AUDIT SISTEM INFORMASI

Penulis :

Wahyuddin S, M. Bobbi Kurniawan Nasution, Angga Aditya Permana, Ratna Dewi, Decky Hendarsyah, Adib Pakarbudi, Yuliana Mose, Purnawarman Musa, Ade Maulana, Hermila A., Nurfitria Ningsi, Iwan Adhicandra, Elsy Rahajeng

ISBN 978-623-198-269-8

AUDIT SISTEM INFORMASI

Wahyuddin S
M. Bobbi Kurniawan Nasution
Angga Aditya Permana
Ratna Dewi
Decky Hendarsyah
Adib Pakarbudi
Yuliana Mose
Purnawarman Musa
Ade Maulana
Hermila A.
Nurfitria Ningsi
Iwan Adhicandra
Elsy Rahajeng

GET PRESS INDONESIA

AUDIT SISTEM INFORMASI

Penulis :
Wahyuddin S
M. Bobbi Kurniawan Nasution
Angga Aditya Permana
Ratna Dewi
Decky Hendarsyah
Adib Pakarbudi
Yuliana Mose
Purnawarman Musa
Ade Maulana
Hermila A.
Nurfitria Ningsi
Iwan Adhicandra
Elsy Rahajeng

ISBN : 978-623-198-269-8

Editor : Dina Ediana, M.Kom.
Penyunting: Yuliatri Novita, M.Hum.
Desain Sampul dan Tata Letak : Tri Putri Wahyuni, S.Pd.

Penerbit : GET PRESS INDONESIA
Anggota IKAPI No. 033/SBA/2022

Redaksi :
Jl. Palarik RT 01 RW 06 Kelurahan Air Pacah
Kecamatan Koto Tangah Padang Sumatera Barat

website: www.getpress.co.id
email: adm.getpress@gmail.com

Cetakan pertama, Mei 2023

KATA PENGANTAR

Dengan mengucapkan puji syukur kehadirat Allah SWT, atas limpahan rahmat dan hidayahNya, maka Penulisan Buku dengan judul Audit Sistem Informasi dapat diselesaikan dengan kerjasama tim penulis. Audit sistem informasi merupakan proses independen dan sistematis untuk mengevaluasi sistem informasi dan memastikan bahwa mereka memenuhi standar dan tujuan bisnis. Audit ini meliputi pemeriksaan terhadap aktivitas dan proses sistem informasi, serta evaluasi terhadap implementasi kontrol sistem informasi. Buku ini ditujukan untuk mahasiswa terutama dibidang ilmu Komputer untuk mempelajari tentang Audit Sistem Informasi. Buku ini berisi tentang konsep dasar kontrol dan audit sistem informasi, prinsip-prinsip dasar audit SI, proses audit sistem informasi, standar dan panduan untuk audit sistem informasi, sistem kontrol internal, kerangka kontrol manajemen dan aplikasi, perencanaan & manajemen audit, proses pengumpulan bukti pada audit sistem informasi, proses evaluasi bukti pada audit sistem informasi, tata kelola IT dan manajemen risiko, ITIL (*Information Technology Infrastructure Library*) V3.

Buku ini masih banyak kekurangan dalam penyusunannya. Oleh karena itu, kami sangat mengaharapkan kritik dan saran demi perbaikan dan kesempurnaan buku ini selanjutnya. Kami mengucapkan terima kasih kepada berbagai pihak yang telah membantu dalam proses penyelesaian Buku ini. Semoga Buku ini dapat menjadi sumber referensi dan literatur yang mudah dipahami.

Padang, April 2023
Penulis

DAFTAR ISI

DAFTAR GAMBAR

DAFTAR TABEL

BAB 1
KONSEP DASAR KONTROL DAN AUDIT SISTEM INFORMASI

1.1 Pendahuluan

Konsep dasar kontrol sistem informasi adalah suatu proses yang memastikan bahwa sistem informasi berfungsi sesuai dengan tujuannya dan melindungi aset-aset penting. Ini meliputi identifikasi risiko, implementasi prosedur keamanan, monitoring aktivitas sistem, dan pemeliharaan catatan. Konsep dasar kontrol dan audit sistem informasi merupakan dasar dari manajemen risiko dan keamanan informasi dalam sistem informasi. Kontrol dan audit sistem informasi memastikan bahwa sistem informasi berfungsi dengan baik dan aman, serta memenuhi standar dan tujuan bisnis. Adapun tujuan dari kontrol sistem informasi adalah untuk memastikan bahwa aktivitas sistem informasi dilakukan sesuai dengan rencana dan memastikan bahwa tujuan sistem informasi tercapai. Kontrol ini meliputi berbagai aspek, seperti keamanan informasi, integritas data, akses terkontrol, dan manajemen konfigurasi.

Kontrol dan audit sistem informasi (SI) adalah dua aspek penting dalam menjaga keamanan dan kehandalan sistem informasi suatu organisasi. Kontrol SI adalah setiap tindakan atau kebijakan yang dilakukan untuk memastikan bahwa informasi yang disimpan, diproses, atau ditransmisikan melalui sistem informasi tersebut terlindungi dan tersedia dengan cara yang tepat. Audit SI, di sisi lain, adalah proses evaluasi independen dari sistem informasi organisasi, termasuk evaluasi atas kontrol SI, guna

memastikan bahwa sistem informasi tersebut berfungsi sesuai dengan tujuan dan kebijakan organisasi.

Konsep dasar audit sistem informasi adalah evaluasi independen terhadap sistem dan proses yang ada dalam sistem informasi untuk memastikan bahwa mereka memenuhi standar dan memenuhi tujuan bisnis. Ini meliputi pengujian kontrol, pengujian fungsionalitas, dan analisis data untuk menilai efektivitas dan efisiensi sistem informasi. Audit sistem informasi merupakan proses independen dan sistematis untuk mengevaluasi sistem informasi dan memastikan bahwa mereka memenuhi standar dan tujuan bisnis. Audit ini meliputi pemeriksaan terhadap aktivitas dan proses sistem informasi, serta evaluasi terhadap implementasi kontrol sistem informasi (Wikipedia, 2023).

Kontrol dan audit sistem informasi sangat penting dalam memastikan bahwa sistem informasi berfungsi dengan benar dan aman, dan memenuhi standar dan tujuan bisnis. Oleh karena itu, konsep dasar kontrol dan audit sistem informasi harus dipahami dan diterapkan oleh semua profesional yang terlibat dalam manajemen sistem informasi.

1.2 Sejarah Kontrol & Audit SI

Sejarah konsep dasar kontrol dan audit sistem informasi bermula pada era komputer pertama, ketika sistem informasi baru mulai digunakan untuk membantu bisnis dan organisasi dalam mengelola data dan informasi mereka. Pada awalnya, sistem informasi hanya digunakan sebagai alat untuk menyimpan dan mengakses data, tetapi seiring waktu, mereka menjadi semakin kompleks dan memerlukan kontrol dan audit untuk memastikan bahwa mereka berfungsi dengan benar dan aman.

Pada tahun 1970-an, konsep dasar kontrol dan audit sistem informasi mulai berkembang dan diterapkan secara luas. Pada tahun 1977, Standar Akuntansi Komputer dan Sistem (COSO) diterbitkan oleh Komite Standar Akuntansi Nasional (AICPA), memberikan panduan untuk kontrol dan audit sistem informasi.

Sejak saat itu, konsep dasar kontrol dan audit sistem informasi terus berkembang dan diperbarui sesuai dengan perkembangan teknologi dan perubahan dalam bisnis dan organisasi. Pada tahun 2013, ISO/IEC 27001:2013 diterbitkan sebagai standar internasional untuk keamanan informasi, memberikan panduan untuk kontrol dan audit sistem informasi dalam era digital.

Pada saat ini, kontrol dan audit sistem informasi menjadi bagian penting dari manajemen risiko dan keamanan informasi, dan memainkan peran penting dalam memastikan bahwa sistem informasi berfungsi dengan benar dan aman serta memenuhi standar dan tujuan bisnis (Sihotang et al., 2023).

1.3 Pengertian Kontrol & Audit SI

Berikut adalah beberapa pengertian konsep dasar kontrol dan audit sistem informasi menurut para ahli:

1.3.1 Konsep dasar kontrol sistem informasi

- Menurut ISO/IEC 27001:2013, kontrol sistem informasi adalah tindakan yang diambil untuk memastikan bahwa aktivitas sistem informasi berlangsung sesuai dengan rencana dan bahwa tujuan sistem informasi dicapai.
- Menurut NIST SP 800-53, kontrol sistem informasi adalah proses yang mengatur aktivitas sistem informasi dan memastikan bahwa aset penting dalam sistem informasi dilindungi.

- Menurut SANS Institute, kontrol sistem informasi adalah proses yang menjamin bahwa sistem informasi bekerja sesuai dengan tujuannya dan melindungi aset-aset penting, seperti data, informasi, dan infrastruktur teknologi informasi.

1.3.2 Konsep dasar audit sistem informasi

- Menurut ISO/IEC 27001:2013, audit sistem informasi adalah proses independen dan sistematis untuk memastikan bahwa sistem informasi bekerja sesuai dengan standar dan memenuhi tujuan bisnis.
- Menurut NIST SP 800-53, audit sistem informasi adalah proses yang mengevaluasi aktivitas dan proses sistem informasi untuk memastikan bahwa mereka sesuai dengan standar dan memenuhi tujuan bisnis.
- Menurut SANS Institute, audit sistem informasi adalah proses yang memeriksa sistem informasi untuk memastikan bahwa mereka bekerja dengan efektif dan efisien serta memenuhi standar dan tujuan bisnis.

1.4 Konsep Dasar Kontrol & Audit SI

Beberapa konsep dasar kontrol dan audit sistem informasi antara lain:

- Kebijakan dan Prosedur
  Organisasi harus memiliki kebijakan dan prosedur yang jelas dan terdokumentasi untuk mengatur penggunaan sistem informasi dan memastikan bahwa kontrol yang diperlukan telah diimplementasikan.
- Pengendalian Akses
  Organisasi harus memiliki kontrol akses yang kuat, termasuk autentikasi, otorisasi, dan manajemen hak

akses, untuk memastikan bahwa hanya pengguna yang sah yang dapat mengakses informasi.

- Manajemen Perubahan
  Organisasi harus memiliki proses yang terdokumentasi untuk mengelola perubahan pada sistem informasi, termasuk pengujian, evaluasi risiko, dan persetujuan.
- Pemantauan dan Pelaporan
  Organisasi harus memantau aktivitas sistem informasi secara berkala untuk mendeteksi insiden keamanan dan pelanggaran kebijakan, serta melaporkannya secara tepat waktu.
- Evaluasi Kinerja
  Audit SI harus dilakukan secara berkala untuk mengevaluasi efektivitas kontrol SI dan memastikan bahwa sistem informasi berfungsi sesuai dengan tujuan organisasi.
- Kepatuhan Regulasi
  Organisasi harus memastikan bahwa sistem informasi mereka mematuhi peraturan dan standar yang berlaku, seperti ISO 27001, HIPAA, PCI DSS, dan GDPR.
- Manajemen Risiko
  Organisasi harus mengevaluasi risiko yang terkait dengan sistem informasi dan mengimplementasikan kontrol yang sesuai untuk mengurangi risiko tersebut.

Dalam praktiknya, kontrol dan audit SI biasanya dilakukan oleh tim keamanan informasi atau auditor independen yang memiliki pengetahuan dan keterampilan khusus dalam bidang ini. Kontrol SI dan audit SI dapat membantu organisasi mengidentifikasi celah keamanan dan kelemahan dalam sistem informasi mereka, serta memberikan rekomendasi untuk meningkatkan keamanan dan kinerja sistem informasi secara keseluruhan (Santoso et al., 2023).

1.5 Cara Kerja Kontrol & Audit SI

Konsep dasar kontrol dan audit sistem informasi biasanya bekerja bersamaan untuk memastikan bahwa sistem informasi suatu organisasi aman, andal, dan efektif. Berikut adalah cara kerja masing-masing konsep dasar tersebut:

1.5.1 Kontrol Sistem Informasi

1. Identifikasi Risiko

   Organisasi harus mengidentifikasi risiko keamanan yang terkait dengan sistem informasi mereka. Risiko ini dapat berasal dari ancaman internal dan eksternal.
2. Penerapan Kontrol

   Setelah risiko diidentifikasi, organisasi harus menerapkan kontrol keamanan yang sesuai untuk mengurangi risiko tersebut. Contoh kontrol termasuk manajemen akses pengguna, enkripsi data, dan pemantauan aktivitas pengguna.
3. Evaluasi Efektivitas: Organisasi harus secara teratur mengevaluasi efektivitas kontrol keamanan mereka untuk memastikan bahwa mereka berfungsi dengan baik. Hal ini dapat dilakukan melalui audit internal atau eksternal.

1.5.2 Audit Sistem Informasi

1. Identifikasi Ruang Lingkup

   Sebelum memulai audit sistem informasi, auditor harus menentukan ruang lingkup audit dan tujuan audit. Ini akan membantu mereka menentukan area fokus dan sumber daya yang dibutuhkan.
2. Evaluasi Keamanan

   Auditor akan mengevaluasi kontrol keamanan organisasi untuk menentukan apakah mereka memadai untuk mengurangi risiko yang diidentifikasi.

3. Penilaian Efektivitas

   Auditor akan mengevaluasi efektivitas kontrol keamanan dengan menggunakan data dan informasi yang dikumpulkan selama audit. Mereka akan menilai kepatuhan organisasi terhadap persyaratan peraturan dan standar yang berlaku.
4. Pelaporan

   Setelah audit selesai, auditor akan menyusun laporan audit yang berisi temuan, rekomendasi, dan kesimpulan mereka. Laporan ini akan disampaikan kepada manajemen organisasi dan dapat digunakan untuk meningkatkan keamanan dan efektivitas sistem informasi mereka.

Kontrol sistem informasi dan audit sistem informasi saling melengkapi untuk memastikan bahwa sistem informasi suatu organisasi berfungsi dengan baik dan terlindungi dari ancaman keamanan. Melalui penerapan kontrol yang tepat dan audit yang teratur, organisasi dapat meminimalkan risiko keamanan dan memenuhi persyaratan peraturan dan standar yang berlaku (Muttaqin et al., 2023; Permana et al., 2023).

1.6 Faktor Kontrol & Audit SI

Terdapat beberapa faktor yang mempengaruhi konsep dasar kontrol dan audit sistem informasi. Berikut adalah beberapa faktor yang perlu dipertimbangkan dalam penerapan kontrol dan audit sistem informasi:

1. Ukuran dan Kompleksitas Organisasi

   Ukuran dan kompleksitas organisasi mempengaruhi jumlah dan jenis kontrol yang diperlukan. Semakin besar dan kompleks organisasi, semakin banyak kontrol yang diperlukan untuk melindungi data dan informasi penting mereka. Oleh karena itu, organisasi besar dan

kompleks mungkin perlu menerapkan kontrol yang lebih ketat dan melakukan audit yang lebih sering.

2. Jenis Data dan Informasi

   Jenis data dan informasi yang disimpan oleh organisasi juga mempengaruhi jenis kontrol yang diperlukan. Data sensitif seperti informasi keuangan dan data pribadi memerlukan kontrol yang lebih ketat daripada data yang tidak sensitif. Oleh karena itu, organisasi perlu mempertimbangkan jenis data dan informasi yang mereka miliki saat menerapkan kontrol sistem informasi dan melakukan audit.

3. Lingkungan Bisnis

   Lingkungan bisnis tempat organisasi beroperasi juga dapat mempengaruhi kontrol sistem informasi dan audit yang diperlukan. Misalnya, organisasi yang beroperasi di industri yang diatur ketat mungkin perlu memenuhi persyaratan regulasi yang lebih ketat daripada organisasi di industri yang tidak diatur.

4. Teknologi Informasi

   Teknologi informasi yang digunakan oleh organisasi juga mempengaruhi jenis kontrol dan audit yang diperlukan. Semakin kompleks dan maju teknologi informasi yang digunakan, semakin sulit untuk melindungi data dan informasi penting. Oleh karena itu, organisasi perlu mempertimbangkan teknologi informasi yang mereka gunakan saat menerapkan kontrol dan audit sistem informasi.

5. Kebutuhan Bisnis

   Kebutuhan bisnis organisasi juga mempengaruhi jenis kontrol dan audit yang diperlukan. Misalnya, organisasi yang memproses transaksi keuangan besar mungkin perlu menerapkan kontrol yang lebih ketat daripada organisasi yang tidak melakukan transaksi keuangan besar (Sugiyanto et al., 2022).

Secara keseluruhan, faktor-faktor ini perlu dipertimbangkan saat menerapkan konsep dasar kontrol dan audit sistem informasi. Dengan mempertimbangkan faktor-faktor ini, organisasi dapat memastikan bahwa kontrol dan audit sistem informasi yang diterapkan sesuai dengan kebutuhan bisnis dan dapat melindungi data dan informasi penting mereka.

1.7 Aplikasi Kontrol & Audit SI

Konsep dasar kontrol dan audit sistem informasi memiliki banyak aplikasi dalam organisasi dan bisnis modern. Beberapa contoh aplikasi konsep tersebut adalah:

1. Keamanan Data dan Informasi
   Organisasi dapat menggunakan kontrol keamanan informasi untuk melindungi data dan informasi penting mereka dari ancaman seperti pencurian, kerusakan, atau manipulasi yang tidak sah. Contoh kontrol keamanan termasuk manajemen akses pengguna, enkripsi data, dan pemantauan aktivitas pengguna.
2. Kepatuhan Regulasi dan Standar
   Organisasi harus mematuhi persyaratan regulasi dan standar yang berlaku terkait dengan keamanan informasi. Contoh regulasi termasuk GDPR dan HIPAA, sedangkan contoh standar termasuk ISO 27001 dan NIST. Kontrol sistem informasi dan audit sistem informasi dapat digunakan untuk memastikan bahwa organisasi mematuhi persyaratan tersebut.
3. Efisiensi dan Efektivitas Sistem Informasi
   Kontrol sistem informasi dapat membantu organisasi meningkatkan efisiensi dan efektivitas sistem informasi mereka. Contoh kontrol termasuk manajemen hak akses pengguna dan otomatisasi proses bisnis. Audit sistem informasi dapat membantu organisasi mengevaluasi

efektivitas sistem informasi mereka dan menemukan cara untuk meningkatkannya.

4. Manajemen Risiko

   Organisasi dapat menggunakan kontrol sistem informasi untuk mengurangi risiko keamanan mereka. Kontrol ini dapat membantu mencegah kehilangan data penting, pelanggaran data, dan serangan siber lainnya. Audit sistem informasi dapat membantu organisasi mengevaluasi risiko mereka dan menentukan apakah kontrol yang ada sudah memadai atau tidak.

5. Responsibilitas

   Kontrol sistem informasi dan audit sistem informasi dapat membantu organisasi memastikan bahwa mereka bertanggung jawab atas sistem informasi mereka. Kontrol dapat membantu mencegah kehilangan data penting atau akses yang tidak sah, sedangkan audit dapat membantu organisasi mengetahui siapa yang bertanggung jawab atas tindakan tertentu dalam sistem informasi.

Secara keseluruhan, konsep dasar kontrol dan audit sistem informasi sangat penting dalam menjaga keamanan, efisiensi, dan efektivitas sistem informasi organisasi. Dengan menerapkan kontrol yang tepat dan melakukan audit secara teratur, organisasi dapat meminimalkan risiko keamanan, mematuhi persyaratan peraturan dan standar yang berlaku, dan meningkatkan kinerja sistem informasi mereka.

DAFTAR PUSTAKA

Muttaqin, M., Yuswardi, Y., Warni, E., Wahyuddin, S., Bagaskara, R., Ambarwari, A., Ekowicaksono, I., Defiariany, D., Gustiana, Z. & Sinambela, M. (2023). *Konsep Dasar Kecerdasan Buatan*. Yayasan Kita Menulis.

Permana, A. A., Wahyuddin, S., Santoso, L. W., Wibowo, G. W. N., Wardhani, A. K., Wahidin, A. J., Yuliastuti, G. E. & Wijayanti, R. R. (2023). *Machine Learning*. Global Eksekutif Teknologi.

Santoso, L. W., Fauzan, R., Kristiana, R., Puspita, S., Nugroho, J. W. & Wahyuddin, S. (2023). *Manajemen Sains*. Global Eksekutif Teknologi.

Sihotang, J. I., Arni, S., Darsin, D., Ashari, I. F., Siregar, M. N. H., Fadhillah, Y., St Amina, H. U., Darwas, R., Wahyuddin, S. & Wirapraja, A. (2023). *Kontrol dan Audit TI*. Yayasan Kita Menulis.

Sugiyanto, G., Rahajeng, E., Rachmat, Z., Hendarsyah, D., Fadli, Z., Gemilang, F. A., Oktavera, R. & Kurnaedi, D. (2022). *Manajemen Sistem Informasi*. Global Eksekutif Teknologi.

Wikipedia. (2023). *Audit teknologi informasi - Wikipedia bahasa Indonesia, ensiklopedia bebas*. https://id.wikipedia.org/wiki/Audit_teknologi_informasi

BAB 2
PRINSIP-PRINSIP DASAR AUDIT SI

Untuk pembahasan pada bagian Bab 2, disini akan dijelaskan pengantar materi Audit (SI) sistem informasi dengan keseluruhan. Pada buku ini akan dijelaskan mengenai tujuan serta alasan di balik audit (TI) Teknologi Informasi dan tata kelola yang bisa mendorong setiap audit pada sector secara publik, baik itu dipemerintah maupun swasta. Dengan alasan apa penting dilakukan audit sistem, dari hal ini apakah karena organisai ataupun perusahaan yang merupakan terbaik sesuai dengan tujuan, visi dan misi dari organisai. Perlu untuk mendalami serta mempelajari dalam setiap aspek pada tahapan audit (SI) sistem informasi sampai mampu untuk mengidentifikasi standar-standar metodologi, dan juga kerangka kerja pada framework yang akan dipergunakan dalam melaksanakan audit TI.

2.1 Konsep audit SI atau TI

Pada tahap Audit sistem informasi(SI) yang merupakan salah satu Tindakan dalam pemeriksaan sistematis dan juga objektif terhadap suatu aspek dari setiap aspek diperusahaan. Audit pada (TI) teknologi informasi bisa saja dilakukan pemeriksaan untuk semua pada proses Teknologi Informasi, aset teknologi informasi juga memiliki kontrol sistem untuk semua level, karena setiap perusahaan dalam mengukur kinerja, perlu diketahui sudah sejauh mana perusahaan atau organisasi telah mematuhi standar yang sudah ditentukan. (Yudatama et al., 2022).

Sedangkan dalam Standar Internasional Pedoman Organisasi Standardisasi atau disebut ISO yang menyatakan bahwa

audit adalah istilah dari audit merupakan sebuah "proses yang independen, sistematis, dan memiliki dokumentasi dalam mendapatkan audit berupa bukti-bukti yang fakta dan juga harus dievaluasi yang objektif supaya bisa ditentukan sudah sejauh mana audit kriteria itu terpenuhi".

2.2 Dasar-dasar Audit TI (Teknologi Informasi)

Pada dasarnya dalam proses audit tentunya bisa membantu setiap organisasi untuk menilai, memahami dan juga meningkatkan penggunaan kontrol untuk melindungi pada setiap teknologi Informasi (TI) yang dapat mengukur kinerjanya, dan sudah tercapainya tujuan sesuai dengan keinginan organisasi tersebut. Dalam kegiatan untuk setiap audit system, yang membedakan untuk melakukan audit adalah catatan mengenai keuangan, proses bisnisnya, dan operasi umum, tetapi aset informasi teknologi perlu juga untuk diperhatikan secara efektif, supaya bisa beroperasi maksimal, bekerja baik dan benar, tepat pada fungsi yang sesuai pada standar dan juga peraturan yang ada. Maka dari itu adanya audit teknologi informasi (TI) sudah tentu sangat menolong pada setiap organisasi untuk tujuan yang dicapai. (Yudatama et al., 2022)

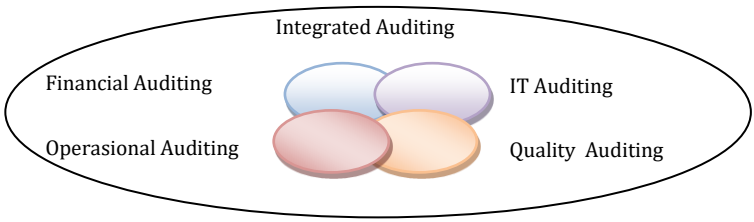
2.2.1Audit Sistem Informasi Atau Teknologi Informasi

Audit (SI) bisa juga disebut dengan (TI) yang merupakan adanya pendekatan pada audit yang formal untuk diperiksa, untuk melaksanakan segala tindakan evaluasi pada proses (TI) secara spesifik yang diukur sejauh mana kemampuan kinerja sistem dan sejauh mana kinerja aset untuk memastikan perencaan proses bisnis perusahaan maupun organisasi.

Menurut pendapat lainnya dari Stephen G, dalam audit teknologi Informasi (TI) yang dibahas adalah mengenai komponen atau juga hal-hal yang berkaitan dalam

mendukung audit, seperti keuangan, manajemen, operasional, serta jaminan, yang ada kaitannya dengan istilah manajemen resiko, dan kepatuhan.

Untuk melaksanakan pada setiap audit (SI) harus memiliki acuan berupa pedoman yang merupakan standar agar bisa menjadi suatu tujuan untuk setiap perusahaan, diantaranya berupa audit internal maupun eksternal yang memiliki tujuan yang berbeda-beda. Pada setiap audit (TI) juga memiliki peranan penting dalam organisasi selain audit financial, audit quality atau audit operasional perusahaan/organisasi, yang dilihat dengan cara konseptualnya, seperti gambar 1 dibawah ini:



Gambar 2.1. *Integrated Auditing* (IT)

Audit teknologi informasi tidak pernah lepas dari setip kegiatan, hal tersebut seperti gambar diatas. Audit bisa saja dilakukan dalam mengukur sudah sejauh mana praktik keuangan yang dilakukan audit dengan (TI), karena setiap audit keuangan harus diatasi kontrol dengan basik teknologi informasi (TI) serta kontribusinya secara efektif. Untuk Audit operasional bisa juga dilakukan dalam pemeriksaan yang terdapat efektivitas untuk setiap bisnis atau fungsi organisasi, efisiennya mendukung tujuan yang teepat pada sasaran organisasi. Dengan kualitas Audit diterapkan maka untuk pemenuhan aspek kegiatan bisnis operasional, manajemen teknologi informasi serta praktik pada keamanan informasi teknologi.

2.2.2 Apakah Audit Perlu Dilakukan

Setiap audit Teknologi Informasi perlu dilakukan agar bisa diukur untuk setiap efektivitas operasional bisnis baik itu proses perusahaan maupun organisasi, dengan mengukur serta menilai kesesuaian standar framework khususnya, yang menunjukkan bahwa kepatuhan terhadap kebijakan/standar bisa mengidentifikasi setiap peluang, perbaikan dalam tingkat kualitas produk, bisnis dan layanan.

Mengapa harus setiap perusahaan/organisasi melakukan audit sistem Informasi (SI) atau Teknologi Informasi, dikarenakan dengan adanya ketergantungan tersebut teknologi informasi merupakan salah satu karakteristik yang umum pada semua organisasi modern, khususnya di era saat ini adalah era diskrupsi 4.0 dan Society 5.0.

Segala sesuatu kegiatan yang dilaksanakan dalam audit, tentunya harus dilakukan supaya memperoleh berupa gambaran sistem informasi (teknologi informasi), dari gambaran itulah, apakah sudah sesuai dengan harapan tujuan dan sudah mencapai efektif yang tidak dari segi biaya ataupun investasi, tetapi harus menguji manfaat dari setiap teknologi informasi yang sudah sesuai dengan standar yang memadai serta sudah diakui perusahaan maupun organisasi.

Sudah banyak aspek untuk setiap audit Sistem Informasi yang bisa memberikan dasar yang akurat atau juga fundamental dalam memproses audit. Untuk pembuatan konsep dalam membantu pengembangan pemahaman tentang peran penting dimainkan oleh audit SI atau TI berupa hal kontribusi untuk pencapaian tujuan organisasi. Banyak sudah organisasi menjalankan audit SI atau TI dilakukan oleh beberapa auditor internal dan juga auditor eksternal perusahaan atau organisasi. Karena auditor teknologi informasi harus mampu memahami pentingnya pemahaman metodologi, standar, dan pendekatan terhadap *framework* yang sesuai sertifikasi dan

harus memiliki persyaratan pengalaman, tetapi harus bersinggungan dengan signifikan dengan manajemen TI pada praktik operasional lainnya secara profesional.

Sangat penting setiap organisasi memiliki sumber daya karyawan yang mempunyai kriteria sebagai auditor SI/TI. Dengan menerapkan performa sistem informasi secara efisien, tentunya harus ada pengukuran untuk kepastian sistem informasi atau teknologi informasi yang difungsikan secara baik dan juga benar dengan kualitas dan efektif tentu akan mendukung setiap bisnis organisasi yang bisa dipastikan adanya aset informasi bersumber daya informasi organisasi dan bisa dijamin secara memadai sesuai dengan toleransi risiko setiap organisasi.

Untuk Audit SI atau TI, difungsikan sebagai salah satu peran penting untuk mencapai strategi program organisasi yang luas memiliki resiko kepatuhan, kualitas, manajemen, dan keamanan informasi, serta tata kelola.

2.2.3 Personal Audit Teknologi Informasi

Dalam pengembangan setiap pemahaman yang punya kaitan dengan tujuan audit maka prakteknya dalam setiap kelompok yang non-auditor pada perusahaan/organisasi seperti administrasi, operasional, manajer dan juga program teknologi informasi serta proyek yang harus dilakukan sosliasasinya. Sumber Daya Manusia yang memilki kaitan dengan sistem Informasi maupun TI semuanya mungkin diminta untuk memberikan beberapa informasi kepada auditor eksternal maupun internal di setiap organisasi. Setiap organisasi pasti memiliki keterkaitan pada setiap informasi dan proses TI. Keterkaitan itu didasari dari keberhasilan organisasi, daya saing, dan kelangsungan hidup, yang membuat pada setiap kebutuhan dalam organisasi untuk dapat dipastikan mana yang benar dalam penerapan teknologi informasinya, karena dari dasar pada

setiap aplikasi SI atau TI yang digunakan. Untuk organisasi yang sudah fokus dalam melaksanakan audit internal perlu dilakukan audit harus disediakan auditor karena wajib harus mendukung setiap kegiatan audit internal dalam organisasi atau perusahaan.

2.2.4 Siapa Pelaksana Audit Teknologi Informasi?

Tahukah anda, siapakah orang yang akan melaksanakan atau melakukan audit Teknologi Informasi?, apakah internal atau eksternal? Terkadang dimunculkan sebuah pertanyaan siapa yang harus melaksanakan audit SI atau TI. Setiap melaksanakan kegiatan audit SI atau TI tentunya bisa saja yang melakukannya auditor internal dengan cara pengendalian dari sebuah organisasi tersebut berupa pengendalian internal dengan fungsi TI. Tetapi, bila perlu untuk pandangan yang professional bisa saja melakukannya terhadap pihak eksternal yang memiliki keterkaitan kinerja teknologi Infomasi dan bisa juga sistem informasi yang bisa dikatakan independent.

Auditor adalah suatu kepentingan dalam audit Teknologi Informasi. Maka, audit Teknologi Informasi internal harus punya kemampuan pengetahuan yang tinggi, keterampilan, dan memiliki kemampuan TI yang luas ahli dalam berprinsip, untuk praktek audit khususnya TI dan prosesnya.

Setiap organisasi/perusahaan sangat membutuhkan audit SI dan TI yang diperlukan untuk pengembangan dalam memiliki personil, pemahaman khusus tentang audit, memiliki resiko manjemen Teknologi Informasi dan memiliki personil yang berpengalaman dalam operasi Teknologi Informasi supaya bisa melakukan audit secara baik yang sesuai dengan ketentuan perusahaan maupun organisasi.

Untuk auditor SI bisa juga disebut teknologi informasi melakukan tugas dalam melakukan evaluasi dan juga penilaian untuk sistem informasi dan Teknologi informasi dari kesiapan Sistem Informasiatau TI yang memiliki dasar dengan kriteria-kriteria tertentu dalam pemilihan kerangka kerja yang sudah ditentukan dan dipergunakan pada setiap organisasi/perusahaan. Dalam setiap evaluasi harus dilakukan atas dasar hasil dari penilaian, dan juga pengujian oleh setiap auditor yang akan diberikan rekomendasi dalam melakukan perbaikan oleh semua pihak manajemen organisasi ataupun perusahaan.

2.2.5 Pemanfaatan Audit Internal dan Eksternal

Pelaksanaan audit sistem informasi atau TI, bisa dilakukan untuk semua auditor internal perusahaan. Dalam pemilihan auditor internal merupakan salah satu karyawan untuk setiap perusahaan/organisasi harus melakukan audit teknologi informasi internal berupa konsultan, dan spesialis outsourcing yang sudah ditetapkan oleh semua organisasi/perusahaan untuk dilakukannya audit internal atau bisa juga dilakukan oleh auditor eksternal yang menyewa untuk perusahaan/organisasi. Dalam kegiatan audit tersebut, untuk langkah prosesnya dan juga prosedurnya yang harus dilakukan auditor internal maupun eksternal tidak jauh beda yaitu, tetap harus memiliki kaidah yang sudah ditentukan sesuai dengan ketentuan setiap audit yang diperlukan.

Untuk tahap audit sistem dan TI internal, audit yang dilakukan dibawah bagian dari audit TI harus memiliki setiap organisasi dan biasanya memakai auditor internal salah satunya adalah karyawan perusahaan/organisasi yang akan melakukan pemeriksaan terhadap auditor TI internal. Sedangkan audit eksternal yang tentunya memiliki banyak kesamaan dengan internal biasanya dilakukan oleh auditor

untuk perusahaan, sepenuhnya terpisah dari setiap organisasi.

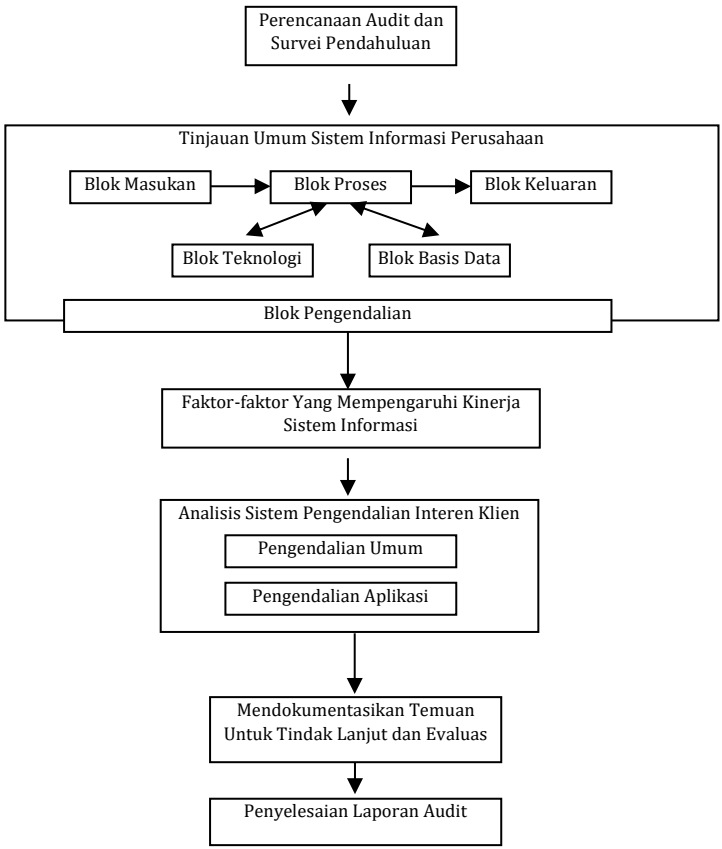
Peran-peran pada staf dalam mempersiapkan dalam dukungan audit eksternal, dijelaskan beberapa manfaat dan tantangan yang selalu terjadi untuk setiap organisasi. Beberapa perusahaan/organisasi sama sekali tidak memiliki tim auditor internal yang menggunakan beberapa pihak konsultan sebagai pelaksana auditor eksternal dengan kualitas yang sudah memiliki pengalaman, yaitu :

1. Penilaian pada setiap teknologi informasi ataupun sistem informasi yang bisa diorganisasikan dengan cara baik
2. Pengukuran sistem sudah bekerja yang efektif, dan efesien.
3. Penilaian yang dipastikan keamanannya untuk setiap aset dan informasi perusahaan.
4. Dipastikan SI/TI sudah memiliki kinerja yang baik dalam mendukung tercapainya tujuan misi organisasi

Untuk setiap kegiatan audit teknologi informasi atau SI tentunya ada manfaat lain yang harus diperlukan dalam setiap organisasi dengan pemeriksaaan secara keseluruhan serta rutin, dan memiliki hasil evaluasi, adanya suatu rekomendasi dalam internal organisasi dan bertanggung jawab atas resiko apabila ada kendala dikemudian hari.

2.2.6 Kerangka Kerja Audit Sistem Informasi

Dari kerangka kerja Audit sistem informasi dapat diuraikan beberapa tahap berdasarkan dari kerangka pikir manajemen, teknologi informasi dan juga pertimbangan untuk sistem ahli yang semuanya mengacu pada kerangka kerja untuk menghasilkan laporan audit sistem informasi.(Yudatama et al., 2022)



Gambar 2.2. Kerangka Kerja Audit Sistem Informasi (SI)

Dari setiap jenis audit biasanya dilakukan diberbagai organisasi, dengan cara auditor internal maupun eksternal yang memiliki pendekatan audit SI. Hal ini dijelaskan bahwa karakteristik dasar dari setiap audit teknologi informasi harus dilakukan sesuai dengan standar, framework maupun memiliki kerangka kerja, dengan adanya metodologi dan juga sumber panduan yang memberikan informasi praktik yang baik untuk melakukan audit.

Metodologi dengan *framework* untuk setiap audit sistem atau TI bisa dibedakan yaitu kegiatan audit TI yang fokus untuk dipilih sesuai dengan komponen SI yang

berbeda, tata kelola, layanan teknologi informasi atau opersionalnya. Dengan kategori teknis atau non-teknis yang bisa digambarkan dari berbagai teknologi dengan arsitekturnya yang juga aspek program dan proyek TI menjadi ruang lingkup audit TI. Fokus pada suatu kegiatan termasuk merupakan proses, yang memiliki rencana audit, dan dikumpulkan untuk peninjauan bukti, berupa analisis dan laporannya, menanggapi adanya temuan dengan mengambil beberapa tindakan korektif yang bisa memanfaatkan peluang dalam melakukan perbaikan adalah salah satu bagian dari setiap *framework* untuk bisa melakukan audit.

Dari semua eksternal maupun Internal yang sudah memilih salah satu dari framework dengan cara memilih mengadopsi metodologi dalam kerangka kerja framework yang baik, terkadang sering dipergunakan sebagai petunjuk untuk standar melaksanakan audit untuk dapat dikembangkan dalam penilaian sebagai salah satu alternatif untuk pengembangkan kerangka kerja sesuai dengan kesepakatan organisasi. Dalam penggunaan framework untuk disajikan dalam kegiatan atau laporan audit biasanya menggunakan framework yang umum, yang terkenal dan mengadopsi metodologi sebagai kerangka kerjanya, termasuk yang fokus kepada yang eksplisit dalam proses audit SI maupun TI dengan tujuan untuk mendukung tata kelola, keamanan informasi, dan nilai-nilai kontrol.

Dari penjelasan diatas, ada beberapa framework kerangka kerja yang digunakan untuk melaksanakan kegiatan audit sistem atau audit Teknologi Informasi diantaranya:

1. *Framework Control Objectives For Information and Related Technology* adalah singkatan dari Cobit 5, yang merupakan framework atau kerangka kerja standar manajemen teknologi informasi yang sudah dikeluarkan oleh IT Governance Institute-ISACA

2. (*Committee of sponsoring Organisations of the Treadway Commission*) COSO, Framework yang meiliki fokus untuk membangun control dengan mencapai tujuan perusahaan yang mengurangi resiko adanya kategori level dalam suatu organisasi, financial maupun kepatuhan.
3. Framework audit keamanan sistem informasi (SI) yang dapat menggunakan Octave Allegro, NISP SP, ISO 27005.

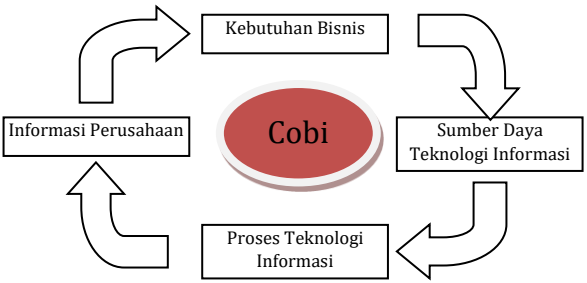
2.2.7 Prinsip-prinsip Cobit

Berikut ini beberapa prinsip-prinsip Cobit 5, diantaranya :

1. *Meeting stakeholders needs* atau memenuhi sebuah keinginan dari pemangku kepentingan. Perusahaan harus menciptakan nilai-nilai bagi stakeholder yang mempertahankan semua keseimbangan antara realisasi manfaat dan mengoptimalkan resiko terhadap penggunaan sumber daya.
2. *Covering the enterprise end-to-end atau mencakup Enterprise End-to-end* yang diintegrasikan terhadap tata kelola perusahaan TI, dalam tata kelola perusahaan, yang mencakup kepada semua fungsi sesrta proses yang ada pada perusahaan dan menganggap semua tata kelola dan manajemen TI untuk perusahaan.
3. *Applying a single integrated framework atau menerapkan single framework* yang terpadu yang saling berkaitan dengan IT standar dan juga praktek terbaik, masing-masingnya harus memberikan bimbingan pada subset dari semua kegiatan TI.(Ekowansyah et al., 2017).

Control Objectives for Information and Related Technology (COBIT) yang merupakan suatu framework panduan audit teknologi informasi yang difungsikan untuk menjembatani

nilai GAP terdapat kebutuhan serta pelaksanaan pemenuhan dalam organisasi maupun instansi, berikut ini gambar prinsip dasar cobit (Mulyawan et al., 2020).



Gambar 2.3. Prinsip Dasar Cobit

2.3 Ringkasan

Dari berbagai aspek perlu untuk fokus dalam audit Sistem Informasi dan juga peran audit Sistem Informasi (SI) yang lebih luas. sedangkan proses Sistem Informasi (SI) harus dilakukan secara detail untuk setiap organisasi dan auditor, sebagian besar standar, kerangka kerja, metodologi, yang bisa dijangkau dengan metode PDCA atau plando check act, dengan tujuan perbaikan. Walaupun proses auditnya mirip diseluruh organisasi maupun industri, tapi ada beberapa macam metodologi dan kerangka framework terhadap kontrol proses yang ada dan bisa diterapkan di setiap organisasi dan perlu disesuaikan oleh auditor internal maupun eksternal sesuai kebutuhan pada manajemen organisasi. Dalam pemahaman audit SI dan TI yang harus memberikan gambaran umum terhadap tujuan audit SI/TI dan alasan organisasi, yang digambarkan berupa subjek dan juga fokus yang berbeda untuk beberapa jenis organisasi tentunya harus patuh pada audit SI/TI yang harus diperlukan untuk sosialisasi dan adanya pelatihan individu di setiap organisasi agar dapat bekerjasama selama proses pelaksanaan audit SI/TI yang sudah berlangsung.

DAFTAR PUSTAKA

Ekowansyah, E., Chrisnanto, Y. H., & Sabrina, N. (2017). Audit Sistem Informasi Akademik Menggunakan COBIT 5 di Universitas Jenderal Achmad Yani. *Prosiding Seminar Nasional Komputer Dan Informatika (SENASKI)*, *2017*, 201–206.

