# BAB II
# TINJAUAN PUSTAKA

## A. Risiko

1. Definisi Risiko

Risiko adalah sebuah kemungkinan kejadian atau peristiwa yang merugikan perusahaan atau bisnis, dimana kejadian tersebut tidak dapat diprediksi (Latifiana, D. 2017). Dalam buku Manajemen Risiko 1 (2015:6) Ikatan Bankir Indonesia merangkum pengertian risiko menurut para ahli sebagai berikut:

a. Menurut Australian *Risk Management Standards*: "Risiko adalah peluang terjadinya sesuatu yang akan mempunyai dampak terhadap tujuan".
b. Menurut David MC Namee dan Georges Selim: "Risiko adalah konsep yang digunakan untuk menyatakan ketidakpastian atas kejadian dan atau akibatnya yang dapat berdampak secara material bagi tujuan organisasi".
c. Menurut *The Institute of Internal Auditor*: "Ketidakpastian terjadinya sesuatu yang dapat berpengaruh pada pencapaian tujuan. Risiko ditanyatakan dalam ukuran konsekuensi dan kemungkinan".
d. Menurut COSO: Risiko didefinisikan sebagai kemungkianan suatu peristiwa akan terjadi dan berdampak buruk terhadap pencapaian sasaran.
e. Menurut SNI ISO 31000 adalah ketidakpastian yang berdampak pada sasaran perusahan yang bersifat negatif maupun positif, tetapi perlu ditindaki yaitu risiko yang berdampak negatif dikarenakan akan menjadi hambatan untuk mencapai sebuah sasaran maupun tujuan dalam perusahaan jangka pendek maupun jangka panjang.

Dari beberapa definisi diatas dapat disimpulkan bahwa risiko adalah sebuah kejadian atau peristiwa yang berdampak berbahaya untuk sebuah organisasi atau perusahaan yang menyebabkan kerugian dimasa yang akan datang.

2. Klasifikasi Risiko

Menurut Djohanputro (2008) dalam Latifiana, D. (2017) menyatakan bahwa untuk memudahkan pengenalan risiko, perlu dilakukan klasifikasi sehingga

mengenal karakter dari risiko. Risiko dapat dikategorikan ke dalam risiko murni dan risiko spekulatif. Cara lain mengklasifikasi risiko adalah mengategorikan ke dalam risiko sistematik dan risiko spesifik.

a. Risiko Murni dan Spekulatif

Risiko murni merupakan risiko yang dapat mengakibatkan kerugian pada perusahaan, tetapi tidak ada kemungkinan menguntungkan. Perusahaan menghadapi berbagai hal dalam risiko ini. Misalnya, kekayaan mesin yang menanggung risiko murni. Ada kemungkinan mesin mengalami kerusakan, mulai dari kerusakan kecil sampai kerusakan besar. Tetapi, tidak mungkin keadaan sebaliknya bisa terjadi. Kekayaan berupa gedung juga ada kemungkinan mengalami kerugian berupa kerusakan atau kehancuran. Sementara itu yang disebut dengan risiko spekulatif adalah risiko yang dapat mengakibatkan dua kemungkinan, merugakan atau menguntungkan perusahaan.

b. Risiko Sistematik dan Spesifik

Risiko sistematik juga disebut risiko yang tidak dapat didiversifikasi. Ciri-ciri dari risiko sistematik adalah tidak dapat dihilangkan atau dikurangi dengan cara penggabungan berbagai risiko. Risiko spesifik atau risiko yang dapat didiversifikasi dapat dihilangkan melalui proses penggabungan (pooling). Konsep risiko sistematik dan spesifik sangat berguna dalam menangani risiko keuangan. Banyak risiko yang berkaitan dengan keuangan perusahaan dapat ditekan dengan menerapakan diversifikasi.

## B. Konsep Manajemen Risiko

1. Pengertian Manajemen Risiko

Menurut Suseno, P. (2022:26) Secara sederhana pengertian manajemen risiko adalah pelaksanaan fungsi-fungsi manajemen dalam penanggulangan risiko, terutama risiko yang dihadapi oleh organisasi/perusahaan, keluarga dan masyarakat. Jadi mencakup kegiatan merencanakan, mengorganisir, menyusun, memimpin/ mengoordinasi dan mengawasi (termasuk mengevaluasi) program penanggulangan risiko. Program manajemen risiko mencakup tugas-tugas: mengidentifikasi risiko-risiko yang dihadapi, mengukur atau menentukan besarnya risiko tersebut, mencari jalan untuk menghadapi atau menanggulangi risiko,

selanjutnya menyusun strategi untuk memperkecil ataupun mengendalikan risiko, mengoordinasi pelaksanaan penanggulangan risiko serta mengevaluasi program penanggulangan risiko yang telah dibuat.

2. Tujuan Manajemen Risiko

Secara umum, tujuan utama dalam manajemen risiko sebuah lembaga keuangan meliputi hal berikut ini.

a. Menyelasarkan antara risk appetite dan strategi

Pimpinan perusahaan bertanggung jawab untuk menentukan risk appetite yang dapat diterima oleh bisnis dari model bisnis dan strategi yang diadopsi oleh mereka. Risk appetite adalah tingkat risiko dapat diterima oleh perusahaan untuk meraih tujuan bisnisnya. Misalkan kita jumpai ada bank yang memutuskan untuk memberikan kredit kepada sektor mikro (UMK), namun ada pula yang fokus kepada usaha menengah.

b. Mengaitkan antara pertumbuhan, risiko, dan imbal hasil

Tujuannya adalah menyediakan dan meningkatkan kemampuan untuk mengidentifikasi dan menilai risiko dan menetapkan tingkat risiko yang dapat diterima relatif terhadap tujuan pertumbuhan dan laba. Misalnya beberapa bank menetapkan target kredit macet di bawah 5% untuk meraih pertumbuhan laba tertentu.

c. Minimalkan guncangan dan kerugian operasional

Yaitu untuk meningkatkan kemampuan dalam mengidentifikasi peristiwa berpotensi risiko, menilai risiko dan menetapkan tanggapan sehingga dapat mengurangi terjadinya guncangan dan kerugian.

d. Identifikasi dan kelola risiko-silang

Setiap produk menghadapi segudang risiko. Perusahaan tidak hanya mengelola risiko secara individual, tetapi juga mengelola dampak yang saling terkait.

e. Memberikan tanggapan terpadu terhadap berbagai risiko

Proses bisnis membawa banyak risiko yang melekat dan bisnis harus terus mencari solusi untuk mengelola risiko.

f. Rasionalisasi modal

Informasi yang lebih akurat mengenai total risiko memungkinkan perusahaan (lembaga keuangan) untuk lebih efektif untuk menilai kebutuhan modal secara keseluruhan dan memperbaiki alokasi modal.

