01.12.00.51

Fakultas : Ekonomi dan Bisnis

Jurusan : Akuntansi

Menyatakan bahwa skripsi ini ditulis dengan sungguh-sungguh dan tidak ada bagian yang merupakan perjiplakan karya orang lain.

Apakah dikemudian hari terbukti bahwa pernyataan ini tidak benar, maka saya sanggup menerima sanksi berupa pembatalan skripsi dengan konsekuensinya.

Palembang,



Dhania Kurnia Putri

KATA PENGANTAR

Puji dan syukur penulis panjatkan ke hadirat Tuhan Yang Maha Esa, karena atas rahmat dan karunia-Nya penulis dapat menyelesaikan skripsi ini yang berjudul **“Pengungkapan Keamanan Siber Pada Perusahaan Sub Sektor Perbankan yang Terdaftar di Bursa Efek Indonesia Periode 2025”**. Penulis menyadari bahwa dalam penyusunan skripsi ini tidak terlepas dari bantuan, bimbingan, serta dukungan dari berbagai pihak. Oleh karena itu, pada kesempatan ini penulis mengucapkan terima kasih yang sebesar-besarnya kepada:

1. Bapak Prof. Dr. Ir. H. Edizal AE, M.S selaku Rektor Universitas Tridianti
2. Ibu Dr. Hj. Msy. Mikial, S.E. M.Si, AK, CA, CSRS selaku Dekan Fakultas Ekonomi dan Bisnis Universitas Tridianti
3. Bapak Riza Syahputera S.E, Ak. CA, CPAI, M.Ak selaku Ketua Program Studi Akuntansi Fakultas Ekonomi dan Bisnis Universitas Tridianti.
4. Ibu Dr. Rosalina Pebrica Mayasari, SE, Ak, M.Si selaku Dosen Pembimbing I yang telah memberi bimbingan dan pengarahan selama penulis menyusun skripsi. Terima kasih atas setiap waktu yang telah diluangkan, setiap arahan yang diberikan, serta setiap masukan dan ilmu yang begitu berharga bagi penulis.
5. Ibu Dr. Lia Sari, S.E, M.Si selaku Dosen Pembimbing II yang telah memberikan bimbingan dan pengarahan dari awal hingga akhir tiada henti selama penulis menyusun skripsi. Ibu Lia tidak hanya membimbing penulis dalam menyelesaikan penelitian ini, tetapi juga mengajarkan arti ketekunan, kedisiplinan, dan tanggung jawab dalam menuntut ilmu.

Terima kasih atas setiap waktu yang telah diluangkan, setiap arahan yang diberikan, serta setiap masukan dan ilmu yang begitu berharga.

Terima kasih atas segala bimbingan, kesabaran, dan kebaikan yang telah Ibu Lia berikan. Jasa dan ilmu yang telah diberikan akan selalu penulis kenang dan menjadi bekal berharga dalam perjalanan kehidupan penulis ke depan.

6. Seluruh Bapak dan Ibu dosen serta staff Fakultas Ekonomi dan Bisnis yang telah memberikan bekal ilmu dan pengarahan selama masa studi.

7. Ayahanda tercinta Amril Nurman, Terima kasih atas segala pengorbanan yang telah Ayah berikan selama ini. Terima kasih karena tidak pernah lelah bekerja keras demi memenuhi kebutuhan dan mewujudkan impian penulis. Terima kasih atas setiap tetes keringat yang mungkin tidak pernah penulis lihat secara langsung, namun penulis rasakan melalui kasih sayang, perhatian, dan perjuangan yang selalu Ayah berikan kepada keluarga. Ayah, mungkin penulis tidak pernah benar-benar memahami seberapa besar perjuangan yang telah Ayah lalui untuk mengantarkan penulis sampai pada titik ini. Di balik senyum yang selalu Ayah tunjukkan, ada banyak lelah yang disembunyikan. Di balik setiap nasihat yang Ayah berikan, tersimpan harapan besar agar penulis dapat menjadi pribadi yang lebih baik dan mencapai masa depan yang lebih cerah. Doa-doa yang Ayah panjatkan dalam diam telah menjadi kekuatan yang mengiringi setiap langkah perjalanan penulis, terutama dalam menyelesaikan pendidikan dan skripsi ini. Semoga Allah SWT senantiasa memberikan kesehatan, kebahagiaan, umur yang panjang, serta melimpahkan keberkahan dalam setiap langkah kehidupan Ayah. Semoga penulis dapat menjadi anak yang membanggakan dan mampu mewujudkan harapan-harapan yang selama ini Ayah titipkan dalam setiap doa. sehingga penulis mampu menyelesaikan skripsi hingga mendapatkan gelar sarjana.
8. Almh Ibunda tercinta Siti Syamsiyah. Ibu, meskipun sekarang engkau telah berada di tempat terbaik di sisi Allah SWT, kasih sayangmu akan selalu hidup di dalam hati penulis. Tidak ada satu hari pun yang berlalu tanpa mengingat segala cinta, pengorbanan, dan perhatian yang telah Ibu berikan selama hidupmu. Kenangan tentang senyummu, pelukan hangatmu, nasihatmu, serta doa-doamu akan selalu menjadi bagian yang tidak terpisahkan dari perjalanan hidup penulis. Tanpa kehadiran dan cinta tulusmu, mungkin langkah ini takkan pernah sampai sejauh ini. terima kasih Ibu, karena telah menjadi madrasah pertama dalam hidup penulis. Terima kasih telah mengajarkan arti ketulusan, kesabaran, keikhlasan, dan kasih sayang yang tidak mengenal batas. Terima kasih atas setiap doa yang pernah

Ibu panjatkan, setiap air mata yang jatuh demi kebahagiaan penulis, serta setiap pengorbanan yang mungkin tidak akan pernah mampu penulis balas hingga akhir hayat.

Ibu, hari ini penulis berhasil menyelesaikan salah satu tahap penting dalam kehidupan penulis. Namun, di antara rasa syukur dan kebahagiaan ini, tersimpan kerinduan yang begitu besar karena penulis tidak dapat melihat senyum bangga Ibu secara langsung. penulis sering membayangkan bagaimana bahagianya Ibu jika dapat menyaksikan penulis berdiri di titik ini. penulis membayangkan pelukan hangat yang selalu menenangkan, serta doa-doa yang akan Ibu panjatkan untuk masa depan penulis.

Skripsi ini adalah salah satu mimpi yang dahulu ingin penulis tunjukkan kepada Ibu. Walaupun kini Ibu tidak lagi berada di samping penulis, penulis percaya bahwa doa dan cinta Ibu masih menyertai setiap langkah penulis dari tempat yang jauh lebih indah. Setiap lembar yang penulis tulis, setiap perjuangan yang penulis lalui, dan setiap keberhasilan yang penulis raih selalu membawa nama Ibu di dalamnya.

Terima kasih banyak untuk segalanya, Ibu. Penulis akan selalu dan akan terus mencintaimu hingga akhir hayat. Penulis mencintaimu selamanya, Ibu.

9. Saudara kandung penulis Febyola Putri Nursiyah, Amartia Dwi Oktaviani dan M. There Agung Nurmansyah, terimakasih telah memberikan dukungan yang luar biasa sehingga menjadikan semangat penulis untuk segera menyelesaikan pendidikan ini.
10. Sahabat seperjuangan, Della Putri Apriliyanti, Nurchaliza Putri, Puput Permatasari, Amelia Purnama Sari, Henny Juniarti dan Widya Miliaulia Terima kasih telah hadir dan menjadi bagian dari perjalanan hidup penulis. Terima kasih untuk setiap tawa yang kita bagi bersama, setiap cerita yang kita dengarkan satu sama lain, serta setiap dukungan yang diberikan di saat penulis merasa lelah dan hampir menyerah. Terima kasih telah menjadi sahabat yang selalu ada di setiap suka dan duka. terimakasih sudah menemani, mendukung, mendengarkan keluh kesah penulis serta

memberikan bantuan dari awal perkuliahan hingga akhir. Kalian bukan hanya sahabat, tetapi juga keluarga yang dipilih oleh hati.