Mulyawan, M. D., Hartati, R. S., & Divayana, Y. (2020). Audit Sistem Informasi Kesiman Kertalangu (SIKEKAL) Menggunakan COBIT 4.1. *Majalah Ilmiah Teknologi Elektro*, *19*(2), 139. https://doi.org/10.24843/mite.2020.v19i02.p03

Yudatama, U., Gustee, K., Komalasari, R., Purabaya, R. H., Solihin, H. H., Herjuna, S. A. S., Moedjahedy, J. H., Sastradipraja, C. K., Muslih, M., Munawar, Z., Cholil, W., Arista, A., Turi, L. O., & Akbar, Z. (2022). *Audit Sistem Informasi: Teori, Framework Dan Studi Kasus Menggunakan Framework* (Issue January). https://play.google.com/books/reader?id=nKJ9EAAAQBAJ

BAB 3
PROSES AUDIT SISTEM INFORMASI

3.1 Pendahuluan

Secara umum, proses audit sistem informasi dapat dilakukan dalam beberapa tahap, antara lain: (Wahyudi, 2018)

1. Perencanaan Audit

   Pada tahap ini, auditor melakukan perencanaan audit dengan menentukan tujuan dan ruang lingkup audit, memahami lingkungan bisnis, serta mengevaluasi risiko-risiko yang mungkin terjadi dalam sistem informasi organisasi.
2. Evaluasi Sistem Pengendalian Internal

   Tahap ini melibatkan evaluasi terhadap sistem pengendalian internal yang ada dalam sistem informasi organisasi, seperti prosedur otomatisasi, pemisahan tugas, dan pengendalian akses. Auditor juga melakukan pemahaman terhadap proses bisnis dan mengidentifikasi area-area yang rentan terhadap kesalahan atau penipuan.
3. Pengumpulan Bukti

   Pada tahap ini, auditor mengumpulkan bukti-bukti yang mendukung temuan mereka selama proses audit, seperti dokumen sistem, log aktivitas, dan catatan transaksi. Bukti-bukti ini akan digunakan untuk mengevaluasi efektivitas dan efisiensi sistem informasi, serta untuk menilai kepatuhan terhadap standar dan regulasi yang berlaku.

4. Analisis Bukti dan Penilaian

   Tahap ini melibatkan analisis bukti-bukti yang telah dikumpulkan oleh auditor dan penilaian terhadap tingkat risiko yang teridentifikasi selama proses audit. Auditor juga akan mengevaluasi kepatuhan terhadap standar dan regulasi yang berlaku, serta melakukan analisis terhadap efektivitas dan efisiensi sistem informasi.
5. Pelaporan Temuan dan Rekomendasi

   Pada tahap ini, auditor menyusun laporan audit yang berisi temuan dan rekomendasi untuk perbaikan sistem informasi organisasi. Laporan ini akan memberikan insight dan rekomendasi bagi organisasi untuk meningkatkan efektivitas dan efisiensi sistem informasi mereka serta memastikan kepatuhan dengan standar dan regulasi yang berlaku.
6. Tindak Lanjut

   Tahap terakhir adalah tindak lanjut atas temuan dan rekomendasi yang disampaikan oleh auditor. Organisasi harus menindaklanjuti temuan dan rekomendasi tersebut untuk memastikan sistem informasi mereka lebih efektif, efisien dan aman.

Setelah tahap tindak lanjut, auditor juga dapat melakukan evaluasi untuk memastikan bahwa rekomendasi dan tindakan perbaikan yang telah diambil sudah sesuai dengan yang disarankan dalam laporan audit. Evaluasi ini dilakukan untuk memastikan bahwa perbaikan sistem informasi sudah efektif dan efisien, serta sudah mematuhi standar dan regulasi yang berlaku.

Selama proses audit sistem informasi, auditor juga perlu memastikan bahwa mereka beroperasi secara independen dan objektif. Auditor harus memiliki pengetahuan yang cukup tentang sistem informasi, serta standar dan regulasi yang berlaku untuk memastikan audit

dilakukan dengan benar. Selain itu, auditor juga harus berkomunikasi dengan baik dengan pemangku kepentingan organisasi untuk memastikan bahwa semua pihak memahami hasil audit dan tindakan yang harus diambil untuk memperbaiki sistem informasi.

Secara keseluruhan, proses audit sistem informasi adalah suatu proses yang penting untuk memastikan bahwa sistem informasi organisasi berjalan dengan baik, efektif, dan aman. Dengan melakukan audit sistem informasi secara teratur, organisasi dapat memastikan bahwa mereka memenuhi standar keamanan dan regulasi yang berlaku, serta mampu mengurangi risiko terjadinya kebocoran data atau pelanggaran keamanan lainnya.

Selain itu, audit sistem informasi juga membantu organisasi untuk meningkatkan efisiensi dan efektivitas sistem informasi mereka, sehingga mereka dapat memberikan layanan yang lebih baik kepada pelanggan dan memperoleh keuntungan yang lebih besar. Audit sistem informasi juga membantu organisasi untuk memperbaiki kelemahan-kelemahan dalam sistem informasi mereka dan mencegah terjadinya kerugian finansial atau reputasi.

Pada akhirnya, audit sistem informasi adalah suatu proses yang penting untuk memastikan bahwa sistem informasi organisasi berjalan dengan baik dan sesuai dengan standar dan regulasi yang berlaku. Dengan melakukan audit sistem informasi secara teratur, organisasi dapat memastikan bahwa mereka dapat meminimalkan risiko, meningkatkan efisiensi, dan memperbaiki sistem informasi mereka secara terus-menerus. Hal ini akan membantu organisasi untuk tetap bersaing dan bertahan dalam dunia bisnis yang semakin kompetitif dan terus berkembang.

Selain itu, audit sistem informasi juga membantu organisasi untuk memperbaiki kualitas data dan informasi mereka, sehingga mereka dapat mengambil keputusan yang lebih baik dan lebih akurat. Dengan memiliki sistem

informasi yang berkualitas, organisasi dapat meningkatkan efektivitas operasional mereka, mengurangi biaya, dan meningkatkan kepuasan pelanggan.

Namun, audit sistem informasi juga memiliki beberapa tantangan. Tantangan pertama adalah ketergantungan pada teknologi. Sistem informasi yang kompleks dan terintegrasi membuat organisasi semakin bergantung pada teknologi. Ketergantungan ini meningkatkan risiko kegagalan sistem dan serangan siber yang dapat merusak operasi bisnis organisasi. Oleh karena itu, auditor sistem informasi perlu memperhatikan faktor-faktor ini saat melakukan audit.

Tantangan kedua adalah perubahan teknologi yang cepat. Perkembangan teknologi yang cepat mengubah cara organisasi bekerja dan memerlukan adaptasi sistem informasi yang cepat. Namun, adaptasi yang cepat juga meningkatkan risiko kegagalan sistem dan pelanggaran keamanan data. Oleh karena itu, auditor sistem informasi perlu memperhatikan perubahan teknologi dan memastikan bahwa organisasi telah mengikuti perkembangan teknologi dan mengambil langkah-langkah yang tepat untuk mengatasi risiko yang terkait.

Dalam menghadapi tantangan ini, auditor sistem informasi perlu memahami dan mengikuti perkembangan teknologi dan tren terbaru dalam bidang sistem informasi. Auditor juga perlu terus belajar dan meningkatkan pengetahuan mereka tentang sistem informasi dan standar dan regulasi yang berlaku, sehingga mereka dapat memberikan saran yang lebih baik dan akurat kepada organisasi.

Selain tantangan teknologi, audit sistem informasi juga dapat menghadapi tantangan lain seperti kurangnya dukungan manajemen, keterbatasan sumber daya, dan kurangnya kesadaran dan pemahaman tentang pentingnya audit sistem informasi. Oleh karena itu, auditor sistem

informasi perlu mengkomunikasikan nilai dari audit sistem informasi dan manfaat yang dapat diperoleh oleh organisasi.

Auditor sistem informasi juga perlu bekerja sama dengan tim manajemen organisasi dan pemangku kepentingan lainnya, seperti tim keamanan informasi dan tim TI, untuk memastikan bahwa audit sistem informasi dilakukan dengan efektif dan efisien. Auditor juga perlu memahami strategi dan tujuan bisnis organisasi dan memastikan bahwa sistem informasi mendukung pencapaian tujuan bisnis tersebut.

Pada akhirnya, audit sistem informasi adalah suatu proses yang penting untuk memastikan bahwa sistem informasi organisasi berjalan dengan baik dan memenuhi standar dan regulasi yang berlaku. Dengan melakukan audit sistem informasi secara teratur, organisasi dapat meminimalkan risiko, meningkatkan efisiensi, dan memperbaiki sistem informasi mereka secara terus-menerus. Oleh karena itu, auditor sistem informasi memiliki peran yang penting dalam membantu organisasi memastikan keamanan, kualitas, dan efektivitas sistem informasi mereka.

3.2 Manfaat Proses Audit Sistem Informasi

Audit sistem informasi memiliki banyak manfaat bagi organisasi, di antaranya:

1. Meminimalkan risiko: Audit sistem informasi membantu organisasi mengidentifikasi dan mengevaluasi risiko yang terkait dengan sistem informasi mereka, termasuk risiko keamanan, privasi, dan kegagalan sistem. Dengan mengetahui risiko yang ada, organisasi dapat mengambil langkah-langkah untuk meminimalkan risiko dan mencegah terjadinya kerugian finansial atau reputasi.

2. Meningkatkan efisiensi: Audit sistem informasi membantu organisasi mengidentifikasi kelemahan dalam sistem informasi mereka dan memberikan rekomendasi untuk meningkatkan efisiensi dan efektivitas sistem. Dengan meningkatkan efisiensi, organisasi dapat mengurangi biaya dan meningkatkan produktivitas.
3. Memastikan kepatuhan: Audit sistem informasi membantu organisasi memastikan bahwa sistem informasi mereka memenuhi standar dan regulasi yang berlaku, termasuk peraturan privasi dan keamanan data. Dengan memastikan kepatuhan, organisasi dapat menghindari sanksi dan penalti, serta mempertahankan reputasi yang baik.
4. Meningkatkan kualitas data: Audit sistem informasi membantu organisasi memastikan bahwa data dan informasi yang digunakan dalam sistem informasi mereka berkualitas dan akurat. Dengan meningkatkan kualitas data, organisasi dapat mengambil keputusan yang lebih baik dan lebih akurat.
5. Meningkatkan kepercayaan: Audit sistem informasi membantu meningkatkan kepercayaan dari pihak luar, seperti pelanggan, investor, dan regulator, terhadap sistem informasi organisasi. Dengan meningkatkan kepercayaan, organisasi dapat memperkuat posisi mereka di pasar dan mendapatkan keuntungan yang lebih besar.
6. Meningkatkan pengawasan dan kontrol: Audit sistem informasi membantu organisasi meningkatkan pengawasan dan kontrol terhadap sistem informasi mereka. Dengan meningkatkan pengawasan dan kontrol, organisasi dapat mengurangi risiko

penyalahgunaan atau kehilangan data dan informasi yang penting.

7. Meningkatkan transparansi: Audit sistem informasi dapat meningkatkan transparansi dalam pengelolaan sistem informasi organisasi. Hal ini membantu memastikan bahwa semua pihak terlibat dalam pengelolaan sistem informasi memiliki pemahaman yang sama tentang tujuan dan prosedur pengelolaan sistem informasi. Dengan meningkatkan transparansi, organisasi dapat mengurangi risiko perselisihan dan meningkatkan kepercayaan stakeholder.
8. Meningkatkan pencegahan dan deteksi kejahatan siber: Audit sistem informasi dapat membantu dalam pencegahan dan deteksi kejahatan siber yang mungkin terjadi pada sistem informasi organisasi. Dalam melakukan audit sistem informasi, auditor dapat mengevaluasi tingkat keamanan sistem informasi dan memberikan rekomendasi untuk meningkatkan keamanannya. Dengan meningkatkan keamanan sistem informasi, organisasi dapat mencegah serangan kejahatan siber dan kerugian yang mungkin timbul.
9. Meningkatkan efektivitas pengelolaan TI: Audit sistem informasi dapat membantu dalam meningkatkan efektivitas pengelolaan TI organisasi. Dalam melakukan audit sistem informasi, auditor dapat mengevaluasi kualitas, penggunaan, dan manajemen TI yang ada di organisasi. Dengan demikian, organisasi dapat meningkatkan efektivitas pengelolaan TI mereka dan mengurangi biaya operasional.
10. Memberikan saran dan rekomendasi: Audit sistem informasi memberikan saran dan rekomendasi yang penting bagi organisasi untuk meningkatkan sistem informasi mereka. Dalam melakukan audit sistem

informasi, auditor dapat menemukan kelemahan dan masalah dalam sistem informasi organisasi, dan memberikan rekomendasi untuk mengatasi masalah tersebut. Dengan menerima saran dan rekomendasi dari auditor, organisasi dapat memperbaiki sistem informasi mereka dan meningkatkan efisiensi dan efektivitas operasional mereka.

11. Meningkatkan kepatuhan: Audit sistem informasi juga membantu organisasi memastikan bahwa mereka mematuhi semua peraturan, kebijakan, dan standar keamanan yang berlaku. Auditor dapat mengevaluasi sistem informasi organisasi untuk memastikan bahwa mereka memenuhi persyaratan kepatuhan, seperti GDPR, HIPAA, atau standar keamanan ISO. Dengan memastikan kepatuhan, organisasi dapat mengurangi risiko denda atau tuntutan hukum, serta mempertahankan reputasi yang baik.
12. Meningkatkan pengawasan dan kontrol: Audit sistem informasi juga dapat membantu meningkatkan pengawasan dan kontrol atas sistem informasi organisasi. Auditor dapat mengevaluasi proses pengawasan dan kontrol yang ada dalam organisasi dan memberikan rekomendasi untuk meningkatkan efektivitasnya. Dengan meningkatkan pengawasan dan kontrol, organisasi dapat mengurangi risiko keamanan dan kehilangan data penting, serta meningkatkan kemampuan mereka untuk mendeteksi dan menanggapi ancaman keamanan.
13. Meningkatkan kualitas data: Audit sistem informasi juga dapat membantu meningkatkan kualitas data dalam organisasi. Auditor dapat mengevaluasi proses pengolahan data, termasuk keakuratan, keberlanjutan, integritas, dan keamanan data. Dengan meningkatkan

kualitas data, organisasi dapat mengurangi risiko keputusan bisnis yang salah, meningkatkan efisiensi operasional, dan memastikan kepatuhan.

14. Memperkuat sistem pengendalian internal: Audit sistem informasi juga dapat membantu organisasi memperkuat sistem pengendalian internal mereka. Auditor dapat mengevaluasi kekuatan dan kelemahan dalam sistem pengendalian internal organisasi dan memberikan rekomendasi untuk meningkatkannya. Dengan memperkuat sistem pengendalian internal, organisasi dapat mengurangi risiko penipuan, kesalahan, dan kehilangan data, serta meningkatkan efisiensi dan efektivitas operasional mereka.
15. Meningkatkan kesiapan menghadapi inspeksi atau audit eksternal: Terakhir, audit sistem informasi juga dapat membantu organisasi meningkatkan kesiapan mereka dalam menghadapi inspeksi atau audit eksternal. Dalam melakukan audit sistem informasi, auditor dapat mengevaluasi tingkat kesiapan organisasi dalam menghadapi inspeksi atau audit eksternal, dan memberikan rekomendasi untuk meningkatkannya. Dengan meningkatkan kesiapan, organisasi dapat mengurangi risiko kehilangan waktu, biaya, dan reputasi akibat inspeksi atau audit yang tidak memuaskan.

Secara keseluruhan, audit sistem informasi adalah proses penting bagi organisasi untuk memastikan bahwa sistem informasi mereka berjalan dengan baik dan memenuhi standar yang berlaku. Dalam melakukan audit sistem informasi, auditor dapat memberikan banyak manfaat bagi organisasi, termasuk meminimalkan risiko, meningkatkan efisiensi, memastikan kepatuhan, meningkatkan kualitas data, meningkatkan kepercayaan,

meningkatkan pengawasan dan kontrol, meningkatkan transparansi, mencegah dan mendeteksi kejahatan siber, meningkatkan efektivitas pengelolaan TI, serta memberikan saran dan rekomendasi bagi organisasi. (Achmad solechan, 2021)

3.3 Hal Penting Dalam Proses Audit Sistem Informasi

Berikut adalah beberapa hal yang harus diperhatikan untuk memulai proses audit sistem informasi:

1. Tujuan audit: Tentukan tujuan audit sistem informasi yang jelas dan terukur, serta sasaran audit yang harus dicapai.
2. Ruang lingkup audit: Tentukan ruang lingkup audit sistem informasi, yang mencakup area atau sistem yang akan diaudit.
3. Tim auditor: Tentukan tim auditor yang akan melakukan audit sistem informasi, yang terdiri dari auditor internal atau eksternal yang berkualitas dan berpengalaman.
4. Rencana audit: Buat rencana audit yang terperinci dan terstruktur, yang mencakup semua tahap audit, termasuk identifikasi risiko, penentuan strategi audit, pengumpulan bukti, analisis bukti, serta penyusunan laporan audit.
5. Identifikasi risiko: Lakukan identifikasi risiko pada sistem informasi organisasi dan tetapkan prioritas audit berdasarkan risiko yang telah diidentifikasi.
6. Pengumpulan bukti: Kumpulkan bukti audit yang cukup dan relevan, termasuk dokumen, catatan, dan wawancara dengan pihak terkait.
7. Analisis bukti: Lakukan analisis bukti audit untuk mengevaluasi efektivitas sistem informasi organisasi dalam mencapai tujuan bisnis dan kepatuhan.

8. Pelaporan: Susun laporan audit yang lengkap, jelas, dan mudah dimengerti, serta sertakan rekomendasi perbaikan yang dapat dilakukan oleh organisasi.
9. Tindak lanjut: Lakukan tindak lanjut atas rekomendasi audit untuk memastikan bahwa tindakan yang diperlukan telah dilakukan dan sistem informasi telah ditingkatkan.
10. Pemantauan: Lakukan pemantauan terhadap sistem informasi organisasi secara teratur untuk memastikan bahwa tindakan perbaikan yang diperlukan telah diambil dan sistem informasi terus berjalan dengan baik.
11. Kepatuhan: Selalu pastikan bahwa sistem informasi organisasi mematuhi semua kebijakan dan regulasi yang berlaku.
12. Manajemen risiko: Lakukan manajemen risiko secara teratur pada sistem informasi organisasi untuk mengidentifikasi, mengevaluasi, dan mengatasi risiko-risiko yang mungkin timbul.
13. Penyusunan strategi: Susun strategi yang tepat untuk meningkatkan sistem informasi organisasi dan pastikan bahwa strategi tersebut sejalan dengan tujuan bisnis dan kebutuhan pengguna.
14. Komunikasi: Pastikan bahwa komunikasi yang efektif dilakukan di antara tim auditor dan manajemen organisasi untuk memastikan bahwa audit sistem informasi berjalan dengan lancar dan semua masalah dapat diatasi dengan tepat waktu.
15. Pemantauan audit: Lakukan pemantauan terhadap seluruh proses audit sistem informasi, mulai dari perencanaan hingga pelaporan, untuk memastikan bahwa audit dilakukan secara profesional dan sesuai dengan standar audit yang berlaku.

Dalam melakukan audit sistem informasi, perlu diingat bahwa proses audit harus dilakukan secara sistematis dan terstruktur, serta memperhatikan semua aspek yang terkait dengan sistem informasi organisasi. Selain itu, auditor juga harus memiliki pengetahuan dan keterampilan yang memadai dalam bidang audit sistem informasi, sehingga dapat melakukan audit dengan efektif dan efisien.

3.4 Perencanaan Audit

Perencanaan audit adalah tahap awal dalam proses audit sistem informasi dan merupakan langkah penting dalam memastikan bahwa audit berjalan dengan sukses dan sesuai dengan tujuan yang ditetapkan. Berikut adalah penjelasan lebih terinci tentang perencanaan audit sistem informasi:

1. Identifikasi tujuan audit: Pada tahap ini, auditor harus menentukan tujuan audit sistem informasi secara jelas dan terukur, serta sasaran audit yang harus dicapai. Tujuan audit harus sejalan dengan tujuan bisnis organisasi, dan harus spesifik dan terukur, sehingga memudahkan untuk mengevaluasi keberhasilan audit.
2. Identifikasi ruang lingkup audit: Auditor harus menentukan ruang lingkup audit sistem informasi, yang mencakup area atau sistem yang akan diaudit. Hal ini perlu dilakukan untuk memastikan bahwa semua aspek yang terkait dengan sistem informasi organisasi telah dicakup dalam audit.
3. Identifikasi risiko: Auditor harus melakukan identifikasi risiko pada sistem informasi organisasi dan menentukan prioritas audit berdasarkan risiko yang telah diidentifikasi. Hal ini penting dilakukan untuk memastikan bahwa audit difokuskan pada risiko-risiko yang memiliki dampak besar terhadap sistem informasi organisasi.

4. Penentuan strategi audit: Auditor harus menentukan strategi audit yang tepat berdasarkan tujuan, ruang lingkup, dan risiko audit. Strategi audit harus mencakup metodologi audit yang digunakan, sumber daya yang diperlukan, dan jadwal audit yang harus dipatuhi.
5. Tim auditor: Auditor harus menentukan tim auditor yang akan melakukan audit sistem informasi, yang terdiri dari auditor internal atau eksternal yang berkualitas dan berpengalaman. Tim auditor harus memiliki pengetahuan dan keterampilan yang memadai dalam bidang audit sistem informasi.
6. Sumber daya: Auditor harus menentukan sumber daya yang dibutuhkan untuk melaksanakan audit, seperti anggaran, teknologi, dan personil. Hal ini penting dilakukan untuk memastikan bahwa audit dapat dilakukan secara efektif dan efisien.
7. Rencana audit: Auditor harus membuat rencana audit yang terperinci dan terstruktur, yang mencakup semua tahap audit, termasuk identifikasi risiko, penentuan strategi audit, pengumpulan bukti, analisis bukti, serta penyusunan laporan audit.
8. Penentuan jadwal audit: Auditor harus menentukan jadwal audit yang sesuai dengan kebutuhan organisasi dan jadwal kerja tim auditor. Hal ini harus memperhitungkan waktu yang diperlukan untuk mengumpulkan bukti, menganalisis bukti, dan menyiapkan laporan audit.
9. Komunikasi dengan pihak terkait: Auditor harus melakukan komunikasi yang efektif dengan pihak terkait dalam organisasi, seperti manajemen senior, tim IT, dan staf operasional. Hal ini penting dilakukan untuk memastikan bahwa audit dilakukan dengan transparan,

dan untuk mendapatkan dukungan dari semua pihak terkait.

10. Pengembangan checklist audit: Auditor harus mengembangkan checklist audit yang mencakup semua area yang akan diaudit, serta standar dan prosedur yang harus dipatuhi. Checklist audit dapat membantu auditor dalam mengumpulkan bukti dan menganalisis kelemahan dalam sistem informasi organisasi.
11. Penilaian kualitas data: Auditor harus menilai kualitas data yang akan digunakan dalam audit sistem informasi, termasuk data yang tersimpan dalam sistem informasi organisasi dan data yang dihasilkan oleh proses bisnis. Hal ini penting dilakukan untuk memastikan bahwa bukti yang diperoleh selama audit dapat diandalkan.
12. Penentuan metode pengumpulan bukti: Auditor harus menentukan metode yang tepat untuk mengumpulkan bukti dalam audit sistem informasi, seperti observasi, wawancara, dan pengujian. Metode pengumpulan bukti yang dipilih harus sesuai dengan tujuan dan ruang lingkup audit, serta harus menghasilkan bukti yang cukup dan relevan.

Dalam melakukan perencanaan audit sistem informasi, auditor harus memastikan bahwa semua aspek yang terkait dengan sistem informasi organisasi telah dicakup dan bahwa audit dilakukan dengan menggunakan metodologi audit yang tepat. Perencanaan audit yang baik akan memastikan bahwa audit sistem informasi berjalan dengan efektif dan efisien, dan dapat menghasilkan laporan audit yang akurat dan bermanfaat bagi organisasi.

Perencanaan audit sistem informasi merupakan tahap awal yang penting dalam proses audit. Dengan melakukan perencanaan yang matang dan terstruktur, auditor dapat

memastikan bahwa audit sistem informasi dilakukan dengan efektif dan efisien, serta menghasilkan laporan audit yang bermanfaat bagi organisasi.

3.5 Evaluasi Sistem Pengendalian Internal

1. Evaluasi sistem pengendalian internal merupakan salah satu tahap penting dalam proses audit sistem informasi. Pada tahap ini, auditor melakukan penilaian terhadap efektivitas sistem pengendalian internal yang diterapkan dalam organisasi untuk melindungi aset, memastikan keakuratan informasi, dan menjaga kepatuhan terhadap peraturan dan kebijakan yang berlaku. Berikut adalah beberapa hal yang perlu diperhatikan oleh auditor dalam melakukan evaluasi sistem pengendalian internal:
2. Memahami kebijakan dan prosedur: Auditor harus memahami kebijakan dan prosedur yang diterapkan dalam organisasi, termasuk kebijakan pengendalian internal. Hal ini penting dilakukan untuk memastikan bahwa auditor memiliki pemahaman yang memadai tentang sistem pengendalian internal yang diterapkan.
3. Menilai desain sistem pengendalian internal: Auditor harus menilai desain sistem pengendalian internal dalam organisasi. Hal ini mencakup penilaian terhadap kecukupan dan kesesuaian kontrol yang diterapkan dengan risiko yang dihadapi oleh organisasi.
4. Melakukan pengujian pengendalian internal: Auditor harus melakukan pengujian pengendalian internal untuk menilai efektivitas kontrol yang diterapkan dalam organisasi. Pengujian ini dapat dilakukan dengan melakukan pengamatan langsung, pengujian dokumen, atau dengan melakukan simulasi.

5. Mengevaluasi kepatuhan terhadap kebijakan dan peraturan: Auditor harus mengevaluasi kepatuhan terhadap kebijakan dan peraturan yang berlaku dalam organisasi. Hal ini mencakup penilaian terhadap pematuhan terhadap kebijakan dan peraturan yang terkait dengan aset, keakuratan informasi, dan pengendalian proses bisnis.
6. Menganalisis temuan pengendalian internal: Setelah melakukan evaluasi, auditor harus menganalisis temuan pengendalian internal yang ditemukan. Auditor harus menilai apakah pengendalian internal yang diterapkan efektif dalam melindungi aset, memastikan keakuratan informasi, dan menjaga kepatuhan terhadap peraturan dan kebijakan yang berlaku.
7. Melakukan pengujian substansi: Auditor harus melakukan pengujian substansi terhadap transaksi dan kejadian dalam organisasi untuk mengevaluasi efektivitas pengendalian internal yang diterapkan. Hal ini mencakup penilaian terhadap integritas data, keaslian transaksi, serta ketepatan dan kelengkapan catatan transaksi.
8. Menilai dampak temuan pengendalian internal: Auditor harus menilai dampak temuan pengendalian internal terhadap laporan keuangan, kinerja organisasi, dan efektivitas pengendalian internal secara keseluruhan. Auditor harus memastikan bahwa temuan pengendalian internal yang signifikan dicatat dan dilaporkan dengan tepat.
9. Membuat rekomendasi perbaikan: Setelah melakukan evaluasi sistem pengendalian internal, auditor harus membuat rekomendasi perbaikan untuk meningkatkan efektivitas pengendalian internal yang diterapkan dalam organisasi. Rekomendasi perbaikan ini dapat mencakup

saran untuk memperbaiki kebijakan dan prosedur, meningkatkan kontrol dan pengawasan, atau mengembangkan pelatihan dan pengembangan karyawan.

10. Memberikan laporan audit: Setelah menyelesaikan evaluasi sistem pengendalian internal, auditor harus menyusun laporan audit yang berisi temuan dan rekomendasi perbaikan. Laporan audit ini harus disampaikan kepada manajemen dan dewan direksi sebagai bagian dari proses akuntabilitas dan transparansi dalam pengelolaan organisasi.

Dalam melakukan evaluasi sistem pengendalian internal, auditor harus memastikan bahwa evaluasi dilakukan secara independen dan objektif, dengan mempertimbangkan perspektif bisnis dan risiko yang berbeda-beda. Evaluasi sistem pengendalian internal yang efektif dapat membantu organisasi dalam meningkatkan efektivitas dan efisiensi pengelolaan risiko, meningkatkan keandalan informasi, serta meningkatkan transparansi dan akuntabilitas dalam pengelolaan organisasi.

Dengan melakukan evaluasi sistem pengendalian internal yang efektif, auditor dapat mengidentifikasi kelemahan dalam sistem pengendalian internal yang diterapkan dalam organisasi, dan memberikan rekomendasi untuk meningkatkan efektivitas sistem pengendalian internal tersebut. Hal ini dapat membantu organisasi dalam meningkatkan pengelolaan risiko dan memastikan keandalan informasi yang dihasilkan oleh sistem informasi organisasi. (Azizah, 2017)

3.6 Pengumpulan Bukti

Pengumpulan bukti adalah tahap dalam proses audit di mana auditor mengumpulkan informasi dan fakta yang dapat digunakan untuk menilai keabsahan dan keandalan informasi yang terdapat dalam sistem informasi organisasi. Tahap pengumpulan bukti dilakukan setelah perencanaan audit dan evaluasi sistem pengendalian internal. Berikut adalah tahapan-tahapan dalam pengumpulan bukti:

1. Menentukan sumber informasi: Auditor harus menentukan sumber informasi yang dapat memberikan bukti yang valid dan relevan. Sumber informasi dapat berupa dokumen, catatan keuangan, laporan keuangan, sistem informasi, atau saksi-saksi yang terkait dengan transaksi atau kegiatan yang sedang diuji.
2. Memilih metode pengumpulan bukti: Auditor harus memilih metode pengumpulan bukti yang paling tepat untuk menilai keandalan dan keabsahan informasi yang sedang diuji. Metode pengumpulan bukti dapat berupa inspeksi, observasi, konfirmasi, atau pengujian.
3. Menyiapkan daftar pertanyaan: Auditor harus menyiapkan daftar pertanyaan yang dapat membantu dalam pengumpulan bukti. Daftar pertanyaan ini dapat berupa pertanyaan terkait dengan kebijakan dan prosedur, pengendalian dan pengawasan, serta kinerja sistem informasi organisasi.
4. Mengumpulkan bukti: Setelah menentukan sumber informasi dan metode pengumpulan bukti, auditor harus mulai mengumpulkan bukti. Auditor harus memastikan bahwa bukti yang dikumpulkan memadai dan dapat digunakan untuk menilai keandalan dan keabsahan informasi yang sedang diuji.
5. Memeriksa dan menganalisis bukti: Setelah mengumpulkan bukti, auditor harus memeriksa dan

menganalisis bukti untuk menilai keandalan dan keabsahan informasi yang sedang diuji. Auditor harus memastikan bahwa bukti yang diperoleh memadai dan dapat dipercaya untuk menilai keabsahan dan keandalan informasi.

6. Membuat kesimpulan: Setelah memeriksa dan menganalisis bukti, auditor harus membuat kesimpulan terkait dengan keandalan dan keabsahan informasi yang sedang diuji. Kesimpulan yang dibuat harus didasarkan pada fakta dan bukti yang diperoleh selama proses pengumpulan bukti.
7. Menyimpan dan mendokumentasikan bukti: Setelah memperoleh bukti, auditor harus menyimpan dan mendokumentasikan bukti tersebut secara sistematis dan akurat. Hal ini penting untuk melacak informasi yang diperoleh selama proses pengumpulan bukti dan sebagai bukti audit di masa depan.
8. Melaporkan temuan audit: Setelah selesai dengan pengumpulan bukti, auditor harus melaporkan temuan audit secara tertulis kepada manajemen. Laporan audit harus mencakup hasil evaluasi sistem pengendalian internal, temuan audit dan rekomendasi perbaikan yang diperlukan. Laporan audit juga dapat mencakup analisis risiko dan rekomendasi untuk mengelola risiko yang terkait dengan sistem informasi organisasi.

Pengumpulan bukti yang efektif dan terstruktur dapat membantu auditor dalam menilai keandalan dan keabsahan informasi yang terdapat dalam sistem informasi organisasi. Hal ini dapat membantu organisasi dalam meningkatkan efektivitas dan efisiensi operasional serta mengelola risiko yang dapat mempengaruhi kinerja organisasi.

Dalam pengumpulan bukti, auditor harus memastikan bahwa semua bukti diperoleh dengan cara yang sah dan bukti tersebut tidak dipengaruhi oleh pihak lain. Auditor juga harus memastikan bahwa bukti yang diperoleh dapat dipertanggungjawabkan dan dapat digunakan untuk menilai keandalan dan keabsahan informasi yang sedang diuji.

Pengumpulan bukti yang efektif dan terstruktur dapat membantu dalam menilai keandalan dan keabsahan informasi yang terdapat dalam sistem informasi organisasi, sehingga manajemen dapat mengambil tindakan yang diperlukan untuk memperbaiki kelemahan yang teridentifikasi dan meningkatkan kinerja organisasi secara keseluruhan.

3.7 Analisis Bukti dan Penilaian

Setelah selesai dengan tahap pengumpulan bukti, auditor akan melakukan analisis bukti dan penilaian untuk menilai apakah sistem informasi organisasi telah memenuhi standar yang diharapkan. Proses analisis bukti dan penilaian mencakup beberapa tindakan seperti:

1. Verifikasi bukti: Auditor harus memeriksa kembali setiap bukti yang telah dikumpulkan untuk memastikan keandalannya. Auditor harus memastikan bahwa bukti tersebut dapat dipertanggungjawabkan dan berasal dari sumber yang sah.
2. Evaluasi bukti: Auditor harus mengevaluasi bukti yang telah dikumpulkan dan membandingkannya dengan kriteria yang telah ditetapkan. Kriteria ini dapat mencakup kebijakan, prosedur, standar industri, atau hukum dan peraturan yang berlaku.
3. Identifikasi kelemahan dan kesenjangan: Auditor harus mengidentifikasi kelemahan dan kesenjangan dalam sistem informasi organisasi dengan membandingkan bukti yang diperoleh dengan kriteria yang telah

ditetapkan. Auditor harus dapat menentukan apakah kelemahan dan kesenjangan ini mempengaruhi sistem secara signifikan atau tidak.

4. Penilaian risiko: Auditor harus mengevaluasi risiko yang terkait dengan kelemahan dan kesenjangan yang telah diidentifikasi. Auditor harus dapat menentukan apakah risiko ini dapat mempengaruhi operasi organisasi secara signifikan atau tidak.
5. Menentukan rekomendasi: Setelah melakukan analisis dan penilaian, auditor harus menentukan rekomendasi untuk memperbaiki kelemahan dan kesenjangan yang telah diidentifikasi. Rekomendasi harus spesifik dan dapat diimplementasikan oleh manajemen organisasi.
6. Melaporkan temuan: Auditor harus melaporkan temuan audit secara tertulis kepada manajemen. Laporan audit harus mencakup hasil evaluasi sistem pengendalian internal, temuan audit, rekomendasi perbaikan yang diperlukan, dan analisis risiko yang terkait dengan sistem informasi organisasi.
7. Melakukan tindak lanjut: Setelah melaporkan temuan audit, auditor harus melakukan tindak lanjut untuk memastikan bahwa rekomendasi yang diberikan telah diimplementasikan dengan benar. Auditor dapat melakukan tindak lanjut dengan melakukan pemantauan atau melakukan audit lanjutan.
8. Mengidentifikasi area audit selanjutnya: Setelah menyelesaikan audit sistem informasi, auditor harus mengidentifikasi area audit selanjutnya untuk dilakukan di masa depan. Ini dapat membantu organisasi dalam memperbaiki kinerja dan efektivitas sistem informasi mereka.

Dalam melakukan analisis bukti dan penilaian, auditor harus memastikan bahwa hasil analisis dan penilaian tersebut akurat dan dapat dipertanggungjawabkan. Auditor juga harus memastikan bahwa rekomendasi yang diberikan spesifik dan dapat diimplementasikan oleh manajemen organisasi. Proses analisis bukti dan penilaian yang efektif dapat membantu dalam menilai kinerja sistem informasi organisasi dan mengidentifikasi area yang memerlukan perbaikan.

Analisis bukti dan penilaian adalah salah satu tahap penting dalam proses audit sistem informasi. Proses ini memastikan bahwa auditor memiliki informasi yang cukup untuk menilai sistem informasi organisasi dan mengidentifikasi kelemahan atau kesenjangan yang mempengaruhi kinerja sistem. Dengan melakukan analisis bukti dan penilaian yang efektif, auditor dapat memberikan rekomendasi yang spesifik dan dapat diimplementasikan oleh manajemen organisasi untuk memperbaiki sistem informasi mereka dan meningkatkan kinerja organisasi secara keseluruhan.

3.8 Pelaporan Temuan dan Rekomendasi

Pelaporan temuan dan rekomendasi adalah tahap terakhir dalam proses audit sistem informasi. Setelah selesai melakukan analisis bukti dan penilaian, auditor harus menyusun laporan audit yang berisi hasil temuan dan rekomendasi untuk diberikan kepada manajemen organisasi. Laporan audit harus disusun secara profesional dan terstruktur dengan jelas, sehingga mudah dipahami dan dapat membantu manajemen organisasi dalam mengambil tindakan yang tepat.

Beberapa hal yang harus diperhatikan dalam pelaporan temuan dan rekomendasi antara lain:

1. Format laporan audit: Laporan audit harus disusun dalam format yang sesuai dengan standar dan

kebutuhan organisasi. Format ini harus mencakup ringkasan hasil audit, tujuan audit, ruang lingkup audit, metodologi audit, temuan audit, rekomendasi audit, dan tindak lanjut yang harus dilakukan oleh manajemen organisasi.

2. Bahasa yang digunakan: Laporan audit harus ditulis dengan bahasa yang mudah dipahami oleh pembaca. Bahasa teknis atau jargon sebaiknya dihindari, kecuali jika pembaca adalah spesialis dalam bidang audit sistem informasi.
3. Isi laporan: Laporan audit harus berisi temuan dan rekomendasi audit yang jelas dan spesifik. Temuan harus dijelaskan dengan rinci, termasuk sumber bukti dan dampaknya terhadap organisasi. Rekomendasi harus praktis, dapat diimplementasikan, dan sesuai dengan kebutuhan organisasi.
4. Bukti audit: Laporan audit harus didukung oleh bukti audit yang cukup dan relevan. Bukti audit ini dapat berupa dokumen, wawancara, atau observasi langsung. Bukti audit harus dijelaskan secara rinci dalam laporan audit.
5. Tindak lanjut: Laporan audit harus mencakup tindak lanjut yang harus dilakukan oleh manajemen organisasi untuk mengatasi temuan dan rekomendasi audit. Tindak lanjut harus jelas, praktis, dan memungkinkan untuk diimplementasikan dalam jangka waktu yang ditentukan.

Dengan menyusun laporan audit yang baik, auditor dapat membantu organisasi dalam meningkatkan kinerja sistem informasi mereka, mengurangi risiko keamanan informasi, dan meningkatkan efektivitas bisnis secara keseluruhan.

Setelah laporan audit disusun, auditor harus menyampaikan laporan ini kepada manajemen organisasi dan menjelaskan temuan dan rekomendasi audit. Auditor juga harus siap untuk menjawab pertanyaan dan memberikan penjelasan yang lebih detail tentang temuan dan rekomendasi.

Selanjutnya, manajemen organisasi harus menindaklanjuti temuan dan rekomendasi yang disampaikan oleh auditor. Tindakan yang harus dilakukan oleh manajemen organisasi akan bergantung pada sifat dan keparahan temuan dan rekomendasi. Beberapa tindakan yang mungkin dilakukan antara lain:

1. Menerapkan tindakan perbaikan: Manajemen organisasi harus segera mengambil tindakan untuk memperbaiki masalah yang ditemukan oleh auditor.
2. Mengembangkan rencana tindakan: Manajemen organisasi harus mengembangkan rencana tindakan yang jelas dan spesifik untuk mengatasi temuan dan rekomendasi audit. Rencana tindakan harus mencakup jangka waktu yang realistis dan sumber daya yang diperlukan.
3. Meningkatkan kebijakan dan prosedur: Manajemen organisasi harus memperbarui kebijakan dan prosedur mereka untuk memastikan keamanan informasi dan efektivitas sistem informasi.
4. Melakukan pelatihan dan pengembangan: Manajemen organisasi harus memberikan pelatihan dan pengembangan untuk meningkatkan pengetahuan dan keterampilan karyawan dalam pengelolaan sistem informasi.
5. Melakukan audit ulang: Manajemen organisasi harus melakukan audit ulang untuk memastikan bahwa

masalah yang ditemukan oleh auditor telah diperbaiki dan sistem informasi berjalan secara efektif.

Dengan melakukan tindakan yang diperlukan untuk mengatasi temuan dan rekomendasi audit, organisasi dapat meningkatkan keamanan informasi, mengurangi risiko kerugian, dan meningkatkan efektivitas sistem informasi secara keseluruhan.

3.9 Tindak Lanjut

Tindak lanjut adalah proses di mana manajemen organisasi menindaklanjuti temuan dan rekomendasi audit yang telah disampaikan oleh auditor. Tindakan yang diambil oleh manajemen organisasi bergantung pada sifat dan keparahan temuan dan rekomendasi. Tujuan dari tindak lanjut adalah untuk memastikan bahwa masalah yang ditemukan oleh auditor telah diperbaiki dan sistem informasi berjalan secara efektif.

Berikut adalah beberapa langkah yang harus dilakukan dalam proses tindak lanjut:

1. Identifikasi dan penilaian risiko: Manajemen organisasi harus melakukan identifikasi dan penilaian risiko untuk memahami konsekuensi dari temuan dan rekomendasi audit. Langkah ini membantu manajemen organisasi memprioritaskan tindakan yang harus diambil.
2. Pengembangan rencana tindakan: Manajemen organisasi harus mengembangkan rencana tindakan yang jelas dan spesifik untuk mengatasi temuan dan rekomendasi audit. Rencana tindakan harus mencakup jangka waktu yang realistis dan sumber daya yang diperlukan.
3. Implementasi rencana tindakan: Manajemen organisasi harus mengimplementasikan rencana tindakan yang

telah dikembangkan. Langkah ini memastikan bahwa masalah yang ditemukan oleh auditor telah diperbaiki.

4. Monitoring dan evaluasi: Manajemen organisasi harus memantau dan mengevaluasi pelaksanaan rencana tindakan. Hal ini membantu memastikan bahwa tindakan yang diambil berhasil mengatasi masalah yang ditemukan oleh auditor.
5. Pelaporan: Manajemen organisasi harus memberikan laporan kepada auditor tentang tindakan yang telah diambil untuk mengatasi temuan dan rekomendasi audit. Laporan ini membantu auditor memastikan bahwa masalah yang ditemukan telah diperbaiki.

Dengan melakukan tindak lanjut yang diperlukan, manajemen organisasi dapat memastikan bahwa masalah yang ditemukan oleh auditor telah diperbaiki dan sistem informasi berjalan secara efektif. Tindak lanjut yang tepat juga membantu organisasi mengurangi risiko kerugian dan meningkatkan keamanan informasi serta efektivitas sistem informasi.

Selain itu, ada beberapa hal penting yang harus diperhatikan dalam proses tindak lanjut, yaitu:

1. Tanggung jawab: Manajemen organisasi harus menetapkan tanggung jawab untuk melaksanakan rencana tindakan. Tanggung jawab harus ditetapkan secara jelas dan spesifik untuk setiap tindakan yang harus dilakukan.
2. Komunikasi: Manajemen organisasi harus berkomunikasi dengan stakeholder yang relevan tentang rencana tindakan yang akan dilaksanakan. Hal ini membantu memastikan bahwa stakeholder

memahami tindakan yang akan dilakukan dan memberikan dukungan yang diperlukan.

3. Sumber daya: Manajemen organisasi harus menyediakan sumber daya yang diperlukan untuk melaksanakan rencana tindakan. Sumber daya dapat mencakup anggaran, personil, atau peralatan yang diperlukan untuk mengatasi masalah yang ditemukan.
4. Monitoring dan pelaporan: Manajemen organisasi harus memantau pelaksanaan rencana tindakan dan memberikan laporan kepada stakeholder yang relevan tentang kemajuan yang telah dicapai. Hal ini membantu memastikan bahwa tindakan yang dilakukan berhasil mengatasi masalah yang ditemukan oleh auditor.
5. Perbaikan berkelanjutan: Manajemen organisasi harus memastikan bahwa sistem informasi terus diperbaiki dan ditingkatkan secara berkelanjutan. Hal ini dapat dilakukan dengan memperbarui kebijakan dan prosedur, memberikan pelatihan kepada personil, atau memperbarui perangkat lunak dan peralatan.

