BAB I
PENDAHULUAN

1.1 Latar Belakang Penelitian

Signalling theory menyatakan bahwa hubungan *principal* dan *agent* dapat menyebabkan asimetri informasi karena biasanya *agent* memiliki lebih banyak informasi daripada *principal*. Laporan keuangan dihasilkan oleh suatu perusahaan untuk memberikan informasi kepada pihak-pihak yang berkepentingan sehingga dapat mengurangi asimetri informasi dan dapat dijadikan dasar untuk membuat keputusan. Pihak-pihak yang berkepentingan dengan perusahaan selaku pengguna informasi perlu memiliki keyakinan atas laporan keuangan yang dihasilkan perusahaan bahwa laporan keuangan tersebut sudah relevan dan dapat diandalkan (*reliable*). Cara yang paling umum digunakan para pengguna laporan keuangan untuk mendapatkan informasi yang dapat diandalkan adalah dengan cara menghadirkan auditor independen (A. Arens et al., 2012). Colbert & Jahera, Jr. (1988) menyatakan bahwa auditor eksternal dalam teori agensi berperan sebagai agen yang memeriksa pekerjaan agen lainnya yakni pekerjaan manajemen, untuk menilai apakah informasi yang dihasilkan manajemen telah sesuai dan berguna bagi para *stakeholders*.

Auditor independen atau disebut juga akuntan publik adalah seseorang yang memiliki izin dan kompetensi untuk memberikan jasa audit yang biasanya bernaung dalam sebuah Kantor Akuntan Publik (KAP). Proses audit biasanya dilakukan oleh sebuah tim perikatan audit yang merupakan suatu tim yang dipimpin oleh akuntan publik dengan beranggotakan staf profesional yang ditugaskan oleh KAP untuk melakukan jasa audit. Setelah memberikan jasa audit, seorang akuntan publik berhak untuk mendapatkan imbalan jasa berdasarkan kesepakatan antara akuntan publik dengan kliennya yang tertuang dalam surat perikatan (Ikatan Akuntan Publik Indonesia, 2016). Imbalan jasa yang diterima oleh akuntan publik ini disebut sebagai *audit fee*. *Audit fee* merupakan salah satu biaya yang disebabkan oleh adanya hubungan *principal-agent* antara auditor, manajemen perusahaan dan pemilik perusahaan, atau yang disebut sebagai *agency cost*.

Auditor perlu mempertimbangkan risiko audit yang akan dihadapi ketika menentukan *audit fee*. Risiko audit mencerminkan kemungkinan kesalahan akuntan publik dalam memberi opini atas laporan keuangan. Kesalahan dalam memberikan opini atas laporan keuangan akan membuat akuntan publik mendapatkan sanksi dari instansi yang berwenang. Contoh akuntan publik yang salah memberikan opini yakni Akuntan Publik (AP) Marlina dan Merliyana Syamsul dari KAP Satrio Bing Eni dan Rekan yang merupakan pemegang afiliasi Deloitte di Indonesia, diberikan sanksi oleh Otoritas Jasa Keuangan (OJK) berupa pembatalan hasil audit kepada SNP Finance yang adalah kliennya dan pelarangan untuk mengaudit sektor perbankan, pasar modal dan Industri Keuangan Non Bank (IKNB). Sanksi ini diberikan kepada AP tersebut karena mereka telah melanggar POJK Nomor 13/POJK.03/2017 tentang Penggunaan Jasa Akuntan Publik dan Kantor Akuntan Publik dengan pertimbangan telah memberikan opini yang tidak mencerminkan kondisi keuangan sebenarnya, menimbulkan kerugian yang besar atas opini tersebut, dan menurunnya kepercayaan masyarakat (Handoko & Soepriyanto, 2018). Kemudian Kasner Sirumapea selaku auditor laporan keuangan tahun 2018 PT Garuda Indonesia (Persero) Tbk diberi sanksi administratif berupa pembekuan Surat Tanda Terdaftar (STTD) selama satu tahun karena dianggap melanggar sejumlah peraturan dan Standar Audit (SA), termasuk SA 700 SPAP tentang Perumusan Suatu Opini dan Pelaporan atas Laporan Keuangan (Otoritas Jasa Keuangan, 2019).