11. Seluruh teman-teman Akuntansi angkatan 2022 yang telah memberikan pengalaman dan pembelajaran selama dibangku kuliah ini.
12. Semua pihak yang telah membantu hingga terselesaikannya skripsi ini yang tidak dapat penulis sebutkan satu persatu.
12. Terakhir, diri saya sendiri yang sudah berjuang mati-matian selama duduk di bangku perkuliahan. Terimakasih sudah bertahan hingga saat ini walau tidak mudah dan tidak pernah menyerah sesulit apapun prosesnya, ini merupakan pencapaian yang patut dibanggakan untuk diri sendiri. Terima kasih karena tetap kuat ketika keadaan tidak berjalan sesuai harapan. Terima kasih karena selalu berusaha bangkit setelah kegagalan, dan terus melangkah meskipun sering kali dihantui rasa takut, ragu, dan khawatir. Semua perjuangan, pengorbanan, dan kerja keras yang telah dilakukan akhirnya membawamu sampai pada titik ini. Penulis menyadari bahwa skripsi ini masih memiliki banyak kekurangan, Oleh karena itu, kritik dan saran yang membangun sangat diharapkan demi perbaikan di masa yang akan datang. Penulis berharap skripsi ini dapat memberikan manfaat bagi pembaca.

Palembang, 20 Juni 2026

Dhania Kurnia Putri

DAFTAR ISI

	Halaman
HALAMAN PERSETUJUAN SKRIPSI	ii
HALAMAN PENGESAHAN SKRIPSI	iii
MOTTO DAN PERSEMBAHAN.....	iv
PERNYATAAN BEBAS PLAGIAT.....	v
KATA PENGANTAR.....	vi
DAFTAR ISI.....	x
DAFTAR TABEL.....	xiv
DAFTAR GAMBAR.....	xv
ABSTRAK.....	xvi
ABSTRACT.....	xvii
DAFTAR RIWAYAT HIDUP	xviii
BAB I PENDAHULUAN	1
12.1 Latar Belakang	1
12.2 Rumusan Masalah	14
12.3 Tujuan Penelitian.....	15
12.4 Manfaat Penelitian.....	15
BAB II TINJAUAN PUSTAKA.....	17
2.1 Landasan Teori.....	17
2.1.1 <i>Stakeholder Theory</i>	17
2.1.2 Pengungkapan Keamanan Siber	22
2.1.3 Bank Usaha Milik Negara (BUMN) dan Bank Non-BUMN	32

2.1.4 Bank Berukuran Besar dan Bank Berukuran Kecil	34
2.1.5 Profitabilitas Bank	37
2.2 Penelitian Lain Yang Relevan.....	41
2.3 Kerangka Berfikir	44
2.4 Hubungan Antar Variabel.....	46
2.4.1. Pengungkapan Keamanan Siber berdasarkan Status Kepemilikan (BUMN dan Non-BUMN)	46
2.4.2. Pengungkapan Keamanan Siber berdasarkan Ukuran Bank	48
2.4.3. Pengungkapan Keamanan Siber berdasarkan Tingkat Profitabilitas.....	50
2.5 Hipotesis Penelitian.....	52
BAB III METODOLOGI PENELITIAN	54
3.1 Tempat dan Waktu Penelitian.....	54
3.1.1 Tempat Penelitian	54
3.1.2 Waktu Penelitian	55
3.2 Sumber dan Teknik Pengumpulan Data	56
3.2.1 Sumber Data	56
3.2.2 Teknik Pengumpulan Data	57
3.3 Populasi dan Sampel	58
3.3.1 Populasi.....	58
3.3.2 Sampel.....	60
3.4 Rancangan Penelitian	60
3.5 Variabel Penelitian dan Definisi Operasional	61

3.6 Instrumen Penelitian.....	63
3.7 Teknik Analisis Data	64
BAB IV HASIL DAN PEMBAHASAN	72
4.1 Hasil Penelitian	72
4.1.1 Gambaran Umum Objek Penelitian.....	72
4.1.2 Gambaran Umum Subsektor Perbankan	75
4.1.3 Sejarah Singkat Perusahaan Penelitian	76
4.1.4 Proses Pengolahan Data Menggunakan SPSS.....	97
4.1.5 Hasil Pengumpulan Data dan <i>Scoring</i> Pengungkapan Keamanan Siber	99
4.1.6 Statistik Deskriptif	108
4.1.7 Hasil Berdasarkan Status Kepemilikan Bank.....	110
4.1.8 Hasil Berdasarkan Ukuran Bank (KBMI).....	112
4.1.9 Hasil Berdasarkan Profitabilitas Bank	114
4.1.10 Hasil Uji Beda Menggunakan SPSS	117
4.2 Pembahasan	119
4.2.1 Pembahasan Tingkat Pengungkapan Keamanan Siber	119
4.2.2 Pembahasan Berdasarkan Status Kepemilikan.....	121
4.2.3 Pembahasan Berdasarkan Ukuran Bank	123
4.2.4 Pembahasan Berdasarkan Profitabilitas	125
BAB V KESIMPULAN DAN SARAN.....	128
5.1 Kesimpulan	128
5.2 Saran.....	129

DAFTAR PUSTAKA	131
LAMPIRAN	142

DAFTAR TABEL

	Halaman
Tabel 1. 1 Jumlah Halaman Teknologi Informasi dalam Laporan Tahunan Bank Tahun 2018-2022	8
Tabel 2. 1 Indeks Pengungkapan Keamanan Siber	26
Tabel 2. 2 Kriteria Tingkat Pengungkapan Keamanan Siber.....	31
Tabel 2. 3 Penelitian Terdahulu	41
Tabel 3. 1 Daftar Populasi	58
Tabel 3. 2 Definisi Operasional Variabel Penelitian	62
Tabel 4. 1 Karakteristik Objek Penelitian.....	75
Tabel 4. 2 Tahapan Pengolahan Data SPSS.....	99
Tabel 4. 3 Matriks Bukti Pengungkapan Keamanan Siber pada Perusahaan Perbankan Tahun 2025	102
Tabel 4. 4 Ringkasan Tingkat Pengungkapan Keamanan Siber	107
Tabel 4. 5 Hasil Statistik Deskriptif Pengungkapan Keamanan Siber	109
Tabel 4. 6 Pengungkapan Keamanan Siber Berdasarkan Status Kepemilikan...	111
Tabel 4. 7 Pengungkapan Keamanan Siber Berdasarkan KBMI	114
Tabel 4. 8 Pengungkapan Keamanan Siber Berdasarkan Profitabilitas	116
Tabel 4. 9 Ringkasan Hasil Uji Beda Pengungkapan Keamanan Siber	118
Tabel 4. 10 Kriteria Pengambilan Keputusan Uji Beda	119

DAFTAR GAMBAR

	Halaman
Gambar 2. 1 Kerangka Berpikir.....	46

ABSTRAK

Dhania Kurnia Putri, “Pengungkapan Keamanan Siber Pada Perusahaan Sub Sektor Perbankan yang Terdaftar di Bursa Efek Indonesia Periode 2025”. (Di bawah bimbingan Ibu Dr. Rosalina Pebrica Mayasari, SE, AK, M.Si dan Dr. Lia Sari, S.E, M.Si)

Penelitian ini bertujuan untuk mengetahui tingkat pengungkapan keamanan siber pada perusahaan subsektor perbankan yang terdaftar di Bursa Efek Indonesia periode 2025, serta menganalisis perbedaan pengungkapan berdasarkan status kepemilikan, ukuran bank, dan profitabilitas. Penelitian ini menggunakan metode kuantitatif deskriptif dengan sumber data sekunder yang diperoleh dari laporan tahunan dan laporan keberlanjutan perusahaan perbankan.

Sampel dalam penelitian ini berjumlah 46 bank yang dipilih menggunakan teknik sampling jenuh. Pengukuran pengungkapan keamanan siber dilakukan dengan metode *content analysis* berdasarkan 73 item pengungkapan, menggunakan skor 1 apabila item diungkapkan dan skor 0 apabila tidak diungkapkan. Teknik analisis data menggunakan pendekatan kuantitatif melalui indeks pengungkapan keamanan siber dan uji beda menggunakan SPSS.

