BAB III
METODE PENELITIAN

1.1 Objek Penelitian

Objek penelitian adalah karakteristik yang melekat pada orang, organisasi, peristiwa, dan hal lainnya yang menjadi subjek penelitian (Nuryaman & Christina, 2015, p. 5). Dengan demikian objek penelitian ini adalah *cybersecurity disclosure* terhadap *audit fee* dengan dimoderasi oleh kompetensi auditor internal pada perusahaan perbankan yang terdaftar di BEI pada tahun 2017 sampai 2019.

1.2 Metode Penelitian

Metode penelitian merupakan sebuah cara ilmiah untuk mendapatkan data dengan tujuan dan kegunaan tertentu. Sebuah metode penelitian yang tepat sangat diperlukan agar peneliti bisa memenuhi tujuan penelitiannya.

1.2.1 Desain Penelitian

Desain penelitian yang digunakan adalah pendekatan kuantitatif dengan studi deskriptif dan kausal. Penelitian deskriptif merupakan penelitian yang bertujuan untuk menjelaskan atau mendeskripsikan keberadaan satu atau lebih variabel. Penelitian ini menggunakan metode kuantitatif karena data penelitian berupa angka serta analisis statistik untuk menguji hipotesis penelitian. Pendekatan kuantitatif digunakan dalam penelitian ini untuk memperoleh data mengenai pengaruh *cybersecurity disclosure* terhadap *audit fee* yang dimoderasi oleh kompetensi auditor internal.

Penelitian ini meneliti hubungan kausal atau sebab akibat antara variabel bebas dan terikat, termasuk juga variabel pemoderasi yang dapat memoderasi pengaruh kedua variabel. Variabel pemoderasi yang digunakan dalam penelitian ini adalah kompetensi auditor internal yang dapat memperkuat atau memperlemah pengaruh *cybersecurity disclosure* terhadap *audit fee*.

Penelitian ini menggunakan unit analisis data industri perbankan karena peneliti mempertimbangkan teknologi informasi yang terus dikembangkan dalam penyediaan jasa perbankan saat ini. Pernyataan ini didukung oleh hasil Indonesia Banking Survey oleh PricewaterhouseCoopers yang menyebutkan bahwa di tahun 2017 84% bank di Indonesia akan terus berinvestasi dalam transformasi teknologi

dan di tahun 2018 hasil survey masih menyatakan bahwa teknologi masih menjadi prioritas utama perbankan selama tiga hingga lima tahun yang akan datang. Selain itu perbankan yang berperan sebagai lembaga yang menampung dan menyalurkan dana masyarakat, perlu terus menjaga risiko keamanan siber supaya masyarakat tidak mengalami kerugian atas risiko ini. Skala dalam penelitian ini merupakan skala interval dan skala rasio.

1.2.2 Definisi dan Operasionalisasi Variabel

1.2.2.1 Definisi Variabel

Variabel penelitian adalah karakteristik yang melekat pada orang, benda, atau subjek lainnya yang nilainya dapat bervariasi atau berbeda antar subjek satu dengan yang lainnya (Nuryaman & Christina, 2015, p. 41). Dalam penelitian ini terdapat variabel bebas (independen), variabel terikat (dependen) dan variabel moderasi. Berikut penjelasan dari tiap variabel:

1. Variabel Dependen (Variabel Terikat)

Variabel dependen adalah variabel yang memberikan reaksi atau respons ketika dihubungkan dengan variabel bebas (Narimawati et al., 2020, p. 5). Variabel dependen yang digunakan dalam penelitian ini adalah:

Y: *Audit Fee*

Audit fee merupakan imbalan yang diterima oleh auditor atau akuntan publik berkaitan dengan jasa audit yang telah diberikan kepada klien. *Audit fee* merupakan salah satu *agency cost* yang dibayarkan untuk mengawasi pihak *agent* atau manajer dalam perusahaan. Nilai *audit fee* dapat diperoleh dari laporan tahunan perusahaan dan dalam penggunaannya memakai logaritma natural dengan rumus: ln FEE = ^{e}log FEE (Calderon & Gao, 2020).