Risiko audit dapat diidentifikasi pada saat akuntan publik melakukan perencanaan audit yang diawali dengan penilaian risiko bisnis klien. Risiko bisnis dapat memengaruhi kemampuan perusahaan untuk mencapai tujuannya, termasuk tujuan untuk mempertahankan keuangan, menjaga nama baik dan kemampuan perusahaan untuk mempertahankan kelangsungan usaha (Cascarino, 2007, p. 35). Standar Audit (SA) 315 Paragraf A32 Insitut Akuntan Publik Indonesia (IAPI) memberikan contoh mengenai hal-hal yang dapat dipertimbangkan oleh auditor dalam memahami risiko bisnis klien yang dapat mengakibatkan kesalahan penyajian material dalam laporan keuangan seperti perkembangan industri, produk dan jasa baru, ekspansi bisnis, ketentuan akuntansi baru, ketentuan regulasi, ketentuan pendanaan periode kini dan masa yang akan datang, pengaruh

pengimplementasian strategi, dan penggunaan teknologi informasi (Institut Akuntan Publik Indonesia, n.d.). Hasil penelitian Paino dkk. (2014) menunjukkan bahwa auditor melakukan perubahan prosedur audit yang signifikan sebagai respon terhadap risiko bisnis klien. Dengan demikian apabila auditor mengidentifikasi risiko yang tinggi atas klien maka auditor akan melakukan upaya lebih dalam pelaksanaan auditnya sehingga memerlukan waktu yang lebih lama dan *audit fee*-nya pun menjadi lebih tinggi (H. Chen et al., 2019; Kim & Fukukawa, 2013).

Audit fee yang dibayarkan oleh klien pada umumnya berbeda-beda karena risiko yang dihadapi oleh perusahaan pun berbeda-beda. Selain itu, *audit fee* juga bergantung pada kesepakatan antara klien dan auditor. Seperti yang terdapat pada tabel 1.1 dapat dilihat bahwa PT Bank Rakyat Indonesia (Persero) Tbk membayar imbalan jasa audit yang jauh lebih tinggi dibanding PT Bank Mandiri (Persero) Tbk, walaupun keduanya sama-sama bergerak di bidang perbankan dan diaudit oleh KAP yang sama.

Tabel 1.1

Perbedaan Besaran Imbalan Jasa Audit

Nama Perusahaan	**Jenis Perusahaan**	**Tahun 2018**	
		KAP	***Audit fee***
PT Bank Rakyat Indonesia (Persero) Tbk	Perbankan	Purwantono, Sungkoro & Surja (Ernst & Young)	Rp13.545.000.000
PT Bank Mandiri (Persero) Tbk	Perbankan	Purwantono, Sungkoro & Surja (Ernst & Young)	Rp7.284.000.000

Sumber: www.idx.co.id

Penentuan *audit fee* juga memunculkan kekhawatiran ketika biaya audit terlalu tinggi (*abnormal high audit fee*). Ketika *audit fee* terlalu tinggi, muncul dua teori yang berlawanan. Teori pertama menyatakan bahwa dengan tingginya

audit fee maka auditor akan meningkatkan kualitas auditnya, sedangkan yang kedua menyatakan bahwa dengan *audit fee* yang terlalu tinggi maka independensi auditor akan berkurang karena terjadi *economic bonding* yang kuat sehingga kualitas audit menurun (Choi et al., 2010; Jung et al., 2016). Hasil penelitian Setyawati & Apandi (2019) menunjukkan bahwa *positive abnormal audit fee* berpengaruh negatif secara tidak signifikan terhadap kualitas audit dan koneksi politik pun secara tidak signifikan memperkuat pengaruh *positive abnormal audit fee* terhadap kualitas audit. Selain itu, penelitian Krauß dkk. (2015) membuktikan secara empiris bahwa *positive abnormal audit fee* secara negatif berkaitan dengan kualitas audit sehingga menyiratkan bahwa premi biaya audit merupakan indikator signifikan dari independensi auditor karena terdapat ikatan ekonomi antara auditor dan klien.