Jadi kegiatan manajemen risiko mencakup semua tindakan untuk memberikan keamanan terhadap operasi perusahaan dan memberikan kedamaian hati serta ketenteraman jiwa yang dibutuhkan oleh seluruh personil dan pihak yang berkepentingan terhadap perusahaan. Secara umum, batas-batas terhadap manajemen risiko sebagai keputusan eksekutif/manajerial yang berkaitan dengan pengelolaan risiko, pada pokoknya mencakup:

a. Menemukan secara sistematis dan menganalisis kerugian-kerugian yang dihadapi perusahaan (melakukan identifikasi terhadap risiko yang dihadapi).
b. Menemukan metode yang paling baik dalam menangani risiko (kerugian) yang dihubungkan dengan pencapaian tujuan perusahaan. Kerangka kerja manajemen risiko.

3. Tahapan Manajemen Risiko

Menurut Siswanti, et al., (2020:16) Menemukan dan menginformasikan risiko perusahaan adalah tugas manajemen perusahaan. Kegiatan ini merupakan hal penting yang harus dilakukan, untuk mencapai tujuan perusahaan. Adapun tahanpan yang harus dilakukan manajemen perusahaan sebagai berikut:

a. Identifikasi sejarah, data dan fakta

Sejarah perusahaan, data dan fakta merupakan informasi akurat dalam mengidentifikasi risiko yang akan terjadi. Seperti: ketidakpuasan pelanggan, turn over karyawan, laporan keuangan, produk yang error sampai ke pasar penjualan dan daur hidup produk menurun.

b. Pengamatan lingkungan.

Lingkungan terbagi menjadi dua, yaitu: Lingkungan eksternal dan lingkungan internal. Pengamatan lingkungan eksternal seperti: selera pasar, produk baru dari pesaing, tata letak lokasi, dan budaya lokasi penjualan. Pengamatan lingkungan internal, hal yang penting yang sering diabaikan oleh perusahaan.

Ketidakpuasan karyawan, penggunaan teknologi, kerjasama tim, dan kelengkapan perangkat perusahaan, merupakan bagian yang harus diamati di lingkungan internal perusahaan.

## C. *Risk Assessment*

1. Definisi dan Tujuan Risk Assessment

*Risk assessment* didefinisikan sebagai sebuah proses estimasian *score* risiko dari *auditable* unit dalam perusahaan. *Risk assessment* ini digunakan untuk mengidentifikasi, mengukur dan menentukan prioritas dari risiko, agar sebagian besar sumber daya diarahkan ke area layak audit dengan *score* atau bobot risiko tinggi. Tujuan *risk assessment* adalah untuk menentukan prioritas risiko masing-masing *auditable* unit, yang pada giliran berikutnya akan menentukan frekuensi, intensitas dan waktu audit. David Mcnamee dari The IIA dalam Tunggal (2007:64) secara garis besar ada 3 langkah dalam melakukan risk assessment dengan pendekat COSO yaitu:

a. Menentukan sasaran dan tujuan organisasi;
b. Menilai risiko (identifikasi, analisa, dan prioritas);
c. Menetapkan pengendalian yang dibutuhkan untuk mengendalikan risiko yang ada.

2. Metode Risk Assessment

Menurut Tunggal (2007:62) orang yang mengetahui risiko yang signifikan yaitu orang yang paling berpengaruh atau penting di dalam suatu organisasi. Jadi dalam melakukan analisa risiko sebaiknya dimulai dengan melakukan pertemuan dengan pimpinan tertinggi dari suatu unit usaha. Ada tiga metode mendasar yang dapat digunakan untuk menemukan risiko yang signifikan.

a. Wawancara (*Interviewing*)

Wawancara dilakukan secara perorangan dengan auditee yang menghasilkan sudut pandang secara individual terhadap risiko yang dapat menghambat pencapaian tujuan.

Keuntungan wawancara:

1) Lebih mudah untuk mengatur wawancara secara perorangan dibandingkan dengan melakukan wawancara secara kelompok.
2) Auditee mungkin akan lebih mudah untuk menyampaikan perhatiannya terhadap suatu masalah yang mungkin tidak akan disamapikannya jika secara kelompok. Hal ini akan meninggalkan cakupan yang lebih luas dalam mengidentifikasi risiko.

Kerugian wawancara:

1) Cakupan dari hasil identifikasi risiko akan lebih sulit dilakukan kategorisasi.
2) Kita harus tetap melakukan *risk workshop* untuk mendapatkan pendapat umum dalam menemukan dampak dan kemungkinan terjadinya risiko.

b. *Risk Workshop*

Risk workshop dilakukan secara bersama-sama yang melibatkan:

1) Pimpinan tertinggi dari suatu unit usaha untuk mengidentifikasi risiko yang signifikan.
2) Kepala departemen untuk mengetahui risiko secara umum yang menghambat operasional.
3) Staf audit untuk menyampaikan risiko yang sudah diketahui sebelumnya.

Hasil dari *risk workshop* adalah daftar risiko yang mungkin dapat menghambat terhadap jalannya operasional perusahaan yang diukur dari dampak dan kemungkinan terjadinya risiko.

c. *The account* (akun/rekening)

Metode yang ketiga yaitu melakukan pemeriksaan terhadap akun-akun atau rekening perusahan yang diperkirakan menjadi perhatian dari manajemen unit.