Dalam melakukan tindak lanjut, manajemen organisasi harus bersikap proaktif dan bertanggung jawab untuk memastikan bahwa masalah yang ditemukan telah diperbaiki dan sistem informasi berjalan dengan efektif. Hal ini tidak hanya penting untuk memenuhi persyaratan audit, tetapi juga untuk menjaga keamanan informasi dan meminimalkan risiko kerugian bagi organisasi.

DAFTAR PUSTAKA

Achmad solechan (2021) 'Audit Sistem Informasi Audit Sistem Informasi.pdf', pp. 1–3.

Azizah, N. (2017) 'Audit Sistem Informasi Menggunakan Framework Cobit 4.1 Pada E-Learning Unisnu Jepara', *Simetris: Jurnal Teknik Mesin, Elektro dan Ilmu Komputer*, 8(1), pp. 377–382. Available at: https://doi.org/10.24176/simet.v8i1.1024.

Wahyudi, A. (2018) 'Tahapan tahapan audit sistem informasi', pp. 1–6.

BAB 4
STANDAR DAN PANDUAN UNTUK AUDIT SISTEM INFORMASI

4.1 Pengertian Audit Sistem Informasi

Audit ataupun pengecekan dalam makna luas bermakna penilaian terhadap sesuatu organisasi, sistem, proses, ataupun produk. Audit dilaksanakan oleh pihak yang kompeten, objektif, serta tidak memihak yang diucap auditor. Tujuan diadakannya audit merupakan buat melaksanakan verifikasi subJek dari audit sudah dituntaskan ataupun berjalan sesuai yang di inginkan dengan standar, serta aplikasi yang sudah disetujui (Wahid, 2022).

Auditing adalah sesuatu pengecekan yang diuji secara kritis serta sistematis oleh pihak yang independen, terhadap laporan keuangan yang sudah disusun oleh manajemen beserta catatan-catatan pembukuan dan bukti-bukti pendukungnya, dengan tujuan menjelaskan pendapat tentang laporan keuangan tersebut. Dari definisi audit yang telah dipaparkan di atas sesuatu proses pengumpulan dan pengevaluasian data yang didapat dengan seluruh kriteria yang telah di tentukan.

Gambar 4.1. Audit Sistem Informasi
Sumber : https://rifqimulyawan.com/blog/pengertian-it-audit

Audit sistem informasi merupakan sesuatu upaya penghimpunan untuk mengevaluasi bermacam fakta supaya dapat memastikan apakah sistem informasi yang digunakan pada suatu industri dapat mengamankan semua aset untuk melindungi integritas informasi, serta sanggup menargetkan industri dalam menentukan target tujuannya secara efisien dan memakai sumberdaya yang terdapat secara lebih efektif.

Ada sebagian komponen yang wajib, ialah audit secara merata pada tingkatan daya guna, efisiensi, availability, confidentiality, reliability, integrity, aspek keamanan, modifikasi program, audit proses, audit sumber informasi, serta pula informasi file maupun database industri (Rizka *et al* ,2022). Audit adalah proses mengenai tentang memperoleh dan mengevaluasi dengan objektif bukti yang berkaitan dengan penilaian melakukan berbagai kegiatan dan acara ekonomi untuk memastikan kesesuaian penciptaan evaluasi dan kriteria dan untuk mengkomunikasikan hasilnya kepada pengguna yang melakukan bisnis di perusahaan. Audit adalah pengumpulan

dan evaluasi bukti tentang informasi untuk memilih dan menyajikan tingkat kesesuaian informasi tersebut dan kategori yang telah ditetapkan.

Audit sistem informasi adalah proses mengumpulkan bukti untuk menentukan apakah sistem pengendalian internal yang memadai telah ditetapkan dan diterapkan dalam sistem informasi, apakah semua aset dilindungi dengan baik dan bebas dari penyalahgunaan, dan untuk memastikan keamanan, Informasi yang efisiensi. efisiensi operasi terkomputerisasi. sistem informasi adalah informasi yang telah diolah dalam bentuk yang berarti bagi penerimanya dan berguna untuk membuat keputusan saat ini atau di masa mendatang informasi adalah informasi yang telah diproses sedemikian rupa sehingga bermakna dan dapat digunakan untuk suatu tugas dalam tindakan yang menentukan. Data disusun sedemikian rupa sehingga memiliki arti dan nilai bagi penerimanya.

Audit sistem informasi adalah proses pengujian infrastruktur TI, di mana diketahui apakah sistem yang digunakan dan beroperasi dapat memastikan keamanan properti yang dimiliki, integritas data, dan efisiensi operasi untuk dicapai. tujuan yang ditetapkan Audit sistem informasi adalah proses mengumpulkan dan mengevaluasi bukti untuk menentukan apakah sistem dapat menjaga integritas data, berkontribusi secara efektif untuk tujuan organisasi, dan menggunakan sumber daya secara efisien.

Tujuan utama manajemen TI adalah untuk memantau kepatuhan pengguna TI. Efisiensi TI dan sesuai tujuannya, antara lain TI dengan strategi kelembagaan yang mempengaruhi keuntungan lembaga, penggunaan TI secara maksimal dapat menjadi peluang untuk memaksimalkan keuntungan lembaga, tanggung jawab penggunaan yang lebih besar sumber daya IT, Adanya informasi yang dapat dilakukan manajemen risiko dengan cepat. (Eva dan Besus, 2022).

Audit sistem data ini gabungan dari bermacam-macam tipe ilmu, ialah ilmu traditional audit, sistem data akuntansi, ilmu komputer, behavioral science, serta pula manajemen sistem data. Standar yang biasanya digunakan dalam audit sistem data merupakan standar yang telah dikeluarkan oleh pihak ISACA, ialah ISACA IS Audit Standard. Lebih dari itu, ISACA juga menghasilkan IS Audit Guidance serta pula IS Auditing Procedure. (Juniati, 2022).

4.2 Jenis-jenis Audit

Berikut adalah beberapa jenis audit, diantaranya Audit Berkaitan dengan kegiatan dimana bukti dikumpulkan dan dievaluasi tentang pernyataan suatu entitas dengan tujuan untuk memberikan pendapat (opini) apakah pernyataan tersebut sesuai dengan peraturan. Kriteria menurut prinsip tanggung jawab yang berlaku secara umum (Wahid, 2022).

1. Audit dalam keuangan
   Mengacu pada kegiatan di mana bukti dikumpulkan dan dievaluasi tentang laporan suatu entitas ekonomi, yang tujuannya adalah untuk memberikan pendapat apakah laporan tersebut memenuhi kriteria yang ditetapkan menurut prinsip akuntansi yang berlaku secara umum.
2. Audit Sistem Informasi
   Merupakan pemeriksaan yang dilakukan terhadap perusahaan yang menangani pengolahan data akuntansi. Biasanya melalui sistem electronic data processing (EDP). Auditor harus memperhatikan hal-hal sebagai berikut:
   a. Alat keamanan melindungi perangkat komputer, baik program, komunikasi atau data, terhadap penggunaan, modifikasi, dan bahkan perusakan yang tidak sah.
   b. Pengembangan program dilakukan dengan kewenangan.
   c. Administrasi khusus dan umum
      Pengembangan program dilakukan dengan kekuatan khusus dan umum manajemen perusahaan.

d. Penanganan acara, file, laporan, catatan komputer yang akurat dan
   Lengkap informasi dalam file laporan yang disimpan di komputer sangat rahasia.

3. Pengendalian manajemen operasional
   Kegiatan dilaksanakan secara efektif dan efisien. Tinjauan investigasi adalah serangkaian kegiatan yang bertujuan untuk mengidentifikasi (mengatur kembali), mengidentifikasi dan memeriksa fakta dan informasi yang ada untuk mengungkapkan kejadian yang sebenarnya. pernyataan mendukung proses hukum atas dugaan perbuatan salah yang dapat merugikan perekonomian masyarakat (organisasi/perusahaan/negara/daerah).

4. Pemeriksaan forensik
   Pemeriksaan forensik bertujuan untuk mencegah terjadinya kecurangan yang dapat dilakukan. ilmu forensik adalah Ilmu forensik bertujuan untuk mencegah penipuan. Hal-hal yang dapat dilakukan ilmu forensik adalah:
   a. Penyidikan
   b. Referensi penipuan di perusahaan atau karyawan
   c. Mengetahui bagaimana kehilangan bisnis,

5. Audit lingkungan audit lingkungan adalah proses manajemen yang mencakup penilaian yang sistematis, tercatat (terdokumentasi) dan obyektif tentang bagaimana kegiatan manajemen organisasi dimaksudkan untuk memfasilitasi. pengendalian administratif dalam pengelolaan dampak lingkungan dan penggunaan komersial dalam peraturan perundang-undangan tentang pengelolaan lingkungan.

6. Audit Kepatuhan Audit kepatuhan, atau sering disebut sebagai audit kepatuhan, adalah jenis audit yang dirancang untuk menentukan apakah suatu perusahaan telah mengikuti Aturan dan praktik yang mematuhi prinsip-prinsip yang ditetapkan oleh pihak internal dan eksternal di

perusahaan/komunitas. Audit kepatuhan digunakan untuk menentukan seberapa baik perusahaan mengikuti aturan, praktik, peraturan pemerintah, dan bahkan undang-undang yang harus diikuti oleh penyedia. (Wahid,2022).

Gambar 4.2. Audit Sistem Informasi
Sumber : https://www.sekolahan.co.id/audit-sistem-informasi/

Pengembangan sistem aplikasi untuk menilai apakah sistem yang digunakan harus diperbarui atau diperbaiki, atau bahkan dihentikan jika tidak lagi memenuhi kebutuhan. atau memiliki kesalahan. Inspektur adalah anggota tim pengembangan system Selanjutnya, mereka membantu tim meningkatkan kualitas pengembangan sistem yang dibuat oleh analis sistem, perancang, dan pemrogram sehingga dapat diterapkan. Dalam hal ini, auditor bertindak sebagai wakil dari manajer proyek dan manajemen sebagai penjamin mutu. Auditor mengevaluasi kinerja fungsi unit fungsional atau sistem informasi, apakah dapat dikelola dengan baik, apakah pemeriksaan yang dilakukan selama pengembangan sistem secara keseluruhan dapat diterapkan dengan benar, apakah sistem komputer yang digunakan dikelola digunakan dengan benar. Dalam pemeriksaan sistem komputer.(Joben *et al*, 2022). dengan menilai tindakan pengendalian umum dari

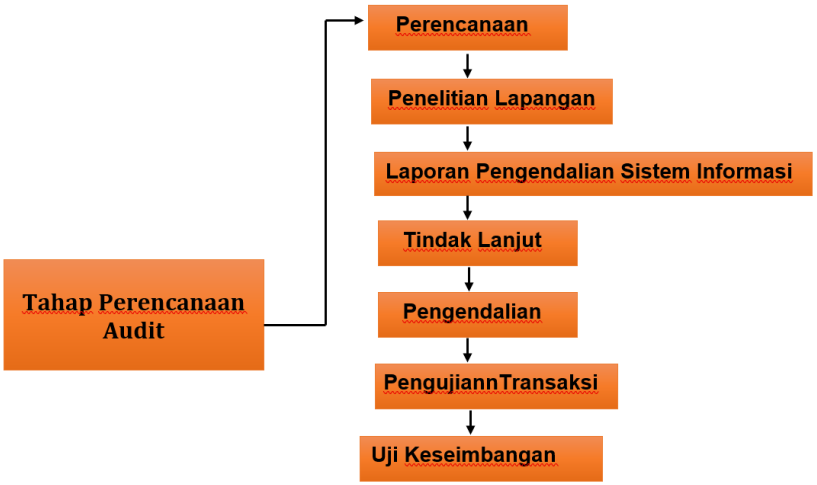
berbagai sistem komputer yang diterapkan oleh perusahaan secara keseluruhan. Berbagai jenis pengujian digunakan sebagai bukti untuk menarik kesimpulan dan membuat rekomendasi kepada manajemen tentang efektivitas, efisiensi, dan juga penghematan sistem (Fendi dan Ismail, 2022).

4.3 Tujuan Audit Sistem Informasi

Tujuan audit sistem informasi adalah sebagai berikut:

a. Tindakan keamanan untuk melindungi peralatan komputer, program, komunikasi dan data terhadap penggunaan, modifikasi atau penghancuran yang tidak sah.
b. Pengembangan dan pengadaan program dilakukan sesuai dengan ketentuan umum dan peraturan manajemen.
c. Perubahan program patuh pada otorisasi dan persetujuan manajemen.
d. Pemrosesan kejadian, arsip, laporan, dokumen, dan catatan komputer lainnya akurat dan lengkap.
e. Sumber data yang tidak tepat atau tidak sah diidentifikasi dan ditangani sesuai dengan praktik manajemen yang ditetapkan.
f. File komputer akurat, lengkap dan rahasia.

4.3.1 Tahap Perencanaan Audit



Gambar 4.3. Tahap Perencanaan Audit

Langkah-langkah tahapan sistem informasi "Audit dan Pengendalian Sistem Informasi" yang dibuat beberapa fungsi seperti perencanaan, pengendalian lapangan, pelaporan dan pengawasan (Lisa dan Rozie,2023).

Berikut adalah tahapan audit sistem informasi, yaitu sebagai berikut:

1. Perencanaan

   Tahap perencanaan yang dilakukan adalah menentukan ruang lingkup, unit-unit yang dapat dikendalikan, standar evaluasi hasil audit dan komunikasi dengan manajemen. dalam suatu organisasi yang bertugas menganalisis visi, misi, tujuan dan sasaran objek penelitian, serta strategi dan kebijakan yang berkaitan dengan proses penelitian. Tahap pertama audit untuk auditor eksternal berarti dari awal penyelidikan atau kelanjutan untuk menentukan penerimaan audit, melibatkan personel audit yang tepat untuk meninjau informasi latar belakang klien,

memahami kewajiban klien yang paling penting dan mengidentifikasi area berisiko

2. Penelitian Lapangan (*Fieldwork*)

   Langkah yang dapat ditindaklanjuti ini adalah pengumpulan data yang dilakukan melalui pengumpulan data dengan pihak terkait. Hal ini dapat dilakukan melalui berbagai metode pengumpulan data yaitu wawancara, survei atau survei lapangan.
3. Pelaporan Pengendalian sistem informasi

   Setelah dilakukan pendataan, diperoleh data yang diolah untuk perhitungan berdasarkan perhitungan tingkat maturitas. Pada tahap ini diberikan informasi berupa hasil pemeriksaan. Tingkat kematangan dihitung berdasarkan hasil wawancara, survei dan kuesioner. Berdasarkan hasil yang mencerminkan kinerja saat ini (current maturity) dan standar yang diharapkan atau kinerja ideal, hal ini menjadi tolak ukur untuk analisis selanjutnya.
4. Tindak Lanjut

   Tujuan dari langkah ini adalah untuk menyusun laporan pemeriksaan berupa rekomendasi tindakan korektif untuk pemeriksaan barang yang diperiksa. Mulai saat ini, hak koreksi menjadi tanggung jawab administrasi objek yang diperiksa, baik itu harus dilaksanakan atau hanya menjadi acuan untuk perbaikan ke depan.
5. Pengendalian

   Fase ini diawali dengan fokus pada pengendalian administratif, jika hasilnya tidak seperti yang diharapkan, maka pengendalian administratif tidak berjalan sebagaimana mestinya. Ketika auditor menemukan kesalahan serius dalam pengendalian administratif, mereka mengeluarkan pernyataan atau memutuskan untuk menguji saldo transaksi dan hasil.

6. Pengujian Transaksi (*Transaction Tests*)
   Pengujian yang meliputi pengecekan log masuk dengan dokumen induk, pengujian nilai aset dan ketelitian perhitungan. Komputer sangat berguna dalam pengujian ini dan auditor dapat menggunakan perangkat lunak audit standar untuk memverifikasi bahwa biaya bank dihitung dengan benar (Diah *et al*,2022).
7. Uji keseimbangan atau hasil umum (*Balance test or general results*) Auditor melakukan pengujian ini sedemikian rupa sehingga dalam penilaian akhir, kehilangan atau pencatatan yang salah merupakan bukti penting, yang menyebabkan kegagalan sistem informasi untuk menyimpan informasi. keseluruhan dan mencapai sistem yang efektif dan efisien. Dengan kata lain, penekanan pada fase ini adalah memantau integritas aset dan data secara objektif.

Perencanaan audit untuk auditor eksternal, hal ini melibatkan pelaksanaan penelitian terhadap klien untuk menentukan apakah pekerjaan audit dapat diterima, menempatkan anggota audit yaitu :

1. Menyiapkan kontrak audit yang telah ditentukan sebelumnya, menghasilkan informasi latar belakang klien, memahami masalah hukum klien, dan juga menganalisis masalah yang sudah ada. Prosedur untuk memahami bisnis klien dan mengidentifikasi risiko audit di dalamnya (Tony dan Martinius, 2022).
2. Pengujian Pengendalian (Test Of Controls) Pada tahap ini, auditor melakukan pengujian pengendalian ketika mereka mengatakan bahwa manajemen risiko berada pada tingkat maksimum, sehingga mengandalkan pengendalian sebagai pembanding untuk mengurangi biaya pengujian yang ada. Pada tahap ini, auditor juga tidak mengetahui apakah identifikasi pengendalian sudah efektif, sehingga diperlukan penilaian yang lebih rinci.

3. Pengujian Transaksi Auditor menggunakan pengujian atas transaksi yang ada untuk menilai apakah terdapat kesalahan atau proses yang tidak biasa dalam aktivitas transaksi yang dapat menyebabkan kesalahan material dalam laporan keuangan. tes mencakup pemantauan log dokumen sumber yang ada, memverifikasi file, dan juga memverifikasi keakuratan data.
4. Pengujian Neraca atau Laba Rugi Komprehensif Untuk mengetahui pendekatan mana yang digunakan pada tahap ini, perlu diperhatikan pemantauan konsistensi harga dan data perusahaan. Beberapa pengujian substantif yang digunakan antara lain inventarisasi, verifikasi kewajiban dan juga penghitungan kembali aset tetap perusahaan.
5. Penyelesaian/penyelesaian audit Pada tahap akhir audit, pihak eksternal audit melakukan beberapa pengujian tambahan atas bukti-bukti yang ada untuk kemudian digunakan sebagai bahan laporan. Cakupan audit sistem informasi ini biasanya lebih terfokus pada semua sumber daya informasi yang tersedia seperti aplikasi, infrastruktur, personel dan data.

Tujuan audit informasi sebagai berikut:

1. Perlindungan aset - aset informasi milik perusahaan seperti perangkat lunak, perangkat keras, sumber daya manusia dan file harus selalu dipelihara dengan sistem pengendalian internal yang baik untuk mencegah penyalahgunaan aset perusahaan. dengan demikian, sistem keamanan aset merupakan hal yang sangat penting yang harus disediakan oleh perusahaan.
2. Menjaga integritas data Integritas data pada dasarnya merupakan salah satu konsep dasar dari sebuah sistem informasi. Pengetahuan itu sendiri terdiri dari kualitas-kualitas tertentu seperti kebenaran, akurasi dan kelengkapan. Jika integritas data tidak dapat dijaga dengan baik maka perusahaan tidak akan lagi

mendapatkan hasil atau laporan yang baik dan sangat memungkinkan untuk mengalami kerugian.

3. Mendukung efisiensi sistem Efisiensi sistem informasi memegang peranan penting dalam proses pengambilan keputusan di perusahaan. Suatu sistem informasi dapat dikatakan efektif hanya jika sistem informasi tersebut sesuai dengan kebutuhan penggunanya.
4. Menjaga efisiensi sistem Efisiensi adalah masalah yang sangat penting ketika komputer kehabisan daya atau perlu menilai kembali apakah efisiensi sistem masih mencukupi atau perlu menambah sumber daya. Mengapa? karena sistem dapat dikatakan efektif jika sistem informasi di dalamnya dapat memenuhi kebutuhan pengguna dengan sumber daya informasi yang terbatas.

4.3.2 Penugasan Audit

Penentuan Pendekatan Sebelum merencanakan dan melaksanakan audit, auditor terlebih dahulu harus menentukan pendekatan yang akan digunakan. Auditor harus dapat menentukan secara akurat teknik pengambilan sampel yang digunakan, teknik pengujian bahan yang akan diaudit, dan antara lain menentukan jenis bukti yang diperlukan untuk memperoleh bukti audit yang tepat (Rohani *et al*,2022).

Tugas audit ini biasanya berdasarkan permintaan manajemen senior, untuk auditor internal tugas audit ini biasanya permanen dan sementara. namun, dalam hal auditor eksternal, perlu diketahui apakah ia masih menjadi auditor lembaga tersebut yang bersangkutan atau tidak. Setelah dipastikan bahwa pemeriksa tetap dipilih sebagai pemeriksa, pemeriksa harus menerima atau menolak penugasan tersebut. Dalam hal ini, auditor harus mempertimbangkan faktor risiko yang dicapainya

berdasarkan hasil audit sebelumnya, ketika ia menerima tugas tersebut. Jika auditor menolak setelah mengidentifikasi risiko tersebut, misalnya karena lembaga ternyata tidak memperhitungkan hasil audit sebelumnya, maka auditor harus mengirimkan surat penolakan.

Menyebutkan dan menjelaskan dasar hukum lembaga auditnya dalam melakukan kegiatan audit. Selain itu, auditor harus mengetahui dan memahami aturan etika yang berlaku. Waktu Pengawas teknis harus dapat memperkirakan waktu yang cukup untuk merencanakan audit sehingga inspektur dapat melaksanakan rencana inisiasi audit (RMA). Waktu yang diperlukan untuk menjadwalkan tugas audit bervariasi menurut proyek (Nurholis dan Joy,2022).

4.3.3 Pelaporan Audit

Laporan keuangan adalah cara atau metode yang berguna untuk mengkomunikasikan informasi keuangan kepada penggunanya. Kualitas pelaporan keuangan harus selalu diperhatikan. Pelaporan keuangan yang berkualitas sangat penting bagi penyedia modal dan pemangku kepentingan lainnya karena dapat menunjukkan sisi positifnya ketika mereka terlibat dalam kegiatan investasi, kepercayaan, mengarahkan sumber daya yang tersedia, dan keputusan untuk meningkatkan efisiensi pasar secara keseluruhan Kurangnya pelaporan keuangan yang berkualitas dapat mempengaruhi keputusan investor dan memberikan penilaian yang buruk terhadap manajemen perusahaan. Kualitas laporan keuangan sangat penting bagi perusahaan, dimana jika laporan keuangan perusahaan berkualitas rendah maka dapat disimpulkan tingkat manajemen laba sangat tinggi begitu juga sebaliknya (Iskandar dan Febrine, 2023).

Laporan keuangan tidak hanya digunakan sebagai bentuk tanggung jawab perusahaan, tetapi juga berperan penting untuk mengetahui kinerja dan keadaan keuangan perusahaan, serta dalam membuat rencana dan keputusan manajemen perusahaan. Manajemen laba digunakan sebagai keputusan manajer ketika mereka memilih prinsip akuntansi yang cenderung mencapai tujuan yang tepat untuk meningkatkan laba dan menghindari kerugian yang dilaporkan. Manajemen laba dapat diakibatkan dari keinginan pemilik modal untuk memperoleh keuntungan yang lebih banyak dari manajemen dengan tujuan untuk meningkatkan nilai perusahaan sehingga manajemen berusaha untuk meningkatkan keuntungan untuk hasil yang baik (Aan dan Andrian, 2023).

DAFTAR PUSTAKA

Wahid Wachyu Adi Winarto,M.Si, Audit Sistem Informasi. PT Nasya Expanding Management (Penerbit-Anggota IKAPI). Cetak Ke-1,februari 2022 ISBN :978-623-423-157-1.

Juniati, Salbya Rizky (2022) Audit Sistem Informasi Menggunakan Cobit 4.1 Pada sekolah Ilmu Ekonomi Indonesia *(STEI).*

Rizka Nurul Wahidah, Nur Lutfiyana, Vanny Fitria Ramadanti, Panji Septiyo, Rian Drefiyanto.2022 Audit Sistem Informasi Mesin Fingerprint pada PT. mental Castindo industritama dengan Menggunakan Framerwork Cobit 5 VOL. XI NO. 02 AGUSTUS 2022 ISSN 2089-8711 E-ISSN 2615-093X | *Audit Sistem Informasi*

https://chairulsulaiman.wordpress.com/2018/10/26/audit-teknologi-sistem-informasi-isaca-iia-coso-dan-iso-1799/

Fendi Veknyo Widiyanto, dan Ismail. 2022. Audit system Informasi SAS pada BPK Penabur Serpong Menggunakan kerangka Cobit 4.1 Vol. 16 - Nomor 1 - April 2022 ISSN: 1412-0232

Tony Soebijono, Martinus Sony Erstiawan. 2022. Audit Sistem Informasi Menggunakan Framework Cobit Pada Sekolah Tinggi "X" Surabaya

Eva Zuraidah, Besus Maula Sulthon 2022. Audit Sistem Informasi Penjualan Pada UMKM MAM Menggunakan Framework Cobit 5. JURIKOM (Jurnal Riset Komputer), Vol. 9 No. 5, Oktober 2022

Iskandar Itan, Febrine.2023. Pengaruh Komite Audit, Direktur dan Auditor Eksternal Terhadap Kualitas Pelaporan Keuangan pada Perusahaan yang Terdaftar di Bursa Efek Indonesia. Jambura Accounting Review, Volume 4 No. 1, Februari 2023. Hal. 27 – 40

Aan Andrianingsih, Andrian Budi Prasetyo.2023. Pengaruh keahlian Keuangan komite Audit dan manajemen terhadap Audit Report LAG. ***Volume 12, Nomor 1, Tahun 2023, Halaman 1-15***
https://sis.binus.ac.id/2021/06/15/audit-sistem-informasi-2/

Lisa Aulia Julica, Rozie Meidy.2023 Analisis Faktor-Faktor Determinan yang Mempengaruhi Kualitas Audit. Vol 4, No 3, Februari 2023, Hal 1064−1073

Rohani Libra Siagian, Mukhlasin Mukhlasin, Reskino Reskino, Renato Sitompul. 2022. Pengaruh Tekanan Anggaran waktu, kompleksitas Tugas, Locus Of Control, dan Etika Profesi terhadap Perilaku Disfungsional Audit. *Vol 3, No. 3, November 2022, pp. 355-369*

Diah Aryati Prihartini, Tommy Kuncara, Early Armein. Implementasi Audit Planning Berdasarkan Standar Profesional Akuntan Publik Pada Kantor Akuntan Publik Abdul Ghonie Dan Rekan .Volume 7 Nomor 1, Januari 2022.

BAB 5
SISTEM KONTROL INTERNAL

5.1 Definisi Sistem Kontrol Internal

Sistem kontrol internal (SKI) merupakan nama lain dari sistem pengendalian internal (SPI). Secara umum sistem kontrol internal merupakan sebuah sistem dari sebuah organisasi yang digunakan untuk melindungi asetnya, dengan cara mengawasi, mengarahkan dan mengukur sumber daya yang ada. Namun secara konsep juga perlu diketahui apa-apa saja definisi sistem kontrol internal menurut para ahli, organisasi dan pemerintah, yaitu sebagai berikut:

- Menurut Sawyer et al. (2003) American Institute of Certified Publik Accountants (AICPA) mendefinisikan bahwa sistem kontrol internal merupakan suatu kegiatan pada suatu organisasi yang saling terkoordinasi, bertujuan untuk melindungi aset, menguji kecermatan dan keabsahan data akuntansi, menaikkan efisiensi operasi, serta membawa ketaatan pada kebijakan-kebijakan yang sudah ditetapkan.
- Menurut Rama and Jones (2005) sistem kontrol internal merupakan kebijakan organisasi yang dipengaruhi oleh pimpinan, pengelola, dan personil lainnya, dalam memberikan kepastian terkait pencapaian mengenai, efektivitas dan efisiensi operasional, ketepatan laporan keuangan, dan kepatuhan terhadap kebijakan yang berlaku.
- Menurut Arens et al. (2007) sistem kontrol internal adalah suatu strategi dan prosedur yang dibuat untuk memberikan kepastian terhadap manajemen bahwa

sasaran dan tujuan organisasi sangat penting untuk dipenuhi.

- Menurut Presiden RI (2008) sistem kontrol internal adalah suatu cara yang integral atas kegiatan yang dilakukan secara kontinu oleh pemimpin dan seluruh staf dalam meneruskan keyakinan yang memadai atas pencapaian tujuan organisasi lewat tindakan yang efektif dan efisien, kemampuan pelaporan keuangan, perlindungan aset negara, dan kepatuhan terhadap peraturan perundang-undangan.
- Menurut Horngren et al. (2009) sistem kontrol internal adalah suatu kegiatan dalam organisasi yang dibentuk untuk melindungi aktiva, memotivasi pekerja supaya mengikuti strategi organisasi, meyakinkan catatan akuntansi yang akurat dan mendorong efisiensi operasional.
- Menurut Pfister (2009) sistem kontrol internal adalah suatu sistem untuk menghindari, mengidentifikasi, dan mengoreksi kesalahan yang mungkin muncul selama pemrosesan informasi.
- Menurut Reeve et al. (2009) sistem kontrol internal adalah kebijakan organisasi dalam menyediakan keyakinan bahwa aset sudah terlindungi dan dimanfaatkan bagi keperluan operasional, informasi bisnis yang tepat, pekerja telah menaati peraturan dan hukum yang berlaku.
- Menurut King (2011) sistem kontrol internal adalah suatu proses yang dilaksanakan dalam pencapaian hasil dan tujuan organiasasi, selain itu juga merencanakan otoritas kinerja, pengaturan, dan pemantauan di seluruh bagian organisasi.
- Menurut Shim (2011) sistem kontrol internal merupakan bagian dari sistem manajemen organisasi untuk melindungi properti, memeriksa kebenaran kinerja, menjamin efektivitas kinerja, sehingga dapat mengurangi atau menemukan kesalahan, serta memperbaikinya tepat waktu, untuk mencapai tujuan organisasi.

- Menurut Swinkels (2012) sistem kontrol internal merupakan strategi organisasi dan sistem instruksi yang diterapkan manajemen organisasi dan dewan direksi, untuk melindungi aset organisasi, memotivasi pekerja untuk mematuhi kebijakan organisasi, melakukan efesiensi operasional, memastikan catatan akuntansi yang tepat dan bisa diandalkan, serta menaati hukum.
- Menurut DiNapoli (2016) sistem kontrol internal adalah suatu proses yang dijalankan oleh pimpinan, manajemen, dan personil lainnya, dalam memberikan kepastian atas tercapainya tujuan yang berhubungan dengan operasi, pelaporan, dan ketaatan.
- Menurut Schandl and Foster (2019) Committee of Sponsoring Organizations of the Treadway Commission (COSO) mengartikan sistem kontrol internal sebagai suatu proses, yang dipengaruhi oleh pimpinan, manajemen, dan personil lainnya, yang dibuat untuk memberikan jaminan tercapainya tujuan organisasi yang berhubungan dengan operasi, pelaporan, dan kepatuhan.

Berdasarkan beberapa definisi yang telah disampaikan, sehingga dapat dirumuskan bahwa definisi sistem kontrol internal adalah suatu tindakan yang dikerjakan oleh seluruh entitas organisasi dalam menentukan kebijakan dan prosedur secara rutin dan memberikan kepastian yang memadai atas pencapaian tujuan organisasi melalui peningkatan efektivitas dan efisiensi operasional, mengamankan aset organisasi, menjaga keakuratan dan keandalan laporan keuangan, memotivasi seluruh entitas mengikuti kebijakan organisasi, dan menaati hukum dan peraturan yang berlaku.

5.2 Jenis Sistem Kontrol Internal

Sistem kontrol internal terdiri dari beberapa jenis, yaitu sebagai berikut:

- Kontrol internal akuntansi:
  Merupakan kontrol terhadap perencanaan, keadalan data, pencatatan, pelaporan, persetujuan, pemisahan fungsi operasional, prosedur *monitoring* dan aset orgnisasi.
- Kontrol internal administrasi:
  Merupakan kontrol terhadap organisasi kerja, kebijakan direksi, efesiensi usaha, manajemen sumber daya, risiko dan mutu.
- Kontrol internal organisasi:
  Merupakan kontrol dalam pemisahan tugas, kegiatan fisik, rekonsiliasi, kebijakan dan prosedur, pemrosesan informasi, transaksi dan aktivitas organisasi.
- Kontrol internal operasional:
  Merupakan kontrol dalam proses bisnis ketika menetapkan kemampuan setiap sumber daya yang digunakan dalam organisasi, tujuannya untuk menjalankan rencana yang telah ada, mengukur kemampuan produksi dan perbaikan rencana operasional.
- Kontrol internal keuangan:
  Merupakan kontrol dalam pengelolaan keuangan yang meliputi kegiatan perencanaan, pengaturan, pengarahan dan pengendalian kegiatan keuangan organisasi.
- Kontrol internal preventif:
  Merupakan kontrol dalam mencegah terjadinya suatu kesalahan dalam organisasi dengan cara melakukan pengecekan seluruh aktivitas organisasi secara rutin.
- Kontrol internal detektif:
  Merupakan kontrol dalam mendeteksi kesalahan yang mungkin terjadi dalam kegiatan organisasi.

- Kontrol internal korektif:
  Merupakan kontrol untuk memberikan koreksi terhadap kesalahan yang telah terdeteksi dalam kegiatan organisasi.
- Kontrol internal usaha:
  Merupakan kontrol dalam mengatur dan menentukan kebijakan keuangan dan operasional usaha.
- Kontrol internal produksi:
  Merupakan kontrol dalam penentuan bahan baku, harga bahan baku, proses produksi, kualitas produksi dan sumber daya manusia.
- Kontrol internal kinerja:
  Merupakan kontrol dalam menetapkan standar kinerja dan evaluasi kerja.
- Kontrol internal pekerja:
  Merupakan kontrol terhadap hal yang berhubungan dengan kegiatan pekerja.
- Kontrol internal waktu:
  Merupakan kontrol terhadap penggunaan waktu dalam suatu organisasi.
- Kontrol internal teknis:
  Merupakan kontrol terhadap teknis pelaksanaan kegiatan dalam organisasi.
- Kontrol internal komunikasi:
  Merupakan kontrol terhadap bagaimana komunikasi dalam organisasi sehingga dapat mengendalikan perilaku personil dalam organisasi.
- Kontrol internal umum:
  Merupakan kontrol terhadap aktivitas yang berhubungan dengan data dan komputer, seperti pemisahan hak akses dan pengolahan data.
- Kontrol internal aplikasi:
  Merupakan kontrol terhadap transaksi dan penggunaan aplikasi komputer meliputi otorisasi, kelengkapan, akurasi dan keandalan pemrosesan, sehingga setiap transaksi tercatat, diproses, mendapat otoritas dan dilaporkan dengan baik.

- Kontrol internal pemerintah:
  Merupakan kontrol terhadap penyelenggaraan seluruh aktivitas di lingkungan pemerintah pusat dan daerah.

5.3 Komponen Sistem Kontrol Internal

Menurut Schandl and Foster (2019) bahwa COSO membagi sistem kontrol internal kedalam lima komponen yaitu sebagai berikut:

- Lingkungan kontrol *(control environment)*:
  Merupakan seperangkat standar, proses, dan struktur yang mempersiapkan dasar untuk melaksanakan kontrol internal di semua bagian organisasi. Menurut Institute of Internal Auditors (IIA) bahwa lingkungan kontrol merupakan landasan dari sistem kontrol internal yang efektif, dibentuk dan dijalankan dalam suatu organisasi untuk pencapaian tujuan strategis, memberikan laporan keuangan yang andal kepada pihak internal dan eksternal, melaksanakan bisnis secara efisien dan efektif, menaati semua hukum dan peraturan yang berlaku, serta melindungi aktiva.
  Lingkungan kontrol memiliki lima prinsip kontrol internal, yaitu:
  - Memperlihatkan kewajiban terhadap integritas dan nilai-nilai etika.
  - Menjalankan tanggung jawab kontrol.
  - Memastikan struktur, wewenang, dan tanggung jawab.
  - Memperlihatkan komitmen terhadap kompetensi.
  - Menegakkan akuntabilitas.
- Penilaian risiko *(risk assessment)*:
  Merupakan dasar dalam memastikan bagaimana risiko akan diatur. Penilaian risiko mengharuskan manajemen untuk memperhitungkan efek dari peluang perubahan dalam lingkungan internal dan eksternal dan kesanggupan dalam mengambil langkah untuk mengelola efef tersebut.

Penilaian risiko memiliki empat prinsip kontrol internal, yaitu:
  - Menetapkan tujuan yang sesuai.
  - Mengidentifikasi dan menganalisis risiko.
  - Memperhitungkan risiko penipuan.
  - Mengidentifikasi dan menganalisis perubahan yang signifikan.
- Aktivitas kontrol *(control activities)*:
  Merupakan tindakan yang membantu manajemen dalam mengurangi risiko dan memastikan tercapainya tujuan. Aktivitas kontrol dapat bersifat pencegahan atau deteksi dan bisa dilaksanakan di seluruh tingkatan organisasi.
  Aktivitas kontrol memiliki tiga prinsip kontrol internal, yaitu:
  - Menentukan dan mengembangkan aktivitas kontrol.
  - Menentukan dan mengembangkan kontrol umum atas teknologi.
  - Mengimplementasikan aktivitas kontrol melalui strategi dan prosedur.
- Informasi dan komunikasi *(Information and Communication)*:
  Informasi diciptakan oleh manajemen, baik bersumber dari internal maupun eksternal guna membantu unsur kontrol internal. Komunikasi berlandaskan sumber internal dan eksternal dimanfaatkan untuk menyebarkan informasi penting ke dalam dan luar organisasi. Komunikasi informasi internal di semua bagian organisasi juga mengizinkan manajemen senior untuk memperlihatkan kepada para pekerja bahwa aktivitas kontrol harus ditanggapi dengan serius.
  Informasi dan komunikasi memiliki tiga prinsip kontrol internal, yaitu:
  - Mempergunakan informasi yang relevan.
  - Berkomunikasi secara internal.
  - Berkomunikasi secara eksternal.

- Aktivitas pengawasan *(monitoring activities)*:
  Merupakan evaluasi secara teratur dan berkelanjutan untuk memverifikasi bahwa setiap bagian dari lima komponen kontrol internal tergolong kontrol yang mempengaruhi prinsip-prinsip dalam setiap komponen dan harus ada serta berfungsi.
  Aktivitas pengawasan memiliki dua prinsip kontrol internal, yaitu:
  - Melaksanakan evaluasi berkelanjutan dan/atau terpisah.
  - Mengevaluasi dan mengkomunikasikan kekurangan.

5.4 Tujuan Sistem Kontrol Internal

Sistem kontrol internal memiliki tujuan yang bermanfaat bagi organisasi, tujuan tersebut adalah sebagai berikut:

- Melindungi seluruh aset organisasi.
- Mendorong peningkatan efektivitas dan efisiensi operasional organisasi.
- Memastikan dan menjaga aktivitas organisasi berjalan sesuai dengan kebijakan yang berlaku.
- Memastikan keakuratan catatan, data dan transaksi akuntansi.
- Mewujudkan laporan keuangan yang akurat, andal dan tepat waktu.
- Memastikan kepatuhan terhadap kebijakan yang telah ditetapkan.
- Mendeteksi kesalahan dan kecurangan dari aktivitas organisasi.
- Meminimalisasi risiko kesalahan dan kecurangan dalam organisasi.
- Mencegah kerugian yang terjadi pada organisasi.
- Memastikan tercapainya tujuan yang telah ditentukan oleh organisasi.
- Memastikan kepatuhan seluruh entitas organisasi terhadap hukum dan peraturan yang berlaku.

5.5 Unsur Sistem Kontrol Internal

Sistem kontrol internal memiliki unsur-unsur penting dalam mencapai tujuan organisasi. Munurut Mulyadi (2014) unsur sistem kontrol internal yaitu meliputi:

- Pemisahan tanggung jawab fungsional dalam struktur organisasi:
  Struktur organisasi merupakan bagan utama dalam pemberian tugas dan tanggung jawab secara fungsional dalam organisasi. Oleh sebab itu harus ada pemisahan fungsi operasional dan penyimpanan dengan fungsi akuntansi. Kemudian setiap fungsi tidak diberikan tanggung jawab penuh dalam melaksanakan semua tahap dalam suatu transaksi, harus dibagi dengan yang lain.
- Wewenang dan prosedur pencatatan transaksi:
  Suatu organisasi harus menata pembagian wewenang otorisasi atas suatu transaksi, karena dalam organisasi setiap transaksi dapat terjadi atas dasar otorisasi dari pejabat yang berwenang, sehingga dapat memberi perlindungan terhadap suatu transaksi akuntansi.
- Praktik sehat dalam aktivitas organisasi:
  Tujuan organisasi tidak dapat tercapai jika praktik aktivitas organisasi tidak dilaksanakan secara sehat. Praktik sehat dalam aktivitas organisasi seperti setiap transaksi dilaksanakan oleh beberapa orang yang berwenang, terdapatnya perputaran jabatan, pengambilan cuti bagi pekerja yang berhak, dan lain-lain.
- Sumber daya manusia yang berkualitas:
  Pelaksanaan praktik sehat dalam aktivitas organisasi harus didukung oleh sumber daya manusia yang berkualitas, sehingga tujuan dari organisasi dapat tercapai. Kualitas sumber daya manusia dapat digambarkan dari kompetensi, keahlian, kejujuran dan tanggung jawab.

5.6 Faktor Yang Mempengaruhi Sistem Kontrol Internal

Sistem kontrol internal dipengaruhi oleh banyak faktor baik dari internal maupun eksternal organisasi. Selain dari lima komponen sistem kontrol internal, secara umum terdapat faktor-faktor yang mempengaruhi sistem kontrol internal (Chen et al., 2017; Chenhall, 2003; Hsiung and Wang, 2014; Hung and Tuan, 2019; Murdayanti et al., 2016; Vu, 2016), diantaranya yaitu:

- Lingkungan ekternal, faktor ini kebanyakan peneliti mengartikan sebagai ketidakpastian. Ketidakpastian merupakan situasi lingkungan di mana probabilitas tidak dapat diprediksi.
- Teknologi, faktor ini merupakan suatu entitas hasil ciptaan melalui perbuatan atau pemikiran untuk mempermudah dalam menyelesaikan suatu masalah sehingga melahirkan suatu nilai tambah.
- Pengetahuan, faktor ini merupakan informasi yang didapat setelah melakukan penginderaan terhadap suatu objek tertentu.
- Kapatuhan, faktor ini merupakan suatu kondisi dimana terdapat ketaatan seseorang terhadap perintah atau aturan yang sudah ditetapkan.
- Kinerja tim, faktor ini merupakan hasil kerja secara kualitas dan kuantitas yang telah dicapai oleh tim dalam melaksanakan perkerjaan sesuai dengan tanggung jawab yang telah dibebankan.
- Struktur organisasi, faktor ini merupakan kerangka kerja formal organisasi yang telah dibagi dan dikelompokan serta dikoordinasikan terhadap seluruh entitas organisasi.
- Ukuran organisasi, faktor ini merupakan gambaran besar atau kecilnya organisasi dan dampaknya terhadap pengelolaan organisasi.

- Strategi organisasi, faktor ini merupakan rencana dalam mengintegrasikan kebijakan organisasi dengan tindakan untuk mencapai tujuan organisasi.
- Budaya organisasi, faktor ini merupakan suatu nilai, kepercayaan, kebiasaan dalam suatu organisasi yang saling berinteraksi dengan struktur formal dalam menghasilkan norma dan perilaku organisasi.
- Manajemen risiko, faktor ini merupakan segala usaha yang dilakukan untuk menghindari terjadinya suatu risiko.
- Kepentingan kelompok, faktor ini merupakan usaha suatu kelompok dalam mempengaruhi kebijakan publik untuk kepentingan anggotanya.
- Kualitas sistem informasi, faktor ini merupakan ukuran kemampuan komponen dalam sistem informasi dalam menghasilkan informasi bagi penggunanya.
- Kualitas pelayanan, faktor ini merupakan landasan utama dalam mengetahui seberapa tingkat kepuasan pengguna sistem.
- Pertumbuhan organisasi, faktor ini merupakan gambaran dari organisasi dalam mengembangkan keahlian dan kompetensinya.