Tabel 1.2 berikut menunjukkan bahwa rata-rata imbalan jasa audit pada tahun 2017 sebesar Rp3.354.263.467, tahun 2018 sebesar Rp3.930.516.084 dan di tahun 2019 sebesar Rp3.596.444.522. Rata-rata imbalan jasa audit ini diambil dari perusahaan perbankan yang dijadikan sampel dalam penelitian sebanyak 26 bank. Tabel ini menunjukkan bahwa ada beberapa bank yang membayar imbalan jasa audit lebih tinggi dari rata-rata *trend* besaran imbalan jasa audit di tahun tersebut seperti misalnya Bank Central Asia (BBCA), Bank Negara Indonesia (BBNI), Bank Rakyat Indonesia (BBRI), Bank Danamon (BDMN), dan lain-lain. Dengan demikian, melalui tabel 1.2 dapat diketahui bahwa *abnormal high audit fee* juga terjadi di perusahaan perbankan di Indonesia.

Tabel 1.2

Besaran Imbalan Jasa Audit yang Terlalu Tinggi/Rendah (dalam Rp)

No.	Kode Bank	2017	2018	2019
1	AGRO	522.111.141	2.800.000.000	1.500.000.000
2	BABP	999.000.000	237.000.000	450.000.000
3	BBCA	6.200.000.000	6.400.000.000	6.900.000.000
4	BBKP	1.960.000.000	2.527.855.000	1.303.124.400
5	BBMD	380.000.000	375.000.000	380.000.000

6	BBNI	7.200.000.000	7.284.000.000	12.900.000.000
7	BBRI	13.545.000.000	13.545.000.000	2.200.000.000
8	BBTN	2.290.000.000	2.367.000.000	2.650.000.000
9	BDMN	4.346.000.000	4.405.000.000	4.405.000.000
10	BEKS	475.000.000	522.500.000	522.500.000
11	BGTG	550.000.000	600.000.000	415.000.000
12	BJBR	2.350.000.000	1.919.000.000	2.700.000.000
13	BJTM	570.000.000	940.000.000	960.000.000
14	BKSW	1.154.000.000	1.352.000.000	1.484.615.000
15	BMAS	650.000.000	725.000.000	550.000.000
16	BMRI	10.000.000.000	11.571.818.182	11.571.818.182
17	BNBA	550.000.000	585.000.000	1.000.000.000
18	BNGA	8.299.494.000	15.037.000.000	13.938.500.000
19	BNII	3.377.745.000	3.377.745.000	3.547.000.000
20	BNLI	5.900.000.000	6.254.000.000	7.100.000.000
21	BTPN	5.555.000.000	5.755.000.000	5.755.000.000
22	BVIC	1.500.000.000	1.976.000.000	1.500.000.000
23	NISP	3.575.000.000	5.100.000.000	4.200.000.000
24	BRIS	900.000.000	1.237.500.000	1.300.000.000
25	PNBN	3.950.000.000	4.750.000.000	3.900.000.000
26	PNBS	412.500.000	550.000.000	375.000.000
Rata-rata		3.354.263.467	3.930.516.084	3.596.444.522

Sumber: www.idx.co.id

Selain itu dalam penentuan *audit fee* juga dapat muncul permasalahan *lowballing*. *Lowballing* merupakan kondisi di mana *non-expert* auditor atau

auditor baru biasanya menetapkan tarif biaya audit yang rendah untuk mendapatkan klien (Hua & Sun, 2016). Kasus seperti ini dapat terjadi karena semakin tingginya persaingan antar KAP. Penelitian DeAngelo pada tahun 1981 menemukan bahwa pada awal penugasan audit, KAP menetapkan *audit fee* yang lebih rendah (DeAngelo, 1981). Penelitian ini didukung oleh penelitian lain yang dilakukan oleh Simon dan Francis (1988) serta Ettredge dan Greenberg (1990) yang menyimpulkan bahwa awal penugasan audit di Amerika Serikat mengandung *lowballing cost* sekitar 25% dari *fee* normal (Ettredge & Greenberg, 2016).

Penetapan *audit fee* di Indonesia diatur oleh Institut Akuntan Publik Indonesia (IAPI) dalam Peraturan Pengurus No. 2 Tahun 2016 tentang Penentuan Imbalan Jasa Audit Laporan Keuangan. Peraturan tersebut memuat indikator batas bawah imbalan jasa per jam yang bisa dijadikan panduan oleh para akuntan publik atau KAP dalam menetapkan imbalan jasa audit yang sesuai agar dapat mencukupi pelaksanaan prosedur audit yang memadai sesuai kode etik, Standar Profesional Akuntan Publik (SPAP), dan ketentuan peraturan perundang-undangan yang berlaku. Akan tetapi, dalam peraturan tersebut IAPI juga menyatakan bahwa akuntan publik dapat menetapkan nilai imbalan yang lebih tinggi sesuai dengan kondisi yang dihadapi karena *audit fee* sesungguhnya dipengaruhi oleh banyak faktor.