## D. Sistem Manajemen Keamanan Informasi

1. Definisi Sistem Manajemen Keamanan Informasi (SMKI)

Sistem manajemen keamanan informasi (SMKI) memberikan solusi lengkap untuk informasi yang unggul pertemuan keamanan dengan menyediakan

prosedur yang diperlukan, alat, dan langkah-langkah untuk meningkatkan dan memelihara informasi organisasi (Jauhary et al., 2022). SMKI merupakan seperangkat unsur yang saling terkait dengan organisasi atau perusahaan yang digunakan untuk mengelola dan mengendalikan risiko keamanan informasi dan untuk melindungi serta menjaga kerahasiaan (*confidentiality*), integritas (*integrity*) dan ketersediaan (*availability*) informasi (Sholikhatin et al., 2018).

2. ISO 27001

Organisasi membutuhkan pengawasan dan peninjauan terhadap keefektifitasan dari kinerja SMKI untuk menjamin pemeliharaan yang tepat pada level perlindungannya. Salah satu kerangka kerja yang meliputi penilaian risiko adalah Standar ISO 27001 yang berhubungan dengan keamanan organisasi secara keseluruhan Calder, A., & Watkins, S. (2012). ISO 27001 menjelaskan syarat-syarat untuk membuat, menerapkan, melaksanakan, memonitor, menganalisa, dan memelihara serta mendokumentasikan Sistem Manajemen Keamanan Informasi (SMKI). ISO 27001 merupakan dokumen standar SMKI yang memberikan gambaran secara umum mengenai apa saja yang harus dilakukan oleh suatu organisasi untuk bisa mengimplementasikan konsep-konsep keamanan informasi pada organisasi.

ISO 27001 adalah standar keamanan unformasi berdasarkan risiko, dengan maksud adalah organisasi membutuhkan proses manajemen risiko (von Solms, 2005). Standar ini memperkenalkan sebuah siklus yang dikenal dengan model "*Plan-Do-Check-Act*" (PDCA). Siklus *Plan-Do-Check-Act* (PDCA) merupakan salah satu sistem manajemen kualitas, yang dipopulerkan oleh Dr. Edwards Deming, seorang ahli manajemen kualitas dari Amerika pada tahun 1950. Tujuan dari model ini adalah untuk menentukan, menerapkan, mengawasi, dan meningkatkan keefektifitasan SMKI organisasi (Saleh & Alfantookh, 2011).

Di dalam ISO/IEC 27001:2005 disebutkan bahwa ISMS (*Information Security Management System*) / SMKI (Sistem Manajemen Keamanan Informasi) merupakan suatu proses yang disusun berdasarkan pendekatan risiko bisnis untuk merencanakan (*Plan*), mengimplementasikan dan mengoperasikan (*Do*), memonitor dan meninjau ulang (*Check*) serta memlihara dan meningkatkan atau

mengembangkan (*Act*) terhadap keamanan informasi perusahaan. Jika mengacu pada pengertian SMKI tersebut, bahwa ISMS adalah suatu pendekatan proses *Plan – Do – Check – Act* (PDCA) maka untuk mengimplementasikannya diperlukan dukungan manajemen. Berikut tahapan dalam model PDCA dalam penelitian (Sholikhatin et al., 2018) :

a. *Plan*

Tahap perencanaan terdapat beberapa aktivitas yang perlu dilakukan antara lain:

1) Ruang lingkup ISMS

Agar sesuai dengan kebutuhan keamanan informasi perusahaan, pemetaan terhadap proses-proses bisnis yang ada, fungsi yang berjalan dalam sistem informasi & aspek-aspek teknologi yang sudah diterapakan. Pemetaan bertujuan untuk mendapatkan gambaran baru, GAP, dan Planning terhadap ISMS.

2) Pendekatan Metodologi berbasis Risiko

Pendekatan ini disesuaiakan dengan kriteria untuk perusahaan yang dapat menggunakan standard/ framework yang paling sesuai untuk diterapkan. Metologi secara umum dibagi dalam beberapa tahap sesuai dengan antara lain:

a) Analisa Risiko

Tahap ini terdapat aktivitas seperti asesmen risiko, indentifikasi threat, vulnerablity, karakterisktik sistem, likelyhood, analisa dampak/menghitung BIA, DLL. Tujuan untuk tahap ini agar memperoleh gambaran detail dari risiko yang ada.

b) *Risk Mitigation*

Pemilihan terhadap mitigaasi risiko yang akan digunakan, strategi mitigasi risiko, cost benefit analysis dan lain-lain. Pemilihan kontrol & metrik pada ISMS bertujuan untuk memperoleh infomasi yang berdasarkan gambaran kondisi ISMS dan target pencapaian dari penerapannya.

c) *Risk Evaluation dan Monitoring*

Monitoring dan evaluasi terhadap risiko yang ada.

d) Penentuan Kebijakan ISMS

Merupakan pernyataan resmi perusahaan terkait ISMS yang dapat berupa Policy, procedure, standard, guideline dan work instruction. SOA (*Statement of Applicability*). Dokumentasi analisis ini terkait dengan kontrol atau kebijakan ISMS tersebut yang dipilih untuk diterapkan. SOA dapat dilakukan sesudah melakukan metodologi berbasis risiko.

b. *Do*

Tahap melaksanakan dari apa yang telah ditentukan & direncanakan didalam tahap sebelumnya yakni "*plan*". Aktivitas ditahap ini antara lain:

1) Mengelola semua *resources* yang mungkin terlibat dalam ISMS mencakup: *acquire, configuration, maintain dan disposal*.
2) Pengawasan implementasi dari ISMS.
3) Pengembangan kebijakan yang disesuaian dengan kerangka yang dihasilkan dalam tahap plan.
4) *Knowledge* transfer dan *user awarness* terhadap ISMS.

c. *Check*

ISMS memerlukan adanya pengukuran untuk tahap perencanaan dan implementasi untuk memberikan gambaran gap antara perencanaan dengan implementasi dan dalam rangka menuju langkah improvement ISMS. Dalam tahap ini aktivitas yang dilakukan sebagai berikut:

1) Pengukuran dari hasil kinerja keseluruhan ISMS yang mecakup pencatatan & pengumpulan bukti-bukti baik fisik/ logik sebagai sarana audit.
2) Pengukuran daya guna dari satu control yang sudah diterapakan.
3) Review keseluruhan ISMS dan memberikan analisa ISMS.

d. *Act*

Seluruh kontrol yang ditetapkan dan telah diterapkan dalam ISMS tidak akan memberikan hasil yang efektif tanpa adanya improvement atau semua itu hanya akan menjadi tumpukan dokumen atau kumpulan file-file tanpa arti. Tahap ini mencakup point penting sebagai berikut:

1) Melakukan peningkatan dari hasil asesmen tahap-tahap ISMS sebelumnya.
2) Memastikan kegagalan tidak terulang kembali.
3) Knowledge transfer dari hasil peningkatan.

3. COBIT 5 dan Enablers

COBIT adalah kerangka kerja yang disusun secara komprehensif untuk membantu perusahaan menciptakan nilai optimal dari Teknologi Informasi (TI) yang dikembangkan oleh ISACA, dengan cara menjaga keseimbangan antara optimalisasi sumber daya dengan manfaat dan tujuan yang diharapkan. Pendekatan dengan menggunakan kerangka COBIT 5 dalam tata kelola TI dilakukan untuk menjamin keselarasan TI dengan tujuan bisnis dan kebijakan strategis (Felayati et al., 2018).

Untuk dapat melaksanakan fungsinya dengan benar, COBIT 5 mempunyai 7 enablers atau disebut juga faktor penggerak. COBIT 5 menyediakan kerangka kerja IT Governance dan control objectives yang rinci bagi manajemen, pemilik proses bisnis, pemakai dan auditor, karena mengelola teknologi informasi secara holistic sehingga nilai yang diberikan oleh teknologi informasi dapat tercapai optimal dengan memperhatikan segala aspek tata kelola teknologi informasi mulai dari sisi people, skills, competencies, services, infrastructure, dan applications yang merupakan bagian dari enabler suatu tata kelola teknologi informasi (Kurnia Candra et al., n.d., 2015). Berikut adalah ketujuh enabler tersebut:

a. *Principles, Policies and Framework*

Prinsip, kebijakan dan kerangka kerja merupakan enablers pertama dari COBIT 5, enablers ini berfungsi untuk merumuskan kebutuhan dan perilaku stakeholder menjadi panduan praktis yang akan digunakan di dalam kegiatan operasional perusahaan khususnya pada sektor IT.

b. *Processes*

Proses sebagai enabler memiliki peran untuk memberikan rincian mengenai rangkaian kegiatan dan aktivitas praktis yang dilakukan untuk mencapai tujuan dari perusahaan. Proses juga diharapkan untuk memberikan hasil keluaran

yang mendukung pencapaian dari bidang IT di dalam perusahaan. Ada 4 tahapan yang harus dipenuhi dalam menjabarkan sebuah proses sesuai dengan COBIT 5 yaitu:

1) *Align, Plan and Organize* yaitu bagaimana proses tersebut dirancang dan diatur.
2) *Build, Acquire and Implement* yaitu bagaimana proses direalisasikan dan diimplementasi.
3) *Deliver, Service and Support* yaitu bagaimana caranya agar proses dapat berfungsi dalam mencapai tujuan organisasi.
4) *Monitor, evaluate and assess* yaitu bagaimana proses dapat dikontrol, dinilai dan dilakukan evaluasi terhadap proses tersebut.

c. *Organizational Structure*

Struktur organisasi menjadi kunci di dalam pengambilan keputusan di dalam organisasi. Keputusan yang dibuat juga harus memenuhi kebutuhan dan tujuan semua stakeholder. Sehingga entitas tersebut bertanggung jawab terhadap keputusan – keputusan dan kebijakan yang dilakukan oleh perusahaan.

d. *Culture, Ethics and Behaviour*

Setiap perusahaan memiliki budaya, etika dan kebiasaan masing – masing, kebiasaan tersebut bisa terjadi karena banyak faktor dan juga dapat bersifat pribadi ataupun organisasi. Beberapa nilai nilai dan tujuan perusahaan hanya dapat dicapai dengan kebiasaan perusahaan yang baik, oleh karena itu dibutuhkan suatu standar untuk memberikan penilaian terhadap sebuah budaya, kebiasaan dan etika. Terkadang faktor budaya, etika dan kebiasaan ini sering dihiraukan walaupun sebenarnya keberhasilan suatu program di dalam perusahaan sangat bergantung terhadap darinya.

e. *Information*

Informasi merupakan faktor yang sangat penting terhadap kegiatan bisnis di dalam suatu perusahaan karena informasi merupakan syarat untuk membuat ‘pergerakan’ di dalam perusahaan seperti membuat keputusan, mengatasi masalah, dll. Tanpa informasi perusahaan akan salah dalam membuat keputusan yang tepat. Kerangka kerja COBIT 5 mengatur arus dari perpindahan informasi yang ada di semua bagian pada organisasi yang digunakan oleh perusahaan.

UNIVERSITAS NASIONAL

f. *Services*

Infrastruktur dan aplikasi termasuk infrastuktur, teknologi dan aplikasi yang menyediakan layanan adalah objek objek menjadi penggerak di dalam COBIT 5. Objek – objek tersebut memberikan layanan terhadap proses teknologi dan informasi bagi perusahaan. Layanan tersebut merupakan penghubung antara pengguna IT dan proses IT yang telah dirancang sebelumnya, sehingga apabila layanan tersebut tidak berfungsi dengan benar maka tujuan IT perusahaan juga tidak akan tercapai.

g. *People, skill and competencies*

Keahlian dan kompetensi berhubungan dengan orang dan yang dibutuhkan untuk menjalankan semua aktifitas yang berhasil dan pembuatan keputusan yang tepat serta mengambil aksi-aksi perbaikan. Ketersediaan tenaga kerja juga merupakan tujuan yang harus dicapai pada bagian penggerak ini. Tenaga kerja harus terseleksi dengan baik sehingga dapat melaksanakan proses dan peran mereka masing – masing sehingga pada akhirnya tujuan perusahaan dapat tercapai dengan efisen dan tepat pada sasaran.