Hasil penelitian menunjukkan bahwa rata-rata tingkat pengungkapan keamanan siber sebesar 14,38%, sehingga masih tergolong rendah. Hasil uji beda menunjukkan terdapat perbedaan signifikan antara bank BUMN dan bank non-BUMN, sedangkan berdasarkan ukuran bank dan profitabilitas tidak terdapat perbedaan yang signifikan. Penelitian ini menunjukkan bahwa pengungkapan keamanan siber pada sektor perbankan masih perlu ditingkatkan sebagai bentuk transparansi dan tanggung jawab perusahaan kepada stakeholder.

Kata Kunci: Pengungkapan Keamanan Siber, Perbankan, Status Kepemilikan, Ukuran Bank, Profitabilitas.

ABSTRACT

Dhania Kurnia Putri, “Cybersecurity Disclosure in Banking Subsector Companies Listed on the Indonesia Stock Exchange for the 2025 Period.” (Under the supervision of Dr. Rosalina Pebrica Mayasari, SE, AK, M.Si and Dr. Lia Sari, S.E, M.Si)

This study aims to determine the level of cybersecurity disclosure among banking subsector companies listed on the Indonesia Stock Exchange for the 2025 period and to analyze differences in disclosure based on ownership status, bank size, and profitability. This study employed a descriptive quantitative method using secondary data obtained from the annual reports and sustainability reports of banking companies.

The sample consisted of 46 banks selected using a saturated sampling technique. Cybersecurity disclosure was measured through content analysis based on 73 disclosure items, with a score of 1 assigned when an item was disclosed and a score of 0 when it was not disclosed. The data were analyzed quantitatively using the cybersecurity disclosure index and difference tests conducted with SPSS.

The results showed that the average level of cybersecurity disclosure was 14.38%, indicating that it remained relatively low. The difference test results revealed a significant difference between state-owned banks and non-state-owned banks. However, no significant differences were found based on bank size and profitability. These findings indicate that cybersecurity disclosure in the banking sector still needs to be improved as a form of corporate transparency and accountability to stakeholders.

Keywords: Cybersecurity Disclosure, Banking, Ownership Status, Bank Size, Profitability.

DAFTAR RIWAYAT HIDUP

Dhania Kurnia Putri lahir di Palembang pada tanggal 13 Juni 2004. Penulis merupakan anak Terakhir dari 4 bersaudara, pasangan dari Bapak Amril Nurman dan Almh Ibu Siti Syamsiah, Pendidikan formal yang telah di tempuh dimulai dari Mi Marfu'ah Palembang, kemudian melanjutkan Pendidikan Sekolah menengah pertama MTs Marfuah Palembang Selanjutnya menyelesaikan Sekolah Menengah SMA Tunas Bangsa Palembang. Hingga saat ini, penulis menempuh Pendidikan tinggi pada program Studi S1 Akutansi, Fakultas Ekonomi dan Bisnis Universitas Tridianti.

BAB I

PENDAHULUAN

1.1 Latar Belakang

Perkembangan teknologi informasi telah mendorong transformasi digital yang sangat pesat dalam berbagai sektor, termasuk sektor perbankan. Digitalisasi memungkinkan layanan keuangan menjadi lebih efisien, cepat, dan mudah diakses oleh masyarakat tanpa batasan ruang dan waktu. Perbankan tidak lagi hanya berfungsi sebagai lembaga intermediasi keuangan, tetapi juga sebagai penyedia layanan berbasis teknologi. Inovasi seperti *Mobile Banking* dan *Internet Banking* menjadi bagian penting dalam operasional bank modern. Hal ini menunjukkan bahwa teknologi telah menjadi fondasi utama dalam industri perbankan. Oleh karena itu, transformasi digital menjadi kebutuhan yang tidak dapat dihindari (Widya et al., 2025).

Namun, di balik kemajuan tersebut, digitalisasi juga membawa berbagai risiko baru yang harus dihadapi oleh perusahaan, khususnya pada sektor perbankan. Ketergantungan bank terhadap sistem teknologi informasi dapat meningkatkan potensi terjadinya gangguan operasional apabila tidak diimbangi dengan sistem keamanan yang memadai. Risiko keamanan siber pada sektor perbankan dapat berupa penyalahgunaan data, peretasan sistem, pencurian informasi nasabah, *malware*, *phishing*, *ransomware*, serta gangguan terhadap sistem layanan digital. Ancaman tersebut menjadi semakin penting karena layanan perbankan saat ini banyak bergantung pada

sistem digital seperti *mobile banking*, *internet banking*, dan transaksi elektronik. Apabila risiko tersebut tidak dikelola dengan baik, perusahaan dapat mengalami kerugian finansial, terganggunya aktivitas operasional, menurunnya reputasi, serta berkurangnya kepercayaan nasabah dan *stakeholder*. Semakin kompleks sistem teknologi yang digunakan, semakin besar pula potensi risiko yang harus dikelola oleh perusahaan. Oleh karena itu, perusahaan perbankan perlu memiliki strategi mitigasi risiko yang efektif agar mampu menjaga keamanan data, stabilitas layanan, dan kepercayaan *stakeholder*. Ancaman keamanan siber menjadi salah satu tantangan utama dalam era digital saat ini (Setiawan, 2025).

Peningkatan penggunaan layanan digital seperti *Mobile Banking* dan aplikasi keuangan turut meningkatkan potensi terjadinya serangan siber. Transaksi elektronik membuka peluang bagi pihak yang tidak bertanggung jawab untuk melakukan penyusupan sistem. Risiko ini semakin kompleks seiring dengan perkembangan teknologi yang semakin canggih. Perusahaan dituntut untuk mampu melindungi sistem informasi yang dimiliki secara optimal. Kegagalan dalam menjaga keamanan dapat berdampak serius terhadap operasional perusahaan. Oleh karena itu, keamanan siber menjadi isu strategis dalam industri perbankan (Jamil et al., 2023).

Ancaman keamanan siber tidak hanya berdampak pada aspek teknis, tetapi juga pada aspek keuangan dan reputasi perusahaan. Serangan seperti *hacking*, *phishing*, dan *malware* merupakan bentuk ancaman yang umum terjadi dalam sistem informasi modern. *Hacking* adalah aktivitas penyusupan

ke dalam sistem komputer atau jaringan secara tidak sah tanpa izin pemiliknya, yang bertujuan untuk mengakses, mencuri, atau merusak data penting dalam sistem (Siringoringo et al., 2023). Sementara itu, *phishing* merupakan bentuk kejahatan siber yang dilakukan dengan cara menipu korban agar memberikan informasi pribadi seperti username, password, maupun data keuangan melalui media yang menyerupai pihak resmi, seperti *email* atau *website* palsu (Tabrani et al., 2024). Adapun *malware* (*malicious software*) adalah perangkat lunak berbahaya yang dirancang untuk merusak, mengganggu, atau menyusup ke dalam sistem komputer, yang mencakup *virus*, *trojan*, *worm*, dan *ransomware* (Fleury & Dubrunquez, 2021).

Ketiga bentuk ancaman tersebut dapat menyebabkan kerugian finansial yang signifikan bagi perusahaan, khususnya di sektor perbankan. Selain itu, kebocoran data nasabah akibat serangan siber juga dapat menurunkan tingkat kepercayaan masyarakat terhadap perusahaan. Kepercayaan merupakan aset utama dalam industri perbankan yang berbasis pada kepercayaan publik. Oleh karena itu, perusahaan harus mampu mengelola risiko siber secara efektif. Upaya perlindungan sistem menjadi sangat penting dalam menjaga keberlangsungan usaha.

Dalam konteks perbankan, keamanan siber memiliki peran yang sangat vital karena bank mengelola data keuangan yang bersifat sensitif. Informasi nasabah, transaksi, serta sistem pembayaran merupakan aset penting yang harus dilindungi. Kegagalan dalam menjaga keamanan informasi dapat menimbulkan dampak luas terhadap stabilitas sistem keuangan. Risiko ini

juga dapat memicu gangguan operasional yang berkelanjutan. Oleh karena itu, perusahaan perbankan perlu memiliki sistem keamanan yang kuat. Hal ini bertujuan untuk memastikan seluruh aktivitas berjalan dengan aman dan terkendali (Jamil et al., 2023).