Tabel 1.3
Indikator Batas Bawah Imbalan Jasa Per Jam Berdasarkan Klasifikasi Berjenjang (dalam Rp)

Kategori Wilayah	**Junior Auditor**	**Senior Auditor**	**Supervisor**	**Manager**	**Partner**
Jabodetabek	100.000	150.000	300.000	700.000	1.500.000
Luar Jabodetabek	70.000	125.000	200.000	500.000	1.200.000

Sumber: Lampiran Peraturan Pengurus No. 2 Tahun 2016 tentang Penentuan Imbalan Jasa Audit Laporan Keuangan

Beberapa hasil penelitian menunjukkan hal-hal yang memengaruhi *audit fee*, diantaranya adalah ukuran perusahaan, kompleksitas audit, lamanya waktu

audit, dan risiko audit. Ukuran perusahaan memiliki pengaruh signifikan postif terhadap *audit fee* karena semakin besar ukuran perusahaan maka transaksinya semakin kompleks sehingga auditor memerlukan waktu yang lebih lama untuk mengambil bukti yang lebih banyak dan *audit fee* pun menjadi lebih tinggi (Shafira & Ghozali, 2017; Yulianti et al., 2019). Kompleksitas audit yang diproksikan dengan jumlah anak perusahaan pun berpengaruh signifikan positif terhadap *audit fee* karena semakin banyak anak perusahaan maka semakin banyak pula pemeriksaan yang diperlukan (Yulianti et al., 2019). Lamanya waktu audit berpengaruh positif dan signifikan terhadap penetapan *audit fee*. Artinya, semakin lama waktu audit yang diperlukan auditor, maka *fee* yang diterima auditor pun akan semakin besar (Saputri et al., 2017). Kemudian risiko audit juga berpengaruh positif terhadap *audit fee* di mana semakin tinggi risiko audit yang dihadapi akuntan publik maka semakin tinggi pula bukti audit yang perlu didapatkan sehingga *audit fee* menjadi lebih tinggi (Saputri et al., 2017; Shafira & Ghozali, 2017).

Selain itu, ada juga beberapa pengungkapan (*disclosure*) yang dapat memengaruhi *audit fee* seperti pengungkapan yang berkaitan dengan *goodwill* (V. Y. S. Chen et al., 2019), pengungkapan narasi tekstual (Hossain et al., 2019), dan pengungkapan risiko keamanan siber (Calderon & Gao, 2020). V. Y. S. Chen dkk. (2019) menemukan pengungkapan terkait *goodwill* secara positif berkaitan dengan biaya audit. Penemuan ini konsisten dengan gagasan bahwa auditor meningkatkan upaya audit mereka untuk mengurangi risiko audit. Hossain dkk. (2019a) menemukan bahwa pengungkapan tekstual memiliki pengaruh positif terhadap biaya audit. Calderon & Gao (2020) menemukan bahwa biaya audit dipengaruhi oleh pengungkapan risiko keamanan siber secara umum.

Indonesia Banking Survey oleh PricewaterhouseCoopers 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 (PricewaterhouseCoopers, 2017, 2018). Oleh karena itu, pengungkapan keamanan siber (*cybersecurity disclosure*) menjadi suatu hal yang mulai diperhatikan, mengingat banyaknya perusahaan yang kini menggunakan

teknologi informasi dalam menjalankan kegiatan operasionalnya sehingga ancaman potensial seperti ancaman siber merupakan risiko baru yang perlu diwaspadai, terutama oleh perusahaan-perusahaan yang bergerak di bidang perbankan. Meningkatnya penggunaan teknologi digital pada perusahaan telah menekankan pentingnya keamanan siber dan peran keamanan siber sebagai dimensi manajemen risiko baru, paling tidak karena ancaman dan risiko siber telah menarik perhatian publik secara signifikan (Haapamäki & Sihvonen, 2019; Li et al., 2018). Menurut Gordon dan Loeb (2006 dalam (Haapamäki & Sihvonen, 2019)) tujuan keamanan siber dapat dibagi ke dalam tiga kategori besar. Pertama, keamanan siber melindungi kerahasiaan informasi pribadi; kedua, memastikan pengguna terotorisasi dapat mengakses informasi secara tepat waktu dan ketiga, kemanan siber melindungi akurasi, keandalan, dan validitas informasi.