5.7 Kajian Sistem Kontrol Internal

Sistem kontrol internal sudah menjadi topik kajian yang cukup populer dikalangan para peneliti. Kajian sistem kontrol internal yang sudah pernah dikaji meliputi kajian kualitatif dan kuantitatif, pernah dikaji oleh (Gal and Akisik, 2020; Karmila and Hendarsyah, 2019; Wali and Masmoudi, 2020; Yin et al., 2020). Namun sebagian besar kajian sistem kontrol internal yang sudah pernah dikaji, kebanyakan dijadikan sebagai faktor yang mempengaruhi suatu variabel. Berdasarkan pencarian data gi google scholar maka ditemukan variabel-variabel yang dipengaruhi oleh sistem

kontrol internal. Variabel tersebut dapat dirincikan sebagai berikut:

- Kualitas, merupakan suatu tingkat penilaian baik atau buruknya taraf, mutu atau derajat sesuatu. Kajian mengenai variabel ini mayoritas membahas tentang kualitas laporan keuangan, seperti yang telah dilakukan oleh (Aziyah and Yanto, 2022; Mirnawati et al., 2021).
- Kinerja, merupakan hasil kerja secara kualitas dan kuantitas yang telah dicapai dalam melaksanakan perkerjaan sesuai dengan tanggung jawab yang telah dibebankan. Kajian variabel ini banyak mengenai kinerja perusahaan, seperti yang telah dilakukan oleh (Cantika et al., 2021; Hoai et al., 2022).
- Tata kelola, merupakan prinsip yang diterapkan oleh perusahaan dalam memaksimalkan nilai perusahaan, meningkatkan kinerja dan kontribusi perusahaan, serta menjaga keberlangsungan perusahaan untuk jangka panjang. Kajian mengenai variabel ini sudah pernah dilakukan oleh (Erliyanti et al., 2022; Hartono and Nugroho, 2022).
- Nilai informasi, merupakan penilaian suatu informasi secara efektif baik dari segi ketepatan, kebenaran, dapat dibuktikan adanya, tidak menduga duga, dan jelas. Kajian tentang variabel ini sudah dilakukan oleh (Agustin et al., 2020).
- Ketepatan waktu, merupakan ketersediaan informasi bagi pembuat keputusan pada saat diperlukan. Kajian mengenai variabel ini lebih mengarah kepada ketepatan waktu laporan keuangan, seperti yang sudah pernah dilakukan oleh (Noviani and Hendarsyah, 2020).
- Kecurangan, merupakan suatu tindakan penipuan dalam melawan hukum, dilakukan dengan sengaja untuk tujuan tertentu. Kajian tentang variabel ini telah dilakukan oleh (Handoyo and Bayunitri, 2021).
- Sistem informasi, merupakan kumpulan elemen-elemen yang saling berinteraksi dan terintegrasi dalam kegiatan mengumpulkan, memasukkan, memproses, menyimpan,

menyediakan dan mendistribusikan informasi, sehingga menjadi bermanfaat dan dapat digunakan untuk proses pengambilan keputusan dalam suatu organisasi (Hendarsyah et al., 2023). Kajian mengenai variabel ini lebih banyak fokus terhadap penerapan sistem informasi, seperti kajian yang sudah dilakukan oleh (Putri and Hendarsyah, 2020).

- Keandalan, merupakan kemampuan organisasi dalam memberikan pelayanan sesuai dengan yang dijanjikan secara akurat dan terpercaya. Kajian mengenai variabel ini juga banyak mengarah pada keandalan laporan keuangan, seperti yang telah dilakukan oleh (Rimah et al., 2021).
- Efektivitas, merupakan suatu keadaan yang menunjukkan tingkat keberhasilan atau percapaian suatu tujuan. Kajian tentang variabel ini sudah pernah dilakukan oleh (Salahudin et al., 2020; Syamsiah, 2020).
- Akuntabilitas, merupakan gambaran dari suatu keadaan yang dapat dipertanggungjawabkan dan akuntabel. Kajian tentang variabel ini sudah pernah dilakukan oleh (Arfiansyah, 2020).
- Perencanaan, merupakan suatu proses dalam menentukan tujuan pada masa yang akan datang dengan menetapkan tahapan-tahapan yang dibutuhkan dalam mencapainya. Kajian mengenai variabel ini sudah pernah dilakukan oleh (Kricy and Simbel, 2021).
- Penerimaan retribusi, merupakan pungutan daerah sebagai pembayaran atas jasa atau pemberian izin tertentu yang dipungut oleh pemerintah daerah. Kajian mengenai variabel ini telah dilakukan oleh (Haryanti and Hendarsyah, 2021).
- Opini audit, merupakan pernyataan dari auditor terhadap kewajaran suatu laporan keuangan dari entitas yang telah diaudit. Kajian tentang variabel ini sudah dilakukan oleh (Winarto, 2020).
- Audit delay, merupakan waktu penyelesaian proses audit yang diukur dari tanggal penutupan tahun buku, sampai

dengan tanggal diselesaikannya laporan audit secara independen. Kajian mengenai variabel ini telah dilakukan oleh (Sutono et al., 2022).

DAFTAR PUSTAKA

Agustin, R., Cahyono, D., Aulin, G., 2020. Kapasitas Sumber Daya Manusia, Pemanfaatan Teknologi Informasi Dan Pengendalian Intern Terhadap Nilai Informasi Pelaporan Keuangan. Int. J. Soc. Sci. Bus. 4, 116. https://doi.org/10.23887/ijssb.v4i1.24068

Arens, A.A., Elder, R.J., Beasley, M.S., 2007. Auditing and Assurance Services: An Integrated Approach, 12th ed. Pearson College Div, London.

Arfiansyah, M.A., 2020. Pengaruh Sistem Keuangan Desa dan Sistem Pengendalian Intern Pemerintah Terhadap Akuntabilitas Pengelolaan Dana Desa. JIFA (Journal Islam. Financ. Accounting) 3, 67–82. https://doi.org/10.22515/jifa.v3i1.2369

Aziyah, W., Yanto, H., 2022. Pengaruh Sistem Pengendalian Intern dan Komitmen Organisasi terhadap Kualitas Laporan Keuangan Pemerintah Daerah dengan Kompetensi Sumber Daya Manusia sebagai Variabel Moderating. Owner 6, 977–989. https://doi.org/10.33395/owner.v6i1.686

Cantika, S., Mukhzarudfa, M., Zulma, G.W.M., 2021. Pengaruh Partisipasi Anggaran, dan Sistem Pengendalian Intern Pemerintah dengan Komitmen Organisasi Sebagai Variabel Moderasi Terhadap Kinerja Manajerial pada Organisasi Perangkat Daerah (OPD) Di Provinsi Jambi. J. Ilm. Univ. Batanghari Jambi 21, 628. https://doi.org/10.33087/jiubj.v21i2.1518

Chen, J.V., Lu, I.-H., Yen, D.C., Widjaja, A.E., 2017. Factors affecting the performance of internal control task team in high-tech firms. Inf. Syst. Front. 19, 787–802. https://doi.org/10.1007/s10796-015-9621-y

Chenhall, R.H., 2003. Management control systems design within its organizational context: findings from contingency-based research and directions for the future. Accounting, Organ. Soc. 28, 127–168. https://doi.org/10.1016/S0361-3682(01)00027-7

DiNapoli, T.P., 2016. Standards for Internal Control in New York State Government [WWW Document]. osc.state.ny.us. URL https://www.osc.state.ny.us/files/state-agencies/guidance/pdf/agencies-ictf-docs-int-control-stds.pdf

Erliyanti, E., Yuliani, R., Hamdani, H., 2022. Pengaruh kompetensi aparatur pemerintah, partisipasi masyarakat, Sistem Pengendalian Intern Pemerintah (SPIP) dan gaya kepemimpinan terhadap good governance pada pengelolaan keuangan SKPD Kabupaten Balangan. Fair Value J. Ilm. Akunt. dan Keuang. 4, 5252–5265. https://doi.org/10.32670/fairvalue.v4i11.1825

Gal, G., Akisik, O., 2020. The impact of internal control, external assurance, and integrated reports on market value. Corp. Soc. Responsib. Environ. Manag. 27, 1227–1240. https://doi.org/10.1002/csr.1878

Handoyo, B.R.M., Bayunitri, B.I., 2021. The influence of internal audit and internal control toward fraud prevention. Int. J. Financ. Accounting, Manag. 3, 45–64. https://doi.org/10.35912/ijfam.v3i1.181

Hartono, A.B., Nugroho, A.H.D., 2022. Pengaruh pengendalian internal terhadap pencegahan fraud dengan intervening good corporate governance. Fair Value J. Ilm. Akunt. dan Keuang. 4, 1912–1920.

Haryanti, F., Hendarsyah, D., 2021. Efek Sistem Pengendalian Internal Terhadap Penerimaan Retribusi Alat Pemadam Api Ringan. J. Ilm. Akunt. Kesatuan 9, 553–562. https://doi.org/10.37641/jiakes.v9i3.902

Hendarsyah, D., Muktiadji, N., Pasaribu, J.S., Sudirjo, F., Putra, R.B., Pratama, B., Utami, R., Sari, D., Hanindito, G.A., Soamole, M.S., Kusumawardhani, D., Purbaratri, W., Solehudin, S., Fauzan, R., Hartanti, D., Amna, A., Permana, A.A., 2023. Sistem Informasi Manajemen. PT. Global Eksekutif Teknologi, Padang.

Hoai, T.T., Hung, B.Q., Nguyen, N.P., 2022. The impact of internal control systems on the intensity of innovation and organizational performance of public sector organizations in Vietnam: the moderating role of transformational leadership. Heliyon 8, e08954. https://doi.org/10.1016/j.heliyon.2022.e08954

Horngren, C.T., Foster, G., Datar, S.M., Rajan, M., Ittner, C., 2009. Cost Accounting: A Managerial Emphasis, 13th ed. Pearson Prentice Hall, India.

Hsiung, H.-H., Wang, J.-L., 2014. Factors of Affecting Internal Control Benefits under ERP System An Empirical Study in Taiwan. Int. Bus. Res. 7, 31–43. https://doi.org/10.5539/ibr.v7n4p31

Hung, D.T., Tuan, T.T., 2019. Factors affecting the effectiveness of internal control in joint stock commercial banks in Vietnam. Manag. Sci. Lett. 1799–1812. https://doi.org/10.5267/j.msl.2019.6.011

Karmila, K., Hendarsyah, D., 2019. Pengaruh Sistem Informasi Akuntansi Retribusi Boarding Pass Pelabuhan Terhadap Sistem Pengendalian Internal. JAS (Jurnal Akunt. Syariah) 3, 158–173.
https://doi.org/10.46367/jas.v3i2.180

King, A.M., 2011. Internal Control of Fixed Assets: A Controller and Auditor's Guide. John Wiley & Sons, Inc., New Jersey. https://doi.org/10.1002/9781118269107

Kricy, Y.D., Simbel, M., 2021. Pengaruh Sistem Pengendalian Intern Pemerintah (SPIP) terhadap perencanaan dan pelaksanaan anggaran dana desa di Kecamatan Mentaya Hulu, Kabupaten Kotawaringin Timur. J. Environ. Manag. 2, 148–158. https://doi.org/10.37304/jem.v2i2.2943

Mirnawati, M., Nirwana, E., Hendarsyah, D., 2021. Determinan Kualitas Laporan Keuangan Satuan Organisasi Perangkat Daerah. Akurasi J. Stud. Akunt. dan Keuang. 4, 31–44. https://doi.org/10.29303/akurasi.v4i1.73

Mulyadi, M., 2014. Sistem Akuntansi, 4th ed. Salemba Empat, Jakarta.

Murdayanti, Y., Hasanah, N., Shodriati, A., 2016. Factors Affecting The Internal Control Weaknesses of Local Governments. Adv. Sci. Lett. 22, 1643–1646. https://doi.org/10.1166/asl.2016.6712

Noviani, A., Hendarsyah, D., 2020. Ketepatan Waktu Pelaporan Keuangan: Sistem Pengendalian Internal dan Sistem Informasi Pengelolaan Keuangan Daerah. J. AKUNTANSI, Ekon. dan Manaj. BISNIS 8, 206–213. https://doi.org/10.30871/jaemb.v8i2.2477

Pfister, J.A., 2009. Managing Organizational Culture for Effective Internal Control: From Practice to Theory. Physica-Verlag, Berlin–Heidelberg.

Presiden RI, 2008. Peraturan Pemerintah Republik Indonesia Nomor 60 Tahun 2008, Tentang Sistem Pengendalian Intern Pemerintah. Indonesia.

Putri, W.S., Hendarsyah, D., 2020. Pengaruh Sistem Pengendalian Internal Terhadap Penerapan Sistem Komputerisasi Haji Terpadu (SISKOHAT): Studi Pada Kantor Kementerian Agama Kabupaten Bengkalis. Inovbiz J. Inov. Bisnis 8, 52. https://doi.org/10.35314/inovbiz.v8i1.1252

Rama, D. V., Jones, F.L., 2005. Accounting Information Systems: A Business Process Approach, 2nd ed. Cengage Learning, Massachusetts.

Reeve, J.M., Warren, C.S., Duchac, J.E., 2009. Principles of Financial and Managerial Accounting. South-Western, Nashville.

Rimah, I., Harmono, H., Sihwahjoeni, S., 2021. Pengaruh Tingkat Kompetensi Sumber Daya Manusia, Teknologi Informasi, Pengendalian Intern Dan Pengawasan Keuangan Terhadap Keandalan Pelaporan Keuangan Kepolisian Resort Provinsi Jawa Timur. J. Akunt. Trisakti 8, 287–308. https://doi.org/10.25105/jat.v8i2.9844

Salahudin, I., Nugroho, G.W., Kartini, T., 2020. Sistem Informasi Akuntansi dan Pengendalian Internal terhadap Efektivitas Penjualan. Budg. J. Business, Manag. Account. 2, 194–207. https://doi.org/10.31539/budgeting.v2i1.1228

Sawyer, L.B., Dittenhofer, M.A., Scheiner, J.H., 2003. Sawyer's Internal Auditing: The Practice of Modern Internal Auditing. Inst of Internal Auditors, Florida.

Schandl, A., Foster, P.L., 2019. COSO Internal Control - Integrated Framework: An Implementation Guide for the Healthcare Provider Industry. The Committee of Sponsoring Organizations of the Treadway Commission (COSO), Durham.

Shim, J.K., 2011. Internal Control and Fraud Detection. Global Professional Publishing, London.

Sutono, S., Sulistiyo, H., Ardi, B.K., 2022. Pengaruh ukuran atau skala perseroan, pergantian auditor dan sistem pengendalian intern terhadap audit delay pada perseroan yang tercatat di Bursa Efek Indonesia. Fair Value J. Ilm. Akunt. dan Keuang. 5, 1848–1855. https://doi.org/10.32670/fairvalue.v5i4.2656

Swinkels, W.H.A., 2012. Exploration of a theory of internal audit: A study on the theoretical foundations of internal audit in relation to the nature and the control systems of Dutch public listed firms. Eburon Academic Publishers, Delft, Netherlands.

Syamsiah, N., 2020. Sistem Pengendalian Intern Terhadap Efektivitas Pemberian Kredit Pada PT. Bank Rakyat Indonesia (Persero) Tbk. Cabang Marisa. AkMen J. Ilm. 17, 501–508. https://doi.org/10.37476/akmen.v17i3.1010

Vu, H.T., 2016. The Research of Factors Affecting the Effectiveness of Internal Control Systems in Commercial Banks-empirical Evidence in Viet Nam. Int. Bus. Res. 9, 144. https://doi.org/10.5539/ibr.v9n7p144

Wali, S., Masmoudi, S.M., 2020. Internal control and real earnings management in the French context. J. Financ. Report. Account. 18, 363–387. https://doi.org/10.1108/JFRA-09-2019-0117

Winarto, H., 2020. Pengaruh Pengendalian Internal Dan Bukti Audit Terhadap Opini Audit (Studi Empiris Di Kantor Akuntan Publik Di Jakarta Timur). J. Akunt. dan Bisnis Krisnadwipayana 7, 1–13. https://doi.org/10.35137/jabk.v7i1.374

Yin, M., Zhang, J., Han, J., 2020. Impact of CEO-board social ties on accounting conservatism: Internal control quality as a mediator. North Am. J. Econ. Financ. 52, 101172. https://doi.org/10.1016/j.najef.2020.101172

BAB 6
KERANGKA KONTROL MANAJEMEN DAN APLIKASI

6.1 Pendahuluan

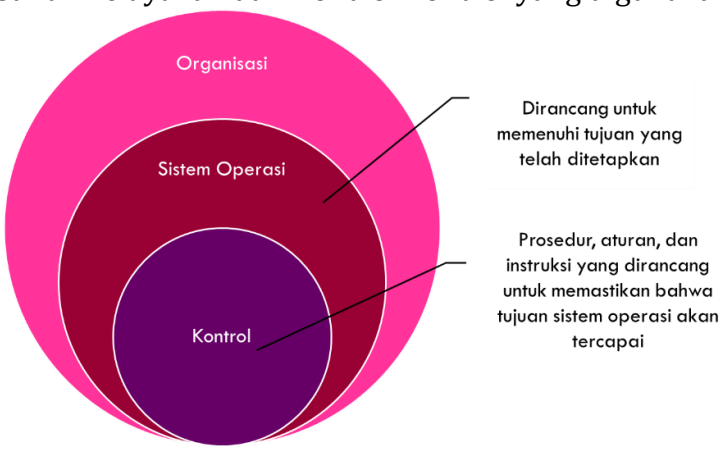
Penerapan sistem informasi merupakan bentuk strategi bagi organisasi dalam mencapai tujuan bisnis. Namun dalam penerapannya, sistem informasi sering mengalami keterbatasan dan kendala yang berdampak pada pencapaian tujuan bisnis organisasi. Oleh karena itu dalam penerapan sistem informasi juga diperlukan Audit Sistem Informasi (SI) untuk menjaga dan memastikan bahwa sistem informasi masih berada pada jalurnya dalam membantu organisasi mencapai tujuan bisnis.

Audit SI merupakan suatu peran dalam organisasi yang berguna untuk mengevaluasi keamanan aset, integritas data, efisiensi sistem, dan efektivitas dalam sistem informasi terkomputerisasi (Sari et al., 2017). Audit ini dibutuhkan oleh organisasi dikarenakan beberapa faktor yang pada akhirnya menjadi sumber risiko dari penerapan sistem informasi. Salah satu tujuan dari audit sistem informasi adalah sebagai bentuk pengamanan aset serta menjaga efektifvitas dan efisiensi sistem dari berbagai ancaman yang dapat menimbulkan risiko buruk dari penerapan sistem informasi. Faktor-faktor yang menyebabkan pentingnya audit SI adalah sebagai berikut (Riyanarto Sarno, 2009):

1. Ancaman kehilangan data.
2. Ancaman yang ditimbulkan sumber daya manusia seperti kesalahan dalam pengelolaan data.
3. Ancaman kerusakan hardware karena tidak adanya kontrol/pengendalian

4. Nilai infrastruktur SI/TI yang sangat mahal baik perangkat keras dan perangkat lunak
5. Biaya yang tinggi apabila ada kerusakan pada infrastruktur SI/TI
6. Kebutuhan keamanan informasi atau *privacy* data organisasi
7. Kebutuhan untuk mengontrol penggunaan perangkat keras dan perangkat lunak.

Auditor sistem informasi secara khusus berfokus pada evaluasi keandalan atau efektivitas dari kontrol atau pengendalian dari sebuah sistem (Musantono et al., 2020). Kontrol merupakan sistem yang mencegah, mendeteksi, atau memperbaiki situasi yang tidak teratur. Dalam pengertian sederhana penerapan SI membutuhkan kontrol untuk mengendalikan sistem informasi sesuai fungsi dan tujuan diterapkannya sistem informasi tersebut. Sedangkan audit memastikan kelayakan dari kontrol-kontrol yang digunakan.



Gambar 6.1. Hubungan Kontrol dan Operasional

Ada banyak bentuk kontrol, bisa dalam bentuk prosedur atau aturan. Terdapat tiga aspek penting dalam kontrol yang harus dipahami, yaitu (Sanyoto Gondodiyoto, 2007):

- Kontrol adalah suatu sistem atau dengan kata lain merupakan sekumpulan komponen yang saling berhubungan dan bekerjasama dalam mencapai tujuan bersama.
- Fokus dari kontrol adalah penanganan situasi tidak teratur yang dapat muncul ketika ada masukan (inputan) yang seharusnya tidak masuk ke dalam sistem.
- Kontrol digunakan untuk mencegah, mendeteksi dan memperbaiki situasi yang tidak teratur, sebagai contoh :
    a. *Preventive control*: instruksi yang diletakkan pada dokumen untuk mencegah kesalahan masukan data. Contoh: kebijakan, pedoman, alur kerja, sop, instruksi
    b. *Detective control*: kontrol yang diletakkan pada program yang berfungsi mendeteksi kesalahan pemasukan data. Contoh: peringatan kesalahan username password, peringatan ketika salah input data
    c. *Corrective control*: program yang dibuat khusus untuk memperbaiki kesalahan pada data yang mungkin timbul akibat gangguan pada jaringan, komputer ataupun kesalahan user yang tidak terdeteksi pada *Detective control*.

Secara umum, kontrol berfungssi untuk mengurangi kerugian yang mungkin terjadi akibat kejadian yang tidak diharapkan dari jalannya sebuah sistem. Tugas auditor adalah memeriksa dan menentukan apakah kontrol telah berfungsi seperti yang diharapkan yaitu dapat mencegah peristiwa-peristiwa yang tidak diharapkan. Auditor harus dapat memastikan bahwa setidaknya ada satu kontrol yang

dapat mengatasi risiko ketika risiko tersebut terjadi. Beberapa kontrol yang digunakan dalam audit sistem informasi adalah kontrol manajemen dan kontrol aplikasi.

6.2 Kontrol Manajemen

Kontrol manajemen atau biasa dikenal dengan kontrol umum (*General Control*) merupakan kontrol yang berkaitan dengan seluruh kegiatan komputerisasi pada suatu organisasi (Reza Aminy, 2017). Kontrol ini merupakan sudut pandang atau perspektif dari manajemen. Maksud dari perspektif manajemen adalah kontrol yang tidak berkaitan langsung dengan suatu aplikasi tertentu. Sebagai contoh adalah ketentuan masuk ruang server dilarang membawa makanan atau minuman, ruang server disertai APAR (Alat Pemadam Api Ringan) dan CCTV merupakan bentuk pengandalian umum dimana ketentuan-ketentuan tersebut tidak langsung dengan operasional sistem pada server.

6.2.1 Kategori Kontrol Manajemen

Kontrol Manajemen (*General control)* sering disebut juga pengendaliam umum merupakan kontrol keseluruhan yang memastikan operasional yang efektif dari prosedur yang telah ditetapkan (Theodorus M. Tuanakotta, 2019). Dalam audit sistem informasi kontrol umum sangat diperlukan bagi organisasi yang belum pernah melakukan audit area ST/TI sebelumnya atau sudah pernah namun cukup lama sekali. Pada audit TI umum, dilakukan pemeriksaan terhadap semua area secara umum dengan tujuan sebagai berikut (Sanyoto Gondodiyoto, 2007):

- Mendeteksi masalah yang lebih besar/ utama
- Mendapatkan kesan secara keseluruhan (overall impression)

- Mengetahui tentang area/proses yang perlu diaudit lebih rinci

Jika melihat dari tujuan tersebut maka muncul pertanyaan apa saja proses yang harus di audit?. Tentu saja untuk menjawab pertanyaan ini maka perlu mengetahui kategori kontrol umum. Banyak sekali pendapat terkait kategori kontrol umum. Ikatan Akuntan Indonesia (IAI) mendefinisikan kategori kontrol umum sebagai berikut (Sanyoto Gondodiyoto, 2007):

1. Kontrol Organisasi dan Manajemen
2. Kontrol Terhadap Pengembangan Pemeliharaan Sistem Aplikasi
3. Kontrol terhadap Operasi Sistem
4. Kontrol terhadap Perangkat Lunak Sistem
5. Kontrol terhadap Keamanan TI

Ada pula pendapat yang menjelaskan bahwa kontrol umum berfokus pada pengolahan informasi secara keseluruhan yang meliputi kontrol terhadap operasi pusat data, akuisisi dan pemeliharaan parangkat lunak sistem, *access security*, pengembangan dan pemeliharaan pengembangan sistem (Yanuar E. Restianto & Icuk Rangga Bawono, 2010). Banyak sekali pendapat yang menjelaskan terkait kategori pada kontrol manajemen. Dari sekian banyak pendapat tersebut dapat ditarik kesimpulan bahwa setidaknya kontrol umum meliputi (Sanyoto Gondodiyoto, 2007):

- Kontrol top manjemen (*top management controls*) yang berkaitan dengan kontrol manajemen system informasi
- Kontrol manajemen pengembangan system (*system development management control*) yang berkaitan

dengan manajemen program (*programming management controls*)

- Kontrol manajemen sumber data (*Data resources management controls*)
- Kontrol manajemen operasi (*Operations management controls*)
- Kontrol manajemen keamanan (*Security administration managemen controls*)
- Kontrol manajemen jaminan kualitas (*Quality assurance management controls*)

6.2.2 Jenis Kontrol Manajemen

Setiap kategori yang ada pada kontrol umum tentu memiliki ruang lingkup tersendiri. Ruang lingkup ini harus dipahami oleh auditor agar auditor dapat mengetahui objek apa saja yang perlu di periksa dalam pelaksanaan audit umum. Pada subbab sebelumnya telah dijelaskan bahwa setidaknya ada enam kategori dalam audit kontrol manajemen. Dari keenam kategori tersebut terdapat jenis-jenis kontrol di dalamnya. Untuk lebih jelasnya kategori dan jenis kontrol manajemen telah dijabarkan seperti yang ada pada Tabel 6.1.

Tabel 6.1. Ruang Lingkup Kontrol Manajemen

Kategori Kontrol	Jenis-jenis Kontrol
Kontrol top manjemen	• Keterlibatan dan tanggung jawab top manajemen terhadap TI • Pengendalian atas struktur organisasi • Perencanaan, pengangggaran dan sistem pembebanan pada pengguna (*end user)*
Kontrol	• Pertisipasi manajemen dan pengguna

Kategori Kontrol	Jenis-jenis Kontrol
manajemen pengembangan	• Ketersediaan standar dan prosedur pengembangan
system	• Manajemen proyek • Pengujian sistem dan konversi • Monitoring dan evaluasi setelah implementasi • Pengendalian pemeliharaan sistem (prosedur otorisasi perubahan sistem, keterlibatan dan persetujuan pengguna akan perubahan sistem, adanya standar dan prosedur melakukan perubahan, pembatasan akses terhadap *source code* sistem)
Kontrol manajemen sumber data	• Kemudahan akses dan pertukaran data antar pengguna • Ketersediaan data • Sistem penyimpanan data yang efisien dan aman • Kemudahan modifikasi data
Kontrol manajemen operasi	• Pemisahan fungsi departemen TI dan non-TI • Pemisahan tugas dan peran dalam departemen TI • Pengendalian personil • Pengendalian perangkat keras dan jaringan • Manajemen operasi
Kontrol manajemen keamanan	• Teknologi pendukung keamanan • Proses penyusunan kebijakan keamanan • Pengguna sistem (End user, staf, departemen TI, manajemen puncak)

Kategori Kontrol	Jenis-jenis Kontrol
Kontrol manajemen jaminan kualitas	• Standar kualitas sistem informasi • Standar pengembangan, implementasi, operasional dan pemeliharaan

6.3 Kontrol Aplikasi

Kontrol Aplikasi atau pengendalian aplikasi (*Application Control*) sering juga disebut kontrol khusus merupakan kontrol yang dirancang secara khusus untuk aplikasi tertentu (Dian Pratiwi & Firdaus Hamta, 2015). Seringkali kontrol ini disebut juga kontrol transaksi. Hal ini dikarenakan kontrol ini dirancang sesuai dengan transaksi pada aplikasi tertentu. Sebagai contoh nasabah akan melakukan transfer melalui aplikasi *mobile banking*, maka akan diminta memasukkan PIN transaksi terlebih dahulu atau ketika mahasiswa akan memilih mata kuliah pada sistem informasi akademik sistem akan memeriksa apakah jumlah sks yang diambil memenuhi batas maksimal sesuai ketentuan jumlah sks. Pada umumnya jika mahasiswa memiliki IPK (Indeks Prestasi Kumulatif) dibawah 3 maka sks maksimal adalah 18 sks maka ketika mahasiswa memilih mata kuliah dan sks melebihi batas yang ditentukan maka sistem akan menolak. Kontrol berupa PIN dan batas pengambilan SKS merupakan bentuk kontrol aplikasi pada sistem tertentu tidak untuk sistem lain.

6.3.1 Kategori Kontrol Aplikasi

Kontrol aplikasi sangat berbeda dengan kontrol umum yang ditetapkan oleh pimpinan. Hal ini dikarenakan kontrol aplikasi dirancang oleh masing-masing sistem atau aplikasi. Kontrol aplikasi merupakan sistem pengendalian internal pada sistem informasi berbasis teknologi yang

berkaitan dengan pekerjaan/kegiatan/ aplikasi tertentu dimana setiap aplikasi memiliki karakteristik dan kebutuhan kontrol yang berbeda-beda (Cantika, 2019). Sebagai contoh aplikasi *mobile banking* tentu akan menghadapi risiko dan kebutuhan pengendalian yang berbeda dengan sistem informasi kepegawaian. Dari contoh ini maka timbul pertanyaan *apa saja yang termasuk dalam kontrol aplikasi*?. Pada dasarnya kontrol aplikasi memiliki beberapa kategori antara lain yaitu:

1. Kontrol batas sistem atau *boundary controls*
2. Kontrol masukan atau *input controls*
3. Kontrol proses pengolahan data atau *process controls*
4. Kontrol keluaran atau *output controls*
5. Kontrol file/basis data atau *files/ database controls*
6. Kontrol komunikasi aplikasi atau *communication controls*

6.3.2 Jenis Kontrol Aplikasi

Pada subbab sebelumnya dijelaskan bahwa setidaknya ada 6 kategori kontrol aplikasi. Perlu diketahui bahwa dari keenam kategori kontrol tersebut tentu memiliki ruang lingkup yang dapat menjadi acuan bagi auditor ketika akan melakukan audit aplikasi. Untuk lebih jelasnya dapat melihat Tabel 6.2

Tabel 6.2. Ruang Lingkup kontrol Aplikasi

Kategori Kontrol	Jenis-jenis kontrol
1. *Boundary Control* (Kontrol Batasan)	• Hak akses ke sistem aplikasi • Identitas Pengguna dan Otentikasi
2*. Input Control* (Kontrol Masukan)	• Otorisasi dan validasi masukan • Transmisi dan konversi data • Penanganan kesalahan
3. *Process Control*	• Pemeliharaan ketepatan data

(Kontrol proses)	• Pengujian terjadwal atas batasan dan kesesuaian pemrosesan
4. *Output Control* (Kontrol Keluaran)	• Rekonsiliasi output • Review dan pengujian hasil pengolahan • Distribusi output • Penyimpanan catatan (*output*)
5. *Database Control* (Kontrol Basis Data)	• Akses basis data • Integritas data
6. *Communication Control* (Kontrol Komunikasi Aplikasi)	• Pengendalian kegagalan unjuk kerja • Gangguan komunikasi

Perlu diketahui bahwa kontrol aplikasi sangat penting. Mengingat bahwa saat ini hampir seluruh organisasi telah menjalankan operasionalnya menggunakan sistem informasi. Sedangkan setiap sistem informasi akan memiliki ancaman dan kerentanan yang berbeda. Oleh karena itu kontrol aplikasi dapat juga dikelompokkan dalam kontrol preventif, kontrol detektif dan kontrol korektif. Hal ini diperlukan agar dapat mengurangi (preventif/detektif) risiko pada sistem yang digunakan. Namun jika ternyata risiko yang dikuatirkan terjadi juga maka perlu kontrol korektif agar dampak yang dihasilkan dapat diminimalisir sekecil mungkin.

6.4 Instrumen Audit Berbasis Risiko

Dalam audit tentu diperlukan sebuah lembar keja audit atau instrumen audit. Pembentukan instrumen audit merupakan bagian dari fase perencanaan audit. Tentu saja ini juga berlaku dalam audit sistem informasi. Oleh karena

itu audit harus membuat instrumen audit mengacu pada kriteria-kriteria yang akan digunakan dalam audit. Hal ini diperlukan agar auditor lebih mudah ketika ingin melakukan audit serta menghindari kemungkinan auditor menanyakan hal-hal diluar kriteria. Dalam subbab ini telah disajikan beberapa contoh instrumen audit sistem informasi berbasis risiko baik kontrol umum dan kontrol aplikasi.

6.4.1 Instrumen Kontrol Manajemen

Dalam melakukan audit, auditor harus mampu menggali informasi pada auditee terkait kategori dan jenis kontrol yang digunakan. Dalam kontrol manajemen terdapat beberapa kategori kontrol yang harus digali oleh auditor. Untuk memudahkan proses penggalian informasi tersebut maka auditor harus menyiapkan instrumen pertanyaan sebagai pedoman dalam pelaksanaan audit. Pada Tabel 6.3 telah dipaparkan beberapa contoh instrumen pertanyaan dari setiap kategori yang dapat digunakan oleh auditor.

Tabel 6.3. Instrumen Pertanyaan Audit *General Control*

1. Kontrol Top Manjemen
• Jika terjadi perubahan pada teknologi yang direncanakan, apa strategi TI organisasi? • Apakah pimpinan memahami tanggung jawab dan perannya dalam konteks risiko perusahaan dan kesadaran akan bertekonologi? • Apakah komite audit memahami risiko TI, dan apakah komite audit dapat melihatnya dalam konteks risiko perusahaan? • Bagaimana eksekutif TI menentukan jumlah SDM yang dibutuhkan untuk TI?
2. Kontrol Manajemen Pengembangan System

• Bagaimana proyek-proyek disetujui dalam organisasi? • Bagaimana proyek-proyek dimulai dan dikelola dalam organisasi? • Jika vendor terlibat dalam pengembangan proyek, bagaimana proses administrasi kotraknya? • Apakah ada laporan status bulanan?
3. Kontrol Manajemen Sumber Data
• Apakah engguna dapat berbagai data? • Apakah data dapat diakses kapan saja, diamana saja dan dapat tersedia dalam bentuk apapun? • Apakah data dapat dimodifikasi dengan mudah oleh pengguna?
4. Kontrol Manajemen Operasi
• Apakah kegiatan yang dilaksanakan TI agar sejalan dengan bisnis? • Bagaimana TI mengatur biayanya? • Apakah TI melakukan penilaian risiko secara berkala?
5. Kontrol Manajemen Keamanan
• Apakah prosedur atau kebijakan terdapat *disaster recovery plan* jika terjadi bencana? • Apakah setiap komputer telah dilengkapi dengan program anti virus? • Apakah setiap computer telah dilakukan scan virus secara rutin? • Apakah terdapat prosedur pembersihan untuk barang-barang yang mudah terbakar di ruang aset sistem informasi?
• Apakah setiap tamu yang datang ke ruang operasional TI diwajibkan melapor?

6. Kontrol Manajemen Jaminan Kualitas
• Apakah TI mempunyai ukuran keberhasilan untuk menilai kinerjanya? • Apakah organisasi TI melaksanakan kajian mengenai kepuasan pengguna mengenai hasil dan biaya proyek TI? • Apakah ada proses untuk membatalkan proyek-proyek yang tujuannya tidak tercapai?

6.4.2 Instrumen Kontrol Aplikasi

Sama halnya dengan kontrol umum, dalam kontrol aplikasi auditor harus mampu memeriksa para aplikasi yang digunakan oleh auditee. Namun kontrol aplikasi sedikit berbeda dengan kontrol manajemen dikarenakan kontrol aplikasi sifatnya teknis. Oleh karena itu untuk memudahkan auditor dalam pemeriksaan kontrol aplikasi, auditor perlu memahami instrumen pertanyaan dalam audit aplikasi. Pada tabel 6.4 telah dipaparkan beberapa contoh instrumen pertanyaan dari setiap kategori yang dapat digunakan oleh auditor dalam audit aplikasi.

Tabel 6.4. Instrumen Pertanyaan Audit *Application Control*

1. Boundary Control (Kontrol Batasan)
• Apakah sistem aplikasi dilengkapi dengan login akses seperti username dan password? • Apakah password yang diketik tidak terlihat (invisible)? • Apakah sistem aplikasi menampilkan pesan jika verifikasi login tidak valid? • Apakah sistem aplikasi hanya dapat diakses oleh orang-
• orang yang terotorisasi? • Apakah telah terdapat batasan-batasan terhadap

kewenangan user dalam mengakses aplikasi? • Apakah sistem aplikasi membatasi ukuran field (panjang maksimal) terhadap login akses (username, password)? • Apakah sistem aplikasi dilengkapi dengan pembatasan sistem umur password?
2. Input Control (Kontrol Masukan)
• Apakah kesalahan yang telah terlanjur diinput dapat didelete? • Saat terlanjur salah dalam edit data, apakah dapat cek data sebelumnya? • Apakah terdapat menu konfirmasi terhadap data sebelum disimpan?
3. Process Control (Kontrol proses)
• Apakah dalam proses penginputan sistem aplikasi menampilkan pesan kesalahan atau error message jika petugas input melakukan kesalahan input? • Apakah delete atau update hanya dapat dilakukan oleh user tertentu yang diberi otoritas? • Apakah penggunaan bahasa, desain warna dan tampilan layar sistem aplikasi sudah baik dan mudah dimengerti, yang mana akan mengurangi kesalahan penginputan data? • Apakah fasilitas menu dalam sistem aplikasi sudah memenuhi kebutuhan user?
4. Output Control (Kontrol Keluaran)
• Apakah sistem aplikasi dapat menghasilkan laporan yang dibutuhkan? • Apakah hasil laporan dapat langsung dicetak saat itu juga?
• Apabila tidak bisa langsung dicetak, apakah ada solusi lain agar laporan tetap bisa tersampaikan?

• Apakah telah dilakukan pemeriksaan ulang setelah laporan tersebut dicetak? • Apakah laporan dari sistem aplikasi dapat dicetak kembali jika ditemukan kesalahan? • Apakah laporan dari sistem aplikasi didistribusikan kepada pihak yang berkepentingan? • Apakah dalam setiap laporan yang dihasilkan sudah tercantum halaman, judul, tanggal, periode, nomor urut, dan jam laporan tersebut dicetak?
5. Database Control (Kontrol Basis Data)
• Apakah sudah terdapat pengendalian terhadap akses ilegal? • Apakah terdapat pengendalian terhadap batasan sistem hak akses agar tidak terjadinya penyalahgunaan database? • Apakah terdapat pilihan untuk hak akses saat admin menambahkan operator untuk akun baru?
6. Communication Control (Kontrol Komunikasi Aplikasi)
• Apakah hardware dan software yang digunakan sekarang cukup memadai untuk mendukung transmisi atau saluran link? • Apakah media transmisi yang digunakan pada sistem aplikasi berjenis bounded media? • Apakah media transmisi yang digunakan pada sistem aplikasi berjenis unbounded media (seperti satelite, microwave, radio frekuensi atau infrared)? • Apakah sistem aplikasi POS dapat diakses dimana saja?

DAFTAR PUSTAKA

Cantika, W. N. (2019). *Pengendalian Audit Sistem Informasi* (pp. 1–10) [Preprint]. Open Science Framework. https://doi.org/10.31219/osf.io/ngqxh

Dian Pratiwi & Firdaus Hamta. (2015). Penerapan Pengendalian Umum dan Pengendalian Aplikasi Dalam Pencapaian Tujuan Pembelian Pada Pt Usda Serojajaya Batam. *Jurnal Equilibiria*, *2*(1), 1–8. https://doi.org/10.33373/jeq.v2i1.748

Musantono, A. E., Wa, B. S., & Nasiri, A. (2020). Evaluasi Pengendalian Aplikasi Pada Sistem Informasi Manajemen Keuangan Menggunakan Framework COSO. *Jurnal Informa : Jurnal Penelitian dan Pengabdian Masyarakat*, *5*(3), 80–85. https://doi.org/10.46808/informa.v5i3.151

Reza Aminy. (2017). *Audit Sistem Informasi: Lima Aspek Audit Sistem Informasi*. Mega Indo Komunika.

Riyanarto Sarno. (2009). *Audit Sistem Informasi & Teknologi Informasi*. ITS Press.

Sanyoto Gondodiyoto. (2007). *Audit Sistem Informasi + Pendekatan COBIT* (Revisi). Mitra Wacana Media.

Sari, W. D., Papilaya, F. S., & Manuputty, A. D. (2017). Evaluasi Pengendalian Aplikasi pada Sistem Informasi Keuangan dan Akuntansi Satya Wacana (SIKASA). *Jurnal Sistem Informasi Indonesia*, *2*(1), 1–13.

Theodorus M. Tuanakotta. (2019). *Audit Internal Berbasis Risiko*. Salemba Empat.

Yanuar E. Restianto & Icuk Rangga Bawono. (2010). *Audit Sistem Informasi menggunakan ActiveData for Excel*. Andi Offset.

BAB 7
PERENCANAAN & MANAJEMEN AUDIT

7.1 Pendahuluan

Ketika kita membuat perencanaan sebenarnya yang kita lakukan yaitu memikirkan keseluruhan kesulitan yang mungkin akan dihadapi kedepannya. Artinya si pembuat perencanaan harus memahami aktivitas yang harus dikerjakan dari awal sampai akhir. Disinilah tingkat kesulitan membuat sebuah perencanaan yang baik. Ada kalimat motivasi yang mengatakan, ”gagal membuat perencanaan sama dengan merencanakan kegagalan.”

Pada bab ini kita akan membahas tahap perencanaan dan manajemen audit sebagai bagian dari proses audit sistem informasi atau teknologi informasi.

7.2 Perencanaan & Manajemen Audit

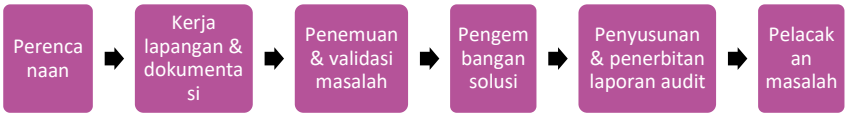
Perencanaan dan manajemen audit mencakup semua aktivitas yang diperlukan untuk memastikan bahwa proses audit yang direncanakan oleh auditor dapat dilaksanakan secara lengkap dan efisien untuk memenuhi tujuan audit organisasi. Auditor yang dipergunakan dapat merupakan auditor dari dalam organisasi maupun auditor dari luar organisasi. Merencanakan audit secara konseptual mirip dengan merencanakan proyek TI atau inisiatif lain yang ditentukan secara terpisah, di mana audit biasanya memiliki tanggal awal dan akhir yang dimaksudkan, mengharuskan organisasi untuk menugaskan personel yang tepat dan

sumber daya yang memadai, dan menghasilkan keluaran yang nyata dalam bentuk dokumentasi, temuan, dan rekomendasi.

Perencanaan audit individual diinformasikan oleh, tetapi terpisah dari, aktivitas pengembangan rencana audit yang lebih luas dalam program audit internal. Dalam konteks audit tunggal, kebutuhan akan audit telah ditentukan, demikian juga dengan prioritas relatifnya, sehingga perencanaan menekankan kegiatan persiapan yang, bila dilakukan dengan benar, memfasilitasi keberhasilan pencapaian tujuan organisasi dan memastikan bahwa tim audit memiliki semua yang diperlukan untuk mulai melaksanakan audit. Perencanaan audit tunggal juga mempertimbangkan pedoman umum dan masukan tentang ruang lingkup, persyaratan sumber daya, garis waktu, protokol, dan informasi pendukung dan menentukan kebutuhan eksplisit, tenggat waktu, kriteria audit, dan persyaratan pembuktian dan prosedural. Selama perencanaan audit, organisasi juga menetapkan ekspektasi tentang laporan audit atau produk kerja lain yang akan disampaikan pada akhir audit. (Gantz Stephen D, 2014)
Gambar 1. Menunjukan enam tahapan dasar dalam proses audit sistem informasi atau teknologi informasi yang dapat dirinci sebagai berikut: 1) Tahap Merencanakan audit; 2) Tahap Kerja lapangan dan dokumentasi; 3) Tahap Identifikasi dan validasi masalah; 4) Tahap Pengembangan solusi; 5) Tahap Penyusunan dan penerbitan laporan audit; serta 6) Tahap Pelacakan masalah.