Salah satu kasus serangan siber di sektor perbankan Indonesia terjadi pada Bank Syariah Indonesia (BSI) pada Mei 2023. Pada saat itu, layanan BSI mengalami gangguan yang berdampak pada sejumlah layanan perbankan, seperti mobile banking, ATM, dan layanan transaksi nasabah. Gangguan tersebut kemudian dikaitkan dengan dugaan serangan ransomware oleh kelompok *LockBit* 3.0, yang mengklaim telah mencuri data dalam jumlah besar dari sistem BSI. Beberapa laporan menyebutkan bahwa data yang diduga bocor mencapai sekitar 1,5 TB dan mencakup data nasabah. Kasus ini menunjukkan bahwa ancaman keamanan siber pada sektor perbankan tidak hanya berdampak pada aspek teknologi informasi, tetapi juga dapat mengganggu layanan operasional, menimbulkan risiko kebocoran data, serta memengaruhi kepercayaan nasabah terhadap lembaga perbankan (Maulana et al., 2024).

Di Indonesia, tingkat ancaman keamanan siber menunjukkan tren yang terus meningkat dari waktu ke waktu. Sektor keuangan menjadi salah satu sektor yang paling rentan terhadap serangan siber. Tingginya jumlah insiden menunjukkan bahwa perlindungan sistem informasi masih perlu ditingkatkan. Kondisi ini mendorong perusahaan untuk lebih memperhatikan aspek keamanan informasi. Selain itu, perusahaan juga perlu meningkatkan

transparansi terkait pengelolaan risiko siber. Hal ini penting untuk meningkatkan kepercayaan *stakeholder* (Naufal & Azmi, 2024).

Transparansi menjadi salah satu aspek penting dalam tata kelola perusahaan modern, khususnya pada sektor perbankan yang memiliki tingkat kepercayaan publik yang tinggi. Perusahaan tidak hanya dituntut untuk menjaga keamanan sistem, tetapi juga untuk mengungkapkan informasi terkait risiko yang dihadapi, termasuk risiko keamanan siber. Salah satu bentuk transparansi tersebut adalah pengungkapan keamanan siber dalam laporan tahunan perusahaan. Informasi ini memberikan gambaran mengenai kesiapan perusahaan dalam menghadapi ancaman digital serta kemampuan dalam mengelola risiko teknologi informasi. Semakin transparan perusahaan dalam mengungkapkan informasi tersebut, semakin tinggi tingkat kepercayaan yang diperoleh dari investor dan *stakeholder*. Oleh karena itu, pengungkapan keamanan siber menjadi bagian penting dalam praktik *Good Corporate Governance* serta diduga memiliki pengaruh terhadap persepsi dan penilaian terhadap Perusahaan (Hendra, 2024).

Pengungkapan keamanan siber merupakan salah satu bentuk pengungkapan sukarela yang dilakukan perusahaan. Informasi ini tidak selalu diwajibkan secara rinci dalam regulasi, namun memiliki peran penting dalam meningkatkan akuntabilitas perusahaan. Dalam praktiknya, tingkat pengungkapan antar perusahaan masih menunjukkan variasi yang signifikan (Kurnia, 2025). Sebagian perusahaan mengungkapkan secara rinci, sementara yang lain masih terbatas. Perbedaan ini menunjukkan adanya variasi

kebijakan dalam penyampaian informasi. Hal ini menjadi fenomena yang menarik untuk diteliti lebih lanjut (Healy, 2001)

Dalam perspektif teori *stakeholder*, perusahaan memiliki tanggung jawab untuk memenuhi kebutuhan informasi para pemangku kepentingan. *stakeholder* tidak hanya terdiri dari pemegang saham, tetapi juga mencakup masyarakat dan pemerintah. Perusahaan harus menjaga hubungan yang baik dengan *stakeholder* melalui transparansi informasi. Pengungkapan keamanan siber menjadi salah satu bentuk tanggung jawab tersebut. Hal ini menunjukkan bahwa perusahaan mampu mengelola risiko dengan baik. Dengan demikian, kepercayaan *stakeholder* dapat tetap terjaga (Freeman & Phillips, 2021).

Pengungkapan keamanan siber berkaitan erat dengan reputasi perusahaan karena informasi yang disampaikan kepada publik mencerminkan bagaimana perusahaan mengelola risiko yang dihadapi. Transparansi dalam pengungkapan memberikan sinyal positif kepada investor dan masyarakat mengenai kesiapan perusahaan dalam menghadapi ancaman siber, sehingga dapat meningkatkan kepercayaan. Sebaliknya, keterbatasan atau kurangnya pengungkapan berpotensi menimbulkan ketidakpastian informasi yang dapat memengaruhi persepsi pasar terhadap perusahaan. Oleh karena itu, pengungkapan keamanan siber menjadi salah satu strategi penting dalam meningkatkan reputasi sekaligus nilai perusahaan (Zaroh & Purwaningsih, 2026).

Untuk memperkuat fenomena tersebut, penelitian sebelumnya menunjukkan bahwa keamanan siber masih bervariasi antar perusahaan. Hal ini terlihat dari perbedaan jumlah dan kedalaman informasi yang disajikan dalam laporan tahunan. Sebagian perusahaan telah mengungkapkan secara rinci, sementara lainnya masih terbatas (Sari, 2025). Variasi ini mencerminkan perbedaan tingkat kesadaran perusahaan terhadap pentingnya transparansi. Kondisi ini menunjukkan bahwa pengungkapan belum dilakukan secara optimal. Oleh karena itu, fenomena ini penting untuk diteliti lebih lanjut.

Data empiris menunjukkan bahwa masih terdapat perusahaan yang belum mengungkapkan informasi terkait teknologi informasi secara memadai. Selain itu, sebagian besar perusahaan hanya menyampaikan informasi dalam jumlah yang terbatas. Kondisi ini mengindikasikan bahwa pengungkapan keamanan siber belum sepenuhnya mencerminkan kompleksitas risiko yang dihadapi. Kurangnya informasi dapat menimbulkan ketidakpastian bagi investor. Hal ini berpotensi memengaruhi keputusan investasi yang diambil. Oleh karena itu, pengungkapan menjadi isu penting dalam penelitian ini.

Salah satu indikator yang dapat digunakan untuk melihat tingkat perhatian perusahaan terhadap teknologi informasi adalah melalui jumlah pengungkapan terkait teknologi dalam laporan tahunan. Semakin banyak informasi yang disampaikan, maka menunjukkan semakin tinggi tingkat

perhatian perusahaan terhadap aspek teknologi, termasuk dalam pengelolaan keamanan siber (Sari, 2025).

Tabel 1. 1
Jumlah Halaman Teknologi Informasi dalam Laporan Tahunan Bank
Tahun 2018-2022

No.	Jumlah Halaman	Jumlah Laporan Tahunan Bank	Persentase
1	0	43	19,19
2	1-5	103	45,98
3	6-10	45	20,09
4	11-15	19	8,48
5	16-20	12	5,36
6	>20	2	0,9
Total		224	100

Sumber: Sari, 2025

Berdasarkan Tabel 1.1, dapat diketahui bahwa dari 224 laporan tahunan bank yang dianalisis selama periode 2018–2022, masih terdapat 43 laporan atau sebesar 19,19% yang sama sekali tidak mengungkapkan informasi terkait teknologi informasi. Kondisi ini menunjukkan bahwa sebagian bank belum memberikan perhatian yang memadai terhadap transparansi informasi teknologi dalam laporan tahunan. Selain itu, sebanyak 103 laporan atau sebesar 45,98% hanya mengungkapkan informasi teknologi informasi dalam jumlah terbatas, yaitu 1–5 halaman. Artinya, sebagian besar bank masih menyampaikan informasi teknologi informasi secara singkat dan belum menggambarkan secara mendalam mengenai pengelolaan risiko teknologi, termasuk risiko keamanan siber (Sari, 2025).