2. Variabel Independen (Variabel Bebas)

Variabel independen atau variabel bebas merupakan variabel yang diukur, dimanipulasi, atau dipilih oleh peneliti dan dapat memengaruhi variabel lain (Narimawati et al., 2020, p. 5). Variabel independen yang digunakan dalam penelitian ini adalah:

X: *Cybersecurity Disclosure*

Cybersecurity disclosure merupakan pengungkapan bagian dari sistem kontrol manajemen yang terintegrasi untuk mengurangi risiko keamanan siber

organisasi. *Cybersecurity disclosure* dapat diperoleh dari laporan tahunan perusahaan berupa kalimat yang menjelaskan tentang bagaimana risiko keamanan siber pada perusahaan dan upaya untuk meminimalisasi risiko tersebut, dengan kata kunci seperti yang terdapat dalam penelitian Gordon dkk. (2010) sebagai berikut.

Tabel 1.1
Kata Kunci Cybersecurity Disclosure

No.	Kata Kunci	No.	Kata Kunci
1	Ukuran keamanan	13	Peretas
2	Autentifikasi	14	Pengawasan keamanan
3	Enkripsi	15	*Denial of Service* (DoS)
4	Virus komputer	16	Keamanan siber
5	Serangan keamanan	17	Serangan siber
6	Pemulihan bencana	18	Insiden keamanan
7	Keamanan informasi	19	*Infosec*
8	Keamanan jaringan/komputer	20	Beban keamanan
9	Kontrol akses	21	Keamanan sistem komputer
10	Intrusi	22	*Cybersecurity*
11	Kontinuitas bisnis	23	Serangan komputer
12	Manajemen keamanan	24	Intrusi komputer

Sumber: Gordon dkk. (2010)

Indikator yang digunakan untuk menilai *cybersecurity disclosure* terdiri atas 40 indikator sesuai dengan *scoring grid* yang dikembangkan dalam penelitian Héroux & Fortin (2020) dari panduan yang dikeluarkan oleh Canadian Securities Administrators (CSA) dan Securities and Exchange Comission (SEC) karena panduan ini dipandang sebagai panduan pengungkapan keamanan siber yang lengkap dan dikeluarkan oleh organisasi dari negara maju yang dapat dijadikan anutan oleh Indonesia. Berikut adalah indikator yang digunakan dalam melakukan *scoring* pada variabel *cybersecurity disclosure*.

Tabel 1.2
Indikator Cybersecurity Disclosure

No.	Indikator	No.	Indikator
Risiko Keamanan Siber		Pencegahan Risiko *Cybersecurity*	
1	Deskripsi umum	22	Kontrol atas akses tidak sah
2	Paparan pihak ketiga	23	Mitigasi tidak memadai
3	Spesifik sesuai perusahaan	24	Rencana pemulihan/respons bencana / insiden
4	Risiko sosial media	25	Pendidikan (Dewan)
Dampak Potensial Insiden *Cybersecurity*		26	Asuransi
5	Gangguan kegiatan/keterlambatan operasional (kehilangan pendapatan)	27	Pendidikan (seluruh staf)
6	Perjanjian kerahasiaan data	28	Ketergantungan pada ahli pihak ketiga
7	Kerusakan reputasi	29	Perlindungan data
8	Litigasi, denda, dan tanggung jawab	30	Pengujian rencana pemulihan
9	Kehilangan atau penghancuran data	31	Penyesuaian dari serangan sebelumnya
10	Akses tidak sah ke informasi yang sensitif	32	Pengendalian dan prosedur pengungkapan yang terkait dengan keamanan siber
11	Penurunan keunggulan kompetitif	Insiden Potensial *Cybersecurity*	
12	Investigasi peraturan	33	Sifat insiden
13	Biaya perbaikan	34	Sumber insiden
14	Premi asuransi yang lebih tinggi	Insiden Keamanan Siber yang Terjadi	

15	Efektivitas pengendalian internal atas pelaporan keuangan	35	Pernah mengalami serangan siber
Tanggung Jawab Atas Strategi *Cybersecurity*		36	Dampak
16	Tanggung jawab disebutkan	37	Detail insiden
17	Komite audit	Item Keamanan Siber Lainnya yang Diungkapkan	
18	Manajemen	38	Undang-Undang
19	Komite risiko	39	Keahlian penerbit regulasi
20	Dewan	40	Lainnya
21	Komite tata kelola		

Sumber: Héroux & Fortin (2020)