## E. Audit

1. Definisi Audit

Secara etimologi, pemeriksaan (audit) berasal dari bahasa latin dengan kata "auderee" yang berarti mendengar. Mendengar yang efektif adalah sebuah aktivitas menyerap informasi dalam suatu media dengan menggunakan alat pendengaran yang diikuti dengan respon yang terprogram. Menurut Alvin, A,A. Randal J.E., Mark S.B. (2005) mendefinisikan auditing sebagai pengumpulan dan evaluasi bukti-bukti dari informasi yang dilakukan oleh orang yang kompeten dan independen, untuk menentukan dan melaporkan tingkat kesesuaian antara informasi tersebut dengan kriteria yang telah ditetapkan.

Audit sebagai sebuah proses sistematik untuk memperoleh dan mengevaluasi bukti secara objektif dengan tujuan untuk menetapkan tingkat kesesuaian antara pernyataan dengan kriteria yang telah ditetapkan, serta penyampaian hasil kepada pemakai yang berkepentingan (Mulyadi, 2016).

Kesimpulannya, auditing adalah proses sistematis yang dilakukan untuk memperoleh dan mengevaluasi bukti secara objektif mengenai asersi-asersi kegiatan dan peristiwa ekonomi dengan tujuan menetapkan derajat kesesuaian antara asersi-asersi tersebut dengan kriteria yang telah ditetapkan lalu mengkomunikasikan hasilnya kepada pihak-pihak yang berkepentingan.

2. Jenis-jenis Audit

Audit pada umumnya terbagi menjadi tiga golongan Mulyadi (2016) yaitu: audit keuangan, audit kepatuhan, dan audit operasional.

a. Audit laporan keuangan (Financial statement audit) adalah audit laporan keuangan berhubungan dengan kegiatan pengumpulan dan pengevaluasian bukti mengenai laporan-laporan suatu entitas dengan maksud untuk memberikan pendapat atau opini tentang laporan tersebut apakah sesuai dengan kriteria dan prinsip akuntansi yang berlaku umum atau tidak.

b. Audit kepatuhan (Compliance audit) adalah audit yang bertujuan untuk memastikan apakah perusahaan telah menaati peraturan dan kebijakan yang berlaku, baik kebijakan yang ditetapkan oleh pihak intern maupun pihak ekstern dari entitas atau perusahaan. Audit ini berperan menentukan sejauh mana ketaatan perusahaan terhadap peraturan, kebijakan, serta peraturan pemerintah yang berlaku dan yang harus dipatuhi oleh entitas yang diaudit.

c. Audit operasional (Operational audit) adalah pemeriksaan terhadap kegiatan operasional sebuah perusahaan, seperti kebijakan akuntansi serta kebijakan operasional manajemen dengan maksud untuk memastikan kegiatan operasi yang dilakukan berjalan secara efektif dan efisien.

3. Jenis-Jenis Auditor

Auditor dapat dibedakan menjadi empat jenis, yaitu auditor pemerintah, auditor forensik, auditor internal, dan auditor eksternal (Thian,2021:1). Berikut penjelasan tugas masing-masing auditor tersebut:

a. Auditor pemerintah adalah auditor yang bertugas melakukan audit atas keuangan negara pada instansi-instasi pemerintah.

b. Auditor forensik adalah auditor yang menggunakan keahlian auditing, akuntansi dan investigasi untuk membantu penyelesaian sengketa keuangan dan pembuktian atas dugaan telah terjadinya tindakan *fraud* (kecurangan).

c. Auditor internal adalah auditor yang bekerja pada satu manajemen perusahaan, sehingga berstatus sebagai karyawan dari perusahaan tersebut. Auditor internal merupakan bagian yang integral dari struktur organisasi perusahaan yang berperan memberikan pengawasan serta penilaian secara terus-menerus. Auditor internal memiliki kepentingan atas efektivitas pengendalian internal di suatu perusahaan.

d. Auditor eksternal adalah pihak luar perusahaan yang melakukan pemeriksaan untuk memberikan pendapat mengenai kewajaran laporan keuangan yang telah disusun oleh manajemen perusahaan klien.

4 Audit Internal

Audit internal adalah penilaian yang sistematis dan objektif yang dilakukan auditor internal terhadap operasi dan pengawasan yang berbeda-beda dalam organisasi untuk menentukan apakah (1) informasi keuangan dan operasi telah akurat dan dapat diandalkan; (2) resiko yang dihadapi perusahaan telah diidentifikasi dan diminimalisasi; (3) peraturan eksternal serta kebijakan dan prosedur internal yang bisa diterima telah diikuti; (4) kriteria operasi yang memuaskan telah terpenuhi; (5) sumber daya telah digunakan secara efisien dan ekonomis; dan (6) tujuan organisasi telah dicapai secara efektif. Semua dilakukan dengan tujuan untuk dikonsultasikan dengan manajemen dan membantu anggota organisasi dalam menjalankan tanggung jawabnya secara efektif (Sawyer et al.,2005:10).

Menurut Gondodiyoto (2007:48) manfaat yang dapat diberikan oleh audit intern adalah: (1) Memonitor aktivitas yang tidak dapat dimonitor oleh manjemen puncak; (2) Mengidentifikasi dan meminimalisasi risiko; (3) Memvalidasi laporan kepada manajemen puncak; (4) Memproteksi manajemen

senior dari kesalahan dari aspek teknis; (5) Memvalidasi informasi yang tersedia untuk mengambil keputusan; (6) Menilai kinerja; (7) Membantu manajer fungsional agar terhindar dari kesalahan teknis, kesalahan prosedur atau penyimpangan dari prinsip manajemen yang baik sehingga dapat merugikan perusahaan.