Ancaman siber bisa saja muncul dari pihak internal yang memiliki akses atau pun peretas dari luar perusahaan yang ingin menembus keamanan perusahaan untuk keuntungan atau kesenangannya sendiri, akibat gangguan natural seperti bencana alam atau pun karena kesalahan teknis. Risiko-risiko keamanan siber ini dapat berupa pencurian perangkat keras, permasalahan sistem telekomunikasi, perangkat lunak yang mudah disabotase, prosedur pengendalian operasi komputer yang dapat diubah dan permasalahan keamanan data itu sendiri (Cascarino, 2007, p. 81).

Risiko keamanan siber dalam bisnis dapat menimbulkan kerugian. Perusahaan yang terkena insiden keamanan siber mengalami kerugian signifikan dalam biaya perbaikan, denda, dan reputasi (Gordon et al., 2010; Rosati et al., 2017). Insiden kejahatan dunia maya juga berdampak negatif terhadap kinerja organisasi (Malik & Islam, 2019). Selain itu perusahaan yang dilaporkan terkena serangan siber juga mengalami dampak dalam hal kinerja saham, di mana saham perusahaan sektor keuangan cenderung bereaksi terhadap serangan siber lebih lama dibanding sektor lain (Tweneboah-Kodua et al., 2018). Hasil penelitian yang dilakukan oleh Tariq (2018) terdapat dua jenis kerugian yang mungkin diderita institusi keuangan setelah mengalami serangan siber yakni, kerugian secara langsung berupa pencurian uang dan pencurian data; dan kerugian secara tidak langsung berupa ketidakpuasan pelanggan dan rusaknya nama baik perusahaan.

Ancaman keamanan siber ini sudah dirasakan oleh beberapa perusahaan perbankan yang ada di Indonesia. Pada tahun 2018 nasabah The Development Bank of Singapore (Bank DBS) diduga mengalami pembobolan dana dengan modus *email hijacking* (www.liputan6.com, 2018). Kemudian pada tahun 2019 dilaporkan bahwa polisi menangkap pelaku pembobolan *e-banking* yang berhasil menguras uang Rp1 miliar dengan memanfaatkan kartu perdana mati (news.detik.com, 2019). Di tahun 2020, nasabah Commonwealth Bank pun disebutkan bahwa rekeningnya telah dibobol melalui pencurian kartu *subscriber identity module* (SIM) (cnnindonesia.com, 2020).

Maka dari itu, sebagai salah satu bentuk risiko yang terdapat dalam sebuah perusahaan, maka risiko kemanan siber juga perlu diungkapkan kepada para pemegang kepentingan (*stakeholders*). Pengungkapan ini berguna untuk mengurangi asimetri informasi antara pihak manajemen perusahaan (*agent*) dan pemilik (*principal*) mengenai risiko keamanan siber yang mungkin terjadi di perusahaan. American Institute of Certified Public Accountans (AICPA) telah mengembangkan kerangka pelaporan keamanan siber yang dapat digunakan oleh perusahaan untuk mengungkapkan informasi yang diperlukan kepada para pemegang kepentingan mengenai program manajemen risiko keamanan siber dan efektivitasnya. Selain AICPA, Security and Exchange Commission (SEC) pun telah mengeluarkan pedoman mengenai pengungkapan risiko keamanan siber. Dengan demikian risiko keamanan siber sudah menjadi bagian penting yang perlu diungkapkan oleh perusahaan supaya para pemangku kepentingan dapat mengetahui bagaimana upaya manajemen dalam meminimalisasi risiko keamanan siber.