Merencanakan bagian yang di audit wajib ditentukan diawal proses. Hal ini akan sangat menentukan keberhasilan dari pekerjaan tim auditor. Potensi ketidakberhasilan dapat terjadi ketika tahap perencaan audit ini dilakuan dengan keliru atau tidak tepat. Apakah yang harus dikerjakan pada tahap perencaan audit ? Pada tahap perencaan audit maka

pihak manajemen harus menetapkan maksud pelaksanaan audit serta menentukan batasan atau ruang lingkup audit.



Gambar 7.1. Tahapan dasar Proses Audit
(Sumber : *IT Auditing*)

Pada tahap perencaan ini perlu dilakukan tindakan penelitian, pemikiran serta pertimbangan dengan cermat dengan memperhatikan:

- Catatan informasi dari manajer audit

  Tim auditor wajib memperoleh informasi yang valid dan sahih sebagai alasan perlunya penjadwalan audit. Informasi yang valid dan sahih tersebut dapat berupa pernyataan lisan yang disampaikan manajer TI, dapat juga berupa permasalah yang diketahui tim auditor dilingkup tersebut. Pada dasarnya tim auditor wajib mendapatkan delegasi informasi kunci dari manager TI untuk menyusun serangkaian langkah audit.
- Penelitian awal

  Penelitian awal wajib dilakukan oleh tim audit dalam ruang lingkup area yang akan diaudit. Penelitian awal ini wajib dilakukan untuk mengetahui dengan cermat apa yang akan dilakukan. Adapun yang dapat dilakukan pada tahap penelitian awal yaitu wawancara dan penelusuran dokumen yang tersedia dalam ruang lingkup area audit. Melalui wawancara dan penelusuran dokumen yang tersedia maka tim auditor dapat memperoleh latar belakang proses bisnis yang dilakukan, memahami area yang akan di audit serta dapat menentukan tingkatan resiko dari proses bisnis pada bagian yang akan di audit. Harus juga disadari bahwa tingkatan resiko dari proses bisnis akan

berkaitan dengan *stakeholders* secara internal maupun eksternal.

- Permintaan pelanggan

  Pelanggan yang meminta proses audit perlu menyadari perannya sebagai stakeholders internal yang mengharapkan keberhasilan dari proses audit. Keberpihakan pada keberhasilan proses audit atas dasar tanggungjawab kepemilikan proses bisnis yang akan di audit. Dengan demikian diperoleh kerjasama yang optimal dengan tim audit. Perlu digarisbawahi bahwa wawancara dengan pelanggan merupakan tahapan pada penelitian awal untuk perencanaan proses audit. Melalui wawancara dengan pelanggan maka diperoleh masukan yang kemudian harus diselaraskan juga secara objektif oleh auditor tentang penilaian resikonya. Sehingga ruang lingkup audit dapat ditentukan batasannya. Walaupun tidak selalu auditor dapat mempergunakan saran dari pelanggan. Pada dasarnya menerima masukan dari pelanggan untuk di daftarkan pada rencana audit dapat menimbulkan keberpihakan pelanggan pada proyek audit sehingga menjamin adanya komunikasi yang terbuka dan jujur, dimana keberhasilan proses audit menjadi yang utama.

- *Checklis* standar audit

  Menyederhanakan pelaksanaan proses audit dapat dilakukan dengan menggunakan *Checklis* standar pada bagian yang akan diaudit. Departemen audit pada masing-masing perusahan kemungkinan telah mempunyai *Checklis* standar audit yang terus menerus dievaluasi dan juga direvisi. *Checklis* standar audit mempunyai beberapa manfaat, yaitu :

  1) Memastikan bahwa audit dilakukan dengan cara yang konsisten dan sesuai dengan standar yang telah ditetapkan. Dengan memiliki daftar item yang harus diperiksa dan dicatat, auditor dapat memastikan

bahwa tidak ada hal yang terlewatkan dan audit dilakukan secara komprehensif.

2) Meminimalkan risiko kehilangan informasi atau data yang penting. Dengan memiliki daftar item yang harus diperiksa, auditor dapat memastikan bahwa semua informasi dan data penting telah dicatat dan diperiksa dengan benar.
3) Memudahkan pengumpulan dan analisis data. Dengan menggunakan checklist standar audit, data yang diperoleh dari audit dapat dikumpulkan dengan mudah dan dianalisis dengan cepat.
4) Memperkuat integritas audit. Dengan menggunakan checklist standar audit, auditor dapat memastikan bahwa audit dilakukan dengan integritas yang tinggi dan tidak ada upaya untuk menghindari atau menyembunyikan informasi yang penting.
5) Meningkatkan efisiensi dan efektivitas audit. Dengan menggunakan checklist standar audit, auditor dapat mempercepat proses audit dan menghemat waktu dan biaya yang diperlukan untuk melakukan audit.

- Riset literatur

  Riset literatur penting dilakukan untuk memperoleh informasi sekunder pada proses bisnis dari area audit. Berbagai referensi berupa materi pelatihan, buku, jurnal dapat dipergunakan sebagai sumber informasi tambahan sehingga tim audit dapat memahami area audit secara lengkap. (Kegerreis Mike et al, 2020).

7.3 Prosedur dan Protokol Audit

Tabel 7.1. mengidentifikasi beberapa sumber utama dari prosedur audit untuk berbagai jenis audit utama. Definisi ruang lingkup dan tujuan audit selama perencanaan audit biasanya berkorelasi dengan kriteria audit yang akan diterapkan auditor pada prosedur dan protokol yang berlaku. Dalam audit internal, personel program audit organisasi umumnya memiliki keleluasaan untuk menentukan prosedur dan protokol yang paling sesuai dengan tujuan audit mereka. Saat menggunakan jasa auditor eksternal, organisasi cenderung tidak mendikte prosedur audit, meskipun prosedur yang direkomendasikan atau diusulkan mungkin merupakan salah satu kriteria yang dipertimbangkan organisasi saat memilih auditor eksternal.

Tabel 7.1. Sumber Prosedur dan Protokol Audit untuk Jenis Audit Utama

Tipe Audit	Prosedur dan Protokol Audit
Audit Financial	Statements on Auditing Standards (SAS)
	Statement on Standards for Attestation Engagements (SSAE)
	International Standards on Auditing (ISA)
	International Professional Practices Framework (IIPF)
Audit Operasional	Standard Audit Program Guides
Audit Sertifikasi	ISO/IEC 17021 ISO 19011
Audit Kualitas	ASQ Quality Auditor Body of Knowledge
Audit sistem Informasi	ISACA IT Audit Framework
	ISO/IEC 27006 , 27007, and 27008
	Federal Information System Controls Audit Manual (FISCAM)

(Sumber : Gantz Stephen D, 2014). “The Basic of IT Audit”)

Pada tabel 7.1. Terlihat bahwa salah satu prosedur dan protokol audit sistem informasi yaitu *ISACA IT Audit Framework*.

ISACA (Information Systems Audit and Control Association) merupakan sebuah organisasi profesional global yang didedikasikan untuk menyediakan sumber daya, standar, dan pelatihan bagi para profesional di bidang audit TI, pengendalian TI, manajemen risiko TI, dan keamanan informasi. Organisasi ini didirikan pada tahun 1969 dan berkantor pusat di Amerika Serikat.

Kebutuhan tersedianya sistem informasi yang handal dalam mendukung keberhasilan organisasi telah menyebabkan framework yang dibangun oleh ISACA dipergunakan secara luas di dunia. Tercatat 140 negara telah menggunakan framework sistem informasi yang dibangun ISACA. COBIT (Control Objectives for Information and Related Technology) adalah sebuah kerangka kerja manajemen TI yang dikembangkan oleh ISACA untuk membantu organisasi dalam merancang, mengimplementasikan, mengoperasikan, dan memantau pengendalian TI dan tata kelola TI. COBIT memberikan panduan terperinci tentang praktik-praktik terbaik dalam manajemen TI, serta memberikan kerangka kerja yang dapat dipergunakan sebagai jaminan TI telah mendukung tujuan bisnis juga memenuhi kebutuhan pengguna.

COBIT telah menjadi salah satu kerangka kerja manajemen TI yang paling terkenal dan banyak digunakan di seluruh dunia. COBIT dapat membantu organisasi untuk meningkatkan efisiensi, efektivitas, dan keandalan sistem TI mereka, serta memastikan kepatuhan dengan persyaratan peraturan dan standar industri.

COBIT (*Control Objectives for Information and Related Technology)* sejak tahun 1996 sebagai framework tata kelola sistem informasi yang telah terstandar secara internasional dikembangkan oleh ISACA. Framework COBIT ini memudahkan organisasi untuk melakukan audit internal sistem informasi yang dipergunakan.

Spesifikasi utama kerangka kerja COBIT yaitu pengelompokkan aktivitas teknologi informasi dalam empat kategori, yaitu:

1. Perencanaan dan pengorganisasian (PO),
2. Akuisisi dan implementasi (AI)
3. Pengoperasian dan pengiriman (DS)
4. Pemantauan dan Evaluasi (ME).

Domain PO menyediakan arahan untuk mewujudkan solusi penyampaian dan penyampaian jasa. AI menyediakan solusi dan menyalurkannya untuk dapat diubah menjadi jasa. Sementara DS menerima solusi tersebut dan membuatnya lebih bermanfaat bagi pengguna akhir. Sedangkan ME memonitor seluruh proses untuk kepastian bahwah arahan yang diberikan telah diikuti.

Namun pada bagian ini pembahasan difokuskan pada kategori PO sebagai bagian perencanaan dan manajemen audit yang menyediakan sepuluh proses teknologi informasi seperti terlihat pada tabel 2. Dalam perencanaan dan organisasi perusahaan ini sudah Mencakup strategi, taktik dan perhatian atas identifikasi bagaimana IT secara maksimal dapat berkontribusi dalam pencapaian tujuan bisnis. Tetapi startegis perlu direncanakan, dikomunikasikan, dan dikelola untuk berbagai perspektif yang berbeda. Disini sebuah pengorganisasian serta infrastruktur teknologi sudah ditempatkan di tempat yang semestinya.

Tabel 7.2. Domain PO Framework COBIT

PO1	Mendefenisikan rencana strategis TI
PO2	Mendefenisikan arsitektur informasi
PO3	Menentukan arahan teknologi
PO4	Menentukan proses TI, organisasi & Keterhubungannya
PO5	Mengelola investasi TI
PO6	Mengkomunikasikan tujuan dan arahan manajemen
PO7	Mengelola sumberdaya TI

PO8	Mengelola kualitas
PO9	Menaksir dan mengelola resiko TI
PO10	Mengelola proyek

PO1 : Mendefenisikan rencana strategis TI

Rencana strategis TI menurut COBIT adalah sebuah dokumen yang mendefinisikan visi, misi, tujuan, dan rencana aksi yang berhubungan dengan pengelolaan dan penggunaan teknologi informasi dalam organisasi. Dalam COBIT, rencana strategis TI meliputi:

1. Tujuan bisnis: Rencana strategis TI harus didasarkan pada tujuan bisnis dan strategi organisasi. Hal ini akan memastikan bahwa teknologi informasi mendukung tujuan bisnis secara efektif.
2. Kebutuhan pengguna: Rencana strategis TI harus memperhatikan kebutuhan pengguna atau pemangku kepentingan (stakeholder) dalam organisasi. Teknologi informasi harus dirancang untuk memenuhi kebutuhan pengguna dan memberikan nilai tambah bagi organisasi.
3. Rencana aksi: Rencana strategis TI harus mencakup rencana aksi yang spesifik dan terukur, serta memperhatikan aspek keuangan, sumber daya manusia, dan teknologi yang dibutuhkan untuk mencapai tujuan.
4. Arsitektur TI: Rencana strategis TI harus mencakup arsitektur teknologi informasi yang digunakan dalam organisasi. Hal ini akan memastikan bahwa teknologi informasi digunakan secara konsisten dan terkoordinasi.
5. Pengendalian: Rencana strategis TI harus memperhatikan pengendalian yang diperlukan untuk memastikan keamanan, integritas, dan ketersediaan teknologi informasi.

Dengan mendefinisikan rencana strategis TI yang berdasarkan COBIT, organisasi dapat mengelola dan mengontrol teknologi informasi dengan lebih efektif dan efisien, serta memastikan bahwa teknologi informasi

mendukung tujuan bisnis dan memberikan nilai tambah yang signifikan bagi organisasi

PO2 : Mendefenisikan arsitektur informasi

Arsitektur informasi menurut COBIT (*Control Objectives for Information and Related Technology*) adalah sebuah konsep yang merujuk pada desain, struktur, dan tata letak dari sistem dan infrastruktur teknologi informasi dalam organisasi. Arsitektur informasi memainkan peran penting dalam mengelola dan mengontrol teknologi informasi dalam organisasi, serta memastikan bahwa teknologi informasi mendukung tujuan bisnis dan kebutuhan pengguna. Dalam COBIT, arsitektur informasi meliputi:

1. Kerangka Kerja: Arsitektur informasi harus didasarkan pada kerangka kerja yang sesuai, untuk memastikan bahwa desain sistem dan infrastruktur teknologi informasi sesuai dengan prinsip dan praktek terbaik.
2. Model Bisnis: Arsitektur informasi harus memperhatikan model bisnis organisasi dan memastikan bahwa teknologi informasi mendukung tujuan bisnis dan memenuhi kebutuhan pengguna.
3. Komponen Teknologi: Arsitektur informasi harus memperhatikan komponen teknologi yang digunakan dalam organisasi, seperti perangkat keras, perangkat lunak, dan jaringan komunikasi.
4. Integrasi: Arsitektur informasi harus memastikan bahwa semua komponen teknologi diintegrasikan dengan baik dan bekerja secara efektif dalam lingkungan organisasi.
5. Keamanan dan Pengendalian: Arsitektur informasi harus memperhatikan keamanan dan pengendalian yang diperlukan untuk melindungi data dan sistem informasi, serta memastikan ketersediaan dan integritas informasi.

Dengan mendefinisikan arsitektur informasi yang berdasarkan COBIT, organisasi dapat mengelola dan mengontrol teknologi informasi dengan lebih efektif dan efisien, serta memastikan bahwa teknologi informasi mendukung tujuan bisnis dan kebutuhan pengguna. Hal ini akan membantu organisasi untuk meningkatkan kinerja dan mencapai tujuan bisnis dengan lebih baik.

PO3 : Menentukan arahan teknologi

Arah teknologi menurut COBIT (*Control Objectives for Information and Related Technology*) adalah panduan atau pedoman yang digunakan untuk memilih, mengimplementasikan, dan mengelola teknologi informasi dalam organisasi. Arah teknologi COBIT dirancang untuk memastikan bahwa organisasi memilih teknologi yang tepat dan memanfaatkannya secara efektif untuk mencapai tujuan bisnis. Dalam COBIT, arah teknologi meliputi:

1. Evaluasi dan Pemilihan Teknologi: Arah teknologi harus memperhatikan evaluasi dan pemilihan teknologi yang sesuai dengan kebutuhan organisasi dan sesuai dengan prinsip dan praktek terbaik.
2. Infrastruktur Teknologi: Arah teknologi harus memperhatikan infrastruktur teknologi yang digunakan dalam organisasi dan memastikan bahwa infrastruktur tersebut mendukung tujuan bisnis dan memenuhi kebutuhan pengguna.
3. Integrasi Teknologi: Arah teknologi harus memastikan bahwa teknologi yang digunakan dalam organisasi diintegrasikan dengan baik dan bekerja secara efektif dalam lingkungan organisasi.
4. Pengelolaan Siklus Hidup Teknologi: Arah teknologi harus memperhatikan pengelolaan siklus hidup teknologi, mulai dari perencanaan, pengembangan, pengimplementasian, pengoperasian, dan pemeliharaan teknologi.

PO4 : Menentukan proses TI, organisasi & Keterhubungannya

Organisasi TI didefinisikan dengan mempertimbang-kan persyaratan untuk staf, keterampilan, fungsi, akuntabilitas, wewenang, peran dan tanggung jawab, dan pengawasan. Organisasi ini disematkan ke dalam kerangka kerja proses TI yang memastikan transparansi dan kontrol serta keterlibatan eksekutif senior dan manajemen bisnis. Komite strategi memastikan pengawasan dewan atas TI, dan satu atau lebih komite pengarah di mana bisnis dan TI berpartisipasi menentukan prioritas sumber daya TI sejalan dengan kebutuhan bisnis. Proses, kebijakan dan prosedur administratif tersedia untuk semua fungsi, dengan perhatian khusus pada kontrol, jaminan kualitas, manajemen risiko, keamanan informasi, kepemilikan data dan sistem, dan pemisahan tugas. Untuk memastikan dukungan tepat waktu dari persyaratan bisnis, TI harus dilibatkan dalam proses pengambilan keputusan yang relevan.

PO5 : Mengelola investasi TI

Konsep pengelolaan investasi TI dalam COBIT (Control Objectives for Information and Related Technology) dirancang untuk membantu organisasi dalam memilih, mengimplementasikan, dan mengelola investasi teknologi informasi secara efektif dan efisien. Pengelolaan investasi TI dalam COBIT mencakup tiga area utama, yaitu:

1. Perencanaan dan Evaluasi Investasi TI: COBIT menekankan pentingnya perencanaan investasi TI yang baik dan evaluasi secara teratur untuk memastikan bahwa investasi TI yang dibuat sejalan dengan tujuan bisnis dan memberikan nilai tambah yang signifikan. Hal ini termasuk dalam mempertimbangkan risiko dan manfaat investasi TI dan membuat keputusan investasi berdasarkan kriteria bisnis yang jelas.
2. Pengimplementasian Investasi TI: COBIT menekankan pentingnya pengimplementasian investasi TI yang efektif

dan efisien, meliputi desain, pengembangan, dan implementasi solusi TI yang tepat, serta memastikan bahwa solusi TI tersebut berjalan sesuai dengan rencana bisnis dan memenuhi kebutuhan pengguna.

3. Monitoring dan Penilaian Investasi TI: COBIT menekankan pentingnya pemantauan dan penilaian investasi TI secara teratur untuk memastikan bahwa investasi TI memberikan nilai tambah yang diharapkan dan membantu organisasi mencapai tujuan bisnis. Hal ini termasuk dalam melakukan audit dan penilaian secara teratur untuk memastikan bahwa investasi TI yang dilakukan masih relevan dan memberikan manfaat yang diharapkan.

PO6 : Mengkomunikasikan tujuan dan arahan manajemen

Manajemen mengembangkan kerangka kerja kontrol TI perusahaan dan mendefinisikan serta mengkomunikasikan kebijakan. Program komunikasi yang berkelanjutan diterapkan untuk mengartikulasikan misi, tujuan layanan, kebijakan dan prosedur, dll., yang disetujui dan didukung oleh manajemen. Komunikasi mendukung pencapaian tujuan TI dan memastikan kesadaran dan pemahaman bisnis dan risiko TI, tujuan dan arah. Proses ini memastikan kepatuhan terhadap hukum dan peraturan yang relevan.

PO7 : Mengelola sumberdaya TI

Tenaga kerja yang kompeten diperoleh dan dipertahankan untuk pembuatan dan pengiriman layanan TI ke bisnis. Ini dicapai dengan mengikuti praktik yang ditentukan dan disetujui yang mendukung perekrutan, pelatihan, evaluasi kinerja, promosi, dan pemberhentian. Proses ini sangat penting, karena manusia adalah aset penting, dan tata kelola serta lingkungan pengendalian

internal sangat bergantung pada motivasi dan kompetensi personel.

PO8 : Mengelola kualitas

QMS dikembangkan dan dipelihara yang mencakup pengembangan proses dan akuisisi standar yang telah terbukti. Ini dimungkinkan dengan merencanakan, menerapkan, dan memelihara QMS dengan menyediakan persyaratan, prosedur, dan kebijakan kualitas yang jelas. Persyaratan mutu dinyatakan dan dikomunikasikan dalam indikator yang terukur dan dapat dicapai. Peningkatan berkelanjutan dicapai dengan pemantauan terus menerus, analisis dan tindakan atas penyimpangan, dan mengkomunikasikan hasilnya kepada pemangku kepentingan. Manajemen mutu sangat penting untuk memastikan bahwa TI memberikan nilai bagi bisnis, peningkatan berkelanjutan, dan transparansi bagi pemangku kepentingan.

PO9 : Menaksir dan mengelola resiko TI

Kerangka kerja manajemen risiko dibuat dan dipelihara. Kerangka tersebut mendokumentasikan tingkat risiko TI yang umum dan disepakati, strategi mitigasi, dan risiko residual. Setiap dampak potensial terhadap tujuan organisasi yang disebabkan oleh peristiwa yang tidak direncanakan diidentifikasi, dianalisis, dan dinilai. Strategi mitigasi risiko diadopsi untuk meminimalkan risiko residual ke tingkat yang dapat diterima. Hasil penilaian dapat dipahami oleh pemangku kepentingan dan dinyatakan dalam istilah keuangan, untuk memungkinkan pemangku kepentingan menyelaraskan risiko ke tingkat toleransi yang dapat diterima.

PO10 : Mengelola proyek

Kerangka manajemen program dan proyek untuk pengelolaan semua proyek TI ditetapkan. Kerangka kerja memastikan prioritas dan koordinasi yang benar dari semua proyek. Kerangka kerja tersebut mencakup rencana induk, penugasan sumber daya, definisi hasil, persetujuan oleh pengguna, pendekatan bertahap untuk pengiriman, QA, rencana pengujian formal, dan pengujian dan tinjauan pasca implementasi setelah pemasangan untuk memastikan manajemen risiko proyek dan pengiriman nilai ke bisnis. Pendekatan ini mengurangi risiko biaya tak terduga dan pembatalan proyek, meningkatkan komunikasi dan keterlibatan bisnis dan pengguna akhir, memastikan nilai dan kualitas penyampaian proyek, dan memaksimalkan kontribusi mereka terhadap program investasi yang dimungkinkan TI. (IT Governance Institute, 2007)

7.4 Penutup

Berikut adalah beberapa saran untuk membahas topik perencanaan dan manajemen audit sistem informasi:

1. Tentukan tujuan audit: Sebelum melakukan audit, tentukan tujuan dan lingkup audit. Tujuan audit dapat berupa pengujian efektivitas kontrol, identifikasi kelemahan dalam sistem informasi, atau penilaian kepatuhan terhadap regulasi dan kebijakan.
2. Identifikasi risiko: Identifikasi dan evaluasi risiko terkait dengan sistem informasi, termasuk risiko keamanan siber, keandalan data, dan integritas sistem.
3. Gunakan kerangka kerja audit: Gunakan kerangka kerja audit yang relevan, seperti COBIT atau ITIL, untuk memandu proses audit. Kerangka kerja ini memberikan panduan dan prinsip dasar untuk melakukan audit sistem informasi.

4. Perhatikan pengendalian: Perhatikan pengendalian yang ada dalam sistem informasi, termasuk kontrol akses, pemantauan aktivitas sistem, dan pengelolaan keamanan.
5. Uji efektivitas pengendalian: Lakukan uji efektivitas pengendalian dalam sistem informasi untuk memastikan bahwa pengendalian bekerja sesuai yang diharapkan.
6. Berikan rekomendasi perbaikan: Setelah melakukan audit, berikan rekomendasi perbaikan yang konkrit dan spesifik, serta tindakan yang dapat dilakukan untuk meningkatkan sistem informasi.
7. Evaluasi tindakan perbaikan: Lakukan evaluasi tindakan perbaikan yang telah dilakukan untuk memastikan bahwa perbaikan telah dilakukan secara efektif dan pengendalian telah ditingkatkan.
8. Laporan hasil audit: Buat laporan hasil audit yang jelas dan komprehensif, serta sampaikan laporan kepada manajemen yang relevan dan pihak yang terkait.

Dengan mengikuti saran-saran tersebut, Anda dapat memahami topik perencanaan dan manajemen audit sistem informasi dengan lebih mudah, serta dapat melakukan proses audit yang lebih berkualitas dan memberikan nilai tambah bagi organisasi.

DAFTAR PUSTAKA

ISACA - Wikipedia bahasa Indonesia, ensiklopedia bebas

Kegerreis Mike, Schiller Mike, Christ Davis & Brian Wrozek (2020). “IT Auditing: Using Controls to Protect Information Assets”.

BAB 8
PERANGKAT DAN METODE PADA AUDIT SISTEM INFORMASI

8.1 Pendahuluan

Audit sistem informasi (SI) merupakan proses pemeriksaan, peninjauan, dan verifikasi dalam suatu aplikasi terhadap keandalan, keamanan, dan ketersediaan informasi yang akan digunakan untuk memproses dan menyimpan dalam sistem informasi. Tujuan dari proses pemeriksaan (audit) sistem informasi dapat memberikan suatu informasi dengan efektif dan didukung oleh beberapa perangkat dan metode yang tepat dalam pemeriksaan sistem informasi (Herlambang & Suharso 2018; Rahmanto et al. 2020).

Berdasarkan tugas dari seorang yang melakukan audit sistem informasi, maka orang tersebut harus mengetahui proses dan cara mengaplikasikan perangkat dan metode audit sistem informasi secara tepat sehingga dapat memberikan hasil penilaian yang akurat dan sesuai dengan evaluasi terhadap sistem informasi yang diperiksa. Oleh karena itu, seorang audit sistem informasi pemahaman tentang perangkat dan seperti mempersiapkan, melaksanakan, dan melaporkan hasil audit.

8.2 Proses Audit Sistem Informasi (SI)

Perangkat dan metode audit sistem informasi digunakan sebagai panduan melakukan audit dan sarana untuk mengumpulkan, menganalisis, dan mengevaluasi suatu data yang terkait dengan sistem informasi (Puspita

2021). Tabel 8.1 menggambarkan beberapa proses dalam audit sistem informasi, yang dimulai dari perencanaan audit hingga tindak lanjut setelah audit dilakukan.

Tabel 8.1. Tahapan Proses Audit Sistem Informasi

No.	Proses	Deskripsi
1	Perencanaan Audit	Identifikasi area audit, penentuan sasaran audit, penentuan cakupan audit, pengembangan rencana audit, dan penentuan sumber daya audit.
2	Pengumpulan Data	Pengumpulan data terkait sistem informasi yang akan diaudit melalui wawancara, observasi, dan dokumen-dokumen terkait.
3	Evaluasi Risiko	Penilaian terhadap risiko yang terkait dengan sistem informasi yang diaudit untuk mengidentifikasi area yang membutuhkan perhatian khusus.
4	Pengujian Kontrol Internal	Melakukan pengujian terhadap kontrol internal yang ada di dalam sistem informasi.
5	Evaluasi Temuan Audit	Melakukan evaluasi terhadap temuan audit dan menentukan tingkat risiko dan dampak yang dihasilkan.
6	Pelaporan Hasil Audit	Menyampaikan hasil audit dengan rekomendasi perbaikan dan pengembangan yang diperlukan.
7	Tindak Lanjut	Memantau dan mengevaluasi tindak lanjut yang diambil sebagai respons atas hasil audit.

Beberapa perangkat dan metode yang dapat digunakan dalam audit sistem informasi antara lain checklist, formulir observasi, software audit, dan teknik sampling.

8.2.1 Proses Pembuatan Checklist

Pemprosesan untuk checklist audit sistem informasi (SI) dapat disesuaikan dengan kategori yang akan di audit, namun umumnya akan menampilkan tahapan-tahapan dari proses audit untuk checklist audit sistem informasi, diantaranya:

1. Persiapan: meliputi pembuatan rencana audit, pembuatan checklist audit, dan pemilihan tim auditor.
2. Dokumentasi: meliputi pemeriksaan dokumen-dokumen yang terkait dengan sistem informasi, seperti spesifikasi sistem, manual pengguna, dan lain-lain.
3. Proses: meliputi pemeriksaan proses-proses yang digunakan dalam sistem informasi, seperti prosedur pengelolaan data, prosedur backup, dan lain-lain.
4. Fungsionalitas: meliputi pemeriksaan kinerja sistem informasi dari segi fungsionalitas, seperti kemampuan sistem memproses data, kecepatan akses, dan lain-lain.
5. Keamanan: meliputi pemeriksaan keamanan sistem informasi, seperti keamanan data, perlindungan terhadap serangan eksternal, dan lain-lain.
6. Sarana: meliputi pemeriksaan sarana-sarana yang digunakan dalam sistem informasi seperti perangkat keras dan perangkat lunak yang digunakan.
7. Laporan: meliputi penyusunan laporan hasil audit yang menyajikan temuan dan rekomendasi selama proses audit.
8. Tindak Lanjut: meliputi pelaksanaan tindakan perbaikan yang diperlukan berdasarkan temuan-temuan selama proses audit.

8.2.2 Proses Perancangan Formulir Observasi

Proses perancangan formulir observasi mengharapkan hasil audit lebih akurat dan memberikan rekomendasi yang berguna bagi sistem informasi yang diaudit. Beberapa proses perancangan formulir observasi yang dilakukan dalam audit SI, diantaranya:

1. Identifikasi area yang akan diamati
   Mengidentifikasi area atau bagian dari sistem informasi yang akan diamati bertujuan untuk memastikan pengamatan atau target yang dilakukan pada area yang relevan dan dapat memberikan informasi yang berguna dalam audit.
2. Penentuan tujuan pengamatan
   Menentukan tujuan dari pengamatan yang dilakukan pada area yang telah diidentifikasi berupa mengumpulkan informasi tentang kebijakan, prosedur, atau kontrol yang ada pada sistem informasi.
3. Pengembangan daftar pertanyaan
   Mengembangkan daftar pertanyaan yang relevan dengan tujuan pengamatan yang telah ditentukan. Daftar pertanyaan ini dapat mencakup berbagai aspek dari sistem informasi seperti keamanan, integritas data, atau ketersediaan sistem.
4. Desain formulir observasi
   Mendesain formulir observasi yang akan digunakan untuk mencatat hasil pengamatan dan jawaban dari daftar pertanyaan. Formulir observasi ini dapat berbentuk tabel atau checklist.
5. Uji coba formulir observasi
   Melakukan uji coba formulir observasi untuk memastikan bahwa formulir tersebut dapat menghasilkan informasi yang relevan dan akurat.

6. Perbaikan dan penyempurnaan formulir observasi
   Melakukan perbaikan dan penyempurnaan pada formulir observasi berdasarkan hasil uji coba dan umpan balik dari pihak yang terlibat dalam audit.

8.2.3 Proses Pemilihan Software Audit

Dalam melakukan audit sistem informasi, pemilihan software audit yang tepat merupakan hal yang sangat penting untuk memastikan keberhasilan audit. Oleh karena itu, proses pemilihan software audit harus dilakukan dengan hati-hati dan cermat, dengan mempertimbangkan beberapa faktor yang relevan.

Beberapa proses pemilihan software audit yang dilakukan dalam audit SI diantaranya :

1. Identifikasi kebutuhan audit
   Mengidentifikasi kebutuhan audit yang akan dilakukan, seperti jenis sistem informasi yang akan diaudit, tujuan audit, serta aspek yang akan diamati dalam audit.
2. Penentuan kriteria pemilihan software audit
   Menentukan kriteria pemilihan software audit berdasarkan kebutuhan audit yang telah diidentifikasi. Kriteria dapat meliputi fitur dan fungsionalitas, keamanan, dukungan teknis, dan biaya.
3. Penelitian dan pemilihan software audit
   Melakukan penelitian dan pemilihan software audit yang memenuhi kriteria yang telah ditetapkan. Software audit yang dipilih harus dapat memenuhi kebutuhan audit yang telah diidentifikasi dan dapat diintegrasikan dengan sistem informasi yang akan diaudit.
4. Pengujian dan evaluasi software audit
   Melakukan pengujian dan evaluasi software audit untuk memastikan bahwa software tersebut dapat bekerja dengan baik dan memenuhi kebutuhan audit yang telah ditetapkan.

5. Implementasi software audit
   Melakukan implementasi software audit pada sistem informasi yang akan diaudit. Hal ini meliputi konfigurasi, instalasi, dan integrasi dengan sistem informasi yang ada.
6. Pelatihan pengguna
   Melakukan pelatihan pengguna untuk memastikan bahwa tim audit dapat menggunakan software audit dengan baik dan efektif.

8.2.4 Proses Analisa dan Teknik Sampling

Dalam melakukan audit sistem informasi, proses analisa dan teknik sampling sangat penting untuk memastikan keakuratan dan representatifitas informasi yang dihasilkan. Melalui analisis dokumen, pengujian substantif, teknik sampling, dan analisis rasio, auditor dapat memperoleh pemahaman yang lebih baik mengenai sistem informasi yang diaudit dan mengidentifikasi risiko-risiko potensial yang mungkin terjadi (Hambali & Musa 2020).

Beberapa proses analisa dan teknik sampling yang dilakukan dalam audit SI diantaranya:

1. Analisis Dokumen
   Menganalisis dokumen-dokumen yang terkait dengan sistem informasi, seperti laporan keuangan, laporan operasional, kebijakan dan prosedur, dan dokumen teknis lainnya. Analisis dokumen dapat membantu dalam memahami bagaimana sistem informasi berfungsi dan mengidentifikasi risiko-risiko potensial yang mungkin terjadi.
2. Pengujian Substantif
   Pengujian substantif dilakukan untuk memverifikasi informasi yang terkandung dalam sistem informasi. Metode yang digunakan dalam pengujian ini dapat berupa pengujian detail, pengujian substantif analitis, dan pengujian substantif konfirmatif.

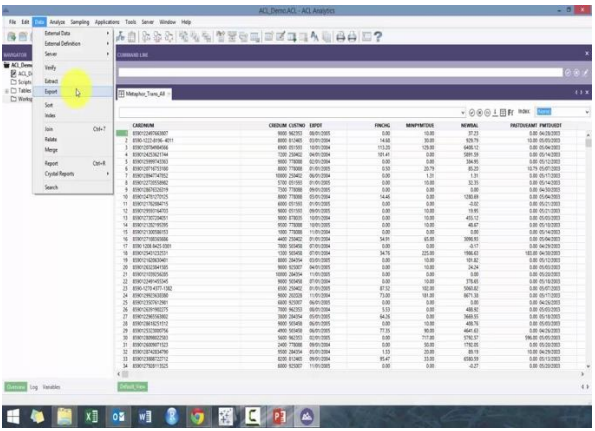
3. Teknik Sampling
   Teknik sampling digunakan untuk memilih sebagian data atau transaksi yang akan diuji secara mendalam, sehingga dapat mewakili populasi keseluruhan. Beberapa teknik sampling yang sering digunakan dalam audit SI adalah sampling acak sederhana, sampling stratifikasi, dan sampling kuota.
4. Analisis Rasio
   Analisis rasio dilakukan dengan membandingkan berbagai rasio keuangan atau operasional yang terkait dengan sistem informasi. Analisis rasio dapat membantu dalam mengidentifikasi tren dan pola yang mungkin terjadi pada sistem informasi.

8.3 Aplikasi Audit Sistem Informasi (SI)

Aplikasi untuk perangkat dan metode audit sistem informasi yang dapat digunakan sesuai dengan kebutuhan dan kondisi sistem yang diaudit, seperti; *Audit Command Language* (ACL), *Interactive Data Extraction and Analysis* (IDEA)

8.3.1 Audit Command Language (ACL)

Audit Command Language (ACL) merupakan aplikasi untuk analisis data dan audit sistem (Will 1975; Will 1983). ACL menyediakan berbagai perangkat analisis data seperti *query*, *sample data*, serta pembuatan laporan yang dapat digunakan untuk audit (Trianico Puspaningrum 2014).



Gambar 8.1. Logo dan Proses ACL dalam Audit Sistem Informasi
(Sumber: google.com)

ACL dalam audit sistem informasi dapat membantu auditor untuk melakukan analisis data dan deteksi fraud dengan memproses data secara cepat dan akurat, dan membantu mengidentifikasi potensi kecurangan atau ketidakpatuhan dengan cepat dan efektif. Cara kerja ACL dalam audit SI adalah sebagai berikut:

1. Mengumpulkan data: Auditor mengumpulkan data dari berbagai sumber, seperti basis data, file teks, dan file Excel, dan mengimpor data ke dalam ACL.
2. Memeriksa integritas data: ACL dapat digunakan untuk memeriksa integritas data, seperti melakukan perhitungan jumlah, rata-rata, dan median untuk memastikan keakuratan data.
3. Menemukan anomali: ACL dapat membantu auditor untuk menemukan anomali dalam data dengan menggunakan fitur deteksi anomali dan pengklasifikasi yang telah disediakan.
4. Menerapkan analisis statistik: ACL dapat digunakan untuk menerapkan analisis statistik pada data untuk menemukan pola atau tren yang mungkin tidak terlihat secara langsung.

5. Melakukan deteksi fraud: ACL dapat digunakan untuk melakukan deteksi fraud dengan menggunakan skrip yang telah dibuat atau dengan membuat skrip khusus yang disesuaikan dengan kebutuhan audit.
6. Membuat laporan: ACL dapat digunakan untuk membuat laporan audit dengan menyajikan hasil analisis dan deteksi fraud yang telah dilakukan.

8.3.2 *Interactive Data Extraction and Analysis* (IDEA)

Menurut (Antcliff et al. 2012), *Interactive Data Extraction and Analysis* (IDEA) merupakan aplikasi untuk analisis data dan audit sistem, dimana aplikasi IDEA menyediakan perangkat analisis data untuk membuat rekonsiliasi, investigasi kecurangan, internal/operational audit, pemindahan file, mempersiapkan laporan manajemen dan analisis-analisis lainnya, termasuk menelusuri security log.

Gambar 8.2. Logo IDEA dalam Audit Sistem Informasi (Sumber: google.com)

8.3.3 *Audit Program Generator* (APG)

Aplikasi APG merupakan aplikasi yang dapat memberikan bantuan kepada auditor dalam memenuhi pemeriksaan standar auditing, mengevaluasi struktur pengendalian internal pada hasil laporan keuangan auditan.

8.3.4 Microsoft Excel

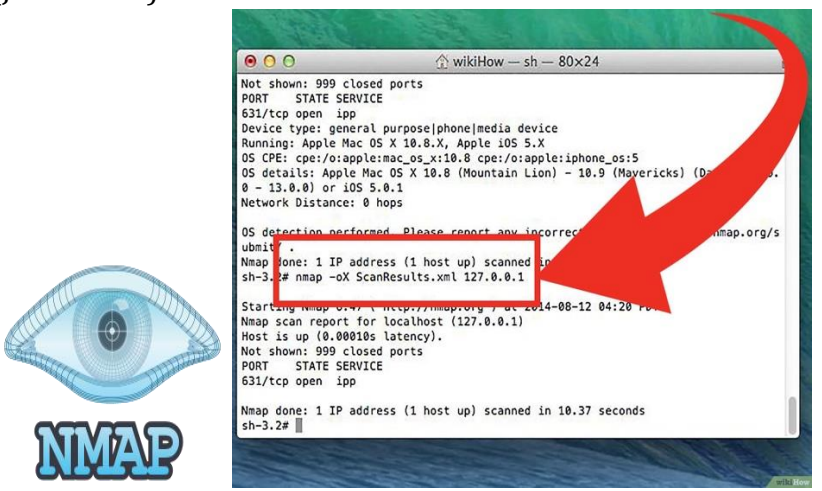
Aplikasi Microsoft Excel merupakan aplikasi pembuatan checklist audit, formulir observasi, dan formulir temuan termasuk menganalisis data dan membuat laporan hasil audit dengan melakukan pengolahan / manipulasi data

yang diperlukan ketida proses pemeriksaan audit yang membutuhkan data-data input serta suatu persamaan untuk hasil yang diperlukan (Dhae 2021).

Gambar 8.3. Logo Microsoft Excel untuk Audit Sistem Informasi
(Sumber: google.com)

8.3.5 Network Mapper (Nmap)

Network Mapper (NMap) merupakan aplikasi audit terhadap sistem keamanan pada suatu jaringan dengan melakukan pemindaian pada jaringan dan mengecek keamanan sistem informasi untuk menemukan host atau komputer serta suatu layanan pada jaringan komputer dengan mengirimkan paket dan menganalisis responnya (Joshi 2021).



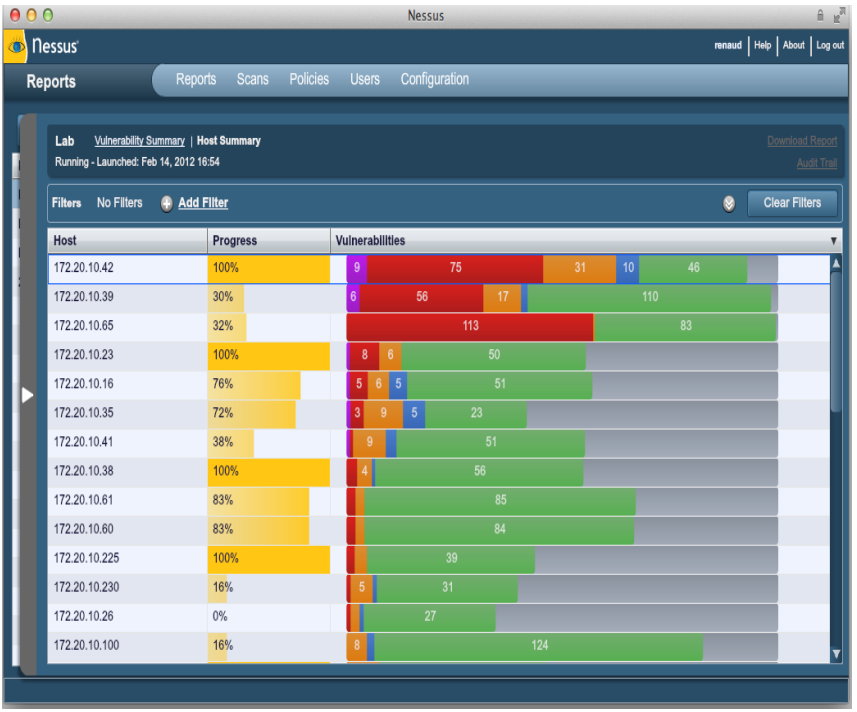
Gambar 8.4. Logo dan Proses Nmap dalam Audit Sistem Informasi
(Sumber: google.com)

8.3.6 Nessus

Nessus memiliki proses audit yang sama dengan Nmap, dimana aplikasi bertujuan untuk mengaudit sistem keamanan pada suatu jaringan. Nessus melakukan pemindai kerentanan suatu sistem pada jaringan dan mengecek keamanan sistem informasi yang dimiliki dan dikembangkan oleh Tenable, Inc.

Gambar 8.5. Logo Nessus untuk Audit Sistem Informasi (Sumber: google.com)

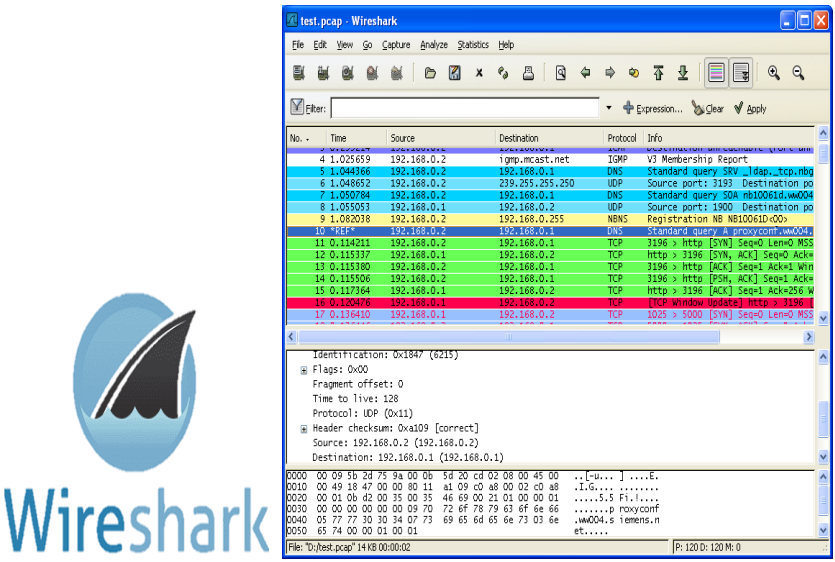
Pada Gambar 8.6 merupakan proses mengidentifikasi kerentanan dan celah keamanan, Nessus memberikan laporan hasil audit yang berisi daftar kerentanan yang ditemukan dan rekomendasi untuk memperbaiki keamanan sistem informasi. Laporan dapat membantu auditor dalam mengambil tindakan yang tepat untuk meningkatkan keamanan sistem informasi, seperti memperbarui perangkat lunak, mengubah konfigurasi sistem, atau melakukan tindakan lainnya.