5. Audit Berbasis Risiko

Audit berbasis risiko merupakan suatu pendekatan yang memungkinkan bagi audit internal untuk memenuhi ekspektasi tersebut melalui metode audit internal untuk menyakinkan kecukupan bahwa risiko pada sebuah perusahaan dikelola sesuai dengan batasan risiko yang ditetapkan perusahaan. Konsep dasar risk-based audit merupakan suatu pendekatan audit atas area-area yang memiliki risiko terbesar dan sangat mempengaruhi perusahaan. Tujuan Pelaksanaan audit berbasis risiko adalah mengembangkan temuan dalam perspektif manajemen risiko dan menyimpulkan hasil pelaporan dalam konteks risiko yang menjadi tujuan proses pelaporan.

Perubahan paradigma dari profesi internal audit menurut definisi internal auditing yang dikeluarkan oleh International Internal Auditing (IIA) tahun 1999 dimana penggunaan istilah kontrol sudah beralih menjadi risiko. Fokus audit saat ini adalah risiko bisnis dari perusahaan bukan system internal control, fokus pengujian adalah semua aktivitas risk manajemen, tidak lagi aktivitas control, fokus dari pelaporan adalah kecukupan dan efektivitas dari strategy management bukan kecukupan dan efektivitas dari internal kontrol dan tujuan dari hasil audit adalah mencapai pelaksanaan manajemen risiko yang sesuai bukan memperbaiki internal control.

Dari perubahan paradigma ini istilah risiko menjadi hal yang sangat krusial karena risiko adalah segala hal yang menyebabkan tujuan dari perusahaan tidak tercapai sehingga internal audit seharusnya melakukan analisa risiko untuk mengidentifikasikan segala risiko yang mungkin terjadi di masa yang akan datang. Analisa risiko itu penting karena manajemen akan mengambil keputusan setiap saat tentang apa yang akan dilakukan berapa banyak waktu dan sumber daya yang dibutuhkan dari suatu kegiatan dan hal-hal penting yang perlu dilaporkan sehingga

internal audit dapat memberikan nilai tambah bagi perusahaan. Dalam konsep audit berbasis risiko, semakin tinggi risiko suatu area, maka semakin tinggi perhatian pada audit area tersebut. Untuk mengidentifikasi suatu risiko bisnis, auditor harus memahami aspek pengendalian dari bisnis termasuk memahami risiko dan pengendalian system dalam mencapai sasaran atau tujuan organisasi (Tunggal, 2012:95).

Menurut Tuanakotta (2013:101-102), ada beberapa manfaat dari suatu audit berbasis risiko adalah sebagai berikut:

a. Fleksibilitas waktu;
b. Upaya tim audit terfokus pada area kunci;
c. Prosedur audit terfokus pada risiko;
d. Pemahaman atas pengendalian internal;
e. Komunikasi tepat waktu.

Secara lebih rinci tujuan audit internal berbasis risiko menurut Tunggal (2007:119) adalah untuk memberikan keyakinan atau kepastian kepada komite audit, dewan komisaris dan direksi, bahwa:

a. Perusahaan telah memiliki proses manajemen risiko, dan proses tersebut telah dirancang dengan baik.
b. Proses manajemen risiko dimaksud telah diintegrasikan oleh manajemen perusahaan ke dalam semua tingkatan organisasi mulai dari tingkat korporasi, divisi sampai unit kerja terkecil dan telah berfungsi sebagaimana yang diinginkan.
c. Kerangka kerja pengendalian internal (*internal control framework*) dan tata kelola yang baik (*governance*) yang ada telah tersedia secara cukup dan berfungsi secara baik guna mengendalikan risiko yang ada.

Hanafi (2009:10) menyatakan bahwa adapun tahapan dalam audit berbasis risiko tersebut adalah: (1) Pendahuluan; (2) Pelaksanaan; (3) Pelaporan.

6. Perbedaan Audit Tradisional dengan Audit Berbasis Risiko

Dalam pendekatan tradisional, auditor akan berfokus pada aktifitas di masa lampau dan mencoba untuk mengungkap aktifitas apa yang menyebabkan kegagalan, sedangkan dalam pendekatan risk based internal audit mencoba untuk

mencegah kesalahan tersebut. Perbedaan dari kedua pendekatan yang dikemukakan oleh Kishali & Pehlivanlı dalam Larasati, D. A., & Bernawati, Y. (2020). Pada pendekatan berbasis risiko, maka auditor akan focus pada kondisi masa kini dan risiko masa mendatang dibandingkan hanya sibuk dengan melakukan pengendalian internal.

Baik pendekatan berbasis tradisional maupun pendekatan berbasi risiko sejak awal telah membertimbangkan risiko di dalam perusahaan. Perbedaannya adalah, dalam pendekatan tradisional berfokus pada natural risk, *control risk*, dan *finding risk* sedangkan dalam pendekatan berbasis risiko mengikutsertakan risiko yang melekat pada entitias (*the institutions' own risks*). Umumnya dalam pendekatan tradisional, internal auditor akan menghabiskan sebagian besar waktunya pada detail perencanaan, teknis dan sistem pengendalian internal. Sedangkan dalam pendekatan berbasis risiko, sebagian besar waktu dari internal auditor dihabiskan untuk memahami bisnis proses dan risiko yang melekat dan bagaiman cara manajemen tersebut.

Pada kedua pendekatan tersebut juga terdapat perbedaan posisi Internal auditor di dalam perusahaan. Pada pendekatan tradisional, internal auditor berada dalam posisi sebagai "*watch dog*" dimana ia menjadi pihak independen dalam melakukan pemeriksaan data akuntansi, pengendalian internal dan pelaksanaan pengawasan. Pada pendekatan berbasis risiko, pihak internal auditor menempatkan dirinya dalam sisi yang sama dengan institusi yang di audit, dan menjadi pihak yang secara rutin menilai system di dalam perusahaan serta memberikan rekomendasi yang penting bagi manajemen. Konsep risk based audit planning digunakan oleh internal auditor untuk memastikan bahwa tindakan audit yang dilakukan telah focus untuk memberikan assurance di dalam perusahaan bahwa tindakan manajemen risiko di perusahaan telah sejalan dengan *risk apetite* yang sebelumnya telah ditetapkan oleh perusahaan (Griffiths, dalam Larasati, D. A., & Bernawati, Y. 2020).