3. Variabel Moderator

Variabel moderator atau disebut juga variabel independen kedua adalah variabel yang kedudukannya dapat memperlemah atau memperkuat hubungan langsung antara variabel dependen dengan variabel independen (Nuryaman & Christina, 2015, p. 43). Variabel moderator yang digunakan dalam penelitian ini adalah:

Z: Kompetensi auditor internal

Kompetensi auditor internal merupakan kemampuan auditor internal pada perusahaan dalam menjalankan tugasnya. Standar Internasional Praktik Profesional Audit Internal 1210 menyatakan bahwa auditor internal harus memiliki pengetahuan, keterampilan, dan kompetensi lain yang dibutuhkan dalam melaksanakan tugas dan tanggung jawabnya termasuk pengetahuan untuk mengevaluasi risiko kecurangan, pengetahuan mengenai risiko dan pengendalian kunci, serta teknik audit berbasis teknologi informasi. Kompetensi auditor internal dapat diketahui melalui pengungkapan yang tertera dalam laporan tahunan mengenai latar belakang pendidikan anggota auditor internal atau pelatihan serta sertifikasi yang diperoleh anggota auditor internal.

1.2.2.2 Operasionalisasi Variabel

Operasionalisasi variabel yang akan digunakan dalam penelitian ini adalah sebagai berikut.

Tabel 1.3

Operasionalisasi Variabel

Variabel	Definisi	Indikator	Pengukuran	Skala
Variabel Dependen: *Audit Fee* (Y)	*Audit fee* merupakan biaya auditor dalam melakukan audit termasuk laba normal dan biaya relevan lainnya yang terkait dengan upaya audit berdasarkan berbagai risiko yang telah dinilai auditor (Jung et al., 2016).	Logaritma natural dari *audit fee*. Dengan rumus sebagai berikut: ln FEE = ^{e}log FEE (Calderon & Gao, 2020).	Variabel ini dilihat dari pengungkapan *audit fee* yang tertera pada laporan tahunan perusahaan.	Rasio
Variabel Independen: *Cybersecurity Disclosure* (X)	*Cybersecurity disclosure* merupakan pengungkapan bagian dari sistem kontrol manajemen yang terintegrasi untuk mengurangi	Risiko *Cybersecurity*: 1 Deskripsi umum 2 Paparan pihak ketiga 3 Spesifik sesuai perusahaan 4 Risiko sosial media	Variabel ini diukur dengan menggunakan metode *scoring*. Setiap indikator penilaian diberi skor=1.	Interval

	risiko keamanan siber organisasi.	Dampak Potensial Insiden *Cybersecurity*: 5 Gangguan kegiatan/keterlambatan operasional (kehilangan pendapatan) 6 Menjanjikan kerahasiaan data 7 Kerusakan reputasi 8 Litigasi, denda, dan tanggung jawab 9 Kehilangan atau penghancuran data 10 Akses tidak sah ke informasi yang sensitif 11 Penurunan keunggulan kompetitif 12 Investigasi peraturan 13 Biaya perbaikan 14 Premi asuransi yang lebih tinggi 15 Efektivitas pengendalian internal atas pelaporan		

		keuangan Tanggung Jawab Atas Strategi *Cybersecurity*: 16 Tanggung jawab disebutkan 17 Komite audit 18 Manajemen 19 Komite risiko 20 Dewan 21 Komite tata kelola Pencegahan Risiko *Cybersecurity*: 22 Kontrol atas akses tidak sah 23 Mitigasi tidak memadai 24 Rencana pemulihan / respons bencana / insiden 25 Pendidikan (Dewan) 26 Asuransi 27 Pendidikan (Seluruh staf) 28 Ketergantungan pada ahli pihak ketiga		

		29 Perlindungan data 30 Pengujian rencana pemulihan 31 Penyesuaian dari serangan sebelumnya 32 Pengendalian dan prosedur pengungkapan yang terkait dengan keamanan siber Insiden Potensial *Cybersecurity*: 33 Sifat insiden 34 Sumber Insiden Keamanan Siber yang Terjadi: 35 Pernah mengalami serangan siber 36 Dampak 37 Detail insiden Item Keamanan Siber Lainnya yang Diungkapkan: 38 Undang-Undang		