Gambar 8.6. Tampilan Hasil Pemindaian oleh Nessus
(Sumber: google.com)

8.3.7 Wireshark

Selain Nmap dan Nessus, terdapat aplikasi yang digunakan untuk audit keamanan sistem dan jaringan (Ndatinya et al. 2015). Lebih dikenal dengan istilah Wireshark yang umumnya digunakan untuk menangkap dan menganalisis lalu lintas jaringan (seperti pada Gambar 8.7)



Gambar 8.7. Logo dan Aplikasi Wireshark dalam Melakukan Audit Sistem Informasi Terhadap Jaringan Komputer (Sumber: google.com)

Menurut (Luthfansa & Rosiani 2021), dalam audit sistem informasi, Wireshark dapat digunakan untuk memantau dan menganalisis lalu lintas jaringan yang terkait dengan sistem informasi yang diaudit. Aplikasi ini dapat membantu auditor dalam memeriksa apakah sistem informasi tersebut mengirimkan atau menerima data yang tidak terenkripsi, memverifikasi kinerja jaringan, dan mengidentifikasi masalah keamanan atau kinerja jaringan yang mungkin terjadi untuk memantau dan menganalisis data yang dikirimkan melalui jaringan, seperti paket data, protokol, dan alamat IP.

Selain itu, Wireshark dapat membantu dalam memeriksa dan memverifikasi kepatuhan terhadap kebijakan keamanan, seperti standar enkripsi, dan mengevaluasi efektivitas sistem keamanan yang diterapkan pada sistem informasi ketika diaudit.

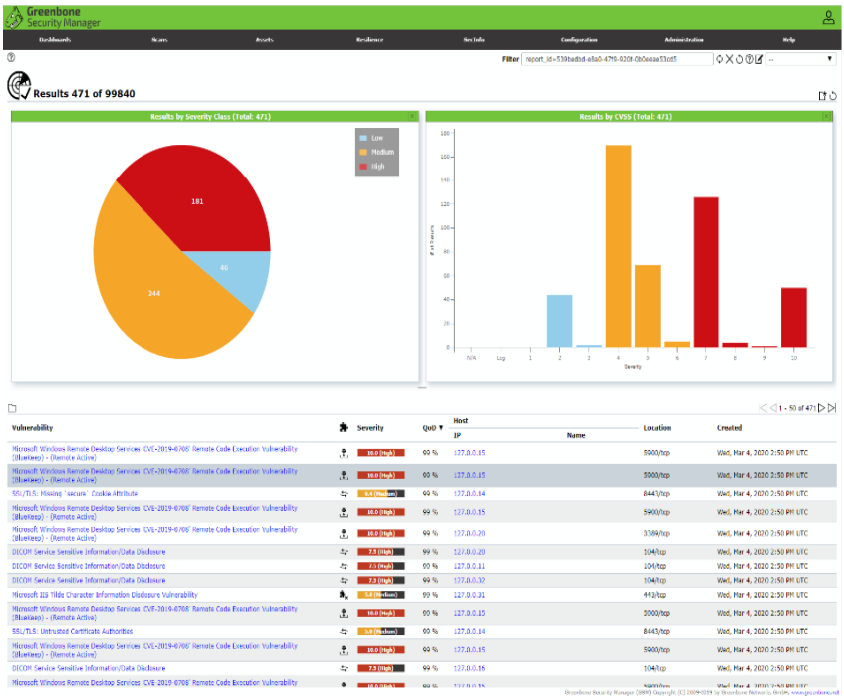
Dalam penggunaannya, Wireshark memerlukan keahlian khusus dalam bidang jaringan dan sistem informasi. Oleh karena itu, seorang auditor yang ingin menggunakan aplikasi ini dalam melakukan audit sistem informasi harus memiliki pengetahuan yang memadai dalam hal jaringan dan sistem informasi, serta dapat menginterpretasikan dan menganalisis data yang telah diperoleh dari aplikasi ini secara efektif.

8.3.8 OpenVAS

Aplikasi yang digunakan untuk audit keamanan sistem lainnya adalah OpenVAS (Rahalkar 2019) yang dapat digunakan untuk melakukan pemindaian pada jaringan dan mengecek keamanan sistem informasi.

Gambar 8.8. Logo dan Proses OpenVAS dalam Audit Sistem Informasi
(Sumber: google.com)

OpenVAS (*Open Vulnerability Assessment System*) adalah salah satu perangkat lunak *open-source* yang digunakan dalam melakukan audit keamanan sistem informasi. OpenVAS dapat digunakan untuk mengidentifikasi kerentanan keamanan pada sistem dan jaringan yang sedang diuji.



Gambar 8.9. Hasil Audit Sistem Informasi menggunakan OpenVAS
(Sumber: google.com)

Beberapa fitur yang ditawarkan oleh OpenVAS dalam audit sistem informasi adalah sebagai berikut:

1. Penemuan Kerentanan
   OpenVAS melakukan pemindai jaringan dan sistem yang ingin diuji untuk menemukan kerentanan keamanan yang mungkin ada.
2. Analisis dan Pemindaian
   Setelah menemukan kerentanan, OpenVAS akan melakukan analisis dan pemindaian yang lebih dalam untuk menguji keamanan sistem dan mengevaluasi respon terhadap kerentanan.
3. Pemantauan Keamanan
   OpenVAS juga dapat digunakan untuk memantau sistem secara terus-menerus dan memberikan peringatan

apabila terjadi ancaman atau kerentanan baru yang muncul.

4. Pelaporan Hasil Audit
   OpenVAS dapat menghasilkan laporan audit terperinci dan memberikan rekomendasi mengatasi kerentanan keamanan.

8.3.9 Metasploit

Metasploit adalah sebuah platform pentesting (penetration testing) yang populer digunakan dalam bidang keamanan informasi dan sering digunakan dalam melakukan audit sistem informasi. Dalam melakukan audit sistem informasi, penggunaan Metasploit dapat membantu auditor untuk menguji dan mengidentifikasi kelemahan pada sistem dan memberikan rekomendasi yang tepat untuk meningkatkan keamanan sistem.

Metasploit menyediakan berbagai alat dan fitur yang berguna dalam menguji keamanan sistem, seperti:

1. Penetration *testing*: Metasploit menyediakan berbagai macam modul dan payload yang dapat digunakan untuk melakukan penetrasi ke dalam sistem, seperti menjalankan shellcode, memanipulasi register, dan melakukan aktivitas jahat lainnya untuk mengetahui kerentanan pada sistem.
2. *Vulnerability scanning*: Metasploit dapat melakukan pemindaian keamanan pada sistem untuk menemukan kerentanan yang mungkin ada pada sistem. Pemindaian ini dapat dilakukan secara otomatis maupun manual dengan bantuan modul-modul khusus yang disediakan oleh Metasploit.
3. *Exploit development*: Metasploit juga dapat digunakan untuk mengembangkan exploit yang ditargetkan untuk memanfaatkan kerentanan pada sistem. Hal ini dapat dilakukan dengan menggunakan bahasa pemrograman yang familiar seperti Ruby.

4. *Reporting*: Metasploit menyediakan laporan yang dapat digunakan oleh auditor untuk mendokumentasikan hasil dari audit sistem informasi yang dilakukan.

Gambar 8.10. Logo dan Tampilan Proses Metasploit dalam Audit Sistem Informasi
(Sumber: google.com)

8.4 Keuntungan serta Kerugian dari Perangkat dan Metode Audit Sistem Informasi (SI)

Audit sistem informasi (SI) memiliki keuntungan dan kerugian yang perlu dipertimbangkan sebelum mengimplementasikan perangkat dan metode audit SI. Penjelasan terhadap keuntungan dan kerugian dari pemanfaatan perangkat dan metode audit sistem informasi yang ditunjukkan pada Tabel 8.2.

Tabel 8.2. Keuntungan dan Kerugian dari Pemanfaatan Perangkat dan Metode Audit Sistem Informasi

Keuntungan	Kerugian
Memastikan kepatuhan terhadap kebijakan dan prosedur yang berlaku	Memerlukan biaya untuk mengembangkan dan implementasi audit SI
Meningkatkan keamanan dan kehandalan sistem informasi	Keterbatasan auditor untuk memeriksa semua aspek sistem informasi
Meningkatkan efisiensi dan efektivitas operasional	Ketergantungan pada kualitas data yang tersedia dan integritas informasi
Mencegah dan mendeteksi penipuan atau pelanggaran keamanan	Keterbatasan mengidentifikasi potensi masalah di masa depan
Meningkatkan transparansi dan akuntabilitas dalam pengelolaan sistem informasi	Keterbatasan pada kemampuan untuk menangani masalah yang dihasilkan dari audit SI
Memberikan saran dan pengembangan sistem informasi	

DAFTAR PUSTAKA

Antcliff, M. et al., 2012. A Case to Provide Students Practice in Basic and Advanced Functions of IDEA Software. *AIS Educator Journal*, 7(1), pp.69–73.

Dhae, Y.K.I.D.., 2021. Audit Informasi pada UPT Bahasa Universitas Nusa Cendana. *Journal of Management : Small and Medium Enterprises (SMEs)*, 14(1), pp.87–103.

Hambali, H. & Musa, P., 2020. Analysis of Governance Security Management Information System Using Index KAMI in Central Government Institution. *Angkasa: Jurnal Ilmiah Bidang Teknologi*, 12(1), pp.89–98.

Herlambang, P. & Suharso, W., 2018. Audit Sistem Informasi Menggunakan Framework COBIT 4.1 Domain Acquire and Implementasi (AI) (Studi Kasus : Dinas Komunikasi dan Informatika Kota Malang). *Jurnal Teknologi dan Manajemen Informatika*, 4(2).

Joshi, S., 2021. What is Nmap And Why You Should Use It? *Industry News*.

Luthfansa, Z.M. & Rosiani, U.D., 2021. Pemanfaatan Wireshark untuk Sniffing Komunikasi Data Berprotokol HTTP pada Jaringan Internet. *Journal of Information Engineering and Educational Technology*, 5(1), pp.34–39.

Ndatinya, V. et al., 2015. Network forensics analysis using Wireshark. *International Journal of Security and Networks*, 10(2), pp.91–106.

Puspita, L., 2021. Control and Audit of Accounting Information Systems. *Control and Audit of Accounting Information Systems*, 5, pp.1–5.

Rahalkar, S., 2019. OpenVAS. In *Quick Start Guide to Penetration Testing*. pp. 47–71.

Rahmanto, Y., Ulum, F. & Priyopradono, B., 2020. Aplikasi Pembelajaran Audit Sistem Informasi dan Tata Kelola Teknologi Informasi Berbasis Mobile. *Jurnal Tekno Kompak*, 14(2), p.62.

Trianico Puspaningrum, M., 2014. The students' perception towards the audit using Audit Command Language (ACL) software. *The Indonesian Accounting Review*, 4(01), p.89.

Will, H.J., 1983. ACL: A language specific for auditors. *Communications of the ACM*, 26(5), pp.356–361.

Will, H.J., 1975. ACL: AUDIT COMMAND LANGUAGE. *INFOR Journal*, 13(1), pp.99–111.

BAB 9
PROSES PENGUMPULAN BUKTI PADA AUDIT SISTEM INFORMASI

9.1 Pendahuluan

Bab Proses Pegumpulan Bukti pada Audit Sistem Informasi bertujuan untuk memberikan pemahaman tentang konsep dasar pengumpulan bukti dalam audit sistem informasi. Audit sistem informasi merupakan suatu kegiatan yang dilakukan untuk mengevaluasi efektivitas dan efisiensi pengelolaan sistem informasi dalam suatu organisasi. Salah satu proses yang krusial dalam audit sistem informasi adalah proses pengumpulan bukti, dimana hal ini dilakukan untuk memperoleh informasi yang akurat dan cukup mengenai sistem informasi yang sedang di-audit.

Dalam proses pengumpulan bukti pada audit sistem informasi, terdapat beberapa prinsip dan teknik yang harus diperhatikan agar pengumpulan bukti yang dilakukan dapat dianggap valid dan memenuhi standar audit. Oleh karena itu, pemahaman yang baik mengenai konsep dasar dan proses pengumpulan bukti pada audit sistem informasi sangat penting bagi auditor dan pihak-pihak yang terkait dalam kegiatan audit.

Pada bab ini, akan dibahas mengenai proses pengumpulan bukti pada audit sistem informasi, mulai dari perencanaan pengumpulan bukti hingga evaluasi hasil pengumpulan bukti. Selain itu, juga akan dijelaskan mengenai teknik-teknik pengumpulan bukti yang dapat digunakan dalam audit sistem informasi, serta etika dan standar profesional yang harus diperhatikan dalam

pengumpulan bukti. Selain itu, kendala dan tantangan yang mungkin dihadapi dalam proses pengumpulan bukti pada audit sistem informasi juga akan dibahas dalam bab ini.

9.2 Konsep Dasar Pengumpulan Bukti pada Audit Sistem Informasi

Pengumpulan bukti dalam audit sistem informasi adalah suatu proses untuk memperoleh informasi dan data yang diperlukan untuk mengevaluasi efektivitas dan efisiensi pengelolaan sistem informasi dalam suatu organisasi. Bukti-bukti yang dikumpulkan harus cukup dan relevan dengan tujuan audit yang telah ditetapkan sebelumnya. Bukti-bukti ini kemudian digunakan sebagai dasar untuk mengevaluasi kepatuhan dan kinerja sistem informasi dalam organisasi, serta untuk menentukan apakah sistem tersebut memenuhi standar audit dan peraturan yang berlaku. Proses pengumpulan bukti pada audit sistem informasi dilakukan dengan memperhatikan prinsip-prinsip audit, termasuk independensi, objektivitas, integritas, kerahasiaan, dan kompetensi.

Tujuan utama dari pengumpulan bukti dalam audit sistem informasi adalah untuk mendapatkan informasi dan data yang akurat dan cukup mengenai sistem informasi dalam organisasi yang sedang di-audit. Bukti-bukti yang dikumpulkan kemudian digunakan sebagai dasar untuk mengevaluasi efektivitas dan efisiensi pengelolaan sistem informasi, serta untuk menentukan apakah sistem tersebut memenuhi standar audit dan peraturan yang berlaku.

Selain itu, pengumpulan bukti dalam audit sistem informasi juga bertujuan untuk mendukung kesimpulan dan temuan audit yang diperoleh. Bukti-bukti yang diperoleh melalui proses pengumpulan bukti dapat digunakan untuk menguji kepatuhan sistem informasi terhadap standar audit, memvalidasi informasi yang diperoleh dari sistem informasi,

serta membantu mengidentifikasi kelemahan dan risiko pada sistem informasi.

Dengan melakukan pengumpulan bukti yang memenuhi standar audit, auditor dapat memberikan keyakinan bahwa temuan dan kesimpulan audit yang dihasilkan dapat diandalkan dan sesuai dengan kriteria yang telah ditetapkan sebelumnya.

9.3 Proses Pengumpulan Bukti pada Audit Sistem Informasi

Proses pengumpulan bukti pada audit sistem informasi dimulai dari perencanaan pengumpulan bukti. Pada tahap ini, auditor menentukan jenis bukti yang harus dikumpulkan, teknik pengumpulan bukti yang akan digunakan, serta sumber-sumber bukti yang akan diambil. Selain itu, auditor juga harus mempertimbangkan faktor-faktor seperti kompleksitas sistem informasi yang sedang di-audit, risiko yang terkait dengan sistem informasi, dan jumlah bukti yang diperlukan untuk memastikan keandalan kesimpulan audit.

Setelah perencanaan, langkah selanjutnya dalam proses pengumpulan bukti adalah pengumpulan bukti. Pada tahap ini, auditor mengumpulkan bukti-bukti yang diperlukan menggunakan teknik-teknik pengumpulan bukti yang telah dipilih. Teknik-teknik pengumpulan bukti yang umum digunakan dalam audit sistem informasi antara lain observasi, wawancara, pengujian substantif, dan analisis dokumen. Selama proses pengumpulan bukti, auditor harus memperhatikan prinsip-prinsip audit seperti independensi, objektivitas, integritas, kerahasiaan, dan kompetensi.

Setelah bukti-bukti terkumpul, auditor harus melakukan evaluasi terhadap bukti-bukti tersebut. Pada tahap evaluasi, auditor mengevaluasi keandalan dan kecukupan bukti yang telah dikumpulkan serta

mengidentifikasi temuan dan kesimpulan audit. Selain itu, auditor juga harus mempertimbangkan apakah kesimpulan dan temuan audit yang diperoleh sesuai dengan tujuan dan standar audit yang telah ditetapkan sebelumnya.

Proses pengumpulan bukti pada audit sistem informasi merupakan tahap yang sangat penting dalam kegiatan audit. Keakuratan, keandalan, dan kecukupan bukti yang dikumpulkan sangat berpengaruh terhadap hasil audit yang diperoleh. Oleh karena itu, auditor harus memastikan bahwa proses pengumpulan bukti dilakukan secara sistematis dan memenuhi standar audit yang berlaku.

9.3.1 Perencanaan Pengumpulan Bukti

Sebelum melakukan pengumpulan bukti, auditor harus melakukan perencanaan pengumpulan bukti agar dapat membantu auditor dalam mengatur tugas audit dengan baik, menentukan metode pengumpulan bukti yang efektif dan memastikan bahwa audit dilakukan secara efisen serta dapat membantu dalam memprioritaskan area audit yang perlu ditinjau dan menentukan tujuan audit yang jelas. Menurut Stephen D. Gantz (2013), terdapat beberapa langkah perencanaan pengumpulan bukti yang dapat dilakukan oleh auditor dalam audit sistem informasi, antara lain:

- Memahami tujuan audit: Auditor harus memahami tujuan audit yang telah ditetapkan oleh manajemen dan bagaimana audit tersebut terkait dengan tujuan bisnis organisasi. Tujuan audit harus jelas dan dapat diukur sehingga auditor dapat menentukan fokus dan skala audit.
- Mengidentifikasi area audit: Auditor harus mengidentifikasi area audit yang perlu ditinjau, termasuk aplikasi, infrastruktur teknologi informasi, dan proses bisnis yang terkait dengan sistem informasi. Auditor harus mempertimbangkan risiko dan dampak yang mungkin terjadi dalam setiap area audit.

- Mengembangkan strategi audit: Auditor harus mengembangkan strategi audit yang sesuai dengan tujuan audit dan area audit yang telah diidentifikasi. Strategi audit harus mencakup metode pengumpulan bukti, pengujian kontrol, dan evaluasi hasil audit.
- Memilih metode pengumpulan bukti: Auditor harus memilih metode pengumpulan bukti yang sesuai dengan tujuan audit dan strategi audit. Metode pengumpulan bukti yang umum digunakan meliputi pengamatan, wawancara, dan pengujian.
- Mengembangkan program audit: Auditor harus mengembangkan program audit yang mencakup rincian tugas-tugas yang harus dilakukan oleh auditor dalam pengumpulan bukti. Program audit harus mencakup jadwal audit, daftar pertanyaan, dan checklist pengujian kontrol.
- Menentukan jadwal audit: Auditor harus menentukan jadwal audit yang memungkinkan pengumpulan bukti dilakukan dengan efektif dan efisien. Jadwal audit harus memperhatikan jadwal operasional organisasi, jadwal libur, dan jadwal pelaporan.

Dalam melakukan perencanaan pengumpulan bukti, auditor harus mempertimbangkan risiko yang mungkin terjadi dan memastikan bahwa pengumpulan bukti dilakukan dengan hati-hati dan sesuai dengan standar audit yang berlaku. Hasil dari perencanaan pengumpulan bukti dapat digunakan oleh auditor untuk mengevaluasi efektivitas dan efisiensi dari sistem informasi serta menyarankan perbaikan dan perbaikan yang diperlukan.

9.3.2 Pelaksanaan Pengumpulan Bukti

Setelah proses perencanaan dilakukan, maka auditor dapat memulai tahapan pengumpulan bukti. Pengumpulan bukti merupakan proses untuk mengumpulkan informasi dan data yang dapat digunakan untuk mendukung

kesimpulan dan temuan audit (Gantz, 2013). Auditor harus memastikan bahwa bukti yang dikumpulkan berasal dari sumber yang sah, akurat, dan dapat dipercaya. Selain itu, auditor juga harus memastikan bahwa bukti tersebut tidak diubah atau dimanipulasi selama proses pengumpulan.

Auditor harus memilih metode pengumpulan bukti yang paling efektif untuk memperoleh bukti yang relevan dan cukup untuk mendukung kesimpulan dan temuan audit (Champlain, 2003). Teknologi informasi dapat digunakan untuk mempercepat proses pengumpulan bukti dan memperoleh bukti yang lebih akurat dan relevan. Namun, auditor juga harus memahami risiko dan kelemahan yang terkait dengan penggunaan teknologi informasi dalam pengumpulan bukti.

9.3.3 Evaluasi Hasil Pengumpulan Bukti

Evaluasi hasil pengumpulan bukti adalah proses untuk menilai kecukupan, keandalan, dan relevansi bukti yang telah dikumpulkan selama audit. Evaluasi dapat dilakukan dengan memeriksa, menganalisis, dan mengevaluasi bukti yang telah dikumpulkan, serta memastikan keandalan dan relevansi bukti tersebut terhadap tujuan audit (Gantz, 2013). Evaluasi hasil pengumpulan bukti pada proses audit memiliki beberapa tujuan, yaitu:

- Menentukan apakah informasi yang diperoleh sudah cukup dan relevan untuk menunjang kesimpulan dan opini auditor.
- Memastikan bahwa informasi yang diperoleh sudah akurat dan dapat dipercaya.
- Menentukan apakah ada indikasi atau bukti yang menunjukkan adanya masalah atau ketidakpatuhan yang signifikan dalam sistem atau entitas yang diaudit.
- Menentukan apakah prosedur pengujian yang telah dilakukan sudah memadai dan efektif.

9.4 Teknik Pengumpulan Bukti pada Audit Sistem Informasi

Teknik pengumpulan bukti pada audit sistem informasi adalah suatu metode yang digunakan oleh auditor untuk memperoleh informasi dan data yang relevan dan cukup dalam mengevaluasi efektivitas dan efisiensi pengelolaan sistem informasi dalam suatu organisasi. Teknik-teknik pengumpulan bukti yang umum digunakan dalam audit sistem informasi antara lain:

Beberapa teknik pengumpulan bukti yang umum digunakan dalam audit antara lain Observasi, wawancara, dokumentasi, pengujian substantif, dan pengamatan fisik (Gantz, 2013).

Dalam memilih teknik pengumpulan bukti yang tepat, auditor harus mempertimbangkan sumber bukti yang tersedia, risiko yang dihadapi perusahaan, dan tujuan audit yang ingin dicapai. Selain itu, auditor juga harus memastikan bahwa teknik pengumpulan bukti yang digunakan telah sesuai dengan standar audit yang berlaku dan dapat memberikan bukti yang cukup dan memadai.

9.4.1 Observasi

Gantz (2013) menjelaskan bahwa observasi merupakan teknik pengumpulan bukti yang melibatkan pengamatan langsung terhadap aktivitas atau proses yang terjadi dalam sistem informasi. Teknik ini dapat dilakukan secara pasif, hanya dengan memperhatikan proses yang terjadi, atau secara aktif dengan mengajukan pertanyaan dan meminta penjelasan terkait proses tersebut.

Dalam observasi, auditor dapat memperhatikan bagaimana sistem informasi berjalan sehari-hari, bagaimana data diproses, dan bagaimana sistem dioperasikan oleh karyawan. Dengan melakukan observasi, auditor dapat memperoleh pemahaman yang lebih mendalam tentang

proses dan aktivitas yang terjadi dalam sistem informasi dan dapat membantu auditor menentukan apakah sistem tersebut efektif, efisien, dan memenuhi standar keamanan yang diperlukan.

Dalam melakukan observasi, auditor dapat menggunakan beberapa teknik, seperti pengamatan langsung terhadap karyawan saat mereka menggunakan sistem informasi, pengamatan terhadap dokumen dan catatan transaksi, atau pengamatan terhadap aktivitas atau proses tertentu yang terjadi dalam sistem informasi. Hasil dari observasi dapat digunakan oleh auditor untuk mengidentifikasi potensi masalah atau kelemahan dalam sistem informasi dan membantu auditor mengambil tindakan yang diperlukan untuk meningkatkan keamanan dan efektivitas sistem informasi.

Berikut adalah beberapa contoh observasi yang dapat dilakukan oleh auditor dalam audit sistem informasi, antara lain (Moeller, 2010) :

1. Pengamatan langsung terhadap penggunaan sistem informasi oleh karyawan: Auditor dapat memperhatikan bagaimana karyawan menggunakan sistem informasi, mulai dari login, memasukkan data, hingga memproses transaksi. Auditor dapat mengamati apakah karyawan mengikuti prosedur yang telah ditetapkan dan apakah ada tanda-tanda kecurangan atau pelanggaran keamanan yang terjadi.
2. Pengamatan terhadap operasi sistem informasi: Auditor dapat mengamati bagaimana sistem informasi beroperasi dan bagaimana data diproses oleh sistem tersebut. Auditor dapat memperhatikan bagaimana sistem menghasilkan laporan dan bagaimana sistem dioperasikan oleh administrator.
3. Pengamatan terhadap sistem jaringan: Auditor dapat mengamati sistem jaringan yang digunakan oleh organisasi dan memperhatikan bagaimana data dikirim dan diterima melalui jaringan tersebut. Auditor dapat

memperhatikan apakah ada potensi ancaman keamanan yang muncul dari penggunaan jaringan.

4. Pengamatan terhadap prosedur keamanan sistem informasi: Auditor dapat memperhatikan prosedur keamanan sistem informasi, seperti prosedur penggunaan kata sandi, prosedur identifikasi pengguna, dan prosedur pengamanan data. Auditor dapat memperhatikan apakah prosedur-prosedur tersebut dilaksanakan dengan baik oleh karyawan.

Dalam melakukan observasi, auditor harus memperhatikan hal-hal yang penting untuk dilindungi, seperti data sensitif dan informasi rahasia organisasi. Auditor juga harus berhati-hati agar tidak mengganggu operasi sistem informasi dan tidak mempengaruhi kinerja karyawan. Hasil dari observasi dapat digunakan oleh auditor untuk mengevaluasi efektivitas dan efisiensi dari sistem informasi serta memastikan bahwa sistem tersebut terlindungi dari ancaman keamanan yang mungkin terjadi.

9.4.2 Wawancara

Wawancara merupakan teknik pengumpulan bukti yang melibatkan percakapan langsung antara auditor dan responden. Wawancara dapat dilakukan untuk memperoleh informasi tentang kebijakan, prosedur, dan praktik kerja yang terkait dengan sistem informasi (Gantz, 2013). Wawancara merupakan teknik pengumpulan bukti yang penting karena dapat memberikan informasi yang tidak dapat diperoleh dari dokumen atau catatan tertulis. Wawancara dapat dilakukan dengan berbagai pihak yang terkait dengan sistem informasi, seperti manajemen, pengguna sistem, dan personel TI (Champlain, 2003).

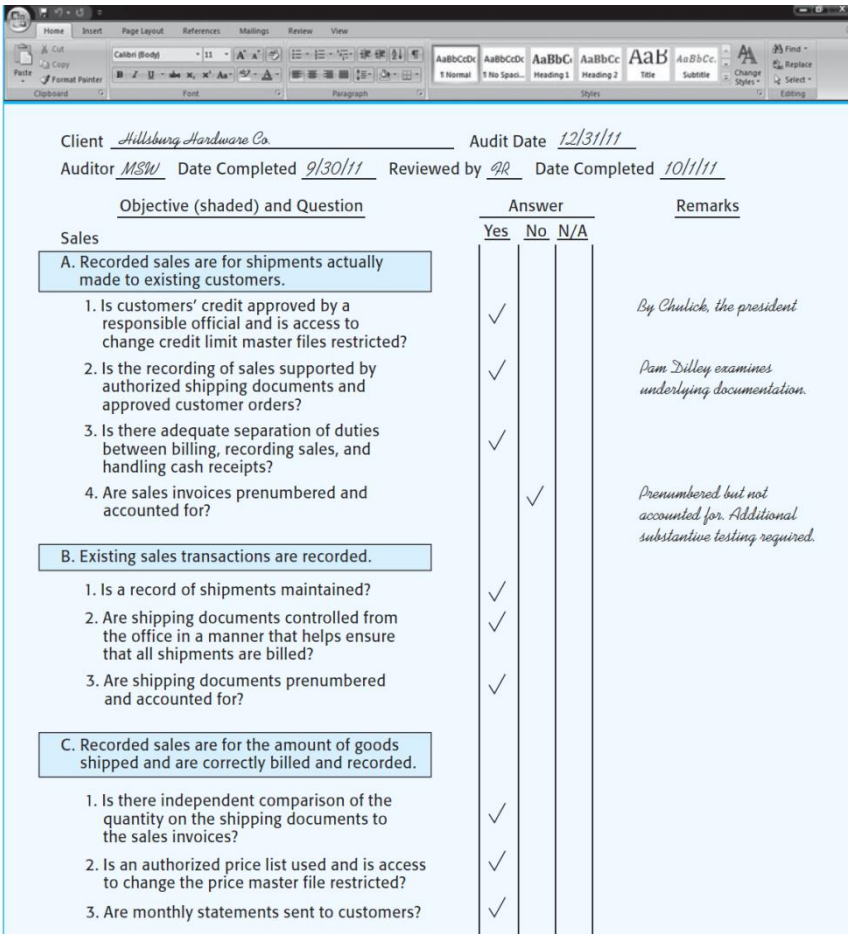
Persiapan yang baik sebelum melakukan wawancara adalah kunci keberhasilan teknik wawancara. Auditor harus memahami tujuan dan ruang lingkup wawancara, serta

menyiapkan pertanyaan yang relevan dan spesifik. Persiapan yang baik dapat membantu auditor untuk memperoleh informasi yang lebih akurat dan lengkap. Selama wawancara, auditor harus membangun hubungan yang baik dengan responden. Auditor harus menghormati waktu dan kebutuhan responden, serta menghindari sikap yang menakutkan atau mengancam. Hubungan yang baik dapat membantu auditor untuk memperoleh informasi yang lebih jujur dan terbuka dari responden (Arens, Elder, & Beasley, 2012).

Auditor harus mencatat hasil wawancara dengan baik. Auditor harus mencatat jawaban responden secara lengkap dan akurat, serta menghindari interpretasi yang berlebihan. Catatan yang baik dapat membantu auditor untuk memahami informasi yang diperoleh dari wawancara dan memperjelas temuan dan kesimpulan audit.

9.4.3 Kuesioner

Kuesioner merupakan teknik pengumpulan bukti dengan memanfaatkan dokumen tertulis yang dapat berupa dokumen fisik maupun elektronik yang diisi oleh responden dan dapat dipandu oleh auditor. Kuesioner berbeda dengan wawancara yang memberikan informasi rinci dan mendalam, kuesioner lebih standar dan kurang fleksibel, dan tidak memungkinkan auditor untuk memperoleh informasi tambahan secara langsung namun, kuesioner biasanya membutuhkan waktu yang lebih cepat dibandingkan dengan wawancara dan memnugkinkan mengumulkan banyak data dari berbagai responden dalam waktu yang relatif singkat dari wawancara (Arens, Elder, & Beasley, 2012). Dalam mengukur jawaban dari setiap pertanyaan pada kuesioner dapat digunakan Skala Likert atau jawaban Ya dan Tidak yang dapat dilihat pada gambar 9.1.



Client Hillsburg Hardware Co. Audit Date 12/31/11

Auditor MSW Date Completed 9/30/11 Reviewed by GR Date Completed 10/1/11

Objective (shaded) and Question	Answer Yes	Answer No	Answer N/A	Remarks
Sales				
A. Recorded sales are for shipments actually made to existing customers.				
1. Is customers' credit approved by a responsible official and is access to change credit limit master files restricted?	✓			By Chulick, the president
2. Is the recording of sales supported by authorized shipping documents and approved customer orders?	✓			Pam Dilley examines underlying documentation.
3. Is there adequate separation of duties between billing, recording sales, and handling cash receipts?	✓			
4. Are sales invoices prenumbered and accounted for?		✓		Prenumbered but not accounted for. Additional substantive testing required.
B. Existing sales transactions are recorded.				
1. Is a record of shipments maintained?	✓			
2. Are shipping documents controlled from the office in a manner that helps ensure that all shipments are billed?	✓			
3. Are shipping documents prenumbered and accounted for?	✓			
C. Recorded sales are for the amount of goods shipped and are correctly billed and recorded.				
1. Is there independent comparison of the quantity on the shipping documents to the sales invoices?	✓			
2. Is an authorized price list used and is access to change the price master file restricted?	✓			
3. Are monthly statements sent to customers?	✓			

Gambar 9.1 Contoh Kuesioner yang digunakan dalam Audit
(Sumber : Arens, Elder, & Beasley, 2012)

9.4.4 Pengumpulan Dokumen

Bukti dokumen adalah salah satu jenis bukti audit yang digunakan oleh auditor untuk mendukung kesimpulan audit. Bukti dokumen adalah data atau informasi yang disimpan dalam bentuk dokumen atau catatan tertulis, seperti faktur, kwitansi, bukti pembayaran, kontrak, perjanjian, dan laporan keuangan. Dokumen tersebut dapat berasal dari klien atau pihak ketiga yang berkaitan dengan klien.

Pengumpulan bukti dokumen dalam audit dilakukan dengan beberapa langkah sebagai berikut (Arens, Elder, & Beasley, 2012):

- Menentukan jenis bukti yang dibutuhkan untuk mendukung kesimpulan audit yang diperoleh. Auditor harus menentukan jenis bukti yang dibutuhkan berdasarkan tujuan audit, risiko audit, dan jenis informasi yang dibutuhkan untuk menyimpulkan tentang kebenaran dan kesesuaian laporan keuangan.
- Mencari dan mengumpulkan dokumen yang dibutuhkan dengan cara meminta dokumen dari klien atau pihak ketiga yang berkaitan dengan klien. Auditor harus mengumpulkan dokumen dari sumber yang dapat dipercaya dan dapat memberikan bukti yang cukup untuk mendukung kesimpulan audit.
- Menyeleksi dokumen yang relevan dan dapat diandalkan untuk digunakan sebagai bukti audit. Auditor harus menyeleksi dokumen yang dapat memberikan bukti yang cukup dan dapat dipercaya untuk mendukung kesimpulan audit.
- Mengorganisir dan menyimpan dokumen dengan rapi sehingga mudah diakses dan dapat dijadikan referensi di masa mendatang. Auditor harus menyimpan dokumen dengan rapi dan mengatur dokumen sesuai dengan kriteria tertentu, seperti jenis dokumen, tanggal, atau kategori lainnya agar mudah diakses dan dijadikan referensi di masa mendatang.

Didalam melakukan audit sistem informasi, ada beberapa jenis dokumen yang dapat dikumpulkan saat melakukan audit sistem informasi antara lain (Gantz, 2013):

- Kebijakan dan Prosedur: Dokumen kebijakan dan prosedur adalah dokumen yang menjelaskan bagaimana sistem informasi berfungsi, bagaimana mengelola dan menjaga keamanan data, serta bagaimana mengelola risiko pada sistem informasi.

- Dokumen Proyek: Dokumen proyek mencakup rencana proyek, jadwal proyek, dan dokumen lain yang terkait dengan proyek pengembangan sistem informasi.
- Dokumen Sistem: Dokumen sistem mencakup desain sistem, dokumentasi teknis, diagram arsitektur jaringan, konfigurasi, dan dokumen pengujian sistem.
- Data dan Catatan: Data dan catatan meliputi dokumen yang memuat informasi terkait data dan catatan pada sistem informasi, seperti log aktivitas, catatan masuk, catatan transaksi, dan dokumen terkait manajemen keamanan data.
- Bukti Fisik: Bukti fisik mencakup dokumen terkait dengan infrastruktur IT fisik, seperti catatan peralatan, dokumen perbaikan, dan kontrak pemeliharaan.
- Laporan Audit Sebelumnya: Laporan audit sebelumnya, termasuk laporan audit internal dan eksternal, serta laporan pemeriksaan kepatuhan, dapat memberikan informasi berharga untuk melakukan audit sistem informasi.

Bukti dokumen tersebut dapat membantu auditor dalam mengevaluasi keamanan dan kehandalan sistem informasi, mengidentifikasi risiko dan masalah, serta memberikan saran perbaikan pada sistem informasi. Oleh karena itu, pengumpulan bukti dokumen merupakan bagian penting dalam melakukan audit sistem informasi.

9.4.5 Pengujian Substantif

Pengujian substantif adalah salah satu pengujian audit yang bertujuan untuk memperoleh bukti bahwa saldo yang ada dalam sistem informasi secara substansial benar. Pengujian ini bertujuan untuk memverifikasi kebenaran dan ketepatan data. Dalam konteks audit TI, pengujian substantif dapat dilakukan untuk menguji keandalan sistem, data dan informasi, serta proses bisnis yang dilakukan oleh sistem (Gallegos & Senft, 2008). Tabel 9.1 menunjukkan beberapa

teknik pengujian substantif yang dapat dilakukan saat melakukan audit sistem informasi.

Tabel 9.1 Pengujian Substantif Audit Sistem Informasi

No	Teknik	Keterangan
1	Pengujian atas detail transaksi	Bertujuan untuk menguji kebenaran dan keabsahan transaksi yang tercatat dalam sistem informasi
2	Pengujian atas detail saldo	Bertujuan untuk menguji kebenaran saldo akun dalam sistem informasi dan memastikan saldo mencerminkan kondoso keuangan sebenarnya
3	Pengujian atas prosedur operasional	Bertujuan untuk menguji efektivitas dan keandalan prosedur operasional yang dilakukan oleh sistem informasi dan memastikan telah berjalan sesuai dengan standar dan kebijakan yang berlaku
4	Pengujian atas keamanan dan privasi	Bertujuan untuk menguji keamanan dan privasi data dalam sistem informasi, serta memastikan bahwa data tersebut telah dijaga dengan baik dari anaman keamanan

Sumber: Gallegos & Senft, 2008

9.5 Etika dan Standar Profesional Pengumpulan Bukti pada Audit Sistem Informasi

Etika dan standar profesional dalam pengumpulan bukti pada audit sistem informasi sangat penting untuk memastikan bahwa proses audit dilakukan secara obyektif, independen, dan akurat. Etika dan standar profesional ini memastikan bahwa auditor mengikuti prinsip-prinsip yang adil dan objektif dalam memperoleh dan mengevaluasi bukti-bukti yang diperoleh selama audit.

Dalam pengumpulan bukti pada audit sistem informasi, auditor harus memperoleh bukti secara independen. Auditor tidak boleh menerima atau mengandalkan pada bukti yang diberikan oleh pihak lain tanpa memverifikasi keabsahannya terlebih dahulu. Auditor juga harus memastikan bahwa bukti yang diperoleh telah diverifikasi dan terdokumentasi dengan baik.

Terakhir, auditor harus memastikan bahwa bukti yang diperoleh telah disimpan dengan aman dan terjaga kerahasiaannya. Buktibukti yang diperoleh harus dilindungi dari akses yang tidak sah dan hanya digunakan untuk tujuan audit yang sah.

Dengan mengikuti etika dan standar profesional dalam pengumpulan bukti pada audit sistem informasi, auditor dapat memastikan bahwa audit dilakukan secara obyektif, independen, dan akurat. Hal ini akan membantu memastikan keandalan informasi yang diperoleh selama audit dan meningkatkan kepercayaan pada hasil audit yang dikeluarkan.

9.5.1 Etika Pengumpulan Bukti

Etika merupakan ilmu yang mempelajari mengenai moralitas manusia (Bertens, 2007). Dalam melakukan audit, auditor perlu untuk menjaga etika agar dapat memastikan bahwa pengumpulan bukti dilakukan dengan cara yang

benar dan andal, serta dapat menjaga integritas dan profesionalisme dalam pelaksanaan tugas audit. Selain itu, auditor juga harus menghindari konflik kepentingan, menjaga independensi, dan menghormati kerahasiaan informasi klien untuk memastikan bahwa audit dilakukan secara objektif dan dapat diandalkan. Ada beberapa prinsip etika yang harus diterapkan oleh auditor dalam pengumpulan bukti antara lain (Kegerreis, Schiller, & Davis, 2020) :

- Kerahasiaan: Auditor harus menjaga kerahasiaan informasi yang diperoleh selama proses audit. Auditor tidak boleh mengungkapkan informasi kepada pihak yang tidak berwenang tanpa persetujuan dari klien.
- Integritas: Auditor harus berintegritas dalam pengumpulan, evaluasi, dan presentasi bukti. Auditor harus jujur dan adil dalam semua interaksi dengan klien dan pihak lain yang terkait dengan audit.
- Kompetensi: Auditor harus memiliki pengetahuan, keahlian, dan pengalaman yang memadai dalam melaksanakan pekerjaan audit dan pengumpulan bukti yang berkaitan dengan sistem informasi.
- Independensi: Auditor harus independen dan bebas dari pengaruh yang dapat mempengaruhi pandangan dan tindakan mereka. Auditor harus dapat melakukan audit secara objektif dan tidak terlibat dalam kegiatan yang dapat menimbulkan konflik kepentingan.
- Profesionalisme: Auditor harus mematuhi aturan dan etika profesi audit serta mempertahankan standar profesionalitas yang tinggi dalam melaksanakan tugasnya.

9.5.2 Standar Profesi Pengumpulan Bukti

Selain Etika, Auditor juga harus mematuhi standar profesional dalam pengumpulan bukti. Standar profesional ini menentukan bagaimana auditor harus mengumpulkan

bukti, apa jenis bukti yang harus dikumpulkan, dan bagaimana cara mengevaluasi bukti yang telah dikumpulkan.

Standar profesional dalam pengumpulan bukti pada audit sistem informasi menekankan bahwa bukti harus diperoleh secara memadai dan relevan. Artinya, bukti yang diperoleh harus cukup untuk mendukung kesimpulan yang dibuat oleh auditor dan relevan dengan tujuan audit. Selain itu, bukti harus diperoleh dengan cara yang obyektif dan tidak memihak. Ada berberapa standart profesi yang berkaitan dengan pengumpulan bukti, yakni : Standar Profesional Akuntan Publik (SPAP) yang dikeluarkan oleh Ikatan Akuntan Indonesia (IAI), International Standards for the Professional Practice of Internal Auditing (IPPF) dan Information Technology Infrastructure Library (ITL).

9.6 Kendala dan Tantangan dalam Pengumpulan Bukti pada Audit Sistem Informasi

Pengumpulan bukti pada audit sistem informasi dapat menghadapi berbagai kendala dan tantangan yang mempengaruhi kualitas dan akurasi bukti yang diperoleh. Salah satu kendala utama adalah keterbatasan akses terhadap sistem informasi yang diaudit. Hal ini dapat terjadi jika perusahaan tidak memberikan akses yang memadai untuk auditor untuk melakukan audit pada sistem informasi mereka. Tanpa akses yang memadai, auditor dapat kesulitan untuk memperoleh bukti yang cukup untuk mendukung kesimpulan mereka.

Selain itu, kompleksitas dan keragaman sistem informasi yang ada di dalam perusahaan dapat menjadi tantangan bagi auditor dalam memilih teknik dan prosedur audit yang sesuai. Setiap sistem informasi memiliki karakteristik dan persyaratan audit yang berbeda, dan auditor perlu memahami dengan baik sistem yang sedang

diaudit untuk memilih teknik dan prosedur audit yang paling tepat.