## F. Konsep Business Process Outsourcing (BPO)

1. Definisi *Outsourcing*

Istilah outsourcing dari kata "*out*" dan "*source*" yang berarti sumber dari luar, merupakan pendekatan manajemen yang memberikan kewenangan pada sebuah agen luar (pihak ketiga) untuk bertanggung jawab terhadap proses atau jasa yang sebelumnya dilakukan oleh perusahaan. Bisa juga didefinisikan sebagai membeli barang atau jasa yang sebelumnya disediakan secara internal (Swink, 1999; Smith et al, 1996; Lankford and Parsa,1999; Elmuti and Kathawala, 2000; dalam Salamah, W.,2011). Ada dua actor pokok dalam proses *outsourcing*, yakni "*outsourced*" dan "*outsourcer*". Yang pertama menunjuk pada perusahaan yang menyerahkan pekerjaan, yang kedua merupakan perusahaan yang menerima pekerjaan (Saunders and Gebelt, dalam Salamah, W., 2011).

2. Tipe Outsourcing

Menurut Komang dan Agus dalam Salamah, W., (2011) tipe outsourcing dibedakan menjadi dua kelompok yaitu *Business Process Outsourcing* dan *Outsourcing* Sumber Daya Manusia.

a. *Business Process Outsourcing* (BPO), jika di Indonesia dikenal dengan pemborongan pekerjaan. *Outsourcing* jenis ini mengacu pada hasil akhir yang dikehendaki. Jika sebuah perusahaan manufaktur ingin mengalihkan penjualan produknya pada perusahaan lain, maka pembayaran kompensasinya berupa jumlah unit yang terjual.

b. *Outsourcing* Sumber Daya Manusia. *Outsourcing* ini mengacu pada kebutuhan penyediaan dan pengelolaan sumber daya manusia. Untuk contoh di atas, perusahaan manufaktur akan bekerja sama dengan perusahaan *outsourcing* (vendor) yang memberikan jasa penyediaan dan pengelolaan tenaga penjual. Kompensasi kepada vendor berupa management fee sesuai kesepakatan.

3. Manfaat *Outsourcing*

Ada banyak alasan dikemukakan dalam mengambil keputusan untuk melakukan strategi outsourcing. Berbagai manfaat yang diperoleh merupakan hal yang sering ditonjolkan, meski tentu saja banyak resiko yang harus dihadapi. (Kremic dalam Salamah, W., 2011) telah melakukan studi literatur terhadap isi lebih dari 200 publikasi dan hasilnya tidak berbeda dengan yang dikemukakan oleh Embleton dan Wright, dalam Salamah, W, (2011) seperti berikut:

a. Penghematan biaya (*cost saving*). Bisa terjadi karena vendor lebih fokus mengelola aktifitas yang dibutuhkan oleh outsourced. Rata-rata perusahaan merealisasikan 9 persen penghematan biaya dan 15 persen peningkatan kapasitas dan kualitas melalui outsourcing.

b. Penghematan waktu (**time saving**). Lebih dari sepertiga (37 persen) perusahaan yang disurvei menyatakan bahwa penghematan waktu merupakan pertimbangan utama.

c. Biaya tersembunyi (*hidden cost*). Banyak organisasi mempunyai biaya tersembunyi yang tidak diketahui sampai dilakukannya strategi outsourcing.

d. Aktifitas inti (*core activity*). Jika perusahaan ingin fokus pada aktifitas inti, maka pengurangan aktifitas yang lain untuk diserahkan kepada pihak luar merupakan pilihan yang harus diambil.

e. Pemasukan kas (*cash infusion*). Karena ada aktifitas yang diserahkan pada pihak luar, maka akan ada fasilitas atau aset yang dijual, sehingga memberikan pemasukan uang kas.

f. Ketersediaan bakat (*talent availability*). Outsourcing menyediakan akses untuk memperoleh sumberdaya yang berbakat yang tidak bisa disediakan perusahaan.

g. Rekayasa ulang (*re-engineering*). Membuat kerjasama dengan vendor membuat manajer berkesempatan mengevaluasi proses bisnis mereka.

h. Budaya korporat (*corporate culture*). Vendor mungkin mempunyai budaya harmonis yang cocok dengan budaya perusahaan. Meskipun begitu untuk melakukan perubahan perlu diperhatikan timbulnya pergolakan yang mungkin terjadi.

i. Fleksibilitas yang lebih besar (*greater flexibility*). Melalui kerjasama dengan vendor perusahaan lebih leluasa menerima permintaan pelanggan baik waktu maupun jumlah, dan mengalokasikan sumberdaya yang dimiliki

j. Akuntabilitas (*accountability*). Vendor komersial dibatasi oleh kontrak untuk menyediakan jasa pada tingkat tertentu yang disepakati, sementara departemen internal tidak selalu bisa dikendalikan pengeluarannya.

k. Akses terhadap spesialis lebih besar (*access to specialist*). Keahlian, peralatan, teknologi dan advis independen dapat diperoleh dari perusahaan outsourcing.

l. Produktivitas lebih tinggi (*greater productivity*). Outsourcing dapat digunakan untuk meningkatkan produktivitas karen beban dibagi dengan vendor.

m. Perbaikan kualitas (*quality improvement*). Outsourcing dapat memperbaiki kualitas karena vendor adalah spesialis di bidangnya.

n. Jarak geografis (*geographical distance*). Outsourcing bisa digunakan untuk mengatasi masalah jarak geografis.