		39 Keahlian penerbit regulasi 40 Lainnya (Héroux & Fortin, 2020).		
Variabel Moderasi: Kompetensi Auditor internal	Kompetensi auditor internal merupakan pengetahuan dan kemampuan yang dibutuhkan oleh seorang auditor internal untuk melaksanakan pekerjaannya (Novyarni, 2014).	Sertifikasi dan pelatihan yang dimiliki auditor internal.	Variabel ini diukur dengan melihat jumlah sertifikasi dan pelatihan yang dimiliki oleh auditor internal.	Rasio

Sumber: diolah oleh penulis dari berbagai sumber

1.2.3 Populasi dan Sampel

1.2.3.1 Populasi Penelitian

Populasi merupakan keseluruhan unit analisis yang sampelnya ditarik (Narimawati et al., 2020, p. 13). Populasi dalam penelitian ini terdiri atas perusahaan-perusahaan perbankan yang terdaftar di Bursa Efek Indonesia pada tahun 2017 sampai dengan tahun 2019 yaitu sebanyak 47 bank.

1.2.3.2 Sampel Penelitian

Sampel penelitian merupakan bagian dari populasi yang berisi beberapa anggota yang telah dipilih sesuai dengan tujuan penelitian (Nuryaman & Christina, 2015, p. 101). Teknik sampling yang digunakan dalam penelitian ini adalah *purposive sampling*. Sampling purposif merupakan teknik pengambilan sampel dengan pertimbangan tertentu yang cocok dengan objek penelitian. Hal-

hal yang dipertimbangkan dalam memilih sampel penelitian ini sesuai dengan beberapa kriteria yaitu:

1. Perusahaan perbankan yang terdaftar di Bursa Efek Indonesia pada tahun 2017 sampai dengan tahun 2019.
2. Listing di Bursa Efek Indonesia sebelum tahun 2017.
3. Tidak mengalami delisting sepanjang tahun 2017 sampai dengan tahun 2019.
4. Mengungkapkan *audit fee* dalam laporan tahunan selama tahun 2017 sampai 2019.

Pemilihan sampel sesuai dengan kriteria yang akan diteliti dapat dilihat pada tabel berikut.

Tabel 1.4

Kriteria Pengambilan Sampel

No.	Kriteria	Jumlah
1.	Perusahaan perbankan yang terdaftar di Bursa Efek Indonesia pada tahun 2017 sampai dengan tahun 2019	47
2.	Listing di Bursa Efek Indonesia sebelum tahun 2017	(4)
3.	Tidak mengalami delisting sepanjang tahun 2017-2019	(2)
4.	Mengungkapkan *audit fee* dalam laporan tahunan selama tahun 2017-2019	(15)
Sampel		26
Dari tahun 2017-2019		3 tahun
Total Observasi (26 × 3 tahun)		78

Sumber: www.idx.co.id, www.bca.co.id, www.bankmandiri.co.id, www.bankmayapada.com, www.ir-bankbsi.com

Terdapat 26 sampel perusahaan perbankan yang memenuhi kriteria yang selanjutnya disajikan dalam tabel berikut.

Tabel 1.5
Sampel Perusahaan Perbankan

No.	Nama Bank
1.	PT Bank Rakyat Indonesia Agroniaga Tbk
2.	PT Bank MNC Internasional Tbk

3.	PT Bank Central Asia Tbk
4.	Bank Bukopin Tbk
5.	PT Bank Mestika Dharma Tbk
6.	PT Bank Negara Indonesia (Persero) Tbk
7.	PT Bank Rakyat Indonesia (Persero) Tbk
8.	PT Bank Tabungan Negara (Persero) Tbk
9.	PT Bank Danamon Indonesia Tbk
10.	PT Bank Pembangunan Daerah Banten Tbk
11.	PT Bank Ganesha Tbk
12.	Bank Pembangunan Daerah Jawa Barat dan Banten Tbk
13.	Bank Pembangunan Daerah Jawa Timur Tbk
14.	PT Bank QNB Indonesia Tbk
15.	PT Bank Maspion Indonesia Tbk
16.	PT Bank Mandiri (Persero) Tbk
17.	Bank Bumi Arta Tbk
18.	PT Bank CIMB Niaga Tbk
19.	PT Bank Maybank Indonesia Tbk
20.	Bank Permata Tbk
21.	PT Bank BTPN Tbk
22.	Bank Victoria International Tbk
23.	PT Bank OCBC NISP Tbk
24.	PT Bank Syariah Indonesia Tbk
25.	Bank Pan Indonesia Tbk
26.	PT Bank Panin Dubai Syariah Tbk

Sumber: www.idx.co.id

Dari hasil yang tersedia maka jumlah populasi secara keseluruhan adalah 47 bank yang diperoleh, dari jumlah bank yang termasuk dalam kriteria yaitu sebanyak 26 dikalikan dengan periode penelitian yaitu selama tiga tahun.