Jika dilihat lebih lanjut, hanya 45 laporan atau 20,09% yang mengungkapkan informasi teknologi informasi sebanyak 6–10 halaman, 19 laporan atau 8,48% sebanyak 11–15 halaman, 12 laporan atau 5,36%

sebanyak 16–20 halaman, dan hanya 2 laporan atau 0,9% yang mengungkapkan lebih dari 20 halaman. Data ini memperlihatkan bahwa semakin tinggi jumlah halaman pengungkapan, semakin sedikit jumlah bank yang melakukannya. Dengan demikian, dapat disimpulkan bahwa pengungkapan informasi teknologi informasi pada sektor perbankan masih rendah dan belum merata. Rendahnya pengungkapan tersebut dapat mencerminkan masih terbatasnya kesadaran perusahaan terhadap pentingnya transparansi risiko teknologi dan keamanan siber kepada *stakeholder*. Oleh karena itu, data ini memperkuat pentingnya penelitian mengenai pengungkapan keamanan siber pada perusahaan subsektor perbankan yang terdaftar di Bursa Efek Indonesia

Temuan ini menunjukkan bahwa tingkat pengungkapan teknologi informasi, termasuk aspek keamanan siber, masih belum merata di antara perusahaan perbankan. Sebagian besar perusahaan cenderung menyampaikan informasi secara terbatas, yang dapat mengindikasikan bahwa pengungkapan terkait keamanan siber belum menjadi prioritas utama dalam laporan tahunan.

Kondisi ini menjadi penting untuk dikaji lebih lanjut, mengingat meningkatnya kebutuhan *stakeholder* terhadap transparansi informasi, khususnya yang berkaitan dengan perlindungan data dan keamanan sistem.

Oleh karena itu, penelitian ini berfokus untuk menganalisis pengungkapan keamanan siber pada perusahaan subsektor perbankan yang terdaftar di Bursa Efek Indonesia periode 2025.

Di samping itu, penelitian mengenai pengungkapan keamanan siber di Indonesia masih tergolong terbatas, padahal isu ini semakin penting dalam era digital, khususnya pada sektor perbankan yang memiliki tingkat risiko tinggi terhadap ancaman siber (Hidayah & Ananda, 2025). Penelitian sebelumnya lebih banyak membahas pengungkapan risiko teknologi atau keamanan siber secara umum, serta hanya meneliti faktor tertentu seperti ukuran perusahaan, struktur tata kelola, profitabilitas, atau umur perusahaan (Tri Wahyu & Masiyah, 2024). Dengan demikian, masih terdapat keterbatasan penelitian yang secara spesifik membandingkan tingkat pengungkapan keamanan siber pada perusahaan perbankan berdasarkan status kepemilikan bank, ukuran bank berdasarkan Kelompok Bank berdasarkan Modal Inti (KBMI), tingkat profitabilitas, dan umur bank secara bersamaan.

Selain itu, penelitian terdahulu belum banyak menggunakan indeks pengungkapan keamanan siber yang lebih komprehensif dan berbasis pada 73 item pengungkapan yang mencakup aspek risiko, tata kelola teknologi informasi, perlindungan data, pengujian keamanan, pemulihan insiden, serta pelaporan insiden keamanan siber. Oleh karena itu, penelitian ini dilakukan untuk mengisi kesenjangan tersebut dengan menganalisis pengungkapan keamanan siber pada perusahaan subsektor perbankan yang terdaftar di Bursa Efek Indonesia periode 2025.

Pemilihan periode 2025 dalam penelitian ini didasarkan pada pertimbangan bahwa laporan tahunan tahun 2025 merupakan data terbaru

yang dapat digunakan untuk melihat praktik pengungkapan keamanan siber perusahaan perbankan setelah adanya penguatan regulasi terkait teknologi informasi dan keamanan siber. OJK menerbitkan POJK Nomor 11/POJK.03/2022 tentang Penyelenggaraan Teknologi Informasi oleh Bank Umum yang mengatur penyelenggaraan teknologi informasi dalam operasional bank (OJK, 2022).

Selain itu, OJK juga menerbitkan SEOJK Nomor 29/SEOJK.03/2022 tentang Ketahanan dan Keamanan Siber bagi Bank Umum sebagai pedoman khusus mengenai ketahanan dan keamanan siber perbankan. Regulasi tersebut mendorong bank untuk lebih memperhatikan tata kelola teknologi informasi, manajemen risiko siber, perlindungan data, serta penanganan insiden siber. Oleh karena itu, tahun 2025 dipilih karena dinilai relevan untuk melihat sejauh mana perusahaan perbankan telah mengungkapkan informasi keamanan siber setelah regulasi tersebut berjalan dalam beberapa tahun (KPMG, 2023).

Pengungkapan keamanan siber menjadi aspek penting dalam menghadapi perkembangan teknologi digital yang semakin pesat, khususnya pada sektor perbankan yang memiliki tingkat risiko tinggi terhadap ancaman siber. Perusahaan perbankan dituntut untuk menyampaikan informasi terkait pengelolaan risiko keamanan siber sebagai bentuk transparansi kepada publik (Jubaedah et al., 2025). Praktik pengungkapan ini mencerminkan sejauh mana perusahaan memberikan informasi mengenai perlindungan sistem dan data yang dimiliki. Oleh karena itu, pengungkapan keamanan siber menjadi hal

yang penting untuk diperhatikan dalam konteks perusahaan perbankan di era digital saat ini.

Perbedaan pengungkapan keamanan siber pada perusahaan perbankan dapat dilihat dari tingkat keluasan, kedalaman, dan keterbukaan informasi yang disampaikan oleh masing-masing bank. Dalam konteks ini, perbedaan tersebut dapat terjadi antara bank BUMN dan bank non-BUMN. Bank BUMN umumnya memiliki tanggung jawab publik yang lebih besar karena berkaitan langsung dengan kepentingan masyarakat luas dan pengawasan pemerintah (Hidayah & Ananda, 2025). Oleh karena itu, bank BUMN cenderung dituntut untuk lebih transparan dalam menyampaikan informasi mengenai pengelolaan risiko keamanan siber. Sementara itu, bank non-BUMN juga memiliki kewajiban untuk menjaga keamanan data nasabah, namun tingkat pengungkapan yang disampaikan dapat berbeda tergantung pada kebijakan internal, kapasitas sumber daya, dan strategi masing-masing perusahaan (OJK, 2021).

Perbedaan tingkat pengungkapan keamanan siber tersebut diduga dipengaruhi oleh beberapa faktor. Pertama, perbedaan status kepemilikan antara bank BUMN dan non-BUMN dapat memengaruhi tingkat transparansi, karena bank BUMN cenderung memiliki tuntutan akuntabilitas publik yang lebih tinggi (Aulia & Bachtiar, 2026). Kedua, ukuran bank berdasarkan total aset juga berpotensi memengaruhi luas pengungkapan, karena bank yang lebih besar umumnya memiliki sumber daya, kompleksitas operasional, serta tingkat risiko yang lebih tinggi (Supratiwi, 2024). Ketiga, profitabilitas bank

dapat mencerminkan kemampuan perusahaan dalam mendukung investasi keamanan siber serta mendorong pengungkapan sebagai sinyal positif kepada para pemangku kepentingan

Berdasarkan kondisi di atas, terdapat kesenjangan antara teori dan praktik dalam pengungkapan keamanan siber. Secara teori, dalam perspektif teori *stakeholder*, perusahaan diharapkan menyampaikan informasi secara transparan guna memenuhi kebutuhan informasi para pemangku kepentingan, termasuk terkait pengelolaan risiko keamanan siber. Namun, dalam praktiknya pada perusahaan subsektor perbankan yang terdaftar di Bursa Efek Indonesia, tingkat pengungkapan keamanan siber masih menunjukkan variasi yang signifikan antar perusahaan. Kondisi ini menunjukkan adanya kesenjangan yang perlu diteliti lebih lanjut. Oleh karena itu, penelitian ini diharapkan dapat memberikan pemahaman yang lebih mendalam serta kontribusi dalam bidang akademik terkait pengungkapan keamanan siber.