Tantangan lainnya adalah terkait dengan jumlah dan sumber bukti yang tersedia. Sistem informasi yang kompleks dan besar dapat menghasilkan ribuan bukti yang harus dikumpulkan dan dievaluasi oleh auditor. Keterbatasan waktu dan sumber daya dapat membuat proses pengumpulan dan evaluasi bukti menjadi sulit dan memakan waktu.

Selain itu, tantangan lainnya adalah terkait dengan integritas dan kredibilitas bukti yang diperoleh. Bukti-bukti yang diperoleh mungkin tidak lengkap atau tidak akurat, dan auditor perlu memastikan bahwa bukti yang diperoleh telah diverifikasi dengan benar dan diperoleh dari sumber yang terpercaya.

Terakhir, faktor keamanan dan privasi juga dapat menjadi kendala dalam pengumpulan bukti pada audit sistem informasi. Auditor perlu memastikan bahwa bukti yang diperoleh telah dilindungi dengan baik dan tidak akan menimbulkan masalah keamanan atau privasi yang dapat membahayakan perusahaan.

Dalam menghadapi kendala dan tantangan dalam pengumpulan bukti pada audit sistem informasi, auditor perlu memilih teknik dan prosedur audit yang tepat dan memastikan bahwa proses audit dilakukan secara obyektif, independen, dan akurat. Hal ini akan membantu memastikan bahwa bukti yang diperoleh selama audit dapat mendukung kesimpulan dan rekomendasi yang dikeluarkan oleh auditor.

DAFTAR PUSTAKA

Kegerreis, M., Schiller, M., & Davis, C. (2020). *IT Auditing Using Controls to Protect Information Assets.* McGraw-Hill Education.

Arens, A. A., Elder, R. J., & Beasley, M. (2012). *Auditing and Assurance Services: An Integrated Approach, 14th Edition.* Boston : Prentice Hall.

Bertens, K. (2007). *Etika.* PT Gramedia Pustaka Utama.

Cascarino, R. (2007). *Auditor's Guide to Information Systems Auditing.* John Wiley & Sons, Inc.

Champlain, J. (2003). *Auditing Information Systems.* John Wiley.

Gallegos, F., & Senft, S. (2008). *Information Technology Control and Audit.* Auerbach Publications.

Gantz, S. (2013). *The Basics of IT Audit: Purposes, Processes, and Practical Information.* Syngress.

Moeller, R. (2010). *IT Audit, Control, and Security.* Wiley.

Otero, & Angel. (2019). *Information Technology Control and Audit.* Auerbach Publications.

Peret, P. (2022). *Information System Audit: How to Control the Digital Disruption.* CRC Press.

BAB 10
PROSES EVALUASI BUKTI PADA AUDIT SISTEM INFORMASI

10.1 Pendahuluan

Setelah melewati proses pengumpulan bukti-bukti audit, maka dilanjutkan dengan proses evaluasi terhadap bukti-bukti audit tersebut. Tahapan ini auditor melakukan analisa satu persatu terhadap bukti-bukti audit yang telah dikumpulkan. Proses penilaian bukti-bukti diharapkan memberikan dua hasil yaitu baik dan tidak baik. Indikator baik dalam penilaian ini bermaksud bahwa auditor menemukan aspek aspek penting dalam sistem. Sedangkan indikator tidak baik yang dimaksud yaitu auditor menemukan sesuatu yang tidak penting dalam sistem. Sehingga dalam hal proses evaluasi bukti, auditor perlu memastikan bahwa dalam sistem sudah tidak ada *error*. Jika pada kenyataannya masih ditemukan *error* maka auditor wajib menemukan solusi yang dapat mengatasi *error* tersebut. Sejalan dengan Sunanto (2014) mengatakan setelah proses audit dilaksanakan, hasil pengolahan dan analisis data akan dinilai kemudian disusun menjadi sebuah rekomendasi terhadap sistem. Rekomendasi tersebut berdasarkan analisis hasil audit yang diharapkan mampu menjadi referensi dalam peningkatan kualitas tata kelola sebuah sistem.

Sering kali terjadi banyak kesalahan dalam sistem, auditor diharapkan mampu menemukan dan melaporkan temuan-temuan tidak wajar dari laporan internal. Pada

semua tahapan audit, hasil temuan dan kesimpulan wajib didokumentasikan dalam bentuk laporan fisik kerja audit. Dokumentasi merupakan hal yang sangat penting tahap evaluasi bukti. Pada tahapan evaluasi ada beberapa aspek penting yang perlu ditinjau seperti aspek perlindunga aset dan intergritas data, aspek efektivitas dan efisiensi sistem, aspek keguanaan dan aspek ekonomis dan aspek kepuasan pengguna.

10.2 Evaluasi Perlindungan Aset dan Integritas Data

Pada bagian ini merupakan cara auditor untuk melakukan evaluasi terhadap aset yang dilindungi dan mengevaluasi pengolahan data *integrity* sebuah sistem yang baik. Evaluasi perlindungan aset dan integritas data biasanya berurusan dengan prosedur evaluasi bukti dan keputusan pertimbangan yang diambil oleh auditor selama audit awal dan selanjutnya. Kualitas, ukuran, dan teknik pengamanan aset dan integritas data ketika diperiksa secara bersama-sama menghubungkan tingkat perhatian terhadap pertimbangan efektivitas biaya, pengendalian internal, dan dampak pengambilan keputusan global menggunakan bukti sedikit demi sedikit. Rancangan sistem pengendalian internal yang tepat, dikombinasikan dengan dampak keamanan dan risiko data yang tepat serta keandalan komputer, membentuk suasana di mana penilaian auditor, serta penilaian manajemen dilakukan (Rushinek & Rushinek, 1989).

Auditor dalam mengukur perlingdungan aset (asset safeguarding) dengan menggunakan *expected loss* yang terjadi jika ada kerusakan, pencurian atau digunakan untuk tujuan yang tidak baik oleh pihak yang tidak berwenang. Sementara, ukuran *data integrity* oleh auditor tergantung

pada tujuan audi dilakukan serta *nature of the data* yang akan difokuskan. Umumnya auditor eksternal akan berfokus pada kemungkinan *error* laporan keuangan sedangkan auditor internal akan berfokus pada kemungkinan terjadinya error di masa akan datang.

10.2.1 Natur of the Global Evaluation Decision

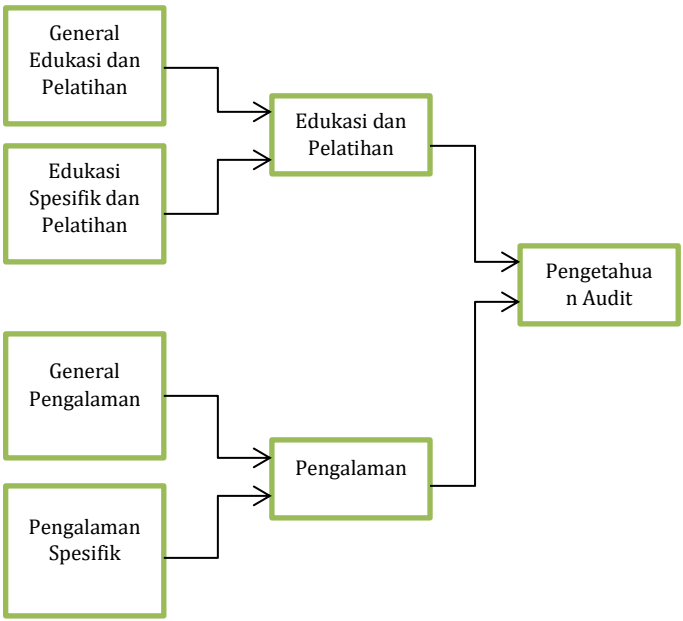
Ketika membuat keputusan dalam evaluasi, auditor harus menemukan dampak kekuatan control dan kelemahan dalam perlindungan aset serta seberapa baik aset tersebut dilindungi. Auditor diharapkan memberi saran dan masukkan kepada pihak manajemen serta membantu dalam mempertimbangkan kemungkinan kerugian dari perlindungan aet dan pemeliharaan integritas data.

10.2.2 Determinants of Judgement Performace

Pada bagian ini mengacu pada Libby dan Luft tahun 1993 yang berpendapat bahwa terdapat empat kategori penentu performa penilaian, yaitu:

1. *Auditor's ablity* (Kemampuan Membuat Keputusan)
   Masing-masing manusia memiliki kemampuan pengetahuan dan memiliki keterbatasan. Namun kemampuan pengetahuan (kognitif) tersebut mampu membentuk kualitas dalam penelitian yang di kaji seperti kemampuan dalam mengindentifikasi korelasi dan pola bayangan. Faktanya hasil penelitian menunjukkan bahwa kita cenderung membuat penilaian heuristik yang kadang tidak sesuai dengan penilaian kualitas tinggi. Tversky dan Kahneman (1974) menyebutkan tiga heuristik yang dapat mengatasi kompleksitas tugas kognitig di waktu yang sama terapi dapat menurunkan kualitas penilaian, yaitu *representative heuristic*, *anchoring and adjurtment heuristic* dan *availability heuristic*.

4. Auditor's Knowledge (Pengetahuan Pembuat Keputusan)
   Sumber pengetahuan auditor berasal dari edukasi dan pelatihan yang diterima serta pengalaman dalam mengaudit. Berikut bagan yang menggambarka sumber pengetahuan audtor.



Gambar 10.1 Skema Pengetahuan Auditor
(Sumber : Libby dan Luft tahun 1993)

2. *Audit Environment*
   Lingkungan audit mendeskipsikan konteks dimana auditor harus membuat penilaian evaluasi. Libby dan Luft (1993) menyebutkan karakteristik yang digunakan auditor dalam membuat penilaian, yaitu *audit technology*, *group process, prior involvement*, dan *accountability*.
3. *Auditor's Motivation*
   Motivasi auditor dalam melaksanakan tugasnya dapat dipengaruhi oleh usaha mereka dalam melaksanakan

tugasnya dan proses kognitif yang dihubungkan dengan tugas.

10.3 Evaluasi Efektivitas dan Efisiensi Sistem

Menurut pendapat Rai (2008) efektifitas merupakan hubungan antara *outcome* dan *output*. Terdapat dua kategori *outcome*, yaitu perubahan kondisi dan perubahan perilaku. Salah satu contoh perubahan kondisi adalah perbaikan mutu kesehatan masyarakat atau kebersihan air. Sementara contoh perubahan perilaku adalah adanya perubahan sikap para pelaku tindak kriminal sering berjalannya sistem peradilan aau perubahan sikap orang tua dan anak berkat peran dinas sosial dalam mengurangi tinda kekerasan dalam keluarga. Perubahan perilaku lebih sulit diukur dari pada perubahan kondisi. Sedangkan menurut Tangkilisan (2005) efisiensi mengandung makna perbandingan antara biaya dan hasil. Rei (2008) juga menuliskan bahwa efisiensi merupakan perbandingan antara *output* dan *input*.

10.3.1. Evaluasi Efektivitas Sistem

Efektivitas merupakan hal yang dituju dan ingin dicapai disesuaikan pada perencanaan yang sudah ditetapkan sebelumnya secara bersama-sama (Waruwu & Masitho, 2016). Efektifitas sistem informasi adalah suatu ukuran seberapa jauh ketercapaian target sistem mulai dari mengumpulkan, memproses, menampilkan hasil serta menyimpan data. Penilaian efektifitas suatu sistem bergantung pada kesesuaian capaian terhadap fungsi utama dari sistem tersebut. Hidayat, Fitrianingrum & Hudiwasono (2021) merumuskan alat penilaian atau *assisment tools* prinsip efektifitas dari sudut padang penelitian. Namun indikator penilaiannya dapat dijadikan acuan penilaian efektifitas sebuah sistem.

Tabel 10.1 *Assisment Tools* Prinsip Efektifitas

Sub Kriteria	Bukti	Rating	Nilai Rating	%	Nilai
Apakah rancangan Kegiatan Penelitian Mampu Mencapai Target	Adakah bukti yang sangat kuat yang menyatakan input dapat mencapai output	3	Sangat efektif	15	0,45
	Tersedianya bukti yang menyatakan bahwa input dapat mencapai output	2	Efektif		0,3
	Terbatasnya bukti yang menyatakan input dapat mencapai output	1	Sebagian efektif		0,15
	Tidak ada bukti yang menyatakan input dapat mencapai output	0	Tidak efektif		0
Apakah hasil kegiatan penelitian dapat di implementasikan	Adakah bukti yang sangat kuat bahwa output dapat dimplementasikan	3	Sangat efektif	10	0,3
	Tersedianya bukti yang menyatakan output dapat diimplementasikan	2	Efektif		0,2
	Terbatasnya bukti yang menyatakan output dapat diimplementasikan	1	Sebagian efektif		0,1
	Tidak terdapat bukti yang menyatakan output dapat	0	Tidak efektif		0

Sumber: Hidayat, Fitrianingrum & Hudiwasono (2021)

Berdasarkan assisment toos prinsip efektifitas di atas, dapat dilihat apakah suatu fungsi setiap kegiatan efektif atau tidak. Ukuran efektif tidaknya sesuai dengan rating dan persen. Persen yang diberikanpun variatif sesuai keinginan auditor.

10.3.2. Evaluasi Efisiensi Sistem

Efisiensi adalah perbandingan terbaik antara suatu kegiatan dengan hasilnya. Menurut Mulyamah (1987), efisiensi merupakan suaru ukuran dalam membandingkan rencana penggunaan masukkan dengan penggunaan yang direalisasikan atau perkaataan lain penggunaan yang sebenarynya. Efisiensi sistem informasi adalah ukuran keberhasilan suatu sistem yang dilihat berdasarkan sumber daya untuk mencapai tujuan dan fungsinya. Umumnya efisien mengacu pada besar kecilnya sumber/biaya untuk mencapai keberhasilan suatu kegiatan. Menurut Steven M. Sheffrin (2003) tujuan dari efisien adalah :

1. Dapat meningkatkan terciptanya keluaran yang diinginkan, dapat dihasilkan secara optimal dengan hanya masukkan yang relativ tetap, atau jika masukkan sekecil mungkin dapat menghasilkan keluaran yang optimal.
2. Dengan meningkatkan efisensi maka keseimbangan antara penyediaan dan kebutuhan akan sumber-sumber terjaga sehingga upaya pencapaian tujuan tidak mengalami hambatan.

Hidayat, Fitrianingrum & Hudiwasono (2021) juga merumuskan alat penilaian prinsip efisiensi berdasarkan sudut pandang *Economic Internal Rate of Return* (EIRR). EIRR merupakan tingkat pengembalian berdasarkan penentuan nilai tingkat bunga (*discount rate*), dimana semua keuntungan masa depan yang dinilai sekarang dengan discount rate tertentu adalah sama dengan biaya kapital atau present value dari total biaya.

Penilaian efisiensi mengacu pada keberhasilan suatu sistem dalam menyelesaikan tugas dan fungsinya dengan minimal coast atau biaya yang dikeluarkan. Seperti hal EIRR, penilaian efisiensi suatu sistem dapat mengadopsi indikator EIRR dengan menyesuaikan dengan fungsi dan tugas dari sistem informasi yang akan di evaluasi aspek efisiensinya.

Tabel 10.2 *Assisment Tools* Prinsip Efisiensi

Sub Kriteria	Bukti	Rating	Nilai Rating	%	Nilai
EIRR (Economic Internal Rate of Return)	Adakah bukti yang sangat kuat yang menyatakan bahwa kegiatan dapat mencapai estimasi EIRR	3	Sangat efisien	10	0,3
	Tersedianya bukti yang menyatakan bahwa kegiatan dapat mencapai estimasi EIRR	2	Efisien		0,2
	Terbatasnya bukti yang menyatakan bahwa kegiatan dapat mencapai estimasi EIRR	1	Sebagian efisien		0,1
	Tidak ada bukti yang menyatakan bahwa kegiatan dapat mencapai estimasi EIRR	0	Tidak efisien		0
Apakah keuntungan ekonomi dapat dicapai dengan biaya paling sedikit	Adakah bukti yang sangat kuat yang menyatakan bahwa keuntungan ekonomi dapat dicapai dengan biaya paling sedikit	3	Sangat efisien	10	0,3
	Tersedianya bukti yang menyatakan bahwa keuntungan ekonomi dapat dicapai dengan biaya paling sedikit	2	Efisien		0,2
	Terbatasnya bukti yang menyatakan bahwa keuntungan ekonomi dapat dicapai dengan biaya paling sedikit	1	Sebagian efisien		0,1
	Tidak terdapat bukti yang menyatakan bahwa keuntungan ekonomi dapat dicapai dengan biaya paling sedikit	0	Tidak efisien		0

Sumber: Hidayat, Fitrianingrum & Hudiwasono (2021)

Berdasarkan alat penilaian prinsip efisiensi di atas, terlihat bahwa suatu kegiatan dapat dikatakan efisien atau tidak berdasarkan kategori rating dan persen. Sama halnya dengan efektifitas, untuk persen dari efisiensi tergantung dari ketetapan editor yang mengaudit.

Lebih lanjut Hidayat, Fitrianingrum & Hudiwasono (2021) menambahkan *asissment tools* secara keseluruhan dari efektifitas dan efisiensi. Hasil penilaian keseluruhan dapat menjadi rekomendasi selanjutnya, apakah perlu pebaikan atau tidak. berikut kategori penilaian rekomendasi :

Tabel 10.3 *Assisment Tools* Prinsip Efisiensi

No	Penilian/Saran	Keterangan	Nilai Rata-Rata
1	Sangat Direkomendasikan	Sangat Baik	1,1 – 1,35
2	Direkomendasikan	Baik	0,46 – 1
3	Direkomendasikan Dengan Syarat Tertentu	Kurang Baik	0,40 – 0,46
4	Dihentikan	Buruk	0 – 0,40

10.4 Evaluasi Kegunaan

Evaluasi kegunaan merupakan tahapan evaluasi bukti untuk melihat fungsi dan kegunaan sistem yang ukur berdasakan penyelesaian terhadap suatu pekerjaan. Indikator evaluasi penilaian pada tahapan ini yaitu:

1. Peningkatan kinerja melalui sistem
   Keberadaan sistem informasi tersebut, dalam penerapannya diharapkan mampu meningkatkan kinerja perusahan. Disini auditor harus mampu menilai kinerja perusahaan melalui ketercapaian tujuan dan fungsi utama dari sistem tersebut
2. Peningkatan produktivitas melalui sistem
   Melalui sistem informasi mampu memberikan pengaruh positif melalui peningkatan produkvitas karyawan

dalam bekerja. Pada tahapan ini auditor harus mampu mengevaluasi bukti berdasarkan hasil produkvitas kerja karyawan selama periode tertentu saat menggunakan sistem informasi.

3. Peningkatan efektivitas

   Bagian ini auditor mengevaluasi bukti berdasarkan peningkatan efektivitas kerja karyawan saat menggunakan sistem informasi
4. Kemudahan bekerja

   Penggunaan sistem informasi diharapkan memberikan kemudahan karyawan dalam bekerja. Auditor harus mengevaluasi sejauh mana sistem informasi tersebut memberi kemudahan pada karyawan dalam bekerja
5. Kegunaan sistem dalam melaksanakan tugasnya.

   Selanjutnya auditor juga perlu melakukan evaluasi terhadap fungsi utama dari sistem informasi. Apakah sistem sudah benar-benar berjalan sesuai dengan tujuan dan fungsinya.

Berdasarkan lima indikator evaluasi tersebut auditor harus melihat ketercapaian dan kesesuaian berdasarkan lima indikator tersebut. Jika ditemukan ada ketidaksesuaian, maka auditor harus membuat rekomendasi terhadap kekurangan yang ditemukan sebagai bahan perbaikan kedepannya.

10.5 Evaluasi Kemudahan Pakai

1. Evaluasi kemudahan pakai merupakan tahapan evaluasi terhadap kemudahan suatu sistem informasi digunakan. Penilaian kemudahan pakai berdasarkan indikator:
2. Mudahnya sistem dipelajari
3. Pada tahapan ini auditor melakukan evaluasi terhadap kemudahan sistem dipelajari.

4. Sistem bekerja sesuai harapan
5. Penting juga dalam melakukan evaluasi sistem informasi melalui fungsi dan tugas utama dari sistem informasi tersebut apakah sudah berjalan sesuai dengan harapan pengguna/karyawan
6. Sistem jelas dan mudah dipahami
7. Dalam hal kemudahan pakai, sistem informasi suatu perusahaan haruslah jelas dan mudah dipahami. Auditor sangat perlu menilai dari segi mudah dipahami.
8. Mudah berinteraksi
9. Sistem informasi juga harus bisa memudahkan penggunanya dalam berinteraksi. Berinteraksi dalam artian tampilan dari sistem informasi yang interaksi dan memudahkan penggunanya
10. Sistem mudah dioperasikan
11. Terakhir auditor perlu menilai dari segi kemudahan aplikasi atau sistem informasi dioperasikan. Terutama terhadap orang baru.

DAFTAR PUSTAKA

Hidayat, T. (2021). Penerapan Prinsip Efektif dan Efisien dalam Pelaksanaan Monitoring Kegiatan Penelitian. Majalah Media Perencana, 2(1), 42-50.

Mulyamah (1987). Manajemen Perubahan. Jakarta: Yudhistira.

Rai, Gusti Agung. (2008). Audit kinerja pada skctor public. Jakarta: Penerbit Salemba Empat

Rushinek, A., & Rushinek, S. F. (1989). *Evaluating Asset Safeguarding and Data Integrity in the EDP Audit*. Managerial Auditing Journal, 4(2).

Steven M. Sheffrin (2003). Economics: Principles in action. Upper Saddle River, New Jersey 07458: Pearson Prentice Hall. ISBN 0-13-063085-3.

Suranto, B., Hanum, F. F., & Haryono, K. (2014). Audit Sistem Informasi RSUD Sleman Untuk Monitoring dan Evaluasi Kinerja Sistem. In Seminar Nasional Informatika Medis (SNIMed) (pp. 48-57).

Tangkilisan, Hessel Nogi S. (2005). Manajemen Publik. Jakarta: Grasindo

Waruwu, H., & Masitho, B. (2016). Efektivitas Pelayanan Paspor Pada Kantor Imigrasi Kelas I Khusus Medan. 4(1), 43–51.

BAB 11
AUDIT TI PADA DOMAIN EDM, APO, DSS, DAN MEA

11.1 Pra Audit TI

Pada dasarnya metodologi *audit/assurance* melibatkan proses pengumpulan data yakni berupa aktivitas Penelaahan dokumentasi kebijakan teknis maupun nonteknis (Fitrianah Devi, 2008) yang menjadi dasar pengembangan organisasi yang kemudian dilanjutkan dengan aktivitas Kunjungan dan wawancara dengan pemangku kepentingan layanan SI/ TI tersebut.

11.2. Pelaksanaan Audit

Pelaksanaan audit diawali dengan melakukan pengujian terhadap kelengkapan kontrol yakni melalui identifikasi kelengkapan serta keefektifan dari *Control Objective* dalam proses TI di organisasi, hasil dari pengujian *Control Objective* tersebut akan menghasilkan sebuah peninjauan mengenai ada/memadainya layanan SI/TI yang telah berjalan. Berikut Domain Proses audit SI/TI menurut *best practice* Cobit 5 (Copy and Lanter, 2012):

11.2.1 Audit IT pada Domain EDM

EDM adalah proses manajemen yang menilai dan mengoptimalkan risiko dan sumber daya terhadap tujuan manajemen *stakeholder*. Ini mencakup praktik dan aktivitas yang dirancang untuk mengevaluasi keputusan strategis,

memberikan arahan TI, dan memantau hasilnya. Lima proses yang dicakup oleh COBIT 5 EDM meliputi::

Tabel 11.1 Domain Proses EDM 01 Cobit 5

Control Objective	
Evaluate Direct and Monitoring (EDM)	
EDM 01 Memastikan pembentukan dan pemeliharaan sistem tata kelola	
EDM 01.01	Mengevaluasi sistem pemerintahan
EDM 01.02	Mengarahkan sistem pemerintahan
EDM 01.03	Memantau sistem tata kelola

Tabel 11.2. Domain Proses EDM 02 Cobit 5

Control Objective	
Evaluate Direct and Monitoring (EDM)	
EDM 02 Memastikan penyampaian manfaat	
EDM 02.01	Mengevaluasi pengoptimalan nilai
EDM 02.02	Optimasi nilai langsung
EDM 02.03	Memantau pengoptimalan nilai

Tabel 11.3. Domain Proses EDM 03 Cobit 5

Control Objective	
Evaluate Direct and Monitoring (EDM)	
EDM 03 Memastikan optimasi risiko	
EDM 03.01	Penilaian manajemen risiko
EDM 03.02	manajemen risiko langsung
EDM 03.03	Pengawasan manajemen risiko

Tabel 11.4. Domain Proses EDM 04 Cobit 5

Control Objective	
Evaluate Direct and Monitoring (EDM)	
EDM 04 Memastikan pengoptimalan sumber daya	
EDM 04.01	Mengevaluasi manajemen sumber daya
EDM 04.02	Manajemen sumber daya langsung
EDM 04.03	Memantau manajemen sumber daya

Tabel 11.5. Domain Proses EDM 05 Cobit 5

Control Objective	
Evaluate Direct and Monitoring (EDM)	
EDM 05 Memastikan transparansi *stakeholder*	
EDM 05.01	Mengevaluasi persyaratan pelaporan *stakeholder*
EDM 05.02	Komunikasi dan pelaporan *stakeholder* langsung
EDM 05.03	Memantau komunikasi *stakeholder*

Sumber : Enabling Process Cobit 5

11.2.2 Audit IT pada Domain APO

APO (Alignment, Planning and Organizing) adalah sebuah proses Konsultasi Penyedia Solusi (BAI) dan Manajemen Layanan dan dukungan Pemasok (sistem pendukung keputusan). Domain APO mencakup aspek strategis dan taktis, identifikasi Kekhawatiran tentang bagaimana IT dapat bekerja dengan baik Penggunaan komersial. Pelaksanaan visi strategis harus direncanakan dan dikomunikasikan dan mengelolanya dari sudut yang berbeda Infrastruktur organisasi dan teknis harus dipersiapkan dengan baik. Domain APO terdiri dari 13 proses :

Tabel 11.6. Domain Proses APO 01-013 Cobit 5

Control Objective	
Align, Plan, and Organize (APO)	
APO 01 Penggunaan Kerangka Manajemen TI.	
APO 01.01	Mendefinisikan struktur organisasi
APO 01.02	Menetapkan peran dan tanggung jawab
APO 01.03	Mempertahankan enabler dari sistem manajemen
APO 01.04	Mengomunikasikan objektif dan arah manajemen

APO 01.05	Mengoptimalkan penempatan fungsi IT
APO 01.06	Mendefinisikan Kepemilikan informasi (data) dan sistem
APO 01.07	Mengelola perbaikan proses yang berkelanjutan
APO 01.08	Menjaga ketaatan terhadap kebijakan dan prosedur

Tabel 11.6. Domain Proses APO 02 Cobit 5

Control Objective	
Align, Plan, and Organize (APO)	
APO 02 Mengelola strategi.	
APO 02.01	Memahami tujuan perusahaan.
APO 02.02	Menilai lingkungan, kapasitas, dan kinerja saat ini.
APO 02.03	Tentukan target kemampuan TI.
APO 02.04	Melakukan analisis kesenjangan
APO 02.05	Menetapkan rencana strategis dan peta jalan.
APO 02.06	Mengomunikasikan strategi dan arah TI.

Tabel 11.7. Domain Proses APO 03 Cobit 5

Control Objective	
Align, Plan, and Organize (APO)	
APO 03 Mengelola arsitektur perusahaan.	
APO 03.01	Mengembangkan visi arsitektur perusahaan
APO 03.02	Mendefinisikan arsitektur referensi.
APO 03.03	Pilih peluang dan solusi.
APO 03.04	Mendefinisikan implementasi arsitektur
APO 03.05	Menyediakan layanan arsitektur perusahaan

Tabel 11.8. Domain Proses APO 04 Cobit 5

Control Objective	
Align, Plan, and Organize (APO)	
APO 04 Mengelola inovasi.	
APO 04.01	Menciptakan lingkungan yang kondusif untuk inovasi
APO 04.02	Menjaga kesadaran akan lingkungan perusahaan
APO 04.03	Pantau dan pindai lingkungan teknis.
APO 04.04	Mengevaluasi potensi teknologi dan ide yang muncul inovasi.
APO 04.05	Tindakan tambahan yang tepat direkomendasikan.
APO 04.06	Pemantauan adopsi dan penggunaan inovasi

Tabel 11.9. Domain Proses APO 05 Cobit 5

Control Objective	
Align, Plan, and Organize (APO)	
APO 05 Mengelola portofolio.	
APO 05.01	Menetapkan bauran investasi target
APO 05.02	Menentukan ketersediaan dan sumber dana
APO 05.03	Mengevaluasi dan memilih program yang akan didana
APO 05.04	Pantau, optimalkan, dan laporkan kinerja portofolio
APO 05.05	Menjaga portofolio investasi
APO 05.06	Mengelola pencapaian manfaat

Tabel 11.10. Domain Proses APO 06 Cobit 5

Control Objective	
Align, Plan, and Organize (APO)	
APO 06 Mengelola *budget* dan biaya	
APO 06.01	Mengendalikan keuangan dan akuntansi
APO 06.02	Prioritaskan alokasi sumber daya
APO 06.03	Membuat dan memelihara anggaran.
APO 06.04	Model dan alokasi biaya.
APO 06.05	Mengelola biaya.

Tabel 11.11. Domain Proses APO 07 Cobit 5

Control Objective	
Align, Plan, and Organize (APO)	
APO 07 mengelola sumber daya manusia	
APO 07.01	Mempertahankan staf yang memadai dan sesuai.
APO 07.02	Identifikasi personel kunci TI.
APO 07.03	Mempertahankan keterampilan dan kemampuan individu
APO 07.04	Mengevaluasi kinerja pekerjaan karyawan.
APO 07.05	Merencanakan dan melacak TI bisnis dan penggunaan sumber daya manusia
APO 07.06	Mengelola staf kontrak.

Tabel 11.12. Domain Proses APO 08 Cobit 5

Control Objective	
Align, Plan, and Organize (APO)	
APO 08 Mengelola hubungan	
APO 08.01	Memahami harapan bisnis.
APO 08.02	Identifikasi peluang, risiko, & hambatan TI untuk menaikkan bisnis
APO 08.03	Mengatur keterkaitan bisnis.
APO 08.04	Berkoordinasi dan berkomunikasi.
APO 08.05	Memberikan saran untuk kemajuan layanan yang berkelanjutan

Tabel 11.13. Domain Proses APO 09 Cobit 5

Control Objective	
Align, Plan, and Organize (APO)	
APO 09 Mengelola perjanjian layanan	
APO 09.01	Identifikasi layanan TI.
APO 09.02	Katalog layanan yang mendukung TI
APO 09.03	Menentukan dan menyiapkan perjanjian layanan.
APO 09.04	Pantau dan laporkan tingkat layanan
APO 09.05	Tinjau perjanjian dan kontrak layanan.

Tabel 11.14. Domain Proses APO 010 Cobit 5

Control Objective	
Align, Plan, and Organize (APO)	
APO 10 Mengelola pemasok	
APO 10.01	Menjabarkan dan menilai keterkaitan dan kerjsama dengan pemasok
APO 10.02	Pilih pemasok
APO 10.03	Kelola hubungan dan kontrak pemasok
APO 10.04	Mengelola risiko pemasok.
APO 10.05	Mengecek prestasi dan kedispilinan pemasok

Tabel 11.15. Domain Proses APO 011 Cobit 5

Control Objective	
Align, Plan, and Organize (APO)	
APO 11 Mengelola kualitas.	
APO 11.01	Menentukan Sistem Manajemen Kualitas (SMK)
APO 11.02	Menetapkan dan mengendalikan standar, praktik, dan prosedur kualitas.
APO 11.03	Fokus manajemen kualitas pada pelanggan.
APO 11.04	Lakukan pemantauan, kontrol, dan ulasan kualitas.
APO 11.05	Bauran manajemen kualitas ke dalam pengembangan penyelesaian dan penyampaian layanan
APO 11.06	Pertahankan perbaikan terus-menerus.

Tabel 11.16. Domain Proses APO 012 Cobit 5

Control Objective	
Align, Plan, and Organize (APO)	
APO 12 Mengelola risiko.	
APO 12.01	Mengumpulkan data.
APO 12.02	Analisis risiko.
APO 12.03	Menjaga profil risiko.
APO 12.04	Mengartikulasikan risiko.
APO 12.05	Mendefinisikan portofolio tindakan manajemen risiko.
APO 12.06	Menanggapi risiko.

Tabel 11.17. Domain Proses APO 013 Cobit 5

Control Objective	
Align, Plan, and Organize (APO)	
APO 13 Mengelola keamanan.	
APO 13.01	Membangun dan memelihara SMKI.
APO 13.02	Identifikasi dan kelola rencana respons risiko keamanan informasi.
APO 13.03	Memantau dan meninjau SMKI.

Sumber : Enabling Process Cobit 5

11.2.3 Audit IT pada Domain DSS

Ranah DSS terkait pelaporan aktual serta bantuan layanan yang dibutuhkan, termasuk layanan (Candra, Atastina and Firdaus, 2015), *security management* dan keberlangsungan, dukungan *user*, serta fasilitas pengelolaan juga data operasional. Ranah DSS terdiri dari 6 proses diantaranya:

Tabel 11.18. Domain Proses DSS 01 Cobit 5

Control Objective	
Deliver, Service and Support (DSS)	
DSS 01 Mengelola perjanjian layanan	
DSS 01.01	Menjalankan prosedur operasi.
DSS 01.02	Kelola layanan TI *outsourcing*
DSS 01.03	Memantau infrastruktur TI.
DSS 01.04	Mengelola lingkungan.
DSS 01.05	fasilitas manajemen.

Tabel 11.19. Domain Proses DSS 02 Cobit 5

Control Objective	
Deliver, Service and Support (DSS)	
DSS 02 Mengelola permintaan dan insiden layanan	
DSS 02.01	Menentukan skema klasifikasi npermintaan layanan dan insiden
DSS 02.02	Catat, kategorikan, dan prioritaskan permintaan dan insiden
DSS 02.03	Validasi, setujui, dan selesaikan permintaan layanan.
DSS 02.04	Menyelidiki, mendiagnosis dan menetapkan insiden.
DSS 02.05	Menyelesaikan dan pulih dari insiden.
DSS 02.06	Membatasi permohonan layanan dan kejadian
DSS 02.07	Memantau kondisi dan menghasilkan laporan

Tabel 11.20. Domain Proses DSS 03 Cobit 5

Control Objective	
Deliver, Service and Support (DSS)	
DSS 03 Mengelola masalah	
DSS 03.01	Mengidentifikasi dan mengklasifikasikan masalah.
DSS 03.02	Menyelidiki dan mendiagnosis masalah.
DSS 03.03	Tingkatkan *bug* yang dikenal.
DSS 03.04	Perbaiki dan tutup masalah.
DSS 03.05	Lakukan manajemen masalah secara proaktif.

Tabel 11.22. Domain Proses DSS 04 Cobit 5

Control Objective	
Deliver, Service and Support (DSS)	
DSS 04 Mengelola kontinuitas	
DSS 04.01	Menjelaskan aturan kelangsungan bisnis, objektif dan cakupan.
DSS 04.02	Mempertahankan strategi kesinambungan.
DSS 04.03	Meningkatkan dan menggunakan setiap umpan balik demi kesinambungan usaha
DSS 04.04	Latih, memeriksa, tinjauan pada BCP
DSS 04.05	Tinjau, pertahankan, dan tingkatkan rencana kesinambungan.
DSS 04.06	Mengadakan pelatihan perencanaan kontinuitas
DSS 04.07	Kelola pengaturan pencadangan.
DSS 04.08	Melakukan tinjauan setelah dimulainya kembali

Tabel 11.23. Domain Proses DSS 05 Cobit 5

Control Objective	
Deliver, Service and Support (DSS)	
DSS 05 Mengelola layanan keamanan	
DSS 05.01	Melindungi dari *malware*
DSS 05.02	Kelola keamanan dan hubungan antar jaringan.
DSS 05.03	Mengendalikan keamanan *endpoint*
DSS 05.04	Mengendalikan identitas *user* dan membuat akses pada terminal
DSS 05.05	mengendalikan *physical access* terhadap aset TI.
DSS 05.06	Melindungi dokumen rahasia dan perangkat *output*
DSS 05.07	Infrastruktur untuk memantau insiden terkait keamanan.

Tabel 11.24. Domain Proses DSS 06 Cobit 5

Control Objective	
Deliver, Service and Support (DSS)	
DSS 06 Mengelola kontrol proses bisnis	
DSS 06.01	Menyesuaikan aktivitas kendali terpendam pada proses bisnis serta tujuan organisasi
DSS 06.02	Mengendalikan proses informasi.
DSS 06.03	Mengatur peran, kewajiban, hak akses, dan tingkat *privilege*
DSS 06.04	Kelola kesalahan dan pengecualian
DSS 06.05	Pastikan penelusuran kegiatan dan akuntabilitas informasi.
DSS 06.06	Lindungi aset informasi.

Sumber : Enabling Process Cobit 5

Hasil pembuktian yang dapat dicek kesesuaiannya dengan kondisi yang ada sebagai alat ukur tersendiri.

11.2.4 Audit TI pada domain MEA

MEA adalah aktivitas manajemen yang mengamati semua proses demi menjamin instruksi yang diberikan diikuti. Seluruh proses TI harus di evaluasi berkala untuk mengamati mutu dan kepatuhannya (Sofa Karimah,Tri Lathif Mardi Suryanto, 2020) Area ini berkaitan dengan manajemen kinerja, pengamatan kendali internal, kepatuhan terhadap aturan, dan tata kelola ranah MEA terdiri dari 3 proses, diantaranya:

Tabel 11.25. Domain Proses MEA 01-03 Cobit 5

Control Objective	
Measure, Evaluate and Assess (MEA)	
MEA 01 Memantau, menilai, mengevaluasi kinerja dan kecocokan untuk digunakan	
MEA 01.01	Menetapkan pendekatan pemantauan.
MEA 01.02	Tetapkan tujuan kinerja dan kepatuhan.

MEA 01.03	Mengumpulkan dan memproses data kinerja dan kepatuhan.
MEA 01.04	Menganalisa dan melaporkan kinerja
MEA 01.05	Memastikan pelaksanaan tindakan korektif

Tabel 11.26. Domain Proses MEA 02 Cobit 5

Control Objective	
Measure, Evaluate and Assess (MEA)	
MEA 02 Memantau, mengevaluasi dan menilai sistem pengendalian internal	
MEA 02.01	Mengawasi pengendalian internal
MEA 02.02	Tinjau efektivitas kontrol proses bisnis
MEA 02.03	Lakukan penilaian mandiri kontrol.
MEA 02.04	Mengidentifikasi dan melaporkan kekurangan pengendalian.
MEA 02.05	Pastikan penyedia garansi independen dan berkualitas
MEA 02.06	Rencanakan inisiatif asuransi.
MEA 02.07	inisiatif jaminan ruang lingkup.
MEA 02.08	Jalankan inisiatif jaminan.

Tabel 11.27. Domain Proses MEA 03 Cobit 5

Control Objective	
Measure, Evaluate and Assess (MEA)	
MEA 03 Pemantauan, evaluasi dan evaluasi kepatuhan terhadap persyaratan eksternal	
MEA 03.01	Identifikasi persyaratan kepatuhan eksternal.
MEA 03.02	Optimalkan respons terhadap permintaan eksternal
MEA 03.03	Konfirmasi kepatuhan eksternal
MEA 03.04	Dapatkan jaminan kepatuhan eksternal

Sumber: Enabling Process Cobit 5

11.3 Tingkat Kematangan

Perhitungan *Maturity Level* dengan Mengukur tingkat kesempurnaan dari layanan sistem informasi dan teknologi informasi berdasarkan data kuesioner yang telah diuji validitas dan reliabilitasnya. Tingkat Maturitas dan Gap Analysis untuk Menentukan Tingkat Maturitas (Suryono, Darwis & Gunawan, 2018) Hasil nilai aktual dan harapan. Skala peringkat maturitas terbagi atas enam tingkatan antara lain:

Indeks Kematangan	Level Kematangan
0 – 0,49	0 – Non-Existent
0,50 – 1,49	1 – Initial / Ad Hoc
1,50 – 2,49	2 – Repeatable but Intuitive
2,50 – 3,49	3 – Defined Process
3,50 – 4,49	4– Manage and Measurable
4,50 –5,00	5 – Optimized

(Sumber : ISACA 2012)

11.4 Pasca Audit

Berdasarkan hasil temuan audit SI/TI yang ada terkait kontrol maupun kondisi layanan yang diterapkan selama ini temuan-temuan hasil audit kemudian dilaporkan kedalam rekomendasi perbaikan (Fitrianah Devi, 2008) jangka pendek, jangka menengah serta jangka panjang, dalam bentuk:

1. Rencana dan Strategi TI
2. Keorganisasian pengelolaan TI
3. Pengembangan fitur layanan TI
4. Pengelolaan basis data
5. Pembenahan jaringan komputer yang memadai

DAFTAR PUSTAKA

Candra, R.K., Atastina, I. and Firdaus, Y. (2015) 'Audit Teknologi Informasi menggunakan Framework COBIT 5 Pada Domain DSS (Delivery , Service , and Support) (Studi Kasus : iGracias Telkom University)', in *e-Proceeding of Engineering*, pp. 1129–1144.

Copy, P. and Lanter, D. (2012) *Cobit 5 : Enabling Processes*. ISACA.

Fitrianah Devi, G.S.Y. (2008) 'Audit Sistem Informasi/ Teknologi Informasi dengan Kerangka Kerja COBIT untuk Evaluasi Manajemen Teknologi Informasi di Universitas XYZ', *Jurnal Sistem Informasi MTI-UI*, 4(1), pp. 37–46.

Sofa Karimah,Tri Lathif Mardi Suryanto, R.R.S. (2020) 'Audit Tata Kelola Teknologi Informasi Menggunakan Kerangka Kerja Cobit 5 Pada Dinas Pekerjaan Umum Kabupaten Tanggamus.', *Jurnal Teknologi dan Sistem Informasi (JTSI)*, 1(1), pp. 39–46.

Suryono, R.R., Darwis, D. and Gunawan, S.I. (2018) Audit Tata Kelola Teknologi Informasi Menggunakan Framework COBIT 5 (Studi Kasus: Balai Besar Perikanan Budidaya Laut Lampung). *Jurnal TEKNOINFO*, 12(1), pp. 16–22.

BAB 12
TATA KELOLA IT DAN MANAJEMEN RISIKO

12.1 Pengertian Tata Kelola IT

12.1.1 Definisi Tata Kelola IT

Tata kelola IT atau IT governance adalah sebuah kerangka kerja yang digunakan oleh perusahaan atau organisasi untuk mengelola dan mengontrol penggunaan teknologi informasi (TI) dengan tujuan memastikan TI tersebut memberikan nilai tambah dan mendukung tujuan bisnis organisasi secara efektif dan efisien. Tata kelola IT melibatkan proses pengambilan keputusan strategis, manajemen risiko, dan pengendalian penggunaan TI dalam organisasi

12.1.2 Tujuan Tata Kelola IT

Tujuan utama dari tata kelola IT adalah untuk memastikan bahwa penggunaan TI di organisasi dikelola secara efektif dan efisien, sehingga dapat memberikan nilai tambah yang signifikan bagi organisasi. Selain itu, tata kelola IT juga bertujuan untuk:

1. Memastikan kepatuhan organisasi terhadap peraturan, standar, dan kebijakan yang berlaku terkait penggunaan TI.
2. Meningkatkan transparansi dan akuntabilitas penggunaan TI dalam organisasi.

3. Meningkatkan kualitas layanan TI dan dukungan untuk bisnis organisasi.
4. Mengoptimalkan penggunaan sumber daya TI organisasi.