1.2.4 Teknik Pengumpulan Data

1.2.4.1 Jenis Data dan Sumber Data

Teknik pengumpulan data yang digunakan dalam penelitian ini adalah sumber data sekunder berupa dokumen. Data sekunder adalah data yang diambil dari pihak kedua yang memiliki data, tidak diambil langsung dari pembuat informasi. Dan dokumen merupakan informasi yang dituangkan secara tertulis dapat berupa catatan, buku, surat, jurnal, laporan dan sebagainya. Dokumen yang digunakan dalam penelitian ini merupakan laporan tahunan (*annual report*) perusahaan perbankan yang terdaftar di Bursa Efek Indonesia (BEI) pada tahun 2017 sampai dengan tahun 2019 dalam website http://idx.co.id serta www.bca.co.id, www.bankmandiri.co.id, www.bankmayapada.com, dan www.ir-bankbsi.com untuk perusahaan perbankan terdaftar di BEI yang tidak menyampaikan laporan tahunan pada website BEI di tahun tertentu.

1.2.5 Teknik Analisis Data

1.2.5.1 Statistik Deskriptif

Penelitian ini menggunakan teknik statistik deskriptif. Statistik deskriptif merupakan statistik yang digunakan untuk menggambarkan atau menganalisis suatu hasil penelitian secara umum. Deskripsi variabel dapat dilihat dari nilai rata-rata (*mean*), nilai maksimum, nilai minimum serta standar deviasi. Penggunaan statistik deskriptif pada penelitian ini bertujuan untuk mengetahui gambaran dari *cybersecurity disclosure*, kompetensi auditor internal, dan *audit fee*.

1.2.5.2 Transformasi Data

Sebelum melakukan uji asumsi klasik dan pengujian hipotesis, peneliti melakukan transformasi data menggunakan Logaritma Natural (Ln) dengan menggunakan aplikasi SPSS 25. Transformasi data dilakukan karena data variabel *audit fee* tidak tersebar secara merata. Data yang diambil dari laporan tahunan perusahaan kemudian ditransformasikan seluruhnya sehingga variabel-variabel dalam penelitian ini menjadi LnCybersecurity Disclosure, LnKompetensi Auditor Internal dan LnAudit Fee. Selanjutnya dalam uji asumsi klasik dan pengujian hipotesis menggunakan data yang telah ditransformasi menggunakan Logaritma Natural (Ln).

1.2.5.3 Uji Asumsi Klasik

Penelitian ini menggunakan model regresi linear berganda. Sebelum melakukan pengujian, model regresi linear harus memenuhi beberapa asumsi dasar demi menghasilkan estimasi *Best Linear Unbiased Estimator* (BLUE), yakni uji heteroskedastisitas, uji normalitas, serta uji autokorelasi.

1. Uji Heteroskedastisitas

   Heteroskedastisitas merupakan keadaan di mana seluruh faktor pengganggu tidak memiliki varian yang sama untuk seluruh pengamatan atas variabel independent. Dalam model regresi seharusnya tidak terjadi heteroskedastisitas, melainkan homoskedastisitas yakni kesamaan varians tetap dari residual satu pengamatan ke pengamatan. Pada penelitian ini pengujian heteroskedastisitas dilakukan dengan melakukan uji Glejser.

   Dasar pengambilan keputusan dalam uji heteroskedastisitas adalah sebagai berikut.

   a. Jika nilai signifikansi > 0.05 maka tidak terjadi heterokedastisitas
   b. Jika nilai signifikansi < 0,05 maka terjadi heterokedastisitas

2. Uji Normalitas

   Uji normalitas dilakukan untuk melihat apakah nilai residual terdistribusi normal atau tidak. Uji ini diperlukan karena model regresi yang baik memiliki nilai residual yang terdistribusi normal. Pengujian normalitas pada penelitian ini dilakukan dengan uji Kolmogorov-Smirnov, dimana asumsi normalitas terpenuhi jika nilai signifikansi berada di atas tingkat tertentu.