Penelitian ini difokuskan pada perusahaan subsektor perbankan yang terdaftar di Bursa Efek Indonesia. Pemilihan sektor ini didasarkan pada tingkat risiko siber yang tinggi serta peran strategis dalam perekonomian. Selain itu, perusahaan perbankan memiliki tingkat ketergantungan yang tinggi terhadap teknologi informasi. Hal ini menjadikan sektor perbankan relevan untuk dikaji dalam konteks keamanan siber. Hasil penelitian diharapkan dapat memberikan kontribusi praktis. Terutama bagi perusahaan dan investor dalam pengambilan keputusan.

Dengan demikian, penelitian ini bertujuan untuk menganalisis pengungkapan keamanan siber pada perusahaan subsektor perbankan yang terdaftar di Bursa Efek Indonesia tahun 2025. Penelitian ini diharapkan dapat memberikan gambaran mengenai praktik pengungkapan keamanan siber pada perusahaan perbankan di Indonesia. Selain itu, penelitian ini juga diharapkan dapat menjadi referensi bagi penelitian selanjutnya dalam bidang pengungkapan informasi perusahaan. Oleh karena itu, penelitian ini memiliki nilai penting secara teoritis dan praktis.

1.2 Rumusan Masalah

Berdasarkan latar belakang yang telah dijelaskan maka dapat dirumuskan permasalahan dalam penelitian ini sebagai berikut :

1. Bagaimana tingkat pengungkapan keamanan siber pada perusahaan subsektor perbankan yang terdaftar di Bursa Efek Indonesia periode 2025?
2. Apakah terdapat perbedaan tingkat pengungkapan keamanan siber antara bank BUMN dan bank non-BUMN?
3. Apakah terdapat perbedaan tingkat pengungkapan keamanan siber pada perusahaan subsektor perbankan yang terdaftar di Bursa Efek Indonesia periode 2025 berdasarkan empat kategori ukuran bank, yaitu KBMI 1, KBMI 2, KBMI 3, dan KBMI 4?
4. Apakah terdapat perbedaan tingkat pengungkapan keamanan siber pada bank dengan profitabilitas tinggi, sedang dan rendah?

1.3 Tujuan Penelitian

Tujuan yang ingin dicapai dalam penelitian ini adalah untuk mengetahui:

1. Untuk mengetahui tingkat pengungkapan keamanan siber pada perusahaan subsektor perbankan yang terdaftar di Bursa Efek Indonesia periode 2025.
2. Untuk menganalisis perbedaan tingkat pengungkapan keamanan siber antara bank BUMN dan bank non-BUMN.
3. Untuk menganalisis perbedaan tingkat pengungkapan keamanan siber pada perusahaan subsektor perbankan yang terdaftar di Bursa Efek Indonesia periode 2025 berdasarkan empat kategori ukuran bank, yaitu KBMI 1, KBMI 2, KBMI 3, dan KBMI 4.
4. Untuk menganalisis perbedaan tingkat pengungkapan keamanan siber pada bank dengan profitabilitas tinggi, sedang dan rendah.

1.4 Manfaat Penelitian

1. Manfaat Teoritis

Penelitian ini diharapkan dapat memberikan kontribusi dalam pengembangan ilmu akuntansi, khususnya terkait pengungkapan informasi non-keuangan mengenai keamanan siber pada perusahaan perbankan. Selain itu, penelitian ini juga dapat menjadi referensi bagi penelitian selanjutnya yang berkaitan dengan pengungkapan keamanan siber.

2. Manfaat Praktis

a. Bagi Perusahaan Perbankan

Penelitian ini diharapkan dapat memberikan gambaran mengenai praktik pengungkapan keamanan siber sehingga dapat menjadi bahan pertimbangan dalam meningkatkan kualitas pengungkapan informasi kepada publik.

b. Bagi Investor

Penelitian ini diharapkan dapat memberikan informasi tambahan terkait pengungkapan keamanan siber pada perusahaan perbankan sebagai bahan pertimbangan dalam pengambilan keputusan.

c. Bagi Peneliti Selanjutnya

Penelitian ini diharapkan dapat menjadi referensi dan bahan perbandingan untuk penelitian selanjutnya yang berkaitan dengan pengungkapan keamanan siber.

DAFTAR PUSTAKA

- Alsadoun, A. A., & Albaz, M. M. (2025). the Impact of Cybersecurity Risk Disclosure and Governance on Firm Value and Stock Return Volatility. *Journal of Governance and Regulation*, 14(1), 194–205. <https://doi.org/10.22495/jgrv14i1art18>
- Angelina Septiani Zaroh dan Sri Budi Purwaningsih. (2026). Personal Data Protection in Banking Cybersecurity Breach Cases: Perlindungan Data Pribadi dalam Kasus Pelanggaran Keamanan Siber di Sektor Perbankan. *Indonesian Journal of Law and Economics Review*, 21(1), 1–13. <https://doi.org/10.21070/ijler.v21i1.1533>
- Arditya, D., Priangga, H., Soelistya, D., Jekti, D., & Andayani, Y. (2019). Jurnal Pengkajian Ilmu dan Pembelajaran Matematika dan IPA. *Prisma Sains*, 1(2), 4.
- Aulia, I., & Bachtiar, Y. (2026). Pengaruh Dewan Komisaris Independen, Komite Audit, Good Corporate Governance dan Kinerja Keuangan terhadap Pengungkapan Sustainability Report : Studi pada Perusahaan BUMN yang Terdaftar di IDX-MES BUMN 17 Tahun 2021-2024. *Ascendia : Journal of Economic and Business Advancement*, 1(3), 195–211.
- Bachtiar, A., Barizki, R. N., & Pranawukir, I. (2024). Strategi Komunikasi Efektif Dalam Menjalin Hubungan Baik dengan Stakeholder Korporat dan Politik. *PUBLISITAS Jurnal of Social Sciences and Politics*, 11(1), 96–113.
- Balaka, M. Y. (2022). Metode penelitian Kuantitatif. *Metodologi Penelitian Pendidikan Kualitatif*, 1, 130.

- Chandra, A., & Setyawan, I. R. (2023). Pengaruh Ukuran Perusahaan, Likuiditas, dan Profitabilitas Terhadap Struktur Modal Perbankan Tahun 2017-2021. *Jurnal Manajerial Dan Kewirausahaan*, 5(4), 838–847.
- Dadang Suhendar, D. R. H. (2021). Pengungkapan Sukarela Berdasarkan Karakteristik Perusahaan dan Kepemilikan Institusional. *Jurnal Akuntansi Berkelanjutan Indonesia*, 4(1), 16–30.
- Elsayed, D. H., Ismail, T. H., & Ahmed, E. A. (2024). The impact of cybersecurity disclosure on banks' performance: the moderating role of corporate governance in the MENA region. *Future Business Journal*, 10(1), 1–15. <https://doi.org/10.1186/s43093-024-00402-9>
- Febriany, N., Marwa, T., & Yusrianti, H. (2025). Impact of Information Disclosure on Banking Risk. *Journal of International Conference Proceedings (JICP)*, 7(5), 1196–1204.
- Firoozi, M. S. M. (2008). Cybersecurity Disclosure in the Banking Industry: A Comparative Study. *Regulation*, 44(June), 1–21.
- Fleury, N., & Dubrunquez, T. (2021). *PDF-Malware : An Overview on Threats , Detection and Evasion Attacks*.
- Freeman, R. E. (2010a). *A Stakeholder Approach to Strategic Management*. 01.
- Freeman, R. E. (2010b). *Strategic Management*. Cambridge University.
- Freeman, R. E., & Phillips, R. A. (2002). Stakeholder Theory: A Libertarian Defense. *Business Ethics Quarterly*, 12(3), 331–349.
- Freeman, R. E., & Phillips, R. A. (2021). Stakeholder Theory and the Resource-Based View of the Firm. *Journal of Management*, 47(7), 1757–1770.