Pengungkapan risiko keamanan siber (*cybersecurity disclosure*) dapat memengaruhi *audit fee* karena auditor dapat menggunakan berbagai informasi termasuk laporan yang dipublikasi, untuk memahami risiko bisnis kliennya sehingga melalui pengungkapan tersebut auditor dapat mengidentifikasi adanya risiko keamanan siber. Jika auditor mengidentifikasi risiko yang berhubungan dengan keamanan siber memiliki dampak yang material terhadap laporan keuangan perusahaan, maka auditor perlu mendesain dan melakukan beberapa prosedur untuk menilai risiko tersebut (Calderon & Gao, 2020). Dengan adanya

permasalahan keamanan siber, maka *inherent risk* dan *control risk* dalam perusahaan meningkat sehingga auditor perlu memperkecil *detection risk* dengan cara melakukan pengujian yang lebih detail. Pengujian yang lebih luas ini menyebabkan *audit fee* yang lebih tinggi (Hogan & Wilkins, 2008 dalam (Calderon & Gao, 2020)).

Penelitian sebelumnya menunjukkan apabila perusahaan mengalami insiden keamanan siber, maka perusahaan tersebut mengalami kenaikan *audit fee* (Haislip et al., 2019; Rosati et al., 2019). Selain itu, pengungkapan yang bersifat narasi juga memiliki hubungan positif dengan *audit fee* (Hossain et al., 2019). Hal ini berkaitan karena pengungkapan keamanan siber juga dituangkan dalam bentuk narasi. Selanjutnya, panjang kata dalam pengungkapan keamanan siber yang meningkat sebesar 10% dapat menaikan *audit fee* sebesar $10.334, peningkatan tingkat kesulitan keterbacaan pengungkapan sebesar satu unit berdasarkan Fog Index dapat meningkatkan *audit fee* sebesar $4.632 dan peningkatan penggunaan istilah hukum sebesar 1% dapat meningkatkan *audit fee* sebesar 2,78% (Calderon & Gao, 2020). Insiden keamanan siber juga berkaitan dengan kenaikan *audit fee*, akan tetapi kenaikan ini menjadi lebih kecil bagi perusahaan yang mengungkapan risiko keamanan siber setelah SEC mengeluarkan panduan pengungkapan keamanan siber pada tahun 2011 (Li et al., 2020).

Untuk meminimalisasi risiko, perusahaan juga memerlukan adanya fungsi pengendalian internal yang merupakan tanggung jawab pihak manajemen. Dalam hal sistem informasi, manajemen perlu memastikan bahwa sistem yang ada dalam perusahaan berfungsi sebagaimana mestinya, keaslian data dan kerahasiaannya terpelihara, ketersediaan sistem ketika diperlukan, akurasi dan kelengkapan data terjamin, dan akses yang hanya diberikan kepada pihak yang diizinkan (Cascarino, 2007, p. 90). Untuk memeriksa keefektifan pengendalian internal, fungsi audit internal sangat diperlukan karena fokus perhatian para auditor internal sering kali diberikan untuk penilaian atas aktivitas pengendalian internal (Hayes et al., 2017, p. 261). Auditor internal melakukan analisis dan penilaian independen atas ketepatan dan keefektifan manajemen risiko dan sistem pengendalian internal perusahaan, juga memberikan asurans yang objektif dan

independen kepada komite audit atas tata kelola perusahaan dan kepatuhan (Soh & Martinov-Bennie, 2011).

Dalam menjalankan tugasnya, auditor internal harus memiliki *code of ethics* yang terdiri atas integritas, objektivitas, kerahasiaan dan kompentensi supaya fungsinya dapat berjalan dengan efektif (Anderson et al., 2017, p. 92). 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. Zahmatkesh & Rezazadeh (2017) menunjukkan bahwa auditor yang memiliki kompetensi professional memiliki pengaruh positif yang signifikan terhadap kualitas audit.

Menurut Institute of Internal Auditor (IIA), auditor internal dirancang untuk membantu perusahaan mencapai tujuannya dengan membawa pendekatan yang sistematis dan disiplin untuk mengevaluasi dan meningkatkan efektivitas manajemen risiko, pengendalian dan proses tata kelola (Institute of Internal Auditing (IIA), n.d.). Dengan demikian, audit internal dapat berperan sebagai pendukung tata kelola perusahaan yang baik (*good corporate governance*) (Curse, 2016). Tata kelola perusahaan yang baik dapat diproksikan dengan transparansi informasi yang disediakan untuk para pemangku kepentingan dalam bentuk pengungkapan keuangan serta transparansi tata kelola dan kinerja, baik yang bersifat sukarela atau wajib (Augustine, 2012). Maka dari itu, audit internal yang efektif akan membentuk tata kelola perusahaan yang baik sehingga transparansi yang diwujudkan melalui pengungkapan sukarela pada laporan keuangan menjadi lebih luas sehingga dapat mengurangi asimetri informasi dalam perusahaan (Purnomo & Bernawati, 2020).