12.1.3 Manfaat Tata Kelola IT

Tata kelola IT dapat memberikan banyak manfaat bagi organisasi, antara lain:

1. Meningkatkan efisiensi dan efektivitas penggunaan TI dalam organisasi.
2. Meningkatkan transparansi dan akuntabilitas penggunaan TI dalam organisasi.
3. Meningkatkan pengelolaan risiko TI dan meminimalkan dampak negatif dari kegagalan TI.
4. Meningkatkan kepatuhan organisasi terhadap peraturan, standar, dan kebijakan yang berlaku terkait penggunaan TI.
5. Meningkatkan kualitas layanan TI dan dukungan untuk bisnis organisasi.
6. Mengoptimalkan penggunaan sumber daya TI organisasi dan meningkatkan nilai tambah TI bagi organisasi.
7. Meningkatkan citra dan reputasi organisasi dalam penggunaan TI.

12.2 Kerangka Tata Kelola IT

1. COBIT (*Control Objectives for Information and Related Technology*)
2. ITIL (*Information Technology Infrastructure Library*)
3. ISO 38500 (*Corporate Governance of Information Technology*)
4. NIST Cybersecurity Framework (*National Institute of Standards and Technology Cybersecurity Framework*)
5. COSO (*Committee of Sponsoring Organizations of the Treadway Commission*)

Kerangka tata kelola IT yang umum digunakan adalah sebagai berikut:

1. ***COBIT (Control Objectives for Information and Related Technology):***

   COBIT adalah sebuah kerangka kerja yang dikembangkan oleh ISACA (Information Systems Audit and Control Association) untuk membantu organisasi dalam mengelola TI secara efektif dan efisien. COBIT mencakup empat domain utama yaitu: perencanaan dan pengorganisasian, akuisisi dan implementasi, pengoperasian dan pemeliharaan, serta pemantauan dan evaluasi. COBIT juga memiliki seperangkat kontrol dan tujuan yang dapat membantu organisasi dalam memastikan kepatuhan terhadap peraturan dan kebijakan terkait TI.

2. ***ITIL (Information Technology Infrastructure Library):***

   ITIL adalah sebuah kerangka kerja terstruktur yang digunakan untuk mengelola dan mengoptimalkan penggunaan layanan TI dalam organisasi. ITIL meliputi sejumlah proses manajemen TI, seperti manajemen perubahan, manajemen kapasitas, manajemen masalah, dan manajemen layanan, yang dirancang untuk membantu organisasi dalam memastikan layanan TI yang berkualitas dan memberikan nilai tambah bagi bisnis organisasi.

3. ***ISO 38500 (Corporate Governance of Information Technology):***

   ISO 38500 adalah sebuah standar internasional yang memberikan pedoman untuk tata kelola TI yang efektif dan efisien dalam organisasi. Standar ini menekankan pentingnya kepemimpinan dan

pengambilan keputusan strategis yang berkualitas dalam pengelolaan TI dalam organisasi.

4. ***NIST Cybersecurity Framework (National Institute of Standards and Technology Cybersecurity Framework):***

   NIST Cybersecurity Framework adalah sebuah kerangka kerja yang dikembangkan oleh National Institute of Standards and Technology (NIST) Amerika Serikat untuk membantu organisasi dalam membangun dan memelihara program keamanan siber yang efektif dan efisien. Kerangka kerja ini mencakup lima domain utama yaitu: identifikasi, perlindungan, deteksi, respons, dan pemulihan, yang dirancang untuk membantu organisasi dalam mengurangi risiko keamanan siber.

5. ***COSO (Committee of Sponsoring Organizations of the Treadway Commission):***

   COSO adalah sebuah kerangka kerja yang dirancang untuk membantu organisasi dalam mengelola risiko dan memperkuat tata kelola perusahaan secara efektif dan efisien. COSO mencakup lima komponen utama yaitu: lingkungan pengendalian internal, penilaian risiko, kegiatan pengendalian, informasi dan komunikasi, serta pemantauan. Kerangka kerja ini juga mencakup seperangkat prinsip dan praktik terbaik yang dapat membantu organisasi dalam mencapai tujuan bisnis secara efektif dan efisien.

12.3 Manajemen Risiko TI

12.3.1 Definisi Manajemen Risiko TI:

Manajemen risiko TI adalah proses identifikasi, analisis, penilaian, dan pengelolaan risiko yang terkait dengan penggunaan TI dalam organisasi. Manajemen risiko

TI bertujuan untuk mengidentifikasi dan mengelola risiko yang dapat mempengaruhi keamanan, ketersediaan, integritas, dan kerahasiaan data dan sistem TI organisasi.

12.3.2 Komponen Manajemen Risiko TI:

Manajemen risiko TI terdiri dari beberapa komponen utama, yaitu:

1. *Identifikasi Risiko*: proses identifikasi potensi risiko yang dapat terjadi dalam penggunaan TI dalam organisasi.
2. *Analisis Risiko*: proses analisis risiko yang diidentifikasi untuk menentukan probabilitas terjadinya dan dampak yang mungkin terjadi.
3. *Penilaian Risiko*: proses penilaian risiko untuk menentukan tingkat risiko yang dihadapi organisasi.
4. *Pengelolaan Risiko*: proses pengelolaan risiko yang dilakukan melalui pengimplementasian kontrol keamanan yang sesuai untuk mengurangi tingkat risiko.

12.3.3 Proses Manajemen Risiko TI:

Proses manajemen risiko TI melibatkan beberapa langkah, yaitu:

1. *Identifikasi risiko TI:* Identifikasi berbagai risiko TI yang dapat mempengaruhi organisasi.
2. *Analisis risiko TI:* Analisis setiap risiko TI yang telah diidentifikasi dengan mempertimbangkan probabilitas terjadinya dan dampak yang mungkin terjadi.
3. *Penilaian risiko TI:* Penilaian tingkat risiko yang dihadapi organisasi.
4. *Pengelolaan risiko TI:* Implementasi kontrol keamanan yang sesuai untuk mengurangi tingkat risiko yang diidentifikasi.
5. *Pemantauan dan peninjauan risiko TI:* Pemantauan dan evaluasi efektivitas kontrol keamanan yang telah diimplementasikan dan melakukan peninjauan risiko secara berkala.

12.3.4 Manfaat Manajemen Risiko TI:

Manajemen risiko TI memiliki banyak manfaat bagi organisasi, antara lain:

1. Membantu organisasi dalam mengidentifikasi dan mengelola risiko yang terkait dengan penggunaan TI, sehingga dapat mengurangi dampak negatif yang mungkin terjadi.
2. Menjamin keamanan, ketersediaan, integritas, dan kerahasiaan data dan sistem TI organisasi.
3. Memastikan kepatuhan organisasi terhadap peraturan dan kebijakan terkait penggunaan TI.
4. Meningkatkan efisiensi dan efektivitas penggunaan TI dalam organisasi.
5. Meningkatkan citra dan reputasi organisasi dalam penggunaan TI.
6. Meningkatkan kualitas layanan TI dan dukungan untuk bisnis organisasi.
7. Mengoptimalkan penggunaan sumber daya TI organisasi dan meningkatkan nilai tambah TI bagi organisasi.

12.4 Hubungan antara Tata Kelola IT dan Manajemen Risiko TI

12.4.1 Bagaimana Tata Kelola IT mendukung Manajemen Risiko TI:

Tata kelola IT membantu manajemen risiko TI dengan menyediakan kerangka kerja dan proses yang terstruktur untuk mengidentifikasi, mengevaluasi, dan mengelola risiko yang terkait dengan penggunaan TI dalam organisasi. Dengan menggunakan kerangka kerja tata kelola IT, organisasi dapat memastikan bahwa penggunaan TI dilakukan sesuai dengan tujuan bisnis, serta memastikan kepatuhan terhadap peraturan dan kebijakan terkait penggunaan TI. Selain itu, tata kelola IT juga membantu organisasi dalam memastikan keamanan, ketersediaan, integritas, dan kerahasiaan data dan sistem TI organisasi.

12.4.2 Bagaimana Manajemen Risiko TI terintegrasi dalam Tata Kelola IT:

Manajemen risiko TI merupakan komponen penting dalam tata kelola IT, karena tata kelola IT bertujuan untuk memastikan penggunaan TI yang efektif dan efisien dalam organisasi, sedangkan manajemen risiko TI bertujuan untuk mengidentifikasi dan mengelola risiko yang terkait dengan penggunaan TI dalam organisasi. Dalam tata kelola IT, manajemen risiko TI terintegrasi dalam beberapa proses, seperti identifikasi risiko, analisis risiko, penilaian risiko, dan pengelolaan risiko. Proses-proses tersebut membantu organisasi dalam memastikan bahwa risiko yang terkait dengan penggunaan TI dalam organisasi telah diidentifikasi dan dinilai, serta dielola dengan cara yang tepat. Selain itu, manajemen risiko TI juga membantu organisasi dalam mengoptimalkan penggunaan sumber daya TI dan meningkatkan nilai tambah TI bagi organisasi. Oleh karena itu, integrasi manajemen risiko TI dalam tata kelola IT sangat penting untuk memastikan penggunaan TI yang efektif dan efisien dalam organisasi, dan untuk meminimalkan dampak negatif dari risiko yang terkait dengan penggunaan TI dalam organisasi.

12.5 Pelaksanaan Tata Kelola IT dan Manajemen Risiko TI

12.5.1 Tahapan Pelaksanaan Tata Kelola IT dan Manajemen Risiko TI:

Pelaksanaan tata kelola IT dan manajemen risiko TI biasanya melibatkan beberapa tahapan, antara lain:

1. *Persiapan*: Tahap awal dalam pelaksanaan tata kelola IT dan manajemen risiko TI adalah persiapan, dimana organisasi melakukan analisis kebutuhan dan merancang kerangka kerja yang sesuai dengan tujuan bisnis dan kebijakan perusahaan.

2. *Perencanaan*: Tahap ini meliputi penetapan tujuan, strategi, dan prosedur yang terkait dengan pengelolaan TI dan manajemen risiko TI. Selain itu, tahap perencanaan juga melibatkan identifikasi risiko TI, pengukuran risiko, dan penetapan rencana tindakan untuk mengurangi risiko.
3. *Implementasi:* Tahap ini melibatkan penerapan prosedur, kontrol, dan rencana tindakan yang telah ditetapkan pada tahap perencanaan.
4. *Monitoring:* Tahap ini melibatkan pemantauan penggunaan TI dan manajemen risiko TI secara berkala, dan evaluasi efektivitas dari tata kelola IT dan manajemen risiko TI dalam mencapai tujuan bisnis organisasi.

12.5.2 Kendala dalam Pelaksanaan Tata Kelola IT dan Manajemen Risiko TI:

Beberapa kendala dalam pelaksanaan tata kelola IT dan manajemen risiko TI adalah:

1. Kurangnya dukungan dan komitmen dari manajemen puncak.
2. Kurangnya sumber daya yang diperlukan untuk menerapkan tata kelola IT dan manajemen risiko TI.
3. Kurangnya pemahaman tentang pentingnya tata kelola IT dan manajemen risiko TI di kalangan karyawan organisasi.
4. Tidak adanya pembaruan terhadap proses dan kerangka kerja yang digunakan dalam tata kelola IT dan manajemen risiko TI.

12.5.3 *Best Practice* Pelaksanaan Tata Kelola IT dan Manajemen Risiko TI:

Beberapa best practice dalam pelaksanaan tata kelola IT dan manajemen risiko TI adalah:

1. Menyediakan dukungan dan komitmen dari manajemen puncak.
2. Melakukan sosialisasi dan pelatihan kepada karyawan tentang pentingnya tata kelola IT dan manajemen risiko TI.
3. Menggunakan kerangka kerja dan proses yang terstruktur dan fleksibel untuk mengelola risiko TI dan penggunaan TI dalam organisasi.
4. Melakukan pemantauan dan evaluasi secara berkala untuk memastikan efektivitas dari tata kelola IT dan manajemen risiko TI dalam mencapai tujuan bisnis organisasi.
5. Melakukan pembaruan terhadap proses dan kerangka kerja yang digunakan dalam tata kelola IT dan manajemen risiko TI secara berkala untuk memastikan relevansi dan efektivitas.

12.6 Kesimpulan

12.6.1 Intisari Tata Kelola IT dan Manajemen Risiko TI:

Tata kelola IT dan manajemen risiko TI merupakan proses penting dalam pengelolaan penggunaan teknologi informasi dalam organisasi. Tata kelola IT bertujuan untuk memastikan penggunaan TI yang efektif dan efisien dalam organisasi, sedangkan manajemen risiko TI bertujuan untuk mengidentifikasi dan mengelola risiko yang terkait dengan penggunaan TI dalam organisasi. Keduanya saling terkait dan saling mendukung dalam pengelolaan TI dalam organisasi.

12.6.2 Peran penting Tata Kelola IT dan Manajemen Risiko TI dalam dunia bisnis dan industri:

Tata kelola IT dan manajemen risiko TI memainkan peran penting dalam dunia bisnis dan industri, karena penggunaan TI yang efektif dan efisien dapat membantu organisasi dalam mencapai tujuan bisnis dan meningkatkan nilai tambah bagi organisasi. Selain itu, manajemen risiko TI juga membantu organisasi dalam meminimalkan dampak negatif dari risiko yang terkait dengan penggunaan TI dalam organisasi. Dengan demikian, implementasi tata kelola IT dan manajemen risiko TI dapat membantu organisasi dalam meningkatkan efisiensi, efektivitas, dan keamanan dalam penggunaan TI dalam organisasi.

DAFTAR PUSTAKA

ISACA. (2019). *COBIT 2019 Framework: Introduction and Methodology.*

Axelos. (2019). *ITIL 4 Foundation: ITIL 4 Edition*.

International Organization for Standardization. (2015). *ISO/IEC 38500:2015 - Corporate Governance of Information Technology.*

National Institute of Standards and Technology. (2018). *NIST Cybersecurity Framework.*

Committee of Sponsoring Organizations of the Treadway Commission. (2017). *Internal Control - Integrated Framework*.

Calder, A., Watkins, S., & Whitman, M. E. (2019). *IT Governance: A Manager's Guide to Data Security and ISO 27001/27002*. Kogan Page Publishers.

Van Grembergen, W., & De Haes, S. (2018). *Governance of IT: An executive guide to ISO/IEC 38500*. Springer International Publishing.

Kim, D., & Solomon, M. (2019). *The DevOps Handbook: How to Create World-Class Agility, Reliability, and Security in Technology Organizations.* IT Revolution.

Disterer, G. (2017). *The Basics of IT Audit: Purposes, Processes, and Practical Information*. CRC Press.

Basu, S. (2017). *Managing Information Risk and the Economics of Security.* Springer International Publishing.

BAB 13
ITIL (*INFORMATION TECHNOLOGY INFRASTRUCTURE LIBRARY*) V3

13.1 Pendahuluan

Saat ini semakin meningkat organisasi atau perusahaan yang menggunakan atau memakai teknologi informasi (TI) untuk kegiatan operasionalnya sehari – hari. Kegiatan operasional tersebut lama kelamaan semakin banyak seiring dengan meningkatnya jumlah pengguna dan area yang ditangani oleh perusahaan. Banyak kejadian – kejadian atau insiden yang dialami oleh perusahaan yang membutuhkan penanganan dan perhatian untuk segera diselesaikan. Kejadian – kejadian tersebut makin meningkat ketika perusahaan berekspansi atau pelanggan memiliki kebutuhan yang semakin meningkat akan layanan perusahaan. Sehingga hal ini menyebabkan perusahaan membutuhkan suatu pengelolaan layanan TI. Terkadang perusahaan tidak mengetahui tingkat seperti apa kualitas layanan perusahaan tersebut. Pengukuran tingkat kematangan juga diperlukan untuk mengetahui bagaimana kualitas layanan yang telah disediakan oleh organisasi. Untuk mengukur tingkat kematangan suatu layanan dapat digunakan kerangka kerja ITIL v3 (*Information Technology Infrastructure Library*) Versi 3.

13.2 Definisi ITIL V3

ITIL adalah kerangka kerja publik yang menggambarkan *Best Practice* dalam pengelolaan layanan TI. Ini memberikan kerangka kerja untuk tata kelola TI dan berfokus pada pengukuran berkelanjutan dan peningkatan kualitas layanan TI yang diberikan, baik dari perspektif bisnis maupun pelanggan. Fokus ini merupakan faktor utama dalam kesuksesan ITIL di seluruh dunia dan telah berkontribusi pada penggunaannya yang produktif dan manfaat utama yang diperoleh oleh organisasi yang menerapkan teknik dan proses di seluruh organisasi mereka (Cartlidge et al., 2007).

13.2.1 Manfaat penggunaan ITIL V3

Adapun manfaat penggunaan ITIL v3 antara lain (Cartlidge et al., 2007) :

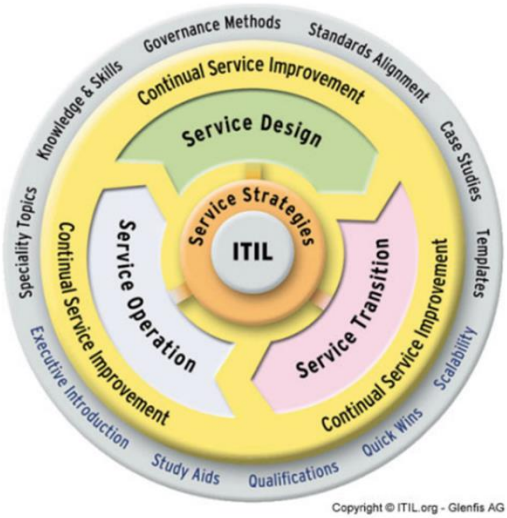
- Meningkatkan kepuasan pengguna dan pelanggan dengan layanan Teknologi Informasi yang ada.
- Meningkatkan ketersediaan layanan (ketersediaan layanan sangat penting untuk saat ini karena layanan TI harus selalu tersedia) yang secara tidak langsung hal ini terkait pada peningkatan keuntungan dan pemasukan pada bisnis perusahaan.
- Penghematan secara finansial atau keuangan dari pengurangan kegiatan yang harus dikerjakan berulang, waktu yang hilang, pengelolaan dan pemakaian sumber daya yang lebih baik.
- Waktu yang tepat untuk memasarkan produk dan layanan yang terbaru.
- Pengambilan keputusan yang lebih tepat dan risiko yang dapat dioptimalkan (mengurangi risiko yang lebih berat).

13.2.2 Konsep ITIL v3

Fitur pada ITIL v3 adalah pengenalan konsep siklus hidup manajemen layanan yang berfokus pada kualitas layanan TI (yaitu *end to end*). Kerangka kerja ITIL ini berfokus pada layanan organisasi sehingga berfokus pada pengguna dan pelanggan.

13.2.3 Siklus Hidup Layanan

Pada kerangka kerja ITIL, penjelasan tentang siklus hidup layanan dengan menggunakan kerangka kerja ITIL dapat dilihat pada gambar berikut yang menjelaskan apa saja komponennya. Berikut tahapan siklus hidup layanan pada kerangka kerja ITIL versi 3 (Baz et al., 2017):



Gambar 13.1. *Service Lifecycle*
(Sumber www.itil.org)

Pada gambar 13.1 menggambarkan suatu kernagka kerja yang terdiri dari Strategi layanan, Desain layanan, Transisi Layanan., Operasional Layanan dan Peningkatan

layanan berkelanjutan. Berikut dijelaskan masing – masing komponen tersebut:

1) Strategi layanan (*Service Strategy*): menyediakan suatu arahan seperti apa dan bagaimana melakukan perancangan, pengembangan dan penerapan manajemen pengelolaan layanan yang tidak hanya sebagai kecakapan institusi akan tetapi juga sebagai suatu aset yang strategis. Bimbingan dilaksanakan pada pedoman–pedoman yang mendasari pelaksanaan pengelolaan layanan yang memiliki manfaat untuk membuat kebijakan, pedoman dan proses pengelolaan layanan di semua siklus hidup layanan ITIL.
2) Desain layanan (*Service Design*): memberikan panduan untuk perencanaan dan pengembangan layanan dan proses manajemen layanan. Ini mencakup prinsip dan metode desain untuk mengubah tujuan strategis menjadi layanan dan aset layanan. Ruang lingkup perencanaan tugas tidak terbatas pada tugas baru. Ini termasuk perubahan dan peningkatan yang diperlukan untuk meningkatkan atau mempertahankan nilai pelanggan selama umur layanan, kesinambungan layanan, pencapaian tingkat layanan, dan kepatuhan terhadap standar dan peraturan. Ini memandu organisasi untuk mengembangkan keterampilan perencanaan untuk manajemen layanan.
3) Transisi layanan (*Service Transition*): Dalam kegiatan untuk mengenalkan layanan baru dan layanan yang mengalami perubahan maka dibutuhkan suatu panduan untuk mengembangkan dan meningkatkan kapasitas yang diperlukan Ini adalah panduan tentang cara menerapkan secara efektif persyaratan strategi layanan yang dikodekan dalam desain layanan ke dalam operasi layanan sekaligus mengelola risiko kegagalan dan

gangguan. Ini memandu manajemen kompleksitas yang terkait dengan perubahan layanan dan proses manajemen layanan, mencegah konsekuensi yang tidak diinginkan dan memungkinkan inovasi. .

4) Pengoperasian layanan (*Service Operation*): Dalam penyampaian dan dukungan untuk layanan maka perlu adanya suatu pedoman untuk sistem layanan mencapai efisiensi dan efektivitas untuk pengguna dan penyedia layanan tersebut. Hal ini jelas bahwa agar operasi layanan menjadi stabil yang ada kemungkinan adanya perubahan dalam suatu rancangan, ruang lingkup, dan tingkat layanan. Ada dua aspek utama pengendalian yaitu reaktif dan proaktif yang diterima organisasi untuk menerima suatu instruksi proses terperinci, cara, dan alat.
5) Peningkatan layanan berkelanjutan (*Continual Service Improvement*): Dalam melestarikan nilai untuk pengguna dapat digunakan cara yaitu melalui desain, penerapan dan pemakaian layanan dengan lebih baik dengan cara membekali kepemimpinan dalam mendukung kegiatan membuat dan melestarikan nilai tersebut. Penggabungan antara prinsip, penerapan dan metode pengelolaan mutu, pengelolaan perubahan dan untuk kegiatan pengelolaan kompetensi. Organisasi belajar bagaimana mencapai peningkatan skala besar dan bertahap dalam kualitas layanan, efisiensi operasional, dan kelangsungan bisnis.

13.3 Studi kasus penggunaan kerangka kerja ITIL v3

13.3.1 Studi pada perusahaan ISP

Suatu perusahaan yang bergerak di bidang *Internet Service Provider* (ISP) untuk operasional sehari – hari perusahaan ini menggunakan sarana teknologi informasi untuk mendukung aktivitas perusahaan tersebut setiap harinya. Saat ini perusahaan tersebut mengalami peningkatan jumlah pelanggan dan area yang ditangani. Permasalahan yang dialami oleh perusahaan tersebut adalah perusahaan dalam hal ini bidang operasional perusahaan belum dapat menangani insiden yang terjadi karena peningkatan jumlah pelanggan ini. Oleh karenanya penting digunakan suatu Manajemen Layanan Teknologi Informasi (ITSM). Untuk memecahkan masalah yang dialami oleh perusahaan maka peneliti menggunakan kerangka kerja ITIL yaitu suatu kerangka kerja yang digunakan oleh perusahaan – perusahaan di dunia untuk mengembangkan kerangka kerja yang memiliki fokus pengelolaan layanan teknologi informasi, pengembangan dan pengoperasian Teknologi Informasi, hal ini membantu perusahaan untuk menyelesaikan permasalahan yang terjadi karena peningkatan jumlah pelanggan dan makin luasnya area yang ditangani perusahaan (*coverage area*). Dengan menggunakan kerangka kerja ITIL maka perusahaan dapat menimplementasikan untuk menyeimbangkan kegiatan operasional layanan ketika menangani insiden atau kejadian yang dialami oleh perusahaan (Lubis et al., 2020).

13.3.2 Studi pada Universitas Negeri

Studi kedua membahas mengenai suatu artikel tentang perancangan perangkat lunak sekaligus pengujian yang terhadap perangkat lunak tersebut di Universitas Islam Negeri Syarif Hidayatullah Jakarta dengan menggunakan

standar ITIL v3. Kajian ini adalah mengenai implementasi Wistleblowing System dengan merancang dan mengembangkan sistem tersebut sesuai standar ITIL v3. Perangkat lunak *service desk* memberikan kenyamanan dalam penerapannya oleh pengguna dan mengelola kegiatan layanan dalam suatu institusi menggunakan standar berdasarkan ITIL v3. Penggunaan atau pengoperasian layanan *Wistleblowing System* dan *service desk* adalah hampir serupa. Hasil kajian ini menyimpulkan bahwa sistem dapat dipakai untuk mengatur atau mengelola layanan untuk mahasiswa / mahasiswi, dosen, dan staf (Hakiem et al., 2022).

13.3.3 Studi pada PT. XYZ

Studi ketiga ini adalah suatu perusahaan yang memiliki dua puluh kantor cabang ingin mengganti sistem ERP lama mereka dengan Microsoft Dinamics AX 365. Proses perubahan dari sistem lama ke sistem baru menggunakan model konversi langsung. Selain itu juga menggunakan konversi pilot. Pada studi ini dihasilkan suatu penemuan bahwa penggunaan *framework* ITIL v3 dan Van Grembergen *Framework* dapat saling berkolaborasi dalam mengembangkan suatu panduan dalm proses alih suatu sistem atau proses transisi suatu sistem. Studi ini mengelola dan memetakan berdasarkan prinsip kerja Van Grembergen. Setelah itu hasilnya akan yaitu suatu pemetaan yang dihasilkan dari framework Van Grembergen akan menjadi bahan kajian dan pertimbangan dalam menyusun tata kelola yang nantinya akan disusun menggunakan ITIL V3. Pada kajian ini hanya menggunakan domain *Service Transition* pada framework ITIL v3. Sehingga hasil penggunaan dua model tersebut dapat digunakan untuk mengembangkan struktur, proses, dan mekanisme relasional setelah proses transisi sistem dilaksanakan. Hal ini bermanfaat untuk cabang yang lain bila ingin malekaukan transisi dari satu

sistem ke sistem yang baru sehingga organisasi dapat menyesuaikan perubahan yang terjadi dari perpindahan suatu sistem ke sistem yang lain. Perubahan akan terus terjadi karena lingkungan juga berubah oleh karenanya organisasi harus terus melakukan perubahan karena apa yang dahulu kegiatan tersebut sukses dilakukan tetapi dengan adanya perubahan lingkungan saat ini organisasi harus dapat beradaptasi dari perubahan yang terjadi. Oleh karenanya organisasi apabila ingin unggul dibanding dengan kompetitornya maka harus mulai melakukan perubahan pada tujuan strategisnya sehingga dapat mencapai keunggulan yang menjadi tujuan organisasi tersebut (Wulandari & Buliali, 2019).

13.3.4 Studi pada Pusat Informasi dan Pangkalan Data Universitas

Studi keempat adalah mengukur tingkat kematangan suatu layanan Teknologi Informasi Pusat Informasi dan Pangkalan Data (PUSTIPANDA) UIN Jakarta menggunakan kerangka kerja ITIL v3. Pertumbuhan mahasiswa dan mahasiswi perguruan tinggi makin hari makin meningkat seiring dengan berjalannya waktu. Ini menyebabkan perguruan tinggi memerlukan kegiatan berbasis teknologi informasi. Keinginan setiap pengguna adalah mendapatkan layanan TI yang memuaskan. Agar layanan yang diberikan kepada pengguna dapat memuaskan seperti yang diinginkan oleh pengguna maka dibutuhkan ITSM (*Information Technology Service Management*). Pengelolaan layanan yang diberikan oleh pihak Pustipanda perlu diukur tingkat kematangannya agar diketahui kualitas layanan yang diberika oleh Pustipanda. Salah satu kerangka kerja yang dibutuhkan yaitu ITIL v3. Layanan teknologi informasi yang disediakan oleh Pustipanda yaitu Sistem Informasi Akademik, Surat elektronik dan internet diberlakukan sama

yaitu pada *service desk*, *incident management* dan problem *management*) (Romadhon, 2017).

13.3.5 Studi pada perusahaan *24Slides*

Studi ke lima ini adalah studi tentang evaluasi kematangan layanan teknologi informasi pada perusahaan multinasional yang bergerak dalam bidang *digital outsourcing* yang memberikan layanan kepada pelanggannya yaitu dengan melakukan *redesign* presentasi dalam bentuk powerpoint. Pada kegiatan operasional perusahan tersebut didukung dengan layanan berbasis internet yang dapat memudahkan perusahaan dalam melakukan kegiatan operasionalnya sehari – hari. Munculnya keinginan untuk melakukan melakukan evaluasi pada layanan TI perusahaan ini karena perusahaan ini sudah 7 tahun berdiri dan sudah saatnya untuk mendapatkan evaluasi. Selain itu ada jarak yang jauh yaitu antar benua untuk mengelola layanan TI diantara dua kantor di perusahaan tersebut. Pada studi ini dilakukan evaluasi terhadap domain *service operation*, setelah itu akan diukur tingkat kematangan kemudian melakukan analisis kesenjangan dan membuat atau memberikan rekomendasi untuk perbaikan perusahaan *24slides* agar memberikan layanan yang terbaik dikemudian hari. Hasil dari studi ini memberikan nilai kematangan atau *maturity* sebesar 2,6 dengan nilai kesenjangan sebesar 0,8. Hasil dari studi ini memberikan rekomendasi yaitu agar perusahaan dapat menjalankan seluruh proses dasar dan membuat dokumentasi dan standarisasi agar dapat mencapai level 3 (Febriant et al., 2019).

DAFTAR PUSTAKA

Baz, M. EL, Armand, M. M., Anong, C., & Mustapha, B. (2017). ITIL Implementation in a Moroccan Stat Organization: The case of incident management process. *International Journal of Advanced Engineering Research and Science*, *4*(4), 71–78. https://doi.org/10.22161/ijaers.4.4.8

Cartlidge, A., Hanna, A., Rudd, C., Macfarlane, I., Winderbank, J., & Rance, S. (2007). An introductory overview of ITIL V3. In *The IT Service Management Forum Limited*. https://doi.org/10.1080/13642818708208530

Febriant, A. B., Mursityo, Y. T., & Rachmadi, A. (2019). Evaluasi Maturity Level Manajemen Layanan Teknologi Informasi Menggunakan Framework Itil V3 Domain Service Operation Pada 24Slides Corporation. *Jurnal Pengembangan Teknologi Informasi Dan Ilmu Komputer*, *3*(6), 5608–5615.

Hakiem, N., Wardhani, L. K., Wahyu, F. N., Anggraini, N., Shofi, I. M., & Setiadi, Y. (2022). Whistleblowing System Deployment using ITIL v3 Framework: Evidence from a Public University in Indonesia. *Jurnal Sistem Informasi*, *18*(1), In Review.

Lubis, M., Annisyah, R. C., & Lyvia Winiyanti, L. (2020). ITSM Analysis using ITIL V3 in Service Operation in PT.Inovasi Tjaraka Buana. *IOP Conference Series: Materials Science and Engineering*, *847*(1). https://doi.org/10.1088/1757-899X/847/1/012077

Romadhon, A. (2017). Mengukur tingkat kematangan layanan IT dengan framework ITIL V3 (Studi kasus: PUSTIPANDA UIN Jakarta). *Jurnal.Atmaluhur.Ac.Id*, *3*, 152. http://jurnal.atmaluhur.ac.id/index.php/knsi2018/article/view/512

Wulandari, D., & Buliali, J. L. (2019). ITIL v3 and Van Grembergen Framework for System Transition Process. *IPTEK Journal of Proceedings Series*, *0*(5), 426. https://doi.org/10.12962/j23546026.y2019i5.6383

BIODATA PENULIS

Wahyuddin S, S.Kom., M.Kom
Dosen STMIK Amika Soppeng

Wahyuddin S. was born at Malaka-Bone-Sulawesi Selatan in 1992. In 2011 he attended STMIK Dipanegara Makassar and was completed in 2015. He was completed after attending 7 semesters and active on an XPcom (Extreme Programmer Computer) campus organization. He was also active as a lecturer assistant for three semesters and taught several courses on programming. He continued his Master of Information systems at UNIKOM Bandung in 2016 and was completed in April 2019. He worked as a lecturer at a campus (STMIK Amika Soppeng) 2019 to present and also a Freelance Web Programmer. Has competence in the field of software engineer, application developer, multimedia, web developer, network security, and data analyst.

BIODATA PENULIS

Muhammad Bobbi Kurniawan Nasution, ST.,M.Kom
Dosen Program Studi Teknik Informatika
Fakultas Teknik
Univa Labuhanbatu

Penulis lahir di Labuhanbilik tanggal 8 September 1985. Penulis adalah dosen tetap pada Program Studi Teknik Informatika, Fakultas Teknik, Universitas Al Washliyah Labuhanbatu. Menyelesaikan pendidikan S1 pada Jurusan teknik Informatika dan melanjutkan S2 pada Jurusan Teknologi Informasi. Penulis menekuni bidang Ilmu Komputer. Adapun judul buku yang sudah pernah diterbitkan adalah Bahasa Pemrograman Python, ISBN 978-623-6957-93-6, Penerbit Mitra Cendekia Media, Tahun 2021.

BIODATA PENULIS

Angga Aditya Permana
Dosen Program Studi Informatika
Universitas Multimedia Nusantara

Angga Aditya Permana (lahir pada Desember 1989 di Jakarta) dosen full time di bidang Computer Science pada Universitas Multimedia Nusantara sejak tahun 2021, fokus penelitian pada kriptografi, steganografi serta keamanan computer, namun pada tahun 2021 sedang mendalami topik bioinformatika dan network science. Angga juga memiliki hobi yaitu touring dan juga bermain bulutangkis, saat ini sedang menjadi mahasiswa program doctoral pada IPB University. Memulai karir pertama kali sebagai Network Enginner tahun 2011 dan memulai profesinya sebagai dosen pada 2013 di kampus swasta yang ada di Jakarta, pernah juga mengajar di kampus negri yang berada di Jakarta dan Tangerang, juga pernah di undang menjadi dosen tamu untuk mengenalkan bioinformatika di kampus negeri di Jakarta. Terimakasih.

BIODATA PENULIS

Ratna Dewi

Penulis Lahir 05 Oktober 1990 di Paya kolak Kecamatan Celala Kabupaten Aceh Tengah Pada tahun 2013 Penulis menyelesaikan Pendidikan S1 Di Sekolah Tinggi Teknik Harapan Medan. Dengan Jurusan SISTEM INFORMASI, kemudian setelah menyelesaikan S1 penulis mengajar di Sekolah SMK Kebangsaan Medan pada tahun 2013 sampai dengan 2016. kemudian di tahun 2018 Penulis Menempuh Pendidikan S2 TEKNIK INFORMATIKA di UNIVERSITAS PUTRA INDONESIA PADANG (YPTK). Dua tahun kemudian Penulis menyelesaikan studi S2 di prodi TEKNIK INFORMATIKA pada tahun 2019.

Di tahun 2020 penulis mengajar di Universitas Gajah Putih di daerah tempat tinggal saya kota Takengon Kabupaten Aceh Tengah. sampai saat ini saya masih menjadi Dosen Tetap. dan untuk mewujudkan karir sebagai dosen profesional, Penulis mulai aktif menulis meneliti dari bidang kepakaran tersebut yaitu tentang ilmu komputer. Harapan penulis ingin memberikan kontribusi positif bagi bangsa dan negara yang sangat tercinta ini.

Email Penulis: dewi90ratna90@gmail.com

BIODATA PENULIS

Decky Hendarsyah
Dosen STIE Syariah Bengkalis Riau

Penulis lahir di bumi minangkabau tepatnya di kota Bukittinggi Sumatera Barat, menghabiskan masa studi dari TK sampai dengan SMA di kota Padangpanjang Sumatera Barat. Kemudian melanjutkan studi pada program studi S1 Sistem Informasi di Universitas Putra Indonesia "YPTK" Padang Sumatera Barat pada tahun 1998. Sebelum melanjutkan S1 pernah menyelesaikan pendidikan program D1 Ilmu Komputer di Institut Pelatihan Komputer (IPK) di kota Bukittinggi. Tahun 2002 pernah bekerja sebagai staf IT di STAIN Batusangkar Sumatera Barat. Tahun 2003 hijrah ke bumi melayu tepatnya di kabupaten Bengkalis Riau. Tahun 2008 melanjutkan studi pada program studi S2 Ilmu Komputer di Universitas Gadjah Mada Yogyakarta. Sejak tahun 2003 sampai saat ini menjadi dosen tetap di STIE Syariah Bengkalis Riau, sekarang ditempatkan sebagai dosen tetap di program studi Manajemen Bisnis Syariah. Pernah menjadi dosen tamu di Politeknik Negeri Bengkalis Riau pada program studi D3 Teknik Informatika dan program studi D4 Teknik Mesin Produksi dan Perawatan dari tahun 2011-2016. Sejak tahun 2019 sampai saat ini, mulai aktif sebagai penulis, editor dan reviewer di beberapa jurnal nasional. Ketertarikan studi yaitu pada bidang ilmu komputer, sistem informasi, *crypthography*, *data and information security*, *steganography, e-commerce*, ekonomi digital, bisnis digital, digitalisasi, *big data*, *data science*, *machine learning* dan *artificial intelligence*.

Email: deckydb@gmail.com
Orcid: 0000-0002-7414-9145 | Google Scholar: hMtfejMAAAAJ
Web of Science: AAC-8741-2021 | Sinta: 6691366

BIODATA PENULIS

Adib Pakarbudi
Dosen Jurusan Sistem Informasi
Institut Teknologi Adhi Tama Surabaya

Penulis lahir di Bandar Lampung pada tanggal 11 November 1992. Penulis telah menempuh pendidikan jenjang S1 di Jurusan Studi Sistem Informasi Institut Teknologi Sepuluh Nopember. Pada tahun 2015 penulis berhasil menyelesaikan studi S1 dengan tugas akhir yang berjudul "Analisis Dampak Technostress Pada Pengguna E-Learning dengan Menggunakan Structural Equation Modeling". Pada tahun 2016 penulis melanjutkan pendidikan jenjang S2 di Program Magister Sistem Informasi, Institut Teknologi Sepuluh Nopember. Pada penelitian tesis ini, penulis mengambil konsentrasi Manajemen Sistem Informasi (MSI) dengan topik adopsi TI dengan objek E-Health. Saat ini penulis menjadi Dosen Jurusan Sistem Informasi di Institut Teknologi Adhi Tama Surabaya. Penulis telah menjadi dosen tetap sejak tahun 2019 hingga sekarang. Bidang minat penulis sesuai dengan penelitian semasa kuliah yaitu Manajemen Sistem Informasi. Kritik dan saran yang membangun dapat disampaikan melalui adib.pakarbudi@gmail. com.

BIODATA PENULIS

Yuliana Mose, S.Kom., M.Si.
Dosen Program Studi Sistem Komputer
Fakultas IPTEK & Keguruan Universitas Trinita

Penulis lahir di Cimahi tanggal 19 Juni 1975. Penulis adalah dosen tetap pada Program Studi Sistem Komputer, Universitas Trinita. Menyelesaikan pendidikan S1 pada program studi informatika dan melanjutkan S2 pada Jurusan manajemen SDM.

BIODATA PENULIS

Dr. Purnawarman Musa, S.Kom., M.T., M.I.Kom
Dosen Program Studi Teknik Elektro
Fakultas Teknologi Industri

Penulis lahir di Gorontalo pada tahun 1975 sebagi dosen tetap di Universitas Gunadarma, menyelesaikan pendidikan pada program studi *Electronic Image and Informatic* dengan gelar Doktor (Dr.) pada bidang Teknologi Infomasi dari Burgundy of University di kota Dijon, France pada tahun 2013. Penulis memperoleh gelar *Master of Engineering* (M.T.) tahun 2006 di Universitas Gunadarma Jakarta - Indonesia, gelar *Master of Communication* (M.I.Kom) tahun 2021 di Universitas Gunadarma, Jakarta - Indonesia dan tahun 1999 menyelesaikan pendidikan S1 jurusan *Computer Engineering* (S.Kom) di Universitas Gunadarma, Jakarta - Indonesia. Penulis menekuni bidang Robotika, IoT, Computer Vision, Kecerdasan Buatan, Remote Sensing dan Sistem Tertanam. Beberap keanggota penulis, diantarnya Ikatan Ahli Informatika Indonesia (IAII) dan Asosiasi Perguruan Tinggi Informatika dan Komputer (APTIKOM).

BIODATA PENULIS

Ade Maulana, S.Kom., M.T.I.
Dosen Program Studi Sistem Informasi
Fakultas Ilmu Komputer Universitas Pelita Harapan
Kampus Kota Medan

Ade Maulana lahir di Kota Medan. Ia tercatat sebagai lulusan Magister Teknologi Informasi Universitas Indonesia. Sebelumnya bekerja dibeberapa perusahaan pada bidang teknologi informasi, namun pada tahun 2020 lalu, memutuskan untuk menghabiskan sebagaian waktunya untuk mengabdi dalam pendidikan Sistem Informasi di Universitas Pelita Harapan kampus kota Medan

BIODATA PENULIS

Hermila A. S.SI., M.Pd.
Dosen Program Studi Pendidikan Teknologi Informasi
Fakultas Teknik Universitas Negeri Gorontalo

Penulis lahir di Polewali Mandar tanggal 25 Juli 1993. Penulis adalah dosen tetap pada Program Studi Pendidikan Teknologi Informasi Fakultas Teknik, Universitas Negeri Gorontalo. Menyelesaikan pendidikan S1 pada Jurusan Sistem Informasi STMIK Profesional Makassar dan melanjutkan S2 pada Jurusan Pendidikan Teknologi Kejuruan Kekhususan Pendidikan Teknik Informatika dan Komputer Universita Negeri Makassar. Penulis sekarang mulai menekuni bidang Menulis.

BIODATA PENULIS

Nurfitria Ningsi
Dosen Program Studi Sistem Informasi
Fakultas Teknologi Informasi Universitas Sembilanbelas November Kolaka Sulawesi Tenggara

Penulis lahir di Pulau Maginti tanggal 3 Mei 1990. Penulis saat ini merupakan dosen aktif dengan bidang minat Pengembangan Sistem Informasi, Tata Kelola dan audit SI/TI, Analisis dan Pemodelan Proses Bisnis, serta Smart Village pada Program Studi Sistem Informasi Fakultas Teknologi Informasi, Universitas Sembilanbelas November Kolaka.

Penulis Menyelesaikan pendidikan S1 pada Jurusan Pendidikan Ekonomi Akuntansi Universitas Haluoleo Kendari Sulawesi Tenggara kemudian melanjutkan studi S2 pada Jurusan Sistem Informasi Institut Teknologi Sepuluh Nopember Surabaya. Saat ini Penulis menekuni bidang Menulis dan Membaca.

BIODATA PENULIS

Iwan Adhicandra, S.T., M.Sc.
Dosen Program Studi Informatika
Universitas Bakrie

Penulis lahir di Jakarta tanggal 1 Desember 1974. Penulis adalah dosen tetap pada Program Studi Informatika, Universitas Bakrie. Menyelesaikan pendidikan S1 pada Jurusan Teknik Elektro bidang Teknik Telekomunikasi di Universitas Trisakti, dan melanjutkan S2 pada Jurusan Teknik Elektro bidang Komunikasi Data di University of Sheffield, Inggris. Penulis adalah Senior Member di Institute of Electrical and Electronic Engineers (SMIEEE).

BIODATA PENULIS

Elsy Rahajeng, S. Kom, M.T.I.
Dosen Program Studi Sistem Informasi
Universitas Islam Negeri (UIN) Syarif Hidayatullah Jakarta

Penulis merupakan lulusan Magister Teknologi Informasi Universitas Indonesia tahun 2008. Mengajar di Program Studi Sistem Informasi Universitas Islam Negeri (UIN) Syarif Hidayatullah Jakarta dari tahun 2010 sampai sekarang. Memiliki pengalaman menjadi anggota tim konsultan Teknologi Informasi di beberapa proyek pada Kementerian di Indonesia (2016 – sekarang). Pengalaman menjadi anggota tim penyusun borang akreditasi BAN PT Program Studi Sistem Informasi UIN Syarif Hidayatullah pada tahun 2012, 2017 dan tahun 2022. Anggota tim SAR (*Self Asessment Report*) AUN QA (ASEAN University – *Quality Assurance*) Program Studi Sistem Informasi UIN Syarif Hidayatullah tahun 2019.