<https://doi.org/10.1177/0149206321993576>

- Gauch, K., Georg, L., Elodie, S., & Enrico, B. (2026). European Cybersecurity Disclosure Practices : A Textual Analysis. *International Journal of Disclosure and Governance*. <https://doi.org/10.1057/s41310-025-00327-x>
- Guthrie, J. (2006). Content Analysis of Social, Environmental Reporting : What is New? *Journal of Human Resource Costing & Accounting*, 10(2), 114–126.
- Harrison, J. S., Freeman, R. E., Harrison, J. S., & Freeman, R. E. (2015). Stakeholder Theory As an Ethical Approach to Effective Management : Applying The Theory to Multiple Contexts. *Review of Business Management*, 17(55), 858–869. <https://doi.org/10.7819/rbgn.v17i55.2647>
- Hawashe, A. A. (2015). Commercial Banks' Attributes and Annual Voluntary Disclosure : The Case of Libya. *International Journal of Accounting and Financial Reporting*, 5(2), 208–233. <https://doi.org/10.5296/ijafr.v5i2.8684>
- Haziq, M., Hafiz, A., Yusof, M., Muhammad, K., Sabarudin, A., & Ghani, E. K. (2021). Can Internal Control, Rules and Regulations and Technology Adoption influence Bank' s Protection of Customers' Data Security? *International Journal of Academic Research in Business and Social Science*, 1(9), 1276–1290. <https://doi.org/10.6007/IJARBSS/v11-i9/10855>
- Healy, P. M., & Palepu, K. G. (2001). Information asymmetry , corporate disclosure , and the capital markets : A review of the empirical disclosure literature. *Journal of Accounting and Economics*, 31, 405–440.
- Hendra, J., Wulandari, T., Ramadhani, S., & Aprilia, N. I. (2025). Analisis Profitabilitas atau Rentabilitas. *Jurnal Ekonomi Bisnis Dan Akuntansi*,

5(April), 114–126.

Hendra, M. (2024). Manfaat dan Urgensi Penerapan Good Corporate Governance dalam Perusahaan. *Jurnal Pendidikan Tambusai*, 8(2), 35477–35485.

Hidayah, E., & Ananda, K. (2025). Cybersecurity Disclosure: Analysis on Banking Companies Listed on the Indonesia Stock Exchange. *International Journal of Economics, Business and Management Research*, 09(12), 237–254.
<https://doi.org/10.51505/ijebmr.2025.91212>

Isnaini, M., Afgani, M. W., Haqqi, A., & Azhari, I. (2025). Teknik Analisis Data Uji Normalitas. *J-CEKI : Jurnal CendekiaIlmiah*, 4(2), 1377–1384.

Jamil, S., Irawan, C. P., & Denpasar, U. M. (2023). Cybersecurity as the Foundation for the Development of Mobile Financial Applications : A Literature Study on Cybercrime and Its Mitigation. *Jurnal Ekonomi, Manajemen, Dan Bisnis*, 1(May), 23–30.

Joshua, L. S. S. (2025). Pengaruh Struktur Modal, Ukuran Perusahaan dan Likuiditas Terhadap Profitabilitas Perusahaan Perbankan (Studi Kasus Perusahaan Perbankan di Indonesia Tahun 2020-2023). *Jurnal Ilmiah Manajemen Ekonomi Dan Akuntansi*, 2(3), 37–47.

Jubaedah, S., Musta, A., Nurlisti, I., & Maulana, B. A. (2025). Cyber risk management disclosure : a stakeholder theory perspective. *Diponegoro International Journal of Business*, 7(2), 133–146.
<https://doi.org/10.14710/dijb.7.2.2024.133-146>

KPMG. (2023). *Ketahanan dan Keamanan Siber bagi Sektor Perbankan Indonesia* (p. 2). <https://assets.kpmg.com/content/dam/kpmg/id/pdf/2023/01/id-seojk->

cyber-newsflash-jan23.pdf

- Kuckartz, U., & Rädiker, S. (2024). *Integrating Artificial Intelligence (AI) in Qualitative Content Analysis*. December, 1–16. www.qca-method.net
- Li, L., & Zheng, X. (2023). The Effect of Sustainability Information Disclosure on the Cost of Equity Capital : An Empirical Analysis Based on Gartner Top 50 Supply Chain Rankings. *Journal Risk Financial Management*, 16, 1–18.
- Lubis, F. K., Wulandari, K. F., Azhari, N., Islam, U., Utara, S., Islam, U., Utara, S., Islam, U., Utara, S., Islam, U., & Utara, S. (2025). Peran Keamanan Siber dalam Meningkatkan Transparansi dan Akuntabilitas terhadap Laporan Keuangan di Bank Syariah Indonesia. *Jurnal Bisnis Net*, 8(1), 496–505.
- Mahajan, R., Marc, W., Sareen, M., Kumar, S., & Panwar, R. (2023). Stakeholder theory. *Journal of Business Research*, 166(June), 1–16. <https://doi.org/10.1016/j.jbusres.2023.114104>
- Marwan. (2023). *Cyber Security Framework Selection : Comparision Of Nist And Iso27001*. 3(1), 245–255.
- Maulana, N., Laurens, T., Faiz, H. A., & Patrianti, T. (2024). Manajemen Krisis PT. BSI Tbk Pasca Peretasan Data Nasabah. *INNOVATIVE: Journal Of Social Science Research*, 4(1), 8244–8258.
- Maulana, W., Mualim, A., Yul, F., Marta, D., & Meiyenti, I. (2025). Comprehensive Cybersecurity Framework for Digital Governance: Threat Assessment, Risk Mitigation, and Regulatory Compliance in Indonesia. *Jurnal Teknik Informatika Dan Teknologi Informasi*, 5(3), 434–450.
- Mazumder, M. M. M., & Hossain, D. M. (2023). Voluntary Cybersecurity

- Disclosure in the Banking Industry of Bangladesh: Does Board Composition Matter? *Journal of Accounting in Emerging Economies*, 13(2), 217–239.
<https://doi.org/10.1108/JAEE-07-2021-0237>
- Muhammad Razan Iftikaar, Ia Kurnia, W. H. (2025). Faktor-Faktor Yang Berpengaruh Terhadap Tingkat Pengungkapan Sukarela Pada Perusahaan Yang Terdaftar di Jakarta Islamic Index. *JIAI (Jurnal Ilmiah Akuntansi Indonesia)*, 10(2), 1–17.
- Muin, A. (2023). *Metode Penelitian Kuantitatif* (1st ed.). CV. Literasi Nusantara Abadi.
- Nasution, A. H., Nasution, B., Saidin, O. K., & Sunarmi. (2020). Transparency of Information Disclosure in the Management of State-Owned Enterprises. *Advances in Social Science, Education and Humanities Research*, 413, 25–28.
<https://doi.org/10.2991/assehr.k.200306.174>
- Naufal, M., & Azmi, A. (2024). Analisa Kasus Kebocoran Data pada Bank Indonesia Dalam Sistem Perbankan. *Jurnal Multidisiplin Ilmu Akademik*, 1(6), 448–458.
- OJK. (2021). *Consultative Paper Manajemen Risiko Keamanan Siber Bank Umum*. Otoritas Jasa Keuangan. (2023). Peraturan OJK No 12 Tahun 2023 - Unit Usaha Syariah. *Www.Ojk.Go.Id*, 1–23.
[https://www.ojk.go.id/id/regulasi/Documents/Pages/Peraturan-Otoritas-Jasa-Kuangan-Nomor-12-Tahun-2023-tentang-Unit-Usaha-Syariah-%28POJK-UUS%29/POJK 12 Tahun 2023 - UNIT USAHA SYARIAH.pdf](https://www.ojk.go.id/id/regulasi/Documents/Pages/Peraturan-Otoritas-Jasa-Kuangan-Nomor-12-Tahun-2023-tentang-Unit-Usaha-Syariah-%28POJK-UUS%29/POJK%2012%20Tahun%2023%20-%20UNIT%20USAHA%20SYARIAH.pdf)
- POJK 11/2022. (2022). *Penyelenggaraan Teknologi Informasi Oleh Bank Umum*

(p. 33).