## G. Penelitian Terdahulu

Berikut penelitian terdahulu yang sesuai sebagai rujukan penelitian ini terdapat pada tabel 2.1

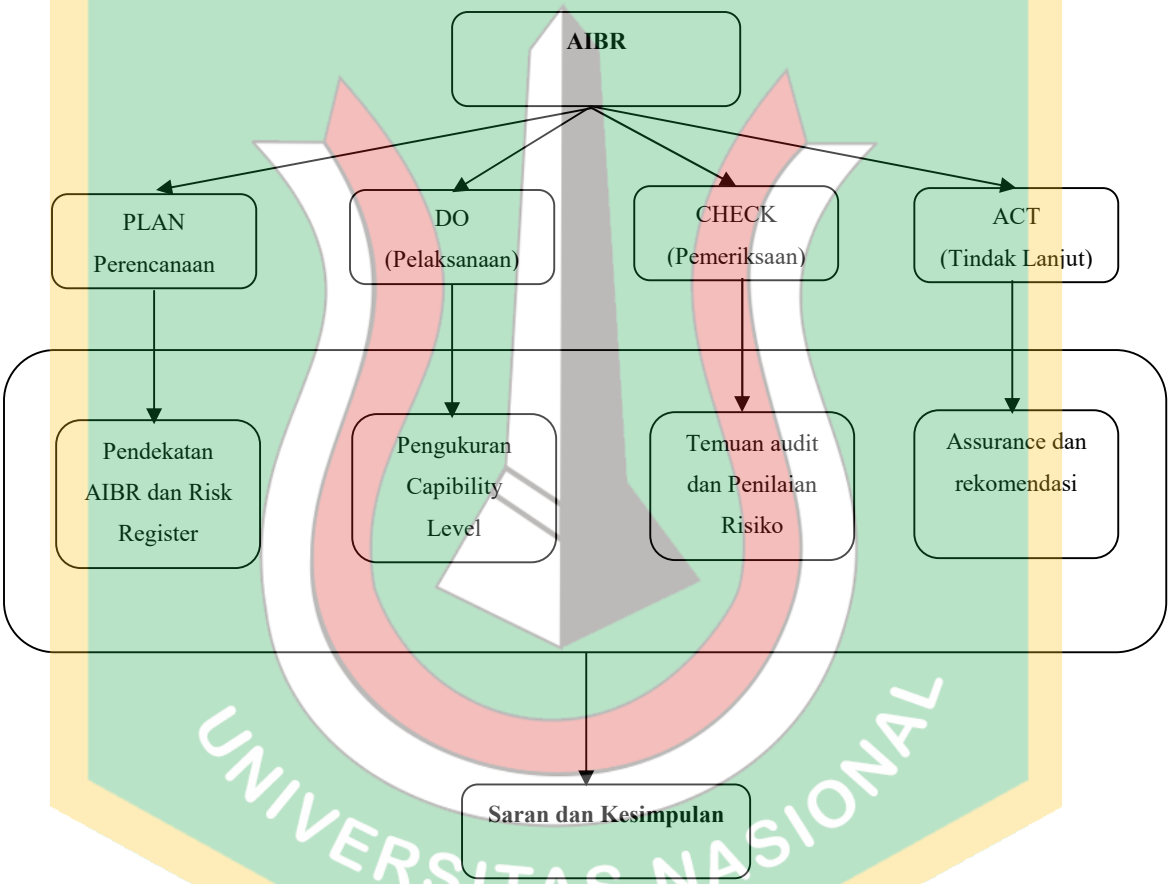
Tabel 2.1 Penelitian Terdahulu

| No | Penulis | Tahun | Judul | Hasil |
|---|---|---|---|---|
| 1 | Kurniawan, C., & Azwir, H. H. | 2019 | Penerapan Metode PDCA untuk Menurunkan Tingkat Kerusakan Mesin pada Proses Produksi Penyalutan | Dengan penerapan metode PDCA pada proses produksi penyalutan, maka berhasil menemukan masalah dan menurunkan tingkat kerusakan mesin pada proses penyalutan. |
| 2 | Sholikhatin, S. A., Setyanto, A., & Luthfi, E. T. | 2018 | Analisis Keamanan Sistem Informasi | Berdasarkan klausul dalam ISO 27001 dan dengan hasil penelitian pada objek, |

| | | | | |
|---|---|---|---|---|
| | | | Dengan ISO 27001 (Studi Kasus: Sistem Informasi Akademik Universitas Muhammadiyah Purwokerto) | penambahan variabel Server Security menjadi penting dalam memaksimalkan sistem manajemen keamanan informasi. |
| 3 | Felayati, F., Mulyana, R., & Witjaksono, R. W. | 2018 | Analisis dan Perancangan Tata Keloladan Pengelolaan Teknologi Informasi Berbasis Kerangka COBIT 5 *Domain Align-Plan-Organise* (APO) | Berdasarkan hasil assessment7 enabler yang dilakukan, kondisi tata kelola TI Diskominfo Jabar saat ini belum diterapkan secara optimal jika dilihat dari cukup banyaknya kesenjangan kondisi tata kelola |
| 4 | Fauza, Q., & Kautsar, A. P. | 2018 | Review Artikel: *Plan-Do-Check-Act* (Pdca) Dalam Meningkatkan Kualitas Pelayanan Kesehatan Di Rumah Sakit | Hasil yang didapatkan yaitu siklus PDCA dapat meningkatkan kualitas pelayanan kesehatan serta menurunkan kesalahan pengobatan. Oleh karena itu dapat disimpulkan bahwa siklus PDCA merupakan intervensi yang efektif untuk dilakukan sehingga dapat diperoleh suatu perbaikan secara terus-menerus dalam suatu organisasi. |
| 5 | Larasati, D. A., & Bernawati, Y. | 2020 | *Risk Based Approach Dan Tren* Mendatang Dalam Internal Audit Tools & Techniques | Risk based audit plan diyakini akan terus dipergunakan auditor dimasa mendatang, karena internal auditor meyakini bahwa apabila perencanaan didasarkan pada risiko kunci yang ada di dalam organisasi, maka akan |

| | | | | |
|---|---|---|---|---|
| | | | | meningkatkan kemampuan Kepala Internal Audit untuk menyesuaikan rencana audit dengan kebutuhan organisasi. |

## H. Kerangka Analisis




Gambar 2.1 Kerangka Analisis

UNIVERSITAS NASIONAL