Dengan semakin banyaknya perusahaan perbankan yang mengembangkan teknologi informasi dalam kegiatan operasionalnya, Otoritas Jasa Keuangan (OJK) mengeluarkan Peraturan Otoritas Jasa Keuangan Nomor 38/POJK.03/2016 tentang Penerapan Manajemen Risiko Dalam Penggunaan Teknologi Informasi oleh Bank Umum. Dalam peraturan tersebut, OJK mengatur tentang pelaksanaan

fungsi audit internal atas penyelenggaraan teknologi informasi dalam Pasal 17 sampai Pasal 19. Pada pasal 18 ayat (4) disebutkan "bank wajib melaksanakan audit intern terhadap seluruh aspek dalam penyelenggaraan dan penggunaan Teknologi Informasi sesuai kebutuhan, prioritas, dan hasil analisis risiko Teknologi Informasi paling sedikit 1 (satu) kali dalam 1 (satu) tahun." Kemudian pada Pasal 30 mengenai pelaporan, OJK mewajibkan setiap bank untuk melaporkan kepada OJK mengenai kondisi penggunaan teknologi informasi, rencana pengembangan serta hasil audit teknologi informasi.

Berdasarkan fenomena-fenomena yang telah dijabarkan mengenai pengungkapan keamanan siber (*cybersecurity disclosure)*, *audit fee*, dan auditor internal, maka peneliti tertarik untuk melakukan penelitian dengan judul "**Pengaruh *Cybersecurity Disclosure* terhadap *Audit Fee* dengan Kompetensi Auditor Internal Sebagai Variabel Moderasi**". Penelitian ini dilakukan dengan menggunakan data sekunder berupa laporan tahunan dari perusahaan sektor perbankan yang terdaftar di Bursa Efek Indonesia pada tahun 2017 sampai 2019.

1.2 Rumusan Masalah Penelitian

Berdasarkan latar belakang yang telah dijelaskan, maka rumusan masalah penelitian ini adalah sebagai berikut:

1. Bagaimana pengaruh *cybersecurity disclosure* terhadap *audit fee*?
2. Bagaimana pengaruh *cybersecurity disclosure* terhadap *audit fee* yang dimoderasi oleh kompetensi auditor internal?

1.3 Tujuan Penelitian

1.3.1 Tujuan Umum Penelitian

Tujuan umum dari penelitian ini adalah untuk menambah kajian literatur yang memberikan bukti empiris mengenai pengaruh *cybersecurity disclosure* terhadap *audit fee*, serta menambah kajian mengenai kompetensi auditor internal.

1.3.2 Tujuan Khusus Penelitian

Berdasarkan uraian latar belakang mengenai *cybersecurity disclosure*, *audit fee* dan auditor internal di atas, maka tujuan penelitian ini adalah sebagai berikut:

1. Mengetahui adanya pengaruh *cybersecurity disclosure* terhadap *audit fee.*
2. Mengetahui pengaruh *cybersecurity disclosure* terhadap *audit fee* yang dimoderasi oleh kompetensi auditor internal.

1.4 Manfaat Penelitian

Manfaat yang diharapkan dari hasil penelitian ini antara lain adalah sebagai berikut:

1. Manfaat Akademis

Penelitian ini diharapkan dapat menambah pemahaman, pengetahuan, dan dapat menjadi referensi bahan diskusi dan penelitian selanjutnya yang berkaitan dengan *cybersecurity disclosure* terhadap *audit fee* dengan kompetensi auditor internal sebagai variabel moderasi.

2. Manfaat praktis

a. Bagi auditor

Penelitian ini dapat dijadikan sebagai pedoman, referensi atau bahan pertimbangan dalam menentukan *audit fee*.

b. Bagi manajemen perusahaan

Penelitian ini diharapkan dapat menjadi masukan dan referensi dalam penyusunan pengungkapan (*disclosure*) dalam laporan tahunan perusahaan.