- R. Edward Freeman, Jeffrey S. Harrison, S. Z. (2018). *Stakeholder Theory*. The British Library.
- Rahman, R., Sani, A. P., Pongoliu, Y. I. D., Manajemen, J., Ekonomi, F., & Negeri, U. (2021). *Faktor Yang Mempengaruhi Kredit Bermasalah Pada Bank BUMN dan Non BUMN Yang Terdaftar di BEI Tahun 2017-2021*. 10(2), 2061–2070.
- Rahmi, Sri Astuty, Diah Retno Dwi Hastuti, Basri Bado, I. (2025). Analisis Pengaruh Ukuran Bank Konvensional Terhadap Stabilitas Keuangan di Indonesia. *Jurnal Akuntansi Keuangan Dan Perbankan*, 6(2), 102–114.
- Rahmi, A. F., Aziz, M. T., & Sukartini, M. (2025). Pengaruh Ukuran Perusahaan, Struktur Modal, dan Good Corporate Governance terhadap Nilai Perusahaan Sektor Perbankan Tahun 2022-2024. *Maeswara: Jurnal Riset Ilmu Manajemen Dan Kewirausahaan*, 3(4), 152–164.
- Rajakulanajagam, R. dan. (2022). Corporate Governance and Corporate Transparency: A Sri Lankan Case. *International Journal of Accountancy*, 2(2), 1–25.
- Ram, M. (2022). The Disclosures of Information on Cybersecurity in Listed Companies in Latin America -Proposal for a Cybersecurity Disclosure Index. *Sustainability*, 14, 1–23.
- Reon Matemane, Varaidzo Denhere, Maatabudi Mokabane, T. A. O. (2024). Sabinet Cybersecurity Risk Disclosure, Board Characteristics and Firm Performance in the Fourth Industrial Revolution Era: Evidence from an Emerging Economy. *African Finance*, 26(1), 34–53.

- Rizky Ramadhanty, A. S. (2020). Analisis Faktor Yang Mempengaruhi Profitabilitas (ROA) Bank Syariah di Indonesia tahun 2014-2018. *Jurnal Ilmu Ekonomi (JIE)*, 4(2), 294–308.
- Sari, L. (2025). Determinan pengungkapan keamanan siber perbankan di Indonesia. *Disertasi, Repository Unsri 2025*, 1–28.
- Sari, W. F., Saputra, D., Yasmin, Y., Belitung, U. B., & Belitung, B. (2024). Analisis Kinerja Keuangan Bank BUMN dan Bank Swasta Indonesia : Studi Komparatif (Financial Performance Analysis of State-Owned Banks and Private Banks in Indonesia : A Comparative Study). *Studi Ilmu Manajemen Dan Organisasi (SIMO)*, 5(2), 269–283.
- Securities, U. S., & Commission, E. (2023). *Final Rule: Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure*. 89(202), 1–186.
- Selpia, D., Fathurrahman, M., Susilawati, M., & Pratiwi, N. (2024). Penerapan Uji Mann-Whitney dalam Perbandingan Prestasi Akademik Mahasiswa Statistika Universitas Hamzanwadi Angkatan 2022 dan 2023. *Jurnal Exbar: Program Studi Statistika Universitas Hamzanwad*, 2(1), 19–28.
- Setiawan, R. (2025). Digitalisasi Perbankan dan Ancaman Keamanan Siber : Tantangan dan Strategi Mitigasi Risiko Operasional. *ASEFBA: Advanced Studies in Economic, Finance and Banking*, 1(1), 73–87.
- Shehata, N. F. (2014). Theories and Determinants of Voluntary Disclosure. *Accounting and Finance Research*, 3(1), 18–26.
<https://doi.org/10.5430/afr.v3n1p18>
- Singh, H. (2023). Voluntary Cybersecurity Risk Disclosures and Firms '

- Characteristics : The Moderating Role of The Knowledge-Intensive Industry. *Asian Journal of Accounting Research*. <https://doi.org/10.1108/AJAR-12-2023-0413>
- Siringoringo, R., Rahmat, E., & Hulu, J. (2023). Pengontrolan Keamanan Sistem Komputer Client Dari Serangan Hacker Dan Virus Komputer Secara Jarak Jauh (Remote Server) Dengan Menggunakan SSH. *METHOMIKA: Jurnal Manajemen Informatika & Komputerisasi Akuntansi*, 7(1), 123–127.
- Sofiani, M., Ramadhanty, D. P., & Jubaedah, S. (2024). Cyber Risk Management Disclosure: The Impact of Firm Size, Profitability, and Intangible Asset. *International Journal of Entrepreneurship and Business Development*, 7(5), 929–937.
- Sugiyono. (2019). *Metode Penelitian Kuantitatif Kualitatif dan R&D* (19th ed.). Alfabeta.
- Sukarame, A. C., Moningka, A. G. S., & Putri, A. T. (2022). Analisa Perbandingan Kinerja Keuangan Bank BUMN Dan Non BUMN. *Jurnal EMBA*, 10(4), 2019–2029.
- Sumbayak, E. L., & Manda, G. S. (2020). Pengaruh Rasio Terhadap Profitabilitas Bank (Studi Kasus Pada Bank BUMN Periode 2008-2018). *Jurnal Akuntansi Berkelanjutan Indonesia*, 3(3), 327–341.
- Sundari, R. (2026). Analisis Perbandingan Teori Keadilan dan Teori Stakeholder dalam Menilai Tanggung Jawab Sosial Syariah Islam. *Scripta Economica: Journal of Economics, Management, and Accounting*, 1(3), 136–143.
- Supratiwi, A. Z. &. (2024). *Tantangan Tata Kelola Ruang Terbuka Hijau: Studi*

- Kasus Kabupaten Kendal Periode Tahun 2020-2024*. 26, 1–11.
- Surat Edaran, 28 (2011).
- Syafrizal. (2025). Determinasi Kinerja Keuangan Bank: Peran Ukuran Perusahaan dan Struktur Modal. *Journal of Economis and Business*, 3(2), 282–290.
- Syamsuddin, N. (2022). *Metode Penelitian Kuantitatif* (Octamaya (ed.); 1st ed.). Sanabil.
- Tabrani Sabrina, Safitri Vivi, Nayla Putu Audy, H. A. U. (2024). Kejahatan Phishing Ditinjau Dari Perspektif Hukum Dan Kejahatan Siber. *Civilia : Jurnal Kajian Hukum Dan Pendidikan Kewarganegaraan*, 3(1), 1–13.
- Tri Wahyu, O., & Masiyah, K. (2024). Seberapa Penting Pengungkapan Cybersecurity bagi Nilai Perusahaan? *Jurnal Akuntansi Multiparadigma*, 15(246), 377–386. <https://doi.org/10.24054/jurnal.akuntansi.v15i246.377-386>.
- Tuhin, M. H. (2014). Does Size Affect The Non-Mandatory Disclosure Level In The Annual Reports Of Listed Banks In Bangladesh? *International Journal of Economics, Commerce and Management*, 2(2), 1–11.
- Turobov, A., Coyle, D., & Harding, V. (2024). *Using ChatGPT for Thematic Analysis*. May. <http://arxiv.org/abs/2405.08828>
- Waluyo Edy, Septian Ahmad, Jerlian Ega, Hidayat Ifmu Nur, Prahadi Muhammad Alfin, Prasetyo Teguh, S. A. I. (2024). Analisis Data Sample Menggunakan Uji Hipotesis Penelitian Perbandingan Menggunakan Uji Anova dan Uji t. *JEBI: Jurnal Ekonomi Dan Bisnis*, 2(6), 775–785.
- Widya, D., Simatangkir, E., Semarang, U. N., Semarang, U. N., Faliha, N. S., & Semarang, U. N. (2025). Keamanan Siber Dalam Perbankan Serta Tantangan

dan Solusi di Era Digital. *Jurnal Multidisiplin Ilmu Akademik*, 2(1), 33–42.

Wulansari, J., & Chandra, S. (2022). Analysis of The Influence of Bank Health Level Using RGEC Method On Financial Performance (ROA) of The Conventional Banking Sector Listed on BEI 2015-2020. *Procuratio : Jurnal Ilmiah Manajemen*, 10(3), 325–335.

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

Zulvani, D., Novita, J. D., Aini, L. N., & Suhatmi, E. C. (2026). Analisis Profitabilitas Pada Perusahaan Bank Central Asia Tbk Tahun 2020-2024. *Jurnal Bisnis Manajemen Dan Akuntansi*, 6(1), 66–76.