   Dasar pengambilan keputusan dalam uji normalitas adalah sebagai berikut.

   a. Jika nilai signifikansi < 0,05 maka data tersebut tidak berdistribusi normal
   b. Jika nilai signifikansi > 0,05 maka data tersebut berdistribusi normal

3. Uji Autokorelasi

Uji autokorelasi dilakukan untuk melihat apakah terdapat nilai yang berkorelasi satu dengan yang lainnya dalam satu variabel. Pengujian autokorelasi dalam penelitian ini dilakukan dengan uji Durbin-Watson.

Dasar pengambilan keputusan dalam uji Durbin-Watson adalah sebagai berikut.

a. Jika du < d < 4-du, maka tidak terjadi autokorelasi
b. Jika 0 < d < dl, maka terjadi autokorelasi

Jumlah n sebanyak 78 dan jumlah variabel independent (k) = 2. Nilai dl dan du yang diperoleh dari tabel Durbin-Watson dengan tingkat signifikansi 0,05 adalah 1,5801 dan 1,6851.

1.2.6 Pengujian Hipotesis

1.2.6.1 Analisis Regresi Linear Sederhana

Persamaan garis linier sederhana dihitung untuk menggambarkan hubungan antara satu variabel bebas dengan variabel terikat (Lind et al., 2014, p. 114). Analisis ini digunakan untuk mengetahui pengaruh positif maupun negatif dari variabel bebas dan variabel terikat. Adapun persamaan umum dari regresi linear sederhana adalah sebagai berikut.

$$\hat{Y} = a + bX + e$$

Sehingga apabila diterapkan pada variabel-variabel yang digunakan dalam penelitian ini, maka rumus persamaannya adalah sebagai berikut.

$$FEE = a + bCYBERDISC + e$$

Keterangan:

FEE	:	Logaritma natural besarnya *audit fee*
CYBERDISC	:	1 untuk setiap indicator pengungkapan keamanan siber
a	:	Konstanta
b	:	Koefisien regresi dari variabel bebas
e	:	*error*

1.2.6.2 Analisis Regresi Moderasi (*Moderated Regression Analysis*)

Variabel moderasi dalam model regresi dapat diuji menggunakan tiga cara yakni uji interaksi (*Moderated Regression Analysis*), uji selisih mutlak dan uji

residual. Penelitian ini menggunakan uji *Moderated Regression Analysis* (MRA) untuk menguji variabel moderasi. Lie (2009) mendefinisikan MRA sebagai aplikasi khusus regresi berganda linear di mana dalam persamaan regresinya mengandung unsur interaksi berupa perkalian dua atau lebih variabel independen dengan rumus persamaan sebagai berikut:

$$\hat{Y} = a + b_1X_1 + b_2X_2 + b_3X_1X_2 + e$$

Lie (2009)

Sehingga apabila diterapkan pada variabel-variabel yang digunakan dalam penelitian ini, maka rumus persamaannya adalah sebagai berikut.

$$FEE = a + b_1CYBERDISC_{it} + b_2COMPETENCE_{it} + b_3CYBERDISC_{it} * COMPETENCE_{it} + e$$

Keterangan:

FEE	:	Logaritma natural besarnya *audit fee*
CYBERDISC	:	1 untuk setiap indicator pengungkapan keamanan siber
COMPETENCE	:	Total sertifikasi dan pelatihan yang dimiliki auditor internal
a	:	Konstanta
b	:	Koefisien regresi dari variabel bebas
e	:	*error*

1.2.6.3 Perumusan Hipotesis

Rumusan hipotesis yang digunakan dalam penelitian ini sebagai berikut.

a. Hipotesis Statistik 1

   H_0: $\beta \leq 0$, *Cybersecurity disclosure* tidak berpengaruh positif terhadap *audit fee*

   H_1: $\beta > 0$, *Cybersecurity disclosure* berpengaruh positif terhadap *audit fee*

b. Hipotesis Statistik 2

   H_0: $\beta = 0$, Kompetensi auditor internal tidak memoderasi pengaruh *cybersecurity disclosure* terhadap *audit fee*

   H_1: $\beta \neq 0$, Kompetensi auditor internal memoderasi pengaruh *cybersecurity disclosure* terhadap *audit fee*